Quest

KACE® Systems Deployment Appliance 9.3

Administrator Guide

Table of Contents

About the KACE Systems Deployment Appliance

The Quest KACE Systems Deployment Appliance provides a network-centric solution for capturing and deploying images. The appliance a seamless cross-platform imaging solution from a single Administrator Console enabling you to provision Microsoft® Windows® and Apple® Mac® platforms. You can deploy the configuration files, user states, and applications as an image to a single device or to multiple devices simultaneously.

The appliance provides the tools necessary to automate deployments in both homogeneous and heterogeneous hardware environments, and provides reliability of large-scale image deployments with multicast and task engine capabilities. The built-in driver feed automatically downloads Quest driver models, and the Package Management feature enables uploading third-party driver packages. You can also integrate the appliance with the KACE Systems Management Appliance to image the KACE Systems Management Appliance inventory. The KACE Systems Deployment Appliance is available as a virtual appliance.

To view information on this appliance, such as its serial number, associated Agent versions, and third-party licenses and open source copyrights, click the version number at the bottom left of the appliance *Dashboard* page.

Getting started

You can set up the appliance by connecting it to your network to configure the network settings from the initial configuration console. After you connect the appliance to your network, you can download the tools required to build a boot environment, change the default passwords, add drivers, and configure other deployment tasks.

Tasks for getting started using the appliance

You can install the appliance and configure the environment to prepare for operating system deployments.

Table 1. Tasks for getting started using the appliance

Task	How to
Install and set up the appliance	Connect the appliance to your network using a monitor and keyboard, and configure the network settings.
Log in to the Administrator Console	Open a web browser and enter the appliance URL: `http://appliance`**_hostname.** This enables you to enter the license key and register the appliance.
Secure your passwords	Change the default passwords. Although not a required task, Quest KACE recommends changing the default passwords during the initial appliance setup.
Dedicate a device as the administrator device	Ensure that you have administrator rights on the device where the appliance is installed.
Download the tools the appliance requires to build a KACE Boot Environment (KBE) or NetBoot environment	Download the Microsoft Windows ADK, the KACE Media Manager, and Microsoft .NET 4.
Create a KACE Boot Environment	Use the Media Manager to create the boot environment. The boot environment provides the drivers and tools to deploy the operating system.
Set a KBE as the default	Select a default boot environment to enable target devices to boot from the appliance.
Update drivers	Add the drivers that the KBE requires, and enable the Driver Feed for automatic updates of drivers.
Configure DHCP server	Set up the DHCP server to network boot target devices from the appliance.

Task	How to
Test the boot environment	Verify that the target devices can boot from the appliance.
Migrate user files and settings	Capture user profiles from a device using the Windows User State Migration Tool (USMT), version 5.0.
Upload operating system source files	Upload the OS source files to the appliance using the Media Manager.
Deploy the OS	Deploy the OS using a scripted installation or a system image deployment.

About the appliance components

The appliance components that support image deployments include a virtual appliance, a utility to build boot environments, a Support Portal, and a virtual Remote Site Appliance (RSA) to network remote boot devices.

The appliance has the following components:

Option	Description
Virtual appliance	The KACE Systems Deployment Appliance is available as a virtual appliance. It uses a VMware or Microsoft Hyper-V infrastructure. For technical specifications, visit https://support.quest.com/kace-systems-deployment-appliance/technical-documents.
Command-Line Console	The Command-Line Console is a terminal window interface to the appliance. The interface is designed primarily to configure the appliance network settings.
Administrator Console	The Administrator Console is the web-based interface used to navigate the appliance. To access the Administrator Console, go to `http://<appliance_hostname>/admin` where `<appliance_hostname>` is the host name of your appliance.
Support Portal	The Support Portal is the web-based interface that enables you to submit tickets to request help or to report issues. You can also to test network connectivity, and enable Quest KACE Technical Support to temporarily access your appliance to troubleshoot issues.
KACE Media Manager	A utility that builds boot environments, uploads the operating system source files, and provides access to the Windows User State Migration Tool (USMT) to upload user profiles the appliance.
Remote Site Appliance (RSA)	Uses the KACE Systems Deployment Appliance license to link a virtual Remote Site Appliances

Option	Description
	(RSA) that enables you to network remote boot devices. Remote Site Appliances are read only.

Log in to the Administrator Console

You can log in to the Administrator Console from any device on the local area network (LAN) after the network settings are configured, and after the appliance restarts.

The default administrator account is the only account on the appliance now. If you lose the password and have not enabled Quest KACE Technical Support access, the password can be reset by enabling SSH root login from the configuration screen and calling Technical Support.

1. Open a web browser and enter the appliance Administrator Console URL:

   http://**hostname**. For example, http://appliance.

   The *Initial Configuration Wizard* page appears.
2. In the *Initial Configuration Wizard*, choose the appliance mode by selecting one of the following options:
   - **Use as a KACE SDA**
   - **Use as a Remote Site Appliance**
3. Click **Next**.
4. Provide the following information:

Setting	Description
License Key	Enter the license key you received in the Welcome email from Quest KACE. Include the dashes. If you do not have a license key, contact Quest KACE Technical Support at https://support.quest.com/contact-support.
Administrator Password	Enter a password for the default admin account. You use this account to log in to the appliance Administrator Console. Remember this password; you cannot log in to the Administrator Console without it. **NOTE:** If you have multiple appliances, Quest KACE recommends using the same password for the admin account on all appliances. This enables you to link the appliances later.
Report User Database Password	Enter a database password that you want the external resources to use when accessing the appliance database. The indicator underneath the *Report User Database Password* field changes color as you type the password string, to indicate the password strength. Red indicates the lowest, and green the highest complexity level. Choose a strong password to prevent unauthorized users from accessing your database records. If you do not specify a password for the Report User, the programs querying the appliance use the

Setting	Description
	default password, which can allow attackers to expose sensitive data. A warning alert on the Home Dashboard appears, prompting you to change the database password.
Samba Password	Enter your Samba share password. The number of bars that appear below this field indicate the password complexity as you type. Choose a strong password to prevent unauthorized users from accessing your database records. A minimum of two bars is required to successfully specify the password.
Two-Factor Authentication	If you want to provide stronger security for users logging into the appliance, select **Enable Two-Factor Authentication**. This feature adds an extra step to the login process. It relies on an authenticator application to generate verification codes. The application generates a new six-digit code at regular intervals. When enabled, end users will be prompted for the current verification code each time they log in. For more details, see Enable Two-Factor Authentication. **NOTE:** If you enable this feature, ensure that appliance server's clock is accurate, as well as the device running the authenticator application. The application relies on current time to create the token. If server's clock is not synchronized with those of the devices running the application, token validation may fail, which may result in account lockouts.
Registration Data	Enter the name of your company or group and the email address of the person or group that you want to receive logs and notifications from the appliance.
Network Connectivity	The KACE Systems Deployment Appliance must be connected to the network to validate the license information.
Default Appliance Theme	The default color theme for the appliance. The Light theme is the default, but you can select the Dark or Hybrid theme, as required. Users can also associate different themes with their account, if the default appliance theme does not suit their needs. For more information, see the *Administrator Guide*.
Time Zone	Select the time zone where the appliance is located. The browser's time zone is selected by default.

5. **Optional**. If you change your mind, and want to switch to the KACE Systems Deployment Appliance or RSA (Remote Site Appliance) mode, click **Change virtual appliance mode**, and select the appliance type.

IMPORTANT: Once you configure and reboot the appliance, you cannot switch to the other virtual appliance mode.

6. Click **Save Settings and Continue**.
7. On the *Data Storage* page that appears, review the provided information and indicate where you want to store data collected by the appliance by selecting one of the following options, as required:
   - **On the virtual appliance (onboard storage)**
   - **To this offboard storage device: Virtual Disk**
8. Complete one of the following steps.
   - To complete the configuration, click **Configure, then reboot appliance**. The appliance restarts. Proceed to the next step.
   - If you do not want to finish the configuration, click **Power off appliance**. The appliance powers off.
9. When the appliance restarts, refresh the browser page.
10. Accept the STA (Software Transaction Agreement), also known as EULA (End User License Agreement), then log in using the login ID admin and the password you chose on the *Initial Configuration* page.
11. **Optional**. Select a theme for the Administration Console for your user account. It appears in the default **Light** theme. If the default theme seems too bright, you can use a different theme, as needed.
    - To choose a different theme, in the top-right corner, click your user name, then click **Select Theme**, and choose **Hybrid** or **Dark**, as needed. The theme you select this way becomes associated with your user account and is applied each time you log in. You can also configure the default theme for the appliance. For more information, see Change a default theme for the appliance.
    - To switch back to the **Light** theme, choose **Select Theme** > **Light**.

NOTE: Reports always appear with a white background, regardless of which theme is selected.

When you complete the configuration, logging in to the KACE Systems Deployment Appliance allows you to access the full set of pages available in the Administrator Console. The Remote Site Console, however, provided with the RSA, provides a limited set of pages that are only applicable to the RSA mode. For example, the Remote Site Console only displays the *Home*, *Settings*, and *Support* menu options on the left navigation pane, that provide access to the relevant pages.

Filter lists and search for information

The Administration Console provides a set of configuration, detail, and list pages. You can filter and search lists, as needed.

List pages allow you to look through a collection of related items, and to drill down on a specific item, to find out specific information about that item on a detail page, or to make changes to it, as applicable.

For example, the *Boot Environments* page displays a list of KACE Boot Environments (KBEs) and NetBoot environments uploaded or imported to the appliance. This page allows you display only the boot environments that use specific operating systems, or to search by the KBE name.

1. Log in to the Administrator Console.
2. Go to a list page. For example, on the left navigation bar, choose **Deployments** > **Boot Environments**.
3. Search for a specific text string on the list page.
   1. In the top-right corner of the page, in the *Search* field, type the search text.
   2. Press Enter or Return to begin the page-level search.

The list page displays only those items that contain the specified text string.

4. Filter the list based on a specific criteria.
   - At the top of the page, on the right of *View By*, click the selected option, and choose a specific criteria, as required. For example, on the *Boot Environments* page, to look for boot environments that use the 64-bit Microsoft Windows OS, choose **Operating System** > **KBE (Windows x64)**

   The list page displays only those items that satisfy the selected criteria.
5. **Optional**. To ensure the list displays the latest information, you can set the Auto Refresh settings for each list page. This is useful when the contents of the list are expected to change as you are reviewing it.

   NOTE: The Auto Refresh settings are disabled by default. Each user can have their own Auto Refresh settings for the different list pages.

   - At the top of the page, on the left of *View By*, click **Auto Refresh**, and indicate how you often you want to refresh the page. For example, to update the page every 15 seconds, choose **Auto Refresh** > **Every 15 Seconds**.

Access product documentation

The Administrator Console provides access to help contents and documentation search. It also allows you to browse related Knowledge Base articles, and to chat with product specialists, when needed.

1. Log in to the Administrator Console.
2. On the right of the Administrator Console, in the top-right corner, click **Need Help**.

   A help pane appears on the right containing high-level information about the related Administrator Console page. The bottom of the help pane includes the following buttons:
   - : Provides access to the KACE Systems Deployment Appliance help contents.
   - : Allows you to browse the Knowledge Base articles associated with the related page.
   - : Starts a chat with a KACE Systems Deployment Appliance product specialist.
   - : Links to the Support page (https://support.quest.com/create-service-request) that allows you to create a service request.
   - : Links to the **Settings > Support** page. This page provides resources for troubleshooting system management issues and contacting Quest Support.
   - : Displays information about your KACE Systems Deployment Appliance installation.
3. Click a link in the page-level Help topic.

   The main Help system appears, displaying the selected topic.
4. Click the **Search** tab in the left pane of the Help system.

   All search terms use an implicit Boolean AND statement. For example, if you search for **Windows provisioning**, Search displays results that contain both words.

   Tip: **TIP:** For a PDF version of the Help system, click the Acrobat button on the right side of the main Help system navigation bar ( ).
5. Search for Knowledge Base articles associated with the related page.
   a. At the bottom of the help pane, click .

   The help pane displays a list of the Knowledge Base articles associated with the page you are viewing in the Administrator Console.

NOTE: Knowledge Base articles are currently only available in English.

b. Use the navigation buttons to look for a specific article.

c. In the search field, type a keyword and press **Enter**. The search string must be at least three characters long.

The search returns a list of all KACE Systems Deployment Appliance Knowledge Base articles containing the specified keyword, including the articles that are not related to the page you are viewing. To see only the articles related that page, clear the search field and press **Enter**.

d. When you find a desired article, click the link in the help pane.

The selected Knowledge Base article appears on a new tab in your browser.

IMPORTANT: To see the article contents, you must log in to the Quest Support site using your Quest user name and password.

6. Chat with a product specialist.

NOTE: This feature is only available when the appliance has active maintenance.

a. Click .

The *Chat with Support* dialog box appears.

b. Type your *Full Name*, *Email Address*, and *Purpose of your Chat*, as applicable, and click **Start Chat**.

The *Chat with Support* dialog box refreshes, showing a list of existing Knowledge Base (KB) articles that may contain information about the specified topic. The list of topics may appear on multiple pages, depending on the type of the requested information.

c. Review the list of KB articles. Use the page navigation controls at the bottom of the list, if applicable. To read a KB article, click the title in the list.

d. If none of the listed KB articles provide the information you need, click **None of the solutions above solved my issue, continue with chat**.

NOTE: You can only use this feature when product specialists are available to respond to your questions. If Live Chat is not available, this is indicated in the dialog box.

The *LIVE CHAT* dialog box appears. The *Full Name*, *Email Address*, *Product* and *Purpose of your Chat* boxes are populated using the information specified in the *Chat with Support* dialog box.

e. Click **Start Chat**.

The *LIVE CHAT* dialog box refreshes.

f. In the *LIVE CHAT* dialog box, type your question, and click **SEND** to start chatting with a product specialist.

7. Open a Support ticket.

a. Click .

Your browser displays the *Submit a Service Request* page (https://support.quest.com/create-service-request) in a new tab or window.

b. Use this page to open a service ticket, as required.

8. Click .

The **Settings > Support** page appears. This page provides resources for troubleshooting system management issues and contacting Quest Support.

9. Review information about your KACE System Deployment Appliance installation.

a. Click .

A dialog box displaying product information appears.

b. To close it, click **Close**.

10. To close the help pane, click **Need Help**.

Configure the language settings

The appliance supports several locales. The Administrator Console and online help can be displayed in English, French, German, Japanese, Portuguese (Brazil), and Spanish. You can set the language used in the UI and in your KACE Boot Environment (KBE) for Windows. You can configure the region settings to determine the default character set to use for numbers such as dates.

1. On the left navigation pane, click **Settings** to expand the section, then click **Language Settings** to display the *Language Settings* page.

   NOTE: Regional settings for scripted installations must match the language of the scripted installation source media; otherwise, messages do not display in the correct language.

2. In the *Language* drop-down list, select a locale for the language to use for the text in the appliance console.

   If you select the **Default** option, the Administrator console will match the language of the browser.

3. In the *Region* drop-down list, select the locale to determine the default character set to use for numbers such as dates.
4. **Optional**: Click **Cancel** to close the page.
5. Click **Save**.

NOTE: Media Manager automatically adds Asian fonts into the boot environment.

The selected language is applied. Administrators who log in to the Administrator Console see the localized version if the target language was also selected in the browser settings.

Change a default theme for the appliance

In a default installation, the Administration Console appears in a default Light theme for every user that logs in. You can change the default theme for the appliance, and any available RSAs, if needed. For example, if your account is configured to display the Dark theme, and the appliance uses the Light theme, the login screen uses the white background.

1. On the left navigation pane, click **Settings** to expand the section, then click **General Settings**.
2. On the *General Settings* page that appears, under *Themes*, click **Default appliance theme**, and choose one of the following options: **Light**, **Hybrid**, or **Dark**.

   When you choose the **Light** or **Hybrid** theme as the default appliance theme, the login page appears with a white background. A dark background is applied when the **Dark** theme is applied as the default appliance theme. The color of the login screen always reflects the configured appliance theme, not the theme associated with your user account. For example, if you choose the Dark theme in the Administration Console, this theme becomes associated with your user account and is applied each time you log in. However if the appliance uses the Light theme by default, your login screen always appears with a white background. After a successful login, the Dark theme is applied.

   NOTE: Reports always appear with a white background, regardless of which theme is selected.

NOTE: For newly created users, the Administration Console uses the default theme. This can be changed on the next login. For more information, see Log in to the Administrator Console.

3. **Optional**: Click **Cancel** to close the page.
4. Click **Save**.

The default theme is applied. Users can also associate a different theme with their account, if the default appliance theme does not suit their needs. For more information, see Log in to the Administrator Console.

Using the Dashboard

The *Dashboard* provides an overview of the appliance activity, links to common tasks, and the Library resources. It also provides alerts and links to news and Knowledge Base articles. You can customize the *Dashboard* to show or hide widgets as needed.

Customize the Dashboard

You can customize the *Dashboard* to add widgets as needed.

1. Log in to the KACE Systems Deployment Appliance Administrator Console.
2. On the left navigation pane, choose **Home** > **Dashboard**.
3. On the Dashboard, mouse-over the widget, then use any of the following options.
   - **Refresh the information in the widget.**
   - **Display information about the widget.**
   - **Hide the widget.**
   - **Drag the widget to a different location on the page.**
   - **Resize the widget.**
4. Click the **Customize** button in the top-right corner of the page to view the available widgets.
5. Click **Install** to show a widget that is currently hidden.

Configuring the appliance

The initial appliance network settings require a monitor and keyboard. After you connect the appliance to your network, you can change the default passwords, link appliances, aggregate links, set the data sharing preferences, and other settings.

Configure the initial network settings

You can configure the network settings for the appliance from the appliance Network Setup Console after you connect a monitor and keyboard directly to the appliance and after the appliance's first boot.

Configure the network settings for the Virtual appliance from the Virtual KACE Systems Deployment Appliance Administrator Console, and configure the RSA from the virtual RSA Administrator Console.

1. Connect a monitor and keyboard directly to the appliance.
2. Power on the appliance. The first-time startup takes 5 to 10 minutes.

   The login screen appears.
3. At the login prompt, enter konfig for both *Login* and *Password*.
4. Choose the language to use for the console. Use the up- and down-arrow keys to move between fields.
5. Configure the following network settings. To select options in a field, use the right and left-arrow keys; to move between fields, use the up- and down-arrow keys.

Field	Description
Host Name	Enter the host name of the appliance. The default is k2000.
Domain Name	Enter the domain the appliance is on. For example, example.com.
IP Address	Enter the static IP address of the appliance.
Network Speed	Select the speed of your network. This speed should match the setting of your LAN switch. If you select *Auto-negotiate*, the system determines the best value automatically provided that the LAN switch supports auto-negotiation.
Default Gateway	Enter the network gateway for the appliance.
Subnet Mask	Enter the subnet (network segment) that the appliance is on. For example, 255.255.255.0.
Primary DNS	Enter the IP address of the primary DNS server the appliance uses to resolve host names.
Secondary DNS	**Optional**: Enter the IP address of the secondary DNS server the appliance uses to resolve host names.

Field	Description
Proxy	**Optional**: Enter proxy server information. **NOTE:** The appliance supports proxy servers that use basic, realm-based authentication requiring usernames and passwords. If your proxy server uses a different authentication type, add the appliance's IP address to the proxy server's exception list.
Save appliance data	The *Save appliance data* setting enables you to save the appliance data to an offboard virtual disk during the initial configuration for a new Virtual appliance and a new Remote Site Appliance. You can also configure offboard storage later for the virtual KACE Systems Deployment Appliance and RSA using the Administrator Console. The *Save appliance data* setting is not available for the physical KACE Systems Deployment Appliance during the initial configuration. Configure the physical appliance to save the appliance data to an offboard-storage device from the Administrator Console. Select one of the following check boxes: • On the virtual appliance (onboard storage) • To this offboard-storage device (Virtual disk) **NOTE:** You can only have one virtual disk connected.

6. Use the down-arrow key to move the cursor to **Save**, and then press **Enter** or **Return**.

   The appliance restarts.
7. Connect a network cable to the port indicated:

Modify the initial network settings

You can modify the initial network settings configured from the appliance Network Setup Console.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Network Settings** to display the *Network Settings* page.
2. Configure the following network settings:

Field	Description
Host Name	Enter the host name of the appliance. The default is k2000.
Domain Name	Enter the domain the appliance is on. For example, example.com.

Field	Description
Primary DNS	Enter the IP address of the primary DNS server the appliance uses to resolve host names.
Secondary DNS	**Optional**: Enter the IP address of the secondary DNS server the appliance uses to resolve host names.
Default Gateway	Enter the network gateway for the appliance.

3. Under *Interface Settings*, configure the following settings for each interface, as required.

Option	Description
Interface	Read-only field. It displays the name of the interface.
IP Address	Enter the static IP address of the interface.
Network Speed	Select the speed of the interface. This speed should match the setting of your LAN switch. If you select *Auto-negotiate*, the system determines the best value automatically provided that the LAN switch supports auto-negotiation.
Netmask	Enter the subnet (network segment) that the interface is on. For example, 255.255.255.0.
MTU	Enter the maximum transmission unit (MTU) of the interface. MTU represents the size of the largest protocol data unit (PDU) that can be communicated in a single-network layer transaction. Consider your hardware and network specifications when configuring this option. The recommended range is from 1500 to 9000, as applicable to your network specifications.
Status	Read-only field. It indicates if the network cable is plugged into the interface.
Deployment Interface	Select this option if you want this interface to be used as a deployment interface.

4. Under *Available Link Aggregation Interfaces*, configure or enable the available interfaces. Link aggregation allows you to combine multiple network interfaces to increase throughput beyond what a single connection can sustain, and to provide redundancy in case a link fails. You can aggregate up to eight network interfaces.

Option	Description
Interface	Read-only field. It displays the name of the link aggregation interface.
IP Address	Enter the static IP address of the link aggregation interface.
Netmask	Enter the subnet (network segment) that the link aggregation interface. For example, 255.255.255.0.
Broadcast	Read-only field. It displays the broadcast address of the link aggregation interface.
Members	Read-only field. It displays the names of network interfaces belonging to this link aggregation interface.

Option	Description
Enabled	Select this option if you want to enable this link aggregation interface. If enabled and the primary/deployment interface is associated with this link aggregation interface, it becomes the primary interface. Each enabled link aggregation interface appears listed under *Active Link Aggregation Interfaces*.

5. **Optional**: Select the *Enable On-board DHCP Server* check box.
6. **Optional**: Select the *Enable NetBoot Server (for Mac OS X clients)* check box.
7. **Optional**: Select the *Use Proxy Server* check box.
8. Click **Save**.

Changing the default passwords

Quest KACE recommends changing the default passwords during the initial setup of the appliance for the administrator, the appliance Samba share directory, and the Boot Manager.

The following passwords are associated with the appliance.

Password	Description
Administrator	The default password is admin. The new password must be six characters or more in length.
Samba Share Password, KACE Media Manager, and KACE Boot Environment (KBE) **NOTE:** All use the same password.	The default password is admin and is used for uploading drivers and backing up and restoring library components, scripted installations, system images, boot environments, network inventory, and network scans. **NOTE:** The *KACE SDA Hostname* field on the KACE Media Manager requires this password.
Boot Manager	By default, Boot Manager authentication is disabled. The Boot Manager contains a bootstrap file that the Windows client Boot Manager downloads during the initial device PXE boot in to the KACE Boot Environment. The Boot Manager interface displays on the target device.
VNC	Enables a connection to a target device that has networked booted.
NetBoot	Used only for Mac devices.

NOTE: Only 7-bit ASCII characters are accepted for KBE remote VNC passwords.

Use the Command Line Console to reset the Administrator's password

If you change the Administrator's password, and become locked out of the appliance **Administrator Console** for some reason, you can re-set the password using the **Command Line Console**.

To change the Administrator's password, you must obtain last 16 characters of your appliance license key, including dashes, using the correct case, as specified. You can use the legacy KACE license key or the Quest license key. The Command Line Console is a terminal window to the appliance. Logging in to the Command Line Console as the `netdiag` user provides access to some basic network diagnostic commands, including `reset_admin_password`, that allows you to change the Administrator's password.

Your full license key is listed in the *Welcome* email from Quest KACE. It is also available on the *Registration and Licensing* page in the Administrator Console (when you have access to it). If you do not have a license key, contact Quest KACE Technical Support at https://support.quest.com/contact-support, or the licensing team to obtain a new key at https://support.quest.com/licensing-assistance. For more information about the *Registration and Licensing* page, see the help topic associated with this page.

Tip: **TIP:** You can access product documentation and additional resources associated with a specific page by clicking **Need Help**. For more information, see Access product documentation.

1. If you have a physical version of the appliance:
    a. Connect a monitor and keyboard directly to the appliance.
    b. Connect a network cable to the port indicated:

    

    c. Power on the appliance.

    The Command Line Console login screen appears on the monitor connected to the appliance.
2. If you have a virtual version of the appliance, power on the virtual machine to boot the appliance.

    The Command Line Console login screen appears.
3. At the prompts, enter:

    Login: `netdiag`

    Password: `netdiag`

    A list of network diagnostic commands appears, including `reset_admin_password`, that allows you to change the Administrator's password.
4. At the command-line prompt, type `reset_admin_password`.
5. When prompted, type the last 16 characters of your license, including dashes. You must use the correct case.

    A message appears, indicating your new password consisting of six characters enclosed in quotation marks. For example:

    ```
    The admin password has been reset to "GTYKpa". Please login immediately and set a more secure password.
    ```
6. Record your new password.
7. Log in to the appliance Administrator Console with your newly changed password.
    a. Open a web browser and navigate to the appliance Administrator Console URL using the following syntax: `http://<host_name>`.

Where `<host_name>` is the name or IP address of the physical or virtual machine on which the appliance is running.

b. In the *KACE Systems Deployment Appliance Administrator Console* login screen, type the following values:

- *Login ID*: `admin`
- *Password*: Type the six characters of your newly changed Administrator's password (not including the quotation marks).

c. Click **Log In**.

The appliance Administrator Console appears, showing the *Dashboard* page.

8. For security purposes, change your Administrator's password. It is recommended use a combination of lowercase and upper case letters, numbers, and symbols in the password. You can update your password on the *User Detail* page. For more information, see Add or edit local administrator accounts.

Change the Samba share password

You can change the Samba share password for the KACE Systems Deployment Appliance or Remote Site Appliance. The Samba share `drivers` and `restore` directories are for uploading drivers and backing up and restoring library components, scripted installations, system images, boot environments, network inventory, and network scans. The `clientdrop` share is for uploading larger files in application tasks.

NOTE: The default account name is `admin` and the default password is also `admin`.

1. **KACE Systems Deployment Appliance only**.
   a. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **General Settings** to display the *General Settings* page.
   b. Under *Server Options*, in *SDA Samba Share Password*, enter a new password.
2. **Remote Site Appliance only**.
   a. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Remote Site Settings** to display the *Remote Site Settings* page.
   b. Under *Samba Options*, in *SDA Samba Share Password*, enter a new password.
3. If your Samba shares are located on a Windows system that uses NTLM (NT LAN Manager) v.1, you must also enable NTLM v.1 configuration in order to access these directories. To do that, select **Enable NTLMv1 in Samba configuration**.
4. Click **Save**.

The account password for the Samba share is changed. Your Windows KACE Boot Environments are updated automatically to include the new password. This process may take a few minutes for each KBE.

Set the VNC® password

The KACE Boot Environment (KBE) includes a Java® VNC client that enables you to connect to and boot remote devices from the KACE Systems Deployment Appliance and the Remote Site Appliance. When you create a NetBoot environment on a Mac OS X® device, the VNC password gets stored in the Mac OS X NetBoot environment.

1. **KACE Systems Deployment Appliance only**.
   a. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **General Settings** to display the *General Settings* page.
   b. Under *Boot Environment Options*, in *VNC Password*, type a password.
2. **Remote Site Appliance only**.

a. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Remote Site Settings** to display the *Remote Site Settings* page.
b. Under *Boot Environment Options*, in *VNC Password*, type a password.

3. Click **Save**.

The next time a device boots from the appliance, it uses the new VNC password to connect.

Enable Boot Manager authentication

The KACE Boot Manager displays on a target device that has PXE booted from the appliance. Boot Manager authentication prevents users from manually selecting a KBE without authenticating with appropriate user credentials. By default, Boot Manager authentication is disabled.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **General Settings** to display the *General Settings* page.
2. Under *PXE Options*, select **Enable Boot Manager Authentication** and provide the Boot Manager user name and password.

   NOTE: The default Boot Manager password is admin.

3. Click **Save**.

The Boot Manager user name and password are set for all PXE boot requests. Active sessions use the previous password if authentication was previously enabled.

Add custom background image to iPXE console

Your iPXE console can be configured to include a background image of your choice.

You can upload a PNG, JPG, JPEG, BMP, or GIF file. The appliance converts the uploaded graphic file to the PNG format. The required image size is 1024 by 768 pixels, any other size is automatically scaled to the required size. If an RSA is linked then a sync will need to be performed to copy the image to the RSA.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **General Settings** to display the *General Settings* page.
2. Under *PXE Options*, select **Use custom background image**, and specify the desired image file either by selecting the file or dragging and dropping it in to the designated area.

   NOTE: Clearing this option reverts the background image to the default KACE® logo.

3. Click **Save**.

Configuring the appliance date and time settings

Appliance deployment operations, scheduled backups, exports, and offboard transfers rely on the date and time of the system clock. By default, the appliance system clock is set to synchronize with the Quest KACE time server. You can change the system clock settings to match your time zone.

Configure the date and time

The appliance logs deployment operations based on the date and time of the appliance system clock. You can set the system clock to match your timezone to prevent unexpected behavior, such as running resource-intensive backups during high network activity.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Date and Time Settings** to display the *Date and Time Settings* page.
2. Specify the following settings:

Option	Description
Timezone	Select a timezone in the drop-down list.
Time Setting	Select an option: • **Automatically synchronize with an Internet time server**. Use an Internet time server. If you select this option, provide the server web address in the *Server* field. • **Set the clock on the appliance manually**. Set the appliance clock manually. Specify the time and date in the drop-down lists. The *Hour* drop-down list uses a 24-hour clock format.
Time Server	Use an Internet time server to set the appliance time. Enter the web address of the time server in the text box. For example: **time.example.com**. By default, the system clock is set to synchronize with the Quest KACE time server. **NOTE:** You can look up the time servers available for your system clock synchronization process using the NIST Internet Time Servers at http://tf.nist.gov/tf-cgi/servers.cgi.

3. Click **Save**.

   The web server restarts, and the settings are applied.

During the restart, active connections might be dropped. When changes are saved, the page automatically refreshes after 15 seconds. After the appliance web server restarts, the updated date and time appear in the bottom right of the Administrator Console.

Manage files on the appliance

The appliance comes with a Filesystem Manager, that allows you to manage files and directories on the appliance.

Use the *Filesystem Manager* page to easily view the file system contents, and add files or directories into the applicable locations, such as the `petemp`, `drivers`, `restore`, `drivers_postinstall`, and `clientdrop` directories.

NOTE: This page does not allow you to download files from the appliance file system.

1. On the left navigation pane, click **Tools** > **Filesystem Manager** to display the *Filesystem Manager* page.
2. On the *Filesystem Manager* page, under *Current Directory*, navigate to the directory where you want to make changes.

   For example, to add files or directories to the post-installation drivers directory, navigate to `/peinst/drivers_postinstall`.

   NOTE: You can only make changes to selected directories. If you navigate to a read-only directory, such as `peinst`, this is indicated on the page.
3. To add a directory, under *Actions*, in the *Directory Name* field, type the directory name, and then click **Add Directory**.
4. To add a file, under *Actions*, complete the following steps:

   NOTE: Some directories, such as `/peinst/drivers/*/`, allow automatic extraction of .zip, .cab, and .msi files. A note appears on the page when you navigate to the applicable directory.

   a. Complete one of the following steps:

   - Click **Select file**, and navigate to the file that you want to add.
   - Drag and drop the file into the indicated location.

   b. Click **Upload File**.
5. To delete a file or a directory, click the trash icon on the right of the file or directory name.

   NOTE: You can only delete an empty directory.

Configure email notifications

You can configure the appliance to send email notifications using an SMTP server.

The *Notifications* page allows you to specify SMTP server settings, and includes a set of email notification templates that you can edit or disable, as required.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Notifications**.
2. On the *Notifications* page, click **Email Notifications**.
3. On the *Email Notifications* tab, in the *SMTP Settings* section, choose one of the following options:

Option	Description
Use Onboard SMTP Server	Select this option if you want to use the internal SMTP server that exists on the appliance.
Use Offboard SMTP Relay	Select this option if you want to send authenticated email through an external SMTP relay. An SMTP relay allows you to route email traffic using a third-party mail server. • **Relay Host**. Type the fully qualified domain name of the SMTP relay host.

Option	Description
Use Offboard SMTP Server	Select this option if you want to use an external SMTP server, and specify the following settings: • **Username**. Type the email address of an account that has access to the external SMTP server, such as `your_account_name@gmail.com`. • **Password**. Type the password of the specified user account. • **Host**. Specify the host name or IP address of an external SMTP server, such as `smtp.gmail.com`. External SMTP servers must allow anonymous (non-authenticated) outbound email transport. Ensure that your network policies allow the appliance to contact the SMTP server directly. In addition, the mail server must be configured to allow the relaying of email from the appliance without authentication. If you specify an IP address, enclose the address in brackets. For example [10.10.10.10]. • **Port**. Enter the port number to use for the external SMTP server. For standard SMTP, use port 25. For secure SMTP, use port 587 (this is the default value). • **Encryption**. Click and select the encryption type that you want to use, as required: **None (Insecure)**, **TLS**, **TLS with Self-Signed Certificate (Insecure)**, **SMTPS**, or **SMTPS with Self-Signed Certificate (Insecure)**. To test your configuration, in the *Test Recipient* field, type your email address, and click **Send Test Email**. After a successful configuration, the appliance sends an email to the specified email address, with *Test Email from KACE Systems Deployment Appliance* as the subject.

NOTE: If you leave any of these fields empty, and attempt to save your changes, a notification appears next to each field that requires input.

4. In the *Notification Templates* section, review the list of available templates.

Option	The appliance sends this notification when..
Appliance Upgrade Available	An upgrade is available for your version.
Appliance Upgrade Completed	An upgrade is successfully installed.
Appliance Upgrade Failed	An upgrade started, but the installation failed.
Remote Site Appliance Sync Completed	A Remote Site Appliance (RSA) synchronization is successfully completed. If you have multiple RSAs, this notification is generated for each remote appliance.
Remote Site Appliance Sync Failed	A Remote Site Appliance (RSA) synchronization started, but it did not complete due to a failure. If you have multiple RSAs, this notification is generated for each remote appliance.
Driver Feed Updates Digest	A list of drivers that are new, updated, installed and updated, and automatically updated drivers that are already installed.
Deployment Started Digest	A deployment process starts. The notification includes a list of all applicable provisioned devices.

Option	The appliance sends this notification when..
Deployment Completed Digest	A deployment is successfully completed. The notification includes the deployment start and end times, followed by a list of all applicable provisioned devices.
Scheduled Exports Digest	A scheduled package export is successfully completed. The notification includes a list of all exported packages.
Daily Appliance Status Digest	Detailed appliance information, sent on a daily basis. The notification includes the appliance maintenance status, support expiration date, the amount of time the appliance was in use, memory, storage, and network details, deployment activity, any linked RSA connection and update data, and a link to the detailed report.
Nightly Update Notifications	Details about nightly updates such as the driver feed version, driver feed revision, and the update status of each the following items: get/set computer name task, Media Manager, and KACE Image Prep.

5. **Optional**. To change the appearance of the email contents, at the top of the *Notification Templates* section, under *Email Styles*, click **Show**, and in the field that appears, change the CSS style settings, as required. For example, you can change the text fonts, background color, or sizes, as applicable.
6. If you want to edit a template, complete the following steps:
    a. In the *Notification Templates* section, in the row containing the template that you want to edit, in the **Actions** column, click the Edit Template button.
    b. In the email template dialog box that appears, make your edits, as applicable.

Option	Description
Email Subject	The subject of the email. You can use plain text or template variables, as required. You can use one or more template variables listed in the *Template Variables* field on the right. For more information about the template engine, click the link below the *Template Variables* field.
Recipients	One or more recipients the email is sent to. If any user emails are created on the appliance, they appear in the drop-down box as you start typing.
Email Body	The content of the email. The template uses a combination of template code, plain text, and template variables. See the *Template Variables* field for reference. **NOTE:** The following line appears at the very beginning of the email body: `{{appliance_email_styles|raw}}`. Do not remove or change that line, otherwise the text formatting defined in the *Email Styles* section will not be applied to sent emails.
Enable Notification	To enable an email template, ensure this check box is selected.

    c. Click **Save** in the dialog box. Alternatively, to discard your changes, click **Revert to Default**.

    The dialog box closes.

    d. To test the template, in the *Notification Templates* section, in the row containing the template that you want to edit, in the **Actions** column, click the Test Template button.

    An email is sent to each recipient specified in the template. The names of any variables specified in the template appear in uppercase characters. They are not replaced with actual values because the related actions (such as deployments) did not take place when the test email is sent.
7. On the *Notification* page, click **Save**.

Configure User Interface notifications

You can configure the appliance to display notifications in the Administrator Console when certain types of manual tasks are performed.

Administrators can configure the notification groups and users for which notifications are generated. A notification bell icon is located in the top-right corner of the screen. When new notifications are available, an orange indicator appears.

User Interface notifications are enabled for administrative accounts by default, all other users must subscribe to them if they want to make the notifications visible. Use the bell icon to show or hide the *Notifications* pane on the right. Each notification has a time stamp. You can delete individual notifications by clicking the Delete icon in the top-right corner of each entry in the list. To clear the list of notifications, click **Dismiss All**.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Notifications**.
2. On the *Notifications* page, click **UI Notifications**.
3. If you want to delete all notifications after a certain time period, click **Auto Delete Notifications After**, and select the desired number of days. The default setting is *Never*, which preserves all notifications, and is a good option for administrators. For users that do not log in as often, you can choose to delete them after a certain period. Choose from the existing options, or select *Custom* and type the applicable number of days.
4. On the *UI Notifications* tab, review the groups of notifications that you can configure:

Group	Description
Source Media Notifications	These notifications appear when: • The upload of source media is completed in Media Manager or using the *Source Media Import* page. • The appliance imports the KACE Boot Environments (KBEs), source media or USMT (Microsoft Windows User State Migration Tool) files. • A Windows Imaging Format (WIM) file is imported using the *System Image Import* page on the appliance. • A USB system image installation is created. • The Samba share password is changed and updated in all KBEs.
Offboard Storage Notifications	These notifications inform users when offboard storage is enabled or disabled.
Driver Feed Notifications	These notifications are displayed when a user manually installs or removes one or more a drivers from the driver feed. The notification reflects the operation outcome, indicating a success, failure, or error.
RSA Notifications	These notifications appear when a new RSA (Remote Site Appliance) is added to the Systems Deployment Appliance.
Deployment Notifications	These notifications show up to indicate a successful completion of a manual deployment or a failure (as applicable). Success notification include a link to the manual *Deployment Details* page, and a failure notification link to the *Manual Deployment Progress* page.

Group	Description
Package Management Notifications	These notifications are displayed to indicate the state of the package import or export, such as the operation start, end, import or export failure, file corruption, invalid contents, state of a manual package import or export, and so on.

5. Review the information available in columns for each notification group:

Option	Description
Recipients	A list of all users that receive notifications associated with this group.
Enabled	An indication of whether the notifications for this group are enabled on the appliance.
Actions	Allows you to make changes to the group.

6. To edit a group:
   a. Click the *Edit Template* button in the *Actions* column for the selected group.
   b. In the dialog box that appears, click the **Recipients** box, and select one or more users.

   NOTE: You can only choose from the existing users accounts that are already defined on the appliance. The `admin` user is always assigned to all UI notifications and can not be removed as a recipient.

   c. Select or clear the **Enable Notifications** check box to allow or prevent notifications from this group from being displayed.

   UI notifications are enabled by default.

   d. Click **Save** to confirm your changes and close the dialog box.
7. On the *Notifications* page, on the *UI Notifications* tab, click **Save**.

Enabling link aggregation

By default, link aggregation is not enabled on the appliance. The appliance requires that your switch is capable of a LACP (802.3ad) connection.

Before you enable link aggregation, set your switch to actively negotiate LACP. See your switch vendor's documentation for details. Passive negotiation mode does not work. If your switch is set to operate in passive mode, the switch cannot negotiate the appliance LACP connection. For an example of a Cisco® switch configuration running the IOS operating system set to active mode, view the online FreeBSD® Handbook.

All interfaces in each EtherChannel must be the same speed and duplex.

Create an aggregate link

The physical appliance provides two ports. You can connect both ports to the network (LAN) to enable link aggregation. You cannot enable link aggregation if offboard storage is configured.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Network Settings** to display the *Network Settings* page.
2. Select the **Enable Link Aggregation** check box.
3. Click **Save**.
4. Enter the *Link Aggregation IP Address*.

   The appliance reboots, and the IP address changes to the link aggregation IP address you entered.

