

Quest®



KACE® Systems Management  
Appliance 13.0

## **Setup Guide for VMware Platforms**



# Table of Contents

<b>Setting up the appliance</b> .....	<b>4</b>
Before you begin.....	4
Install the virtual KACE SMA on a VMware ESX or VMware ESXi server.....	4
Power-on the appliance and log in to the Administrator Console.....	5
Configure initial network settings manually (optional).....	7
Accessing the Administrator Guide and online Help.....	11
Scheduling training.....	12
About us.....	12
Technical support resources.....	12
<b>Configuration de l'appliance</b> .....	<b>14</b>
Avant de commencer.....	14
Installation de l'appliance virtuelle KACE SMA sur un serveur VMware ESX ou VMware ESXi.....	14
Mettre l'appliance sous tension et se connecter à la Console d'administration.....	15
Configurer les paramètres réseau initiaux manuellement (facultatif).....	18
Accès au Guide de l'administrateur et à l'aide en ligne.....	23
Programmation des formations.....	23
Qui nous sommes.....	23
Ressources du support technique.....	24
<b>Einrichten der Appliance</b> .....	<b>25</b>
Vorbereitung.....	25
Installieren der virtuellen KACE SMA auf einem VMware ESX- oder VMware ESXi-Server.....	25
Einschalten der Appliance und Anmelden bei der Administratorkonsole.....	26
Anfängliche Netzwerkeinstellungen manuell konfigurieren (optional).....	29
Zugriff auf das Administratorhandbuch und die Onlinehilfe.....	34
Zeitplanung für Schulungen.....	34
Über uns.....	35
Ressourcen für den technischen Support.....	35
<b>アプライアンスのセットアップ</b> .....	<b>36</b>
はじめに.....	36
VMware ESXまたはVMware ESXiサーバへの仮想KACE SMAのインストール.....	36
アプライアンスの電源投入と管理者コンソールへのログイン.....	37
手動による初期ネットワーク設定の構成（オプション）.....	39
管理者ガイドおよびオンラインヘルプへのアクセス.....	44
トレーニングのスケジュール設定.....	44
当社について.....	45
テクニカルサポートのリソース.....	45
<b>Configuração do equipamento</b> .....	<b>46</b>
Antes de começar.....	46
Instalar o KACE SMA virtual em um servidor VMware ESX ou VMware ESXi.....	46
Ligue a solução e faça login no Console do administrador.....	47
Definir as configurações iniciais de rede manualmente (opcional).....	49
Acessar o Guia do administrador e a Ajuda on-line.....	54
Programação de treinamento.....	55
Sobre nós.....	55
Recursos de suporte técnico.....	55
<b>Configuración del dispositivo</b> .....	<b>57</b>

Antes de comenzar.....	57
Instale el SMA virtual de KACE en un servidor VMware ESX o VMware ESXi.....	57
Encienda el dispositivo e inicie sesión en la Consola del administrador.....	58
Configure los ajustes de red iniciales de forma manual (opcional).....	60
Acceso a la Guía para el administrador y la ayuda en línea.....	65
Programación de la capacitación.....	66
Acerca de nosotros.....	66
Recursos del soporte técnico.....	66
<b>Legal notices.....</b>	<b>68</b>

# 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.



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 \(optional\)](#).



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 <b>Welcome</b> email from Quest. If you do not have a license key, contact <b>Quest Software Support</b> at <a href="https://support.quest.com/contact-support">https://support.quest.com/contact-support</a> .
Company Name	The name of your company or group.
Administrator Email	The email address where you want to receive communications from Quest.
Password	<p>The password for the default <b>admin</b> account, which is the account you use to log in to the appliance <b>Administrator Console</b>. The default <b>admin</b> 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.</p> <div data-bbox="568 727 1023 959" style="border-left: 1px solid #0070C0; padding-left: 10px;"> <p><b>i</b> If you have multiple KACE SMA or KACE SDA (Systems Deployment) appliances, Quest recommends that you use the same password for the <b>admin</b> account on all appliances. This enables you to link the appliances later. For more information, see the appliance <b>Administrator Guide: Accessing the Administrator Guide and online Help</b>.</p> </div>
Two-Factor Authentication	<p>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.</p> <div data-bbox="568 1225 1023 1430" style="border-left: 1px solid #0070C0; padding-left: 10px;"> <p><b>i</b> 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</p> </div>



