KACE® Systems Management Appliance 15.1

Setup Guide for VMware Platforms

Table of Contents

Setting up the appliance **3**
- Before you begin 3
- Install the virtual KACE SMA on a VMware ESX or VMware ESXi server 3
- Power-on the appliance and log in to the Administrator Console 4
- Configure initial network settings manually (optional) 5
- Accessing the Administrator Guide and online Help 9
- Scheduling training 9
- About us 10
  - We are more than just a name 10
  - Our brand, our vision. Together 10
  - Contacting Quest 10
  - Technical support resources 10

Index **11**

Setting up the appliance

This guide explains how to set up the virtual KACE Systems Management Appliance (SMA) on VMware® ESX® or VMware ESXi™ host systems.The virtual KACE SMA does not require dedicated hardware.

For additional documentation, go to https://support.quest.com/kace-systems-management-appliance/technical-documents.

Before you begin

Before you set up the appliance, there are a number of preliminary actions you need to take.

1. Purchase a virtual KACE SMA license from Quest sales at https://www.quest.com/company/contact-us.aspx.
2. Decide whether to use a DHCP server to automatically assign an IP address to the appliance, or to obtain a static IP address for the appliance.
3. If you obtain a static IP address for the appliance, enter the appliance's hostname in the A record of your internal DNS (domain name system) server. The A record defines the hostname for the MX record, and this enables users to send email tickets to the Service Desk. By default, the appliance's hostname is `k1000`, but Quest recommends to change this name to a more unique value during initial setup.

   IMPORTANT: Leaving the appliance name unchanged can cause problems when additional KACE SMA appliances are introduced. Multiple KACE SMA appliances with identical names belonging to the same network will have the same IP address, which can cause problems for these appliances.
4. Decide whether to use a split DNS. This is useful if the appliance connects to the Internet using a reverse proxy, or if you place the appliance in a perimeter network or screened subnet. A DMZ adds an additional layer of security to a LAN (local area network).

Install the virtual KACE SMA on a VMware ESX or VMware ESXi server

You can install the virtual KACE SMA on a host system that has the VMware vSphere® client or the vSphere Web Client installed.

Before you install the virtual KACE SMA, you need to install the VMware vSphere client, or the vSphere Web Client on your host system. Run the vSphere client on a computer that is on the same network as the designated host because importing across a WAN does not work.

1. To download the virtual KACE SMA, go to https://support.quest.com/kace-systems-management-appliance/download-new-releases. To obtain your customer login credentials, contact Quest Software Support at https://support.quest.com/contact-support.
2. In the *Virtual Appliance* section, download the compressed OVF (Open Virtualization Format) file to your vSphere Client system.
3. Extract the files.
4. Launch the vSphere client program, then click **File** > **Deploy OVF Template**.
5. Browse to the folder where you extracted the files and select the OVF file.

The installation wizard appears and offers you installation choices.

6. Select the components that your implementation requires: data center, datastore, and so on.
7. Click **Finish**.
8. Confirm the appliance settings. Check for a valid network and any other settings you need.

Power-on the appliance and log in to the Administrator Console

When the appliance is powered on for the first time, you can log in to the KACE SMA **Administrator Console** from any computer on your LAN provided that a DHCP server is available to assign an IP address to the appliance. This enables you to use the setup wizard to configure initial network settings.

If a DHCP server is not available, you can configure initial network settings using the **Command Line Console**. See Configure initial network settings manually (optional).

NOTE: Your browser setting determines locale formats used for date and time information displayed in the **Administrator Console** the first time you log in. For information about changing the language settings, see the appliance **Administrator Guide**: Accessing the Administrator Guide and online Help.

1. Power on the virtual machine to boot the appliance. This takes 5 to 10 minutes.

   The Command Line Console login screen appears, and it shows the appliance's DHCP network settings.

2. On any computer connected to your LAN, open a browser and go to the URL shown on the Command Line Console login screen. For example, `http://<unique_KACE_SMA_appliance_name>.local/admin`.

   The *Software Transaction Agreement* page appears.

3. Accept the agreement.

   The *Initial Setup* wizard appears.

4. Verify that you have the information required to configure the appliance, then click **Next**.
5. Review the information on the *Diagnostic Console Two-Factor Authentication* page that appears, and record the secret key and offline tokens in a secure place, as instructed.
6. On the *Licensing and Administrator Settings* page, provide the following information:

Option	Description
License Key	The license key you received in the **Welcome** email from Quest. If you do not have a license key, contact **Quest Software Support** at https://support.quest.com/contact-support.
Company Name	The name of your company or group.
Administrator Email	The email address where you want to receive communications from Quest.
Password	The password for the default **admin** account, which is the account you use to log in to the appliance **Administrator Console**. The default **admin** account is the only account on the appliance at this time. If you forget the password for this account, the system might have to be reset to factory defaults which can result in loss of data.