NOTE: The subnet mask changes to match the NIC.

Configuring the data sharing preferences

Data sharing preferences determine how much of your appliance information is shared with Quest KACE. In addition, data sharing preferences determine whether information from ITNinja is displayed in the Administrator Console.

When you accept the End User License Agreement (EULA), you agree that Quest may collect, store, aggregate, and analyze information about your appliance usage.

By default, the appliance collects, stores, and shares the following data with Quest:

- **Server fields**: MAC Address, Company Name, Serial Number, Model, Network Addresses (External Customers), and Network Addresses (Internal Customers).
- **Licensing**: Product Version, Enabled Modules, Node Counts, Network Addresses (Internal Customers, and License Key.
- **EULA acceptance logs**
- **Status/Uptime/Load Averages**
- **Current Table Usage**: Number of scripted installations, system images, pre-installation tasks, post-installation tasks, user states, and so on.
- **Machine/Manufacturer/Model**: Manufacturer, Model, and Number of Machines.
- **Appliance Disk Information**: RAID Status, Physical Drivers, Adapter Information, and so on. Disk information is only available for the physical appliance.

Share basic appliance data usage

You can configure the appliance to share summary appliance usage or only basic appliance usage data with Quest.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **General Settings** to display the *General Settings* page.
2. Under *Data Sharing*, clear the first check box: *Share summary usage data about hardware, software, and the appliance with Quest*.

   Clearing the first check box automatically disables the second check box: *Share detailed usage data and crash reports (required for ITNinja community features)*.
3. Click **Save**.

   The appliance collects the following basic usage data:

   - **Server fields**: MAC Address, Company Name, Serial Number, Model, and Network Addresses (External Customer), and Network Addresses (Internal Customers).
   - **Licensing**: Product Version, Enabled Modules, Node Counts, and License Key.
   - **EULA acceptance logs**

Share detailed usage data

Sharing detailed appliance data usage helps Quest to understand how products work in your environment, provides more information to the Support team for troubleshooting issues, and helps with product enhancements.

Integration with the ITNinja community requires access to all levels of data.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **General Settings** to display the *General Settings* page.
2. Under *Data Sharing*, select the first two check boxes: *Share summary usage data about the hardware, software, and the appliance with Quest* and *Share detailed data and crash reports (required for ITNinja community features)*.
3. Click **Save**.

   When you share detailed data usage, the appliance collects the default information and the following data:

   - **appliance Server Crash Logs**
   - **UI Access Statistics**

Participate in KACE Beta program

KACE Beta program provides early access to new product features and updates. You can choose to participate in the program and receive notifications when a Beta version of the KACE Systems Deployment Appliance becomes available.

Beta notifications may target specific configurations. Enabling them does not trigger automated upgrades to Beta versions, or automatically register this appliance for the Beta program. Beta enrollment is still required to participate, and details are provided in the notifications.

NOTE: Notifications appear in the pane on the right. This is where the appliance displays applicable alerts, as configured. Use the bell icon to show or hide the *Notifications* pane. To clear the list of notifications, click **Dismiss All**. For information on managing the information that appears on this pane, see Configure User Interface notifications.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **General Settings** to display the *General Settings* page.
2. Under *Data Sharing*, select *Enable beta notifications from KACE*.
3. Click **Save**.

Linking Quest KACE appliances

If you have multiple Quest KACE appliances, you can link them. Appliance linking enables you to log in to one appliance and access all linked appliances from the drop-down list in the top-right corner of the Administrator Console, without having to log in to each appliance separately.

You must enable linking on each K-Series appliance, and configure the link connections on each appliance, such as Names and Keys. If the appliance that you are adding is SSL enabled, use SSL to establish a successful connection.

Linking the Remote Site Appliance (RSA) establishes the RSA as an extension of the appliance, which enables you to synchronize the components you want to use at the remote site. You can network boot, perform system image and scripted installation deployments, and migrate users profiles to devices at remote sites.

You cannot transfer resources or components among linked appliances. See Importing and exporting appliance components.

NOTE: Linking K3000 appliances requires setting up LDAP authentication for each appliance. See Configure an LDAP server for user authentication.

Enable appliance linking

You can enable linking to log in to one appliance and access multiple linked KACE Systems Management Appliance, KACE Systems Deployment Appliance, or Remote Site Appliance from one Administrator Console as long as the administrator user account for each appliance has the same password.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **KACE Linking** to display the *KACE Linking* page.
2. Select the **Enable KACE Linking** check box to display the connection settings.
3. In *Host Name*, enter a unique, logical name to identify this KACE Systems Deployment Appliance or Remote Site Appliance. This name appears in the drop-down list in the top-right corner of the page next to the login information when appliances are linked.
4. In *Remote Login Expiration*, enter the number of minutes to keep the link open. When this time period expires, provide login credentials when switching to a linked appliance. The default is 120 minutes.
5. In *Request Timeout*, enter the number of seconds that this appliance waits for the linked appliance to respond to a linking request. The default is 10 seconds.
6. Click **Save**.

   Systems Deployment Appliance

   The *KACE Linking Key Fingerprint* and *KACE Linking Key (this server)* appear.
7. Copy the text in the *Host Name* field and the *KACE Linking Key (this server)* fields and paste it in a central location, such as a Notepad file.

   Tip: **TIP:** To copy the linking key, simply click the contents of the *KACE Linking Key (this server)*. A message briefly appears at the bottom of the field, indicating that the text is successfully copied.

   The text that you paste in Notepad is the text that you copy and paste in the *Names* and *Keys* from one appliance to the other linked appliances.
8. Repeat the preceding steps on each appliance you want to link.

When linking is enabled on all appliances, add the Names and Keys to the appliances. See Add Names and Keys to appliances.

NOTE: Each KACE Systems Management Appliance comes with a default organization (named `Default`). If your appliance is linked with the `Default` organization on a KACE Systems Management Appliance, and the organization name changes, you must provide the new organization name:

1. On the left navigation pane, click **Settings** > **Control Panel** > **Linked Appliances**.
2. On the *Linked Appliances* page that appears, click the name or IP address of the linked KACE Systems Management Appliance.
3. On the *Edit Linked Appliance Detail* page that appears, in the *Default ORG Name* field, type the organization name, and click **Save**.

Generate KACE Linking Hash

A KACE Linking Hash string allows you to link a primary KACE Systems Deployment Appliance with a Remote Site Appliance (RSA) during the RSA installation. The generated hash string is only active for five minutes.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **KACE Linking** to display the *KACE Linking* page.
2. Select the **Enable KACE Linking** check box to display the connection settings.
3. Click **Generate Hash**.
4. Copy the text in the *KACE Linking Hash (valid for 5 minutes)* field and paste it in a central location, such as a Notepad file.

Tip: **TIP:** To copy the linking key, simply click the contents of the field. A message briefly appears at the bottom of the field, indicating that the text is successfully copied.

This key is only valid for five minutes. You can generate a new one when that period expires. You can regenerate the hash string while the current one is still valid. This is useful in case you are not sure how long ago the hash was generated.

If you navigate away from the page after generating the hash string, and then return to it, the linking hash field remains filled unless five minutes expire by the time the page is rendered.

The text that you paste in Notepad is the text that you copy and paste in the *Parent SDA Linking Hash* field in the *KACE Remote Site Appliance Initial Configuration Wizard*. For more information, see the *KACE Systems Deployment Appliance Setup Guide*.

Add Names and Keys to appliances

After linking is enabled on the appliances, configuring linking on each appliance requires copying the linking key from the remote appliance *KACE Linking* page to a central location, then pasting the key to the appliance to which you are linking.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **KACE Linking**, and select the **Enable KACE Linking** check box.

   The **Manage Linked Appliances** option is now available from the *Control Panel*.
2. Select **Choose Action** > **New** to display the *Add Linked Appliance* page.
3. In *Host Name*, enter IP address of the appliance that you want to link.

   If you are linking an RSA to an appliance, the host name must match the host name set on the RSA *Network Settings* page.
4. In *Linking Key*, paste the key that you copied to a central location to the appliance to which you are linking.
5. Click **Save**.
6. After both links are created, go to the *Edit Linked Appliance Detail* page, and click **Test Connection** to verify the connection between the two linked appliances.

   The *Linked Appliances* page appears.

The next time that you log into the appliance, the linked appliances appear on the drop-down list in the top-right corner of the page next to the login information. To switch to a different appliance, select its name in the drop-down list.

Disable linked appliances

You can disable linking as needed. After appliance linking is disabled, you can continue to switch between the KACE Systems Deployment Appliance or RSA that were linked until you log off.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **KACE Linking** to display the *KACE Linking* page.
2. Clear the *Enable KACE Linking* check box.
3. Click **Save**.

Migrating appliances

If you want to migrate settings and images from one appliance to another, you can easily do that using the *Appliance Migration Wizard*. This is useful, for example, when you want to quickly move the data between virtual appliances.

NOTE: You must enable linking on both the source and destination appliance, however you do not need to configure the appliance connections. The *Appliance Migration Wizard* connects the appliances and disconnects them after the migration. For more information about appliance linking, see Enable appliance linking.

Migrate appliance data

The *Appliance Migration Wizard* allows you to easily move settings and images from one appliance to another. The migration does not work on the associated Remote Site Appliances (RSA). However, any links to the RSAs associated with the source appliance are migrated to the destination appliance. The source and destination appliances must be on the same version. The migration process overwrites all data on the destination appliance and replaces it with those from the source appliance. The host name, IP address and license key of the destination appliance are not affected by the migration.

IMPORTANT: Quest Software highly recommends that you perform the migration with both the source and destination appliances on the same network and same subnet. If required, the destination appliance can be moved to its appropriate subnet after the migration has completed.

1. Open two tabs in your web browser. On each tab, log in to the Administrator Console for the source and destination appliance.
2. Ensure that appliance linking is enabled on each appliance. You can enable appliance linking on the *KACE Linking* page, or by using the link in the *Appliance Migration Wizard*. For complete information about appliance linking, see Linking Quest KACE appliances.

   NOTE: While it is mandatory to enable appliance linking before you start the migration process, you do not need to actually link the source and destination appliances. The *Appliance Migration Wizard* connects the appliances and disconnects them after the migration.
3. On each appliance, in the Administrator Console, on the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Appliance Migration** to display the *Appliance Migration Wizard*.

NOTE: As you go through the wizard, you will need to switch between the source and destination appliances in your web browser. To easily distinguish between the two appliances, you can apply different themes to each of them. For example, you can apply the Dark theme to the source appliance, and the Light theme to the destination appliance. For more information about choosing different themes, see Change a default theme for the appliance.

4. If appliance linking is not enabled on each appliance, this is indicated in the wizard. Click *KACE Linking* in the *Appliance Migration Wizard*, and enable appliance linking using the *KACE Linking* page. When done, return to the *Appliance Migration Wizard* to complete the migration.
5. Specify the source and destination appliances.
    a. On the source appliance, in the *Appliance Migration Wizard*, on the *Select Appliance Type* page, select **Migration Source**, and click *Next*.
    b. On the destination appliance, in the *Appliance Migration Wizard*, on the *Select Appliance Type* page, select **Migration Destination**, and click *Next*.
6. Link the source and destination appliances.

    You do not need to link the appliances using the standard process. Instead, you copy custom linking keys from one appliance to another. The appliance key specifies the appliance version, host name or IP address, and the linking key. The keys appears in encrypted form in the wizard. The custom link is only available during the migration process.

    For complete information about linking appliances using the standard process, see Linking Quest KACE appliances.

    a. On the source appliance, in the *Appliance Migration Wizard*, on the *Copy Source Key* page, left-click the field to copy the key.
    b. On the destination appliance, in the *Appliance Migration Wizard*, on the *Apply Source Key* page, paste the key into the field, and click **Next**.
    c. On the source appliance, in the *Appliance Migration Wizard*, on the *Copy Source Key* page, click **Next**.
    d. On the destination appliance, on the *Copy Destination Key* page, left-click the field to copy the key.
    e. On the source appliance, on the *Apply Destination Key* page, paste the key into the field, and click **Next**.
    f. On the destination appliance, on the *Copy Destination Key* page, click **Next**.
7. On the destination appliance, in the *Appliance Migration Wizard*, on the *Approve Migration* page, click **Approve Migration**.
8. Approve the appliance migration.
    a. On the destination appliance, in the *Appliance Migration Wizard*, on the *Approve Migration* page, click **Approve Migration**.
    b. In the *Confirm* dialog box that appears, click **Yes**.

    The destination appliance goes into migration mode. The *SDA Migrating* page appears in your browser window.
9. Start the appliance migration.
    a. On the source appliance, in the *Appliance Migration Wizard*, on the *Begin Migration* page, indicate which action you want the source appliance to take after the migration process completes. To do that, on the page, select one of the following options:

    - **Return to Dashboard**: The Dashboard page is displayed.
    - **Shutdown**: The appliance shuts down.
    - **Reboot**: The appliance reboots.

    b. Click **Begin Migration**.

NOTE: You must approve the migration on the destination appliance in order to start the migration process, as described in the previous step. If the migration is not approved on the destination appliance, the **Waiting for Approval** button appears instead of **Begin Migration**.

c. In the *Confirm* dialog box that appears, click **Yes**.

The source appliance goes into migration mode. The *SDA Migrating* page appears in your browser window. The log of the migration process appears for each appliance. The log contents are different for each appliance as they reflect what happens on each end of the process. When the migration process finishes, the destination appliance restarts, and the login page appears.

Setting up user accounts and user authentication

You can add user accounts to the appliance and set up the accounts using local authentication. If you require external user authentication, such as an LDAP or an Active Directory® server, you can configure an external server to enable users to log in to the Administrator Console using their domain credentials.

Local Authentication

Use the default local authentication when an LDAP service, such as Active Directory, is not available in the environment.

External LDAP Server Authentication

Use your domain credentials to log in to the Administrator Console. See Use an LDAP server for authentication.

Two-Factor Authentication (2FA)

Provide stronger security for users logging into the appliance by adding 2FA to the login process . See Use an LDAP server for authentication.

NOTE: If you have linked appliances, you can use single sign-on if you use the same login and password on all linked appliances.

Add or edit local administrator accounts

You can create and edit local administrator user accounts. Adding users to the appliance database stores the user information locally and requires only the user name, email address, password, and permissions.

1. On the left navigation pane, click **Settings > Control Panel**to display the *Control Panel*, then click **Users** to display the *Users* page.
2. Select **Choose Action** > **New** to display the *User Detail* page.
3. Complete the user account form:

Option	Description
User Name	**Required**: Enter a login ID.
Full Name	**Required**: Enter the first and last name of the user.
Email	**Required**: Enter the email address of the user.
Domain	Enter the domain that the user is using.
Budget Code	**Optional**: Enter the budget code of the department where the user is located.
Location	**Optional**: Enter the site or location of the user.

Option	Description
Password	**Required**: Enter the default password for the user. The password is required to activate the user. If the *Password* field is blank, the user cannot log in to the Administrator Console.
Confirm Password	Re-enter the password.
Permissions	Role of the user on this appliance. Administrators have full read/write access. Read-only administrators can log in and view settings and run reports; they cannot access the Administrator Console. Select the permissions: • **Admin**: Read/write access to the Administrator Console. • **ReadOnly Admin**: View all pages; no change access.
Two Factor Authentication Required	Select this option if you want this user to log in with a 2FA verification code. For more information, see Enable Two-Factor Authentication.
Reset Token	Click if you want to re-authenticate this user with a new 2FA verification code.

4. **Optional**: Click **Cancel** to close the page.
5. Click **Save**.

The user appears in the local account list and can now log in to the Administrator Console.

You can apply a label to a group of users.

Configure an LDAP server for user authentication

LDAP authentication requires creating a login account for the appliance on your LDAP server. The appliance uses this account to read and import user information from the LDAP server. The account needs read-only access to the *Search Base DN* field on the LDAP server. The account does not require write access, because the appliance does not write to the LDAP server.

For information on adding user accounts to the appliance, see Add or edit local administrator accounts.

NOTE: When LDAP is enabled, all local accounts become inactive except for the administrator account.

When logging in, the appliance automatically queries the listed external servers. The timeout for a server is approximately 10 seconds. To decrease login delays, Quest KACE recommends deleting the sample LDAP server.

1. On the left navigation pane, click **Settings**, then click **User Authentication** to display the *Authentication Settings*.
2. Select *External LDAP Server Authentication* and click **Add New Server**.

All servers must have a valid IP address or host name; otherwise, the appliance times out, resulting in login delays when using LDAP authentication.

3. Provide the following information to add a server:

Field	Description
Server Friendly Name	The name to identify the server.
Server Host Name (or IP)	The IP address or the host name of the LDAP server. If the IP address is not valid, the appliance waits to timeout, resulting in login delays during LDAP authentication. **NOTE:** To connect through SSL, use an IP address or host name. For example: `ldaps://hostname`. If you have a non-standard SSL certificate installed on your LDAP server, such as an internally-signed certificate or a chain certificate that is not from a major certificate provider such as VeriSign, contact Quest KACE Technical Support at https://support.quest.com/contact-support for assistance.
LDAP Port Number	The LDAP port number. The default is 636 (secure LDAP). The non-secure LDAP port 389 can also be used, however keep in mind that such connections can easily expose user names and passwords to malicious parties, and as such should be avoided.
Search Base DN	The area of the LDAP tree that the appliance should start to search for users. For example to search for the IT group, specify `OU=it,DC=company,DC=com`.
Search Filter	The search filter, for example:**LDAP_attribute**=KBOX_USER, where **LDAP_attribute** is the name of the attribute containing a unique user ID and **KBOX_USER** is a variable that the appliance replaces at runtime with the login ID that you enter. For example when using Active Directory, enter samaccountname=KBOX_USER. For most other LDAP servers, enter UID=KBOX_USER.
LDAP Login	The credentials of the account that the appliance uses to log in to the LDAP server to read accounts. For example: `LDAP Login:CN=service_account,CN=Users, DC=company,DC=com`. If no username is provided, an anonymous bind is attempted.
LDAP Password (if required)	The password of the account that the appliance uses to log in to the LDAP server.

Field	Description
User Permissions	The user permissions. • **Admin**: Read/write access to the Administrator Console. • **ReadOnly Admin**: View all pages; no change access.
Test User Password	The LDAP username and password to test on the LDAP server. See Test the LDAP server.

Record the *Search Base DN* and the *Search Filter* criteria because you use this same information to import user data and to schedule user imports.

4. **Recommended**: Click the **Remove** icon next to any external servers that are not configured to actual servers in your environment.
5. Click **Save**.

The next time users log in, they are authenticated against the LDAP servers in the order listed.

NOTE: The administrator account always authenticates against the internal database, even when an account with the same name exists in an external LDAP.

Test authentication on an external LDAP. See Test the LDAP server.

Test the LDAP server

You can test authentication on the LDAP server using a valid username and password to determine if the server is able to perform a successful authentication.

1. Select an LDAP profile.
2. In *Search Filter*, replace the **KBOX_USER** variable with a valid login ID to test. The syntax is `samaccountname=username`.
3. Enter the corresponding password for the LDAP account.
4. Click **Test Settings**.

   If the test is successful, the authentication setup is complete for this user, and other users in the same LDAP container.
5. Change the username in *Search Filter* back to the system variable **KBOX_User**.

Delete user accounts

You can delete user accounts.

1. On the left navigation pane, click **Settings > Control Panel**to display the *Control Panel*, then click **Users** to display the *Users* page.
2. Select the check box next to one or more accounts.
3. Select **Choose Action** > **Delete**.
4. Click **Yes** to confirm.

Reviewing user sessions

The KACE Systems Deployment Appliance and the Remote Site Appliance keep track of your user sessions. You can review a list of the most recent sessions, or see all sessions for a specific appliance.

To allow the appliance to display the location associated with the logged-in user's public IP address, you must install a location database. See Install and configure the location database.

You can see all of your user sessions on the *Recent Sessions* page. For a quick list of the latest sessions, use the *My Recent Sessions* pane. See View a list of user sessions.

Install and configure the location database

User session details include the IP address of the currently logged-in user. This information is displayed on the *Recent Sessions* page. For public IP addresses you can also display the geographical location associated with a specific IP address, however this requires a location database to be installed on the KACE Systems Deployment Appliance and each Remote Site Appliance. You can install the MaxMind *Geolocation* database free of charge and display user locations for any public IP address.

MaxMind offers country and city databases. A city database is typically larger in size and takes longer to install. A country database provides only the name of the country associated with each public IP address, while a city database allows the appliance to display the city, state (if applicable), and the country.

You can periodically refresh the location database by installing an updated version. While it is possible to install multiple databases over time, the most recently installed database overwrites the contents of the previous version. For example, if a country database is already installed, and you install a city database on the appliance, the *Location* column on the *Recent Sessions* page reflects the information from the newly installed city database.

For complete information about MaxMind Geolocation databases, visit https://www.maxmind.com/.

NOTE: Locations cannot be displayed when a private IP address is used to access the appliance.

1. Download a location database from https://www.maxmind.com/.

   NOTE: To download a database file from MaxMind, start by creating a user profile. You must download a file that uses the `MMDB` format, not a `CSV` file.

2. Log in to the KACE *Systems Deployment Appliance Administrator Console* or *Remote Site Administrator Console*.
3. Complete one of the following steps, as applicable.

   - **KACE Systems Deployment Appliance only.**
     1. Log in to the *Systems Deployment Appliance Administrator Console*.
     2. Click **Settings > Control Panel** to display the *Control Panel*, then click **General Settings** to display the *General Settings* page.
   - **Remote Site Appliance only.**
     1. Log in to the *Remote Appliance Console*.
     2. Click **Settings > Control Panel** to display the *Control Panel*, then click **Remote Site Settings** to display the *Remote Site Settings* page.

4. On the page that appears, under *MaxMind Geolocation Database*, point to the downloaded `tar.gz` file.

   You can do that either by clicking **Select file** and providing the path to the downloaded file, or by dragging and dropping the file into the indicated area.

5. Click **Update Database**.

It may take a few minutes for the database installation to complete, depending on the type of database being installed. When the installation is complete, the *Database Type* and *Database Version* fields provide the relevant details.

NOTE: A city database typically takes longer to install and update than a country database due to its file size.

Next, you can go to the *Recent Sessions* page and review the location data for the current user. See View a list of user sessions.

View a list of user sessions

Use the *Recent Sessions* page to view all sessions associated with your account. You can review your user sessions on the KACE Systems Deployment Appliance, or each Remote Site Appliance, as applicable. Alternatively, to see the latest sessions, in the top-right corner, click the Recent Sessions icon, and review the list in the *My Recent Sessions* pane that appears.

In case the appliance detects multiple sessions for the current user, the icon displays a red exclamation point.

1. On the left navigation pane, click **Audit Log** to expand the section, then click **Recent Sessions** to display the *Recent Sessions* page.
2. Review the list of user sessions.

   Each entry displays your user name, the browser used, your operating system, IP address, the session duration, the date and time of the last activity, and any applicable actions. For the users with a public IP address, it also shows the location, if you have a location database installed. See Install and configure the location database.

Configuring security settings

You can enable SSH to allow the Quest KACE Technical Support team to access your appliance for remote support. Other security settings include enabling SNMP to allow remote monitoring, and enabling Offboard Database Access to allow the appliance database to be available to external programs, which can be useful for reporting. Enabling SSL provides a secure web browser to run the appliance.

Enable SSH Root Login (KACE Support)

Enabling SSH provides remote access to the Quest KACE Support team. Quest KACE recommends enabling SSH before you begin to use the appliance. SSH remote access is the only method that the Support team can use to diagnose and fix problems if the appliance becomes unresponsive.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Security** to display the *Security Settings* page.
2. Select the *Allow SSH Root Login (KACE Support)* check box.
3. Click **Save**.

Enable SNMP monitoring

The SNMP agent on the appliance enables remote monitoring of the appliance.

The internal SNMP agent uses the standard UDP port 161 and cannot be configured using TRAP and INFORM methods. If you have a primary SNMP agent configured on a different device, it can send `GET`, `GETNEXT`, and `GETBULK` requests to the appliance and have the appliance return the requested information.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Security** to display the *Security Settings* page.
2. Click **Enable SNMP Monitoring** to display the *SNMP Community String* field.
3. Enter a unique community string, for example `newString`.

   If the community name contains spaces, enclose it in quotation marks (" "). Quest KACE recommends creating a unique string. The default is `KaceSDA`.

   NOTE: In versions prior to 7.0, the community string is set to `public` by default. If you upgrade from a pre-7.0 version, and SNMP monitoring is disabled, the community string changes from `public` to `KaceSDA`. If SNMP monitoring is enabled, the community string stays set to `public`, you should update it to prevent security issues. Warnings appear on the *Dashboard* and on the *Security Settings* page, alerting you to update the community string.
4. Click **Save**.

Set session timeout

You can configure session timeout to meet your security requirements.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Security** to display the *Security Settings* page.
2. Click **Server Session Timeout** and select a desired value.
3. Click **Save**.

Enable database access

You can enable database access to allow external programs, such as Crystal Reports or Excel® to query the appliance database so that you can create your own reports. By default, the appliance does not allow external connections to the database.

The account for external access to the database is username: report and password: box747.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Security** to display the *Security Settings* page.
2. Select the *Enable Database Access* check box.
3. In *Report User Database Password* and *Verify Password*, specify the database password that you want the external resources to use when accessing the appliance database.

   The indicator underneath the *Report User Database Password* field changes color as you type the password string, to indicate the password strength. Red indicates the lowest, and green the highest complexity level. Choose a strong password to prevent unauthorized users from accessing your database records.

   If you do not specify a password for the Report User, the programs querying the appliance use the default password, which can allow attackers to expose sensitive data. A warning alert on the Home Dashboard appears, prompting you to change the database password. For more information about the Dashboard, see Using the Dashboard.
4. Click **Save**.

You might have to reboot the appliance before external programs can query the appliance database.

Prevent brute-force login attacks

You can configure the appliance to prevent multiple consecutive attacks from obtaining appliance credentials.

The *Brute Force Detection* settings on the *Security Settings* page allow you to configure the number of failed authentication attempts within a specified time frame, after which the appliance prevents any logins for that user name.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Security** to display the *Security Settings* page.
2. On the *Security Settings* page, under *Brute Force Detection*, specify the following:
   - The maximum number of failed login attempts. You can specify any value between three and ten attempts. The default setting is three attempts.
   - The number of minutes during which the appliance prevents that specific user from logging in. You can specify any number of minutes between one and 60. The default setting is five minutes.

When the appliance disables a user from logging in, other users are not affected and can log in to the appliance during the specified time period, when they provide valid credentials.

3. Click **Save**.

Enable SSL using an existing certificate

By default, SSL is disabled. You can use an existing SSL certificate, an intermediate certificate, or a self-signed certificate to run your appliance on a secure web browser. Using an existing certificate requires having an SSL private key and ensuring that port 80 is open.

NOTE: If you do not have a valid certificate, the appliance can generate a Certificate Signing Request (CSR) that you can send to your Certificate Signing Authority. You can download the private key and save it in a safe place. See Generate private key for new SSL certificate.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Security** to display the *Security Settings* page.
2. Click **Enable SSL** and click **I already have an SSL certificate, Can I use it?**
3. Click **Use My Certificate**.
4. Under *Optional SSL Settings*, select one of the following certificate types:
   - **Private Key & Certificate (most common).**
   - **What if I also have an intermediate certificate?**
   - **PKCS-12 (.pkcs12, .pfx, .p12)**

   Enter the password for the PKCS-12 SSL formatted certificate.
5. Browse to the key or certificate and click **Apply Certificate**.

The secure web browser using `https` is available.

Generate private key for new SSL certificate

By default, SSL is disabled. You can generate a private key to enable SSL after you generate a new certificate. You can use a valid self-signed certificate if you have a private key or a PKCS-12 file, and the private key and certificate were generated from the same Certificate Signing Request (CSR).

Export your appliance components to a different location and enable SSH in case there is an error that might require the appliance to stop the key generation.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Security** to display the *Security Settings* page.
2. Click **Enable SSL** to use a new certificate or a valid self-signed SSL certificate. Note that Quest KACE does not recommend using a self-signed certificate.
   - Generate a new SSL certificate:
     1. Click **Get New SSL Certificate** to display the *SDA Advanced SSL Settings* wizard.
     2. Fill in the fields to generate a CSR.
     3. Download the private key and save the key in a safe place to use to enable SSL when you get a valid certificate from your Certificate Signing Authority.

4. Copy or download the generated CSR and send it to your Certificate Signing Authority.

- Use a self-signed certificate:
  - Click **Can I use a self-signed certificate instead?**, then click **Save and Restart Apache**.

Disable SSL

You can disable the secure web browser that the appliance is running on by disabling SSL (Secure Sockets Layer).

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Security** to display the *Security Settings* page.
2. Click **Enabled ports: 80, 443 (change)**.
3. Clear the following check boxes:
   - *Enable port 443 (HTTPS)*
   - *Forward port 80 to port 443*
4. Click **Apply Changes**.

The HTTPS browser is now unavailable.

Enable Two-Factor Authentication

Two-Factor Authentication (2FA) provides stronger security for users logging into the appliance by adding an extra step to the login process. It relies on the authenticator app to generate verification codes. The app generates a new six-digit code at regular intervals. When administrators enable 2FA on the appliance, applicable end users are prompted for a verification code each time they log in.

Start by installing the authenticator app on your mobile Android or iOS device. You can download the app from Google Play and Apple App Store.

Only users with Admin-level permissions have the ability to enable 2FA. Read-only administrators cannot manage this feature.

NOTE: Using the `reset_admin_password` command to reset the administrator's password also resets the 2FA token. For more information about this command, see Use the Command Line Console to reset the Administrator's password.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Security** to display the *Security Settings* page.
2. On the *Security Settings* page, under *Two-Factor Authentication*, select **Enable Two-Factor Authentication**.
3. Click **Save**.
4. Complete the 2FA configuration on the *Configure Two-Factor Authentication* page that appears.
   a. Click the iOS or Android icon to display the applicable QR code.
   b. Scan app store QR code to download the authenticator app.
   c. Use the authenticator app on to scan the QR code.

   The 6-digit code that appears is valid for 30 seconds. If you enable this feature, ensure that appliance server's clock is accurate, as well as the device running the authenticator app. The app relies on current time to create the token. If the server's clock is not synchronized with those of the devices running the authenticator app, token validation may fail, which may result in account lockouts.

   d. In the *Verification Code* field, type the 6-digit code from the authenticator app.
   e. Click **Finish Configuration**.

The *Configure Two-Factor Authentication* page closes and the Dashboard appears, indicating that you are now logged in to the appliance with the newly configured 2FA credentials.

5. Complete additional 2FA configuration options, as applicable.
    a. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Security** to display the *Security Settings* page.
    b. When you enable 2FA on the appliance, only those users who have 2FA enabled can log in using this additional layer of security. To enforce 2FA for all users logging into the appliance, under *Two-Factor Authentication*, select **Require Two-Factor Authentication for all users**. This option overrides the 2FA configuration associated with individual user accounts. For more information, see Add or edit local administrator accounts.
    c. To specify the length of time during which users who require 2FA can bypass 2FA authentication, under *Transition Window*, specify the desired time period. This way, for example, if a user leaves their phone at home and cannot generate a new code, they can still access the appliance during the specified amount of time.
6. Click **Save**.

Preparing for deployment

Appliance deployments require that you have 20 percent disk space. You can download and install the tools required to build the boot environment, upload the operating system installation source media, and enable the appliance to connect to target devices.

Set up the deployment environment

You can set up your appliance network connection between the target devices to PXE boot from the target devices to the appliance, download the required tools to build your KACE Boot Environment (KBE), and load the source media and user profiles to the appliance.

1. Set up an administrator device.
2. Create a network connection between the target devices and the appliance using a DHCP server to direct PXE boot requests from the target device to the appliance. See Enable the on-board DHCP server.
    a. Use the built-in appliance DHCP server if there is no existing DHCP server on your network, and if you are using the appliance in a closed lab environment.
    b. Use your existing DHCP server if the appliance is on a corporate network.
3. Download the Media Manager. See Download and install the KACE Media Manager.
    a. Download and install the Windows ADK required to create a KACE Boot Environment using the Media Manager. See Download and install Windows ADK.
    b. Upload the OS source media to the Media Manager. See Upload files using the KACE Media Manager.
4. Capture user profiles from a device, upload the profiles to the appliance to migrate the profiles to target devices. See Upload USMT software from the appliance.

Prepare and capture the image from the device. See Capture system images.

Enable the on-board DHCP server

If you are testing the appliance on a private network or in a small environment that does not have a DHCP server, the appliance can act as the DHCP server by enabling this option on the appliance.

Ensure that there is the only one DHCP server on the network, and that you configure the router to forward the DHCP requests to the appliance.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Network Settings** to display the *Network Settings* page.
2. Select the *Enable On-Board DHCP Server* check box.

   The DHCP range fields appear.
3. In *DHCP Pool Start*, enter the lowest IP address in the range.
4. In *DHCP Pool End*, enter the highest IP address in the range.
5. Click **Save**.

DHCP is enabled.

Configure the offboard DHCP server

When you turn on a device for the first time, you can select the NIC or Network Boot option from the BIOS boot menu. Windows deployments require target devices to boot from somewhere other than the local drive. When you select the NIC or Network Boot option, the device sends an PXE request to the DHCP server to locate the iPXE server. In this case, the appliance is the PXE server. You can configure an offboard DHCP server to acknowledge the appliance to enable target devices to UEFI boot from the appliance.

The steps might vary depending on which DHCP server you are using. Use the following settings for options `066` and `067` on any DHCP server.

If you are not using the Microsoft DHCP, see the following Knowledge Base article for additional information: https://support.quest.com/kace-systems-deployment-appliance/kb/112037

1. Open the configuration application for your DHCP server.
2. Set the following options for each subnet or scope that you want target devices to be able to boot from the appliance:

   - **Set *Option 066* to the IP address of the appliance.**

     This option might appear as *Next-Server*, *Boot Server Host Name* or *TFTP server name*.

     NOTE: You might not be able to set *Option 66* on some Cisco networking equipment. As an alternate configuration, you can set the *sname* and *244* options to the appliance IP address.

   - **Set *Option 067* to the string `ipxe.efi` (for UEFI devices), and `undionly.kpxe` (for BIOS devices).**

     This option might also appear as *Boot File Name*. Copy and paste the `ipxe.efi` or `undionly.kpxe` string as the *Boot File Name* option.

     NOTE: You can only have one PXE or TFTP server on a subnet. Disable other imaging tools on the subnets where you want to test the appliance.

The DHCP server automatically redirects PXE-compliant Windows devices to the appliance the next time the devices start up while connected to the network. The devices download the bootstrap file, and use the environment setup to boot.

Download and install the KACE Media Manager

You can download and install the KACE Media Manager from the appliance to a device with the Windows ADK installed. The KACE Media Manager uploads the KACE Boot Environment (KBE) using the Windows ADK.

The Media Manager requires the full installation of Microsoft .NET 4.0. Download and install .NET 4.0 from http://www.microsoft.com/en-us/download/details.aspx?id=17851.

The appliance periodically checks for updated versions of the Media Manager. When a new version becomes available, a warning alert appears on the Home Dashboard. It is recommended to use the latest version of the KACE Media Manager on managed devices. For more information about the Dashboard, see Using the Dashboard.

1. On the left navigation pane, click **Library**, then click **Library Overview** to display the *Library Overview* page.
2. Under *Source Media*, select **Choose Action** > **Download Media Manager** to display the *Media Manager* page.
3. Click **Download for Windows**.

The *File Download* window appears.

4. Click **Run** or **Save** to download the installation file to the device, then double-click the file to start the installation.

   The *Welcome* window appears.

5. Run the Media Manager from **Start** > **All Programs** > **Quest** > **KACE Media Manager**.

   For more information, see About the Media Manager.

Build a KACE Boot Environment. See Create a Windows boot environment.

About the Media Manager

The KACE Media Manager is an utility that allows you to build the KACE Boot Environment (KBE), and to upload OS-related files to the appliance.

The Media Manager includes the following pages. You can select each page by clicking the appropriate button in the left pane.

- Create KBE page
- Upload Source Media page
- Upload USMT page
- General Settings page

Create KBE page

This page contains several tabs, each containing a group of settings that you can use to create a KBE.

To ensure successful KBE builds are created, the Media Manager requires a minimum of 5 Gb of disk space on the device. If insufficient space is detected, the Media Manager reports an error and quits the process.

Tab	Option	Description
General	**Name**	The name of the KBE. This value is automatically generated, but you can change it, if required.
	Architecture	**Windows only**. The OS architecture of the KBE. Select the **32-bit** or **64-bit** architecture, as needed.
	Language	The language of the KBE.
	Upload KBE	Click to upload the KBE to the appliance.
	Upload Custom ISO	Click to upload the Custom ISO to the appliance.
	Upload Custom WIM	Click to upload the Custom WIM to the appliance.
Server Configuration	**Use DHCP to find SDA**	Allows the Media Manager to use its DHCP server to locate the appliance.
	Use the SDA static IP Address	If the network where the appliance is located prevents it from being located through DHCP, use this option to specify the static IP address of the appliance. Boot environments

Tab	Option	Description
		created using this option will not work in an RSA (Remote Site Appliance).
	Use the RSA static IP Address	Select this option to specify the static IP address of the RSA to create boot environments for an RSA.
Device Configuration	**Find Device IP Address by DHCP**	Allows you to locate the target device (that is booting into the KBE) through DHCP. This is the default setting, however, it only works when the target device uses DHCP.
	Assign a static IP Address	The static IP address of the target device. Both the appliance and the target device must use either a static IP address or DHCP. You cannot assign a static IP address to a device and configure the appliance to use DHCP. If you select this option, you can only boot one device at a time.
	Set a range of static IP Address	Use this option to specify a range of static IP devices. It allows you to boot multiple devices at the same time. If you select this option, when the boot environment starts up, they can choose which address to assign to each device.
Advanced Options	**NOTE:** .NET/Powershell, Secure Startup, and Platform ID are installed automatically in all new KBEs.	
	Scratch Space in Mb	Choose the size of the scratch space on the target device. 64 MB is the default value. If you need more space, for example, if you add more drivers or apps, increase this value, to 128, 256, or 512 MB, as needed.
	Add ADSI Drivers	Adds Active Directory Service Interfaces (ADSI) drivers. You can select this option, for example, if you want to query Active Directory while the target device boots.
	Add ODBC Drivers	Adds ODBC (Open Database Connectivity) drivers. Select this option if you want the target device to establish a database connection.
	DCCTK/Command Configure	Indicates if Dell Client Configuration Toolkit, also known as Command Configure, is installed. This tool allows you to manipulate Dell BIOSes If it is installed, it is added to the KBE and can be used to issue commands to configure the device BIOS, such as changing the BIOS password, or change the boot order.
	UEFI ISO	Allows the KBE to create Unified Extensible Firmware Interface compliant device. This option is only supported on 64-bit systems.
	Sync KBE time with server	Synchronizes the KBE system time with the time set on the appliance.
	Set KBE Time Zone	Sets the KBE time zone. If this option is cleared (default setting), the KBE time zone is set to PST (Pacific Standard Time). If you select it, the KBE uses the time zone of the

Tab	Option	Description
		system running the Media Manager, but you can choose a different time zone, as required.
	Add files to KBE	Allows you to add custom files to the KBE. For example, you can add portable applications to the KBE, such as anti-virus scanner.
	Launch UltraVNC	Select this option if you want to launch UltraVNC on target devices. This open source tool enables the target device to access another computer remotely over a network connection.
	KACE Deployment Menu	Select this option if you want to display the *KACE Deployment Menu* when the target device boots, or clear it, if you do not the menu to appear.
	Run Driver Feed Advisor	Specifies the path to the driver feed for the target device model.
	Add Enhanced Storage	Allows you to add Enhanced Storage to target devices. This feature allows Windows to discover additional storage functionality and to manage the storage devices on target systems. For more information about Enhanced Storage, see your Windows documentation.
	ISO size restriction override	If your organization does not have ISO file size restrictions in place, you can use this option to create larger ISO images.
	Enable SMB v.1	Use this option if you want the target device to use this older version of the SMB protocol.
	Change KBE Background	Apply a custom image to the KBE background screen to replace the default Quest background.
Driver Options	**Inject drivers from the SDA**	Adds the latest downloaded drivers to the KBE. This is the default setting for new KBEs.
	Inject drivers from a local directory	Adds drivers from the local machine to the KBE. Click **Browse** to specify the directory.
DOS Commands		Type the commands that you want to run after starting the KBE.
	Remember DOS Command	Select if you want these commands to run each time the KBE starts.

Upload Source Media page

This page allows you to specify and upload source media files to the appliance.

Option	Description
Source Media Name	The name of the source media that you want to upload to the appliance.

Option	Description
Source Media Type	Allows you to either automatically detect the OS of the selected source media (available for most operating systems), or select one from the list, as needed.
Source Media Path	The path to the ISO file.
Upload Source Media	Click to upload the source media to the appliance.

Upload USMT page

This page allows you to specify and upload USMT (User State Migration tool) files to the appliance.

Option	Description
WAIK or WADK Path	The path displayed reflects your setting of the *WAIK or WADK Path* on the General Settings page.
Upload USMT	Click to upload the USMT (User State Migration Tool) to the appliance.