Option	Description
7.	<p>Follow the on-screen instructions to complete the initial setup.</p> <p>When the initial setup is complete, the appliance restarts and the <b>Administrator Console</b> login page appears.</p> <p> If you change the appliance IP address, go to the new address to display the login page.</p>
8.	<p>Log in to the Administrator Console using the login ID admin and the password you chose during initial setup.</p> <p>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.</p>
9.	<p><b>Two-Factor Authentication only.</b> 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 <b>Finish Configuration</b>. A new verification code is required on each subsequent login.</p> <p>To skip this step, click <b>Skip Configuration</b>. You can only bypass this step during a configured transition window. For more information, see the Administrator Guide.</p>

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**.

- Power on the virtual machine to boot the appliance. This takes 5 to 10 minutes.  
The **Command Line Console** login screen appears.
- At the prompts, enter:  
Login: konfig  
Password: konfig
- Choose the language to use for the Command Line Console. Use the up- and down-arrow keys to move between fields.
- 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
<b>KACE SMA DNS Hostname</b>	<p>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.</p> <p> 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.</p>
<b>Automatically generate server name</b>	<p>Select this check box to enable the system to generate the KACE SMA web server name using this format: <b>Hostname.Domain</b>. For example: &lt;unique_KACE_SMA_appliance_name&gt;.example.com. Clear this check box to enter a custom web server name.</p>
<b>KACE SMA Web Server Name</b>	<p>Enter the fully qualified domain name of the appliance. This is the <b>Hostname</b> concatenated with <b>Domain</b>. For example: &lt;unique_KACE_SMA_appliance_name&gt;.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.</p>
<b>DHCP</b>	<p>(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.</p>
<b>Manual IPv4 Configuration</b>	<p>Specify the IPv4 address and provide the Static IP Address, Domain, Subnet Mask, Default Gateway, Primary DNS, or Secondary DNS settings for the appliance.</p> <p> The IPv4 address is required whether or not an IPv6 address is available. The IPv6 address is optional.</p>



Option	Description
<b>SLAAC</b>	<p>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.</p>
<b>Manual IPv6 Configuration</b>	<p>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.</p>
<b>Disable IPv6</b>	<p>Select this option if you want to disable an IPv6 address for the appliance. This is the default setting.</p>
<b>SMTP Server</b>	<p>(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.</p>
<b>SSH Enabled</b>	<p>(Optional) Select this option to enable SSH (secure) access to the appliance <b>Administrator Console</b>. Quest recommends that you enable SSH during the initial setup. When the setup is complete, you can change the setting in the <b>Administrator Console</b> as needed.</p>
<b>Proxy</b>	<p>(Optional) Enter proxy server information.</p> <p> 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.</p>

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
<b>License Key</b>	The license key you received in the <b>Welcome</b> email from Quest. If you do not have a license key, contact <b>Quest Software Support</b> at <a href="https://support.quest.com/contact-support">https://support.quest.com/contact-support</a> .
<b>Company Name</b>	The name of your company or group.
<b>Administrator Email</b>	The email address where you want to receive communications from Quest.
<b>Password</b>	The password for the default <b>admin</b> account, which is the account you use to log in to the appliance <b>Administrator Console</b> . The default <b>admin</b> 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.



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](#)**.

<b>Two-Factor Authentication</b>	If you want to provide stronger security for users logging into the appliance, set this to Enabled.
----------------------------------	---

## Option

## Description

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.



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.



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.

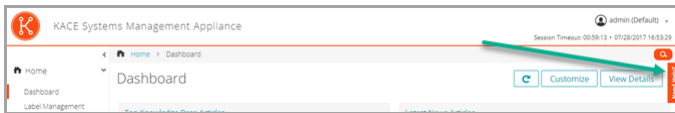
13. **Two-Factor Authentication only.** Follow the instructions on the Configure Two-Factor Authentication page to generate a Google Authenticator verification code using your smart phone. In the Verification Code field, type the Google Authenticator code, and click **Finish Configuration**. A new verification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

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit [www.quest.com](http://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.

# Configuration de l'appliance

Ce guide explique comment configurer l'appliance virtuelle de gestion des systèmes KACE (SMA) sur les systèmes hôtes VMware® ESX® ou VMware ESXi™. L'appliance KACE SMA ne requiert aucun matériel dédié.

