KACE® Systems Deployment Appliance 7.2

Administrator Guide
# Table of Contents

About the KACE Systems Deployment Appliance................................................................. 10  
Getting started..................................................................................................................... 11  
  Tasks for getting started using the KACE SDA............................................................. 11  
  About the KACE SDA components.............................................................................. 12  
  Log in to the Administrator Console.......................................................................... 13  
  Filter lists and search for information........................................................................... 14  
  Access product documentation...................................................................................... 15  
  Configure the language settings.................................................................................. 17  
  Change a default theme for the appliance................................................................. 17  
Using the Dashboard............................................................................................................ 19  
  Customize the Dashboard............................................................................................. 19  
Configuring the KACE SDA.................................................................................................. 20  
  Configure the initial network settings...................................................................... 20  
  Modify the initial network settings......................................................................... 21  
  Changing the default passwords.............................................................................. 23  
    Use the Command Line Console to reset the Administrator's password.............. 24  
    Change the Samba share password................................................................... 25  
    Set the VNC® password................................................................................... 26  
    Enable Boot Manager authentication................................................................. 26  
  Configuring the appliance date and time settings..................................................... 26  
    Configure the date and time.............................................................................. 26  
  Enabling link aggregation.......................................................................................... 27  
    Create an aggregate link.................................................................................. 27  
  Configuring the data sharing preferences...................................................................... 28  
    Share basic appliance data usage.................................................................... 28  
    Share detailed usage data............................................................................. 29  
Linking Quest KACE appliances.......................................................................................... 29  
  Enable appliance linking................................................................................... 30  
  Add Names and Keys to appliances.................................................................. 30  
  Disable linked appliances................................................................................. 31  
Migrating appliances........................................................................................................ 31  
  Migrate appliance data.................................................................................. 31  
Setting up user accounts and user authentication.............................................................. 34  
  Add or edit local administrator accounts.............................................................. 34  
  Configure an LDAP server for user authentication............................................... 35  
  Test the LDAP server.................................................................................. 37
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete user accounts</td>
<td>37</td>
</tr>
<tr>
<td>Configuring security settings</td>
<td>38</td>
</tr>
<tr>
<td>Enable SNMP monitoring</td>
<td>38</td>
</tr>
<tr>
<td>Enable SSL using an existing certificate</td>
<td>38</td>
</tr>
<tr>
<td>Generate private key for new SSL certificate</td>
<td>39</td>
</tr>
<tr>
<td>Disable SSL</td>
<td>40</td>
</tr>
<tr>
<td>Enable database access</td>
<td>40</td>
</tr>
<tr>
<td>Enable SSH Root Login (KACE Support)</td>
<td>40</td>
</tr>
<tr>
<td>Prevent brute-force login attacks</td>
<td>40</td>
</tr>
<tr>
<td>Preparing for deployment</td>
<td>42</td>
</tr>
<tr>
<td>Set up the deployment environment</td>
<td>42</td>
</tr>
<tr>
<td>Enable the on-board DHCP server</td>
<td>42</td>
</tr>
<tr>
<td>Configure the offboard DHCP server</td>
<td>43</td>
</tr>
<tr>
<td>Download and install the KACE SDA Media Manager</td>
<td>43</td>
</tr>
<tr>
<td>About the Media Manager</td>
<td>44</td>
</tr>
<tr>
<td>Download and install Windows ADK</td>
<td>49</td>
</tr>
<tr>
<td>Upload OS installation or source files</td>
<td>49</td>
</tr>
<tr>
<td>View source media details</td>
<td>50</td>
</tr>
<tr>
<td>View or update source media metadata</td>
<td>50</td>
</tr>
<tr>
<td>Choosing the type of deployment</td>
<td>50</td>
</tr>
<tr>
<td>Supported images types</td>
<td>51</td>
</tr>
<tr>
<td>Managing device inventory</td>
<td>52</td>
</tr>
<tr>
<td>Configure and run a network scan</td>
<td>52</td>
</tr>
<tr>
<td>Add network inventory to the appliance</td>
<td>52</td>
</tr>
<tr>
<td>Scan active and non-active devices on the network</td>
<td>53</td>
</tr>
<tr>
<td>Add devices manually</td>
<td>53</td>
</tr>
<tr>
<td>Join devices to a domain</td>
<td>54</td>
</tr>
<tr>
<td>Issue a Wake-on-LAN request</td>
<td>54</td>
</tr>
<tr>
<td>Deploy to devices in the KACE SMA inventory</td>
<td>55</td>
</tr>
<tr>
<td>View device details from a network scan</td>
<td>55</td>
</tr>
<tr>
<td>Apply a KUID to the KACE SMA Agent</td>
<td>56</td>
</tr>
<tr>
<td>Collect the computer name</td>
<td>56</td>
</tr>
<tr>
<td>Apply the computer name</td>
<td>57</td>
</tr>
<tr>
<td>Delete devices from Device Inventory</td>
<td>57</td>
</tr>
<tr>
<td>Delete devices from Network Inventory</td>
<td>57</td>
</tr>
<tr>
<td>Unregister devices</td>
<td>57</td>
</tr>
<tr>
<td>About the device action icons</td>
<td>58</td>
</tr>
<tr>
<td>Run an action on devices</td>
<td>59</td>
</tr>
</tbody>
</table>
Access remote devices using a VNC session................................................................. 59
Using labels..................................................................................................................... 60
  Create and apply labels................................................................................................. 60
  Remove components from a label............................................................................... 60
  Delete a label from the appliance................................................................................. 61
  View the components assigned to a label................................................................. 61
Creating a Windows or Linux Boot Environment.............................................................. 62
  Create a Windows boot environment........................................................................... 62
  Create a Linux boot Environment............................................................................... 63
  Update Windows drivers............................................................................................. 63
  Set new KBE as default for the appliance................................................................. 64
  Best practices: Create a KACE Boot Environment (KBE) for Windows................... 64
Managing drivers........................................................................................................... 66
  Add drivers to system images...................................................................................... 66
  Adding drivers to scripted installation deployments.................................................. 67
    Enable Driver Feed to automate driver updates...................................................... 67
    Install driver packages to the appliance................................................................. 67
    Disable Driver Feed................................................................................................. 68
    Create folders to add device-specific drivers......................................................... 68
    Generate KACE SDA package to import large driver files...................................... 68
    Import driver packages to the appliance............................................................... 69
    Understanding KACE Boot Environment drivers.................................................... 69
    Add network and storage drivers manually............................................................. 70
    Re-cache the network and storage driver directory............................................... 70
    Add drivers as a post-installation task..................................................................... 71
    View list of missing drivers...................................................................................... 71
Managing network drivers............................................................................................. 71
  Download network and storage drivers................................................................. 72
  Import driver packages............................................................................................... 73
  Display device compatibility....................................................................................... 73
  View driver compatibility details.............................................................................. 73
  Export drivers............................................................................................................. 74
  Re-cache drivers........................................................................................................ 74
Managing operating system drivers............................................................................... 74
  Enable Driver Feed for scripted installations......................................................... 75
  Enable Driver Feed for system images................................................................. 75
  Disable Driver Feed................................................................................................. 75
  Download operating system driver packages......................................................... 76
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Off-Board Package Transfer</td>
<td>144</td>
</tr>
<tr>
<td>Upload packages for import</td>
<td>145</td>
</tr>
<tr>
<td>Import appliance components</td>
<td>146</td>
</tr>
<tr>
<td>Package components to export</td>
<td>146</td>
</tr>
<tr>
<td>Package file names</td>
<td>147</td>
</tr>
<tr>
<td>Managing disk space</td>
<td>149</td>
</tr>
<tr>
<td>Verify available disk space</td>
<td>149</td>
</tr>
<tr>
<td>Delete images not associated with devices</td>
<td>149</td>
</tr>
<tr>
<td>Delete images associated with devices</td>
<td>150</td>
</tr>
<tr>
<td>Delete unassigned scripted installations</td>
<td>150</td>
</tr>
<tr>
<td>Delete unassigned boot environments</td>
<td>150</td>
</tr>
<tr>
<td>Delete source media</td>
<td>150</td>
</tr>
<tr>
<td>Delete unassigned pre-installation tasks</td>
<td>151</td>
</tr>
<tr>
<td>Delete unassigned post-installation tasks</td>
<td>151</td>
</tr>
<tr>
<td>Enabling offboard storage</td>
<td>151</td>
</tr>
<tr>
<td>Add a virtual disk for offboard storage</td>
<td>151</td>
</tr>
<tr>
<td>Revert offboard data to onboard storage</td>
<td>152</td>
</tr>
<tr>
<td>Configure an off-board storage device</td>
<td>153</td>
</tr>
<tr>
<td>Best practices for using external storage</td>
<td>153</td>
</tr>
<tr>
<td>Troubleshooting appliance issues</td>
<td>155</td>
</tr>
<tr>
<td>Test device connections on the network</td>
<td>155</td>
</tr>
<tr>
<td>Enable a tether to Quest KACE Technical Support</td>
<td>156</td>
</tr>
<tr>
<td>Open a support ticket</td>
<td>157</td>
</tr>
<tr>
<td>Troubleshooting the Boot Manager</td>
<td>157</td>
</tr>
<tr>
<td>Test whether a target device can network boot</td>
<td>157</td>
</tr>
<tr>
<td>Change the Boot Manager interface</td>
<td>158</td>
</tr>
<tr>
<td>Set the Boot Manager timeout</td>
<td>158</td>
</tr>
<tr>
<td>Select the local hard disk boot method</td>
<td>158</td>
</tr>
<tr>
<td>Change the network delay time</td>
<td>159</td>
</tr>
<tr>
<td>Recovering devices</td>
<td>159</td>
</tr>
<tr>
<td>Recover corrupted devices</td>
<td>159</td>
</tr>
<tr>
<td>Downloading the KACE SDA log files</td>
<td>160</td>
</tr>
<tr>
<td>Download all appliance log files</td>
<td>160</td>
</tr>
<tr>
<td>View the appliance log files</td>
<td>160</td>
</tr>
<tr>
<td>Appliance log types and descriptions</td>
<td>160</td>
</tr>
<tr>
<td>Shutting down and rebooting the appliance</td>
<td>163</td>
</tr>
<tr>
<td>Power off the appliance</td>
<td>163</td>
</tr>
<tr>
<td>Reboot the appliance</td>
<td>164</td>
</tr>
</tbody>
</table>
The Quest KACE Systems Deployment Appliance (SDA) provides a network-centric solution for capturing and deploying images. The KACE SDA provides 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 KACE SDA 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 KACE SDA with the KACE Systems Management Appliance (SMA) to image the KACE SMA inventory. The KACE SDA is available as a virtual appliance.

To view information on this KACE SDA, 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 KACE SDA

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

Table 1. Tasks for getting started using the KACE SDA

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

<table>
<thead>
<tr>
<th>Task</th>
<th>How to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure DHCP server</td>
<td>Set up the DHCP server to network boot target devices from the KACE SDA.</td>
</tr>
<tr>
<td>Test the boot environment</td>
<td>Verify that the target devices can boot from the appliance.</td>
</tr>
<tr>
<td>Migrate user files and settings</td>
<td>Capture user profiles from a device using the Windows User State Migration Tool (USMT), version 5.0.</td>
</tr>
<tr>
<td>Upload operating system source files</td>
<td>Upload the OS source files to the KACE SDA using the Media Manager.</td>
</tr>
<tr>
<td>Deploy the OS</td>
<td>Deploy the OS using a scripted installation or a system image deployment.</td>
</tr>
</tbody>
</table>

### About the KACE SDA components

The KACE SDA 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 KACE SDA has the following components:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual appliance</td>
<td>The KACE SDA is available as a virtual appliance. It uses a VMware or Microsoft Hyper-V infrastructure. For technical specifications, see <a href="http://documents.quest.com/kace-systems-deployment-appliance/technical-specifications-for-virtual-appliances/">http://documents.quest.com/kace-systems-deployment-appliance/technical-specifications-for-virtual-appliances/</a>.</td>
</tr>
<tr>
<td>Command-Line Console</td>
<td>The Command-Line Console is a terminal window interface to the KACE SDA. The interface is designed primarily to configure the appliance network settings.</td>
</tr>
<tr>
<td>Administrator Console</td>
<td>The Administrator Console is the web-based interface used to navigate the KACE SDA. To access the Administrator Console, go to <a href="http://%3CKACE_SDA_hostname%3E/admin">http://&lt;KACE_SDA_hostname&gt;/admin</a> where <code>&lt;KACE_SDA_hostname&gt;</code> is the host name of your appliance.</td>
</tr>
<tr>
<td>Support Portal</td>
<td>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.</td>
</tr>
</tbody>
</table>
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://KACE_SDA.
   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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Key</td>
<td>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 <a href="https://support.quest.com/contact-support">https://support.quest.com/contact-support</a>.</td>
</tr>
<tr>
<td>Administrator Password</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.

| 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. |
When you complete the configuration, logging in to the KACE SDA 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Connectivity</td>
<td>The KACE SDA and the Virtual KACE SDAs must be connected to the network to validate the license information.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Select the timezone where the appliance is located.</td>
</tr>
</tbody>
</table>

5. **Optional.** If you change your mind, and want to switch to the KACE SDA or RSA 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. **Optional.** If you change your mind, and want to switch to the KACE SDA or RSA 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.