General Settings page

This page allows you to specify general settings that the Media Manager needs to access the appliance. This is the initial page you see when you run the Media Manager for the first time.

Section	Option	Description
SDA Settings	**SDA Hostname**	The IP address of the system where the appliance is running.
	SDA IP Address	The IP address segments of the system where the appliance is running.
	Samba Share Password	The password of the Samba share on the appliance. The Samba share is used for storing and backing up files. This password must match the password that you entered in the *SDA Samba Share Password* field on the *General Settings* page.
	Remember Password	Select if you want to remember the Samba share password.
	Ping SDA	Click to test the connection to the appliance. If a connection fails, "Connection failed" appears in red. Similarly, "Connection successful" in green is displayed when the connection is successful.
Other Settings	**WAIK or WADK Path**	**Windows only**. The path to the Windows Assessment and Deployment Kit (WADK) or Windows Automated Installation Kit (WAIK) files that you want to upload.
	Theme	The theme of the Media Manager: *Dark* or *Light*.

Section	Option	Description
	DISM Log Level	Specifies the maximum output level shown in the DISM (Deployment Image Servicing and Management) logs. The default log level is 3. The following logging levels are available: • 1 - Errors only • 2 - Errors and warnings • 3 - Errors, warnings, and informational • 4 - All of the information listed previously, plus debug output

Download and install Windows ADK

Building a KACE Boot Environment requires installing the Windows Assessment and Deployment Kit (Windows ADK) for Windows 7 and higher and Windows Server® 2012 devices.

You need ISO mounting software or a blank DVD, and a Windows device or a Windows Server with administrator privileges.

1. Download and install the Windows ADK, see http://www.microsoft.com/en-us/download/details.aspx?id=30652.
2. Under *Select the features you want to install*, select all of the features in the list.

Download and install the KACE Media Manager to the same device where you installed the Windows ADK. For instructions, see Download and install the KACE Media Manager.

Upload files using the KACE Media Manager

You can use the KACE Media Manager to upload the operating system source and installation files to the appliance.

Uploading the source media requires:

- The KACE Media Manager and .NET 4.0.
- Installation disks or mounted ISO image.

For more information about this tool, see About the Media Manager.

Alternatively, you can use the *Source Media Import* page to upload Windows and Linux `.iso` files to the appliance. Quest recommends that you use this page to upload `.iso` files for some platforms (such as CentOS) because Microsoft Windows causes the file names to become truncated. For more information, see Upload files from shared directory.

NOTE: Uploading the source files can take several hours.

1. Insert the operating system disk in to the media drive on the device where the Media Manager is installed.
2. Click **Start** > **All Programs** > **Quest** > **KACE Media Manager** to display the KACE Media Manager.
3. In Media Manager, in the left pane, click **General Settings**.

   The *General Settings* page appears on the right.

NOTE: This page appears by default if this is the first time you run the Media Manager.

4. On the *General Settings* page, in the *SDA Hostname* field, enter the IP address of the appliance.
5. In the *SDA IP Address* field, enter the IP address segments of the appliance.
6. In the *SDA Samba Share Password* field, enter the password. This password must match the password that you entered in the *SDA Samba Share Password* field on the *General Settings* page.

   NOTE: If you change the Samba share password, create a KBE using the new password.

7. In Media Manager, in the left pane, click **Upload Source Media**.

   The *Upload Source Media* page appears on the right.
8. On the *Upload Source Media* page, in *Source Media Name*, type a unique logical name.

   This name identifies the image on the appliance; it is used to assign the image to scripted installations and boot actions.
9. In *Source Media Type*, allow the Media Manager to either automatically detect the OS of the selected source media (available for most operating systems), or select one from the list, as needed.
10. In *Source Media Path*, click **Browse** and select the location of the image.

    When attempting to upload media to the RSA (Remote Site Appliance), the Media Manager displays the error: **Invalid Response: Please check the hostname provided**.

    Verify that the IP address is the actual IP address of the KACE Systems Deployment Appliance, and not the RSA.
11. Click **Upload Source Media**.

When the process completes, the image appears on the KACE Systems Deployment Appliance *Source Media* page. If *Source Media Notifications* are enabled for your user account, a new notification appears. For more information, see Configure User Interface notifications.

Upload files from shared directory

You can use the *Source Media Import* page to upload Windows and Linux `.iso` images to the appliance.

Alternatively, you can use the KACE Media Manager to upload files. However, Quest recommends that you use this page to upload `.iso` files for some platforms (such as CentOS) because Microsoft Windows causes the file names to become truncated. For more information, see Upload files using the KACE Media Manager.

NOTE: Copying and uploading files can take several hours.

1. Copy the `.iso` file that you want to upload to the appliance's `clientdrop` Samba share.
2. On the left navigation pane, click **Library** to expand the section, then click **Source Media** to display the *Source Media* page.
3. Select **Choose Action** > **Import from Clientdrop** to display the *Source Media Import* page.
4. On the *Source Media Import* page, in the *Source Media Name* field, type the name that you want to use for associate with the `.iso` file. For example: *Windows 10 2004 September Update*.
5. Click **Source Media ISO** and select the `.iso` file that you want to upload.
6. Click **Import**.

When the process completes, the image appears on the KACE Systems Deployment Appliance *Source Media* page. If *Source Media Notifications* are enabled for your user account, a new notification appears. For more information, see Configure User Interface notifications.

View source media details

You can view information about source media, such as the file size and the date that the files were uploaded to the appliance.

1. On the left navigation pane, click **Library** to expand the section, then click **Source Media** to display the *Source Media* page.
2. Under *Name*, select the image to display the *Source Media Detail* page.

   NOTE: You can modify the name of the image and add notes to indicate changes to the image.
3. **Optional**: Click **Cancel** to close the page.
4. Click **Delete** to remove the source media from the appliance.
5. Click **Save**.

Fingerprint source media OS

Fingerprinting an OS allows you to examine its operating system platform and category.

1. On the left navigation pane, click **Library** to expand the section, then click **Source Media** to display the *Source Media* page.
2. Select a source media whose OS you want to fingerprint.
3. Select **Source Media** > **Fingerprint**.

   An alert appears at the top of the page, indicating that the selected source media is about to be fingerprinted. After a few moments, the *Operating System* and *Category* columns of the selected source media are populated with the related information. If the source media is still not recognized, that is indicated in the Operating System column.

View or update source media metadata

You can view the versions and architecture of the supported operating systems, and to update that metadata periodically, as needed.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **General Settings** to display the *General Settings* page.
2. To view the available versions and architecture for each supported OS, under *Source Media Metadata*, click **View Metadata**.

   A dialog box appears, showing the list of the supported operating systems. To close it, click **Close**.
3. To update the source media metadata with the latest information, click **Update Metadata**.

For more information about source media metadata, visit https://support.quest.com/kace-systems-deployment-appliance/kb/278470.

Choosing the type of deployment

You can deploy the operating system to different devices models, and the appliance will pull the drivers from its resource library for scripted installation deployments. You can copy the state of a device, such as all of the drives, the OS and system settings, programs, and files to perform system image deployments.

Scripted installation deployments

Use a scripted installation when using an ISO for the OS and create an answer file for the deployment.

System image deployments

Capture an image from a device including all of the device drives, the OS, system settings, programs, and files.

Deployment methods

- **Automated Deployments**: Uses boot actions to initiate scripted installation and system images deployments. Supports unicast and multicast deployments.
- **Manual Deployments**: Use manual deployments when deploying directly from the source media, for USB image deployments when the target device is not connected to the network.

NOTE: Both deployment methods load the devices in to a KACE Boot Environment or a NetBoot environment to initiate the deployment. For Mac devices, see .

Supported images types

You can capture WIM and K-Image from devices with Windows 7 and higher and UEFI image from devices with Window 8 higher. You can also capture DMG images from Mac OS X devices.

Image types

WIM images

- The WIM image file-based format stores information as files, rather than as sectors. You can add multiple files to a WIM image.
- WIM images provide faster OS installations.
- Multicast WIM image deployments enable you to broadcast one image to multiple devices at the same time to reduce network bandwidth if the routers on your network support multicast. The target devices must have the bandwidth for the image.
- UEFI WIM image deployments larger than 4GB must be provisioned from a network resource, because images larger than 4GB cannot be deployed using a USB flash device.
- WIM image deployments are hardware independent.

K-Images

- The K-Image file-based format stores files as sectors, enables easy editing, and uses de-duplication to eliminate the need to rebuild images.
- K-Images enable you to edit a base image that changes often without having to re-send the entire image or having to recapture or deploy the image.
- K-Image deployments are hardware independent.

UEFI images

- You can capture WIM UEFI images and UEFI K-Images.
- UEFI K-Images larger than 4GB must be provisioned from a network resource, because images larger than 4GB cannot be deployed using a USB flash device.
- Target devices must be UEFI-compatible and require creating a UEFI partition using the *Create UEFI Partitions* pre-installation task.

Managing device inventory

When a device boots in to the KACE Boot Environment (KBE), the appliance identifies the device by its MAC address, lists the device on the *Device Inventory* page, and uploads its hardware inventory information to the appliance. The MAC address and other information about the device appear on the list. The appliance lists devices that are on the network, but have not booted in to the appliance on the *Network Inventory* page.

About adding devices to the appliance Inventory:

- You can list devices in a comma-separated (CSV) formatted file, and upload the file to the appliance.
- You can run a Network Scan to detect devices on the network.
- You can issue a Wake-on-LAN request to power on remote devices.
- You can enter the MAC address to add devices to a boot action deployment.
- You can run device actions, which are scripted actions that can be performed on managed devices.
- You can unregister devices.

Configure and run a network scan

You can configure a Network Scan, or select and run an existing scan to detect devices that are on the network. Running the scan discovers the configured IP range and creates a *Network Inventory* item on the appliance for each address in the range. The MAC address and port status can only be detected for devices on the same subnet as the appliance.

1. On the left navigation pane, click **Devices** to expand the section, then click **Network Scans** to display the *Network Scans* page.
2. Manage the network scan using the following options:
   - **Select Choose Action > New to display the *Network Scan Detail* page to configure the IP range for the scan. The process scans the configured IP range and creates a *Network Inventory* item for each address in the range.**
   - **Select a scan from the list, then select Choose Action > Run Now.**
3. Click **Save**.

Add network inventory to the appliance

You can list devices in a comma-separated (CSV) formatted file and upload the CSV file to the appliance to add devices to the appliance. The appliance identifies the devices listed in the file in the order of IP address, MAC address, and host name.

Each line in the CSV file must specify the IP Address, MAC Address (with colons), and Host Name (optional) in a comma-separated format. For example: 192.168.2.44,00:22:5f:51:eb:df,appliance.

1. On the left navigation pane, click **Devices**, then click **Network Inventory** to display the *Network Scan Inventory* page.
2. Select **Choose Action** > **Upload** to display the *Upload Network Inventory* page.
3. Click **Browse** and select the CSV file.
4. Click **Upload Inventory** to view the list of devices on the *Network Scan Inventory* page.

Select **Choose Action** > **Send Wake-on-LAN** to power on the devices, then create a boot action. See Create a boot action.

Scan active and non-active devices on the network

When performing a network scan, you can specify if the scan should display a list of all IP addresses whether the device is live or not.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **General Settings** to display the *General Settings* page.
2. Under *Server Options*, select the *Display empty scan results in inventory* check box for the network scan to create and display a record for every IP address in the specified range whether the device is live or not. If you do not enable the *Display empty scan results in inventory* check box, the network scan displays only the IP addresses in the range that are live.

Add devices manually

When creating or modifying a boot action, you can add devices to system image and scripted installation deployments by entering the device's MAC address. The devices are added to the appliance inventory when the deployment is initiated.

1. On the left navigation pane, click **Deployments**, then click **Automated Deployments** to display the *Automated Deployments* page.
2. Select the name of the deployment of which you want to add devices to display the *Automated Deployment Detail* page.
3. Under *Options* > *Schedule*, select one of the following to run the deployment:
    a. *Run at next boot*: Initiates the deployment on the next network boot.
    b. *Schedule to run later*: Specifies a day and time: *Run once on: every* (day), *at*: H (hour), and M (minute). *Run repeatedly* runs the deployment every day at the time you specify.
4. Select the deployment *Type*.

    For multicast deployments, you can click **Edit default multicast settings** to change the multicast settings this deployment. To change the settings for all multicast deployments, see Edit the default multicast settings.
5. Under *Devices*, click or enter one or more MAC addresses to add devices that are not in the inventory, then click **Next**. You can also click **Paste multiple MAC addresses** to add multiple MAC addresses, and you can add devices by type from the *View All* drop-down list.
6. Click **Save**.

Join devices to a domain

After you configure and assign a name to a device, you can join the device to a domain using the built-in *Example: Join Domain* post-installation task.

You can customize the script using the command-line parameters: **my_domain**, **admin_user**, **admin_password**, and **primary_dns_IP**.

NOTE: The built-in *Example: Join Domain* post-installation application task uses the `join_domain.vbs` Visual Basic script. The `join_domain.vbs` script joins devices running Windows 7 versions and higher.

Table 2. Command-line parameters for joining a domain

Parameter	Description
my domain	The name of the domain to which the script joins the devices.
admin user	The UID of the domain administrator with permission to join the devices to the domain.
admin password	The password of the domain administrator account.
primary dns IF	**Optional**: The IP address of the primary DNS server.

1. In *File*, click **Replace** to upload a different script.
2. On the left navigation pane, click **Library** to expand the section, then click **Post-installation Tasks** to display the *Post-installation Tasks* page.
3. Click **Example: Join Domain**.

   The *Post-installation Task Detail* page appears.
4. Click **Duplicate** at the bottom of the page.

   A new task named *Copy of Example: Join Domain* is created.
5. In *Name*, enter a logical name for the task, such as Join **MyCompany** Domain.
6. In *Command Line*, change **my_domain**, **admin_user**, and **admin_password**.
7. Select the *Reboot Required* check box to reboot the appliance and run the next task in the sequence.
8. Click **Save**.

   The task is now available to assign to a scripted installation or a sysprepped system image deployment.

Issue a Wake-on-LAN request

Wake-on-LAN enables you to power on devices remotely from the appliance. You can power on devices that are connected to your network, but have not booted in to the appliance and devices that have booted in to the appliance if the devices are equipped with a Wake-on-LAN-enabled network interface card (NIC) and BIOS.

You can power on a group of devices in a label or wake devices individually. See Create and apply labels.

1. On the left navigation pane, select **Devices** > **Device Inventory** to power on devices that have booted in to the appliance or select **Network Inventory** to power on devices that have not booted in to the appliance.
2. Select the devices to power on.
3. Select **Choose Action** > **Send Wake-on-LAN**.

After devices are powered on, you can go to the left navigation pane, and click **Deployments** to create a boot action and run the deployment now or schedule the deployment to run later.

Deploy to devices in the KACE Systems Management Appliance inventory

When the appliance is linked to one or more KACE Series Management Appliances v5.4 and higher, you can deploy the OS to devices listed on the *KACE SMA Inventory* page.

1. On the left navigation pane, click **Devices**, then click *KACE SMA Inventory* to select the devices to image.
2. Select **Choose Action** > **New Boot Action**.
3. Create the boot action, see Create a boot action.

View device details from a network scan

You can view whether the appliance was able to reach a device, if the device requested a network boot from the appliance, the TCP and UDP port status, and the drivers that the device requires against the available drivers.

1. On the left navigation pane, click **Devices**, then click **Network Inventory** to display the *Network Scan Inventory* page.
2. Select the device to view the following details:

Option	Description
Ping Status	Shows whether the appliance was able to reach this device.
PXE Status	Indicates whether this device (identified by the MAC Address) has ever requested a network boot from the appliance.
TCP Port Status	Shows the state of TCP ports scanned during the last Network Scan that included this device. An *open* status indicates that the appliance was able to open a connection to a network server running on the device.
UDP Port Status	Shows the state of the UDP ports scanned by the last Network Scan that included this device. **NOTE:** An open/filtered state indicates that the appliance did not receive a port closed message from the device and was unable to determine the status. Most firewall software does not send port closed messages from the device, so results might appear incorrect.

Option	Description
Driver Compatibility Report	Lists the drivers that the device requires against the available drivers for scripted installations.

Apply a KUID to the KACE Agent

Retaining the unique identifier (KUID) of target devices prevents numerous devices from checking in to the appliance with the same KUID number. You can use the built-in *Apply KUID to KACE Agent* post-installation task to retain the KUID, which identifies the KACE Agent installed on target devices. You can also modify the script for the built in *Apply KUID to KACE Agent* post-installation task.

On Windows systems, the appliance retrieves the KUID of a system, stores it temporarily, and then copies it to the workstation after the deployment.

For Mac systems, the appliance includes some scripts that can used to implement this process. For more information, see http://www.itninja.com/blog/view/maintain-kuid-of-a-macintosh-system-using-the-k200.

1. On the left navigation pane, click **Library** to expand the section, then click **Post-installation Tasks** to display the *Post-installation Tasks* page.
2. Click **Apply KUID to KACE Agent** to display the *Post-installation Task Detail* page.
3. In *Name*, enter a logical name to identify the task.
4. Select a *Runtime Environment*. See About runtime environments.
5. In *File*, click **Replace** to upload a different script.

   The uploaded file can be a single file, or a ZIP archive containing multiple files. ZIP archives are uncompressed on the appliance before deployment starts.
6. Next to *Upload file*, click **Browse** to select the appropriate file.
7. Select the *Reboot Required* check box to reboot the appliance and run the next task in the sequence.

See Assign tasks to system deployment or Assign tasks to scripted installation deployment.

Delete devices from Device Inventory

You can delete devices from *Device Inventory*, which lists all of the devices that have booted in to the appliance.

1. On the left navigation pane, click **Devices**, then click **Device Inventory** to display the *Device Inventory* page.
2. Select the devices to delete.
3. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Delete devices from Network Inventory

You can delete devices from *Network Inventory*, which lists all known devices including devices detected during a network scan, devices that have booted in to the KBE, devices uploaded from an inventory file, and devices added using the MAC address.

Deleting devices from Network Inventory that have booted in to the KBE deletes the corresponding *Device Inventory* devices. If you delete the MAC address from the *Network Inventory*, the record is removed from the *Device Inventory* and any corresponding boot actions are also deleted.

1. On the left navigation pane, click **Devices**, then click **Network Inventory** to display the *Network Scan Inventory* page.
2. Select the devices to delete.
3. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

Unregister devices

You can delete devices from *Device Inventory* to unregister devices and to free up a licensed seat.

Deleting devices from *Device Inventory* deletes the corresponding *Network Inventory* devices if the device in Network Inventory has booted in to the KBE. If you delete the MAC address from a *Network Scan*, the record is removed from the *Device Inventory* and any corresponding boot actions are also deleted.

When you reach the device limit associated with your license, a warning alert appears on the Home *Dashboard*. To purchase additional seats, visit https://support.quest.com/contact-us/licensing, and then go to the *Registration and Licensing* page to update your license key. For more information about the Dashboard, see Using the Dashboard.

1. On the left navigation pane, click **Devices**, then click **Device Inventory** to select the devices to unregister.
2. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

About the device action icons

The appliance provides device action icons, which are scripted actions that can be performed on managed devices. There are several pre-programmed actions available. To run device actions, you must have the Administrator Console open in Internet browser.

Table 3. Device action icons

Remote access program	Host requirements	Client requirements	Description
SecureCRT	`crt.exe`	SSH client	Connects to devices by default using SSH on port 8443.
DameWare® Mini Remote Control	`dwrcc.exe`	DMRC client	Installs on the device the first time a connection

Remote access program	Host requirements	Client requirements	Description
			is opened.
Microsoft Remote Desktop	`mstsc.exe`	Remote Desktop	Opens a remote desktop session with the device. Only supports Windows devices.
Ping	`ping.exe`	None	Handles the connection request if the device is online.
PuTTY	`putty.exe`	None	Opens an SSH connection from the browser host to the target device.
Telnet	`telnet.exe`	None	Opens a session from the browser host to the target device.
TightVNC	`vncviewer.exe`	None	Opens a session from the

Remote access program	Host requirements	Client requirements	Description
			browser host to the target device.
VNC-Java Remote Control	None	VNC Java Client	Opens a session from the browser host to the target device that has network booted in to the KBE. Requires a Java virtual machine (JVM).

Run device actions

You can run device actions, which are scripted commands that you run on devices remotely. To run device action on remote devices, the programs must be installed on the devices.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **General Settings** to display the *General Settings* page.
2. Under *Server Options*, select a program from the **Icon: Action:** drop-down list next to *1* or add your own action.
3. Enter your own action, in *Icon: Device Action* next to *2* enter:

   ```
   executable_name appliance_host_name | appliance_host_IP
   ```

   where `appliance_host_name` and `appliance_host_IP` are the host name and IP address of the appliance. Some programs require a protocol, port, or URL. For example, Microsoft Edge requires leading slashes to indicate a network address: `\\appliance_host_name`.

   The **executable_name** is the full path to the program start-up file on the browser host, including the command-line parameters. To start the session, the software must be present on the browser host and the target device.

NOTE: If you specify a static host name or IP address, the icon starts a session with the specified address only.

4. Click **Save**.

The appliance displays the device action icon next to host name or IP address of the device on the *Device Inventory* page.

Access remote devices using a VNC session

You can access remote devices using the pre-programmed VNC-Java Remote Control device action.

The VNC program must be selected from the **Icon: Action:** drop-down list on the *General Settings* page. See Run device actions.

1. Boot the target device in to the KACE Boot Environment.
2. Log in to the KACE Systems Deployment Appliance Administrator Console.
3. On the left navigation pane, click **Devices**, then click **Device Inventory** to display the *Device Inventory* page.
4. In the menu bar *Host / IP Address* column, click the device action.

   A new browser displays the host name or IP address of the device. If the device is available, a password prompt appears.
5. Type the correct VNC password and click **OK**.

You can change the VNC password. For more information, see Set the VNC® password.

The Boot Manager appears on the target device. You can perform deployments and troubleshoot devices.

Using labels

Labels enable you to organize the appliance components, which can be useful for grouping new devices, grouping devices by deployment type, users, user state templates, and user profiles and data. You can apply the same label to more than one component.

Create and apply labels

You can manually apply labels to users, devices, scripted installations, system images, user states, or USMT scan templates with criteria that is specific to your environment.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Labels** to display the *Labels* page.
2. Select **Choose Action** > **New** to display the *Label Detail* page.
3. Assign a name to the label and add any notes to identify the label.

   If you modify the name of an existing label, the appliance automatically updates the label for all of the components to which the label was applied.
4. Click **Save**.
5. Go to the page for the component to which you want to apply the label.
6. Select the check box next to the components that you want to apply the label.
7. Select **Choose Action** > **Apply Labels** to display the *Apply Labels* page.
8. Select one or more labels that you want to apply, then drag the labels to the *Apply these labels* section, and click **Apply Labels**.

   The label name appears next to the component.

You can filter components by label from the **View by** drop-down list.

Remove components from a label

You can remove users, devices, scripted installations, system images, user states, and USMT scan templates from a label.

1. Go to the page for the component, and select the components that you want to remove from a label. For example, to remove devices from a label:
   a. On the left navigation pane, click **Devices** , then click **Device Inventory**, to display the *Device Inventory* page, and to view the devices to which a label is applied.
   b. Select the devices that you want to remove from the label.
2. Select **Choose Action** > **Remove Labels** to display the *Remove Labels* window, then select the labels, and click **Remove Labels**.

Delete a label from the appliance

When you delete a label from the appliance, any components that were assigned to the label are automatically removed.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Labels** to display the *Labels* page.
2. Select the check box next to the label you want to delete.
3. Select **Choose Action** > **Delete**, then click **Yes** to confirm.

You can also delete labels from the *Label Detail* page.

View the components assigned to a label

You can view the components assigned to a label.

1. Go to the page for the component to which you want to view the label.
2. Select **View by** > **Label**, and click the label name under that group.

The components assigned to that label display in the list.

Creating a Windows or Linux Boot Environment

You can create a KACE Boot Environment (KBE) for Windows systems using the KACE Media Manager. For Linux systems, when you upload a Linux source media, the appliance automatically creates a Linux boot environment.

For Windows boot environments, install the Windows ADK and the KACE Media Manager on the Administrator device where you installed the appliance. The Windows ADK provides network card drivers that the KBE requires to boot target devices. Target devices must be on the same network as the appliance.

You can import a KBE from a different location, by exporting the KBE from a different appliance, and saving the exported `.pkg` file to the appliance `restore` directory. See Import appliance components.

NOTE: The KBE for Windows contains fonts for most scripts, such as Latin, Greek, and Cyrillic. If you add Asian fonts after you build the KBE, the appliance requires that you rebuild the KBE. By default, the embedded font support in the KBE is disabled. You can enable font support using the language options on the *Language* page.

Create a Windows boot environment

You can use the KACE Media Manager to create a Windows KACE Boot Environment (KBE) or a NetBoot environment to boot devices to capture images and to deploy operating systems.

Download and install the KACE Media Manger. See Download and install the KACE Media Manager. For more information about this tool, see About the Media Manager.

1. Run the Media Manager from **Start** > **All Programs** > **Quest** > **KACE Media Manager**.
2. In Media Manager, in the left pane, click **General Settings**.

   The *General Settings* page appears on the right.

   NOTE: This page appears by default if this is the first time you run the Media Manager.
3. On the *General Settings* page, in the *SDA Hostname* field, enter the IP address of the appliance.
4. In the *SDA IP Address* field, enter the IP address segments of the appliance.
5. In the *SDA Samba Share Password* field, enter the password. This password must match the password that you entered in the *SDA Samba Share Password* field on the *General Settings* page.

   NOTE: If you change the Samba share password on the *General Settings* page, all Windows boot environments are automatically updated to use the new password.
6. In the *WAIK or WADK Path* field, provide the path to the applicable Windows AIK or ADK files. For example:
   - WinPE 10 Win10 x86 ADK `C:\Program Files\Windows Kits\10`
   - WinPE 4 Win8 x64 ADK `C:\Program Files(x86)\Windows Kits\8.1`

   If you installed the Windows ADK somewhere else, browse to and select the correct path.
7. In Media Manager, in the left pane, click **Create KBE**.

The *Create KBE* page appears on the right.

8. On the *Create KBE* page, on the *General* tab, in *Name*, review the KBE name. This automatically-generated string identifies the KBE on the appliance. You can update the KBE name, if needed.

   When you upload the KBE to the appliance, the process first verifies that the name is unique on the appliance. If there is already a KBE with the same name on the appliance, an error message appears, instructing you to change the KBE name. The process creates the KBE only after a successful verification of the provided KBE name.

9. In *Architecture*, select the KBE architecture you are booting in to, for example **32-bit** or **64-bit**.
10. Set the language for your region from the *Language* drop-down list.
11. Before you start the upload, update the WinPE related drivers necessary to boot the target device in to the KBE. See Update Windows drivers.
12. Click **Upload KBE**.

    The new KBE appears on the *Boot Environments* and *Source Media* pages.

Set the new KBE as the default.

Create a Linux boot Environment

When you upload a Linux source media, the appliance automatically creates a Linux boot environment.

1. Specify the source media used to install the OS during deployment, such as CD-ROM or network install. To do that, open the *Boot Environment Detail* page for this KBE, and select the appropriate **PXE Initrd File** option.
2. Specify one or more package repositories associated with this OS. To do that, open the *Source Media Detail* page associated with this KBE, and under *Package Repositories*, specify the URLs, as required.
3. **Optional**. To save Linux packages used during the installation to the appliance, on the *General Settings* page (KACE Systems Deployment appliance only), or *Remote Site Settings* page (Remote Site Appliance only), under *Linux Repository Cache Options*, select **Enable Repository Caching**. Selecting this option speeds up deployments and decreases overall bandwidth usage in organization with a high number of managed devices.

The name of the newly created Linux boot environment is the same as the name of the Linux source media with the `BE` suffix. For example, if you upload a Linux source media called `CentOS`, the appliance assigns `CentOS BE` as the boot environment name.

Update Windows drivers

You can update the Windows Pre-installation Environment (WinPE) related drivers necessary to build a KACE Boot Environment (KBE) and add the drivers to the appropriate `kbe_windows_x64` or the `kbe_windows_x86` share directory on the appliance.

1. Go to https://support.quest.com/kb/111717 to download the drivers. Use your Support credentials to log in, then select **KBE Driver Pack**.
2. Navigate to the `<appliance>/driver_packs` folder to download the appropriate WinPE driver pack.
3. Manually copy the drivers to one of the following directories:
   - **\\<appliance_IP>\drivers\kbe_windows_x86**
   - **\\<appliance_IP>\drivers\kbe_windows_x64**
4. Re-cache the drivers. See Re-cache drivers.

Set the new KBE as the default.

Set new KBE as default for the appliance

You can set a KACE Boot Environment (KBE) as the default KBE for the appliance.

NOTE: You can also set the default KBE for each linked RSA. For more information, see Set default KBE for the RSA.

If you change the share password, create a new KBE using the new password.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **General Settings** to display the *General Settings* page.
2. Under *Boot Environment Options*, select the new KBE.
3. Click **Save**.

Tip: **TIP:** When you review the details of a KBE using the *Boot Environment Detail* page, the *Default* field indicates if the selected KBE is a default boot environment.

Hide boot environments from the PXE boot menu

Preboot Execution Environment (PXE) is a standard client–server environment that allows administrators to boot a PXE-enabled system using a collection of files stored on a network server. In a default installation, a PXE boot menu lists all Windows and Linux boot environments that exist on the appliance. Boot environments provide the drivers and other resources that a target device requires to network boot from the appliance.

In some cases, your appliance may have one or more older KACE Boot Environments (KBEs) that you do not want to appear in the PXE (Preboot Execution Environment) boot menu. You can choose to display or hide boot selected boot environments available on the KACE Systems Deployment Appliance, or on all associated Remote Site Appliances.

1. On the left navigation pane, click **Deployments**, then click **Boot Environments** to display the *Boot Environments* page.
2. Select the boot environment that you want to install to the USB flash device to display the *Boot Environment Detail* page.
3. To hide this boot environment from the KACE Systems Deployment Appliance PXE boot menu, select **Hide Boot Environment from SDA PXE Boot Menu**.
4. To hide this boot environment from the PXE boot menu of all associated Remote Site Appliances, select **Hide Boot Environment from all RSA PXE Boot Menus**.

   After selected this option, if you want this boot environment to appear on a specific Remote Site Appliance, and to remain hidden on all other Remote Site Appliances, on the *Remote Site Detail* page, under *Boot Environments*, in the row containing the newly hidden Boot Environment, you must clear the **Hidden** check box. Making this change does not affect any other Remote Site Appliances.
5. Click **Save**.
6. Initiate the PXE boot menu on the associated appliance, and verify that the newly hidden boot environment no longer appears in the list.

Best practices: Create a KACE Boot Environment (KBE) for Windows

Some business environments can have strict policies and software that may keep the KACE Media Manager from creating a KACE Boot Environment (KBE) successfully.

You may need to set up an isolated system for the purpose of creating KBEs. Here is the recommended flow of actions:

- Set up a system or a virtual machine (VM) that can reach the appliance with the following software:
  - Windows 7, 8, 8.1 or 10
  - Windows AIK, Windows ADK 8, Windows ADK 8.1 or Windows 10 ADK
  - The latest version of the KACE Media Manager

- Do not add that system to your domain.
- Do not install any security or anti-virus software.

The recommended process for creating a new KBE is provided below.

1. Prepare the KBE drivers.
   a. Move out (or delete) any items in the `kbe_windows_xXX` directories located in the appliance drivers share (`\\`**appliance**`\drivers`).
   b. Download the KBE Driver Pack for the desired WinPE version. For more information, visit https://support.quest.com/kb/SOL111717.
   c. Extract the downloaded driver pack and copy the contents from the desired architecture's folder into the `kbe_windows_xXX` directory located in the appliance drivers share.

   NOTE: You should only have the drivers for one WinPE version at a time in the `kbe_windows_xXX` directories.
2. Build the KBE.
   a. Open the KACE Media Manager.
   b. On the *General Settings* page, enter the appliance IP address.
   c. Enter the Samba share password.
   d. Ensure the *WAIK or WADK Path* field points to the correct version of Windows AIK or Windows ADK:
      - WinPE 3 needs to point to the Windows AIK installation directory.
      - WinPE 4 needs to point to the Windows ADK 8.0 installation directory.
      - WinPE 5 needs to point to the Windows ADK 8.1 installation directory.
      - WinPE 10 needs to point to the Windows ADK 10 installation directory.
   e. On the *Create KBE* page, on the *General* tab, review the automatically generated name for the boot environment. You can edit this value, but keep in mind that the KBE name must be unique. Quest recommends that you include the architecture, WinPE version, and the date in the name. For example: `WinPE 5 x64 4-5-2019`.
   f. Select the desired architecture.
   g. Select the desired language.
   h. Click **Upload KBE**.

If you need to add additional drivers for your model to work, contact Quest Support to ensure the driver pack is updated with those drivers.

Managing drivers

You can manage the network and mass storage drivers required to build the KACE Boot Environment from the `drivers` share directory. You can manage the drivers that the operating system requires by enabling the Driver Feed, which downloads and installs drivers to the `driver_postinstall` directory.

The appliance's driver library is a network share that stores the drivers that the appliance and Remote Site Appliance deployments use. The appliance automatically installs the drivers as part of the deployment, and enables uploading drivers for peripherals and hardware that are not included in the Source Media or the KACE Boot Environment (KBE). The appliance hosts Samba shares, and provides three directories to help you manage drivers.

Downloaded drivers are stored in the `drivers_postinstall` share directory using the following folder structure:

- **Virtual devices**: `<OS_name>/<OS_version>/<OS_platform>/any/vmware|hyperv/`. For example: `/windows/7/x64/any/vmware/`.
- **Physical devices**: `<OS_name>/<OS_version>/<OS_platform>/<build_version>|any/<manufacturer>/<system_ID>/`. For example: `/windows/7/x64/any/dell/049a/`.

Ensure that you set the appliance Samba Share Password on the *General Settings* page.

About adding drivers to the drivers_postinstall directory

- You can add device drivers that do not get updated from the Driver Feed to the `drivers_postinstall` directory.
- You can organize the drivers under the `drivers_postinstall` directory using the above folder structure.

About adding drivers to the drivers directory

- You can add any driver type to the drivers directory. Quest recommends only adding the network and storage drivers required to build the KACE Boot Environment (KBE).
- The drivers directory is organized into subdirectories: two boot environments and a directory for each of the supported operating systems. Each KBE and operating system type requires its own driver versions. You can create folders under the drivers share directory to organize the drivers.
- The added drivers must match the version of the WinPE that you are using.
- Drivers that are included in a single `.exe` or `.msi` file require extracting the files before adding the drivers to the folder.

About adding drivers to the restore directory

- You can add driver packages that are larger than 1.5 GB to the `restore` directory.

NOTE: The *Package Management Export* feature creates packages for larger driver files that you can import from the `restore` directory to the appropriate `drivers` share directory to make the drivers available to the appliance.

Add drivers to system images

Enabling the Driver Feed for sysprepped system images captured from the KACE Systems Deployment Appliance and the Remote Site Appliance (RSA) adds the drivers automatically when you deploy the image. You can also install missing drivers on the device where you captured the image, re-capture the image, then upload the image to the appliance.

Use the Microsoft Sysprep tool to generalize the image to resolve duplicate device names and duplicate security identifiers (SIDs). For more information on the best practices for capturing images, go to https://support.quest.com/kb/121734.

For sysprepped system images captured from an RSA, the corresponding drivers should be available on the KACE Systems Deployment Appliance and synchronized from the KACE Systems Deployment Appliance to the RSA.

For Windows K-Images and WIM images, the *Sysprepped* field on the *System Image Detail* page indicates if an image is sysprepped.

1. On the left navigation bar, click **Deployments**, then click **System Images** to display the *Systems Images* page.
2. Select the image to display the *System Image Detail* page.
3. Under *Deploy options*, ensure the **Use driver feed (only with Sysprepped images)** check box is selected.

   Optional. You can enable this option by default on the *General Settings* page:

   1. Open the Administrator Console in a new browser instance or tab.
   2. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **General Settings** to display the *General Settings* page.
   3. Under *Imaging Options*, select the *Enable driverfeed for newly captured sysprepped images* check box. Selecting this option automatically adds drivers to the target system deployed with newly captured sysprepped system images.
   4. Click **Save**, and return to the *Deploy Options* on the *System Image Detail* page.
4. **Optional**: Click **Duplicate** to copy the image and edit it, as needed.
5. Click **Save**.

Adding drivers to scripted installation deployments

You can enable the Driver Feed to update the appliance with the latest device-specific driver packages automatically. When this feature is enabled, any older driver versions that are detected are deleted from the appliance, and replaced with their latest versions. You can also get the drivers from a manufacturer's website or from a different resource, and add the drivers manually to a scripted installation deployment.

During a scripted installation deployment, the appliance automatically pulls all of the drivers from the drivers directory in to the scripted installation. When device drivers or other drivers are in the drivers directory, the scripted installation might fail.

Enable Driver Feed to automate driver updates

When you enable the *Driver Feed*, the appliance performs nightly checks for the latest device-specific drivers. If there is a newer version, the feed updates the database and displays the available drivers on the *Driver Feed* page.

You can enable the Driver Feed for images captured from the appliance and images captured from a Remote Site Appliance (RSA).

1. On the left navigation bar, click **Library** to expand the section, then click **Driver Feed**.
2. Select **Choose Action** > **Manage Driver Feed Settings** to display the *Driver Feed Settings* page.
3. Select the *Enable Driver Feed* check box and click **Save**.
4. **Optional**. If you want to download updated drivers as they become available, select **Automatically Download Updated Drivers**. To disable this option, clear the check box.
5. Click **Check for Updates**.
6. Click **Save**.

The *Driver Feed Status* displays `Checking for Updates`. You can view the list of available driver packages on the *Driver Feed* page, and download and install packages to the appliance. You can also subscribe to an email notification for driver feed activity. For more information, see Configure email notifications.

NOTE: The *Dashboard* enables you to install the *Driver Feed* widgets that show which drivers are new, updated drivers, and drivers that have been updated based on what is installed.

Install driver packages to the appliance

You can select specific driver packages to download and install from the Driver Feed to make them available to the appliance for scripted installation and system image deployments.

1. On the left navigation bar, click **Library** to expand the section, then click **Driver Feed**.
2. Select one or more packages to download and install.

   The drivers are installed in the `drivers_postinstall` share directory.
3. Select **Choose Action** > **Download**.

   When the process completes, the *Status* column displays Installed into driver share. You can view the installed drivers on the *Drivers* page.
4. On the left navigation bar, click **Library** to expand the section, then click **Drivers** to display the *Drivers* page.

Disable Driver Feed

Disabling the Driver Feed prevents the feed from overriding newly added drivers. You can disable the Driver Feed for images captured from a appliance and for images captured from a Remote Site Appliance (RSA).

You can manually add and remove drivers. For example, you can add device drivers that do not get updated from the Driver Feed or device drivers to the `drivers_postinstall` directory. You can add and remove network and storage drivers to the `drivers` directory.

1. On the left navigation pane, click **Library** to expand the section, then click **Driver Feed**.
2. Select **Choose Action** > **Manage Driver Feed Settings** to display the *Driver Feed Settings* page.
3. Clear the *Enable Driver Feed* check box.
4. Click **Save**.

Create folders to add device-specific drivers

When adding drivers manually, you can create folders to organize the device-specific drivers by assigning the manufacturer name to a folder, and adding subfolders under the manufacturer name to organize further.

View the appliance Driver Compatibility Report, which lists the drivers that the device requires compared to the drivers available on the Source Media.

1. Access the `drivers_postintal`l share directory of your appliance from the UNC path `\\<appliance>\drivers_postinstall` where `<appliance>` is either the IP address or the DNS name of the appliance.
2. Create the folder using the Manufacturer name\OS Name\Model name structure.

   The path to the drivers, including the driver name, cannot exceed 255 characters, and the directories and driver names do not support special characters. You can run the `driver_feed_discovery_tool.vbs` script on the device to get the device model and manufacturer name. The script is located in the `drivers_postinstall\feeds_tools` directory.

Generate appliance package to import large driver files

You can generate a package for files that you download from a manufacturer's website or from a different source and for files that are larger than 1.5 GB. The appliance `restore` share directory is the repository for storing packages and files that you can import to the appliance.

The *Package Management Export* feature creates a `.pkg` file. The `.pkg` file contains the drivers and an `.xml` file with the same name as the `.pkg` file. The `.xml` file contains metadata about the drivers. A separate package is created for each selected driver package.

1. On the left navigation pane, click **Settings** to expand the section, then click **Package Management** to display the *Package Management* page.
2. Click **Export SDA Packages** to display the *Export List* page.
3. Select the driver package to export.
4. Select **Choose Action** > **Export Selected**.

   Ensure that export completes before selecting a different export.

If you start an export of a package while an export process is in progress, the package waits in the queue. The packaging process can take a few minutes to several hours to complete, depending on the size and number of items in the package. The *Status* column indicates when each export completes.

Next, import the driver packages to the appliance.