Pour obtenir de la documentation supplémentaire, rendez-vous sur <https://support.quest.com/kace-systems-management-appliance/technical-documents>.

## Avant de commencer

Avant de configurer l'appliance, vous devez effectuer un certain nombre de tâches.

1. Achetez une licence virtuelle KACE SMA auprès du service commercial Quest à l'adresse <https://www.quest.com/company/contact-us.aspx>.
2. Décidez si vous souhaitez utiliser un serveur DHCP pour attribuer automatiquement une adresse IP à l'appliance, ou si vous préférez obtenir une adresse IP statique pour l'appliance.
3. Si vous obtenez une adresse IP statique pour l'appliance, saisissez le nom d'hôte de l'appliance dans l'enregistrement A de votre serveur DNS (Domain Name System) interne. L'enregistrement A définit le nom d'hôte de l'enregistrement MX et permet, par conséquent, aux utilisateurs d'envoyer des tickets par courrier électronique au Service Desk. Par défaut, le nom d'hôte de l'appliance est k1000, mais Quest vous recommande de modifier ce nom par un nom unique plus personnalisé lors de la configuration initiale.



Le fait de ne pas modifier le nom de l'appliance par défaut peut provoquer des problèmes lorsque des appliances KACE SMA supplémentaires sont ajoutées. Plusieurs appliances KACE SMA avec des noms identiques et appartenant au même réseau partageront la même adresse IP, ce qui peut générer des problèmes pour ces appliances.

4. Décidez s'il convient d'utiliser ou non une infrastructure Split DNS. Cela peut être utile si l'appliance se connecte à Internet au moyen d'un proxy inverse ou si elle est placée dans un périmètre réseau ou un sous-réseau filtré. La zone DMZ permet d'ajouter un niveau de sécurité supplémentaire à un réseau LAN (Local Area Network).

## Installation de l'appliance virtuelle KACE SMA sur un serveur VMware ESX ou VMware ESXi

Vous pouvez installer l'appliance virtuelle KACE SMA sur un système hôte sur lequel est installé le client VMware vSphere® ou le web client vSphere.

Avant d'installer l'appliance virtuelle KACE SMA, vous devez installer le client VMware vSphere ou le web client vSphere sur votre système hôte. Exécutez le client vSphere sur un ordinateur

situé sur le même réseau que l'hôte désigné. En effet, l'importation ne fonctionne pas sur un réseau étendu (WAN).

1. Pour télécharger l'appliance virtuelle KACE SMA, accédez à la page <https://support.quest.com/kace-systems-management-appliance/download-new-releases>. Pour obtenir vos informations d'identification, contactez le Support Quest Software à l'adresse <https://support.quest.com/contact-support>.
2. Dans la section Appliance virtuelle, téléchargez le fichier compressé OVF (Open Virtualization Format) vers votre système client vSphere.
3. Procédez à l'extraction des fichiers.
4. Lancez le programme client vSphere, puis cliquez sur **Fichier > Déployer le modèle OVF**.
5. Recherchez le dossier où vous avez extrait les fichiers et sélectionnez le fichier OVF.  
L'Assistant d'installation s'affiche et vous propose différents choix d'installation.
6. Sélectionnez les composants nécessaires pour votre environnement (centre de données, magasin de données, etc.).
7. Cliquez sur **Terminer**.
8. Vérifiez les paramètres de l'appliance. Recherchez un réseau valide et vérifiez les autres paramètres dont vous avez besoin.

## Mettre l'appliance sous tension et se connecter à la Console d'administration

Lorsque vous mettez l'appliance sous tension pour la première fois, vous pouvez vous connecter à la **Console d'administration** de l'appliance KACE SMA depuis n'importe quel ordinateur sur votre réseau local, à condition qu'un serveur DHCP soit disponible pour attribuer une adresse IP à l'appliance. Cela vous permet d'utiliser l'assistant d'installation afin de configurer les paramètres réseau initiaux.

Si aucun serveur DHCP n'est disponible, vous pouvez configurer les paramètres réseau initiaux à l'aide de la **Console de ligne de commande**. Voir [Configurer les paramètres réseau initiaux manuellement \(facultatif\)](#).