Option	Description
	NOTE: If you have multiple KACE SMA or KACE SDA (Systems Deployment) appliances, Quest recommends that you use the same password for the **admin** account on all appliances. This enables you to link the appliances later. For more information, see the appliance **Administrator Guide**: Accessing the Administrator Guide and online Help.
Two-Factor Authentication	If you want to provide stronger security for users logging into the appliance, set this to *Enabled*. This feature adds an extra step to the login process. It relies on the Google Authenticator app to generate verification codes. The app generates a new six-digit code at regular intervals. When enabled, end users will be prompted for the current verification code each time they log in. **NOTE:** If you enable this feature, ensure that KACE SMA server's clock is accurate, as well as the device running Google Authenticator. Google Authenticator relies on current time to create the token. If server's clock is not synchronized with those of the devices running Google Authenticator, token validation may fail, which may result in the account lockouts.

7. Follow the on-screen instructions to complete the initial setup.

   When the initial setup is complete, the appliance restarts and the Administrator Console login page appears.

   NOTE: If you change the appliance IP address, go to the new address to display the login page.

8. Log in to the Administrator Console using the login ID admin and the password you chose during initial setup.

   If Two-Factor Authentication was enabled on the *Licensing and Administrator Settings* page in the *Initial Setup* wizard, the *Configure Two-Factor Authentication* page appears.

9. **Two-Factor Authentication only**. Follow the instructions on the *Configure Two-Factor Authentication* page to generate a Google Authenticator verification code using your smart phone. In the *Verification Code* field, type the Google Authenticator code, and click **Finish Configuration**. A new verification code is required on each subsequent login.

   To skip this step, click Skip Configuration. You can only bypass this step during a configured transition window. For more information, see the *Administrator Guide*.

The **Administrator Console** appears and the appliance is ready for use.

Configure initial network settings manually (optional)

If a DHCP server is not available and you cannot log in to the appliance **Administrator Console**, you can configure initial network settings manually using the **Command Line Console**.

1. Power on the virtual machine to boot the appliance. This takes 5 to 10 minutes.

The Command Line Console login screen appears.

2. At the prompts, enter:

   Login: **konfig**

   Password: konfig

3. Choose the language to use for the Command Line Console. Use the up- and down-arrow keys to move between fields.
4. Configure the following network settings. Use the right- and left-arrow keys to select options in a field; use the up- and down-arrow keys to move between fields.

Option	Description
KACE SMA DNS Hostname	Enter the hostname of the appliance. The default is k1000, but Quest recommends to change this name to a more unique value during initial setup. Leaving the appliance name unchanged can cause problems when additional KACE SMA appliances are introduced. **IMPORTANT: Multiple KACE SMA appliances with identical names belonging to the same network will have the same IP address, which can cause problems for these appliances.**
Automatically generate server name	Select this check box to enable the system to generate the KACE SMA web server name using this format: **Hostname**.**Domain**. For example: <unique_KACE_SMA_appliance_name>.example.com. Clear this check box to enter a custom web server name.
KACE SMA Web Server Name	Enter the fully qualified domain name of the appliance. This is the **Hostname** concatenated with **Domain**. For example: <unique_KACE_SMA_appliance_name>.example.com. Devices connect to the appliance using this name. Quest recommends that you add a static IP address entry for the appliance to your DNS server. If you use an SSL certificate, the hostname must be fully qualified and it must match the name on the certificate.
DHCP	(Optional) Select this option to use DHCP (Dynamic Host Configuration Protocol) to automatically obtain the IPv4 address and other network configuration information for the appliance. If you select this option, you do not need to provide the Static IP Address, Domain, Subnet Mask, Default Gateway, Primary DNS, or Secondary DNS settings.
Manual IPv4 Configuration	Specify the IPv4 address and provide the Static IP Address, Domain, Subnet Mask, Default Gateway, Primary DNS, or Secondary DNS settings for the appliance. **NOTE:** The IPv4 address is required whether or not an IPv6 address is available. The IPv6 address is optional.