9. 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.

10. When the appliance restarts, refresh the browser page.

11. 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.

12. Select a theme for the Administration Console that best suits your needs. 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.
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.
   a. In the top-right corner of the page, in the Search field, type the search text.
   b. 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 (SDA) help contents.
   - : Allows you to browse the Knowledge Base articles associated with the related page.
   - : Starts a chat with a KACE Systems Deployment Appliance (SDA) 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 (SDA) 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:** For a PDF version of the Help system, click the Acrobat button on the right side of the main Help system navigation bar (PDF).

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 SDA 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 (SDA) 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

You can set the language used for text in the appliance console, configure the region settings to determine the default character set to use for numbers such as dates, and select a font for the text used in your KACE Boot Environment (KBE) for Windows.

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. Under KBE Optional Font Support, select a locale to determine the language to use for the text in your KACE Boot Environment (KBE) for Windows.

   If you add Asian fonts, be sure to rebuild the KBE using the Media Manager.

5. Optional: Click Cancel to close the page.

6. Click Save.

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.

<table>
<thead>
<tr>
<th>NOTE:</th>
<th>Reports always appear with a white background, regardless of which theme is selected.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOTE:</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 to view the Dashboard.
2. 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.
3. Click the Customize button in the top-right corner of the page to view the available widgets.
4. Click Install to show a widget that is currently hidden.
Configuring the KACE SDA

The initial KACE SDA 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 KACE SDA from the KACE SDA 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 KACE SDA 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Enter the host name of the appliance. The default is k2000.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Enter the domain the appliance is on. For example, example.com.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the static IP address of the appliance.</td>
</tr>
<tr>
<td>Network Speed</td>
<td>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.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Enter the network gateway for the appliance.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Enter the subnet (network segment) that the appliance is on. For example, 255.255.255.0.</td>
</tr>
<tr>
<td>Primary DNS</td>
<td>Enter the IP address of the primary DNS server the appliance uses to resolve host names.</td>
</tr>
</tbody>
</table>
**Modify the initial network settings**

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

1. On the left navigation pane, click **Settings** to display the Control Panel, then click **Network Settings** to display the Network Settings page.

2. Configure the following network settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Enter the host name of the appliance. The default is k2000.</td>
</tr>
</tbody>
</table>
Modify the initial network settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>Enter the domain the appliance is on. For example, example.com.</td>
</tr>
<tr>
<td>Primary DNS</td>
<td>Enter the IP address of the primary DNS server the appliance uses to resolve host names.</td>
</tr>
<tr>
<td>Secondary DNS</td>
<td><strong>Optional:</strong> Enter the IP address of the secondary DNS server the appliance uses to resolve host names.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Enter the network gateway for the appliance.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Read-only field. It displays the name of the interface.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the static IP address of the interface.</td>
</tr>
<tr>
<td>Network Speed</td>
<td>Select the speed of the interface. This speed should match the setting of your LAN switch. If you select <em>Auto-negotiate</em>, the system determines the best value automatically provided that the LAN switch supports auto-negotiation.</td>
</tr>
<tr>
<td>Netmask</td>
<td>Enter the subnet (network segment) that the interface is on. For example, 255.255.255.0.</td>
</tr>
<tr>
<td>MTU</td>
<td>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.</td>
</tr>
<tr>
<td>Status</td>
<td>Read-only field. It indicates if the network cable is plugged into the interface.</td>
</tr>
<tr>
<td>Deployment Interface</td>
<td>Select this option if you want this interface to be used as a deployment interface.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Read-only field. It displays the name of the link aggregation interface.</td>
</tr>
</tbody>
</table>
Changing the default passwords

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

The following passwords are associated with the KACE SDA.

<table>
<thead>
<tr>
<th>Password</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>The default password is admin. The new password must be six characters or more in length.</td>
</tr>
<tr>
<td>KACE SDA Samba Share Password, Media Manager, and KACE Boot Environment (KBE)</td>
<td>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.</td>
</tr>
<tr>
<td>Boot Manager</td>
<td>By default, Boot Manager authentication is disabled. The Boot Manager contains a bootstrap file that the Windows client Boot Manager downloads during</td>
</tr>
</tbody>
</table>

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. Optional: Select the Use SMTP Server check box.
9. Click Save.
Use the Command Line Console to reset the Administrator's password

If you change the Administrator's password, and become locked out of the KACE SDA 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 KACE SDA 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 KACE SDA. 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:** 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:

   ![Image of a physical appliance](image)

   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.

<table>
<thead>
<tr>
<th>Password</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>the initial device PXE boot in to the KACE Boot Environment. The Boot Manager interface displays on the target device.</td>
<td></td>
</tr>
<tr>
<td>VNC</td>
<td>Enables a connection to a target device that has networked booted.</td>
</tr>
<tr>
<td>NetBoot</td>
<td>Used only for Mac devices.</td>
</tr>
</tbody>
</table>

**NOTE:** Only 7-bit ASCII characters are accepted for KBE remote VNC passwords.
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 KACE SDA Administrator Console with your newly changed password.
   a. Open a web browser and navigate to the KACE SDA 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 KACE SDA 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 KACE SDA 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 KACE SDA Samba share password. 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. On the left navigation pane, click Settings to display the Control Panel, then click General Settings to display the General Settings page.
2. In KACE 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 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. On the left navigation pane, click Settings to display the Control Panel, then click General Settings to display the General Settings page.
2. 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 SDA Boot Manager displays on a target device that has PXE booted from the KACE SDA. 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 to display the Control Panel, then click General Settings to display the General Settings page.
2. 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.

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 KACE SDA system clock is set to synchronize with the Quest KACE time server. You can change the system clock settings to match your timezone.

Configure the date and time

The KACE SDA 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 to display the Control Panel, then click Date and Time Settings to display the Date and Time Settings page.
2. Specify the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timezone</td>
<td>Select a timezone in the drop-down list.</td>
</tr>
</tbody>
</table>
### Time Setting

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Setting</td>
<td>Select an option:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Set the clock on the KACE SDA 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.</td>
</tr>
</tbody>
</table>

### 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](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.

## Enabling link aggregation

By default, link aggregation is not enabled on the KACE SDA. 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 KACE SDA LACP connection. For an example of a Cisco® switch configuration running the IOS operating system set to active mode, view the online [FreeBSD® Handbook](https://www.freebsd.org/doc/). All interfaces in each EtherChannel must be the same speed and duplex.

## Create an aggregate link

The physical KACE SDA 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** 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 KACE SDA 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 KACE SDA 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.
- **KACE SDA Disk Information**: RAID Status, Physical Drivers, Adapter Information, and so on. Disk information is only available for the physical KACE SDA.

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** to display the **Control Panel**, then click **General Settings** to display the **General Settings** page.
2. Under **Share With Quest**, 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** to display the **Control Panel**, then click **General Settings** to display the **General Settings** page.

2. Under **Share With Quest**, 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:

- KACE SDA Server Crash Logs
- UI Access Statistics

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 SMA (Systems Management Appliance), KACE SDA, or remote (RSA) appliances 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 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 SDA or remote (RSA) 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.

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: 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 SMA comes with a default organization (named Default). If your KACE SDA is linked with the Default organization on a KACE SMA, 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 SMA.
3. On the Edit Linked Appliance Detail page that appears, in the Default ORG Name field, type the organization name, and click Save.

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 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 SDA or remote (RSA) appliances that were linked until you log off.

1. On the left navigation pane, click Settings 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 KACE SDA, 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 KACE SDA 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 KACE SDA. 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 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, and click Next.
   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 destination appliance, on the Copy Destination Key page, left-click the field to copy the key, and click Next.
   d. On the source appliance, on the Apply Destination Key page, paste the key into the field, and 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, 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 Begin Migration button appears disabled.
   b. 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 KACE SDA 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.

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 KACE SDA 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 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td><strong>Required</strong>: Enter a login ID.</td>
</tr>
<tr>
<td>Full Name</td>
<td><strong>Required</strong>: Enter the first and last name of the user.</td>
</tr>
<tr>
<td>Email</td>
<td><strong>Required</strong>: Enter the email address of the user.</td>
</tr>
<tr>
<td>Domain</td>
<td>Enter the domain that the user is using.</td>
</tr>
<tr>
<td>Budget Code</td>
<td><strong>Optional</strong>: Enter the budget code of the department where the user is located.</td>
</tr>
<tr>
<td>Location</td>
<td><strong>Optional</strong>: Enter the site or location of the user.</td>
</tr>
<tr>
<td>Password</td>
<td><strong>Required</strong>: Enter the default password for the user.</td>
</tr>
</tbody>
</table>

The password is required to activate the user. If the Password field is blank, the user cannot log in to the Administrator Console.
Configure an LDAP server for user authentication

LDAP authentication requires creating a login account for the KACE SDA 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 KACE SDA, 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Friendly Name</td>
<td>The name to identify the server.</td>
</tr>
<tr>
<td>Server Host Name (or IP)</td>
<td>The IP address or the host name of the LDAP server. If the IP address is not valid, the appliance</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>waits to timeout, resulting in login delays during LDAP authentication.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> To connect through SSL, use an IP address or host name. For example: \texttt{ldaps://hostname}.</td>
</tr>
<tr>
<td>LDAP Port Number</td>
<td>The LDAP port number, which is usually 389 (LDAP) or 636 (secure LDAP).</td>
</tr>
<tr>
<td>Search Base DN</td>
<td>The area of the LDAP tree that the appliance should start to search for users. For example to search for the IT group, specify \texttt{OU=it,DC=company,DC=com}.</td>
</tr>
<tr>
<td>Search Filter</td>
<td>The search filter, for example: \texttt{LDAP_attribute=KBOX_USER}, where \texttt{LDAP_attribute} is the name of the attribute containing a unique user ID and \texttt{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 \texttt{samaccountname=KBOX_USER}. For most other LDAP servers, enter \texttt{UID=KBOX_USER}.</td>
</tr>
<tr>
<td>LDAP Login</td>
<td>The credentials of the account that the KACE SDA uses to log in to the LDAP server to read accounts. For example: \texttt{LDAP Login:CN=service_account,CN=Users,DC=company,DC=com}. If no username is provided, an anonymous bind is attempted.</td>
</tr>
<tr>
<td>LDAP Password (if required)</td>
<td>The password of the account that the KACE SDA uses to log in to the LDAP server.</td>
</tr>
<tr>
<td>User Permissions</td>
<td>The user permissions.</td>
</tr>
<tr>
<td></td>
<td>• Admin: Read/write access to the Administrator Console.</td>
</tr>
<tr>
<td></td>
<td>• ReadOnly Admin: View all pages; no change access.</td>
</tr>
<tr>
<td>Test User Password</td>
<td>The LDAP username and password to test on the LDAP server. See Test the LDAP server.</td>
</tr>
</tbody>
</table>
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** 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.
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 KACE SDA.

Enable SNMP monitoring

The SNMP agent on the KACE SDA 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 Master SNMP agent configured on a different device, it can send GET, GETNEXT, and GETBULK requests to the KACE SDA and have the appliance return the requested information.

1. On the left navigation pane, click Settings 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.

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 KACE SDA 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 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 KACE SDA 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 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 KACE 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 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 database access

You can enable database access to allow external programs, such as Crystal Reports or Excel® to query the KACE SDA 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 to display the Control Panel, then click Security to display the Security Settings page.
2. Select the Enable Database Access check box.
3. Click Save.

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

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 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.

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** 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**.
Preparing for deployment

KACE SDA 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 KACE SDA 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 KACE SDA 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 KACE SDA 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 SDA 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 OS installation or source files.
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.

Enable the on-board DHCP server

If you are testing the KACE SDA on a private network or in a small environment that does not have a DHCP server, the KACE SDA 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 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 KACE SDA is the PXE server. You can configure an offboard DHCP server to acknowledge the appliance to enable target devices to UEFI boot from the KACE SDA.

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 KACE SDA:
   - Set Option 066 to the IP address of the KACE SDA. 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 KACE SDA 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 KACE SDA.