Votre paramètre de navigateur détermine les paramètres régionaux utilisés pour la date et l'heure affichées dans la **Console d'administration** au cours de votre première connexion. Pour plus d'informations sur la modification des paramètres de langue, consultez le **Guide de l'administrateur** de l'appliance : [Accès au Guide de l'administrateur et à l'aide en ligne](#).

1. Mettez la machine virtuelle sous tension pour démarrer l'appliance. Cette opération dure entre 5 et 10 minutes.

L'écran de connexion à la **Console de ligne de commande** s'affiche et indique les paramètres réseau DHCP de l'appliance.

2. Sur tout ordinateur connecté à votre réseau local, ouvrez un navigateur et accédez à l'URL indiquée sur l'écran de connexion à la Console de ligne de commande. Par exemple, `http://<unique_KACE_SMA_appliance_name>.local/admin`.

La page Contrat de transaction du logiciel apparaît.

3. Acceptez le contrat.  
L'assistant Installation initiale s'affiche.
4. Vérifiez que vous disposez de toutes les informations nécessaires pour configurer l'apppliance, puis cliquez sur **Suivant**.
5. Vérifiez les informations de la page Authentification à deux facteurs de la Console de diagnostic qui s'affiche, et conservez la clé secrète et les jetons hors ligne en lieu sûr, comme demandé.
6. À la page Paramètres de licence et d'administrateur, fournissez les informations suivantes :

Option	Description
<b>Clé de licence</b>	Saisissez la clé de licence que vous avez reçue dans le courrier électronique de <b>bienvenue</b> envoyé par Quest. Si vous ne disposez d'aucune clé de licence, contactez le <b>Support Quest Software</b> à l'adresse <a href="https://support.quest.com/contact-support">https://support.quest.com/contact-support</a> .
<b>Nom de l'entreprise</b>	Nom de votre entreprise ou organisation.
<b>E-mail de l'administrateur</b>	Adresse e-mail à laquelle vous souhaitez recevoir les communications de Quest.
<b>Mot de passe</b>	Mot de passe du compte <b>admin</b> par défaut, qui est le compte que vous utilisez pour vous connecter à la <b>Console d'administration</b> de l'apppliance. Le compte <b>admin</b> par défaut est le seul compte défini sur l'apppliance à ce stade. Si vous oubliez le mot de passe de ce compte, il vous faudra probablement rétablir les paramètres d'usine par défaut du système, ce qui peut entraîner une perte de données.



Si vous disposez de plusieurs appliances KACE SMA ou KACE SDA (déploiement des systèmes), Quest vous recommande d'utiliser un mot de passe identique pour le compte **admin** de chaque appliance. Cela vous permet de lier les appliances entre elles par la suite. Pour plus d'informations, consultez le **Guide de l'administrateur**



## Option

## Description

de l'appliance : [Accès au Guide de l'administrateur](#) et à [l'aide en ligne](#).

### Authentification bifactorielle

Si vous voulez fournir une sécurité accrue aux utilisateurs se connectant à l'appliance, définissez cette option sur **Activé**. Cette fonction ajoute une étape au processus de connexion. Elle s'appuie sur l'application Google Authenticator pour générer des codes de vérification. L'application génère un nouveau code à six chiffres à intervalles réguliers. Lorsque cette option est activée, les utilisateurs sont invités à saisir le code de vérification actif à chaque connexion.



Si vous activez cette fonction, assurez-vous que l'horloge du serveur KACE SMA est précise, ainsi que sur le périphérique exécutant Google Authenticator. Google Authenticator s'appuie sur l'heure actuelle pour créer le jeton. Si l'horloge du serveur n'est pas synchronisée avec celles des périphériques exécutant Google Authenticator, la validation du jeton peut échouer, ce qui peut entraîner le verrouillage du compte.

7. Suivez les instructions affichées à l'écran pour finaliser la configuration initiale.

Une fois la configuration initiale terminée, l'appliance redémarre, puis la page de connexion à la **Console d'administration** s'affiche.



Si vous modifiez l'adresse IP de l'appliance, utilisez la nouvelle adresse pour afficher la page de connexion.

8. Connectez-vous à la Console d'administration avec l'ID de connexion admin et le mot de passe que vous avez défini lors de la configuration initiale.

Si l'authentification à deux facteurs a été activée sur la page Paramètres de licence et d'administrateur de l'assistant de configuration initiale, la page Configurer l'authentification à deux facteurs s'affiche.