Import driver packages to the appliance

You can import device-specific and network or storage driver packages from the `restore` share directory to the appliance. The Import feature is useful when drivers packages are larger than 1.5 GB and when you need to download driver packages from a manufacturer's website, such as audio, video, and chipset drivers that have complex configurations or dependencies.

1. On the left navigation pane, click **Settings** to expand the section, then click **Package Management** to display the *Package Management* page.
2. Click **Import SDA** Packages to display the Import List page, which lists all of the packages in the `restore` share directory.

   For more information, see Import appliance components.

3. Select the driver package to import.

   If the drivers are required for network booting, add the WinPE package.

4. Select **Choose Action** > **Import Selected**.

If the drivers are network or storage drivers, re-cache the drivers. See Re-cache the network and storage driver directory.

Understanding KACE Boot Environment drivers

When adding the network and storage drivers for the KACE Boot Environment (KBE), the drivers share directory requires re-caching the corresponding driver folder and building a new KBE.

There are two boot environment folders in the `drivers` share directory, and a folder for each supported operating system. Each KBE and operating system type requires its own driver version.

The `drivers` share directory has the following directory structure:

- `kbe_windows_x86`
- `kbe_windows_x64`

You can store any type of drivers in the drivers directory, but Quest recommends storing only the network drivers to this directory.

Add network and storage drivers manually

You can get the network and storage drivers from the manufacturer's website or from a different resource, and add the drivers manually.

Move any drivers that are currently stored in the `drivers` directory to a different source or device to prevent conflict. When switching from a lower version of WinPE KBE to a higher version or conversely, remove any drivers that were downloaded from the Driver Feed because the drivers are similar. Also, to avoid slow deployments, remove drivers for devices that are no longer in your environment.

The driver files from a manufacturer's site generally consist of `.inf`, `.sys`, and `.cat` files. There might be dependent files that the `.inf` file requires to load the drivers.

1. Access the drivers share directory of your appliance from the UNC (Universal Naming Convention) path `\\<appliance>\drivers`, where `<appliance>` is either the IP address or the DNS name of the appliance.
2. Download and extract the drivers from the manufacturer's website or any other source to a device that can access the appliance `drivers` share directory.
3. Add the driver files to the folder that corresponds to the process to which you want to make the drivers available. For example, add the `KBE_driver_pack/kbe_windows_x86` directory in to the corresponding `kbe_windows_x86` directory on the appliance. Also, copy the contents of the `KBE_driver_pack/kbe_windows_x64` directory in to the corresponding `kbe_windows_x64` directory on the appliance.

   NOTE: Do not combine Windows 7, Windows 8, Windows 8.1, and Windows 10 drivers in the same KBE folder. You cannot add drivers for WinPE 5.0, which uses the drivers for Windows 8.1 to a folder for WinPE 4.0, which uses the drivers for Windows 8.0. Windows ADK 8.0 supports WinPE 4.0. Windows ADK 8.1 supports WinPE 5.0.

   For additional information on Quest KBE driver packs, go to https://support.quest.com/kb/111717.
4. Re-cache the drivers. See Re-cache the network and storage driver directory.

   Adding drivers requires re-caching the drivers, and rebuilding the KBE to make the newly added drivers available.

Use the latest version of the KACE Media Manager and the Windows ADK to build the WinPE KBE for Windows 7 and later. The Media Manager cannot overwrite an existing KBE; do not name a KBE using a name that exists.

Re-cache the network and storage driver directory

Re-caching the drivers notifies the appliance that updates have been made to the drivers, and makes the drivers available to Media Manager to build a boot environment for scripted installations only. You can re-cache only the directories where changes were made to the drivers, or re-cache the entire driver database.

Verify that the drivers are in the `drivers/kbe_windows_x86` or the `drivers/kbe_windows_x64` directory before you re-cache.

NOTE: Re-caching drivers only scans the `drivers` share directory, not the `drivers_postinstall` directory.

1. On the left navigation bar, click **Library** to expand the section, then click **Drivers** to display the *Drivers* page.
2. Select **Choose Action** > **Manage Drivers**, and click **Recache All Drivers**. You can also select only the directories where changes were made to update the appliance faster.

   NOTE: Removing drivers before re-caching might cause booting, installation, or recovery errors that can result in a system failure and compromise the results in the Driver Compatibility Report.

Add drivers as a post-installation task

You can create a `.zip` file for drivers, then upload the `.zip` file to the appliance as a post-installation task.

Adding drivers as a post-installation task is useful when device-specific drivers are not in the Driver Feed, to add drivers, and to add drivers that do not get installed as part of the operating system during a scripted installation.

1. On the left navigation pane, click **Library** to expand the section, then click **Post-installation Tasks** to display the *Post-installation Tasks* page.
2. On the list page that appears, select **Choose Action** > **Add Application**.
3. In *Name*, enter a logical name to identify the task, such as Install Dell E6410 Chipset Drivers.
4. Select a *Runtime Environment.* See About runtime environments.
5. Next to *Upload file*, click **Browse** to select the appropriate file.
6. Select the *Reboot Required* check box to reboot the appliance and run the next task in the sequence.
7. In *Notes*, add a note to identify the task.
8. Click **Save**.

See Adding tasks.

View list of missing drivers

After a device network boots in to the KACE Boot Environment (KBE), the appliance automatically records the device's hardware inventory details. The Driver Compatibility Report lists the drivers that the device requires against the drivers available on the Source Media.

1. Log on to the appliance Administrator Console.
2. On the left navigation pane, click **Devices**, then click **Device Inventory** to display the *Device Inventory* page.
3. Click the host name or IP address of the device to display the *Device Detail* page.
4. Under *Driver Compatibility Report*, select the operating system, then click **Show Compatibility**.

Managing network drivers

You can manually download drivers to the `drivers` share directory, which is organized in to subdirectories. You can store any type of drivers to the `drivers` directory, but Quest KACE recommends storing only the network drivers to this directory.

There are two boot environment folders in the `drivers` share directory and a folder for each supported operating system. Each KBE and operating system type requires its own driver version.

The drivers share directory has the following directory structure:

- kbe_windows_x32
- kbe_windows_x64

You can create subdirectories under the KBE folders to organize the newly added drivers.

Best practices for adding drivers

- Name the folder using the device brand name, then create a subfolder with the name of the drivers to add the driver files.
- The path to the drivers, including the driver name cannot exceed 255 characters; the directories and driver names do not support special characters.
- The appliance does not install .exe or .msi files. Extract the files, then add the drivers to the folder.
- Do not combine Windows 7, Windows 8, Windows 8.1, and Windows 10 drivers in the same KBE folder. You can only add drivers for one platform type to a folder. You cannot add drivers for WinPE 5.0, which uses the drivers for Windows 8.1 to a folder for WinPE 4.0, which uses the drivers for Windows 8.0.

  NOTE: Windows ADK 8.0 supports WinPE 4.0. Windows ADK 8.1 supports WinPE 5.0. Windows ADK 10 supports WinPE 10.0.

- Re-cache added drivers, and build a new KBE using the Media Manager. The Media Manager uses the Windows ADK installed on the device to rebuild the KBE, and automatically adds the drivers to the KBE folder.
- Do not name a KBE using name that already exists: the Media Manager cannot overwrite an existing KBE.

Download network and storage drivers

You can go the Quest KACE Support site to download the network and mass storage drivers required to build the KACE Boot Environment (KBE).

1. Move any drivers that are currently stored in the drivers share directory to a different location.

   NOTE: When switching from one version of WinPE KBE to another, remove any drivers that were downloaded from the Driver Feed because the drivers are similar. To avoid slow deployments, remove drivers for devices that are no longer in your environment.

2. For instructions on adding drivers, re-caching, and building a new KBE, see https://support.quest.com/kace-systems-deployment-appliance/kb/111717.

   The extraction process creates a KBE_driver_pack directory, which contains the kbe_windows_x86 and the kbe_windows_x64 directories. The kbe_windows_x86 and kbe_windows_x64 directories each contain a dell-winpe-a0x and kace directory.

3. Access the drivers share directory of your appliance from the UNC path \\<appliance>\drivers where <appliance> is either the appliance IP address or the DNS name.
4. Copy the contents from the KBE_driver_pack/kbe_windows_x86 directory in to the corresponding kbe_windows_x86 directory on the appliance. Also, copy the contents of the KBE_driver_pack/kbe_windows_x64 directory in to the corresponding kbe_windows_x64 directory on the appliance.
5. Create the directory structure for the driver types, for example .inf, .sys, and .cat.

There might be dependent files that the .inf file requires to load the drivers, or you can add drivers that are not in the driver package. Quest KACE recommends placing all files in the same directory as the .inf, .sys, and .cat files.

The command-line tasks from Windows are complete. You can log in to the KACE Systems Deployment Appliance Administrator Console to re-cache the driver directory to which you added the drivers.

6. On the left navigation pane, click **Library** to expand the section, then click **Drivers** to display the *Drivers* page.
7. Select **Choose Action** > **Add Drivers**, and re-cache the directory to which you added drivers.

The driver re-cache scans only the `drivers` share directory. The `drivers_postinstall` directory does not require re-caching.

Use the latest version of the KACE Media Manager and the Windows ADK to build the WinPE KBE for Windows 7 and higher. The new KBE includes the new drivers.

Import driver packages

You can import drivers to a different device or share drivers between KACE SDAs. The appliance lists the driver packages that have been exported and saved with the `.pkg` extension in the `restore` directory.

For information on exporting drivers, see Export drivers.

1. On the left navigation pane, click **Settings** to expand the section, then click **Package Management** to display the *Package Management* page.
2. Click **Import SDA Packages** to display the *Import List* page, which lists all of the packages in the `restore` share directory.
3. Select the package that you what you want to import.
4. Select **Choose Action** > **Import Selected**.

If the drivers are network or storage drivers, re-cache the drivers. See Re-cache drivers.

Display device compatibility

For attended scripted installations, you can add the built-in *Display Device Compatibility* pre-installation task. This task enables you to verify whether all the drivers for the hardware for a device to which you are deploying the operating system are in the appliance prior to running a scripted installation. If there is a discrepancy, the list of hardware without drivers is displayed and the scripted installation is stopped.

1. On the left navigation pane, click **Deployments**, then click **Scripted Installations** to display the *Scripted Installations* page.
2. Select the appropriate scripted installation to display the *Scripted Installation Detail* page.
3. Under *Installation Plan*, add the *Display Device Compatibility* task to the *Run Pre-installation Tasks* column to upload the hardware inventory and display the list of incompatible devices on the target device console.
4. Click **Save**.

View driver compatibility details

After a device network boots in to the KACE Boot Environment (KBE) on the appliance, the appliance automatically records the device's hardware inventory details. You can view the device details and the *Driver Compatibility Report*, which lists the drivers that the device requires against the available drivers for scripted installations.

Network boot the device.

The driver compatibility report is built after you re-cache the drivers, so the report is only run against the drivers in the `drivers` share directory.

1. Log on to the KACE Systems Deployment Appliance Administrator Console.
2. On the left navigation pane, click **Devices**, then click **Device Inventory** to display the *Device Inventory* page.
3. Click the host name or IP address of the device to display the *Device Detail* page.
4. Under *Driver Compatibility Report*, select the operating system, then click **Show Compatibility**.

The compatibility report compares the drivers that the device requires to the drivers available on the source media. You can add missing drivers.

Export drivers

The appliance generates a `.pkg` file that contains the drivers and an `.xml` file with the same name as the `.pkg` file. The `.xml` file contains metadata about the drivers. The `.pkg` and the `.xml` files are saved in the `\appliance_hostname \restore` directory.

1. On the left navigation pane, click **Settings** to expand the section, then click **Package Management** to display the *Package Management* page.
2. Click **Export appliance Packages** to display the *Export List* page.
3. Select the driver package to export.
4. Select **Choose Action** > **Export Selected**.

If you start an export of a different package while an export is in progress, the package waits in the queue.

The packaging process can take a few minutes to several hours to complete, depending on the size and number of packages. The status column indicates when each export completes.

Re-cache drivers

Re-caching the drivers notifies the appliance that updates have been made to the drivers.

Verify that the drivers are in the `drivers/kbe_windows_x86` or the `drivers/kbe_windows_x64` `drivers` directory before you re-cache. Re-caching drivers only scans the `drivers` share directory, not the `drivers_postinstall` directory.

1. On the left navigation pane, click **Settings** to expand the section, then click **Appliance Maintenance** to display the *Appliance Maintenance* page.

   NOTE: You can only update the appliance if your license is up to date. When your license expires, a message appears at the top of the page, instructing you to update your license. The *License Maintenance Status* field on this page indicates the state of your license. To update your license, obtain a new key from your KACE sales representative, and update it on the *Registration and Licensing* page. If one or more Remote Site Appliances (RSAs) are associated with this appliance, the new license key is automatically updated on those RSAs after a synchronization.

2. Under *Utilities* in the *Driver Recache*, section, click **Recache All Drivers**.

   You can also re-cache only the drivers that changed by selecting the specific directory.

Managing operating system drivers

Enabling the *Driver Feed* gets the latest drivers that the operating system requires, then you can select which drivers you want to download. The model-specific packages contain drivers for Windows scripted installations.

About Windows operating system drivers

- You can run the `\<your_appliance_box>\drivers_postinstall\feed_tools\copy_drivers_debug.vbs` script on the device to get the system ID and manufacturer name.
- The Driver Feed adds the operating system and other hardware-related drivers to the `drivers_postinstall` directory using the following folder structure:
  - **Virtual devices**: `<OS_name>/<OS_version>/<OS_platform>/any/vmware|hyperv/`. For example: `/windows/7/x64/any/vmware/`.
  - **Physical devices**: `<OS_name>/<OS_version>/<OS_platform>/<build_version>|any/<manufacturer>/<system_ID>/`. For example: `/windows/7/x64/any/dell/049a/`.

Enable Driver Feed for scripted installations

When you enable the *Driver Feed* to get the latest drivers, you can select which drivers you want to download. The appliance organizes the drivers by device model that the operating system requires for scripted installation deployments.

You can also enable the *Driver Feed* for sysprepped system images. For more information, see Enable Driver Feed for system images.

1. On the left navigation pane, click **Library** to expand the section, then click **Driver Feed**.
2. Select **Choose Action** > **Manage Driver Feed Settings** to display the *Driver Feed Settings* page.
3. Select the *Enable Driver Feed* check box and click **Save**.
4. **Optional**. If you want to download updated drivers as they become available, select **Automatically Download Updated Drivers**. To disable this option, clear the check box.
5. Click **Check for Updates**.
6. **Optional**: Click **Cancel** to close the page.
7. Click **Save**.

The *Driver Feed Status* displays **Checking for Updates**. You can view the list of available driver packages on the *Driver Feed* page, and download and install packages to the appliance.

Enable Driver Feed for system images

Enable the *Driver Feed* for sysprepped system images to get the missing drivers. You can install the drivers on the device where you captured the image, re-capture the image, then upload the image to the appliance. Quest KACE recommends using the best practices for capturing images to avoid installing drivers in system images.

Use the Microsoft Sysprep tool to generalize the image to resolve duplicate device names and duplicate security identifiers (SIDs).

For more information on the best practices for capturing images, see https://support.quest.com/kace-systems-deployment-appliance/kb/121734.

For Windows K-Images and WIM images, the *Sysprepped* field on the *System Image Detail* page indicates if an image is sysprepped.

1. On the left navigation pane, click **Deployments**, then click **System Images** to display the *Systems Images* page.
2. Select the image for the deployment to display the *System Image Detail* page.
3. Under *Deploy options*, ensure the **Use driver feed (only with Sysprepped images)** check box is selected.

   Optional. You can enable this option by default on the *General Settings* page:

   1. Open the Administrator Console in a new browser instance or tab.
   2. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **General Settings** to display the *General Settings* page.

3. Under *Imaging Options*, select the *Enable driverfeed for newly captured sysprepped images* check box. Selecting this option automatically adds drivers to the target system deployed with newly captured sysprepped system images.
4. Click **Save**, and return to the *Deploy Options* on the *System Image Detail* page.

4. **Optional**: Click **Cancel** to close the page.
5. **Optional**: Click **Duplicate** to copy the image and edit it as needed.
6. Click **Save**.

Disable Driver Feed

You can disable the *Driver Feed* to manually download and install drivers, drivers from a different appliance, or drivers stored on a different device.

1. On the left navigation pane, click **Library** to expand the section, then click **Driver Feed**.
2. Select **Choose Action** > **Manage Driver Feed Settings** to display the *Driver Feed Settings* page.
3. Clear the *Enable Driver Feed* check box.
4. **Optional**: Click **Cancel** to close the page.
5. Click **Save**.

Download operating system driver packages

If the *Driver Feed* is enabled, you can view the list of the latest driver packages available from the *Driver Feed*, and download and install the drivers to the appliance.

1. On the left navigation pane, click **Library** to expand the section, then click **Driver Feed**.
2. Select the package(s) that you want to download and install.

   The drivers get installed in the `drivers_postinstall` share directory.
3. Select **Choose Action** > **Download and Install Packages**.

   When the process completes, the *Status* column displays `Installed into driver share`. You can view the installed drivers on the *Drivers* page.
4. On the left navigation pane, click **Library** to expand the section, then click **Drivers** to display the *Drivers* page.

Add drivers to OS as a post-installation task

You can upload driver installation files for drivers that have complex configurations or dependencies, such as chipset drivers that provide the hardware instructions. Creating a `.zip` file of the drivers enables you to add the drivers to the operating system using a post-installation task.

Quest KACE recommends enabling the *Driver Feed* to get the latest drivers to select which drivers you want to download.

1. On the left navigation pane, click **Library** to expand the section, then click **Post-installation Tasks** to display the *Post-installation Tasks* page.
2. Select **Choose Action** > **Add Application** to display the *Post-installation Task Detail* page.
3. In *Name*, enter a logical name to identify the task, such as Install Dell E6410 Chipset Drivers.
4. Select a *Runtime Environment.* See About runtime environments.
5. Next to *Upload file*, click **Browse** to select the appropriate file.
6. Select the *Reboot Required* check box to reboot the appliance and run the next task in the sequence.
7. In *Notes*, add a note to identify the task.
8. Click **Save**.

See Adding tasks.

Capturing images

You can capture UEFI images, WIM images, and K-Images after you boot the device with the image that you want to capture in to the KACE Boot Environment (KBE). The KBE Main Menu loads on to the device when the device boots in to the KBE. You capture images from the device using the *KBE Main Menu*. You can verify that there is enough disk space on the appliance for the image and prepare the image for capture.

Preparing for capture

Follow the best practices for capturing images, such as ensuring that the image is up-to date and that there is enough space on the appliance for the image.

The Quest KACE Support team provides best practices for capturing images. For more information, see, https://support.quest.com/kace-systems-deployment-appliance/kb/121734.

Best practices to prepare for capturing images for deployment:

- Ensure that there is 20 percent free space on the appliance.
- Use only the volume license media instead of the OEM media.
- Create an administrator profile to set up as the default administrator user.
- Capture a non-sysprepped version of your primary image first in case you have to restore the image to the original device.
- Sysprep the image.
- Capture a sysprepped image to the appliance and verify that there is enough space on the appliance for the image.

Capture system images

You can capture images with the KACE Systems Deployment Appliance or remote (RSA) appliances, after you boot the device in to the KACE Boot Environment (KBE).

Run the Sysprep tool on the image to remove any system-specific settings before you boot the device in to the KBE. Quest KACE recommends capturing a non-sysprepped version of your gold image first in case you have to restore the image to the original device.

After the device boots in to the KBE, you can access the built-in VNC remote control software to capture images from remote devices to the KACE Systems Deployment Appliance.

IMPORTANT: Capture of OEM images for purposes of deployment to machines other than the one it is captured from is a violation of Microsoft's Licensing agreement. To create an image for deployment to multiple machines ensure you use Microsoft Volume License Media. Please reference KB 135252 for full details and a link to Microsoft's Licensing brief on re-imaging rights.

1. Boot the device with the image that you want to capture in to the KBE. From the *KBE Main Menu* on the device, click **Imaging**.

Tip: **TIP:** The information appearing at the bottom of this screen provides details about the KACE Systems Deployment Appliance or RSA connected to this KBE, such as its IP address, OS version, architecture, boot mode, Mac address, and other relevant data.

If the device boots in to the hard drive instead of the KBE, boot the device in to the KBE.

2. Click **Capture image of this device**.
3. In *Image Name*, enter a name that identifies the image on the appliance.
4. In *Image Type*, select the type of the image file that you want to create, as required.
5. If you want to capture the image directly to the server, select **Capture directly to server**.

   When an image is captured locally, it is sent to the server through network sockets. Some network configurations may cause issues when files are transferred this way. Streaming the image directly to the server causes its files to be copied directly to the server share instead of using network sockets.

   Only those images captured directly from the server can also be deployed directly from the server.

   - WIM images captured directly to the server must also be deployed directly from the server. This option cannot be changed on the image detail page.
   - If you choose not to select this option, and there is not enough disk space locally, the image is streamed directly to the server.
6. Click **Force continue on errors** to continue the capture and the upload process even if warnings and fatal errors occur.
7. Click **Include debug output in log** to enable debugging level logging and upload the logs to the *Appliance Logs* page.

   Turning on debugging might increase the time it takes to capture and upload the image.
8. Click **Start capture**.

   - A progress bar appears at the bottom of the page, indicating how much progress has been made through the task for each selected partition. You have an option to cancel the capture, if required.
   - When the capture process is complete, a new system image entry appears on the *System Images* page in the KACE Systems Deployment Appliance Administrator Console, and also in the Remote Site Console, if the image is captured using an RSA.
   - If the user subscribed to this UI notification, a notification icon appears in the KACE Systems Deployment Appliance Administrator Console, and also in the Remote Site Console, indicating when the image capture starts, fails, or finishes.
   - The KACE Systems Deployment Appliance assigns an ID to each captured system image.

   Tip: **TIP:** Each system image captured with the KACE Systems Deployment Appliance or its linked RSAs has a unique ID. This allows the appliance to keep track of all the different system images captured with the linked (KACE Systems Deployment Appliance) or remote (RSA) appliances, and to synchronize any images, as you edit them. To find out an ID of a specific system image, hover over the system image name on the *System Images* page. The ID appears in the bottom-left corner.

   NOTE: An image captured on an RSA is only stored on the RSA and does not synchronize. After configuring an image captured from an RSA, on the KACE Systems Deployment Appliance, synchronize that RSA prior to deployment.

Configure the image with all of the required files, tools, and software using a deployment task sequence. You can edit some images or specify their deployment tasks, as required. For more information, see the following topics:

- Edit a system image
- Assign tasks to system deployment

.

Create a single partition

You can add the built-in *Create Single Partition* pre-installation task to create a single primary partition.

1. On the left navigation pane, click **Library** to expand the section, then click **Pre-installation Tasks** to display the *Pre-installation Tasks* page.
2. Select **Create Single Partition** to display the *Pre-installation Task Detail* page.
3. **Optional**: In *Name*, change the name to identify the task.
4. Enter a script to create a partition.
5. In *Notes*, add a note to identify the task.
6. Click **Save**.

   The task is now available to assign to scripted installations, sysprepped system images, and non-sysprepped system image deployments.

Format C drive as NTFS

You can add the built-in *Format C: as NTFS* pre-installation task to format and set the C drive as an NTFS file system.

1. On the left navigation pane, click **Library** to expand the section, then click **Pre-installation Tasks** to display the *Pre-installation Tasks* page.
2. Select **Format C: as NTFS** to display the *Pre-installation Task Detail* page.
3. **Optional**: In *Name*, change the name to identify the task.
4. Click **Save**.

   The task is now available to assign to scripted installations, sysprepped system images, and non-sysprepped system image deployments.

Create a UEFI partition

You can add the built-in *Create UEFI Partitions* pre-installation task, which uses a DiskPart script, to create a Unified Extensible Firmware Interface (UEFI) hard drive partition on Windows 7 x64 SP1 or higher x64 UEFI-enabled devices.

The NTFS format does not work on UEFI-enabled devices. UEFI-enabled devices use the GUID Partition Table (GPT), which uses a global unique identifier for devices that is different from the commonly used Master Boot Record partitioning style in the BIOS.

1. On the left navigation pane, click **Library** to expand the section, then click **Pre-installation Tasks** to display the *Pre-installation Tasks* page.
2. Select **Create UEFI Partitions** from the list to display the *Pre-installation Task Detail* page.
3. **Optional**: In *Name*, change the name to identify the task.
4. In *DISKPART Script*, verify that the command-line options match the ones you want to use.

   The KACE Boot Environment (KBE) automatically identifies the hidden EFI partition while capturing the UEFI image, and assigns the drive letter S during the capture.

   For more information on DiskPart commands, see Common DiskPart command-line options.

5. Click **Save**.

   The task is now available to assign to scripted installations, sysprepped system images, and non-sysprepped system image deployments.

Use the *Apply UEFI Partition* mid-level task to apply the partition.

Apply a UEFI partition

You can apply the UEFI partition that you created as a pre-installation task.

1. On the left navigation pane, click **Library** to expand the section, then click **Post-installation Tasks** to display the *Post-installation Tasks* page.
2. Click **Apply UEFI Partitions** to display the *Post-installation Task Detail* page.
3. In *Name*, enter a logical name to identify the task.
4. Select a *Runtime Environment.* See About runtime environments.
5. In *BAT Script,* verify the script and make any necessary changes.
6. Click **Save**.

   The task is now available to assign to scripted installations, sysprepped system images, and non-sysprepped system image deployments.

Capture System-provided WIM images

You can capture WIM images for faster deployments using automated multicast deployments to send the same WIM image to multiple devices simultaneously. You can also deploy WIM images across all devices in the enterprise, and across hard disks of any size in the KACE Boot Environment (KBE).

The device with the image that you want to capture does not have to match the target devices for deployments; however, drivers are required for each device model to which you are deploying the image.

1. Boot the device with the image that you want to capture in to the KBE. From the *KBE Main Menu* on the device, click **Imaging**.

   If the device boots in to the hard drive instead of the KBE, boot the device in to the KBE.
2. Click **Capture image of this machine**.
3. In *Image Name*, create a name to identify the image.

   The appliance automatically adds the `.wim` extension.
4. In *Image Source*, select the drive letter from where you are capturing the image.

   The appliance automatically adds the colon to the drive letter, for example `C:`
5. Select **Windows Imaging Format (Fast compression)** for Image type.
6. Click **Start capture** to upload the image to the *System Images* page.

   A progress bar appears at the bottom of the page, indicating how much progress has been made through the task for each selected partition. You have an option to cancel the capture, if required.

Edit a system image

You can rename, replace, remove, or edit K-Images and WIM images.

Before modifying a system image, make a backup copy.

The *System Image Detail* page allows you to view the image settings, add a boot action, download the log files for the image, and set the options for how the appliance responds to errors. For Windows K-Images and WIM images, it also indicates if an image is sysprepped.

You can only edit system images on the appliance that captured them. For example, if you view the details of a system image captured by the appliance, you can edit that image on the *System Image Detail* page in the appliance Administrator Console, but not in the KACE Remote Appliance Console. If that system image is captured on the appliance and synced to the RSA, the *System Image Detail* page in the KACE Remote Appliance Console only allows you to review the system image details, but not to edit them. A link appears on this page that allows you to quickly navigate to the *System Image Detail* in the appliance Administrator Console, and edit the system image, as required.

The Installation Plan enables you to create a task sequence by adding the available pre-installation, mid-level, and post-installation tasks to run in the order that you place the tasks for the deployment.

The *Browse Files* option is only available for system images.

1. Select the name of the image to display the *System Image Detail* page to edit the image.
2. Click **Browse Files** to open the *Browsing Files* dialog box to edit the images with the following options:
   - **K-Images only.**
     - Click **Add Drive** to add a partition. The drive name must contain an uppercase letter with a colon at the end.
     - To rename or remove a drive, click the appropriate icon next to the desired drive letter.
   - **Windows K-Images an WIM images only.**
     - To add the contents of a ZIP file, navigate to the directory where you want to add the files, click **Add Zipped Files**, navigate to the desired ZIP file, and click **Submit**, then click **Commit**. The contents of the zipped file are extracted to the selected location. To verify the contents of the system image after committing the change, when the dialog box closes, on the *System Image Detail* page, click **Browse Files** and review the list of files.
     - To rename or remove a drive, click the appropriate icon next to the desired drive letter.
   - **All images.**
     - To add a directory, click **Create Directory**, then type the name of the new directory that you want to add.
     - To add a file, click **Add File**, navigate to the desired file, and click **Submit**.
     - To add the contents of a ZIP file, navigate to the directory where you want to add the files, click **Add Zipped Files**, navigate to the desired ZIP file, and click **Submit**, then click **Commit**. The contents of the zipped file are extracted to the selected location. To verify the contents of the system image after committing the change, when the dialog box closes, on the *System Image Detail* page, click **Browse Files** and review the list of files.
     - To rename, delete, or replace files, hover over the file name, and click the appropriate icon.
     - To rename, delete or download a directory, click the appropriate icon next to the desired directory.
     - To download a file, click the file name.
     - To drill down to the directory contents, click the directory name.

   NOTE: When you replace a file with a different file, the appliance replaces the contents of the files, but retains the original filename.
3. **Optional: WIM images only**. Obtain additional system image information from the Windows registry.
   a. Next to *Registry Info*, click **Show**.
   b. Review the contents of the Windows registry items for the selected system image.
4. **Optional**. Review the latest log file recorded during the system image capture, if applicable.
   - Click **Server Log** to see what the server recorded during the image capture.
   - Click **Client Log** to see what the server recorded during the image capture.

   If size of the log file is greater than 500 kb, you can also download the log file.
5. **Optional: Configuration files only**.

a. Next to *Config XML*, click **Show**, and review the file contents that appear. The contents of the file are read only.
b. To download the file, under the file contents, click **Download XML File**.

6. **Optional: Task files only**.

   NOTE: Read-only users do not have access to this field.

   a. Next to *Task XML*, click **Show**, and review the file contents that appear. The contents of the file are read only.
   b. To download the file, under the file contents, click **Download XML File**.
7. **Optional**: Under *Deploy Options*, select **Remove local files not in image** when restoring the original image to a device, and when files have been added or modified on the device that is not in the original image.
8. Assign tasks to the system image, as required. For more information, see Assign tasks to system deployment.
9. When you finish your edits, click **Cancel** to roll back the changes, or **Save** to apply the changes to the image.

Import WIM images

You can import an existing WIM image to your collection of system images on the appliance. This allows you to manage system images created by a third-party vendor.

To import a WIM image, place a copy of the image file to the appliance's Samba `clientdrop` share.

NOTE: You can only import an image contained in a single WIM file, consisting of a single partition.

During a WIM image import, you must specify its OS architecture. The appliance detects if the imported image is `sysprepped` or not.

NOTE: When the appliance starts importing a system image, if it detects an `unattend` file, it flags the image as `sysprepped`. If the image does not include that file, the appliance flags it as not being `sysprepped`.

This feature is available on the KACE Systems Deployment Appliance and the Remote Site Appliance (RSA).

1. On the left navigation pane, click **Deployments**, then click **System Images** to display the *Systems Images* page.
2. Select **Choose Action** > **Import** to display the *System Image Import* page.
3. Specify the following options:

Option	Description
Image Name	Type the name that you want to assign to this system image.
Operating System	Select the OS architecture used by the WIM image.
Wim File	Select the name of the WIM image file on the Samba `clientdrop` share.

4. Click **Import**.

The *System Image Import* page closes and the *System Images* list page refreshes, showing the newly imported WIM image in the list. In the row containing the imported image, the *Status* column indicates the state of the import operation.

5. **Optional**. When the import is complete, observe the imported image details, and make any changes, as required.
    a. On the*System Images* page, in the row containing the imported image, click the *Name* column to display the *System Image Details* page.
    b. Review the contents of the page.
    c. To download the WIM image, in the *Wim Management* section, in the row containing the partition that you want to download, *Actions* column, click the Download icon. In the dialog box that appears, specify the name to give to the WIM file. Then click **Save**.
    d. Replace the imported WIM image with another one. This is useful, for example if you import a wrong WIM image, or if you make any changes to the WIM image, and want to import the updated image.

    NOTE: Like the original WIM image, the replacement image must also be stored in the Samba `clientdrop` share of the associated KACE Systems Deployment Appliance or RSA, in order to be accessible.

    To do that, also in the row containing the partition that you want to replace, in the *Actions* column, click the Replace icon. In the dialog box that appears, select the desired image file, and click **Replace**.

    The *System Image Details* page closes and the *System Images* list page refreshes, indicating that the WIM image is being replaced in the row containing the imported image, in the *Status* column.

    e. To review the contents of the log file created during image import, click **Show the log for this System Image**.

    The contents of the log appear on the page. Use this information to find out whether the image was captured on the appliance or imported from the `clientdrop` share, who and when imported the image, or whether the image was replaced and by which user. If the image consists of multiple partitions, the log shows any operations performed on the specific partitions.

Managing answer files for Sysprepped images

The appliance allows you to create and manage answer files for Sysprepped Windows images.

Sysprep (System Preparation) is a Microsoft tool for capturing OS images. It removes device-specific information from a Windows installation, allowing it to be deployed to other target devices.

NOTE: You can access this tool by clicking the *Sysprep Creator Wizard* link on the *Library Overview* page.

System administrators typically use answer files (`unattend.xml`) to fully automate the configuration and deployment of Windows systems. Each answer file contains a set of pre-defined values required by Windows system installation, eliminating the need for user interaction during the installation.

Create answer files for Sysprepped images

The *Sysprep Creator Wizard* guides you through the steps to create an answer file for Sysprepping an image.

1. On the left navigation pane, click **Library** to expand the section, then click **Sysprep Unattend Files** to display the *Sysprep Unattend Files* page.
2. Select **Choose Action** > **Sysprep Creator Wizard**.

NOTE: You can also start the wizard by clicking the link on the *Library Overview* page.

3. In the *Sysprep Creator Wizard* that appears, on the *System Information* page, complete the following steps:
    a. Provide the following information:

Option	Description
Name	The name of the `unattend.xml` file configuration. The name you provide here identifies this configuration on the *Sysprep Unattend Files* page.
Operating System	The target operating system.
Architecture	The operating system architecture.

    b. Click **Next**.
4. On the *Configuration* page, complete the following steps:
    a. Provide the following information:

Option	Description
Registration Data	
Owner	The name of the user for which the operating system is installed.
Organization	The name of the organization to which the operating system is licensed.
General Settings	
Time Zone	The time zone where the system is used.
Location	The country where the system is used.
Primary Language	The language the operating system uses.
Fallback Language	The fallback language of the operating system, in case the selected language is not available.
Local Administrator Account	
Username	The name of the local administrator's account for this system.
Password	The administrator user's password.
Enable the built-in Administrator Account	Select this option if you want to enable the built-in Administrator account on the target system. This is useful if you want to run or install programs and apps on the target system before a user account is created.
Number of times to auto-login	Specify the number of times the system automatically logs in to the account defined in the *Networking* area.
Networking	

Option	Description
Join a workgroup	Select this option if you want the target system to join a specific work group, and in the **Workgroup Name** field, specify the name of the group.
Join a domain	Select this option if you want the target system to join a specific domain, and provide the following information: • **Fully Qualified Domain Name (FQDN)**: The fully qualified domain name. • **Credentials to join the domain**: Specify the **Username** and **Password** for accessing this domain.

b. Click **Next**.

5. On the *Windows Setting* page, complete the following steps:
   a. Provide the following information:

Section	Description
Out of Box Experience	Use this section to provide the Windows Out-Of-Box Experience (OOBE) settings, as required. For example, you can select the size of icon, disable automatic daylight savings, or hide wireless setup. For complete information about these settings, see your Windows documentation.
Windows Activation	Specify the Windows system settings, such as if and when to install Windows updates, replicate the profile of the user running Sysprep, or disable User Access Control (UAC). For details, see your Windows documentation.

   b. Click **Next**.

6. On the *Miscellaneous Setting* page, complete the following steps:
   a. Enable or disable each of the following settings, and provide the relevant information that appears in each group of settings, as required. For complete details, see your Windows documentation.

Option	Description
Internet Explorer Options	
Enable IE Options	Select if you want to enable Internet Explorer options and provide the related settings that appear, such as whether to block pop-ups or disable the First Run wizard.
OEM Information	
Enable OEM Information	Select if you want to specify OEM options and provide the related settings that appear, such as the manufacturer name or device model.
Taskbar Links	
Enable Taskbar Links	Select if you want to specify links on the Windows taskbar, provide the related links.
Advanced Options	

Option	Description
Enable Advanced Options	Select if you want to enable advanced Windows options such as whether to **Persist all installed Plug and Play devices,** or to **Reset activation grace-period timer**.

b. Click **Save**.

Your configuration for creating answer files for Sysprepped images is complete. The *Sysprep Creator Wizard* closes and the *Sysprep Creator Wizard Options* page appears.

7. Review the options listed on the *Sysprep Creator Wizard Options* page, and make a selection, as applicable.
   - **View Sysprep Unattend File Detail**: Click to see the contents of the `unattend.xml` file that can be generated using your newly created configuration. The *Sysprep Unattend File Detail* page appears, showing the `unattend.xml` file details. For more information about this page, see View and edit answer file configurations.
   - **View Sysprep Unattend Files List**: Click to see the *Sysprep Unattend Files* list page. This page shows all configurations defined on the appliance that can be used to generate Sysprepped `unattend.xml` files.
   - **Download Unattend File**: Click to download the `unattend.xml` file generated using this newly created configuration.
   - **Download Unattend File with KACE Image Prep**: Click to download the `unattend.xml` file generated using this newly created configuration, together with the KACE Image Prep.
   - **Download KACE Image Prep**: Click to download the KACE Image Prep.

   NOTE: You can also download the KACE Image Prep using the **Choose Action** menu on the *Sysprep Unattend Files* page.

View and edit answer file configurations

The *Sysprep Unattend Files* page lists all answer file configurations defined on the appliance that can be used to generate Sysprepped files. From here, you can open a specific answer file configuration, and review and edit the relevant details on the *Sysprep Unattend File Detail* page.

1. On the left navigation pane, click **Library** to expand the section, then click **Sysprep Unattend Files** to display the *Sysprep Unattend Files* page.
2. On the *Sysprep Unattend Files* page, in the *Name* column, click a configuration name.

   The *Sysprep Unattend File Detail* page appears.
3. Review the contents of the *Sysprep Unattend File Detail* page.
4. Use the *Notes* field to provide any specific information about this configuration.
5. **Optional.** If you want to make changes to the contents of the `unattend.xml` that is created using this configuration, you can do so in the *XML* field.

   Basic XML validation is available. If you break the XML syntax, an error message appears when you try to save your changes.
6. Click any of the following links to download the related components, as required:
   - **Download Unattend File**: Click to download the `unattend.xml` file generated using this newly created configuration.
   - **Download Unattend File with KACE Image Prep**: Click to download the `unattend.xml` file generated using this newly created configuration, together with the KACE Image Prep.
   - **Download KACE Image Prep**: Click to download the KACE Image Prep.

NOTE: You can also download the KACE Image Prep using the **Choose Action** menu on the *Sysprep Unattend Files* page.

7. Click **Save**.

   The *Sysprep Unattend File Detail* page closes and the*Sysprep Unattend Files* page appears, listing all answer file configurations.

NOTE: These configurations are view-only and cannot be edited.

Best practices for creating Windows system images

This topic provides information about KACE-recommended best practices for creating a Windows Golden System Image.

Audit the appliance before beginning

- Keep 20 percent of available space (or more) on the appliance.
- Back up and remove un-used images, then copy and remove those images from the restore share directory.
- Remove test images, or images that have been updated. (Updated or outdated.)

CAUTION: Never run a "Delete Unused System Images Files" or delete an image while capturing an image.

Start fresh

- Create the golden image in a virtual machine to keep it clean of extra drivers. This also is helpful in updating the image on a regular basis.
- Do not image or create a golden master image of a machine that comes directly from the manufacturer. Only use volume license media. Avoid using OEM Media. For more information see https://support.quest.com/kb/135252.
- If applying updates that occurred after capturing the image, only deploy a non-sysprepped image back to original machine.
- Update images every couple of months and run a cleanup on the images.

Configure the workstation

The following KB articles are recommended best practice methods for creating the base OS installation for System Image capture. If using a Legacy enabled BIOS, use the Single Partition Golden Image KB. If the BIOS is in UEFI mode, use the UEFI KB. Kace highly recommends minimal partitions on your base OS.

- **UEFI vs. Legacy BIOS Imaging**: https://support.quest.com/kb/190265
- **Single Partition Golden Image**: https://support.quest.com/kb/187971
- **UEFI Imaging**: https://support.quest.com/kb/186950
- **Understanding Imaging, KKE Videos**: https://support.quest.com/kb/video-articles?k=understanding%20imaging

If not following the above KB articles, use the following guidelines:

- If working from a machine that was deployed with the appliance (Scripted Install or Image), make sure to delete the KACE directory on the root of the drive and delete `%allusersprofile%\quest\kace`.
- If working with a machine that had previously been sysprepped, make sure to delete `sysprep_succeeded.tag` from `windows\system32\sysprep`.
- Install all patches and updates.
- Create an administrator profile and customize the profile that is to be set up as default.
- KACE recommends creating a base image, and using post-installation tasks to deploy your software at a later time. This will make your images more flexible when having to deploy to numerous departments, or different types of users.
- If creating a "full" image, avoid installing software that is updated regularly (flash, reader, and so on), make these into post-install tasks and leverage the KACE Systems Management Appliance for updates.