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 SDA Media Manager

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


1. On the left navigation pane, click Library 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 SDA 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 SDA 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.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Name</td>
<td>The name of the KBE. This value is automatically generated, but you can change it, if required.</td>
</tr>
<tr>
<td></td>
<td>Architecture</td>
<td>Windows only. The OS architecture of the KBE. Select the 32-bit or 64-bit architecture, as needed.</td>
</tr>
<tr>
<td></td>
<td>Language</td>
<td>The language of the KBE.</td>
</tr>
<tr>
<td></td>
<td>Upload KBE</td>
<td>Click to upload the KBE to the appliance.</td>
</tr>
<tr>
<td></td>
<td>Upload Custom ISO</td>
<td>Click to upload the Custom ISO to the appliance.</td>
</tr>
<tr>
<td></td>
<td>Upload Custom WIM</td>
<td>Click to upload the Custom WIM to the appliance.</td>
</tr>
<tr>
<td>Server Configuration</td>
<td>Use DHCP to find SDA</td>
<td>Allows the Media Manager to use its DHCP server to locate the appliance.</td>
</tr>
<tr>
<td></td>
<td>Use the SDA static IP Address</td>
<td>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 created using this</td>
</tr>
<tr>
<td>Tab</td>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>About the Media Manager</td>
<td>Use the RSA static IP Address</td>
<td>Select this option to specify the static IP address of the RSA to create boot environments for an RSA.</td>
</tr>
<tr>
<td>Device Configuration</td>
<td>Find Device IP Address by DHCP</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Assign a static IP Address</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Set a range of static IP Address</td>
<td>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.</td>
</tr>
<tr>
<td>Advanced Options</td>
<td>Scratch Space in Mb</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Add ADSI Drivers</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Add ODBC Drivers</td>
<td>Adds ODBC (Open Database Connectivity) drivers. Select this option if you want the target device to establish a database connection.</td>
</tr>
<tr>
<td></td>
<td>DCCTK/Command Configure</td>
<td>Indicates if Dell Client Configuration Toolkit, also known</td>
</tr>
<tr>
<td>Tab</td>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UEFI ISO</td>
<td>Allows the KBE to create Unified Extensible Firmware Interface compliant device. This option is only supported on 64-bit systems.</td>
</tr>
<tr>
<td></td>
<td>Sync KBE time with server</td>
<td>Synchronizes the KBE system time with the time set on the appliance.</td>
</tr>
<tr>
<td></td>
<td>Set KBE Time Zone</td>
<td>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 system running the Media Manager, but you can choose a different time zone, as required.</td>
</tr>
<tr>
<td></td>
<td>Add files to KBE</td>
<td>Allows you to add custom files to the KBE. For example, you can add portable applications to the KBE, such as anti-virus scanner.</td>
</tr>
<tr>
<td></td>
<td>Launch UltraVNC</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>KACE Deployment Menu</td>
<td>Select this option if you want to display the KACE Deployment Menu when the target device boots, or clear it, if you do not want the menu to appear.</td>
</tr>
<tr>
<td></td>
<td>Run Driver Feed Advisor</td>
<td>Specifies the path to the driver feed for the target device model.</td>
</tr>
<tr>
<td></td>
<td>Add .NET 4</td>
<td>Select to add .NET 4 to the KBE.</td>
</tr>
<tr>
<td></td>
<td>Add Powershell</td>
<td>Select to add PowerShell to the KBE. If you select this option, it is added to the KBE.</td>
</tr>
</tbody>
</table>

KACE Systems Deployment Appliance 7.2 Administrator Guide

About the Media Manager
<table>
<thead>
<tr>
<th>Tab</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>option, .NET 4 is added to the KBE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Add Enhanced Storage</strong></td>
<td>Allows you to add Enhanced Storage to target devices. This feature allows Windows to discover additional storage functionality and to manage the storage devices natively. For more information about Enhanced Storage, see your Windows documentation.</td>
</tr>
<tr>
<td></td>
<td><strong>ISO size restriction override</strong></td>
<td>If your organization does not have ISO file size restrictions in place, you can use this option to create larger ISO images.</td>
</tr>
<tr>
<td></td>
<td><strong>Enable SMB v.1</strong></td>
<td>Use this option if you want the target device to use this older version of the SMB protocol.</td>
</tr>
<tr>
<td></td>
<td><strong>Change KBE Background</strong></td>
<td>Apply a custom image to the KBE background screen to replace the default Quest background.</td>
</tr>
<tr>
<td></td>
<td><strong>Font Support</strong></td>
<td>Select the fonts that you want to install, as required.</td>
</tr>
<tr>
<td></td>
<td><strong>DOS Commands</strong></td>
<td>Type the commands that you want to run after starting the KBE.</td>
</tr>
<tr>
<td></td>
<td><strong>Remember DOS Command</strong></td>
<td>Select if you want these commands to run each time the KBE starts.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source Media Name</strong></td>
<td>The name of the source media that you want to upload to the appliance.</td>
</tr>
<tr>
<td><strong>Source Media Type</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Source Media Path</strong></td>
<td>The path to the ISO file.</td>
</tr>
<tr>
<td><strong>Upload Source Media</strong></td>
<td>Click to upload the source media to the appliance.</td>
</tr>
</tbody>
</table>
Upload USMT page

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAIK or WADK Path</td>
<td>The path displayed reflects your setting of the WAIK or WADK Path on the General Settings page.</td>
</tr>
<tr>
<td>Upload USMT</td>
<td>Click to upload the USMT (User State Migration Tool) to the appliance.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDA Settings</td>
<td>SDA Hostname</td>
<td>The IP address of the system where the appliance is running.</td>
</tr>
<tr>
<td></td>
<td>SDA IP Address</td>
<td>The IP address segments of the system where the appliance is running.</td>
</tr>
<tr>
<td></td>
<td>Samba Share Password</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Remember Password</td>
<td>Select if you want to remember the Samba share password.</td>
</tr>
<tr>
<td></td>
<td>Test SDA Connection</td>
<td>Click to test the connection to the appliance, and to verify the Samba share password. If a connection fails, &quot;Connection failed&quot; appears in read. Similarly, &quot;Connection successful&quot; in green is displayed when the connection is successful.</td>
</tr>
</tbody>
</table>

Other Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAIK or WADK Path</td>
<td>Windows only. The path to the Windows Assessment and Deployment Kit (WADK) or Windows Automated Installation Kit (WAIK) files that you want to upload.</td>
</tr>
<tr>
<td>Theme</td>
<td>The theme of the Media Manager: Dark or Light.</td>
</tr>
</tbody>
</table>
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.

2. Under Select the features you want to install, select all of the features in the list.

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

Upload OS installation or source files

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

Uploading the source media requires:

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

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

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 SDA Media Manager to display the KACE SDA Media Manager.
3. In Media Manager, in the left pane, click General Settings.

The General Settings page appears on the right.

4. On the General Settings page, in the SDA Hostname field, enter the IP address of the KACE SDA.
5. In the SDA IP Address field, enter the IP address segments of the KACE SDA.
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, 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 SDA, and not the RSA.

11. Click Upload Source Media.

When the process completes, the image appears on the KACE SDA Source Media page.

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 KACE SDA.

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.

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 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 KACE SDA 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 image 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 into a KACE Boot Environment or a NetBoot environment to initiate the deployment. For Mac devices, see Imaging Mac devices.

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 into 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 KACE SDA 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.
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 KACE SDA inventory when the deployment is initiated.

1. On the left navigation pane, click 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.
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.

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 to display the Control Panel, then click General Settings to display the General Settings page.
2. 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 KACE SDA inventory when the deployment is initiated.

1. On the left navigation pane, click 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.
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.

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,KACE_SDA.

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.
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>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>my_domain</td>
<td>The name of the domain to which the script joins the devices.</td>
</tr>
<tr>
<td>admin user</td>
<td>The UID of the domain administrator with permission to join the devices to the domain.</td>
</tr>
<tr>
<td>admin password</td>
<td>The password of the domain administrator account.</td>
</tr>
<tr>
<td>primary_dns_IF</td>
<td>Optional: The IP address of the primary DNS server.</td>
</tr>
</tbody>
</table>

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 KACE SDA. 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 SMA inventory

When the KACE SDA 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping Status</td>
<td>Shows whether the appliance was able to reach this device.</td>
</tr>
<tr>
<td>PXE Status</td>
<td>Indicates whether this device (identified by the MAC Address) has ever requested a network boot from the appliance.</td>
</tr>
<tr>
<td>TCP Port Status</td>
<td>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.</td>
</tr>
<tr>
<td>UDP Port Status</td>
<td>Shows the state of the UDP ports scanned by the last Network Scan that included this device.</td>
</tr>
</tbody>
</table>
Collect the computer name

You can add a pre-installation task to collect the name of a target device.

1. On the left navigation pane, click **Deployments**, then click **System Images** to display the **Systems Images** page.
2. Select the image to which you want to add the task.
   The **System Image Detail** page appears.
3. Under **Installation Plan > Available Pre-installation Tasks**, move the **Collect Computer Name** task to the **Run Pre-installation Tasks** column.
4. Click **Save**.
Apply the computer name

You can assign the Apply Computer Name post-installation task to a deployment.

1. On the left navigation pane, click Deployments, then click System Images to display the Systems Images page.
2. Select the image to which you want to add the task.
   The System Image Detail page appears.
3. Under Installation Plan > Available Post-installation Tasks, move the Apply Computer Name task to the Run Post-installation Tasks column.
4. Click Save.

Delete devices from Device Inventory

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

1. On the left navigation pane, click Devices 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.

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.

Internet Explorer® requires ActiveX to start these programs on the local device. Other browsers do not support ActiveX. Telnet or VNC-Java Remote Control works with other browsers such as Safari® and Firefox®.

Table 3. Device action icons

<table>
<thead>
<tr>
<th>Remote access program</th>
<th>Host requirements</th>
<th>Client requirements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecureCRT</td>
<td>crt.exe</td>
<td>SSH client</td>
<td>Connects to devices by default using SSH on port 8443.</td>
</tr>
<tr>
<td>DameWare® Mini Remote Control</td>
<td>dwrcc.exe</td>
<td>DMRC client</td>
<td>Installs on the device the first time a connection is opened.</td>
</tr>
<tr>
<td>Explorer</td>
<td>explorer.exe</td>
<td>Windows/SMB share</td>
<td>Displays shared directories for the device. The full path of the start-up file is required.</td>
</tr>
<tr>
<td>Microsoft Remote Desktop</td>
<td>mstsc.exe</td>
<td>Remote Desktop</td>
<td>Opens a remote desktop session with the device. Only supports Windows devices.</td>
</tr>
<tr>
<td>Ping</td>
<td>ping.exe</td>
<td>None</td>
<td>Handles the connection request if the device is online.</td>
</tr>
<tr>
<td>PuTTY</td>
<td>putty.exe</td>
<td>None</td>
<td>Opens an SSH connection from the browser host to the target device.</td>
</tr>
<tr>
<td>Telnet</td>
<td>telnet.exe</td>
<td>None</td>
<td>Opens a session from the browser host to the target device.</td>
</tr>
<tr>
<td>TightVNC</td>
<td>vncviewer.exe</td>
<td>None</td>
<td>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).</td>
</tr>
<tr>
<td>VNC-Java Remote Control</td>
<td>None</td>
<td>VNC Java Client</td>
<td>Opens a session from the browser host to the target device.</td>
</tr>
</tbody>
</table>
Run an action on devices