9. **Authentification à deux facteurs uniquement.** Suivez les instructions figurant sur la page Configurer l'authentification à deux facteurs pour générer un code de vérification Google Authenticator en utilisant votre smartphone. Dans le champ Code de vérification, saisissez le code d'authentification Google Authenticator et cliquez sur **Terminer la configuration**. Un nouveau code de vérification est nécessaire pour chaque nouvelle connexion.


Pour ignorer cette étape, cliquez sur **Ignorer la configuration**. Vous ne pouvez ignorer cette étape que pendant une fenêtre de transition configurée. Pour plus d'informations à ce sujet, consultez le document Administrator Guide (Guide de l'administrateur).

La **Console d'administration** s'affiche et vous pouvez utiliser l'appliance.



## Configurer les paramètres réseau initiaux manuellement (facultatif)

Si aucun serveur DHCP n'est disponible et que vous ne pouvez pas vous connecter à la **Console de ligne de commande** de l'appliance, vous pouvez configurer les paramètres réseau initiaux manuellement à l'aide de la **Console d'administration**.

1. Mettez la machine virtuelle sous tension pour démarrer l'appliance. Cette opération dure entre 5 et 10 minutes.  
L'écran de connexion à la **Console de ligne de commande** s'affiche.
2. À l'invite de connexion, saisissez :  
ID de connexion : konfig  
Mot de passe : konfig
3. Choisissez la langue de la Console de ligne de commande. Utilisez les touches fléchées haut et bas pour vous déplacer d'un champ à l'autre.
4. Configurez les paramètres réseau ci-dessous. Utilisez les touches fléchées droite et gauche pour sélectionner les options dans un champ et les touches fléchées haut et bas pour vous déplacer d'un champ à l'autre.

Option	Description
<b>Nom d'hôte DNS du KACE SMA</b>	<p>Entrez le nom d'hôte de l'appliance. Par défaut, le nom d'hôte de l'appliance est k1000, mais Quest vous recommande de modifier ce nom par un nom unique plus personnalisé lors de la configuration initiale. Le fait de ne pas modifier le nom de l'appliance par défaut peut provoquer des problèmes lorsque des appliances KACE SMA supplémentaires sont ajoutées.</p> <p> Plusieurs appliances KACE SMA avec des noms identiques et appartenant au même réseau partageront la même adresse IP, ce qui peut générer des problèmes pour ces appliances.</p>
<b>Générer automatiquement le nom du serveur</b>	Cochez cette case pour permettre au système de générer le nom du serveur Web KACE SMA au format suivant :

Option	Description
<b>Nom du serveur Web du KACE SMA</b>	<p><b>Nom d'hôte.Domaine.</b> Exemple : &lt;unique_KACE_SMA_appliance_name&gt;.example.com. Décochez cette case pour saisir un nom de serveur Web personnalisé.</p> <p>Saisissez le nom de domaine complet de l'appliance. Il s'agit du <b>Nom d'hôte</b> concaténé avec le <b>Domaine</b>. Exemple : &lt;unique_KACE_SMA_appliance_name&gt;.example.com. Les périphériques se connectent à l'appliance en utilisant ce nom. Quest recommande d'ajouter une entrée d'adresse IP statique pour l'appliance sur votre serveur DNS. Si vous utilisez un certificat SSL, vous devez spécifier un nom d'hôte complet qui correspond au nom du certificat.</p>
<b>DHCP</b>	<p>(Facultatif) Sélectionnez cette option pour utiliser le DHCP (Dynamic Host Configuration Protocol) afin d'obtenir automatiquement l'adresse IP et d'autres informations de configuration du réseau pour l'appliance. Si vous sélectionnez cette option, vous n'avez pas besoin de fournir l'adresse IP statique, le domaine, le masque de sous-réseau, la passerelle par défaut, le DNS principal ou les paramètres du DNS secondaire.</p>
<b>Configuration IPv4 manuelle</b>	<p>Spécifiez l'adresse IPv4 et indiquez l'adresse IP statique, le domaine, le masque de sous-réseau, la passerelle par défaut, le DNS principal ou les paramètres du DNS secondaire pour l'appliance.</p> <div data-bbox="560 1046 1020 1126" style="border-left: 1px solid black; padding-left: 10px;"> <p><b>i</b> L'adresse IPv4 est requise, qu'une adresse IPv6 soit disponible ou non. L'adresse IPv6 est facultative.</p> </div>
<b>SLAAC</b>	<p>Sélectionnez cette option si vous souhaitez utiliser SLAAC (Stateless Address Autoconfiguration), proposée par IPv6, pour configurer les paramètres du réseau de l'appliance. SLAAC autorise les appareils à sélectionner leurs propres adresses IPv6 en fonction du préfixe publié depuis leur interface connectée.</p>
<b>Configuration IPv6 manuelle</b>	<p>Sélectionnez cette option si vous souhaitez spécifier manuellement l'adresse IPv6. Si vous sélectionnez cette option, vous devez spécifier</p>