  CAUTION: It is NOT recommended to install applications such as anti-virus, encryption (such as Dell™ Data Protection), security, virtual CD software, any software that emulates hardware, or the KACE Agent in the image. These can often interfere with the image deployment process.

  If the image is captured in WIM format, keep **at least 60%** of the drive space on each partition as free/available.

Sysprep, capture and deployment guidelines

- Capture the image without sysprepping OR if using a virtual machine (VM): use the snapshot feature to have a copy of the non-sysprepped OS and customizations. If capturing a non-sysprepped image, remember this must be deployed back to the exact same hardware.

  NOTE: Creating a golden master on a virtual machine leverages creating snapshots at different stages, such as prior to sysprepping. This allows a restore to a previous snapshot much quicker than re-deploying a system. This also allows for easy testing of deployments to another virtual machine. Testing driver injection would require deployment to specific models.
- If there is an issue with sysprep, and these happen often, it is best to restore a non-sysprepped image to the original machine, which will also avoid rearm issues. With the VM option, reverting back to a snapshot will allow updates to the system.
- If capturing the non-sysprepped image to the appliance, be descriptive in your naming of captured images; include whether the machine is sysprepped, and include the version or date of the capture.
- Descriptive names enable system administrators to choose the correct image to deploy from the drop-down list in KBE.
- Use the notes field in the appliance Administrator Interface as a change and audit log.

Sysprep

- Sysprep is a Microsoft tool that they require for capturing an OS image to deploy to a different system. You can either use the Microsoft Sysprep tools and command line or use the KACE Sysprep Creator Wizard if you do not have an `unattend.xml` file.
- If you configured a "default" account, ensure to set it to `True` in the `unattend.xml` file. The sysprep creator wizard has an option to copy the current profile to the default profile.
- When running sysprep by command line and not the Sysprep Creator/Executor, use the `/generalize`, `/oobe`, `/shutdown`, and the `/unattend` switches.
- Shutdown is preferred so that the PXE boot isn't missed on a reboot. If using the option, sysprep must be run from the customized account.

Capture

- Verify that enough space is available on the appliance and then capture the sysprepped image.
- After the capture, reboot the sysprepped machine to verify that mini setup runs correctly.
- Test to make sure everything in the image works as desired.
- Capturing an image across the WAN is not recommended. Please limit image capturing to only the local LAN where the appliance is physically located.

Deploy

- Add Pre/Mid/Post Installation tasks to your image on the appliance.
- Test your deployment on a different workstation for verification.
- If deploying an image to a remote location, please consider using a Remote Site Appliance (RSA) for best performance. Deploying an image across the WAN is not recommended.

Post-installation tasks

- Be consistent with naming tasks. Adding prefixes such as "App-" or "Script-", "OSConfig-" "Mid-" helps to keep tasks organized.
- Consider the ordering of your post-installation tasks in terms of placing prerequisites before the applications that require them.
- Use `cscript` with VB scripts. For example: `cscript myscript.vbs`
- When creating a ZIP file for an application task, select the contents to archive so that the file you call is in the root of the ZIP file.
- For `.msi` deployments, use the install switch last. For example: `msiexec /qn /norestart /i agent.msi`
- Use `CLONEPREP=1` on the `.msi` Agent install if it is not intended to have the Agent to -check in, and create a KUID until the next reboot. For example: `msiexec /i agent.msi HOST=blah CLONEPREP=1`
- If using 3.5 SP1 or earlier:
  - Use the `start /wait` command when deploying software through appliance post-installation tasks.
  - Use `call` when using `.bat` scripts in application tasks. For example: `call myscript.bat`

Capturing user states

The appliance uses the Windows User State Migration Tool (USMT) to migrate user profiles by running the USMT Scan State and Load State utilities. Before scanning devices for user states, you can configure the USMT Scan Templates that set the Scan State utility parameters and enable you to specify which data to migrate and which data to exclude from the capture. You can upload and install the USMT from the appliance or from the KACE Media Manager.

The USMT Scan State utility (Scanstate.exe) scans a device for data, and captures the information in a `.mig` file. The USMT Load State utility (Loadstate.exe) installs the data and settings from the `.mig` file on to a destination or target device. The Load State utility also enables you to migrate users states to devices manually.

Scan User States Offline: You can use the *Scan User State Offline* pre-installation task to scan user states from any device and upload the user state to the appliance.

Deploy User States: You can use the *Deploy User States* post-installation task to deploy the user states to target devices.

Upload USMT software from the appliance

Scanning user states requires the Windows User State Migration Tool software (USMT) included in the Windows ADK (Automated Deployment Kit). You can upload the USMT software version 5.0 directly from the appliance. The appliance captures the user states by running the USMT Scan State utility on a device.

You can also upload USMT version 3.0.1 from the appliance.

1. On the left navigation pane, click **Library** to expand the section, then click **User States** to display the *User States* page.
2. Select **Choose Action** > **Upload**.
3. Select the appropriate OS to which you plan to deploy the user states, and click **Show me instructions**.

Upload USMT software from Media Manager

You can upload and install the USMT software version 5.0 from the latest version of the Media Manager.

1. On the device where the KACE Media Manager is installed, run the Media Manager from **Start** > **All Programs** > **Quest** > **KACE Media Manager**.
2. In Media Manager, in the left pane, click **General Settings**.

   NOTE: This page appears by default if this is the first time you run the Media Manager.
3. In *SDA Hostname*, enter the IP address of the appliance.
4. In *SDA IP address*, enter the IP address segments of the appliance.
5. In *Samba Share Password*, enter the password you used to log in.
6. Click **Upload USMT**.
7. Click **Browse** and confirm that the path to the appropriate Windows ADK is correct.

For example:

- WinPE 10 Win10 x86 ADK `C:\Program Files\Windows Kits\10`
- WinPE 10 Win8 x64 ADK `C:\Program Files(x86)\Windows Kits\10`

8. Click **Start Upload**.

Create USMT Scan Template

You can create a scan template to specify which data to migrate, for example include user-specific files and settings and exclude user profiles and data. You can use the template for online and offline user state migrations from the appliance.

1. Open the KACE Systems Deployment Appliance Administrator Console or the KACE Remote Site Appliance.
2. **KACE Remote Site Appliance only**. Ensure the following steps are completed:
   - The USMT Toolkit is uploaded to the linked KACE Systems Deployment Appliance.
   - The RSA is synchronized with its KACE Systems Deployment Appliance, causing the USMT Toolkit to be pushed out to the RSA.
3. On the left navigation pane, click **Library** to expand the section, then click **USMT Scan Templates** to display the *USMT Scan Template* page.
4. Select **Choose Action** > **Add Scan Template** to display the *USMT Scan Template Detail* page.
5. In *Name*, type a unique name to identify the template.
6. Set the *User selection options*:
   - **Select the *Scan all available user states* check box to scan all of the user states on a device.**
   - **Select the *Specify users to excluded* check box to exclude the user states set from the scan. You can Include the user states for exclusion in a comma-separated list in the `config.xml` file created using the `/genconfig` option in the ScanState Tool.**
7. Set the *Command-line options* that the appliances uses to run the scan. Most cases use the default command-line options.
8. Set the *Content configuration options* to control which data to capture and migrate using the customized configuration `config.xml` file. Use this feature to exclude Windows and Document components only. Generate the configuration file on a workstation with the same files and folders, applications, and component setup as the device from which you are scanning the user states.
   - **Select the *Exclude Files* check box to choose file types to exclude. You can also list the file extensions in a comma-separated list.**
   - **Select the *Specify config file* check box to select the Windows components to include or exclude.**
9. Click **Save**.

The template appears in the list on the *USMT Scan Templates* page.

Scan user states

You can specify which data and settings to migrate or to exclude from the device from which you are scanning new user states. You can capture user states with the KACE Systems Deployment Appliance, or any linked RSA appliances.

When you synchronize a linked RSA with the KACE Systems Deployment Appliance, any user states on the appliance also appear on the *User States* list page in the KACE Remote Appliance Administrator Console. When you review individual user state contents, the ability to edit applicable fields and log contents are only available for those user states that are

captured locally, but not for any of the user states captured on a linked appliance. Any user states captured on an RSA can be exported.

To scan user states, SMB (Server Message Block) version 2.0 or later must be enabled on the client system.

Create or modify a USMT Scan Template to specify which data and settings to migrate or to exclude. When scanning devices running Windows 7 and higher, configure the following settings:

- Turn off simple file sharing or the firewall.
- Enable the default administrator account.
- Turn off Windows Defender.
- Enable file and print sharing.
- Set User Account Control (UAC) to never notify.

1. Open the KACE Systems Deployment Appliance Administrator Console or the KACE Remote Site Appliance.
2. **KACE Remote Site Appliance only**. Ensure the following steps are completed:
   - The USMT Toolkit is uploaded to the linked KACE Systems Deployment Appliance.
   - The RSA is synchronized with its KACE Systems Deployment Appliance, causing the USMT Toolkit to be pushed out to the RSA.
3. On the left navigation pane, click **Library** to expand the section, then click **User States** to display the *User States* page.
4. Select **Choose Action** > **New** to display the *Scan New User State* page.
5. Select the USMT version and template.
6. Complete the *Client Device Detail* information:

Option	Description
HostName/IP	The fully qualified host name or IP address for the device that you are scanning. Use a comma, semi-colon, or a new line as a delimiter to enter a range of devices.
Domain	The domain name if the device that you are scanning is connected to a domain.
User Name	Administrator privileges on the device that you are scanning.
Password	Administrator privileges on the device that you are scanning.

7. Click **Next**.

   When the process completes successfully, a list of profiles appears.
8. Select the profiles that you want to migrate on to the appliance, and click **Next**.

   The *Results Log* appears.
9. Click **Finish**.

If the scan fails, go to *Settings* > *Appliance Logs* and check the USMT error log. Stop any processes that should not be running, for example Windows Defender.

- The capture process adds a user entry to the image to the *User States* page in the KACE Systems Deployment Appliance Administrator Console, and also in the Remote Site Console, if the user state is captured using an RSA.
- The KACE Systems Deployment Appliance assigns an ID to each captured user state.

Tip: **TIP:** Each user state captured with the KACE Systems Deployment Appliance or its linked RSAs has a unique ID. This allows the appliance to keep track of all the different user states captured with the linked KACE Systems Deployment Appliance or RSA, and to synchronize any user states, as you edit them. To find out an ID of a user state, hover over the user state on the *User States* page. The ID appears in the bottom-left corner.

The selected user states are uploaded to the appliance and appear in the list on the *User State* page. You can deploy the user states to target devices by assigning the *Deploy User States* post-installation task to a scripted installation or system image deployment.

Scan user states offline

Scanning user states offline enables you to capture the user profiles from devices that are assigned to a deployment. The appliance captures the profiles if the *Scan User States Offline* pre-installation task is assigned to the scripted Installation or system image, then deploys the selected user states with the *Deploy User States* post-installation task. When scanning user states, you can also choose to load additional user states that are available on the appliance.

1. Complete one of the following steps:
   - **On the left navigation pane, choose Deployments > System Images to display the *System Images* page. Then click a system image name to display the *System Image Detail* page.**
   - **On the left navigation pane, choose Deployments > Scripted Installations to display the *Scripted Installation* page. Then click a scripted installation name to display the *Scripted Installation Detail* page.**
   - **On the left navigation pane, choose Deployments > Custom Deployments to display the *Custom Deployments* page. Then click a custom deployment name to display the *Custom Deployments Detail* page.**
2. Select the name of the scripted installation or the system image deployment to which you want to migrate the user states.

   The *Scripted Installation Detail* or the *System Image Detail* page appears.
3. Under *Installation Plan*, move the *Scan User States Offline* Pre-installation Task from the *Available Pre-installation Tasks* column to the *Run Pre-installation Tasks* column. Ensure that you place the *Scan User State Offline* first in the list and that you add the *Deploy User States* post-installation task.

If a user profile on a target device matches a user profile on the existing user state records, the process overwrites the existing record.

4. Click **Save**.

   The appliance rebuilds the scripted installation or the system image.

Deploy user states to target devices automatically

The appliance captures user states if the *Scan User States Offline* pre-installation task is assigned to a scripted installation or system image deployment, then loads the captured user states using the *Deploy User States* post-installation task.

1. Complete one of the following steps:
   - **On the left navigation pane, choose Deployments > System Images to display the *System Images* page. Then click a system image name to display the *System Image Detail* page.**
   - **On the left navigation pane, choose Deployments > Scripted Installations to display the *Scripted Installation* page. Then click a scripted installation name to display the *Scripted Installation Detail* page.**
   - **On the left navigation pane, choose Deployments > Custom Deployments to display the *Custom Deployments* page. Then click a custom deployment name to display the *Custom Deployments Detail* page.**
2. Select the name of the scripted installation or the system image deployment to which you want to deploy the user states.

   The *Scripted Installation* or the *System Image Detail* page displays.
3. Under *Installation Plan*, move the *Deploy User States* Post-installation Task from the *Available Post-installation Tasks* column to the *Run Post-installation Tasks* column.
4. Click **Save**.

   The appliance rebuilds the scripted installation or the system image deployment.

Deploy user states to target devices manually

When you scan a device and capture the user states to the appliance, the USMT creates a `.mig` file, which contains the user states of the device. You can download and copy the `.mig` file from the appliance to any location on a target device that you want to update with the new user states.

The USMT ScanState utility performs the backup and generates the `.mig` file. The USMT LoadState utility performs the restore process using the `.mig` file. Running the LoadState utility in Administrator mode loads the user states to a target device.

1. On the left navigation pane, click **Library** to expand the section, then click **User States** to display the *User States* page.
2. Select a profile to display the *User State Detail* page.
3. Click **Download User State File**.

   The *Opening USMT.MIG* dialog box appears.
4. Click **Save File** and save the file to any location.
5. Copy the entire `.mig` file on to a target device.
   a. On the target device, create a local store, such as `MyUserStates`, with a subfolder named `USMT`, and copy the `.mig` file to the `USMT` folder.
   b. Run the `loadstate.exe`. on the `USMT` folder on the target device.

Use the following command-line options to deploy the user states:

- Local account: loadstate.exe StorePath /i:miguser.xml /i:migapp.xml /lac /lae
- Domain account: loadstate.exe StorePath /i:miguser.xml /i:migapp.xml

Creating scripted installations

You can upload an existing answer file (Windows) or `preseed/kickstart` file (Linux), or perform a server-based attended setup (Windows or Linux).

Prepare for a scripted installation:

- Set the PXE boot manually for older devices.
- Verify that remote site networks do not require adjustments.
- Note that each device model requires an individualized installation to accommodate driver compatibility.
- Copy, then modify the scripted installation to specify the hard drive size if the same device models have different-size hard drives.

Create a scripted installation

The *Create a Scripted Installation* wizard guides you through the steps to define the scripted installation. The settings that you specify in the `config.xml` file must be compatible with the hardware. **Windows only**: If the hardware cannot handle the settings, the Windows installer causes the unattended scripted installation to fail.

Extract the ISO file of OS to its own directory, then upload that directory to the KACE Systems Deployment Appliance server as the source media using the Media Manager, and ensure that you re-cache the drivers.

1. On the left navigation pane, click **Deployments**, then click **Scripted Installations** to display the *Scripted Installations* page.
2. Select **Choose Action** > **New**.

   Follow the steps provided by the *Create a Scripted Installation* wizard.

   NOTE: Scripted installation deployments to UEFI-enabled devices require creating a UEFI partition using the *Create UEFI Partitions* pre-installation task and booting from a UEFI bootable FAT32 formatted USB flash device.

Next, using the wizard, upload an existing answer file (Windows) or `preseed/kickstart` file (Linux), or perform a server-based attended setup (Windows or Linux).

Edit a scripted installation

You can rename, duplicate, remove, or edit scripted installations.

The *Scripted Installation Detail* page allows you to view the image settings, add a boot action, download the log files for the image, and set the options for how the appliance responds to errors.

The *Installation Plan* enables you to create a task sequence by adding the available pre-installation, mid-level, and post-installation tasks to run in the order that you place the tasks for the deployment.

1. On the left navigation pane, click **Deployments**, then click **Scripted Installations** to display the *Scripted Installations* page.
2. Select the scripted installation from the list to display the *Scripted Installation Detail* page.
3. To change the installation source media containing the operating system, see Modify a scripted installation to change the source media.
4. To modify the setup configuration file used to deploy the operating system, see Modify scripted installation setup configuration file.
5. **Optional: Configuration files only**.
    a. Next to *Config XML*, click **Show**, and review the file contents that appear. The contents of the file are read only.
    b. To download the file, under the file contents, click **Download XML File**.
6. **Optional: Task files only**.

    NOTE: Read-only users do not have access to this field.

    a. Next to *Task XML*, click **Show**, and review the file contents that appear. The contents of the file are read only.
    b. To download the file, under the file contents, click **Download XML File**.
7. Assign tasks to the scripted installation, as required. For more information, see Assign tasks to scripted installation deployment.
8. When you finish your edits, click **Cancel** to roll back the changes, or **Save** to apply the changes to the image.

Create a configuration file

You can create your own configuration file or modify an existing one with the configuration tasks that are typically prompted for during an attended scripted installation. The type and name of the file depends on the OS used in the scripted installation. For example, for Microsoft Windows systems, you create or modify an answer file, `unattend.xml`, while Debian Ubuntu uses a `preseed.cfg` file.

1. On the left navigation pane, click **Deployments**, then click **Scripted Installations** to display the *Scripted Installations* page.
2. Select **Choose Action** > **New** to display the *Create a Scripted Installation* page.
3. Enter a *Name*, and select the source files from the *Source Media* drop-down list, then click **Next**.
4. Select which method to use to create the configuration file:
    - *Walk me through creating a <configuration> file for unattended setup*: **Creates a configuration file using the unattended Installation wizard.**

      NOTE: The name of the configuration file displayed in these options depends on the target platform. For example, Windows uses an *answer* file (`unattend.xml`), while Ubuntu uses a *preseed* file (`preseed.cfg`) file.
    - *Upload an existing <configuration> file for unattended setup*: **Uploads a configuration file for unattended installation.**
    - *No <configuration> file; This will be a server-based attended setup*: **Creates a basic configuration file that requires user input to complete the installation.**
5. Click **Walk me through creating a <configuration> file for unattended setup**, then click **Next**.
6. **Windows only**. Complete the answer form.

Set the following value in the answer file to disable the Windows 8 animation on login. Setting the value enables you to see the *Task Error page* on target devices:

- **`EnableFirstLogonAnimation` registry key to 0 (zero).**

7. **Linux only**. In the *Configuration* step, provide the following information.

Section	Option	Description
Select Preseed Template		Click and select the template that you want to use for this configuration. The list of templates that appear depends on the previously selected platform under *Source Media*.
Template Data	**Root Password**	Specify the root password for this configuration. If you want to disable root login for the target system, select **Disable root login**.
	NOTE: If you choose the server template, this is the only option that appears. All of these options are available with the desktop template.	
	User Account	To add a new user account using this method, select **Create User Account**. Any user accounts that are created this way are granted `sudo` access. Provide the full name, user name, and password for the account.
	Time Zone	Select the time zone for the target system.
	Time Zone Server	Specify the host name of the applicable time zone server.
	Language	Select the locale for the target system.
	Desktop GUI	Select the graphical user interface that you want to use on the target system: *GNOME Desktop Environment*, or *KDE Desktop Environment*, as applicable. **NOTE:** For Ubuntu GNOME and KDE desktop deployment, the repository URL must be enabled.

NOTE: The information you provide on this page cannot be changed. If updates are required, you must create a new scripted installation with the desired configuration.

8. Click **Next** to display the *Pre-installation and Post-installation Tasks* page, and add the required pre-installation and post-installation tasks.
9. **Windows only**. Select the *Task Error Handling* option for how you want the appliance to respond to errors.
10. Click **Next**.

    The *Scripted Installation Creation* page displays the status.
11. When the process completes, click **Finish**.

    The *Create a Scripted Installation* page refreshes and displays the results.
12. **Optional**. To view the contents of the answer or configuration file, open the *Scripted Installation Detail* page for the newly created scripted installation, and under *Setup Configuration*, click **Show**. You can make edits to this file, if needed. Any edits you make in the file contents affect only the selected scripted installation.

Deploy the scripted installation from *Automated Deployments* or as a manual deployment from the KBE Main Menu, which displays on the target device after the target device boots in to the KBE.

Registration Data settings

The settings for the Registration Data vary depending on the operating system or the Source Media that was used.

Field	Description
Name	Identifies the user to which the license is assigned.
Organization	Identifies the company or organization.
Product Key	Enter the product activation key.
Volume or Multi-Activation Licensing	For Volume licenses, enter the MAK (Multiple Activation Key) or KMS (Key Mgt System) setup key.
Install image	**Windows 10 only**. Windows 10 ISO images include all Windows editions. Click this field and select the Windows Edition that you want to install. Other supported Windows versions. Automatically detects the installation image using the product key.

Administrator Account settings

Creates the local administrator account during the installation process and sets whether the device automatically logs in to the account after the device reboots. Post-installation tasks, such as renaming the device and installing software require the script to automatically log back in to the device with an administrator account.

Field	Description
Username	Enter the user name for the administrator account. This account is created during the installation process.
Password	Enter the password for the administrator account. Leave the field blank for no password. Automatically logs in the administrator account to the target device after booting.
Automatically log computer in to the Administrator account	Automatically logs in the administrator account to the target device after booting. Selecting this check box enables the post-installation task to run automatically for at least the first boot.
Disable automatic login after: device boots	Disables the automatic login of the administrator account after the specified number of boots.

General settings

Sets the language and device screen settings.

Field	Description
Time Zone	Select the devices's time zone.
Regional and Language Option	Select the device default operating system language.
Screen colors	Select the devices's screen colors. The recommended setting is Windows default, unless you know that all of the target devices require the same setting.
Screen area	Select the device's screen area. The recommended setting is Windows default, unless you know that all of the target devices require the same setting.
Refresh Frequency	Select the devices's screen refresh rate. The recommended setting is Windows default, unless you know that all of the target devices require the same setting.
Hide Wireless Setup	Select this option if you want to disable wireless setup for the device. This option should be selected in most cases, unless you already have a post-installation task that handles this setting.
Disable Consumer Features (Enterprise and Education Editions of Windows 10 only)	Windows 10 only. Select this option if you want to disable the installation of apps into Windows 10 tiles after the deployment.

Network settings

The Network settings control the initial network-related settings. The recommended setup is to leave the *Device Name* field blank to generate a random name, and to join the computer to a *Workgroup* to enable scripted installation deployments to additional target devices. You can rename the computer and join the computer to the domain using a post-installation task.

Field	Description
Device Name	Enter a device name or leave the field blank to generate a name automatically.
Workgroup	Join the device to a workgroup.
Domain	Select the check box if the target device is a part of a domain.

Field	Description
Create a computer account in the domain	Select the check box to add a device account in the domain.
Domain Administrator	Enter the name of the domain administrator. **NOTE:** The administrator must have permissions to add devices to the domain. Disable the Local Administrator when a device joins the domain.
Password	The administrator password for the domain.

Windows Components setting

Selecting the *Enable Automatic Updates* check box enables the Windows update feature during installation.

Modify a scripted installation to change the source media

You can change the installation source media containing the operating system.

Your scripted installation includes a reference to the source media, containing the ISO file of the OS that will be deployed to target machines during the installation. You can change a source media associated with a scripted installation. This can be useful, for example, when you want to start using a newer version of the same OS that includes some critical patches.

1. On the left navigation pane, click **Deployments**, then click **Scripted Installations** to display the *Scripted Installations* page.
2. Select the scripted installation from the list to display the *Scripted Installation Detail* page.
3. Click **Source Media**, and select the new source media that you want to associate with this scripted installation.
4. Click **Save**.

Specify deployment options

You can change the deployment options to hide the scripted installation from the KACE Boot Environment (KBE), when needed.

1. On the left navigation pane, click **Deployments**, then click **Scripted Installations** to display the *Scripted Installations* page.
2. Select the scripted installation from the list to display the *Scripted Installation Detail* page.
3. Under *Deploy Options*, select or clear the **Hide Deployment from KBE** check box, as required.

   When selected, the scripted installation does not appear available for selection in the KBE.

Modify scripted installation setup configuration file

You can modify the setup configuration file used to deploy the operating system.

1. On the left navigation pane, click **Deployments**, then click **Scripted Installations** to display the *Scripted Installations* page.
2. Select the scripted installation from the list to display the *Scripted Installation Detail* page.
3. Next to *Setup Configuration*, click **Show**, and enter your changes.
4. Click **Save**.

Install Vista MBR

You can add the built-in *Install Vista/2008/7/8/2012 MBR* pre-installation task to restore the boot sector on devices running Windows Vista, Windows 2008 Windows 7 and higher, and Windows Server 2012.

1. On the left navigation pane, click **Library** to expand the section, then click **Pre-installation Tasks** to display the *Pre-installation Tasks* page.
2. Select **Install Vista/2008/7/8/2012 MBR** to display the *Pre-installation Task Detail* page.
3. **Optional**: In *Name*, change the name to identify the task.
4. In *Notes*, add a note to identify the task.
5. Click **Save**.

   The task is now available to assign to scripted installations, sysprepped system images, and non-sysprepped system images.

Install XP 2003 MBR

You can add the built-in *Install XP 2003 MBR* pre-installation task to restore the boot sector on devices running Windows 2000, Windows XP, or Windows Server 2003.

1. On the left navigation pane, click **Library** to expand the section, then click **Pre-installation Tasks** to display the *Pre-installation Tasks* page.
2. Select **Install XP 2003 MBR** to display the *Pre-installation Task Detail* page.
3. **Optional**: In *Name*, change the name to identify the task.
4. In *Notes*, add a note to identify the task.
5. Click **Save**.

   The task is now available to assign to scripted installations, sysprepped system images, and non-sysprepped system images.

Creating a task sequence

You can create a task sequence to include all of the tasks to build and capture an operating system image. The appliance Task Engine runs the tasks on the target devices in a reliable order and reports deployment feedback on the appliance and on the target devices. Task sequencing enables you to view which image was deployed to which device and to view the progress of tasks running on a device. If a task fails, you can edit the task on the target device.

You can use the built-in pre-installation, mid-level, and post-installation tasks, and add your own tasks to scripts that you can run in a task sequence. You can create a task sequence for automated boot action scripted installation, and for system image, multicast, manual, and custom deployments.

Create the task sequence on the *System Image Detail*, *Scripted Installation Detail*, or *Custom Deployment Detail* page under the *Installation Plan*. When building the task sequence, remember to place the prerequisites before the applications that require them.

Adding tasks

You can add the built-in pre-installation, mid-level, and post-installation tasks. You also have the option to use the *Choose Action* menu selections to add your own tasks to a script to run as a pre-installation, mid-level, or post-installation task. The appliance runs the task in the runtime environment that you specify. You can also upload a single file or a ZIP archive containing multiple files to run as tasks. You can duplicate and customize the built-in tasks.

There are different types of tasks you can add, depending on whether you want to run them before, during, or after image deployment. The following table indicates the types of tasks that are available for each stage.

Task type	Pre-installation task?	Mid-level task?	Post-installation task?	See topic:
Application	Yes	Yes	Yes	Add Application
BAT Script	Yes	Yes	Yes	Add BAT Script
Custom HAL Replacement	No	Yes	No	Add Custom HAL Replacement
DISKPART Script	Yes	No	No	Add DiskPart Script
Import Managed Installation	No	No	Yes	Adding Managed Installation tasks
Naming Rule	Yes	Yes	Yes	Add Naming Rule
Powershell Script	Yes	Yes	Yes	Add PowerShell Script
Service Pack	No	No	Yes	Add Service Pack

Task type	Pre-installation task?	Mid-level task?	Post-installation task?	See topic:
Shell Script	Yes	Yes	Yes	Add Shell Script
KACE Agent Installer	No	No	Yes	Add KACE Agent Installer
Windows Script	Yes	Yes	Yes	Add Windows Script

If you want to create a ZIP file, and one or more of your files contain Unicode characters in the file name, the tool you use to create the ZIP file must support Unicode characters. If you notice that after uploading a ZIP file one or more tasks whose file names contain Unicode characters appear to be missing, check the contents of the following directories:

- `\\<appliance_hostname>\peinst\applications\<task_ID>\contents`
- `\\<appliance_hostname>\peinst\preinstall\<task_ID>\contents`

If the files are not found in either directory, use different tool to create a ZIP file, and repeat the process.

You can add a task by going to the appropriate task list page and using the **Choose Action** menu. Tasks can also be deleted by selecting them in the list and selecting **Delete** from the **Choose Action** menu. You can also delete a task from the task detail page. Attempting to delete a task that is associated with an existing system image, scripted installation, or custom deployment prompts a notification, asking you to verify that you want to delete the selected task, and all of its related files.

Add Application

You can upload a single file or a ZIP archive containing multiple files to run as a pre-installation, mid-level, or post-installation task.

1. Complete one of the following steps:
    a. On the left navigation pane, click **Library** to expand the section, then click **Pre-installation Tasks** to display the *Pre-installation Tasks* page.
    b. On the left navigation pane, click **Library** to expand the section, then click **Mid-level Tasks** to display the *Mid-Level Tasks* page.
    c. On the left navigation pane, click **Library** to expand the section, then click **Post-installation Tasks** to display the *Post-installation Tasks* page.
2. On the list page that appears, select **Choose Action** > **Add Application**.
3. On the page that appears, in *Name*, enter a logical name for the task, such as Install Adobe Reader 11.
4. Select a Runtime Environment:
    - **Pre-installation and mid-level applications**: Select *SDA Boot Environment (Windows)*, *SDA Boot Environment (Linux)* or *SDA Boot Environment (Mac OS X)*, as applicable.
    - **Post-installation applications**: Select *Windows*, *Linux*, or *Mac OS X*, as applicable.

    For more information, see About runtime environments.
5. Select the file that you want to upload by completing one of the following steps.
    - To upload a file, under *Upload File*, click **Browse** and select the appropriate file, or drag and drop the file into the *Drop file here* area. A progress bar appears, indicating the state of the file upload process.

NOTE: You can only upload files that are up to 1.8 GB in size. For larger files, use the `clientdrop` Samba share.

- To select a file from the `clientdrop` Samba share on the appliance, under *Select file from clientdrop share*, click **Select clientdrop file**, and choose the file.

NOTE: You can upload a file using only one of the above steps. If you use both, the last one takes precedence.

6. In *Full Command Line*, enter the command-line parameters for the task.
7. Select the *Reboot Required* check box to reboot the appliance and run the next task in the sequence.
8. In *Expected Return Code*, enter a code that the task should return, if applicable. Otherwise, leave the default value of zero '0'.

   In general, most tasks exit with a zero '0' code, indicating success, but you can set it to any positive value, as applicable. Some installers exit with a different code, even when the install is successful. For example, anti-virus installers are typically successfully installed but exit with a different return code because they require a device reboot.
9. In *Notes*, add a note to identify the task.
10. Click **Save**.

    The task is now available to assign to scripted installations, sysprepped system images, and non-sysprepped system image deployments.

Add BAT Script

You can create your own batch scripts to run as a pre-installation, mid-level, or port-installation task in the KACE Boot Environment for Windows before or after installing the operating system, or re-imaging a target device.

1. Complete one of the following steps:
   a. On the left navigation pane, click **Library** to expand the section, then click **Pre-installation Tasks** to display the *Pre-installation Tasks* page.
   b. On the left navigation pane, click **Library** to expand the section, then click **Mid-level Tasks** to display the *Mid-Level Tasks* page.
   c. On the left navigation pane, click **Library** to expand the section, then click **Post-installation Tasks** to display the *Post-installation Tasks* page.
2. On the list page that appears, select **Choose Action** > **Add BAT Script**.
3. On the page that appears, in *Name*, enter a logical name to identify the task.

   The task runs in the KACE Boot Environment (Windows).
4. In *BAT Script*, enter the script.

   You can use the following commonly used commands available from within the KACE Boot Environment (KBE):

   - bcdedit.exe
   - bootsect.exe
   - chkdsk.exe
   - format.com
5. Select the *Reboot Required* check box to reboot the appliance and run the next task in the sequence.
6. In *Expected Return Code*, enter a code that the task should return, if applicable. Otherwise, leave the default value of zero '0'.

   In general, most tasks exit with a zero '0' code, indicating success, but you can set it to any positive value, as applicable. Some installers exit with a different code, even when the install is successful. For example, anti-

virus installers are typically successfully installed but exit with a different return code because they require a device reboot.

7. In *Notes*, add a note to identify the task.
8. Click **Save**.

   The task is now available to assign to scripted installations, sysprepped system images, and non-sysprepped system image deployments.

See Assign tasks to system deployment or Assign tasks to scripted installation deployment.

Add Custom HAL Replacement

You can replace the Hardware Abstraction Layer (HAL) using a mid-level task to customize the target device's HAL.

HAL replacement is only supported for system images.

1. On the left navigation pane, click **Library** to expand the section, then click **Mid-level Tasks** to display the *Mid-level Tasks* page.
2. Select **Choose Action** > **Add Custom HAL Replacement** to display the *Mid-level Task Detail* page.
3. In *Name*, enter a logical name for the task.

   The task runs in the KACE Boot Environment (Windows).

4. Click **Browse** to upload the following files:
   - *Upload HAL DLL*
   - *Upload NTKRNLPA.EXE*
   - *Upload NTOSKRNL.EXE*

   NOTE: If a filename is different from what displays in the *Upload* field, the files is renamed when uploaded to the appliance.

   The files are copied to the target devices `Windows\System32` directory as part of the mid-level task.
5. In *Expected Return Code*, enter a code that the task should return, if applicable. Otherwise, leave the default value of zero '0'.

   In general, most tasks exit with a zero '0' code, indicating success, but you can set it to any positive value, as applicable. Some installers exit with a different code, even when the install is successful. For example, anti-virus installers are typically successfully installed but exit with a different return code because they require a device reboot.

6. In *Notes*, add a note to identify the task.
7. Click **Save**.

   The task is now available to assign to scripted installations, sysprepped system images, and non-sysprepped system image deployments.

See Assign tasks to system deployment.

Add DiskPart Script

You can add and run a DiskPart script as a pre-installation task on a Windows device that has booted in to the KACE Boot Environment (KBE) to erase all the data on a hard drive or partition, create new partitions, and assign drive letters.

Back up the components that you want to save before running this task.

For more information, see Common DiskPart command-line options.

1. On the left navigation pane, click **Library** to expand the section, then click **Pre-installation Tasks** to display the *Pre-installation Tasks* page.
2. Select **Choose Action** > **Add DISKPART Script** to display the *Pre-installation Task Detail* page.
3. In *Name*, enter a name to identify this task. For example, Single NTFS Partition C.

   The name is the identifier for the tasks that display on the *Scripted Installation Detail* and *System Image Detail* pages.
4. In *DISKPART Script*, enter the script according to the partition that you are creating on the device, for example:

   - **select disk 0**

     clean
     create partition primary
     select partition 1
     active
     assign
     exit
5. In *Expected Return Code*, enter a code that the task should return, if applicable. Otherwise, leave the default value of zero '0'.

   In general, most tasks exit with a zero '0' code, indicating success, but you can set it to any positive value, as applicable. Some installers exit with a different code, even when the install is successful. For example, anti-virus installers are typically successfully installed but exit with a different return code because they require a device reboot.
6. In *Notes*, add a note to identify the task.
7. Click **Save**.

See Assign tasks to scripted installation deployment or Assign tasks to system deployment.

Common DiskPart command-line options

You can use DiskPart scripts to select objects, remove partitions for a disk, create a partition, make partition active, and to assign drive letters.

Selecting objects

- `select disk=[n]`
- `select partition=[n]`
- `select volume=[{n|d}]`

  Use the parameter `n` to specify the number of the object to select. You can also select Volumes by the drive letter, specified as `d`.

Cleaning a disk

- `clean [all]`

Removes all partitions from a disk. The `all` parameter specifies that every sector on the disk is zeroed.

Creating partitions

- `create partition primary [size=n] [offset=n]`
- `create partition extended [size=n] [offset=n]`
- `create partition logical [size=n] [offset=n]`

Creates a primary, extended, or logical partition. If size is not specified, the partition consumes the remaining available space. If offset is not specified, the partition is created in the first available space. After the partition is created, it is selected.

Making the Boot partition

- `active`

Marks the currently selected partition as the active or bootable partition.

Assigning drive letters

- `assign [letter=d]`
- Assigns a drive letter to the currently selected partition. If a letter is not specified, the first available letter (starting with C) is used.

Adding Managed Installation tasks

On the KACE Systems Management Appliance, Managed Installations (MI) are the primary mechanism for deploying applications to managed devices. Each Managed Installation is associated with a specific application title, version, and its command line. For complete information about Managed Installations, see the KACE Systems Management Appliance **Administrator Guide**.

The KACE Systems Deployment Appliance has a mechanism to install applications as part of the deployment process. Importing a Managed Installation from the KACE Systems Management Appliance allows you to quickly add it to a system deployment task sequence, when needed.

Link appliances

To enable importing of Managed Installations, you must link the KACE Systems Deployment Appliance with the KACE Systems Management Appliance that contains Managed Installations that you want to import.

1. Complete the following configuration steps on the KACE Systems Management Appliance:

Step	For complete details, see this topic in the KACE Systems Management Appliance *Administrator Guide*:
• Link the KACE Systems Management Appliance with the KACE Systems Deployment Appliance and enable access to the Federation API settings. 1. In the KACE Systems Management Appliance *System Administration Console*, click **Settings**. 2. On the *Control Panel*, click **Link Settings**. 3. On the *Linked Appliance Enablement* page, select the following check boxes: ▪ **Enable Appliance Linking** ▪ **Enable Federation API access settings**	*Enable appliance linking*
• Enable Federation API access to the linked KACE Systems Deployment Appliance. 1. In the KACE Systems Management Appliance *Administrator Console*, select an Organization associated with a linked KACE Systems Deployment Appliance, and click **Settings**. 2. On the *Control Panel*, click **Federation API Settings**. 3. On the *Federation API Settings* page, select **Enable access**.	*Enable access to Federation API settings*

Step	For complete details, see this topic in the KACE Systems Management Appliance *Administrator Guide*:
4. Grant the *Administrator* role to the linked KACE Systems Deployment Appliance. 5. Repeat these steps for each Organization associated with the KACE Systems Management Appliance.	

View and import Managed Installations

Use the *Import Managed Installations* page to review the applications that you want to import.

Ensure your KACE Systems Deployment Appliance is linked to the KACE Systems Management Appliance from which you want to import one or more Managed Installations. For more information, see Link appliances.

NOTE: Each KACE Systems Management Appliance comes with a default organization (named `Default`). If your appliance is linked with the `Default` organization on a KACE Systems Management Appliance, and the organization name changes, you must provide the new organization name:

1. On the left navigation pane, click **Settings** > **Control Panel** > **Linked Appliances**.
2. On the *Linked Appliances* page that appears, click the name or IP address of the linked KACE Systems Management Appliance.
3. On the *Edit Linked Appliance Detail* page that appears, in the *Default ORG Name* field, type the organization name, and click **Save**.

1. On the left navigation pane, click **Library** to expand the section, then click **Post-installation Tasks** to display the *Post-installation Tasks* page.
2. On the *Post-Installation Tasks* page, select **Choose Action** > **Import a Managed Installation**.
3. On the *Import Managed Installations* page that appears, just above the list of Managed Installations, click *KACE Systems Management Appliance*, and ensure this field points to the correct KACE Systems Management Appliance.

Tip: **TIP:** Your appliance may be linked to multiple KACE Systems Management Appliances.

4. Click *View By*, and choose the managed organization and the type of Managed Installation: *Software* or *Software Catalog*.

   Your selection depends on the type of application that you want to import. All applications installed on the devices managed by the KACE Systems Management Appliance are listed when you select *Software*. Some of those applications are also in the Software Catalog. The Software Catalog is a database that contains standardized information about more than 60,000 Windows and Mac applications and software suites. For more information about Software applications, and the Software Catalog, see the KACE Systems Management Appliance **Administrator Guide**.

5. To look for a specific application, type the application name in the *Search List* field.
6. Review the list of Managed Installations.

The following information is available for each Managed Installation:

- **Name**: The application name.
- **Version**: The application version.
- **Publisher**: The application publisher.
- **Imported**: An indicator of whether a Managed Installation is already imported to the KACE Systems Deployment Appliance.

7. To import a Managed Installation to the appliance, select the row containing the Managed Installation entry, and select **Choose Action** > **Import**.

   The *Import Managed Installations* page refreshes, and a message appears at the top of the page, indicating that the import is in progress. You can review the progress of the import operation on the *Package Management Queue* page. For more information about this page, see Importing and exporting appliance components. When the import finishes, the imported Managed Installation appears on the *Post-Installation Tasks* list.

Next, edit the post-installation task containing the imported Managed Installation. For more information, see Edit Managed Installation task.