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** to display the **Control Panel**, then click **General Settings** to display the **General Settings** page.
2. 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 KACE_SDA_host_name | KACE_SDA_host_IP
   ```

   where KACE_SDA_host_name and KACE_SDA_host_IP are the host name and IP address of the appliance. Some programs require a protocol, port, or URL. For example, Internet Explorer requires leading slashes to indicate a network address: \KACE_SDA_host_name.

   The executable_name is the full path to the program start-up file on the browser host, including the command-line parameters that the ActiveX components on the appliance use to open the session. 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 an action on devices**.

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** 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 KACE SDA 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 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 to display the Device Inventory page 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 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 SDA 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 SDA Media Manager on the Administrator device where you installed the KACE SDA. 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 KACE SDA.

You can import a KBE from a different location, by exporting the KBE from a different KACE SDA, and saving the exported .pkg file to the KACE SDA 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 SDA 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 SDA Media Manager. See Download and install the KACE SDA Media Manager. For more information about this tool, see About the Media Manager.

1. Run the Media Manager from Start > All Programs > Quest > KACE SDA 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 KACE SDA.
4. In the SDA IP Address field, enter the IP address segments of the KACE SDA.
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, under Linux Repository Cache Settings, 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 <KACE_SDA>/driver_packs folder to download the appropriate WinPE driver pack.

3. Manually copy the drivers to one of the following directories:
   •  \<KACE_SDA_IP>\drivers\kbe_windows_x86
   •  \<KACE_SDA_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 to display the Control Panel, then click General Settings to display the General Settings page.
2. Under Default KACE Boot Environments, select the new KBE.
3. Click Save.

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.

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

Some business environments can have strict policies and software that may keep the KACE SDA 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 KACE SDA 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 SDA 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 KACE SDA drivers share (\KACE_SDA\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 KACE SDA 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 SDA Media Manager.
   b. On the General Settings page, enter the KACE SDA 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 Dell drivers to the driver_postinstall directory.

The KACE SDA driver library is a network share that stores the drivers that the KACE SDA 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 KACE SDA hosts Samba shares, and provides three directories to help you manage drivers.

Ensure that you set the KACE SDA Samba Share Password on the General Settings page.

About adding drivers to the drivers_postinstall directory

- You can add non-Dell device drivers and Dell-specific device drivers that do not get updated from the Driver Feed to the drivers_postinstall directory.
- You can create the folders to organize the drivers under the drivers_postinstall directory using the Manufacturer name\OS Name\Model name 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 SDA 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](https://support.quest.com/kb/121734).
For sysprepped system images captured from an RSA, the corresponding drivers should be available on the KACE SDA and synchronized from the KACE SDA 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, select the Use driver feed (only with Sysprepped images) check box.
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 KACE SDA with the latest Dell device-specific driver packages automatically. 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 KACE SDA 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 KACE SDA performs nightly checks for the latest Dell 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 KACE SDA 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. Click Check for Updates.
5. 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.

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 KACE SDA and for images captured from a Remote Site Appliance (RSA).

You can manually add and remove drivers. For example, you can add Dell specific-device drivers that do not get updated from the Driver Feed or non-Dell 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 KACE SDA Driver Compatibility Report, which lists the drivers that the device requires compared to the drivers available on the Source Media.

1. Access the drivers_postinstall share directory of your KACE SDA appliance from the UNC path \\
\<KACE_SDA>\drivers_postinstall where <KACE_SDA> is either the IP address or the DNS name of the KACE SDA.
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 KACE SDA 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 KACE SDA restore share directory is the repository for storing packages and files that you can import to the KACE SDA.
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 KACE SDA from the UNC (Universal Naming Convention) path `\<KACE_SDA\>\drivers`, where `<KACE_SDA>` is either the IP address or the DNS name of the KACE SDA.
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 SDA 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 Dell device-specific drivers are not in the Driver Feed, to add non-Dell 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.

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 KACE SDA Administrator Console.
2. On the left navigation bar, click Devices 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.


- 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 KACE SDA from the UNC path \\<KACE_SDA\>\drivers where <KACE_SDA> is either the KACE SDA 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 SDA 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 KACE SDA 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 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 KACE SDA 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** 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 \KACE_SDA_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 KACE SDA 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-caching 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 the Dell 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_KACE_SDA_box>\drivers_postinstall\feed_tools \driver_feed_discovery_tool.vbs script on the device to get the model and manufacturer name.
- The Driver Feed adds the operating system and other hardware-related drivers to the drivers_post_install directory.
- The folder structure is <Manufacturer name>\<OS Name>\<Model name>.
Enable Driver Feed for scripted installations

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

You can 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. Click Check for Updates.
5. Optional: Click Cancel to close the page.
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.

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, select the Use driver feed (only with Sysprep’d images) check box.
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 non-Dell drivers, drivers from a different KACE SDA, 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 Dell 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 into the KACE Boot Environment (KBE). The KBE Main Menu loads on to the device when the device boots into 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 master image first in case you have to restore the image to the original device.
- Sysprep the image.
- Capture a sysprepped image to the KACE SDA and verify that there is enough space on the appliance for the image.

Capture system images

You can capture images with the KACE SDA or remote (RSA) appliances, after you boot the device into the KACE Boot Environment (KBE).

Run the Sysprep tool on the image to remove any system-specific settings before you boot the device into 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 into the KBE, you can access the built-in VNC remote control software to capture images from remote devices to the KACE SDA.

**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 into 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 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.

   - The KACE SDA assigns an ID to each captured system image.

**TIP:** Each system image captured with the KACE SDA 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 SDA) 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 SDA, 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**

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 native 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 KACE SDA automatically adds the `.wim` extension.
4. In **Image Source**, select the drive letter from where you are capturing the image.
   
   The KACE SDA 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 KACE SDA, you can edit that image on the System Image Detail page in the KACE SDA Administrator Console, but not in the KACE Remote Appliance Console. If that system image is captured on the KACE SDA 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 KACE SDA 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 and 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. When you finish your edits, click Cancel to roll back the changes, or Save to apply the changes to the image.
4. 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.
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.

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Name</td>
<td>Type the name that you want to assign to this system image.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Select the OS architecture used by the WIM image.</td>
</tr>
<tr>
<td>Wim File</td>
<td>Select the name of the WIM image file on the Samba clientdrop share.</td>
</tr>
</tbody>
</table>

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 SDA 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.

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 KACE SDA 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 KACE SDA (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 SMA 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 SMA 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 KACE SDA, 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 KACE SDA 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 KACE SDA 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 KACE SDA is physically located.

Deploy

- Add Pre/Mid/Post Installation tasks to your image on the KACE SDA.
- 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 KACE SDA post-installation tasks.
  - Use call when using .bat scripts in application tasks. For example: call myscript.bat
Capturing user states

The KACE SDA 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 KACE SDA or from the KACE SDA 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 KACE SDA. 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 SDA Media Manager is installed, run the Media Manager from **Start > All Programs > Quest > KACE SDA 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 SDA.
   - The RSA is synchronized with its KACE SDA, 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 SDA, or any linked RSA appliances.
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 SDA.
   - The RSA is synchronized with its KACE SDA, 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HostName/IP</td>
<td>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.</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain name if the device that you are scanning is connected to a domain.</td>
</tr>
<tr>
<td>User Name</td>
<td>Administrator privileges on the device that you are scanning.</td>
</tr>
<tr>
<td>Password</td>
<td>Administrator privileges on the device that you are scanning.</td>
</tr>
</tbody>
</table>

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. Terminate 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 SDA assigns an ID to each captured user state.
TIP: Each user state captured with the KACE SDA 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 SDA 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 KACE SDA, 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 SDA 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).

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.

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select Preseed Template</strong></td>
<td></td>
<td>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 <strong>Source Media</strong>.</td>
</tr>
<tr>
<td><strong>Template Data</strong></td>
<td><strong>Root Password</strong></td>
<td>Specify the root password for this configuration. If you want to disable root login for the target system, select <strong>Disable root login</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE</strong>: If you choose the server template, this is the only option that appears. All of these options are available with the desktop template.</td>
</tr>
<tr>
<td><strong>User Account</strong></td>
<td></td>
<td>To add a new user account using this method, select <strong>Create User Account</strong>. Any user accounts that are created this way are granted <strong>sudo access</strong>. Provide the full name, user name, and password for the account.</td>
</tr>
<tr>
<td></td>
<td><strong>Time Zone</strong></td>
<td>Select the time zone for the target system.</td>
</tr>
</tbody>
</table>
### Registration Data settings

The settings for the Registration Data vary depending on the operating system or the Source Media that was used.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Identifies the user to which the license is assigned.</td>
</tr>
<tr>
<td>Organization</td>
<td>Identifies the company or organization.</td>
</tr>
<tr>
<td>Product Key</td>
<td>Enter the product activation key.</td>
</tr>
<tr>
<td>Volume or Multi-Activation Licensing</td>
<td>For Volume licenses, enter the MAK (Multiple Activation Key) or KMS (Key Mgt System) setup key.</td>
</tr>
</tbody>
</table>

### Section Options and Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time Zone Server</strong></td>
<td>Specify the host name of the applicable time zone server.</td>
</tr>
<tr>
<td><strong>Language</strong></td>
<td>Select the locale for the target system.</td>
</tr>
<tr>
<td><strong>Desktop GUI</strong></td>
<td>Select the graphical user interface that you want to use on the target system: GNOME Desktop Environment, or KDE Desktop Environment, as applicable.</td>
</tr>
</tbody>
</table>

**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.
### 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter the user name for the administrator account. This account is created during the installation process.</td>
</tr>
<tr>
<td>Password</td>
<td>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.</td>
</tr>
<tr>
<td>Automatically log computer in to the Administrator account</td>
<td>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.</td>
</tr>
<tr>
<td>Disable automatic login after: device boots</td>
<td>Disables the automatic login of the administrator account after the specified number of boots.</td>
</tr>
</tbody>
</table>

### General settings

Sets the language and device screen settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Zone</td>
<td>Select the device’s time zone.</td>
</tr>
<tr>
<td>Regional and Language Option</td>
<td>Select the device default operating system language.</td>
</tr>
<tr>
<td>Screen colors</td>
<td>Select the device’s screen colors. The recommended setting is Windows default, unless you know that all of the target devices require the same setting.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Enter a device name or leave the field blank to generate a name automatically.</td>
</tr>
<tr>
<td>Workgroup</td>
<td>Join the device to a workgroup.</td>
</tr>
<tr>
<td>Domain</td>
<td>Select the check box if the target device is a part of a domain.</td>
</tr>
<tr>
<td>Create a computer account in the domain</td>
<td>Select the check box to add a device account in the domain.</td>
</tr>
<tr>
<td>Domain Administrator</td>
<td>Enter the name of the domain administrator.</td>
</tr>
<tr>
<td>Password</td>
<td>The administrator password for the domain.</td>
</tr>
</tbody>
</table>

NOTE: The administrator must have permissions to add devices to the domain. Disable the Local Administrator when a device joins 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**.

Modify scripted installation configuration file

You can modify the installation 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 KACE SDA Task Engine runs the tasks on the target devices in a reliable order and reports deployment feedback on the KACE SDA 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.

<table>
<thead>
<tr>
<th>Task type</th>
<th>Pre-installation task?</th>
<th>Mid-level task?</th>
<th>Post-installation task?</th>
<th>See topic:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Add Application</td>
</tr>
<tr>
<td>BAT Script</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Add BAT Script</td>
</tr>
<tr>
<td>Custom HAL Replacement</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Add Custom HAL Replacement</td>
</tr>
<tr>
<td>DISKPART Script</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Add DiskPart Script</td>
</tr>
<tr>
<td>Import Managed Installation</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Adding Managed Installation tasks</td>
</tr>
<tr>
<td>Naming Rule</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Add Naming Rule</td>
</tr>
<tr>
<td>Powershell Script</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Add PowerShell Script</td>
</tr>
<tr>
<td>Service Pack</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Add Service Pack</td>
</tr>
</tbody>
</table>
### 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.
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 **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.

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 **Notes**, add a note to identify the task.

6. 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 \( \text{all} \) 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 (SDA) with the KACE Systems Management Appliance (SMA) 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 SMA Administrator Guide:**
   --- | ---
   Link the KACE SMA with the KACE SDA and enable access to the Federation API settings. | *Enable appliance linking*
   1. In the KACE SMA 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
   4. Enable Federation API access to the linked KACE SDA.
   1. In the KACE SMA Administrator Console, select an Organization associated with a linked KACE SDA, and click **Settings**.
   2. On the Control Panel, click **Federation API Settings**.
   3. On the Federation API Settings page, select **Enable access**.
   4. Grant the Administrator role to the linked KACE SDA appliance.
   5. Repeat these steps for each Organization associated with the KACE SMA.

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 (SDA) is linked to the KACE Systems Management Appliance (SMA) from which you want to import one or more Managed Installations. For more information, see **Link appliances**.
NOTE: Each KACE SMA comes with a default organization (named Default). If your KACE SDA is linked with the Default organization on a KACE SMA, 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 SMA.
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 SMA, and ensure this field points to the correct KACE SMA.
   
   TIP: Your KACE SDA may be linked to multiple KACE SMAs.
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 SMA 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 SMA 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 KACE SDA, 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 (SMA) 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 **Post-installation Tasks** to display the **Post-installation 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Created</strong></td>
<td>The date and time when the task was created.</td>
</tr>
<tr>
<td><strong>Modified</strong></td>
<td>The date and time when the task was last modified.</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>The name of the task.</td>
</tr>
<tr>
<td><strong>Application</strong></td>
<td>The name of the application associated with the task.</td>
</tr>
<tr>
<td><strong>Runtime Environment</strong></td>
<td>The OS on which the application can be installed. See About runtime environments.</td>
</tr>
<tr>
<td><strong>Full Command Line</strong></td>
<td>The command line for the task, including any command-line parameters, as defined in the Managed Installation.</td>
</tr>
<tr>
<td><strong>Notes</strong></td>
<td>Additional information about the task.</td>
</tr>
</tbody>
</table>

**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.

**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.
Add Naming Rule

You can set up a naming database text file to assign names to devices and use a post-installation task to upload the file to the appliance.

Set up a naming database file using the following format:

```
mac_address = hostname
```

For example: 001122334455 = workstation55

The appliance uses the Workstation Name Changer tool, which is a compatible text file to assign a unique name to devices using the command-line parameters that you specify in the naming database. For more information, see http://newstuff.clarke.co.nz/wsname.

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 Naming Rule to display the Post-installation Task Detail page.
3. In Name, enter a logical name for the task, such as Assign name to workstation.
4. Next to Upload File, click Browse to select the appropriate file.
5. Select the Reboot Required check box to reboot the appliance and run the next task in the sequence.
6. Click Save.

The task is now available to assign to scripted installations, sysprepped system images, and non-sysprepped system image deployments.
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.
5. In Notes, add a brief description of the task.
6. Click Save.

   The task detail page closes, and the list page appears, showing the newly created task in the list.

7. On the list page, click the task name.
8. On the task detail page that appears, review the contents of the Full Command Line field, and make any changes, as required.
9. 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.

   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 Notes, add a brief description of the task.
6. Click Save.

   The task detail page closes, and the list page appears, showing the newly created task in the list.

7. On the list page, click the task name.
8. On the task detail page that appears, review the contents of the Full Command Line field, and make any changes, as required.
9. 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. Select the **Reboot Required** check box to reboot the appliance and run the next task in the sequence.
6. 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 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.

Add KACE SMA Agent Installer

You can download the KACE SMA 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 SMA Agent post-installation task to prevent a duplicate asset on the KACE SMA appliance if the KUID of the KACE SMA Agent that was installed on the target device was not maintained. The KACE SMA Agent software is in the \SMA_host_name\client\agent_provisioning directory. For an explanation of available command-line options and Agent configuration properties, see the KACE SMA Administrator Guide. The KACE SMA 5.4 Agent and higher 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 KACE SMA Agent Installer to display the KACE SMA Agent Installer Detail page.
3. In Name, change the name to identify the task, for example KACE SMA 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 Parameter, 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. 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. In Notes, add any notes to identify the task.
6. Click Save.
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 and scripted installations.

The process of creating tasks for MAC OS X and Windows 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 tasks for a Windows system image, select Choose Action > New Windows Task Group.
   b. To create a group of tasks for a Mac OS X system image, select Choose Action > New Mac OS X 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.

   i. 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: 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: 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.
About runtime environments

The runtime environment determines when the KACE SDA task engine runs the task.

<table>
<thead>
<tr>
<th>Runtime environment</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KACE Boot Environment (Windows)</td>
<td>Runs before the first boot of the operating system.</td>
</tr>
<tr>
<td>Windows</td>
<td>Runs after the first boot of the Windows operating system.</td>
</tr>
<tr>
<td>KACE Boot Environment (Mac OS X)</td>
<td>Runs before the first boot of the operating system.</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>Runs on the first boot of Mac operating system using a login hook.</td>
</tr>
<tr>
<td>KACE Boot Environment (Linux)</td>
<td>Runs before the first boot of the operating system.</td>
</tr>
<tr>
<td>Linux</td>
<td>Runs after the first boot of the Linux operating system.</td>
</tr>
</tbody>
</table>
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 KACE SDA 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 KACE SDA, you can edit that image on the **System Image Detail** page in the KACE SDA Administrator Console, but not in the KACE Remote Appliance Console. If that system image is captured on the KACE SDA 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 KACE SDA 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, 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:** 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:** 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:** 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 SDA 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, 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: 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: 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: 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, 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.
   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: 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: 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.
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 KACE SDA 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 KACE SDA, 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 📲.

   **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:** 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>To replace a file associated with the task (if available), click Replace, and select the appropriate file.</td>
</tr>
<tr>
<td>Parameters</td>
<td>Edit the task parameters, as required.</td>
</tr>
<tr>
<td>Notes</td>
<td>Add a note about the task. For example, John’s task to create a partition.</td>
</tr>
</tbody>
</table>

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

KACE SDA 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 to display the Automated Deployments page.
2. Select Choose Action > New Boot Action to display the Automated Deployment Detail page.
3. Under Boot Action Details:
   a. Assign a Name to the boot action.
   b. In the From box, select the KACE SDA 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 KACE SDA, 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:
Set default boot action

By default, devices that are not in the KACE SDA Device Inventory boot in to the KACE SDA Main Menu. For example, devices on your network that have been scanned display in your KACE SDA Network Inventory.

To set a default boot action:

1. On the left navigation pane, click **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.
can set the boot action to boot to the hard drive for devices that are not in the KACE SDA Device Inventory or Network Inventory.

1. On the left navigation pane, click **Settings** to display the **Control Panel**, then click **General Settings** to display the **General Settings** page.

2. Set the **Default Boot Action** to one of the following options:
   - **Boot to the KACE SDA Main Menu** for devices that are not in the KACE SDA 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** 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.
   - **Use driver feed (only with Sysprepped images)**: Select to enable the Driver Feed for sysprepped system images to obtain missing drivers. For more information, see Enable Driver Feed for system images. For Windows K-Images and WIM images, the Sysprepped field on the System Image Detail page indicates if an image is sysprepped.
   - **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.
   - **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** 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 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 Create a multicast DMG image deployment.

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 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 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 to view the deployments currently running.
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** 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 KACE SDA 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 KACE SDA Imaging Utility displays immediately and provides menu options to capture and deploy images.

Install a boot environment to a USB device

You can download the KACE Boot Environment (KBE) to a USB flash device for UEFI image deployments and for manual deployments when a device is not connected to the network.

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 Save.
7. Go to the directory that contains the downloaded .zip file and extract the files.
8. Insert the USB flash device in to the device from which you want to copy the image.
9. Go to the directory that contains the extracted files, and click install.exe.
   The Boot Environment page appears.
10. Select the flash drive, then select the file system format NTFS or FAT32/UEFI, and click Format and Install.
The boot environment is created on the flash device.

Copy an image to a USB flash device

After you create a bootable USB flash device with the KACE Boot Environment loaded, you can copy an image from the appliance to the USB device to deploy the image manually from the USB device.

Verify that the captured image that you want to deploy was captured from the C drive and not the D drive; otherwise, when you insert the USB device into the target device, the KACE SDA USB image installs the image on to the USB device instead of the C drive.

1. On the left navigation pane, click Deployments, then click System Images to display the Systems Images page.
2. Under Name, select the appropriate image to display the System Image Detail page.
3. Select the Create bootable USB flash drive image for this System Image check box.
4. Click Save.

A background process starts building the installer for the system image.

Instructions appear on the USB Flash Drive Installer page on how to get the USB image on to the flash drive.

Create a USB device driver directory

USB devices do not connect and mount to the drivers in the KACE SDA share directory. You can manually create the drivers share directory structure on the USB device, and copy the contents from the appliance drivers share directory to the USB device.

For versions 3.6 and higher:

1. Browse to usb:\KACE\ and verify that the drivers_postinstall directory exists. If not, create a drivers_postinstall directory.
2. Access the drivers_postinstall share directory on the appliance, for example: \KACE_SDA\drivers_postinstall.
3. Copy the contents from the feed_tools directory from the KACE SDA drivers_postinstall directory on to the USB device drivers_postinstall directory.

Add drivers to USB images

When you deploy an image from a USB device and the device does not connect and mount to the appliance drivers_postinstall share directory, you can manually copy the drivers to the USB device by importing the drivers to the appliance, and creating a mid-level post-installation task to add the drivers.
For information on adding drivers to a USB image deployment, see https://support.quest.com/kb/SOL111365, then log in to the KACE Systems Deployment Appliance Administrator Console.

1. On the left navigation pane, click **Settings** to expand the section, then click **Package Management**, and click **Import KACE SDA Packages**.
2. Select the package that you want to import.
3. Select **Choose Action** > **Import Selected**.
4. On the left navigation pane, click **Deployments**, then click **System Images** to display the **Systems Images** page.
5. Select the image to display the **System Image Detail** page.
6. Under **Installation Plan**, move the task that you created to add the drivers from the **Available Mid-Level Tasks** column to the **Run Mid-Level Tasks** column.
7. Add any other pre-installation and post-installation tasks to configure the deployment.

Adding the appliance IP address to Internet Explorer Trusted Sites section (on the target device with the image that you want to capture to a USB device) ensures that the post-installation tasks run successfully after the device reboots in to the OS.

8. Click **Save**.

Create a bootable USB flash drive image. See Install a boot environment to a USB device.

---

**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 device'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.