Option	Description
	<p>l'adresse IPv6, la longueur du préfixe et la passerelle par défaut pour l'apppliance.</p> <p> L'adresse IPv6 est facultative. L'adresse IPv4 est requise, qu'une adresse IPv6 soit disponible ou non.</p>
<b>Désactiver IPv6</b>	<p>Sélectionnez cette option si vous souhaitez désactiver une adresse IPv6 pour l'apppliance. Il s'agit du paramètre par défaut.</p>
<b>Serveur SMTP</b>	<p>(Facultatif) Spécifiez le nom d'hôte ou l'adresse IP d'un serveur SMTP externe, comme smtp.gmail.com. Les serveurs SMTP externes doivent autoriser le trafic de messagerie sortant anonyme (non authentifié). Assurez-vous que vos stratégies de réseau permettent à l'apppliance de communiquer directement avec le serveur SMTP. En outre, le serveur de messagerie doit être configuré pour permettre le relais du courrier électronique de l'apppliance sans authentification. Si vous ne fournissez pas les informations du serveur SMTP, l'apppliance KACE SMA envoie les e-mails par le biais de son serveur SMTP interne.</p>
<b>SSH activé</b>	<p>(Facultatif) Sélectionnez cette option pour activer l'accès SSH (sécurisé) à la <b>Console d'administration</b> de l'apppliance. Quest vous recommande d'activer le protocole SSH au cours de l'installation initiale. Lorsque la configuration est terminée, vous pouvez modifier les paramètres dans la <b>Console d'administration</b> si nécessaire.</p>
<b>Proxy</b>	<p>(Facultatif) Saisissez les informations concernant le serveur proxy.</p> <p> l'apppliance prend en charge les serveurs proxy utilisant l'authentification de base axée sur le domaine, qui demande un nom d'utilisateur et un mot de passe. Si votre serveur proxy utilise un type d'authentification différent, ajoutez l'adresse IP de l'apppliance à la liste des exceptions du serveur proxy.</p>

- Appuyez sur la touche fléchée bas pour déplacer le curseur vers Enregistrer, puis appuyez sur la touche **Entrée** ou **Retour**.

L'appliance redémarre.

6. Sur tout ordinateur connecté à votre réseau local, ouvrez un navigateur et accédez à l'URL de la Console d'administration de l'appliance. Par exemple, `http://<unique_KACE_SMA_appliance_name>.local/admin`.

La page Contrat de transaction du logiciel apparaît.

7. Acceptez le contrat.

L'assistant Installation initiale s'affiche.

8. Vérifiez que vous disposez de toutes les informations nécessaires pour configurer l'appliance, puis cliquez sur **Suivant**.
9. Vérifiez les informations de la page Authentification à deux facteurs de la Console de diagnostic qui s'affiche, et conservez la clé secrète et les jetons hors ligne en lieu sûr, comme demandé.
10. À la page Paramètres de licence et d'administrateur, fournissez les informations suivantes :

Option	Description
<b>Clé de licence</b>	Saisissez la clé de licence que vous avez reçue dans le courrier électronique de <b>bienvenue</b> envoyé par Quest. Si vous ne disposez d'aucune clé de licence, contactez le <b>Support Quest Software</b> à l'adresse <a href="https://support.quest.com/contact-support">https://support.quest.com/contact-support</a> .
<b>Nom de l'entreprise</b>	Nom de votre entreprise ou organisation.
<b>E-mail de l'administrateur</b>	Adresse e-mail à laquelle vous souhaitez recevoir les communications de Quest.
<b>Mot de passe</b>	Mot de passe du compte <b>admin</b> par défaut, qui est le compte que vous utilisez pour vous connecter à la <b>Console d'administration</b> de l'appliance. Le compte <b>admin</b> par défaut est le seul compte défini sur l'appliance à ce stade. Si vous oubliez le mot de passe de ce compte, il vous faudra probablement rétablir les paramètres d'usine par défaut du système, ce qui peut entraîner une perte de données.