Edit Managed Installation task

When you add a Managed Installation from the linked KACE Systems Management Appliance to run as a mid-level task, you can edit it, as required.

Ensure the Managed Installation associated with the task you want to view or edit is imported into the KACE Systems Deployment Appliance. For more information, see View and import Managed Installations.

1. On the left navigation pane, click **Library** to expand the section, then click **Mid-level Tasks** to display the *Mid-level Tasks* page.
2. On the *Mid-level Tasks* page, click the name of the task containing a Managed Installation to display the *Mid-level Task Detail* page.
3. Review and update the following fields, as applicable:

Option	Description
Created (read-only)	The date and time when the task was created.
Modified (read-only)	The date and time when the task was last modified.
Version (read-only)	The version number of the task object on the KACE Systems Deployment Appliance. Every time a task changes, this number increases. Use it as a reference, to verify if the task was changed after your last update. **NOTE:** For example, changing the command-line parameters associated with the application executable results in version change. If you want to overwrite your changes and re-import the original Managed Installation, under Managed Installation Import Details, click Import Again.
Name	The name of the task.
Application (read-only)	The name of the application associated with the task.
Runtime Environment	The OS on which the application can be installed. See About runtime environments.

Option	Description
	NOTE: A KACE Boot Environment (KBE) built with the 5.0 Media Manager or the KBE Manipulator functionality is required, in order to include PowerShell in the KBE, to enable a Windows KBE runtime environment PowerShell task to work as expected.
Full Command Line	The command line for the task, including any command-line parameters, as defined in the Managed Installation.
Expected Return Code	A code that the task should return, if applicable. In general, most tasks exit with a zero '0' code, indicating success, but you can set it to any positive value, as applicable. Some installers exit with a different code, even when the install is successful. For example, anti-virus installers are typically successfully installed but exit with a different return code because they require a device reboot.
Notes	Additional information about the task.
Managed Installation Import Details	Information about the Managed Installation on the KACE Systems Management Appliance (read-only): • **KACE SMA Server**: The name or IP address on which the server is running. • **KACE SMA Organization**: The name of the organization in which the Managed Installation is defined. • **Imported version**: The version number of the Managed Installation object on the KACE Systems Management Appliance. You can use this number to verify if the original object was changed, and to import the latest version. If you made any changes to the task after importing the Managed Installation (such as modifying command-line parameters), and you want to revert to its original state, click **Import Again**.
Deployment Details	Information about the deployments referencing this task (read-only): • **Scripted Installations**: A list of any scripted installations referencing this task. • **System Images**: The system images containing this application.

4. Click **Save**.

   The task is now available to assign to scripted installations, sysprepped system images, and non-sysprepped system image deployments.

Add Naming Rule

You can create a naming rule to obtain a computer name as a pre-installation task, or name a device during mid- or post-installation. To automatically assign device names, you can use a text file and attach it to the task, or use the appliance database. Additional options for specifying the computer name are available.

The appliance includes two scripts to obtain or assign computer names: `getcomputername` and `setcomputername`. Each script has a 32- and 64-bit version. For more information about these scripts, visit https://www.itninja.com/blog/view/get-set-computername.

By default, the `/log` switch is added to the script command line, allowing the appliance to create a log file each time the script runs. You can also use the `/debug` switch if you want to see messages from the script at runtime.

These tasks work with sysprepped images (where an `unattend` file is specified) and with scripted Windows installations.

1. Complete one of the following steps:
    a. On the left navigation pane, click **Library** to expand the section, then click **Pre-installation Tasks** to display the *Pre-installation Tasks* page.
    b. On the left navigation pane, click **Library** to expand the section, then click **Mid-level Tasks** to display the *Mid-Level Tasks* page.
    c. On the left navigation pane, click **Library** to expand the section, then click **Post-installation Tasks** to display the *Post-installation Tasks* page.
2. Select **Choose Action** > **Add Naming Rule** to display the task detail page.
3. In *Name*, enter a logical name for the task, such as Assign name to workstation.
4. Under *Select Architecture*, choose the architecture of the device OS to which the naming rule applies: **x64** (64-bit) or **x86** (32-bit).
5. **Obtaining computer name in pre-installation tasks only**.
    a. Observe the contents of the *Full Command Line*.

    The specified command collects the computer name from the device's Windows registry and stores it in a text file, next to the computer's MAC address. To prompt the user for a different name, use the `/dialog` switch.
6. **Assigning computer name in mid-level or post-installation tasks only**. The options provided in each task type are identical with the exception of the `\in_windows` switch, that only appears in post-installation tasks.
    a. Click **Select Method of Naming** and choose one of the following options:

    - **Set computer name to the current computer name**: Leaves the computer name unchanged.
    - **Prompt for the computer name**: The `/dialog` switch is added to the contents of the *Full Command Line*, causing a dialog box to appear, prompting the user to specify the computer name.
    - **Rename using variable replacement**: The `/name` switch is added to the contents of the *Full Command Line*. Replace `<TEXT_AND_VARIABLES>` as needed, using a combination of text and the following variables, as required:
        - **$Serial**: The serial number of the client device.
        - **$Make**: The manufacturer of the client device or motherboard.
        - **$Model**: The model of the client device or motherboard.
        - **$Chassis**: The chassis type of the client device.
        - **$FormFactor**: The device type: `D` for Desktop, `L` for Laptop, `VM` for a VMware virtual machine.
        - **$Asset**: The asset tag of the client device.
        - **$OS**: The OS version of the client device (such as W7, WXP, W2K8, and so on).
        - **$Arch**: The OS architecture of the client device.
        - **$Mac**: The MAC address of the active NIC.

      For example:
      ```
      setcomputername_x64.exe /name:$OS$Arch-$Serial
      ```
    - **Rename using a data file**: Uses a data file to rename devices.

      1. Create a text file and list the entries using the following syntax:
         ```
         <mac_address|serial_number> = <device_name>
         ```
         For example:
         ```
         001122334455 = workstation55
         ```

```
001122334456 = workstation56
001122334457 = workstation57
```

2. Attach the file to the task. Click **Select file** and specify the file, or drag and drop the file in the *Drop file here* area.
3. Configure the contents of the *Full Command Line* field:
   - **/rdf**: The name of the newly created file. This switch automatically displays the name of the attached file.
   - **/dfk**: The type of device identifier used in the file: `$Serial` or `$Mac`.

   For example:
   ```
   setcomputername_x64.exe /log /rdf:my_file.txt /dfk:$Mac
   ```

- **Rename using the SMA/K1 database**: Uses the KACE Systems Management Appliance database to retrieve the contents of the `host_name` field for each device. This is indicated by the `/k1mysql` switch in the *Full Command Line* field. Additional identifiers are required.

1. Verify that the access to the KACE Systems Management Appliance database is enabled. On the KACE Systems Management Appliance, go to **Settings** > **Control Panel** > **Security Settings**, and ensure **Enable database access** is selected. If the option is disabled and you enable it, you must reboot the KACE Systems Management Appliance before this change can take effect. For more information, see the KACE Systems Management Appliance *Administrator Guide*.
2. In the *Full Command Line* field, supply information to the following switches:
   - **/k1ipaddress**: The IP address of the machine on which the KACE Systems Management Appliance is running.
   - **/k1dbname**: The name of the organization on the appliance. The default is `ORG1`.
   - **/k1dbuser**: The name of the user account on the appliance. The default is `R1`.
   - **/k1dbpass**: The user password. The default is `box747`.

   For example:
   ```
   setcomputername_x64.exe /log /k1mysql /k1ipaddress:192.0.2.0 /k1dbname:ORG1
   /k1dbuser:R1 /k1dbpass:box747
   ```

- **Rename using the SDA/K2 database**: Uses the KACE Systems Deployment Appliance database to retrieve device names. This is indicated by the `/k2mysql` switch in the *Full Command Line* field.
  - Verify that the access to the KACE Systems Deployment Appliance database is enabled. On the KACE Deployment Appliance, go to **Settings** > **Security** , and ensure **Enable database access** is selected.

7. **Post-installation tasks only**. Select the *Reboot Required* check box to reboot the appliance and run the next task in the sequence.
8. In *Expected Return Code*, enter a code that the task should return, if applicable. Otherwise, leave the default value of zero '0'.

   In general, most tasks exit with a zero '0' code, indicating success, but you can set it to any positive value, as applicable. Some installers exit with a different code, even when the install is successful. For example, anti-virus installers are typically successfully installed but exit with a different return code because they require a device reboot.
9. Click **Save**.

The task is now available to assign to scripted installations, sysprepped system images, and non-sysprepped system image deployments.

See Assign tasks to scripted installation deployment or Assign tasks to system deployment.

Add PowerShell Script

You can run PowerShell script as a pre-installation, mid-level, or post-installation task in the KACE Boot Environment (Windows) runtime environment or the Windows runtime environment.

1. Complete one of the following steps:
    a. On the left navigation pane, click **Library** to expand the section, then click **Pre-installation Tasks** to display the *Pre-installation Tasks* page.
    b. On the left navigation pane, click **Library** to expand the section, then click **Mid-level Tasks** to display the *Mid-Level Tasks* page.
    c. On the left navigation pane, click **Library** to expand the section, then click **Post-installation Tasks** to display the *Post-installation Tasks* page.
2. On the list page that appears, select **Choose Action** > **Add Powershell Script**.
3. On the page that appears, in *Name*, enter a logical name for the task, such as My PowerShell script.
4. Under *Upload File*, click **Select File**, and navigate to the PowerShell script.
5. Select the *Reboot Required* check box to reboot the appliance and run the next task in the sequence.
6. In *Expected Return Code*, enter a code that the task should return, if applicable. Otherwise, leave the default value of zero '0'.

    In general, most tasks exit with a zero '0' code, indicating success, but you can set it to any positive value, as applicable. Some installers exit with a different code, even when the install is successful. For example, anti-virus installers are typically successfully installed but exit with a different return code because they require a device reboot.

7. In *Notes*, add a note to identify the task.
8. Click **Save**.

    The task is now available to assign to scripted installations, sysprepped system images, and non-sysprepped system image deployments.

9. On the list page, click the task name.
10. On the task detail page that appears, review the contents of the *Full Command Line* field, and make any changes, as required.
11. If you made any changes to the command line, click **Save**, or click **Cancel** to return to the list page.

Add Provisioning Package

Provisioning packages contain collections of configuration settings. You can use them to quickly configure a Windows device without having to install a new image. You can run a provisioning package as a post-installation task in the Windows runtime environment.

1. On the left navigation pane, click **Library** to expand the section, then click **Post-installation Tasks** to display the *Post-installation Tasks* page.
2. On the list page that appears, select **Choose Action** > **Add Provisioning Package** to display the *Post-installation Task Detail* page.
3. On the page that appears, in *Name*, enter a logical name for the task, such as My Provisioning Package.
4. Under *Upload File*, click **Select File**, and navigate to the Provisioning Package file.

The **Reboot Required** option is selected by default and cannot be disabled. This is because a device reboot occurs each time this task runs.

5. In *Expected Return Code*, enter a code that the task should return, if applicable. Otherwise, leave the default value of zero '0'.

   In general, most tasks exit with a zero '0' code, indicating success, but you can set it to any positive value, as applicable. Some installers exit with a different code, even when the install is successful. For example, anti-virus installers are typically successfully installed but exit with a different return code because they require a device reboot.

6. In *Notes*, add a note to identify the task.
7. Click **Save**.

   The task is now available to assign to scripted installations, sysprepped system images, and non-sysprepped system image deployments.

8. On the list page, click the task name.
9. On the task detail page that appears, review the contents of the *Full Command Line* field, and make any changes, as required.
10. If you made any changes to the command line, click **Save**, or click **Cancel** to return to the list page.

Add Service Pack

You can install service packs automatically as they become available for the operating system to devices on local and remote networks. If you have a service pack stored at a different location, you can browse to and upload that service pack manually.

The Service pack task runs in the Windows environment after booting in to the operating system.

1. On the left navigation pane, click **Library** to expand the section, then click **Post-installation Tasks** to display the *Post-installation Tasks* page.
2. Select **Choose Action** > **Add Service Pack** to display the *Post-installation Task Detail* page.
3. In *Name*, enter a logical name to identify the task.
4. Download the service pack automatically or manually.

   - **From the *Service Pack* drop-down list, select the service pack, and click Download Service Pack automatically.**

     The *Command Line* field is automatically populated with the recommended parameters based on the service pack selection. If you modify this line, include the service pack filename.

   - **Select Upload Service Pack manually, and click Browse to upload the file. For more information, see About uploading files.**

     NOTE: When you upload the service pack manually, in *Parameters*, enter the command-line parameters to run the service pack.

5. In *Full Command Line*, enter the command-line parameters for the task.
6. Select the *Reboot Required* check box to reboot the appliance and run the next task in the sequence.
7. In *Expected Return Code*, enter a code that the task should return, if applicable. Otherwise, leave the default value of zero '0'.

   In general, most tasks exit with a zero '0' code, indicating success, but you can set it to any positive value, as applicable. Some installers exit with a different code, even when the install is successful. For example, anti-virus installers are typically successfully installed but exit with a different return code because they require a device reboot.

8. In *Notes*, add a note to identify the task.
9. Click **Save**.

   The task is now available to assign to scripted installations, sysprepped system images, and non-sysprepped system image deployments.

See Assign tasks to scripted installation deployment or Assign tasks to system deployment.

Add Shell Script

You can create your own shell scripts to run as a pre-installation, mid-level, or post-installation task in the KACE Boot Environment (Mac OS X) before deploying the operating system or re-imaging a target device.

1. Complete one of the following steps:
    a. On the left navigation pane, click **Library** to expand the section, then click **Pre-installation Tasks** to display the *Pre-installation Tasks* page.
    b. On the left navigation pane, click **Library** to expand the section, then click **Mid-level Tasks** to display the *Mid-Level Tasks* page.
    c. On the left navigation pane, click **Library** to expand the section, then click **Post-installation Tasks** to display the *Post-installation Tasks* page.
2. On the list page that appears, select **Choose Action** > **Add Shell Script**.
3. On the page that appears, in *Name*, enter a logical name to identify the task.
4. Select a Runtime Environment:
    - **Pre-installation and mid-level shell scripts**: Select *SDA Boot Environment (Mac OS X)*.
    - **Post-installation shell scripts**: Select *Mac OS X*.

    For more information, see About runtime environments.
5. In *Shell Script*, enter the script.
6. In *Expected Return Code*, enter a code that the task should return, if applicable. Otherwise, leave the default value of zero '0'.

    In general, most tasks exit with a zero '0' code, indicating success, but you can set it to any positive value, as applicable. Some installers exit with a different code, even when the install is successful. For example, anti-virus installers are typically successfully installed but exit with a different return code because they require a device reboot.
7. In *Notes*, add a note to identify the task.
8. Click **Save**.

    The task is now available to assign to scripted installations, sysprepped system images, and non-sysprepped system image deployments.

Add KACE Agent Installer

You can download the KACE Agent file to a local directory, then upload the installer as a single file or a ZIP archive to run as a post-installation task. The appliance runs the task in the runtime environment that you specify.

You can assign the *Apply KUID to KACE Agent* post-installation task to prevent a duplicate asset on the KACE Systems Management Appliance if the KUID of the KACE Agent that was installed on the target device was not maintained. The KACE Agent software is in the \\KACE_Systems_Management_Appliance_host_name\client\agent_provisioning directory. For

an explanation of available command-line options and Agent configuration properties, see the KACE Systems Management Appliance *Administrator Guide*. The KACE Agent does not require .NET 4.0 to install.

1. On the left navigation pane, click **Library** to expand the section, then click **Post-installation Tasks** to display the *Post-installation Tasks* page.
2. Select **Choose Action** > **Add SMA Agent Installer** to display the KACE Agent Installer detail task page.
3. In *Name*, change the name to identify the task, for example KACE Agent for Windows.
4. Select a *Runtime Environment.* See About runtime environments.
5. Next to *Upload*, click **Browse** to select the appropriate file.
6. In *Full Command Line*, enter the command-line parameters for the task.
7. Select the *Reboot Required* check box to reboot the appliance and run the next task in the sequence.
8. In *Expected Return Code*, enter a code that the task should return, if applicable. Otherwise, leave the default value of zero '0'.

   In general, most tasks exit with a zero '0' code, indicating success, but you can set it to any positive value, as applicable. Some installers exit with a different code, even when the install is successful. For example, anti-virus installers are typically successfully installed but exit with a different return code because they require a device reboot.
9. In *Notes*, add a note to identify the task.
10. Click **Save**.

    The task is now available to assign to scripted installations, sysprepped system images, and non-sysprepped system image deployments.

See Assign tasks to scripted installation deployment or Assign tasks to system deployment.

Add Windows Script

You can run Windows scripts as a pre-installation, mid-level, or post-installation task in the KACE Boot Environment (Windows) runtime environment.

1. Complete one of the following steps:
   a. On the left navigation pane, click **Library** to expand the section, then click **Pre-installation Tasks** to display the *Pre-installation Tasks* page.
   b. On the left navigation pane, click **Library** to expand the section, then click **Mid-level Tasks** to display the *Mid-Level Tasks* page.
   c. On the left navigation pane, click **Library** to expand the section, then click **Post-installation Tasks** to display the *Post-installation Tasks* page.
2. On the list page that appears, select**Choose Action** > **Add Windows Script**.
3. On the page that appears, in *Name*, enter a logical name for the task, such as Collect computer information before formatting.
4. Next to *Upload*, click **Browse** to select the appropriate file, such as a VBScript or a JavaScript.
5. Select the *Reboot Required* check box to reboot the appliance and run the next task in the sequence.
6. In *Expected Return Code*, enter a code that the task should return, if applicable. Otherwise, leave the default value of zero '0'.

   In general, most tasks exit with a zero '0' code, indicating success, but you can set it to any positive value, as applicable. Some installers exit with a different code, even when the install is successful. For example, anti-virus installers are typically successfully installed but exit with a different return code because they require a device reboot.
7. In *Notes*, add a note to identify the task.
8. Click **Save**.

   The task is now available to assign to scripted installations, sysprepped system images, and non-sysprepped system image deployments.

Working with task groups

Task groups allow you to create a sequence of common tasks to build and capture a system image.

You can easily reuse a task group, when needed, to create system images of the same type and function. For example, you can create a task group that builds a Microsoft Windows 10 system with a Microsoft Office suite, and associate one or more task groups with system images and scripted installations each time you need to re-create a common deployment scenario.

Add task group

A default installation includes two sample task groups for partitioning and formatting a drive for Mac OS X and Windows. You can add and manage task groups that best suit your business needs, to easily reuse common deployment scenarios, and associate task groups with system images, scripted installations, or custom deployments, as applicable.

The process of creating tasks for Mac OS X, Windows, and Linux are the same, however the collection of tasks available for these two operating systems is different, and it only contains the tasks that apply to the respective runtime environment.

1. On the left navigation pane, click **Library** to expand the section, then click **Task Groups** to display the *Task Groups* page.
2. Complete one of the following steps:
    a. To create a group of Windows tasks, select **Choose Action** > **New Windows Task Group**.
    b. To create a group of Mac OS X tasks, select **Choose Action** > **New Mac OS X Task Group**.
    c. To create a group of Linux tasks, select **Choose Action** > **New Linux Task Group**.

    The *Task Group Detail* page appears.
3. In the *Name* field, type the name of the task group.
4. **Optional**. In the *Notes* field, provide additional information, if required.
5. Under *Installation Plan*, add the tasks in the order that you want the tasks to run.

    To add a task to the installation plan, drag and drop it to the left column, click the plus sign, or double-click the task in the right column, as desired.

    Available tasks are sorted alphabetically in each list on the right. If there are more than six available tasks in a list, expand the drawer to see the entire list, or scroll up or down, as needed.

    a. Add tasks from the *Available Pre-installation Tasks* column to the *Run Pre-installation Tasks* column.

    NOTE: If you choose to erase the drive contents, ensure that the *Format C* task follows the *Create Single Partition* task.

    b. Add tasks from the *Available Mid-Level Tasks* column to the *Run Mid-Level Tasks* column.
    c. Add tasks from the *Available Post-installation Tasks* column to the *Run Post-installation Tasks* column.

Tip: **TIP:** Filters are available for each task type. For example, to look for a specific pre-installation task, in the *Available Pre-Installation Tasks* column, in the *Filter Pre-Installation Tasks* field, type the task name.

Tip: **TIP:** To remove a task from the installation plan, drag and drop it to the right column, click the minus sign, or double-click the task in the left column.

Tip: **TIP:** To remove all tasks from a column, click the button in the column header, on the right. For example, to remove all assigned pre-installation tasks, in the *Run Pre-Installation Tasks* column, in the column header bar, click *Remove all Pre-Installation Tasks*.

6. Complete one of the following steps:
   - **To create a copy of this task group, click Duplicate.**
   - **To save your changes, click Save.**

About uploading files

You can upload a single file or a ZIP archive containing multiple files to run as a pre-installation or as a post-installation task. The appliance runs the task in the runtime environment that you specify.

About runtime environments

The runtime environment determines when the appliance task engine runs the task.

Runtime environment	Description
KACE Boot Environment (Windows)	Runs before the first boot of the operating system.
Windows	Runs after the first boot of the Windows operating system.
KACE Boot Environment (Mac OS X)	Runs before the first boot of the operating system.
Mac OS X	Runs on the first boot of Mac operating system using a login hook.
KACE Boot Environment (Linux)	Runs before the first boot of the operating system.
Linux	Runs after the first boot of the Linux operating system.

Set task error handling option

You can set the task error handling for devices with the Windows operating system to prompt on errors or to continue on errors. You can also enable the *Cancel* button to display on target devices to cancel a failed task.

1. Complete one of the following steps:
   - **On the left navigation pane, choose Deployments > System Images to display the *System Images* page. Then click a system image name to display the *System Image Detail* page.**
   - **On the left navigation pane, choose Deployments > Scripted Installations to display the *Scripted Installation* page. Then click a scripted installation name to display the *Scripted Installation Detail* page.**
   - **On the left navigation pane, choose Deployments > Custom Deployments to display the *Custom Deployments* page. Then click a custom deployment name to display the *Custom Deployments Detail* page.**
2. Click **Task Error Handling** and choose the desired option:
   - ***Prompt on errors*: Opens the *Task Error* page, which enables you to edit the target device, retry the task, resume the deployment, or reboot the device with an option to cancel or continue.**
   - ***Continue on errors*: Continues the deployment without prompting.**
3. Select the *Show cancel button on client* check box to display the *Cancel* button on the *Task Engine* page on the target device.

Assign tasks to system deployment

You can configure the steps on the appliance or a remote (RSA) appliance which are necessary (or required) to run a system deployment. Pre-installation tasks run before the operating system setup starts and mid-level tasks run after the operating system is deployed. Post-installation tasks run after the operating system reboots and the target devices are logged in for the first time.

You can only edit system images on the appliance that captured them. For example, if you view the details of a system image captured by the appliance, you can edit that image on the *System Image Detail* page in the appliance Administrator Console, but not in the KACE Remote Appliance Console. If that system image is captured on the appliance and synced to the RSA, the *System Image Detail* page in the KACE Remote Appliance Console only allows you to review the system image details, but not to edit them. A link appears on this page that allows you to quickly navigate to the *System Image Detail* in the appliance Administrator Console, and edit the system image, as required.

1. On the left navigation pane, click **Deployments**, then click **System Images** to display the *Systems Images* page.
2. Select the image to view the *System Image Detail* page.
3. If you want to add any tasks specified in a task group, under *Installation Plan*, click **Choose a task group**, select a desired task group, and click **Apply**.
   - Only those task groups associated with the OS of the selected system image appear in the list. For example, if you selected a Windows system image, the list displays the task groups that can be applied to Windows systems.
   - You can add multiple task groups to a system image, scripted installation, or custom deployment.
   - Tasks associated with task groups are always added to their respective deployment stages in a system image, scripted installation, or custom deployment. For example, when you add a task group, the pre-installation tasks from that task group will appear under *Run Pre-installation Tasks*.
   - The order of tasks associated with the task groups that you add to a system image, scripted installation, or custom deployment reflect the order in which these task groups are added: the tasks added to the first task group

appear at the top of the list, followed by the tasks associated with the task group that is added after the first one, and so on.

4. If you want to delete all tasks previously added to the system deployment, including any tasks associated with task groups, click **Clear All Tasks**.
5. Under *Installation Plan*, add the tasks in the order that you want the tasks to run.

   To add a task to the installation plan, drag and drop it to the left column, click the plus sign, or double-click the task in the right column, as desired.

   Available tasks are sorted alphabetically in each list on the right. If there are more than six available tasks in a list, expand the drawer to see the entire list, or scroll up or down, as needed.

   a. Add tasks from the *Available Pre-installation Tasks* column to the *Run Pre-installation Tasks* column.

   NOTE: If you choose to erase the drive contents, ensure that the *Format C* task follows the *Create Single Partition* task.

   b. Add tasks from the *Available Mid-Level Tasks* column to the *Run Mid-Level Tasks* column.

   c. Add tasks from the *Available Post-installation Tasks* column to the *Run Post-installation Tasks* column.

Tip: **TIP:** Filters are available for each task type. For example, to look for a specific pre-installation task, in the *Available Pre-Installation Tasks* column, in the *Filter Pre-Installation Tasks* field, type the task name.

Tip: **TIP:** To remove a task from the installation plan, drag and drop it to the right column, click the minus sign, or double-click the task in the left column.

Tip: **TIP:** To remove all tasks from a column, click the button in the column header, on the right. For example, to remove all assigned pre-installation tasks, in the *Run Pre-Installation Tasks* column, in the column header bar, click *Remove all Pre-Installation Tasks*.

6. **KACE Systems Deployment Appliance only**. Click **Save**.
7. **RSA only**. Choose one of the following steps, as applicable:

   - **To attach the tasks to the image and synchronize the tasks from the appliance to the RSA, click Save and Sync.**
   - **To only attach the tasks to the image and synchronize the tasks from the appliance to the RSA at a later time, click Save.**

   The *System Image Detail* page closes and the *System Images* list page appears. If you selected **Save and Sync**, a message at the top of the page indicates that the changes made to the system image are being synchronized with the appliance. When the process finishes, the updated system image is now available for deployment from the RSA. For information on how to deploy system images, see Deploy the image manually.

Assign tasks to scripted installation deployment

You can configure the steps that the appliance takes to run a scripted installation deployment. Pre-installation tasks run before the operating system setup starts and mid-level tasks run after the operating system is deployed. Post-installation tasks run after the operating system reboots and the target devices are logged in for the first time.

1. On the left navigation pane, click **Deployments**, then click **Scripted Installations** to display the *Scripted Installations* page.
2. Select the scripted installation to view the *Scripted Installation Detail* page.
3. If you want to add any tasks specified in a task group, click **Choose a task group**, select a desired task group, and click **Apply**.
   - Only those task groups associated with the OS of the selected system image appear in the list. For example, if you selected a Windows system image, the list displays the task groups that can be applied to Windows systems.
   - You can add multiple task groups to a system image, scripted installation, or custom deployment.
   - Tasks associated with task groups are always added to their respective deployment stages in a system image, scripted installation, or custom deployment. For example, when you add a task group, the pre-installation tasks from that task group will appear under *Run Pre-installation Tasks*.
   - The order of tasks associated with the task groups that you add to a system image, scripted installation, or custom deployment reflect the order in which these task groups are added: the tasks added to the first task group appear at the top of the list, followed by the tasks associated with the task group that is added after the first one, and so on.
4. If you want to delete all tasks previously added to the scripted installation deployment, including any tasks associated with task groups, under *Installation Plan*, click **Clear All Tasks**.
5. Under *Installation Plan*, add the tasks in the order that you want the tasks to run.

   To add a task to the installation plan, drag and drop it to the left column, click the plus sign, or double-click the task in the right column, as desired.

   Available tasks are sorted alphabetically in each list on the right. If there are more than six available tasks in a list, expand the drawer to see the entire list, or scroll up or down, as needed.

   a. Add tasks from the *Available Pre-installation Tasks* column to the *Run Pre-installation Tasks* column.

   NOTE: If you choose to erase the drive contents, ensure that the *Format C* task follows the *Create Single Partition* task.

   b. Add tasks from the *Available Mid-Level Tasks* column to the *Run Mid-Level Tasks* column.

   c. Add tasks from the *Available Post-installation Tasks* column to the *Run Post-installation Tasks* column.

Tip: **TIP:** Filters are available for each task type. For example, to look for a specific pre-installation task, in the *Available Pre-Installation Tasks* column, in the *Filter Pre-Installation Tasks* field, type the task name.

Tip: **TIP:** To remove a task from the installation plan, drag and drop it to the right column, click the minus sign, or double-click the task in the left column.

Tip: **TIP:** To remove all tasks from a column, click the button in the column header, on the right. For example, to remove all assigned pre-installation tasks, in the *Run Pre-Installation Tasks* column, in the column header bar, click *Remove all Pre-Installation Tasks*.

6. Click **Save**.

Assign tasks to custom deployment

You can configure the steps that the appliance takes to run a custom deployment. Pre-installation tasks run before the operating system setup starts and mid-level tasks run after the operating system is deployed. Post-installation tasks run after the operating system reboots and the target devices are logged in for the first time.

1. On the left navigation pane, click **Deployments**, then click **Custom Deployments** to display the *Custom Deployments* page.
2. On the *Custom Deployments* page, click a custom deployment name to display the *Custom Deployment Detail* page for the selected item.
3. If you want to add any tasks specified in a task group, click **Choose a task group**, select a desired task group, and click **Apply**.
   - Only those task groups associated with the OS of the selected system image appear in the list. For example, if you selected a Windows system image, the list displays the task groups that can be applied to Windows systems.
   - You can add multiple task groups to a system image, scripted installation, or custom deployment.
   - Tasks associated with task groups are always added to their respective deployment stages in a system image, scripted installation, or custom deployment. For example, when you add a task group, the pre-installation tasks from that task group will appear under *Run Pre-installation Tasks*.
   - The order of tasks associated with the task groups that you add to a system image, scripted installation, or custom deployment reflect the order in which these task groups are added: the tasks added to the first task group appear at the top of the list, followed by the tasks associated with the task group that is added after the first one, and so on.
4. If you want to delete all tasks previously added to the custom deployment, including any tasks associated with task groups, under *Installation Plan*, click **Clear All Tasks**.
5. Under *Installation Plan*, add the tasks in the order that you want the tasks to run.

   To add a task to the installation plan, drag and drop it to the left column, click the plus sign, or double-click the task in the right column, as desired.

   Available tasks are sorted alphabetically in each list on the right. If there are more than six available tasks in a list, expand the drawer to see the entire list, or scroll up or down, as needed.

   a. Add tasks from the *Available Pre-installation Tasks* column to the *Run Pre-installation Tasks* column.

   NOTE: If you choose to erase the drive contents, ensure that the *Format C* task follows the *Create Single Partition* task.

   b. Add tasks from the *Available Mid-Level Tasks* column to the *Run Mid-Level Tasks* column.

   c. Add tasks from the *Available Post-installation Tasks* column to the *Run Post-installation Tasks* column.

Tip: **TIP:** Filters are available for each task type. For example, to look for a specific pre-installation task, in the *Available Pre-Installation Tasks* column, in the *Filter Pre-Installation Tasks* field, type the task name.

Tip: **TIP:** To remove a task from the installation plan, drag and drop it to the right column, click the minus sign, or double-click the task in the left column.

Tip: **TIP:** To remove all tasks from a column, click the button in the column header, on the right. For example, to remove all assigned pre-installation tasks, in the *Run Pre-Installation Tasks* column, in the column header bar, click *Remove all Pre-Installation Tasks*.

6. Click **Save**.

Edit deployment tasks

You can edit tasks associated with system image or scripted installation deployments. Each task represents a step that the appliance takes to run a system image or scripted installation deployment. Pre-installation tasks run before the operating system setup starts, and post-installation tasks run after the operating system is deployed and the target devices are logged in for the first time.

System image deployment tasks only. You can only edit system image deployment tasks when you are using the appliance Administrator console. The KACE Remote Site Appliance does not allow you to edit any task parameters. That is because the *System Image Detail* page in the KACE Remote Site Appliance displays all tasks that exist on the associated appliance, and therefore they can only be edited in that KACE SDA's Administrator console.

1. Complete one of the following steps:
   - **On the left navigation pane, choose Deployments > System Images to display the *System Images* page. Then click a system image name to display the *System Image Detail* page.**
   - **On the left navigation pane, choose Deployments > Scripted Installations to display the *Scripted Installation* page. Then click a scripted installation name to display the *Scripted Installation Detail* page.**
   - **On the left navigation pane, choose Deployments > Custom Deployments to display the *Custom Deployments* page. Then click a custom deployment name to display the *Custom Deployments Detail* page.**
2. Under *Installation Plan*, locate the task that you want to edit, and click ℹ.

   Tip: **TIP:** Filters are available for each task type. For example, to look for a specific pre-installation task, in the *Available Pre-Installation Tasks* column, in the *Filter Pre-Installation Tasks* field, type the task name.

   Tip: **TIP:** To remove a task from the installation plan, drag and drop it to the right column, click the minus sign, or double-click the task in the left column.

   A dialog box appears, showing the task details.
3. Edit the task, as required.

Option	Description
File	To replace a file associated with the task (if available), click **Replace**, and select the appropriate file.
Parameters	Edit the task parameters, as required.
Notes	Add a note about the task. For example, John's task to create a partition.

4. **BAT scripts only**. In the *BAT Script* box, type the name of the BAT script.
5. **DISKPART scripts only**. In the *DISKPART Script* box, type the name of the DISKPART script.
6. Click **Save** to close the dialog box.
7. On the *System Image Detail* or *Scripted Installation Detail*page, click **Save**.

Automating deployments

Appliance boot actions automate scripted installation, system image, and multicast WIM and DMG image deployments by initiating the deployment the next time that the target device network boots in to the KACE Boot Environment (KBE) or NetBoot Environment at a scheduled time.

The appliance boot process requires that the device Network Interface Card (NIC) is in the BIOS boot order because the appliance identifies devices by their MAC address.

You can create a boot action for one device or for multiple devices, and assign multiple boot actions to the same device by managing the boot action schedule.

When you make changes to an existing boot action, the boot action with previous information is deleted automatically.

Create a boot action

You can create a boot action to automate scripted installation, system image, and KACE Boot Environment and NetBoot environment deployments to devices that are in *Device Inventory*, *Network Inventory*, scanned devices, or to any device with a known MAC address.

1. On the left navigation pane, click **Deployments**, then click **Automated Deployments** to display the *Automated Deployments* page.
2. Select **Choose Action** > **New Boot Action** to display the *Automated Deployment Detail* page.

   NOTE: You can assign multiple boot actions to the same device by managing the schedule for the deployment.
3. Under *Boot Action Details*:
   a. Assign a *Name* to the boot action.
   b. In the *From* box, select the appliance or a linked RSA appliance containing the deployment that you want to automate.
   c. Select a deployment from the *Deployment* drop-down list.

   System images only. The list of system images depends on your selection in the *From* box:

   - If you selected the appliance, the list displays all system images that exist on the appliance.
   - If you selected an RSA, the list displays all system image that are synchronized to the RSA and also any images that are captured with the RSA.

   Only use WIM images for Windows multicast deployments, and use DMG images for Mac OS X multicast deployments.

   d. Add *Notes* to identify the boot action.
4. Under *Options* > *Schedule*, select one of the following to run the deployment:
   a. *Run at next boot*: Initiates the deployment on the next network boot.
   b. *Schedule to run later*: Specifies a day and time: *Run once on: every* (day), *at*: H (hour), and M (minute). *Run repeatedly* runs the deployment every day at the time you specify.
5. Under *Options* > *Type*, select a unicast or multicast deployment.

   NOTE: You cannot schedule multicast ASR deployments to run later.
6. If you select a multicast deployment:

a. **Optional**: In *Timeout to wait for connection 'Ready to receive' state*, increase the timeout to allow target devices more time to network boot. The default is ten minutes.
b. Click **Show advanced settings** to change the default multicast address, control channel port, multicast hops, transmission rate, and log level.
c. To use these settings for automated deployments going forward, select the **Make these the default settings** check box.

For complete information about multicast settings, see Edit the default multicast settings.

7. **Optional**: For multicast deployments, in *Timeout to wait for connection 'Ready to receive' state*, increase the timeout to allow target devices more time to network boot. The default is 10 minutes. Click **Show advanced settings** to change the default multicast address, control channel port, and transmission rate for this deployment. .
8. Under *Devices*, enter one or more MAC addresses, or select devices from the *View All* drop-down list to add devices to the deployment.

   You can filter devices by type to show devices that match the specified criteria.
9. Click **Save**.

   The *Automated Deployments* page lists the boot action.

Run deployment on next network boot

You can initiate a scripted installation or a system image deployment of the operating system the next time that one or more target devices boot in to the KACE Boot Environment (KBE).

1. On the left navigation pane, click **Deployments**, then click **Automated Deployments** to display the *Automated Deployments* page.
2. Under *Name*, select the boot action to display the *Automated Deployment Detail* page.
3. Under *Options* > *Schedule*, select *Run at next boot* to deploy the image on the next network boot.
4. Click **Save**.

On the left navigation pane, click **Progress** to view the status of an automated deployment currently running or click **Audit Log** to view the status of completed automated deployments.

Modify a boot action

You can add devices to a boot action, remove devices, change the scheduling options, switch from a unicast or to a multicast deployment for WIM and DMG images, and rename the boot action. You cannot change the image for a boot action.

1. On the left navigation pane, click **Deployments**, then click **Automated Deployments** to display the *Automated Deployments* page.
2. Under *Name*, select the boot action to display the *Automated Deployment Detail* page.
3. Make any necessary changes to the boot action.
4. Click **Save**.

   The *Automated Deployments* page lists the boot action.

Set default boot action

By default, devices that are not in the appliance Device Inventory boot in to the *KBE Main Menu*. For example, devices on your network that have been scanned display in your appliance Network Inventory. You can set the boot action to boot to the hard drive for devices that are not in the appliance Device Inventory or Network Inventory.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **General Settings** to display the *General Settings* page.
2. Under *PXE Options*, set the default boot action to one of the following options:
   - *Boot to the KBE Main Menu* **for devices that are not in the appliance Device Inventory.**
   - *Boot to the hard drive* **for devices that have not booted in to the KBE. Include devices that are not in Network Inventory**
3. Click **Save**.

Configure new WIM images to stream directly from or to the server

When you capture or deploy WIM images, you have an option to stream the image directly from or to the server instead of using a local drive.

After an image is captured locally, it is sent to the server through network sockets. Some network configurations may cause issues when files are transferred this way. Streaming the image directly to the server causes its files to be copied directly to the server share instead of using network sockets.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **General Settings** to display the *General Settings* page.
2. Set the *Imaging Options* as required:
   - *Default setting to capture WIM files directly to server (individual captures can be changed on the KBE image capture page)***: Select this option for the default setting in the KBE to stream directly to the server.**
     - WIM images captured directly to the server must also be deployed directly from the server. This option cannot be changed on the image detail page.
     - If you choose not to select this option, and there is not enough disk space locally, the image is streamed directly to the server.
   - *Default setting to deploy new WIM files directly from server (individual deployments can be changed on the image detail page)***: Select this option so the default setting on newly captured images is to deploy directly from the server.**

     NOTE: This setting will only apply to those WIM images that have been captured directly to the server.
3. Click **Save**.

Specify deployment options

The *System Image Detail* page allows you to view the image settings, add a boot action, download the log files associated with the image, and set the options for how the appliance responds to errors. It also allows you to specify deployment options.

1. Under *Deployments*, select the deployment to display the *System Image Detail* page.
2. Under *Deploy Options*, select any of following options, as required:
   - **Deploy directly from server**: Select this option if you want to deploy this WIM image directly from the server. WIM images captured directly to the server must also be deployed directly from the server. In that case, this option appears selected, and cannot be changed.
   - **Force continue on errors**: Select this option if you want to continue the capture and the upload process even if warnings and fatal errors occur.
   - **Include debug output in log**: Select to enable debugging level logging and upload the logs to the *Appliance Logs* page.

     CAUTION: This option considerably increases the time of deployment. Only use it while troubleshooting.
   - **Use driver feed (only with Sysprepped images)**: Select to enable the Driver Feed for sysprepped system images to obtain missing drivers. For Windows K-Images and WIM images, the *Sysprepped* field on the *System Image Detail* page indicates if an image is sysprepped. Optionally, enable this option by default:
     1. Open the Administrator Console in a new browser instance or tab.
     2. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **General Settings** to display the *General Settings* page.
     3. Under *Imaging Options*, select the *Enable driverfeed for newly captured sysprepped images* check box. Selecting this option automatically adds drivers to the target system deployed with newly captured sysprepped system images.
     4. Click **Save**, and return to the *Deploy Options* on the *System Image Detail* page.
   - **Shutdown target device after last task**: Select if you want to turn off the target device when the image is installed.
   - **Allow Appliance to calculate Auto Logon Count for Unattend file**: Select this option if you want to enable the appliance to calculate the number of auto logon attempts that take place during installation. The number of auto logon attempts is written to the Unattend.xml file, that contains parameters for a Windows system setup. When this option is enabled, the appliance calculates the auto logon count by adding the number of system reboots that are specified in the tasks contained in the installation plan.
   - **Hide Deployment from KBE**: Select this option if you want to hide the system image from the KACE Boot Environment (KBE).