```
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 SDA to deploy system images, the list that appears shows the relevant images captured by the KACE SDA.
• 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 SDA.
```

4. Select **Restart Automatically after deployment** to reboot the device after the image is applied.
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 execute 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. 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**.

7. 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.

8. Assign tasks to the custom deployment, as required. For more information, see **Assign tasks to custom deployment**.
Imaging Mac devices

The KACE SDA provides the KACE SDA Imaging Utility, which enables you to capture images and to perform unicast deployments. You can perform multicast deployments from the KACE Systems Deployment Appliance Administrator Console if your network configuration supports multicast routing.

The KACE SDA Media Manager enables you to create a NetBoot image of the Mac OS X hard disk that the KACE SDA puts into memory. The NetBoot image enables you to capture the image as a system image for deployment. The integrated NetBoot server enables network-based image deployments to Mac devices that are on the same subnet as the KACE SDA. You can use the KACE SDA Remote Site Appliance (RSA) to boot images to devices on different subnets if the RSA is synchronized with the appliance.

Mac OS X deployments do not support user state migrations, scripted installations, or the driver share and driver compatibility report.

**IMPORTANT:** The KACE SDA does not support the new AFPS file system introduced in version 10.13.

Download the Media Manager for Mac OS X

You can download and install the KACE SDA Media Manager for Mac OS X from the appliance to a device where you have an administrator account. The Media Manager uploads the Mac OS X installation media to the KACE SDA, and creates images and the NetBoot environment to boot Mac devices in to the appliance.

Download the Media Manager to the device with the source media that you want to upload to the KACE SDA.

1. On the left navigation pane, click **Library** to expand the section, then click **Source Media** to display the **Source Media** page.
2. Select **Choose Action > Download Media Manager** to display the **Media Manager** page.
3. Click **Download for Mac OS X**.
4. The Media Manager downloads to the **Downloads** folder.
5. Select **System Preferences** from the Mac, then click and unlock **Security & Privacy** to make changes.
6. Select the **General** tab, and under **Allow applications downloaded from:**, select the **Anywhere** check box.
7. Click the **Media Manager** application to run it.

Create a NetBoot environment image

You can create a NetBoot environment image using the KACE SDA Media Manager for Mac OS X to boot Mac devices in to the appliance.
Reboot the device while leaving the time sync off. For more information on resolving the error while creating a NetBoot image, go to https://support.quest.com/kb/125875.

1. Open the Media Manager, and click **Create NetBoot Image**.
2. In **KACE SDA Hostname**, enter the host name or IP address of the appliance.
3. In **Source Media Name**, assign a name to identify the Mac OS version.
   
   The process first verifies that the name is unique on the appliance. If there is already a NetBoot image with the same name on the appliance, an error message appears, instructing you to change the NetBoot image name. The process can proceed with creating the image only after a successful verification of the provided image name.
4. **Versions 10.12, 10.11, 10.10, and 10.9 only.** In **Source Media Path**, click **Browse** to navigate to the Mac OS X installation source media to upload to the KACE SDA. For example: /Applications/Install OS X Yosemite.app.
5. **Versions 10.8 and 10.7 only**
   a. Right-click **Install OS X Mavericks.app**, then click **Show package contents**.
   b. Navigate to **Contents > SharedSupport**, and double-click **InstallESD.dmg** to mount the image to the desktop.
   c. In **Source Media Path**, click **Browse** to navigate to the mounted InstallESD volume.
6. Right-click **Install OS X Mavericks.app**, then click **Show package contents**.
7. Navigate to **Contents > SharedSupport**, and double-click **InstallESD.dmg** to mount the image to the desktop.
   
   The **OS X Install ESD** icon appears on your desktop.
8. In **NetBoot Password**, enter a password, and in **Confirm Password**, re-enter the password.
9. Click **Start Build**.

After the NetBoot image upload completes, the image is created and is available on the Source Media and Boot Environments pages.

Enable the NetBoot server, then capture the system image to use for deployment using the KACE SDA Imaging Utility. See Capture a Mac OS X image.

Enable the NetBoot server

You can enable the NetBoot server after you create the NetBoot image. The built-in NetBoot server enables the Mac OS X network boot process.

1. On the left navigation pane, click **Settings** to display the Control Panel, then click **General Settings** to display the General Settings page.
2. Under Default KACE Boot Environments, select a NetBoot image from the Mac OS X Intel (NetBoot) dropdown list.

   Ensure that you select the appropriate image, because images for various OS X versions can appear in the list. If there is only one OS X NetBoot image available, that image is selected by default.

   **TIP:** When you review the details of a NetBoot image using the Boot Environment Detail page, the Default field indicates if the selected NetBoot image is a default boot environment.
3. On the left navigation pane, click **Settings** to display the Control Panel, then click **Network Settings** to display the Network Settings page.
4. Select the Enable NetBoot Server (for Mac OS X clients) check box.

   Two BSDP field boxes appear.
5. Accept the default BSDP settings and click **Save**.
The Mac Boot Service Discovery Protocol (BSDP) is the standard extension of the DHCP, which enables the Mac network boot process.

6. From the Mac device, click the System Preferences icon, select Startup Disk, then select the appropriate KACE SDA Network to boot in to the NetBoot image and restart the OS.

The KACE SDA Imaging Utility appears.

7. Enter the NetBoot password.

Capture the image.

Customize the image before capture

You can customize the image on the source Mac device before capturing the image as a system image for deployment. You can add any non-native applications and files to the image that your standard corporate image requires.

1. Add any non-native applications and files to the image before you capture the image as a system image for deployment, for example, Acrobat or Oracle® applications.

2. Delete any Apple apps that you do not want to include in the system image for deployment to your corporate users, for example, GuitarBand® GameCenter.

3. To save space, delete the Mac OS X installer from the /Applications directory, if it exists. For example, /Applications/Install OS X Mavericks.app.

Capture the image as a system image for deployment.

Capture a Mac OS X image

The KACE SDA Imaging Utility enables you to capture Mac images for deployments from a device that has network booted in to the KACE SDA or the RSA.

You can capture a system image to use across multiple Mac hardware devices. Use the current version of the Mac OS image; older versions will cause an error because the certificate from Apple is no longer valid. You can change the date to a date prior to the expiry date on the device where you are creating the NetBoot environment and image.

1. Boot the target device in to the NetBoot image to display the KACE SDA Imaging Utility.

2. Double-click the KACE SDA Imaging Utility icon on the dock.

3. Select Capture image.

4. In Image Name, enter a name to identify the image on the appliance, such as ASR or DMG to identify the image on the KACE SDA as a Mac image.

5. Select the appropriate volume to capture. Typically, the volume is Macintosh® HD.

6. Select Capture Apple ASR format Image to capture the image in the Mac native image format.

7. Select Start Capture.

- The capture process adds an image entry to 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.

- The KACE SDA assigns an ID to each captured system image.
TIP: Each image captured with the KACE SDA 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 SDA) 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.

8. Click OK.

The Capture Finished prompt appears, and the appliance displays the image on the System Images page.

9. Select the image, then create a task sequence by assigning pre-installation and post-installation tasks. You can also add your own tasks to a shell script and run the script as a pre-installation or post-installation task.

Customize image before deployment

You can customize the Mac OS X image using the built-in pre-installation tasks, or add your own customizations to a shell script that you run as a pre-installation task.

1. On the left navigation pane, click Deployments, then click System Images to display the Systems Images page.

2. Select the appropriate Mac OS X image to display the System Image Detail page.

3. In the Installation Plan section, under Available Pre-installation Tasks, move any tasks that you want to run to the Run Pre-installation Tasks section.

You can add other tasks, such as collecting the device name. You can also edit any tasks on the System Image Detail page, if needed. After you finish adding and editing tasks, deploy the image.

Create a single HFS plus partition

You can assign the Create Single HFS + Partition on disk0 pre-installation task to create a single partition in HFS + format using either the APM or GPT format.

1. On the left navigation pane, click Deployments, then click System Images to display the Systems Images page.

2. Select the image to which you want to add the task.

The System Image Detail page appears.

3. Under Installation Plan > Available Pre-installation Tasks, move the Create Single HFS + Partition on disk0 task to the Run Pre-installation Tasks column.

4. Click Save.

Apply the Mac OS X ByHost preferences

You can add the Apply Mac OS X ByHost Preference post-installation task to remove application preference files stored in the Byhost directory on Mac devices.

The numbers in the filenames are the MAC address of the device or the UUID on the system.

1. On the left navigation pane, click Deployments, then click System Images to display the Systems Images page.

2. Select the image to which you want to add the task.
Change the Mac OS X computer name

You can assign the Example: Change Computer Name Mac OS X post-installation task to change the name of a Mac OS X computer. You can customize the built-in Example: Change Computer Name Mac OS X post-installation task template before using it.

1. On the left navigation pane, click Deployments, then click System Images to display the Systems Images page.
2. Select the image to which you want to add the task.
   The System Image Detail page appears.
3. Under Installation Plan > Available Post-installation Tasks, move the Example: Change Computer Name Mac OS X task to the Run Post-installation Tasks column.
4. Click Save.
Join device to an Active Directory Domain

You can assign the Example: Join Active Directory Domain Mac OS X post-installation task to join Mac OS X devices to an Active Directory Domain. You can customize the built-in Example: Join Active Directory Domain Mac OS X post-installation task template before using it.

1. Under Deployments, select the deployment to display the System Image Detail page.
2. Select the image to which you want to add the task.
   
   The System Image Detail page appears.
3. Under Installation Plan > Available Post-installation Tasks, move the Example: Join Active Directory Domain Mac OS X task to the Run Post-installation Tasks column.
4. Click Save.

Perform a unicast Mac OS X image deployment

For unicast deployments, you can use the KACE SDA Imaging Utility to capture and deploy Mac OS X images to devices that are on the same subnet as the appliance. You can download the Remote Site Appliance (RSA) to the KACE SDA to deploy images to devices on different subnets.

1. Boot the target device in to the NetBoot image to display the KACE SDA Imaging Utility.
2. Click the KACE SDA Imaging Utility icon in the Dock to start the application.
3. Click Deploy Image.
4. Select the image from the Image Name drop-down list.
5. Click Start Deploy.

Environment variables for any script

Quest KACE provides environment variables that you can use with the task engine to access the full path of hardware drives in the NetBoot environment, and to access the basename of device drives.

Quest KACE environment variables:

- $KACE_SYSTEM_DRIVE_PATH: Accesses the full path of the hardware drives in the NetBoot environment, such as /Volumes/SomeDrive.
- $KACE_SYSTEM_DRIVE_NAME: The basename of the system drive. For the above example, SomeDrive in /Volumes/SomeDrive.

Performing multicast Mac OS X image deployments

You can perform multicast Mac OS X image deployments from the KACE Systems Deployment Appliance Administrator Console if your network configuration supports multicast routing. The KACE SDA supports multicast
deployments for El Capitan, Yosemite, Mavericks, Mountain Lion, and Lion system images, versions 10.11, 10.10, 10.9, 10.8 and 10.7. You can assign boot actions to initiate the deployments. Multicast deployments from the KACE SDA Imaging Utility cannot trigger a boot action. Multicast deployments support only single-partition images.

For Mountain Lion, you can copy the source media on to a DVD, see http://www.itninja.com/question/how-to-create-mac-dvd-for-mountain-lion-10-8-for-k2000-netboot.

Create a multicast DMG image deployment

You can create a boot action to initiate deployments for Mac OS X DMG images on the next network boot. The target devices must be on the same network as the KACE SDA.

1. On the left navigation pane, click Deployments to display the Automated Deployments page.
2. Under Name, select the boot action to display the Automated Deployment Detail page.
3. Under Options, select Run at next boot to deploy the image on the next network boot.
   
   You cannot schedule multicast deployments to run later for DMG images.
4. Optional: Under Type, select Multicast, then click Show advanced settings.
   
   • 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.
   
   • In Transmission Rate, lower the default transmission rate from its default of 8MB for higher transfer reliability.
   
   For complete information about multicast settings, see Edit the default multicast settings.
5. Under Devices, enter one or more MAC addresses to add devices that are not in the inventory, then click Next.
6. Click Save.

7. Reboot the device using one of the following options:
   
   • If the device is on: Under System Preferences, select the Startup Disk, then select the KACE NetBoot Environment.
   
   • If the device is not on: Power on the device, then press the Option key, and click KACE NetBoot Environment.

You can view the deployment progress. For more information, see View the Mac OS X multicast deployment progress.

View the Mac OS X multicast deployment progress

The KACE Systems Deployment Appliance Administrator Console displays the status of multicast deployments and the progress of the tasks running for the deployment on the Progress > Automated Deployments page.

You cannot view the status of multicast deployments from the target device.

1. On the left navigation pane, click Progress to display the Automated Deployment Progress page.
2. Select the boot action to display the Boot Action Detail page.
3. Under Devices, click Details next to the device MAC address to display the progress of the tasks running.
You can view the success or failure of completed multicast Mac image deployments on the Audit Log > Automated Deployments page.

NOTE: If a deployment fails, re-deploy the image separately to a device where the deployment failed.

View the Mac OS X multicast deployment log files

You can view the log files for Mac OS X multicast deployments.

1. On the left navigation pane, click Settings, then click Appliance Logs to display the Appliance Logs page.
2. Under KACE SDA Server, click Multicast Log to view the multicast deployment log files.
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 SDA and link the RSA using the license key that comes with your KACE SDA. When you link the RSA to the 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

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KACE SDA</td>
<td>Install and configure the KACE SDA to download the RSA.</td>
</tr>
<tr>
<td>RSA License</td>
<td>Use the same KACE SDA license key sent to you by Quest KACE.</td>
</tr>
<tr>
<td>Virtual Machine host</td>
<td>See the RSA host system requirements.</td>
</tr>
<tr>
<td>Network settings</td>
<td>Assign a static IP address and (optional) host name to the RSA.</td>
</tr>
<tr>
<td></td>
<td>Save the RSA data on the RSA or to a virtual disk.</td>
</tr>
<tr>
<td>Optional: LDAP</td>
<td>Use the LDAP server IP address or host name.</td>
</tr>
<tr>
<td>Network boot configuration</td>
<td>For Windows devices: The DHCP server scope that directs the network boots to the RSA on the remote DHCP scopes.</td>
</tr>
</tbody>
</table>
RSA host system requirements

The device at the remote site that hosts the RSA must meet the following requirements:

Table 5. RSA host system requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Machine</td>
<td>Ensure that the virtual host software is installed:</td>
</tr>
<tr>
<td></td>
<td>- VMware:</td>
</tr>
<tr>
<td></td>
<td>- ESX®/ESXi™ 5.5 or later</td>
</tr>
<tr>
<td></td>
<td>- vSphere 4</td>
</tr>
<tr>
<td></td>
<td>- Hyper-V:</td>
</tr>
<tr>
<td></td>
<td>- Windows 2012 or 2012 R2</td>
</tr>
<tr>
<td>Hardware</td>
<td>2GHz processor (Intel®-VT or AMD-V™ capable), 4GB RAM, and 1TB of free disk space.</td>
</tr>
<tr>
<td>Ports</td>
<td>Ports 22 and 80 must be open.</td>
</tr>
</tbody>
</table>

Install the RSA on a VMware or Hyper-V host

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® or Microsoft® Windows® Hyper-V® host, see the Setup Guide for VMware Platforms and Setup Guide for Hyper-V Platforms. You can also consult the VMware or Microsoft Windows documentation for instructions on opening an OVF 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 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 KACE SDA 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 SDA to an RSA

Linking the appliance to the Remote Site Appliance (RSA) enables the KACE SDA to be aware of the RSA. Linking enables you to access the RSA and the KACE SDA from the same session if the user name and password on the linked appliances match.

1. On the left navigation pane, click Settings 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 SDAs. 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.