Si vous disposez de plusieurs appliances KACE SMA ou KACE SDA (déploiement des systèmes), Quest vous recommande d'utiliser un mot de passe identique pour le compte **admin** de chaque appliance. Cela vous permet de lier les appliances entre elles par la suite. Pour plus d'informations,

## Option

## Description

consultez le **Guide de l'administrateur** de l'appliance : [Accès au Guide de l'administrateur et à l'aide en ligne](#).

### Authentification bifactorielle

Si vous voulez fournir une sécurité accrue aux utilisateurs se connectant à l'appliance, définissez cette option sur **Activé**. Cette fonction ajoute une étape au processus de connexion. Elle s'appuie sur l'application Google Authenticator pour générer des codes de vérification. L'application génère un nouveau code à six chiffres à intervalles réguliers. Lorsque cette option est activée, les utilisateurs sont invités à saisir le code de vérification actif à chaque connexion.



Si vous activez cette fonction, assurez-vous que l'horloge du serveur KACE SMA est précise, ainsi que sur le périphérique exécutant Google Authenticator. Google Authenticator s'appuie sur l'heure actuelle pour créer le jeton. Si l'horloge du serveur n'est pas synchronisée avec celles des périphériques exécutant Google Authenticator, la validation du jeton peut échouer, ce qui peut entraîner le verrouillage du compte.

11. Suivez les instructions affichées à l'écran pour finaliser la configuration initiale.

Une fois la configuration initiale terminée, l'appliance redémarre, puis la page de connexion à la **Console d'administration** s'affiche.



Si vous modifiez l'adresse IP de l'appliance, utilisez la nouvelle adresse pour afficher la page de connexion.

12. Connectez-vous à la Console d'administration avec l'ID de connexion admin et le mot de passe que vous avez défini lors de la configuration initiale.

Si l'authentification à deux facteurs a été activée sur la page Paramètres de licence et d'administrateur de l'assistant de configuration initiale, la page Configurer l'authentification à deux facteurs s'affiche.

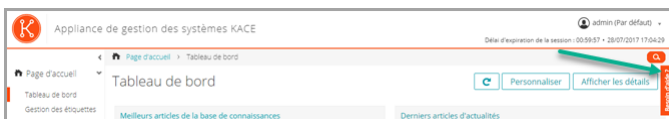
13. **Authentification à deux facteurs uniquement.** Suivez les instructions figurant sur la page Configurer l'authentification à deux facteurs pour générer un code de vérification Google Authenticator en utilisant votre smartphone. Dans le champ Code de vérification, saisissez le code d'authentification Google Authenticator et cliquez sur **Terminer la configuration**. Un nouveau code de vérification est nécessaire pour chaque nouvelle connexion.

Pour ignorer cette étape, cliquez sur **Ignorer la configuration**. Vous ne pouvez ignorer cette étape que pendant une fenêtre de transition configurée. Pour plus d'informations à ce sujet, consultez le document Administrator Guide (Guide de l'administrateur).

La **Console d'administration** s'affiche et vous pouvez utiliser l'appliance.

## Accès au Guide de l'administrateur et à l'aide en ligne

Pour obtenir de l'aide sur l'utilisation de la **Console d'administration**, cliquez sur le lien Aide situé en haut à droite de l'interface pour ouvrir l'aide contextuelle. Pour accéder au système d'aide principal, cliquez sur les liens des rubriques de l'aide contextuelle.



## Programmation des formations

Afin de vous aider à commencer à utiliser l'appliance, Quest propose un programme de formations appelé QuickStart. Ce programme fournit une assistance à distance pour aider à obtenir votre solution rapidement afin de commencer l'approvisionnement, la gestion, la sécurité et la maintenance de vos périphériques connectés au réseau.