     NOTE: Scripted deployments marked as hidden from KBE do not appear in the *Deployment* drop-down list on the *Automated Deployment Detail* page when creating a boot action.
   - **Use Unattend File from Library**: Select this option if you want to use one of the Sysprepped `unattend` files stored on the appliance as a mid-level task, and select a desired `unattend` file. Selecting this option enables the mid-level task automatically. The OS and architecture of the `unattend` file must match those of the system image to make the file available for selection.
   - **Set Auto Logon Count (Leave blank for no change):** Select this option if you want to limit the number of auto logon attempts that take place during system installation. You can enter any value between zero and 99.

Schedule a deployment

You can schedule system image or scripted installation deployments to a single device or to multiple devices to run later. You can also schedule multiple deployments to the same device. You cannot schedule Mac OS X image deployments to run later.

You can add or remove devices when you schedule a deployment.

1. On the left navigation pane, click **Deployments**, then click **Automated Deployments** to display the *Automated Deployments* page.
2. Select **Choose Action** > **New Boot Actions** or select an existing boot action to display the *Automated Deployment Detail* page.
3. Under *Options* > *Schedule*, select one of the following to run the deployment:
    a. *Run at next boot*: Initiates the deployment on the next network boot.
    b. *Schedule to run later*: Specifies a day and time: *Run once on: every* (day), *at*: H (hour), and M (minute). *Run repeatedly* runs the deployment every day at the time you specify.
4. Click **Save**.

Delete a boot action

You can delete boot action deployments if they become out-of-date or to save disk space.

1. On the left navigation pane, click **Deployments**, then click **Automated Deployments** to display the *Automated Deployments* page.
2. Select the boot action deployment to delete.
3. Select **Choose Action** > **Delete**.
4. Click **Yes** to confirm.

Create a multicast WIM image deployment

You can create a multicast deployment for WIM images to send one image once to multiple devices at the same time. Multicast deployments reduce the network bandwidth if the routers on your network support multicast, and if the target devices have the hard disk space for the image. Multicast deployments support only single-partition images.

Create a boot action for each WIM image that you want to multicast.

NOTE: Only one multicast deployment can take place at a time.

Determine if your network requires modifying the settings on the hardware to enable multicast images to reach the target devices. For information on creating a multicast DMG image deployment, see .

NOTE: Go to http://www.itninja.com/community/dell-kace-k2000-deployment-appliance for information on your specific routers and switches.

1. On the left navigation pane, click **Deployments**, then click **Automated Deployments** to display the *Automated Deployments* page.
2. Under *Name*, select the deployment from the list to display the *Automated Deployment Detail* page; otherwise, see Create a boot action and Schedule a deployment.
3. **Optional**: Under *Boot Action Details,* rename or add notes to identify the boot action.
4. Under *Options* > *Type*, select **Multicast**.

   Optional: Click **Show advanced settings** to change the default multicast settings for this deployment. To change the settings for all multicast deployments, see Edit the default multicast settings.
5. Under *Devices* > *Selected Devices*, click or select a Mac address. You can also click **Paste multiple MAC addresses** to paste in multiple address, and you can filter device by type to show devices that match the specified criteria from the *View All* drop-down list to
6. Click **Save**.

   The *Automated Deployments* page lists the boot action.

On the left navigation pane, click **Deployments**, then click **System Images** to select the image assigned to the boot action to add pre-installation and post-installation tasks, and to configure the error handling.

Edit the default multicast settings

The changes that you make to the default multicast settings apply to all new multicast deployments.

You can change the multicast settings on a per deployment basis. Navigate to the *Deployments* page, and select the boot action to display the *Automated Deployment Detail* page, then click Show advanced settings.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Default Multicast Settings** to display the *Default Multicast Settings* page.
2. Change the *Timeout to wait for connection 'Ready to receive' state* for the duration that the appliance waits for all target devices to connect. The default is 10 minutes.

   NOTE: Consider the connection time that it might take for a task to run or for a device to boot. If you set the timeout to 10 minutes and only one device connects after 5 minutes, the appliance resets to 10 minutes to wait for the remaining devices to connect.
3. Select the **Multicast Protocol**, as required by your environment:
   - **Pragmatic General Multicast (PGM)**
   - **NACK-Oriented Reliable Multicast (NORM)**
     - The Internet Group Management Protocol (IGMP) is a sub-set of the NORM, and is also supported.

   While PGM appears to provide faster data transfer, NORM can typically handle higher transmission rates and is in general more reliable. Choose the protocol that best suits your needs.
4. Set a different IPv4 *Multicast address* if a different service is using the default address.
5. If another device on your network is using port 2112, specify another port number in the *Control channel port* field.
6. In the *Multicast hops* field, type the number of multicast hops over subnets. The default value is 1, but you can change it to suit your needs.
7. Lower the *Transmission Rate*, if required.

The transmission rate determines the success or failure of the deployment. The default is 8MB.

8. If you want to revert to the settings included with the default installation, click **Reapply factory settings**.
9. Adjust the *Log level*, as needed by selecting one of the following options:
    - **Fatal errors only**
    - **Fatal errors and warnings**
    - **Trace logging**
    - **Detailed logging**
    - **Verbose logging**
10. Click **Save**.

View automated deployments in progress

You can view the progress of automated deployments that are currently running, the status of assigned tasks, and which image was deployed to which device.

1. On the left navigation pane, click **Progress**, click **Automated Deployments** to display the **Automated Deployment Progress** page.
2. Under *Name*, select the boot action to display the *Automated Deployment Detail* page.
3. Under the *Devices* menu bar, click **Details** to view the status of the assigned tasks.

On the left navigation pane, click **Audit Log** to view the success or failure of completed automated deployments.

View completed automated deployments

You can view the success or failure of completed automated deployments, the status of assigned tasks, and which image was deployed to which device.

1. On the left navigation pane, click **Audit Log**.
2. Under *Name*, select the boot action to display the *Boot Action Log Detail* page.
3. Under the *Devices* menu bar, click **Details** to view the status of the assigned tasks.

The image must be re-deployed separately to the devices where the deployment failed.

Edit failed tasks

If a task fails, you can edit the task from the device where it failed.

Use a VNC or Remote Desktop connection to connect to the target device.

NOTE: The *Client Task Error* screen displays only on target devices with the Windows operating system.

1. Select one of the following options:
   - **Open a *Command Prompt* to run commands on the device.**
   - **Open *Notepad* to modify any file.**
   - **Open *Edit Tasks.xml file with Notepad* to change the `Tasks.xml` file.**
   - ***Edit the Registry* to change the OS configuration information.**
   - ***Retry failed task* to run the task again.**
   - ***Resume task execution* to continue the deployment with the failed task.**
   - ***Reboot machine* to restart the deployment.**
   - ***Shut down machine* to power off the device.**

     NOTE: You can view failed tasks on the appliance *Audit Log* page.

View the automated deployment image details

You can view the details of the image assigned to an automated boot action deployment.

1. On the left navigation pane, click **Progress**, then click **Automated Deployments** to display the *Automated Deployment Progress* page.
2. In the *Deployment* menu option, select the image for the boot action to view the *System Image Detail* or *Scripted Installation Detail* page.

Performing manual deployments

You can deploy images manually using a USB flash device. Manual deployments are useful when the target device is not connected to the network, when deploying directly from the source media, and when deploying UEFI images.

You can download an image from the appliance to a USB device after you load the KACE Boot Environment or the NetBoot environment on to the USB device.

After the boot environment and image are on the USB device, create the appliance driver share directory structure on the USB device and add the required drivers. When the USB device configuration is complete with the boot environment, the image and the drivers, you can boot the target devices in to the boot environment.

When you boot Windows devices in to the KACE Boot Environment, the *KBE Main Menu* displays immediately and provides menu options to capture and deploy images.

When you boot Mac OS X devices in to the NetBoot environment, the *appliance Imaging Utility* displays immediately and provides menu options to capture and deploy images.

Download the boot environment as bootable ISO

You can download a bootable ISO to a USB flash drive for the KACE Boot Environment (KBE) or for the NetBoot environment.

If you are downloading a KACE Boot Environment, verify that the KBE that you are downloading has all of the required drivers. If you add or remove any drivers before downloading the KBE, you must rebuild the KBE.

1. On the left navigation pane, click **Deployments**, then click **Boot Environments** to display the *Boot Environments* page.
2. Select the boot environment that you want to install to the USB flash device to display the *Boot Environment Detail* page.
3. Select the **Create bootable USB Flash drive image for this Boot Environment** check box and save the file.

   This process creates a bootable USB image and displays the *Status* as *Completed*.
4. On the *Boot Environment Detail* page, select **Download bootable USB flash drive image for this Boot Environment**.
5. **Optional**. Indicate how you want to boot this environment.
   - If you want the user to choose a PXE boot using the `memdisk` utility, select **Use Memdisk to boot this Boot Environment for BIOS clients**. Use this option for legacy BIOS boot environments to enable PXE boots.
   - If you clear this option, the boot environment will use `wimboot`.
6. Click *Download bootable ISO for this Boot Environment* to start the download.

Network boot a target device

You must network boot the target device in to the KACE Boot Environment (KBE) to access the KBE Main Menu to deploy the operating system manually.

Before you boot the target device in to the KBE, you can change the duration that the Boot Manager is active on the target device to prevent the boot sequence from interruption, such as a user changing the boot sequence option to boot from the local drive. See Set the Boot Manager timeout.

1. Boot the target device in to the KBE.
   - **For local devices, go to the BIOS on the target device and select Network Controller to network boot the target device in to the KBE.**
   - **For remote devices, initiate a remote desktop connection or open VNC-Java Remote Control session on the device to network boot the target device in to the KBE.**
2. Select the interface for the Boot Manager (the black screen), based on whether the device Network Interface Card (NIC) supports integrated graphics.
   - **Graphical Menu: Supports selecting options using arrow keys.**
   - **Text Menu: Supports older NICs that do not support integrated graphics, but allows using arrow keys.**
   - **Basic Menu: Supports NICs that do not have integrated graphic support and cannot recognize arrow keys.**
3. Select the architecture for the KBE that supports the devices's hardware.

   The device boots in to the K000 Boot Environment, and the KBE Main Menu appears.

Deploy the image manually

You can perform scripted installation or system image deployments manually from the KBE Main Menu.

Network boot the device in to the KBE to launch the KBE Main Menu. After the device boots, you can access the device remotely using a VNC-Java Remote Control session. See Access remote devices using a VNC session.

NOTE: Depending on the bandwidth of your network, the number of tasks, and the size of the images you are deploying, manual deployments might take several minutes to a few hours to complete.

1. From the KBE Main Menu, click the deployment type, for example **Imaging**.
2. Click **Deploy image to this device**.
3. In *Image Name*, click the name of the image you want to install on this machine.

   Only system images relevant to the architecture of the selected KBE appear in the list.
   - If you are using the KACE Systems Deployment Appliance to deploy system images, the list that appears shows the relevant images captured by the KACE Systems Deployment Appliance.
   - If you are using an RSA (Remote Site Appliance) to deploy system images, the list that appears shows only those images captured by the RSA, together with any images synced from the associated KACE Systems Deployment Appliance.
4. Ensure the **Restart Automatically after deployment** check box is selected to reboot the device after the image is applied.

   Optional. You can enable this option by default on the *General Settings* page:

   a. Open the Administrator Console.

b. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **General Settings** to display the *General Settings* page.
c. Under *Imaging Options*, select the *Default setting to automatically reboot after manual deployment* check box. Select this check box if you want the target system to reboot automatically after a manual deployment.
d. Click **Save**, and return to the KBE Main Menu.

5. Click **Start deploy**.

   A progress bar appears at the bottom of the page, indicating how much progress has been made through the task.

   The VNC-Java Remote Control session remains open while the tasks performed in KBE are run. From the session, you can view the progress of the pre-installation and image installation tasks, as well as any post-installation tasks that are performed in the KBE by re-establishing a connection.

   If one or more of deployment tasks fail, the *Task Error* page appears, displaying the failure details. Depending on the nature of the issue, you can retry or resume the execution of the failed task, or cancel the deployment. Alternatively, you can re-start or shut down the device, if required. A message box appears, indicating the outcome of the selected operation, such as: `Image deployment failed. See log for details.`

   If a deployment fails without the user's interaction, the *Deploy Log* field appears on the Windows Imaging page, containing the log entries. If the deployment is cancelled by the user, the *Deploy Log* also appears, but the field is not populated.

View the manual deployments in progress

You can view the list of manual deployments that are in progress and the details for a selected boot action for the deployment to verify which image was deployed to which device.

1. On the left navigation pane, click **Progress**, then click **Manual Deployments** to display the *Manual Deployment Progress* page.
2. Under *Name*, select the boot action for the deployment to display the *Deployment Details* page.
3. In the *Devices* menu bar, click **Details** next to the device MAC address to view the progress of the tasks that are running for the deployment.

View the completed manual deployments

You can view the list of completed manual deployments and the details for a selected boot action to verify which image was deployed to which device.

1. On the left navigation pane, click **Audit Log** to expand the section, then click **Manual Deployments** to display the *Manual Deployment Log* page.
2. Under *Name*, select the boot action for the deployment to display the *Deployment Details* page.
3. In the *Devices* menu bar, click **Details** next to the device MAC address to view the success or failure of the tasks there were run for the deployment.

Managing custom deployments

You can use custom Windows deployments to capture and run a collection of specific tasks that you want to apply to a user's system, instead of deploying a brand-new image to the system which requires deleting the contents of the target device.

For example, you can use a custom deployment template to bring in a user's system just to capture their profile using USMT (User State Migration Tool), and to migrate it to another system, before shutting down the original system. Another example for using custom deployments is to simply upgrade a system's OS, without applying a new image.

Create or modify a custom deployment

You can create or modify a custom Windows deployment to carry out one or more specific tasks on the target device.

1. On the left navigation pane, click **Deployments**, then click **Custom Deployments** to display the *Custom Deployments* page.
2. Complete one of the following steps:
   - **On the *Custom Deployments* page, click a custom deployment name to display the *Custom Deployment Detail* page for the selected item.**
   - **On the *Custom Deployments* page, click Choose Action > New to create a new custom deployment.**
3. On the *Custom Deployment Detail* page, in the *Custom Deployment Name* field, type the name that you want to assign to this custom deployment.
4. Click **Architecture** and select the target system architecture, as required.
5. **Optional**. In the *Notes* field, type some additional information about this custom deployment.
6. **Optional: Configuration files only**.
   a. Next to *Config XML*, click **Show**, and review the file contents that appear. The contents of the file are read only.
   b. To download the file, under the file contents, click **Download XML File**.
7. **Optional: Task files only**.

   NOTE: Read-only users do not have access to this field.

   a. Next to *Task XML*, click **Show**, and review the file contents that appear. The contents of the file are read only.
   b. To download the file, under the file contents, click **Download XML File**.
8. Click **Task Error Handling** and indicate how you want to handle errors that are encountered during task execution. You can either *Continue on Errors* or *Prompt on errors*, as required. For more information, see Set task error handling option.
9. Under *Deploy Options*, select any of following options, as required:
   - **Force continue on errors**: Select this option if you want to continue the capture and the upload process even if warnings and fatal errors occur.
   - **Shutdown target device after last task**: Select if you want to turn off the target device when the image is installed.
   - **Hide Deployment from KBE**: Select this option if you want to hide the custom deployment from the KACE Boot Environment (KBE).

NOTE: Custom deployments marked as hidden from KBE do not appear in the *Deployment* drop-down list on the *Automated Deployment Detail* page when creating a boot action.

10. Assign tasks to the custom deployment, as required. For more information, see Assign tasks to custom deployment.
11. When you finish your edits, click **Cancel** to roll back the changes, or **Save** to apply the changes to the image.

Managing offline deployments

KACE Systems Deployment Appliance allows you to create an offline deployment downloadable as an ISO that can be installed directly to a USB drive. WIM files are split into 3.5 Gb file so that they can be placed on a FAT32 system for UEFI deployments.

The *Offline Deployments* list page shows all offline deployments that exist on the appliance. From here, you can create a new offline deployment.

Create an offline deployment

You can create an ISO file for an offline Windows deployment and add desired elements, such as a specific system image, boot environment, system drivers, user states, and license seats.

1. On the left navigation pane, click **Deployments**, then click **Offline Deployments** to display the *Offline Deployments* list page.
2. On the *Offline Deployments* list page, click **Choose Action** > **New** to create a new offline deployment.
3. In the *Create an Offline Deployment* wizard that appears, on the *Select System Image* page, complete the following steps:
    a. Provide the following information:

Option	Description
Name	The name of the offline deployment. This is also the name of the downloadable ISO file that becomes available for download when you finish creating this offline deployment.
License Seats	The number of managed devices assigned to this deployment. Your KACE Systems Deployment Appliance license defines the number of seats that you can manage. Any seats you assign to this deployment affect the remaining number of devices. You can review the *License Usage/Capacity* in the *About Appliance* dialog box. To access it, open the *About* tab on the *Need Help* panel. For more information about this panel, see Access product documentation.
System Image	The system image associated with this deployment. You can use any system image available on the appliance. For more information about capturing system images, see Capturing images.

    b. Click **Next**.
4. On the *Select Boot Environment* page, complete the following steps:
    a. Select the boot environment that you want this deployment to use. The items that appear available for selection are based on the previously selected system image.

    If the *Deploy User State* post-installation task is assigned to the selected image, the *Select User States* step in the wizard is displayed, allowing you to include one or more of the previously captured user states in the offline deployment.

    b. Click **Next**.
5. **Select User States step only**. Specify one or more user states that you want to include in this deployment.
    a. Click **User states scanned with** to filter captured user states by version.

b. In the *Available User States section*, click the plus icon on the left of each user state that you want to add to the deployment.

Similarly, to remove a user from the deployment, in the *Selected User States* section, click the minus icon on the left of each user state that you want to remove.

c. Click **Next**.

6. **Optional**. On the *Select Drivers (Optional)* page that appears, specify one or more user drivers that you want to include in this deployment.
   a. By default, this page lists all drivers downloaded from the driver feed. If you want to display only the drivers associated with a specific OS version, click **Operating System**, then select the OS version, and click **Apply Filters**.
   b. In the *Available Drivers*, click the plus icon on the left of each driver that you want to add to the deployment.

   Similarly, to remove a driver from the deployment, in the *Selected Drivers* section, click the minus icon on the left of each user state that you want to remove.

   c. Click **Next**.
7. On the *Offline Deployment Overview* page, review the elements included in the offline deployment. If you want to make any modifications, use the **Previous** button to return to the desired step in the wizard.
8. Click **Create ISO**.

   The *Create an Offline Deployment* wizard closes, and the *Offline Deployment* list page refreshes, showing information about a newly created ISO file.

When you finish creating an ISO image for this offline deployment, the appliance updates the device inventory with the devices to which this offline deployment is applied. You can review them on the *Device Inventory* page. Each of these devices uses *KACE Offline Node* as the device model. For more information about the device inventory, see Managing device inventory.

About the Remote Site Appliance

The Remote Site Appliance (RSA) acts as a local boot server, which enables you to network boot devices for deployments to remote sites. You can synchronize and upload images to the RSA, and capture system images or user states from the RSA.

You can install the RSA directly from your KACE Systems Deployment Appliance and link the RSA using the license key that comes with your KACE Systems Deployment Appliance. When you link the RSA to the KACE Systems Deployment Appliance, the RSA is available from the appliance Administrator Console. There is no limit to the number of RSAs that you can install using the license key.

The *Remote Sites* tab in the KACE Systems Deployment Appliance Administrator Console enables you to synchronize the appliance to the RSA to access the components that you plan to deploy to the remote sites. For example, you can synchronize boot environments, tasks, drivers, and captured user profiles.

Remote Site Appliance setup requirements

The RSA requires a free IP address to assign to the RSA and VMware® or Hyper-V® host software, such as VMware ESXi™, VMware vSphere®, or Microsoft® Windows® Hyper-V. The RSA configurable DHCP server scope enables devices to network boot to the RSA. Devices that cannot network boot require a bootable ISO file or a USB KACE Boot Environment (KBE). The boot DVD requires setting option 066 or 244 to recognize the appliance.

RSA setup requirements

Table 4. RSA setup requirements

Requirement	Description
KACE Systems Deployment Appliance	Install and configure the appliance to download the RSA.
RSA License	Use the same appliance license key sent to you by Quest KACE.
Virtual Machine host	See the RSA host system requirements.
Network settings	Assign a static IP address and (optional) host name to the RSA. Save the RSA data on the RSA or to a virtual disk.
Optional: LDAP	Use the LDAP server IP address or host name.
Network boot configuration	For Windows devices: The DHCP server scope that directs the network boots to the RSA on the remote DHCP scopes. For Mac devices: The NetBoot server that directs Mac BSCP requests from the remote devices to the RSA.

RSA host system requirements

The device at the remote site that hosts the RSA must meet recommended requirements. For details, see the *Technical Specifications for Virtual Appliances*.

Install the RSA on a host device

You can install the RSA on the host device where you installed the virtual host software as long as no other RSAs exist on the same subnet.

Download the RSA installation package from the Support Portal to the device at the remote site that is going to host the RSA.

For complete information on how to install the RSA on a VMware®, Microsoft® Windows® Hyper-V®, or Nutanix host, see the appropriate setup guide. You can also consult the VMware, Windows, or Nutanix documentation for instructions on opening an appliance file in other host software.

Configure the RSA network settings from the console.

Configure the RSA network settings

You can open a browser to access the initial configuration console to configure the RSA with an IP address and host name.

By default, SSH is enabled on the RSA and you cannot disable it.

1. In the VMware host software, power on the RSA to boot the RSA (rebooting takes 5 to 10 minutes), then proceed with the initial network configuration.
2. At the login prompt, enter `konfig` for both the *Login* and *Password*.
3. Use the up -and down- arrow keys to move between the fields to configure the network settings.
4. Press the down-arrow key until **Save** is selected, then press **Enter**.

   The RSA reboots. Configure the network settings.
5. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Network Settings** to display the *Network Settings* page.
6. Select the **Enable On-Board DHCP Server** check box.

   The on-board DHCP server assigns a specific range of IP addresses to your networked devices and automatically sets up re-direction for Windows device boots to the appliance.

Go to **Settings** > **User Authentication** to set up LDAP authentication on the RSA. The RSA and the appliance manage users separately, so it is possible to grant access to a user on the appliance and not to a user on the RSA.

Link the KACE Systems Deployment Appliance to an RSA

Linking the appliance to the Remote Site Appliance (RSA) enables the KACE Systems Deployment Appliance to be aware of the RSA. Linking enables you to access the RSA and the KACE Systems Deployment Appliance from the same session if the user name and password on the linked appliances match.

In most cases you can link an RSA with the KACE Systems Deployment Appliance at installation time. However, if you clear the configuration on an RSA, making it unaware of the KACE Systems Deployment Appliance, use this procedure to link it to the RSA.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **KACE Linking** to display the *KACE Linking* page.
2. Click **Enable KACE Linking** to display the connection settings.
3. In *Host Name*, enter a unique, logical name for this appliance. This name appears in the drop-down list in the top-right corner of the page next to the login information when appliances are linked.
4. In *Remote Login Expiration* enter the number of minutes to keep the link open. When the time period expires, provide login credentials when switching to a linked appliance. The default is 120 minutes.
5. In *Request Timeout*, enter the number of seconds the appliance waits for a remote appliance to respond to a linking request. The default is 10 seconds.
6. Click **Save** to display the *KACE Linking Key Fingerprint* and the *KACE Linking Key (this server)* fields.
7. Copy the text in the *Name* field and the text in the *Key* field and paste it in a central location, such as a Notepad file.

   The text that you paste in Notepad is the text that you copy and paste in the *Names* and *Keys* from one appliance to the other linked appliances.
8. Repeat the preceding steps on each RSA that you want to link.

   You can also link multiple KACE Systems Deployment Appliances. For more information, see Enable appliance linking.

Add the RSA to the *Remote Sites* tab to configure the components that you want to synchronize to the RSA.

Set default KBE for the RSA

You can set a default KACE Boot Environment (KBE) for the Remote Site Appliance (RSA).

When you select a default KBE for the RSA, this is indicated on the *Remote Site Detail* page, under *Boot Environments*. For more information about this page, see the associated help page.

NOTE: You can also set the default KBE for the linked appliance. For more information, see Set new KBE as default for the appliance.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Remote Site Settings** to display the *Remote Site Settings* page.
2. Under *Default RSA Boot Environments*, select the default KBE for each OS architecture, as required.
3. Click **Save**.

Review RSA settings

You can add the RSA to the KACE Systems Deployment Appliance Administrator Console to enable you to synchronize the components to deploy at the remote site. The RSA extends only one KACE Systems Deployment Appliance; however, there is no limit to the number of RSAs that you can add to the KACE Systems Deployment Appliance.

You can synchronize scripted installations, system images, boot environments, and user states to the RSA.

When you synchronize a linked RSA with the KACE Systems Deployment Appliance, any user states on the appliance also appear on the *User States* list page in the KACE Remote Appliance Administrator Console. When you review individual user state contents, the ability to edit applicable fields and log contents are only available for those user states that are captured locally, but not for any of the user states captured on a linked appliance. Any user states captured on an RSA can be exported.

Pre-installation and post-installation tasks that deployments use are considered dependencies, and are automatically pushed to the RSA.

NOTE: RSA synchronization is not available during an off-board storage migration.

1. On the left navigation pane, click **Deployments**, then click **Remote Sites** to display the *Remote Site Appliances* page.
2. On the *Remote Site Appliances* page, click the *Host Name* column of the RSA whose settings you want to review.
3. On the *Remote Site Detail* page, scroll down to *Boot Environments*. Synchronize the boot environment to network boot the remote devices to the RSA, and to test the RSA configuration. Then select the other components that you want to synchronize to the RSA.

   Any check boxes that appear disabled in this section represent the components that can not be added or removed. For example, if you can not remove a specific boot environment because the check box representing it is disabled, that is because the synced image requires it by default.
4. Review the options listed under *Scripted Installations*, *System Images*, and *User States*, and ensure that only those components that you want to deploy are selected.
   - When you view this page in the KACE Systems Deployment Appliance Administrator Console, any system images already captured by the RSA, and not the KACE Systems Deployment Appliance, are listed under *System Images*, however these options appear disabled. That is because these images already exist on that RSA and cannot be removed by simply clearing these options synchronizing it with the KACE Systems Deployment Appliance.
   - Any images that are captured by the associated KACE Systems Deployment Appliance appear in the list and can be selected or cleared, as required.
5. Scroll down to *Dependencies*. Review the options listed here, to ensure that only those components that you want to deploy are selected.

   For example, the *USMT Toolkit* option in this section appears disabled. The USMT Toolkit allows you to capture user states. When you synchronize the RSA with the KACE Systems Deployment Appliance, and the USMT Toolkit is already uploaded to the KACE Systems Deployment Appliance, the USMT Toolkit is added to the RSA, allowing it to capture user states. You cannot clear this option. For information on how to upload the USMT Toolkit to the KACE Systems Deployment Appliance, see Upload USMT software from Media Manager.
6. Verify if the RSA version matches the KACE Systems Deployment Appliance version, and upgrade it, if needed:
   a. Observe the details appearing under *Upgrade Remote Site*:
      - *Upgrade Status*: Indicates if the RSA is up to date.
      - *Current Version*: Displays the current RSA version.
      - *Last Check*: Shows the date and time the RSA version was checked.
      - *License Synced:* Indicates if the RSA license matches the license specified on the associated KACE Systems Deployment Appliance.
   b. To check the RSA version, click **Check Remote Site Version**.
   c. To upgrade the RSA to the latest version, click **Upgrade Remote Site**.

   Tip: **TIP:** You can also upgrade one or more RSAs from the Remote Site Appliances page by selecting one or more appliances in the list and selecting **Choose Action** > **Upgrade**.

   d. To synchronize the linked KACE Systems Deployment Appliance license with the RSA (if applicable), click **Sync License**.

Tip: **TIP:** You can also synchronize the license on the Remote Site Appliances page by selecting one or more appliances in the list and selecting **Choose Action** > **Sync License**. Similarly, to synchronize the data on one or more RSAs with the data on the associated KACE Systems Deployment Appliance, select **Choose Action** > **Sync Data**.

7. If you made any changes to the settings on this page, click **Save and Sync**.

   Save and Sync is disabled if:

   - An off-board storage migration is in progress.
   - If the RSA and linked KACE Systems Deployment Appliance do not have a matching license. To enable it, under *Upgrade Remote Site*, click **Sync License**. When the license is successfully synchronized, click **Save and Sync**. You can also synchronize the licenses of multiple RSAs on the *Remote Site Appliances* list page. To do that, select them in the list and click **Choose Action** > **Sync License**.
   - If the RSA is not on the same version as the linked KACE Systems Deployment Appliance. To update it, click **Upgrade Remote Site**. When the RSA is successfully upgraded, click **Save and Sync**. You can also upgrade multiple RSAs on the Remote Site Appliances list page. To do that, select them in the list and click **Choose Action** > **Upgrade**.

   The RSA is locked until the synchronization completes.

Next steps

You can use the newly added RSA to capture or deploy system images, scan user states and create USMT templates, create boot actions, or to import or export packages containing system images.

For complete information, see the following topics:

- Capture system images
-
- Assign tasks to system deployment
- Deploy the image manually
- Scan user states
- Create USMT Scan Template
- Importing and exporting appliance components

Tip: **TIP:** You can also use Boot Actions assigned to a specific RSA. For more information, see Create a boot action.

Importing and exporting appliance components

You can import and export KACE Systems Deployment Appliance or Remote Site Appliance (RSA) components, such as drivers, network inventory, boot environments, and tasks to a different network location, a different appliance, or an RSA, using packaging.

IMPORTANT: Only system images can be imported and exported from an RSA. Any tasks included with system images imported or exported from the RSA will be removed.

When importing and exporting components, the appliance picks up packages from the appliance `restore` share directory. When you create a package, the `.pkg` file contains the `index.xml` file with the package metadata and the package files are saved in the `\\`**appliance_host_name**`\restore` share directory.

Packages can be large because they contain full disk images or entire operating systems. Keep the package files together when storing and copying them from the appliance to other network locations.

Schedule the export of components

You can set up a schedule to export components from an appliance, or a Remote Site Appliance (RSA) at regular intervals if you created a package for the components and stored the package in the appliance or RSA `restore` directory.

You can export the database, but only the Quest KACE Technical Support team can re-import the database back to the appliance.

IMPORTANT: Only system images can be exported from an RSA. Any tasks included with system images exported from the RSA will be removed.

1. On the left navigation pane, click **Settings** to expand the section, then click **Package Management** to display the *Package Management* page.
2. Click **Export SDA Packages** to display the *Export List* page.
3. Select the components you want to export at a regular interval.
4. Select **Choose Action** > **Schedule Export for Selected** to display the *Schedule Export* page.
5. Select the date and time to schedule the export.
6. Click **Save**.

The job appears in the queue on the *Package Management Queue* page and runs at the specified time.

NOTE: Removing a job from the queue also removes the job from the schedule on the *Export List* page.

Use Off-Board Package Transfer

You can use the *Off-Board Package Transfer* feature to automatically transfer packages that have been exported to the appliance or the Remote Site Appliance (RSA) `restore` directory to a remote FTP/SFTP server or Samba file share. You can specify a directory for the transfer, and the transfer process creates the directory on the remote server, copies all `.xml`

and `.pkg` files to that location using the `/<Path>/data_<timestamp>` naming convention. You can also delete the transferred files from the `restore` directory.

NOTE: Packages cannot be imported while an off-board package transfer is in progress.

1. On the left navigation pane, click **Settings** to expand the section, then click **Package Management** to display the *Package Management* page.
2. Click **Off-Board Package Transfer** to display the *Off-Board Package Transfer* page.
3. Click **Enable Offboard Package Transfer** to set the transfer details.

Option	Action
Schedule Run	Select the interval and time for the transfer.
Offboard Package Transfer Protocol	Select which file transfer protocol to use to place the files on the remote site. When using the SFTP protocol, password-based authentication must be enabled explicitly on the file server.
Offboard Package Transfer Server	Type the host name or IP address of the device to which the files are transferred.
Path or Share Name	Type the path to the directory or share name for the transfer. Enter the Samba share name without any forward or backward slashes.
User Name	Type the user name for the appliance to use. Entering the user name requires write-access to the remote location.
User Password	Type the password required to access the remote location.
Cleanup Restore	Delete the files automatically from the `restore` share directory on the appliance or an RSA after a successful transfer.

4. Click **Save**.

The job appears in the queue on the *Package Management Queue* page and runs at the specified time.

NOTE: Removing a job from the queue also removes the job from the schedule on the *Export* page.

On the left navigation pane, click **Settings**, then click **Appliance Logs** to expand the section, then click **Scheduled Action Server**, and select **Output Log** to view the results of the transfer.

Upload packages for import

You can upload packages stored on an external device or server to the KACE Systems Deployment Appliance or Remote Site Appliance (RSA) `restore` directory, then import the packages to the appliance.

To import packages larger than 1.5GB, place them in the `\\[appliance|RSA]_host_name\restore` share directory first.

1. On the left navigation pane, click **Settings** to expand the section, then click **Package Management** to display the *Package Management* page.
2. Complete one of the following steps:
   - **On the *Package Management* page, click Upload Packages.**
   - **On the *Package Management* page, click Import KACE SDA Packages On the *Import List* page that appears, select Choose Action > Upload Package for Import.**
3. On the *Import Package* page, click **Select file** to specify the `.pkg` file to import, or simply drop the file into the indicated area.
4. Click **Import Package**.

The appliance adds a copy of the components to the library.

If the package contains drivers, re-cache the drivers. On the left navigation pane, click **Library > Drivers**, then select **Choose Action** > **Recache Drivers** to display the *Managing Drivers* page.

Import appliance components

You can import components stored in a different location, a different appliance directly, or to a Remote Site Appliance (RSA), if the package containing the components is smaller than 1.5GB.

If you exported the database, only the Quest KACE Technical Support team can re-import the database back to the appliance.

IMPORTANT: Only system images can be imported to an RSA. Any tasks included with system images imported to the RSA will be removed.

1. On the left navigation pane, click **Settings** to expand the section, then click **Package Management** to display the *Package Management* page.
2. Click **Import SDA Packages** to display the *Import List* page.
3. Select the check box next to the package you want to import.
4. Select **Choose Action** > **Import Selected**.

   The import process starts. Be sure to allow any import operation to complete before altering any package or database configuration.

   NOTE: Depending on the size and number of components in the package, the import process can take several minutes to several hours. Importing images takes longer than exporting images. When you export an image, the appliance locates and packages all of the files associated with that image in to one `.pkg` file. When the process is reversed, the image files are checked against the appliance image store to ensure that only new files are uploaded.

The new components appear on the *Package Management* > *Import List* page.

Package components to export

You can export the components stored on the appliance, such as drivers, network inventory, boot environments, and tasks to a different network location. You can also export system images and user states from a Remote Site Appliance (RSA). This is useful to back up and restore components.

IMPORTANT: Only system images and user states can be exported from an RSA. Any tasks included with system images exported from the RSA will be removed.

You can export the database, but you cannot re-import the database. Exporting components from the appliance is an internal task and cannot run in tandem with other internal tasks, such as re-caching drivers, creating scripted installations, or rebuilding boot environments.

1. On the left navigation pane, click **Settings** to expand the section, then click **Package Management** to display the *Package Management* page.
2. Click **Export SDA Packages** to display the *Export List* page.
3. Select only a few components at a time; otherwise, the export cannot complete.

   If the package is green, you cannot export it until you change the version number of the package, re-cache the drivers, and save any changes made to the package.

   The selected export items are compressed and placed in the `\[appliance|RSA]_hostname\restore` share directory. A `.pkg` file is created for each component that you select.

   NOTE: While the export is processing, changing any Network, Security, or Date and Time settings causes the appliance to reboot, stop the export process, and lock the Exports feature.
4. Select **Choose Action** > **Export Selected**.

   Ensure that export completes before selecting a different export.

The packaging process starts. Exporting packages might take a few minutes to several hours to complete depending on the size of the file. The *Status* column indicates when each export completes.

NOTE: If the status column shows *Completed* or *Exporting* next to each component, but the *Currently* : status in the upper-right corner displays *Idle*, contact the Quest KACE Technical Support to access your appliance through the tether and clear the error.

The size of the exported package is smaller than the one on the appliance, and can vary in size due to file export compression and package attachments.

Package file names

You can import and export KACE Systems Deployment Appliance or Remote Site Appliance (RSA) components to packages. The following syntax conventions apply to package file names. Follow these guidelines when you import or export appliance packages to quickly find a particular component.

File contents	File name
Pre-installation task	Syntax: PR<ID><Unix_time_stamp>_<microseconds> Example: PR33_1519839187_5248.pkg
Mid-level installation task	Syntax: MI<ID><Unix_time_stamp>_<microseconds> Example: MI26_1519792380_3567.pkg
Post-installation task	Syntax: PO<ID><Unix_time_stamp>_<microseconds> Example: PO17_1519831620_4922.pkg
Database package	Syntax: DB<ID><Unix_time_stamp>_<microseconds> Example: DB12_1519822800_1546.pkg
KImage	Syntax: KI<ID><Unix_time_stamp>_<microseconds> Example: KI56_1519827865_4213.pkg
Scripted installation	Syntax: SI<ID><Unix_time_stamp>_<microseconds>

File contents	File name
	Example: SI59_1519834064_2984.pkg
Driver package	Syntax: DR<ID><Unix_time_stamp>_<microseconds> Example: DR15_1519823348_3284.pkg
Network inventory package	Syntax: NI<ID><Unix_time_stamp>_<microseconds> Example: NI36_1519814733_1976.pkg
Custom deployment	Syntax: CU<ID><Unix_time_stamp>_<microseconds> Example: CU88_1519794461_5889.pkg
Boot environment	Syntax: BE<ID><Unix_time_stamp>_<microseconds> Example: BE52_1519798711_2802.pkg
Network scan	Syntax: NS<ID><Unix_time_stamp>_<microseconds> Example: NS37_1519818962_3011.pkg
User State	Syntax: US<ID><Unix_time_stamp>_<microseconds> Example: US27_1519805822_2846.pkg
Task Group	Syntax: TG<ID><Unix_time_stamp>_<microseconds> Example: TG16_1519811097_1390.pkg
USMT (User State Migration Tool) Scan template	Syntax: ST<ID><Unix_time_stamp>_<microseconds> Example: ST39_1519808167_5225.pkg

Managing disk space

You can view the *Disk Usage* pie chart on the appliance *Dashboard* to verify how much storage space is available on your appliance. You can migrate data on the appliance to an offboard-storage device, and migrate data stored on the virtual appliance or Remote Site Appliance (RSA) to an additional virtual disk to free up space. You can also delete unused images, boot environments, source media, and tasks.

Verify available disk space

For optimal performance, the appliance requires approximately 20 percent free disk space. You can verify the available disk space from the *Disk Usage* pie chart on the *Dashboard*.

1. Log in to the KACE Systems Deployment Appliance Administrator Console.
2. On the left navigation pane, choose **Home** > **Dashboard**.

   The *Disk Usage* pie chart displays a view of the storage information, which is updated every 10 minutes and every 60 minutes when storage is offboard.
3. Mouse over any section in the *Disk Usage* pie chart to view the percentage of available disk space for a component.

Delete images not associated with devices

You can delete system images that are not associated with a licensed device that has booted from the appliance, and images that have been replaced after a capture.

Consider backing up your system images before removing unused system image files. See Schedule the export of components.

1. On the left navigation pane, click **Settings** to expand the section, then click **Appliance Maintenance** to display the *Appliance Maintenance* page.

   NOTE: You can only update the appliance if your license is up to date. When your license expires, a message appears at the top of the page, instructing you to update your license. The *License Maintenance Status* field on this page indicates the state of your license. To update your license, obtain a new key from your KACE sales representative, and update it on the *Registration and Licensing* page. If one or more Remote Site Appliances (RSAs) are associated with this appliance, the new license key is automatically updated on those RSAs after a synchronization.
2. Under *Utilities* > *Delete unused system image files*, click **Delete**.

   The appliance deletes all unused system image files from the file server.

The items are permanently removed from the appliance, and the available disk space displays on the *Dashboard*.

Delete images associated with devices

You can delete system images that become obsolete, large, or out-of-date to free up disk space.

1. On the left navigation pane, click **Deployments**, then click **System Images** to display the *Systems Images* page.
2. Select the items that you want to remove.
3. Select **Choose Action** > **Delete**.

The items are permanently removed from the appliance, and the available disk space displays on the *Dashboard*.

Delete unassigned scripted installations

Delete scripted installations when an operating system type becomes obsolete or is otherwise unused in your environment.

1. On the left navigation pane, click **Deployments**, then click **Scripted Installations** to display the *Scripted Installations* page.
2. Select the items that you want to remove.
3. Select **Choose Action** > **Delete**.

The items are permanently removed from the appliance, and the remaining disk space displays on the *Dashboard* page.

Delete unassigned boot environments

When building a new KACE Boot Environment (KBE) or NetBoot environment, the previous boot environments remain on the appliance. You can delete cumulative boot environments.