Option	Description
SLAAC	Select this option if you want to use SLAAC (stateless address auto-configuration), offered by IPv6, to configure the appliance's network settings. SLAAC allows devices to select their own IPv6 addresses based on the prefix that is advertised from their connected interface.
Manual IPv6 Configuration	Select this option if you want to manually specify the IPv6 address. If you select this option, you must specify the IPv6 address, prefix length, and default gateway for the appliance. **NOTE:** The IPv6 address is optional. The IPv4 address is required whether or not an IPv6 address is available.
Disable IPv6	Select this option if you want to disable an IPv6 address for the appliance. This is the default setting.
SMTP Server	(Optional) Specify the hostname or IP address of an external SMTP server, such as `smtp.gmail.com`. External SMTP servers must allow anonymous (non-authenticated) outbound email transport. Ensure that your network policies allow the appliance to contact the SMTP server directly. In addition, the mail server must be configured to allow the relaying of email from the appliance without authentication. If you do not provide SMTP server information, the KACE SMA sends email using its internal SMTP server.
SSH Enabled	(Optional) Select this option to enable SSH (secure) access to the appliance **Administrator Console**. Quest recommends that you enable SSH during the initial setup. When the setup is complete, you can change the setting in the **Administrator Console** as needed.
Proxy	(Optional) Enter proxy server information. **NOTE:** The appliance supports proxy servers that use basic, realm-based authentication, requiring usernames and passwords. If your proxy server uses a different kind of authentication, add the appliance's IP address to the proxy server's exception list.

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

   The appliance restarts.

6. On any computer connected to your LAN, open a browser and go to the appliance Administrator Console URL. For example, `http://<unique_KACE_SMA_appliance_name>.local/admin`.

   The *Software Transaction Agreement* page appears.

7. Accept the agreement.

The *Initial Setup* wizard appears.

8. Verify that you have the information required to configure the appliance, then click **Next**.
9. Review the information on the *Diagnostic Console Two-Factor Authentication* page that appears, and record the secret key and offline tokens in a secure place, as instructed.
10. On the *Licensing and Administrator Settings* page, provide the following information:

Option	Description
License Key	The license key you received in the **Welcome** email from Quest. If you do not have a license key, contact **Quest Software Support** at https://support.quest.com/contact-support.
Company Name	The name of your company or group.
Administrator Email	The email address where you want to receive communications from Quest.
Password	The password for the default **admin** account, which is the account you use to log in to the appliance **Administrator Console**. The default **admin** account is the only account on the appliance at this time. If you forget the password for this account, the system might have to be reset to factory defaults which can result in loss of data. **NOTE:** If you have multiple KACE SMA or KACE SDA (Systems Deployment) appliances, Quest recommends that you use the same password for the **admin** account on all appliances. This enables you to link the appliances later. For more information, see the appliance **Administrator Guide**: Accessing the Administrator Guide and online Help.
Two-Factor Authentication	If you want to provide stronger security for users logging into the appliance, set this to *Enabled*. This feature adds an extra step to the login process. It relies on the Google Authenticator app to generate verification codes. The app generates a new six-digit code at regular intervals. When enabled, end users will be prompted for the current verification code each time they log in. **NOTE:** If you enable this feature, ensure that KACE SMA server's clock is accurate, as well as the device running Google Authenticator. Google Authenticator relies on current time to create the token. If server's clock is not synchronized with those of the devices running Google Authenticator, token validation may fail, which may result in the account lockouts.

11. Follow the on-screen instructions to complete the initial setup.

When the initial setup is complete, the appliance restarts and the Administrator Console login page appears.

NOTE: If you change the appliance IP address, go to the new address to display the login page.

12. Log in to the Administrator Console using the login ID admin and the password you chose during initial setup.

    If Two-Factor Authentication was enabled on the *Licensing and Administrator Settings* page in the *Initial Setup* wizard, the *Configure Two-Factor Authentication* page appears.

13. **Two-Factor Authentication only**. Follow the instructions on the *Configure Two-Factor Authentication* page to generate a Google Authenticator verification code using your smart phone. In the *Verification Code* field, type the Google Authenticator code, and click **Finish Configuration**. A new verification code is required on each subsequent login.

    To skip this step, click Skip Configuration. You can only bypass this step during a configured transition window. For more information, see the *Administrator Guide*.

The **Administrator Console** appears and the appliance is ready for use.

Accessing the Administrator Guide and online Help

For help using the **Administrator Console**, click the Help link in the top-right corner of the interface to open the context-sensitive Help. To access the main Help system, click the links in context-sensitive Help topics.

Scheduling training

To help you begin using the appliance, Quest provides a training program called QuickStart. This program provides remote assistance to help get your solution up and running quickly to begin provisioning, managing, securing and servicing your network-connected devices.

To find out more about this program, visit one of the following links:

- **KACE Systems Management Appliance**: https://support.quest.com/kace-systems-management-appliance/professional-services/332
- **KACE Asset Management Appliance**: https://support.quest.com/kace-asset-management-appliance/professional-services/331

To register, submit a request at:

- **KACE Systems Management Appliance**: https://www.quest.com/register/113381
- **KACE Asset Management Appliance**: https://www.quest.com/register/113379

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/company/contact-us.aspx or call 1-949-754-8000.

Technical support resources

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.

Index

L

license key
administrator password 4

S

settings
initial configuration 4