Add and sync the RSA to the appliance

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 SDA; however, there is no limit to the number of RSAs that you can add to the KACE SDA.

You can synchronize scripted installations, system images, and user states to the RSA. 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. Select Choose Action > New to display the Add a Remote Site Appliance page.
3. In Remote Site Appliances, select the IP address for the RSA.
4. Click Next.
   The KACE SDA connects to the RSA and registers it as an extension. When the process completes, the Remote Site Detail page appears.

   NOTE: Each RSA has its own Remote Site Detail configuration page.

5. 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.

6. 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 SDA Administrator console, any system images already captured by the RSA, and not the KACE SDA, 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 SDA.
   - Any images that are captured by the associated KACE SDA appear in the list and can be selected or cleared, as required.

7. Scroll down to Dependencies and click Show. 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 SDA, and the USMT Toolkit is already uploaded to the KACE SDA, 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 SDA, see Upload USMT software from Media Manager.

8. If you are viewing this page for an existing RSA, to verify if the RSA version matches the KACE SDA 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 SDA.

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: 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 SDA license with the RSA (if applicable), click Sync License.

   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 SDA, select Choose Action > Sync Data.

9. Click Save and Sync.

   Save and Sync is disabled if:
   ▪ An off-board storage migration is in progress.
   ▪ If the RSA and linked KACE SDA 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 SDA. 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.

The RSA is ready for network booting.

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 more information, see the following topics:
   ▪ Capture system images
   ▪ Capture a Mac OS X image
   ▪ Assign tasks to system deployment
   ▪ Deploy the image manually
   ▪ Scan user states
   ▪ Create USMT Scan Template
   ▪ Importing and exporting appliance components

   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 SDA or Remote Site Appliance (RSA) components, such as drivers, network inventory, boot environments, and tasks to a different network location, a different KACE SDA, 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 `\KACE_SDA_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 KACE SDA, or a Remote Site Appliance (RSA) at regular intervals if you created a package for the components and stored the package in the KACE SDA 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 KACE SDA.

**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 KACE SDA 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule Run</td>
<td>Select the interval and time for the transfer.</td>
</tr>
<tr>
<td>Offboard Package Transfer Protocol</td>
<td>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.</td>
</tr>
<tr>
<td>Offboard Package Transfer Server</td>
<td>Type the host name or IP address of the device to which the files are transferred.</td>
</tr>
<tr>
<td>Path or Share Name</td>
<td>Type the path to the directory or share name for the transfer. Enter the Samba share name without any forward or backward slashes.</td>
</tr>
<tr>
<td>User Name</td>
<td>Type the user name for the appliance to use. Entering the user name requires write-access to the remote location.</td>
</tr>
<tr>
<td>User Password</td>
<td>Type the password required to access the remote location.</td>
</tr>
<tr>
<td>Cleanup Restore</td>
<td>Delete the files automatically from the restore share directory on the KACE SDA or an RSA after a successful transfer.</td>
</tr>
</tbody>
</table>

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 SDA 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 `\\[KACE_SDA|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 KACE SDA 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 KACE SDA.

**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 KACE SDA 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 KACE SDA, such as drivers, network inventory, boot environments, and tasks to a different network location. You can also export system images from a Remote Site Appliance (RSA). This is useful to back up and restore components.

**IMPORTANT:** Only system images 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 KACE SDA 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 \[KACE_SDA|RSA\]_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, terminate 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 KACE SDA through the tether and clear the error.

**Package file names**

You can import and export KACE SDA 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.

<table>
<thead>
<tr>
<th>File contents</th>
<th>File name</th>
<th>File extension</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix</td>
<td>Syntax</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pre-installation task</td>
<td>PR</td>
<td>_&lt;ID&gt;&lt;Unix_time_stamp&gt;&lt;microseconds &gt;.pkg</td>
<td>PR33_1519839187_5248.pkg</td>
</tr>
<tr>
<td>Mid-level installation task</td>
<td>MI</td>
<td>_&lt;ID&gt;&lt;Unix_time_stamp&gt;&lt;microseconds &gt;.pkg</td>
<td>MI26_1519792380_3567.pkg</td>
</tr>
<tr>
<td>Post-installation task</td>
<td>PO</td>
<td>_&lt;ID&gt;&lt;Unix_time_stamp&gt;&lt;microseconds &gt;.pkg</td>
<td>PO17_1519831620_4922.pkg</td>
</tr>
<tr>
<td>Database package</td>
<td>DB</td>
<td>_&lt;ID&gt;&lt;Unix_time_stamp&gt;&lt;microseconds &gt;.pkg</td>
<td>DB12_1519822800_1546.pkg</td>
</tr>
<tr>
<td>KImage</td>
<td>KI</td>
<td>_&lt;ID&gt;&lt;Unix_time_stamp&gt;&lt;microseconds &gt;.pkg</td>
<td>KI56_1519827865_4213.pkg</td>
</tr>
<tr>
<td>Scripted installation</td>
<td>SI</td>
<td>_&lt;ID&gt;&lt;Unix_time_stamp&gt;&lt;microseconds &gt;.pkg</td>
<td>SI59_1519834064_2984.pkg</td>
</tr>
<tr>
<td>Driver package</td>
<td>DR</td>
<td>_&lt;ID&gt;&lt;Unix_time_stamp&gt;&lt;microseconds &gt;.pkg</td>
<td>DR15_1519823348_3284.pkg</td>
</tr>
<tr>
<td>File contents</td>
<td>File name</td>
<td>File extension</td>
<td>Example</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------</td>
<td>----------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>Network inventory package</td>
<td>NI</td>
<td>NI&lt;ID&gt;&lt;Unix_time_stamp&gt;&lt;microseconds&gt;</td>
<td>NI36_1519814733_1976.pkg</td>
</tr>
<tr>
<td>Custom deployment</td>
<td>CU</td>
<td>CU&lt;ID&gt;&lt;Unix_time_stamp&gt;&lt;microseconds&gt;</td>
<td>CU88_1519794461_5889.pkg</td>
</tr>
<tr>
<td>Boot environment</td>
<td>BE</td>
<td>BE&lt;ID&gt;&lt;Unix_time_stamp&gt;&lt;microseconds&gt;</td>
<td>BE52_1519798711_2802.pkg</td>
</tr>
<tr>
<td>Network scan</td>
<td>NS</td>
<td>NS&lt;ID&gt;&lt;Unix_time_stamp&gt;&lt;microseconds&gt;</td>
<td>NS37_1519818962_3011.pkg</td>
</tr>
<tr>
<td>User State</td>
<td>US</td>
<td>US&lt;ID&gt;&lt;Unix_time_stamp&gt;&lt;microseconds&gt;</td>
<td>US27_1519805822_2846.pkg</td>
</tr>
<tr>
<td>Task Group</td>
<td>TG</td>
<td>TG&lt;ID&gt;&lt;Unix_time_stamp&gt;&lt;microseconds&gt;</td>
<td>TG16_1519811097_1390.pkg</td>
</tr>
<tr>
<td>USMT (User State Migration Tool) Scan template</td>
<td>ST</td>
<td>ST&lt;ID&gt;&lt;Unix_time_stamp&gt;&lt;microseconds&gt;</td>
<td>ST39_1519808167_5225.pkg</td>
</tr>
</tbody>
</table>
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 KACE SDA. You can migrate data on the KACE SDA to an offboard-storage device, and migrate data stored on the virtual KACE SDA 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. Go to the 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.

2. Mouse over any section in the 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 KACE SDA 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 KACE SDA. 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 KACE SDA 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 KACE SDA 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 KACE SDA 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 KACE SDA 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 SDA 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 Virtual KACE SDA 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 Virtual KACE SDA 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 Virtual KACE SDA or RSA is unavailable during migration.

1. On the left navigation pane, click **Settings** 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 SDA 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 KACE SDA or RSA as long as the data does not exceed the onboard storage capacity. The KACE SDA 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.


1. On the left navigation pane, click **Settings** 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 KACE SDA 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 KACE SDA 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](http://www.itninja.com/community/dell-kace-k2000-deployment-appliance) website for device-specific configuration instructions that are not available from the KACE SDA.

1. On the left navigation pane, click Settings 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 KACE SDA 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 KACE SDA 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 KACE SDA. 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 KACE SDA (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 KACE SDA by its own private network

The KACE SDA 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 KACE SDA front-end network. Connecting the storage server over the KACE SDA front-end network effectively cuts your network bandwidth in half, making a 1 GB network a 500 MB network. During capture/deployment the data must come to the KACE SDA from the storage server and then from the KACE SDA 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 KACE SDA should be connected on the same physical switch (VLAN/subnet). Any latency of packets caused by 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 KACE SDA 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 KACE SDA, 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 KACE SDA 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 KACE SDA 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 KACE SDA 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 KACE SDA Advisor, which is a utility that queries the database of your KACE SDA, to gather information about your appliance in an HTML report to help with gathering data or troubleshooting the KACE SDA. For more information, or to download the KACE SDA 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 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](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** 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** 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. 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**.

Quest KACE Technical Support now has remote access to your appliance.

### 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** 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 KACE SDA.

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.

   **NOTE:** If the Boot Manager does not load, select a different interface type. See **Change the Boot Manager interface**.

The target device successfully boots.
Change the Boot Manager interface

The Boot Manager displays immediately after you network boot devices to select the architecture for the KACE Boot Environment (KBE) that supports the device's hardware. You can select a menu or text interface for the Boot Manager.

1. On the left navigation pane, click Settings to display the Control Panel, then click General Settings to display the General Settings page.
2. In the Boot Manager Style drop-down list, select the appropriate option:
   - Graphical Menu: This menu supports using arrow keys.
   - Text Menu: This menu supports older devices that have NICs that do not support integrated graphics, but allows using arrow keys.
   - Basic: This menu does not support using arrow keys to select menu options. Enter the letter combination corresponding to the boot environment that you need.
3. Click Save.

The Boot Manager interface is changed for all devices that boots in to the appliance.

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 to display the Control Panel, then click General Settings to display the General Settings page.
2. 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** to display the **Control Panel**, then click **General Settings** to display the **General Settings** page.

2. 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. 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**.

### Change the network delay time

You can change the amount of time that the appliance waits for the DHCP server to respond after the network drive is mounted. The connection time occurs before proceeding with the boot process when booting from the KACE Boot Environment (KBE).

You can change the default **KBE Network Bringup Delay** time, which is 15 seconds, in cases where you have a high-latency network, and devices might not be able to boot in to the KACE Boot Environment (KBE) within the allocated time.

1. On the left navigation pane, click **Settings** to display the **Control Panel**, then click **General Settings** to display the **General Settings** page.

2. In **KBE Network Bringup Delay**, enter the duration in seconds.
   
   Increasing the network delay time in 5-second intervals provides more time to access the KBE. In high latency networks, you may need to increase the delay to ensure that there is enough time to fully load the KBE.

3. 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 KACE SDA 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 KACE SDA 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 downloaded as a single `.tgz` file.
4. Extract the files to view its contents.
5. 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 KACE SDA 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


Table 6. Appliance Logs

<table>
<thead>
<tr>
<th>Log type</th>
<th>Log name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>System Messages</td>
<td>Displays system messages from the operating system running the KACE SDA.</td>
</tr>
<tr>
<td></td>
<td>Outgoing Mail Log</td>
<td>Displays logs of email messages sent from the KACE SDA.</td>
</tr>
<tr>
<td></td>
<td>Data Storage</td>
<td>Displays external storage configurations on the KACE SDA.</td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>Web Server</td>
<td>Access Log</td>
<td>Displays the request log file for the Apache™ Web server.</td>
</tr>
<tr>
<td>Log type</td>
<td>Log name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Error Log</td>
<td>Displays the error log file for the Apache Web server.</td>
<td></td>
</tr>
<tr>
<td>KACE SDA Server</td>
<td>Output Log</td>
<td>Displays messages from system updates, cleanup tasks, offboard storage updates, driver feed and documentation updates.</td>
</tr>
<tr>
<td>Error Log</td>
<td>Displays errors from system updates, cleanup tasks, offboard storage updates, driver feed updates and documentation updates.</td>
<td></td>
</tr>
<tr>
<td>Multicast Log</td>
<td>Displays program execution details about multicast imaging jobs.</td>
<td></td>
</tr>
<tr>
<td>File Servers</td>
<td>TFTP Transfer Log</td>
<td>Displays KACE SDA boot errors and requests.</td>
</tr>
<tr>
<td>NETBIOS Name Server</td>
<td>Displays messages from the NetBIOS server on the KACE SDA.</td>
<td></td>
</tr>
<tr>
<td>Windows File Server</td>
<td>Displays messages from the Samba service, which shares the folders on the KACE SDA.</td>
<td></td>
</tr>
<tr>
<td>Task Processor</td>
<td>Output Log</td>
<td>Displays messages from the KACE SDA server task processor, which runs tasks in the background. The tasks that can be processed include:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Importing source media that the Media Manager uploads.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Importing a WIM or K-Image.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Rebuilding driver cache.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Rebuilding a KBE environment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Creating and updating scripted installations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Synchronizing data with an RSA (Remote Site Appliance).</td>
</tr>
<tr>
<td>Error Log</td>
<td>Displays errors in the tasks that the KACE SDA server task processor performs.</td>
<td></td>
</tr>
<tr>
<td>Log type</td>
<td>Log name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Privileged Action Server    | Output Log     | Displays output from the privileged action server, which is tasks that require elevated permissions. These tasks include:  
|                             |                | • Changing any KACE SDA 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 KACE SDA 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.                             |
|                             | Export Log     | Displays output and errors of any export jobs.                             |
Log type | Log name | Description
--- | --- | ---
**Download Logs** | Downloads the KACE SDA 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.

### 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 KACE SDA 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.


   The appliance shuts down.

To enable the appliance, press the power switch.

Reboot the appliance

You can reboot the KACE SDA 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 KACE SDA 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 KACE SDA 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 \<KACE_SDA>\restore share.
2. Copying the data from 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 hang the process, 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 KACE SDA 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 `<KACE_SDA>\drivers` share. As of KACE SDA version 3.5, there should be fewer items in these folders, as driver feed drivers (and manually built driver feeds) reside in `<KACE_SDA>\drivers_postinstall` instead of `<KACE_SDA>\drivers`.

Things to consider

Evaluate the total size of the items to be exported and the available disk space on the KACE SDA. Each exported object is placed in the KACE SDA 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 KACE SDA. Once the available free space falls below 20 GB, many standard operations on the KACE SDA 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 KACE SDA).

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 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