1. On the left navigation pane, click **Deployments**, then click **Boot Environments** to display the *Boot Environments* page.
2. Select the items that you want to remove.
3. Select **Choose Action** > **Delete**.

   The boot environments are removed from the *Boot Environments* page, but remain in the appliance database. You can permanently delete boot environments from the *Source Media* page.

Delete source media

You can delete source media on the appliance that you are no longer using to free up disk space. You cannot delete a source media that is attached to a boot environment.

1. On the left navigation pane, click **Library** to expand the section, then click **Source Media** to display the *Source Media* page.
2. Select the check box next to the source media you want to delete.
3. Select **Choose Action** > **Delete**.

The items are permanently removed from the appliance, and the available disk space displays on the *Dashboard*.

Delete unassigned pre-installation tasks

You can delete unused pre-installation tasks to free up disk space.

1. On the left navigation pane, click **Library** to expand the section, then click **Pre-installation Tasks** to display the *Pre-installation Tasks* page.
2. Select the items that you want to remove.
3. Select **Choose Action** > **Delete**.

The items are permanently removed from the appliance, and the available disk space displays on the *Dashboard*.

Delete unassigned post-installation tasks

You can delete unused post-installation tasks to free up disk space.

1. On the left navigation pane, click **Library** to expand the section, then click **Post-installation Tasks** to display the *Post-installation Tasks* page.
2. Select the items that you want to remove.
3. Select **Choose Action** > **Delete**.

The items are permanently removed from the appliance, and the available disk space displays on the *Dashboard*.

Enabling offboard storage

You can move the data stored on the physical appliance to an external Network Attached Storage (NAS) device to free up disk space on the appliance. You can also move the data stored on a virtual appliance or a Remote Site Appliance (RSA) to an additional virtual disk.

Enabling offboard storage copies all the data from the internal drive, such as images, pre-installation and post-installation tasks, user profiles, source media, boot environments, and drivers to the offboard storage device. Although the data remains on the appliance, deployment activity points to the offboard storage device.

You can migrate data stored on an offboard storage device back to the appliance or RSA if the data does not exceed the onboard storage capacity.

Add a virtual disk for offboard storage

You can add a virtual disk to migrate data stored on a virtual KACE Systems Deployment Appliance or on a Remote Site Appliance (RSA) to an additional virtual disk to free up disk space.

Power off the appliance, add the virtual disk, and then power on the appliance.

Configuring a virtual disk for your KACE Systems Deployment Appliance or RSA requires the following:

- Ensuring that the virtual disk capacity is at least 250GB. You cannot use a virtual disk with less storage capacity than the KACE Systems Deployment Appliance or RSA onboard storage. For example, if you have 250GB of onboard data, the virtual disk must have more than 250GB of available storage.
- Planning for your data migration because it can take several hours depending on the amount of data and the network speed. The KACE Systems Deployment Appliance or RSA is unavailable during migration.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Data Storage** to display the *Data Storage* page.
2. Click **Change to offboard storage** to display the *Data Storage Configuration*.

   - If the virtual disk is not added or connected properly, you cannot perform the data migration.
   - If there is more than one virtual disk connected, remove the additional virtual disks so that there is only one virtual disk connected. Restart the procedure to return to the *Data Storage Configuration* page.

3. Click **Verify device**.

   The KACE Systems Deployment Appliance starts checking whether it can be reached and configured. *Show Details* displays the status of the verification.
4. Click **Migrate** to copy the data to offboard storage.

   The progress bar displays the status.
5. After the migration completes, click **Close**.
6. Verify that the storage type is changed.

If you encounter any errors, click **Settings** to expand the section, then click **Appliance Logs** to display the *Appliance Logs* page, and select *Data Storage Configuration* logs.

Revert offboard data to onboard storage

You can migrate data stored on an offboard storage device back to the appliance or RSA as long as the data does not exceed the onboard storage capacity. The appliance verifies whether it has enough space for the data. If the data on the device exceeds the available space on the appliance, the offboard data is not migrated.

For information on the appliance data storage capacity, go to http://documents.quest.com/kace-systems-deployment-appliance/technical-specifications-for-virtual-appliances/.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Data Storage** to display the *Data Storage* page.
2. Click **Change to offboard storage** to display the *Data Storage Configuration wizard*.
3. Do one of the following to revert offboard data back to onboard storage:

   - **Added new data to the offboard-storage device:**

     a. Click **Revert to original data that was on the appliance before migrating to offboard storage.** Any new data stored on the offboard-storage device after migrating the onboard data to the offboard storage will be lost.
     b. Click **Next** and select **Yes, revert to onboard storage**.

   - **No new data added data to the offboard-storage device:**

     a. Click **Copy data from offboard storage to the appliance.**
     b. Click **Verify storage space**.

After the appliance verifies whether it has enough space to accept the data from the device, confirm that you want to continue the migration.

c. Click **Migrate**.

- **If you are migrating RSA data to a virtual disk, synchronize the RSA with the appliance before migrating the data to the virtual disk.**

  NOTE: The RSA becomes inaccessible when you reboot the RSA during reverse migration from offboard to onboard storage.

  a. On the left navigation pane, click **Deployments**, and click **Remote Sites** to display the *Remote Site Appliance* page.

  b. Select the RSA, then select **Choose Action > Sync**.

Configure an off-board storage device

You can add an external Network Attached Storage (NAS) device to migrate data stored on a physical appliance to free up disk space on the appliance. When you migrate the data to an offboard storage device, the data stored on the appliance is no longer accessible.

Plan your data migration because it can take several hours depending on the amount of data and the network speed. During migration, the appliance is not accessible.

Go to the http://www.itninja.com/community/dell-kace-k2000-deployment-appliance website for device-specific configuration instructions that are not available from the appliance.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Data Storage** to display the *Data Storage* page.
2. Click **Change to offboard storage** to display the *Data Storage Configuration wizard*.
3. Select the storage device for the appliance.

   Ensure that the device storage capacity is at least 250GB. An offboard-storage device cannot have less storage capacity than the appliance onboard storage. For example, if you have 250GB of onboard data, the offboard-storage device must have more than 250GB of available storage.

4. In *Address*, type the host name or the IP address of the offboard-storage device.

   In *Share Path*, type the full path of the share configured on the offboard-storage device.
5. Configure the device settings, then click **Verify device settings**.

   Read the device instructions and verify that you have properly configured the settings listed for the offboard-storage device. Use a private network and if possible, restrict access by IP address to prevent security vulnerabilities.

   The appliance checks whether the device is reachable and configurable. *Show details* displays the status of the verification.
6. Click **Migrate** to copy the data to offboard storage.

   The progress bar displays the status.
7. After the migration completes, click **Close**.
8. Verify that the storage type is changed.

If you encounter any errors, click **Settings** to expand the section, then click **Appliance Logs** to display the *Appliance Logs* page, and select *Data Storage Configuration* logs.

Best practices for using external storage

Moving to external storage makes all your deployments, image captures, media uploads, and downloads dependent on the stability and speed of the external server and its network connection to the appliance. To that end, there are several recommendations to follow.

The external storage server is a dedicated device

It should not provide shares or other functionality to other machines or devices in order to avoid resource conflicts. The data can only be passed to the appliance (and out of the client machine) as quickly as the storage server can provide it. If the storage server is tied up sending data to other devices it will impact deployment/capture times and could even lead to deployment failure.

The external storage server is connected to the physical appliance by its own private network

The appliance has two network ports, the second network port should be used to connect the external storage server on its own private network isolated from the appliance front-end network. Connecting the storage server over the appliance front-end network effectively cuts your network band width in half, making a 1 GB network a 500 MB network. During capture/deployment the data must come to the appliance from the storage server and then from the appliance to the client. Using the front end network means the data must traverse the front end NIC twice. This will have a drastic performance impact and could lead to failed deployments due to network congestion. Additionally, the storage server and the appliance should be connected on the same physical switch (VLAN/subnet). Any latency of packets caused be traversing multiple switches/routers directly translates to longer or failed deployments and should be avoided.

The external storage server should be enterprise class hardware

Since the appliance deployment speed is dependent on the storage server being able to keep up with the load, any delay caused by a slow storage server will translate into long deployments or failed deployments. Therefore, as an example, if using a network-attached storage (NAS) device, a desktop or SOHO (small office/home office) model would not be appropriate. Likewise the use of a virtual machine as a storage server is discouraged, in testing and in the field we have found no matter how robust the infrastructure, the virtual server, specifically NFS (network file system) is not reliable under heavy load.

The drives on the storage server are high speed high performance drives

Any time the storage server must delay sending data to the appliance, because it is waiting to read the drives, will translate into longer deployments or failed deployments. There are many different drive manufacturers so it is not possible to rate them, all but as an example Western Digital® drives come in four types: Green (echo friendly), Blue (consumer), Red (low-grade raid), and Black (high performance). We would recommend using only the Black high performance drives. If your storage server is using SAN (storage area network) drives ensure they can produce performance equal to or better than the high performance physical drives. It is recommended SAN drives are bench marked tested as some operating systems can not utilize the throughput the SAN is rated for.

Anti-virus software is not installed on your storage server

If you must have an anti virus on your storage server, it must be configured to ignore the appliance share completely. Most anti-virus software solutions use a scan on access which means any file accessed is scanned before being sent out across the network. WIM files are going to be several GB in size, causing the scan to take a very long time, which in turn will cause deployment timeout issues. Also many anti-virus software solutions choose to quarantine uploaded files if they seem to be compromised. This is especially true for driver files which could be catastrophic when they get quarantined, causing deployments to fail with blue screens because the driver needed it no longer part of the image. Further anti-virus and security policies can make or force changes to the file permissions or ownership, causing the appliance to no longer have access to them.

For additional information, visit https://support.quest.com/kace-systems-deployment-appliance/kb/111864. This article provides a list of tested NAS devices, however there are others that provide adequate functionality. KACE does not

publish any specifications for Windows-based storage servers, so it is important if using a Windows machine to ensure it runs on modern enterprise-class hardware.

Troubleshooting appliance issues

You can access the appliance Support Portal to request a Support team tether to your appliance. You can also test the Boot Manager, recover devices, and download log files from the Administrator Console, which can be useful during troubleshooting.

You can also download the appliance Advisor, which is a utility that queries the database of your appliance, to gather information about your appliance in an HTML report to help with gathering data or troubleshooting the appliance. For more information, or to download the appliance Advisor, go to http://www.itninja.com/blog/view/k2-advisor.

Test device connections on the network

You can use the ping program to test network connectivity.

1. On the left navigation pane, click **Support > Support Portal** to display the *KACE Support Portal* panel.
2. Click **Troubleshooting** to display the *Support Troubleshooting Tools* page.
3. From the *Tool* drop-down list, select **ping**.
4. Enter the IP address of the device and click **Test**.

   Results are displayed.
5. **Optional**. Use other programs, as needed. Simply select the program from the drop-down list, and click **Test**.

The following programs are available:

- **nslookup**: A network administration command-line tool available for many computer operating systems for querying the Domain Name System to obtain domain name or IP address mapping or for any other specific DNS record.
- **arp**: The Address Resolution Protocol (arp) is a communication protocol used for discovering the link layer address associated with a given IPv4 address, a critical function in the Internet protocol suite.
- **dig**: A network administration command-line tool for querying Domain Name System servers. dig is useful for network troubleshooting and for educational purposes
- **ifconfig**: A system administration utility in Unix-like operating systems for network interface configuration. The utility is a command line interface tool and is also used in the system startup scripts of many operating systems.
- **iostat**: A computer system monitor tool used to collect and show operating system storage input and output statistics.
- **traceroute**: A computer network diagnostic tool for displaying the route and measuring transit delays of packets across an Internet Protocol network.
- **curl**: cURL is a computer software project providing a library and command-line tool for transferring data using various protocols. The cURL project produces two products, libcurl and cURL.
- **Service Status**: Displays a list of services running on the appliance.
- **showmount**: Displays the shares available on a specific IP address.
- **tcpdump**: A common packet analyzer that runs under the command line. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.
- **netcat**: a computer networking utility for reading from and writing to network connections using TCP or UDP. Netcat is designed to be a dependable back-end that can be used directly or easily driven by other programs and scripts.
- **Display Free Disk Space**: Shows the available disk space on the appliance.
- **database**: Provides database response metrics.
- **netstat**: displays network connections for the Transmission Control Protocol (both incoming and outgoing), routing tables, and a number of network interface (network interface controller or software-defined network interface) and network protocol statistics.
- **smbstatus**: A very simple program that displays the Samba status and lists the current Samba connections.
- **smbversion**: Displays the Samba version.
- **top**: A task manager program found in many Unix-like operating systems. It produces an ordered list of running processes selected by user-specified criteria, and updates it periodically.

Enable a tether to Quest KACE Technical Support

You can access the Quest Support Portal to request a tether to your appliance to enable Quest KACE Technical Support to troubleshoot issues.

Obtain a tethering key by contacting Quest KACE Technical Support at https://support.quest.com/contact-support.

To ensure security, enable remote access to the appliance after the Support team authorizes you to do so.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **Security** to display the *Security Settings* page.
2. Select the *Allow SSH Root Login (KACE Support)* check box.
3. Click **Save**.
4. On the left navigation pane, click **Support > Support Portal** to display the *KACE Support Portal* panel.
5. *Under Contact Quest KACE*, click **Enter a Tether key** to display the *Support Tether Key* page.
6. Observe the alert at the top of the page.

   By enabling a tether, you allow KACE Technical Support to access your appliance. Ensure that this process complies with your organization's security guidelines. By default, a tether expires after 21 days, but you can disable an enabled tether it at any time.
7. In the text field, type the description of the problem, and complete one of the following steps.
   - **To obtain the tether key automatically and send the message to Technical Support, click Enable Tether.**

     If the process fails, select **Enable Tether** and type the tether key, as prompted. Click **Save**.
   - **To use a tether key provided by Technical Support, click I already have a tether key, then select Enable Tether and type the tether key, as prompted. Click Save.**

The *Support Tether Key* page displays the date and time the tether key expires, and the tether log. Quest KACE Technical Support now has remote access to your appliance. To disable the tether at any time, click **Disable Tether**.

Open a support ticket

You can open support tickets from within the appliance and enter the details to troubleshoot appliance-related issues, send bug reports, and to request enhancements.

1. On the left navigation pane, click **Support > Support Portal** to display the *KACE Support Portal* panel.
2. Under *Contact Quest KACE*, click **Submit a Ticket** to display the *New Support Ticket* page.
3. Provide the required information, then click **Send**.

Troubleshooting the Boot Manager

You can change the Boot Manager interface for devices that do not support the integrated graphics required to load the KBE and configure how long the Boot Manager displays on target devices. You can also set the duration that the appliance waits for the DHCP server to respond, and test device network connectivity.

Test whether a target device can network boot

If the Network Interface Card (NIC) on the target device supports network booting, you can test whether a target device can boot from the appliance.

1. Set the BIOS on the target device to boot from the network.
2. Restart the target device.

   The target device searches for the network boot server.
3. From the Boot Manager, select the architecture for the KBE that supports the device's hardware.

   The target device boots from the KBE.

The target device successfully boots.

Set the Boot Manager timeout

When you network boot a device in to the KACE Boot Environment (KBE), you can specify how long the Boot Manager displays on a target device.

Typically, in a test environment where you are setting up and troubleshooting devices, you can increase the timeout. In a production environment; however, decreasing the timeout to a few seconds should discourage users from attempting to interrupt the boot sequence.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **General Settings** to display the *General Settings* page.
2. Under *PXE Options*, in *Boot Manager Timeout*, enter the duration in seconds.

   The default value is 15 seconds. You can increase the timeout up to 15 minutes or 900 seconds; an increased timeout period might cause users to interrupt the boot sequence.
3. Click **Save**.

The Boot Manager timeout for all PXE boots from the appliance is changed.

Select the local hard disk boot method

When you boot a device from the hard drive, you can specify how you want the device to boot.

Both local and chain boot methods are available, but the chain boot method is recommended.

1. On the left navigation pane, click **Settings > Control Panel** to display the *Control Panel*, then click **General Settings** to display the *General Settings* page.
2. Under *PXE Options*, click *Local Hard Disk Boot Method (BIOS)*, and select the boot method for BIOS devices.
   - **Chain Boot**: Select this option if you want to use iPXE to chain-boot the device to its hard drive.
   - **Local Boot**: Select this option if you want to use built-in iPXE commands to do a boot from the hard drive.
3. Also under *PXE Options*, click *Local Hard Disk Boot Method (UEFI)*, and select the boot method for UEFI devices.
   - **Chain Boot**: Select this option if you want to run a UEFI script to load the Windows UEFI boot manager.
   - **Local Boot**: Select this option if you want to use built-in iPXE commands to do a boot from the hard drive.
4. Click **Save**.

Recovering devices

The KBE Main Menu, which loads on target devices after you network boot a device in to the appliance, provides a *Recovery* menu option. You can modify or replace files, and edit the registry to boot unresponsive devices.

Recover corrupted devices

You can restore corrupted devices or devices that cannot boot from its hard drive.

1. From the *KBE Main Menu* on the target device, click **Recovery**.

The recovery tools appears.

2. Click the recovery tool you want to run.

   Closing the registry editing window saves the changes you made.

3. Click **Back to Main Menu** to exit the tool.

Downloading the appliance log files

You can download log files directly from the Administrator Console, which can be useful during troubleshooting.

Download all appliance log files

You can download all of the appliance log files to track and review what is happening on the appliance to help identify any problems that might occur.

1. On the left navigation pane, click **Settings** to expand the section, then click **Appliance Logs** to display the *Appliance Logs* page.
2. Scroll to the bottom of the page and click **Download All Logs** to display the *Appliance Logs* page.
3. Click **OK**.

   The log files are download as a single `.tgz` file.

4. Extract the files to view its contents.

   You can provide access to any log files or screenshots of problems to help Quest KACE Technical Support diagnose and resolve issues.

You can enable a tether to Quest KACE Technical Support so that a Quest KACE representative can connect to your appliance for troubleshooting. See Enable a tether to Quest KACE Technical Support.

View the appliance log files

You can view log files that the appliance creates and maintains automatically.

1. On the left navigation pane, click **Settings** to expand the section, then click **Appliance Logs** to display the *Appliance Logs* page.
2. Click the name of the log file that you want to view.

   The log content displays on the page chronologically. You can view by *Oldest on top* or by *Newest on top*.

Appliance log types and descriptions

You can view a description of the log files for System, Web Server, appliance Server, File Servers, Task Processor, Privileged Action Server, Scheduled Action Server, User State Migration, Import and Export, REST API, and Update .

Table 5. Appliance Logs

Log type	Log name	Description
System	System Messages	Displays system messages from the operating system running the appliance.
	Outgoing Mail Log	Displays logs of email messages sent from the appliance.
	Data Storage Configuration	Displays external storage configurations on the appliance.

Log type	Log name	Description
Web Server	Access Log	Displays the request log file for the Apache™ Web server.
	Error Log	Displays the error log file for the Apache Web server.
SDA Server	Output Log	Displays messages from system updates, cleanup tasks, offboard storage updates, driver feed and documentation updates.
	Error Log	Displays errors from system updates, cleanup tasks, offboard storage updates, driver feed updates and documentation updates.
	Multicast Log	Displays program execution details about multicast imaging jobs.
	Output Log	Displays messages from system updates, cleanup tasks, offboard storage updates, driver feed and documentation updates.
	Output Enhanced Log	Displays enhanced messages, such as errors and related stack trace from system updates, clean up tasks, offboard storage updates, driver feed and documentation updates.
	Error Log	Displays errors from system updates, cleanup tasks, offboard storage updates, driver feed updates and documentation updates.
	Multicast Log	Displays program execution details about multicast imaging jobs.
	Upgrade Log	Displays messages generated during the appliance upgrade
File Servers	TFTP Transfer Log	Displays appliance boot errors and requests.
	NETBIOS Name Server	Displays messages from the NetBIOS server on the appliance.
	Windows File Server	Displays messages from the Samba service, which shares the folders on the appliance.

Log type	Log name	Description
Task Processor	Output Log	Displays messages from the appliance server task processor, which runs tasks in the background. The tasks that can be processed include: • Importing source media that the Media Manager uploads. • Importing a WIM or K-Image. • Rebuilding driver cache. • Rebuilding a KBE environment. • Creating and updating scripted installations. • Synchronizing data with an RSA (Remote Site Appliance).
	Error Log	Displays errors in the tasks that the appliance server task processor performs.
Privileged Action Server	Output Log	Displays output from the privileged action server, which is tasks that require elevated permissions. These tasks include: • Changing any appliance settings such as network, region and locale, date and time, or SSL. • Performing upgrades. • Running the reboot or power-off command. • Migrating to or importing from external storage. • Setting file permissions on imported media. • Synchronizing license key with an RSA.
	Error Log	Displays errors that occur while the privileged action server is running.
Scheduled Action Server	Output Log	Displays messages from the appliance scheduled tasks. These scheduled tasks include: • Check for drive failures. • Update the disk usage chart and external-storage status. • Check for Driver Feed updates from Quest KACE. • Check for server updates. • Rotate the log. • Disk cleanup.
	Error Log	Displays errors in the scheduled task.
User State Migration	Failed Error Log	Displays failures in the online USMT scanning process.
Import and Export	Import Log	Displays output and errors of any import jobs.

Log type	Log name	Description
	Export Log	Displays output and errors of any export jobs.
	Download Logs	Downloads the appliance log files as a single `.tgz` file.
Nightly Updates	Output Log	Displays messages from the nightly updates to the system.
	Error Log	Displays any errors from the nightly updates.
REST API	API Log	Displays output and errors from the REST API.
Appliance Updates	Update Log	Displays output from any appliance updates that have been applied.
FreeBSD Logs	FreeBSD Daily Output Log	Displays the daily run output from FreeBSD.
	FreeBSD Daily Security Output Log	Displays the daily security run output from FreeBSD.
	FreeBSD Weekly Output Log	Displays the weekly run output from FreeBSD.
	FreeBSD Weekly Security Output Log	Displays the weekly security run output from FreeBSD.
	FreeBSD Monthly Output Log	Displays the monthly run output from FreeBSD.
	FreeBSD Monthly Security Output Log	Displays the monthly security run output from FreeBSD.

Shutting down and rebooting the appliance

You might need to shut down or reboot the appliance from time to time when troubleshooting or performing maintenance tasks.

Before shutting down or rebooting the appliance, ensure that none of the following processes are active:

- Package imports or exports
- Source media uploads
- System image uploads or rebuilds
- Scripted installation rebuilds
- Deployments
- RSA syncs
- Driver downloads through Driver Feed
- User state scans

Power off the appliance

You can power off the appliance and restart it if a deployment has stalled, or if there is a problem with the network connection. Powering off the appliance requires pressing the Power button again to turn it on.

Before shutting down the appliance, ensure that no processes are active.

1. On the left navigation pane, click **Settings** to expand the section, then click **Appliance Maintenance** to display the *Appliance Maintenance* page.

   NOTE: You can only update the appliance if your license is up to date. When your license expires, a message appears at the top of the page, instructing you to update your license. The *License Maintenance Status* field on this page indicates the state of your license. To update your license, obtain a new key from your KACE sales representative, and update it on the *Registration and Licensing* page. If one or more Remote Site Appliances (RSAs) are associated with this appliance, the new license key is automatically updated on those RSAs after a synchronization.

2. In *Utilities* > *Power Management*, click **Power Off**.

   The appliance shuts down.

To enable the appliance, press the power switch.

Reboot the appliance

You can reboot the appliance to restart if a deployment has stalled or if there is a problem with the network connection. When you reboot the appliance, it automatically powers on the appliance.

Before rebooting the appliance, ensure that no processes are active.

1. On the left navigation pane, click **Settings** to expand the section, then click **Appliance Maintenance** to display the *Appliance Maintenance* page.

   NOTE: You can only update the appliance if your license is up to date. When your license expires, a message appears at the top of the page, instructing you to update your license. The *License Maintenance Status* field on this page indicates the state of your license. To update your license, obtain a new key from your KACE sales representative, and update it on the *Registration and Licensing* page. If one or more Remote Site Appliances (RSAs) are associated with this appliance, the new license key is automatically updated on those RSAs after a synchronization.

2. In the *Utilities* section, click **Reboot**.
3. After a few minutes, refresh the browser.

   You are returned to the *Login* page.

Best practices for backing up appliance data

To prevent loss of data caused by failed hardware or a failed upgrade, it is important to plan and implement a backup plan. The appliance itself cannot be backed up, but critical data (such as images, tasks, and scripted installs) can and should be backed up on a regular basis.

Backing up the data consists of two tasks:

1. Exporting the data to the `\\<appliance>\restore` share.
2. Copying the data frm the `restore` share to an external storage server.

Both of these tasks can be done manually or as scheduled jobs depending on business needs. Either way is fine, but each method has drawbacks that need to be addressed.

The main problem with running backups manually is remembering to do so on a regular basis. Since both exporting and copying the data to offsite storage can take hours depending on the amount of data at hand, running them manually can be problematic. Scheduled backups also have issues such as ensuring the offsite storage server has enough disk space, scheduling the export and offsite transfer jobs so they do not overlap and prevent the process from responding, and maintaining the ID, password, and address of the offsite storage server.

Setting up a data export

For information about the steps for setting up a data export, visit https://support.quest.com/kace-systems-deployment-appliance/kb/115080.

Any items scheduled to be exported will only be exported if the *Version* and *Version backed up* (displayed on the *Exports* page) are different. The line showing the item is either white or yellow if that is the case. This mechanism prevents multiple copies of the same version from being constantly exported into the restore share. While this does save space on the restore share, and consequently on the remote storage server, it also means the backup files should not be deleted from the storage server out of hand, as the object (an image, scripted Install, or a post-installation task) is not exported again until its version number changes. This means if an object is exported, copied to the offsite storage, deleted from the restore share, and then subsequently deleted from the offsite storage for any reason, you will no longer have a backup of that object and it will not be exported again unless it is edited and saved, which increments the version number (causing the object to show up as yellow on the *Exports* list). This way, the management of the offsite storage server is critical to ensure needed backed up objects are not accidentally deleted because there is no easy way to instruct the appliance to start over and export everything from the beginning.

What to export

- **Do export**: ASR (MAC) Images, K-images, boot environments, WIM images, scripted installations, tasks, and user states.
- **Don't export (unless you know you need these)**: The database, network inventory, and network scans.
- **Don't export**: Driver folders, unless you know you have something in them you will need.

> **NOTE:** Drivers listed here correspond to folders listed in the `\\<appliance>\drivers` share. There are just a few items in these folders, as driver feed drivers (and manually built driver feeds) reside in `\\<appliance>\drivers_postinstall` instead of `\\<appliance>\drivers`.

Things to consider

Evaluate the total size of the items to be exported and the available disk space on the appliance. Each exported object is placed in the appliance restore share as two files: a `.pkg` file containing the data, and an `.xml` file describing the contents of the package file. Both files must be kept together and are needed in order to restore the object. As these files are written to the restore share, their size is subtracted from the total free space of the appliance. Once the available free space falls below 20 GB, many standard operations on the appliance may begin to fail for lack of space to complete. Therefore it is critical that

the total size of the exported objects does not exceed the available free space (minus the 20 GB of reserved space needed for a healthy appliance).

If the total size of the data to be backed up is greater than the available free space, it is a good idea to break the export/off-board transfer into four tasks (two export/transfer pairs), and to run them at different times of the week. This would require the **Clean up Restore**box to be selected on the off-board transfer setup page.

It is critical that enough time be allowed between the export job and the transfer task, to ensure the exports complete before the transfer task starts, in order to avoid hanging the transfer task which requires a Level 3 ticket to fix. To that end it is recommended leaving 24 hours between the time you expect the export task to complete and the start of the transfer task. This gives a safety margin so a slow export task will not collide with the transfer task.

Setting up off-board package transfer for exported objects

TFor information about the steps for setting up an off-board package transfer, visit https://support.quest.com/kace-systems-deployment-appliance/kb/115080.

Things to consider

The off-board storage server must have sufficient size (in terms of disk space) for the ID used to contain all the data on the appliance. In fact it should have much more free space than the total data as multiple version of a task should be backed up in case an object needs to be reverted to an older version, for some reason.

Determine how much impact will pushing the backup data have on the available network band width and what other resources might that impact. If the Off-board storage server is used for other applications, will they impact the transfer duration or will they suffer detrimental effects during the transfer process?

On the off-board package transfer set up page, if the **Clean up Restore** box is checked, after each object is copied to the remote storage server (off-board server) it will be deleted from the appliance restore share, freeing up needed space on the disk. Using this option is a recommended way to save space on the appliance, but it requires careful management of the files stored on the off-board storage server, to avoid deletion of needed backups.

How often one needs to back up is directly dependent on the amount of changes made to the appliance data over time. In most cases, a weekly backup is sufficient, but its solely a function of the environment you have and the risk you are willing to assume. Most people start the exports on a Friday night and the off-board transfer early Sunday morning (for example, 2:00 AM), but again this depends on your environment.

If you choose to set up automatic exports/off-board transfer, keep in mind you may from time to time need to back things up manually, as a need arises.

Updating appliance software

You can check for and install appliance software updates. When you update the appliance, custom configurations, such as the boot environments, Boot Manager, and default boot actions are preserved. Update the Remote Site Appliance (RSA) OVF image each time you update the appliance software.

View the appliance version

You can view the version of your appliance from any page, and you can check for and apply appliance software updates from the *Appliance Maintenance* page.

Choose one of the following methods to view the appliance version:

- View the appliance version from any page.
    1. Click the **About Appliance** link in the lower-right corner of the *Need Help* panel to view version and copyright information.
- View the current software version, and check for and apply appliance software updates.
    1. On the left navigation pane, click **Settings** to expand the section, then click **Appliance Maintenance** to display the *Appliance Maintenance* page.

    NOTE: When your license expires, a message appears at the top of the page, instructing you to update your license. The *License Maintenance Status* field on this page indicates the state of your license. To update your license, obtain a new key from your KACE sales representative, and update it on the *Registration and Licensing* page. If one or more Remote Site Appliances are associated with this appliance, the new license key is automatically updated on those RSAs after a synchronization.

    2. Verify the current software version number under **SDA Appliance Updates** > **Current Version** .

Check for and apply automatic updates

You can check whether a newer version of the appliance software is available.

NOTE: Always back up appliance components before installing updates or upgrading the appliance software. For instructions, see Use Off-Board Package Transfer.

Reboot the appliance before upgrading. If your appliance is on an earlier version, upgrade to the minimum version and enable SSH before proceeding with the installation. If using an RSA, upgrade the RSA OVF image to the current version. The appliance requires internet access to apply software updates.

Some updates take a few hours to apply and might require the appliance to reboot.

1. On the left navigation pane, click **Settings** to expand the section, then click **Appliance Maintenance** to display the *Appliance Maintenance* page.

NOTE: You can only update the appliance if your license is up to date. When your license expires, a message appears at the top of the page, instructing you to update your license. The *License Maintenance Status* field on this page indicates the state of your license. To update your license, obtain a new key from your KACE sales representative, and update it on the *Registration and Licensing* page. If one or more Remote Site Appliances (RSAs) are associated with this appliance, the new license key is automatically updated on those RSAs after a synchronization.

2. The *KACE SDA Updates* section displays the status of the appliance software. If the software is not up-to-date, under *Automatic Updates*, click **Check for Server Updates**.

   If your appliance license has expired, this is indicated in the *Update Status* field, instructing you to obtain and register a new license. To do that, request a new key from your KACE sales representative, and enter it on the *Registration and Licensing* page.

3. When an update is available, back up your appliance components to a different location before applying the update. See Use Off-Board Package Transfer.

Each time you update the appliance software, update the RSA OVF image.

Update the appliance manually

You can apply patches and updates to the appliance software and database manually when an appliance does not have internet access.

Download the latest `kbin` file to a device that you can access from the appliance. Reboot the appliance before upgrading. If your appliance is on an earlier version, upgrade to the minimum version and enable SSH before proceeding with the installation. Each time you update the appliance software, update the RSA (Remote Site Appliance) OVF image.

Some updates take a few hours to complete and might require the appliance to reboot.

1. On the left navigation pane, click **Settings** to expand the section, then click **Appliance Maintenance** to display the *Appliance Maintenance* page.

   NOTE: You can only update the appliance if your license is up to date. When your license expires, a message appears at the top of the page, instructing you to update your license. The *License Maintenance Status* field on this page indicates the state of your license. To update your license, obtain a new key from your KACE sales representative, and update it on the *Registration and Licensing* page. If one or more Remote Site Appliances (RSAs) are associated with this appliance, the new license key is automatically updated on those RSAs after a synchronization.

2. In the *Appliance Updates* section, under *Manual Updates*, select the update file.

   If your appliance license has expired:

   - You can still apply security patches and hotfixes, as applicable.
   - To renew your license, request a new key from your KACE sales representative, and enter it on the *Registration and Licensing* page.

3. Click **Update Server**.

If your appliance license has expired, and you attempt to update the server, the *Maintenance Has Expired* message box appears, as described in the above step. Otherwise, the *KACE Appliance Upgrade Console page* appears, displaying the upgrade log.

4. Observe the contents of the log as the appliance is being upgraded.
   - The upgrade can take some time, depending on the number of system images on the appliance.
   - During the upgrade, the database is backed up. If there is not enough space on disk to back up the database, the upgrade will stop.
   - The appliance reboots several times during the upgrade process. This is indicated in the message at the top of the page, followed by a page refresh.
   - The upgrade process removes PXE Linux causing the `K2000.0` and kbox2000.0 files to be removed. After the upgrade, you must update your DHCP configuration to use the new files, `undionly.kpxe` and `ipxe.efi`.
   - If any issues are encountered during the upgrade, they are indicated in an error message, instructing you to contact Quest Support.

   After the upgrade is complete, you are automatically redirected to the Software Transaction Agreement (STA) page, also known as EULA (End User License Agreement).
5. Accept the EULA, then log in using the your admin ID and password.

The update is applied.

Glossary

A

action icons

Remote connection programs built in to the KACE Systems Deployment Appliance (appliance).

Administrator Console

The web-based interface to control the appliance.

answer file

A file that defines the settings to install the operating system. The answer file is used for unattended scripted installations.

B

Boot Manager

The boot menu that displays on target devices immediately after a target device boots in to the appliance and enables the selection of the KACE Boot Environment (KBE).

Boot Manager timeout period

The length of time that the Boot Manager remains active on a target device.

BSCP

Mac computer's built-in BSCP (Base Station Control Protocol) and bootstrap file that displays the option to boot from the local hard drive or from the server.

BSDP (Boot Server Discovery Protocol)

A standards-conforming extension of DHCP developed by Apple that allows Mac computers to boot from bootable images on a network instead of a local storage media.

C

clean installation

An installation of an operating system on a hard drive that has been erased.

D

DHCP scope

The range of possible IP addresses that the DHCP server can lease to devices on the same subnet as the appliance.

disk imaging

Provides an exact sector-by-sector or file-by-file copy of all the contents of a device's hard disk to an image file.

DISKPART

A Windows utility built into the appliance that uses scripts to manage objects such as disks or partitions.

Driver Feed

A built-in tool that adds the latest drivers to the `drivers_postinstall` share directory that you can download and install to the appliance.

driver re-cache

Updates drivers manually added to the `drivers` share directory for boot environments and scripted installations.

driver share directory

A local appliance directory that manages the network and mass storage drivers required to build the KACE Boot Environment from the `drivers` share folder and the drivers that the operating system requires from the `drivers_postinstall` folder.

driver slipstreaming

Automates OS installations with the correct drivers. It also integrates patches or service packs in to the installation, and enables direct software updates.

H

Hardware Abstraction Layer

Enables customizing the target device's HAL (Hardware Abstraction Layer) after a K-Image deployment.

Hardware-independent deployment

Enables using a single scripted installation to provision multiple hardware configurations. The appliance automatically adds the appropriate drivers with the scripted installation.

I

ImageX

Provides the ability to capture, modify, and apply file based disk images for rapid deployment of Windows image (`.wim`) files for copying to a network. ImageX also works with other technologies that use `.wim` images, such as Windows Setup, Windows Deployment Services (Windows DS), and the System Management Server (SMS) Operating System Feature Deployment Pack.

initial configuration console

The command-line interface that displays after connecting a monitor to the appliance to configure the network settings.

ITNinja

Sponsored by Quest KACE, ITNinja.com (formerly AppDeploy.com) is a product agnostic IT-focused community website where IT professionals share information and ask questions about system-deployment related topics.

G

Gold Master

A reference machine used as the basis for image capture. The appliance automates the Gold Master creation process through scripted installations.

K

KACE Boot Environment (KBE)

A boot environment that is a scaled-down version of an operating system for performing various Windows-based tasks on target devices. KBE allows for disk imaging, scripted installations, recovery, file browsing, and inventory collection.

KBE Main Menu

The user interface for the KACE Boot Environment that enables image captures, scripted installation and system image deployments, and device recovery.

K-Image

A file-based format that enables easy editing of computer and server images, eliminating the need to rebuild images.

Knowledge Base

Quest KACE Knowledge Base articles with updated solutions to real-world KACE Systems Deployment Appliance problems that administrators encounter. Visit https://support.quest.com/resources/kb.

L

linking

The process of connecting multiple K-Series appliances and having the ability to access linked appliances from one Administrator Console if the administrator user account for each appliance has the same password.

Load State utility

A Microsoft User State Migration Tool utility that enables migrating data and settings manually from the `.mig` file on to target devices.

login hook

Instructs the Mac OS X to run a certain script immediately after the user logs on, but before other login processes are performed.

M

mid-level task

A mid-level task is a post-installation task that runs in the KACE Boot Environment runtime environment.

Media Manager

An appliance utility that builds the KACE Boot Environment, and uploads the operating system source files and the Windows User State Migration Tool (USMT) to the appliance for Windows. The Media Manager for Mac OS X builds the NetBoot Environments.

O

OEM key

A single computer license used to install Windows 7 and higher at the factory. Typically, mid-sized organizations use this license to leverage the initial software license that is included with the device.

offboard database access

An appliance setting that enables external reporting programs to connect to and query the appliance database.

offboard storage

Uses an external NAS device to expand the appliance internal storage capacity. It also expands Remote Site Appliance (RSA) and Virtual appliance storage capacity by using an additional virtual disk. When external storage is enabled, internal storage is no longer available.

offline user migration scan

The appliance captures the user states using the *Scan User States Offline* pre-installation task.

online user migration scan

The appliances migrates the captured user states using the *Deploy User State* post-installation task.

P

Package Management

An appliance feature that enables importing, exporting, and transferring appliance components to a different location.

post-installation tasks

Tasks run after deploying an operating system, for example configuring the computer name, joining domains, and installing drivers.

PXE boots

Boots from the network without the target environment where the operating system is installed. PXE boots do not require an external storage device such as a USB or a CD or DVD drive.

R

Remote Site Appliance (RSA)

The RSA is a virtual instance of the KACE Systems Deployment Appliance that downloads directly from the KACE Systems Deployment Appliance and uses the same license key. The RSA network boots devices for deployments to remote sites. The linking featured displays the RSA on the Administrator Console.

Remote site management

Enables deployments to remote sites without the need for dedicated hardware or personnel at remote facilities.

retail key

A single key for a computer. Typically small organizations that do not have a high volume of installations use this key.

S

scripted installation

Automates the installation of an operating system and provides hardware-independent provisioning of desktops, laptops, and servers.

Scan State utility

A Microsoft Windows User State Migration Tool (USMT) utility that enables scanning and capturing user profiles and configurations to include or exclude data.

Sysprep

The Microsoft Sysprep tool removes all system-specific information and resets the device.

System-provided imaging

OS-specific formats such as Microsoft WIM and Apple DMG images that are compatible with the appliance.

T

tether

A Quest KACE Technical Support team connection to your device for troubleshooting.

U

user states

User-specific files and settings on a device that can be scanned, captured, and uploaded to the appliance using the Microsoft Windows User State Migration Tool (USMT).

User State Migration

Transfers user-specific files and settings along with the operating system and applications on to target devices.

USMT Scan Template

A template that defines user-specific files and settings to exclude from scans.

V

VNC password

A Java VNC client included with the appliance to enable connections to the target devices while it is booting from the appliance.

Volume KMS

A multi-seat license the KMS server manages and hosts. Typically enterprise customers use this key.

Volume MAK

A multi-seat license that Microsoft enables and manages; it requires internet access to complete the activation. Typically, mid-sized enterprise organizations use this key.

W

WIM (Windows Imaging Format)

An appliance supported file-based disk image format used as part of the Windows operating system standard installation procedure.

Windows PE

Prepares a computer for Windows installation, copies disk images from a network file server, and initiates Windows setup.

WSName.exe

An appliance supported utility that uses a text file to rename Windows target devices.

Windows ADK

The Windows Assessment and Deployment Kit (Windows ADK) is a collection of tools required to build the KACE Boot Environment (KBE) for Windows 7 and higher and Windows Server 2012 computers.

About us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product.

Legal notices

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, Join the Innovation, and KACE are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

KACE Systems Deployment Appliance Administrator Guide

Updated - January 2025

Software Version - 9.3

Index

E

F

G

H

S

T

U

V

W