For 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 KACE SDA. 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 KACE SDA restore share, freeing up needed space on the disk. Using this option is a recommended way to save space on the KACE SDA, 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 KACE SDA 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 KACE SDA software.

View the appliance version

You can view the version of your KACE SDA 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 KACE SDA link in the lower-left corner 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 (RSAs) 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 KACE SDA 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 KACE SDA 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 SDA is on an earlier version, upgrade to the minimum version and enable SSH before proceeding with the installation. Each time you update the SDA software, update the RSA 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 SDA.

Administrator Console
The web-based interface to control the KACE Systems Deployment Appliance (KACE SDA).

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 KACE SDA and enables the selection of the KACE Boot Environment (KBE).

Boot Manager style
The Boot Manager interface can display as a graphical menu, or as a text menu for devices that do not have a network interface card that supports integrated graphics.

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 KACE SDA.

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 KACE SDA that uses scripts to manage objects such as disks or partitions.

Driver Feed
A built-in tool that adds the latest Dell 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 KACE SDA 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 KACE SDA 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 KACE SDA 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 KACE SDA 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 (SDA) problems that administrators encounter. Visit https://support.quest.com/resources/kb.
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.

mid-level task
A mid-level task is a post-installation task that runs in the KACE Boot Environment runtime environment.

Media Manager
A KACE SDA 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.

Native imaging
OS-specific formats such as Microsoft WIM and Apple DMG images that are compatible with the KACE SDA.

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
A KACE SDA setting that enables external reporting programs to connect to and query the KACE SDA database.

offboard storage
Uses an external NAS device to expand the KACE SDA internal storage capacity. It also expands Remote Site Appliance (RSA) and Virtual KACE SDA 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.

Package Management
A KACE SDA feature that enables importing, exporting, and transferring KACE SDA 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 SDA that downloads directly from the KACE SDA and uses the same KACE SDA 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.

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 KACE SDA 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 KACE SDA 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.
WIM (Windows Imaging Format)
A KACE SDA 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
A KACE SDA 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 provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. 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

© 2020 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser’s personal use without the written permission of Quest Software Inc.

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

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.

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

<table>
<thead>
<tr>
<th>Icon</th>
<th>Legend</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td><strong>CAUTION:</strong> A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.</td>
</tr>
<tr>
<td>![Icon]</td>
<td><strong>IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:</strong> An information icon indicates supporting information.</td>
</tr>
</tbody>
</table>

KACE Systems Deployment Appliance Administrator Guide

Updated - February 3 2020

Software Version - 7.2
A
about the Media Manager 44
action icon
about built-in programs 58
opening a VNC session with action icon 59
performing actions on devices 59
setting default program 59
Apple certificate error
resolving expired certificate error 131
appliances
migrating 31, 31
authentication
configuring LDAP server 35
testing LDAP 37
automated deployments
viewing deployment log 124
viewing deployment progress 123
viewing image details 124
B
boot actions
booting to KBE 118
creating a boot action 118, 118
defining behavior 119
delete image for 122
deploying boot actions 118
modifying 119
running at next network boot 119
setting default boot action 119
boot environment
deleting KBE or NetBoot 150
Boot Manager
about default timeout 158
changing interface 158
changing timeout 128, 158
selecting interface 128
testing device network boot 157
troubleshooting 157
booting to local drive 118
brute-force attacks
preventing 40
C
capturing system images 77
capturing system images, best practices for Windows 83
Command Line Console
changing passwords 24
community string
creating unique string 38
components
importing and exporting 144
configuring the KACE SDA 20
about data sharing 28
changing the date and time 26
changing the default passwords 23
configuring network settings 20
enabling link aggregation 27
modifying initial network settings 21
sharing basic data usage 28
sharing detailed data usage 29
synchronizing the KACE SDA system clock 26
creating custom deployments 130
custom deployments 130
creating a custom deployment 130
modifying a custom deployment 130
custom HAL replacement
adding as a mid-level task 101
D
dashboard
about 19
customizing 19
data
exporting and importing 144
date and time
configuring 26
delete
assigned scripted installation 150
deleting
boot environments 150
post-installation tasks 151
pre-installation tasks 151
source media 150
system images 150
deployments
about automated deployments 50
about manual deployments 50
choosing deployment type 50
creating multicast WIM deployments 122
delete boot action 122
deploying scripted installations 50
deploying system images 50
imaging Mac devices 131
scheduling 121
devices

about device inventory 52
about driver compatibility report 55
about network inventory 52
adding devices from a csv file 52
adding to deployment 53
deleting device inventory 57
deleting network inventory 57
deploying to devices in KACE SMA inventory 55
issuing a Send Wake-on-LAN 54
powering on 54
running a network scan 52
scanning all devices on network 53
scanning network for all devices 52
unregistering devices 57
using MAC address to add 53
viewing details 55
DHCP
configuring offboard server 43
enabling DHCP server 42
disk space
viewing available 149
DiskPart scripts
using common commands 102
documentation
searching the KACE SDA Help system 15
domain
joining devices 54
driver feed
disabling 68, 75
downloading driver packages 76
enabling driver feed system images 75
enabling driver feed to automate updates 67
enabling for scripted installations 75
folder structure 74
drivers
about network 71
about operating system 74
add to scripted installation deployments 67
add to system images 66
adding drivers
network drivers 70
storage drivers 70
adding to USB deployments 126
copying drivers manually 126
create folders for device-specific drivers 68
displaying devices requiring drivers 73
downloading network drivers 72
enabling driver feed to automate updates 67
exporting 74
importing 69, 73
importing large files 68
installing as post-installation task 71, 76
installing drivers 67, 68, 71, 76
installing missing system image 75
installing to the appliance 67
KBE drivers 69
managing network and OS 66
network drivers

add manually 70
obtaining model and manufacture name 74
on the appliance 67
re-caching 70, 74
storage drivers
add manually 70
updating 63
uploading as a ZIP file 71, 76
view missing drivers 71
viewing compatibility report 73

E
error handling
configuring continue on errors 113
configuring prompt on errors 113
displaying cancel button on target device 113
export
components 146
file naming conventions 147
transferring packages to remote location 144
exports
scheduling 144
external storage
about device storage capacity 153, 153
best practices 153
migrating appliance data 153
migrating virtual appliance data 151
reverting data 152

F
failed tasks
editing 124
editing Tasks.xml file 124
retrying 124
filter
lists 14

G
getting started
about KACE SDA components 12
about network connectivity 13
about the license key 13
adding administrator password 13
adding registration data 13
adding timezone 13
changing the default theme for the appliance 17, 17
configuring language settings 17
default theme 17
default theme for the appliance 17
for the appliance 17
logging in to the appliance 13
preparing for deployment 11
tasks for using the KACE SDA 11
themes 17

H
Help system and PDF 15
images
- capturing 77
- capturing from the KACE SDA Main Menu 77
- capturing system images, best practices for Windows 83, 83
- capturing WIM images 77, 80
- editing K-Images 80
- editing WIM images 80
- importing WIM images 82, 82
- preparing for capture 77
- import components
- file naming conventions 147
- importing components 146
- installing configuring virtual disk space 140
- RSA 140

K
KACE SMA
- applying KUID to Agent 56
- deploying to inventory 55
KBE
- building Linux KBE 63
- building Windows KBE 62
- building Windows KBE, best practices 64
- required tools 62
- setting default 64, 141
KUID
- applying as a post-installation task 56

L
labels
- applying to component 60
- deleting from appliance 61
- organizing components 60
- removing components 60
- viewing components by label 61
language settings
- optional font support 17
LDAP
- server configuring 35
- LDAP server
- using external LDAP server 34
license key
- obtaining 13
link aggregation
- enabling 27
linking
- adding names and keys 30
- disabling linked appliances 31
- enabling appliance linking 30
- linking the RSA 29
lists
- searching 14
local administrator
- adding account 34

local authentication
- using default 34
log files
- viewing 160

M
Mac devices
- about multicast deployments 136
- adding devices to deployment 137
- applying computer name 135
- booting across subnets 131
- changing device name 135
- changing multicast timeout 137
- changing multicast transmission rate 137
- collecting computer name 134, 135
- initiating deployment at next boot 137
- join Active Directory domain 136
- viewing deployment progress 137
- viewing multicast OS X log files 138
Mac image
- customizing image before capture 133
- Mac image deployment
- adding ByHost Preferences post-installation task 134
- creating NetBoot image 131
- downloading Media Manager for Mac OS X 131
- enabling NetBoot server 132
- performing a unicast deployment 136
- running KACE environment variables 136
Mac images
- capturing 133
- customizing before deployment 134
- managing disk space
- deleting boot environments 150
- deleting post-installation tasks 151
- deleting pre-installation tasks 151
- deleting source media 150
- deleting system images 150
- formatting the C drive 79
- managing user states
- about online and offline user state migrations 86
- creating a USMT scan template 87
- uploading USMT from Media Manager 86
- uploading USMT from the appliance 86
manual deployments 125
- changing boot manager timeout 128
- copying drivers to USB device 126
- copying image to USB device 126
- creating a bootable flash device 127
- deploying image from KBE 128
- network boot device 128
- viewing completed deployments 129
- viewing deployments in progress 129
Media Manager
- about 44
- downloading 43
- running 86
- uploading OS installation files 49
mid-level tasks
adding a PowerShell Task 108
adding a shell script 109
adding a Windows script 110
adding applications 100
adding as batch script 101
adding custom HAL replacement 101
adding Managed Installations 103, 105
assigning to custom deployment 116
assigning to scripted installation deployment 115
assigning to system deployment 113
migrating appliances 31, 31
modifying custom deployments 130
multicast deployments
  editing default multicast settings 122

N
network scan
  configuring IP range 52
  running 52
  scanning all devices on network 53
  scanning only live devices on network 53

O
offboard access
  enabling 40
offboard storage
  about virtual disk capacity 151
  adding virtual disk 151
  best practices 153
  configuring network storage device 153
  migrating virtual appliance data 151
  migrating Virtual KACE SDA and RSA data 151
  reverting data 152

P
package management
  about the index.xml file 144
  displaying available packages 145
  enabling off-board package transfer 144
  exporting components 144, 146
    file naming conventions 147
  importing and exporting KACE SDA components 144
  importing components 146
    file naming conventions 147
  uploading packages for import 145
package management queue
  removing files 144
  viewing scheduled jobs 144
packages
  about packages containing drivers 145
  deleting files 144
  downloading and installing drivers 76
  importing drivers 126
  size limitation 145
  transferring automatically 144

partitions
  assigning new drives 102
  creating new partitions 102
  creating single boot partition 102
  running DiskPark script to erase data 102
passwords
  changing Samba share 25
  changing the Administrator password 23
  changing the default passwords 23
  enabling Boot Manager authentication 26
  setting VNC 26
PDF of Help system 15
post-installation tasks
  adding a PowerShell Task 108
  adding a provisioning package 108
  adding a shell script 109
  adding a Windows script 110
  adding applications 100
  adding as batch script 101
  adding KACE SMA Agent installer 110
  adding Managed Installations 104, 104
  applying KUID to KACE SMA Agent 56
  applying Windows computer name 57
  assigning to custom deployment 116
  assigning to scripted installation deployment 115
  assigning to system deployment 113
  deleting 151
  installing a service pack 109
  joining domain 54
  link appliances 104
  load user states on devices 90
  renaming target devices 107
  uploading files
    file size limitation 112
  view Managed Installations 104
pre-installation task
  formatting C drive as NTFS 79
pre-installation tasks
  adding a PowerShell Task 108
  adding a shell script 109
  adding a Windows script 110
  adding applications 100
  adding as batch script 101
  adding DiskPart script 102
  assigning to custom deployment 116
  assigning to scripted installation deployment 115
  assigning to system deployment 113
  collecting Windows computer name 56
  creating a single partition 79
  deleting 151
  editing in scripted installation deployment 117
  editing in system image deployment 117
  file size limitation 112
  installing Windows MBR 97
  installing XP MBR 98
post-installation tasks
  editing in scripted installation deployment 117
  editing in system image deployment 117
  uploading files 112
preparing for deployment
  downloading deployment tools 42
  downloading Media Manager 43
  enabling DHCP server 42
  setting up deployment environment 42

R
  Remote Site Appliance (RSA)
    configuring network settings 140
    extending the KACE SDA 142
    installing 140
    linking to KACE SDA Deployment Appliance 141
    requirements for 139, 139
    setting up 139, 139
  RSA
    linking 29
  runtime environments
    about 112

S
  scheduling
    exports 144
  scripted installation
    delete assigned 150
    modifying source media 97
  scripted installation setup file
    about the windows components setting 97
    adding administrator account settings 95
    adding registration data settings 94
    configuring general settings 95
    configuring network settings 96
    modifying configuration file 97
  scripted installations
    adding a new scripted installation 92
    best practices 92
    creating a configuration file 92
    creating an answer file 92
  search
    documentation 15
    lists 14
    online Help 15
  security settings 38
    disabling SSL 40
    enabling offboard access 40
    enabling SNMP monitoring 38
    enabling SSH 40
    enabling SSL 38
    generating certificate 39
    generating private SSL key 39
    preventing brute-force attacks 40
  service pack
    installing as a post-installation task 109
  software version
    viewing appliance 167
  source media
    deleting 150
    modifying source media metadata 50
    modifying source media name 50
    viewing source media details 50
    viewing source media metadata 50
  SSL certificates 38
  system images
    about K-Images 51
    about UEFI images 51
    about WIM images 51
    deleting 150
    deleting unused 149
  task groups
    adding 111, 111
    assigning to custom deployment 116
    assigning to scripted installation deployment 115
    assigning to system deployment 113
  task sequencing
    adding built-in mid-level tasks 99
    adding built-in post-installation tasks 99
    adding built-in pre-installation tasks 99
    adding task groups 111
    creating 99
  terminal window interface 24
  tickets
    creating and submitting 157
    requesting enhancements 157
  troubleshooting 160
    about troubleshooting 155
    backing up appliance data 164
    Boot Manager 157
    Boot Manager style 158
    changing network delay time 159
    creating and submitting a ticket 157
    downloading appliance log files 160
    enabling remote technical support 156
    obtaining a tether key 156
    powering off appliance 163
    preventing interruptions of PXE boot 158
    rebooting appliance 164
    recovering corrupted devices 159
    recovering devices 159
    select local hard disk boot method 158
    shutting down and rebooting appliance 163
    testing device network boot 157
    using the KBE Recovery menu 159
    verifying devices on network 155
    viewing appliance log files 160
  U
  UEFI devices
    applying a UEFI partition 80
    creating a UEFI partition 79
    updating appliance 167
    checking and applying updates automatically 167
    performing manual updates 168
    updating from downloaded file 168
    viewing software version 167
    uploading
      OS installation source media 49
      USB deployments
        installing boot environment to device 125
        selecting FAT32/UEFI format 125
user accounts
   adding local administrator 34
   authenticating 34
   deleting 37
user states
   about the .mig file 90
   capturing offline 89
   creating a USMT scan template 87
   excluding data from capture 87
   loading on devices 90
   loading on devices manually 90
   scanning online 87
users
   authenticating 34
USMT
   uploading from Media Manager 86
   uploading from the appliance 86
V
VNC
   setting password 26
W
WIM images
   capture new images to server 120
   deploy new images from server 120, 121
Windows Assessment and Development Kit (ADK)
   downloading and installing 49