Pour en savoir plus sur ce programme, cliquez sur l'un des liens suivants :

- **Appliance de gestion des systèmes KACE** : <https://support.quest.com/kace-systems-management-appliance/professional-services/332>
- **Appliance de gestion des actifs KACE** : <https://support.quest.com/kace-asset-management-appliance/professional-services/331>

Pour vous inscrire, envoyez une demande à :

- **Appliance de gestion des systèmes KACE** : <https://www.quest.com/register/113381>
- **Appliance de gestion des actifs KACE** : <https://www.quest.com/register/113379>

## Qui nous sommes

Quest crée des solutions logicielles qui rendent tangibles les avantages des nouvelles technologies, dans un environnement IT de plus en plus complexe. De la gestion des bases de données et des systèmes à la gestion d'Active Directory et d'Office 365, en passant par la résilience de la cybersécurité, Quest aide ses clients à relever, dès maintenant, leur prochain défi IT. Dans le monde entier, plus de 130 000 entreprises, dont 95 % des entreprises du classement Fortune 500, comptent sur Quest pour assurer une gestion et un suivi proactifs de leur prochaine

initiative, pour trouver la solution aux prochains défis complexes de Microsoft et pour garder une longueur d'avance sur la prochaine menace. Quest Software. Quand le présent rencontre le futur. Pour plus d'informations, visitez le site [www.quest.com](http://www.quest.com).

## Ressources du support technique

Le support technique est disponible pour les clients Quest disposant d'un contrat de maintenance valide et les clients qui utilisent des versions d'évaluation. Vous pouvez accéder au portail du support technique Quest à l'adresse <https://support.quest.com/fr-fr/>.

Ce portail propose des outils d'auto-dépannage qui vous permettront de résoudre des problèmes rapidement et sans aide extérieure, 24 h/24 et 365 j/an. Il permet d'effectuer les opérations suivantes :

- Soumettre et gérer une demande de service
- Consulter les articles de la base de connaissances
- Vous inscrire pour recevoir des notifications sur les produits
- Télécharger des logiciels et de la documentation technique
- Visionner des vidéos de procédure
- Participer aux discussions de la communauté
- Discuter en ligne avec des ingénieurs du support technique
- Découvrir des services capables de vous aider avec votre produit



# Einrichten der Appliance

In diesem Handbuch wird erklärt, wie Sie die virtuelle KACE Systemverwaltungs-Appliance (SMA) auf VMware® ESX® oder VMware ESXi™ Host-Systemen einrichten. Die virtuelle KACE SMA erfordert keine dedizierte Hardware.

Weitere Einzelheiten zur Dokumentation finden Sie unter <https://support.quest.com/kace-systems-management-appliance/technical-documents>.

## Vorbereitung

Vor dem Einrichten der Appliance müssen Sie einige Vorbereitungen treffen.

1. Erwerben Sie eine virtuelle KACE SMA Lizenz bei Quest Sales über <https://www.quest.com/company/contact-us.aspx>.
2. Sie können entscheiden, ob Sie einen DHCP-Server für die automatische Zuweisung einer IP-Adresse zur Appliance oder eine statische IP-Adresse für die Appliance verwenden möchten.
3. Wenn Sie eine statische IP-Adresse für die Appliance verwenden, geben Sie den Hostnamen der Appliance in den A-Datensatz Ihres internen DNS-Servers (Domain Name System) ein. Der A-Datensatz definiert den Hostnamen für den MX-Datensatz. Dadurch können Benutzer E-Mail-Tickets an den Service Desk senden. Standardmäßig ist der Hostname des Geräts k1000, aber Quest empfiehlt, den Namen während der Ersteinrichtung zu ändern.  

i

Wird der Gerätenamen nicht geändert, kann es zu Problemen kommen, wenn zusätzliche KACE SMA Geräte hinzugefügt werden. Wenn mehrere KACE SMA Geräte mit identischen Namen zum selben Netzwerk gehören, haben diese dieselbe IP-Adresse. Dies kann bei diesen Geräten zu Problemen führen.
4. Entscheiden Sie, ob Sie ein Split-DNS verwenden möchten. Dies kann nützlich sein, wenn die Verbindung der Appliance mit dem Internet über einen Reverseproxy, durch Hinzufügen zu einem Umkreisnetzwerk oder zu einem überwachten Subnetz hergestellt wird. Durch eine DMZ wird ein LAN (lokales Netzwerk) um eine zusätzliche Sicherheitsebene erweitert.

## Installieren der virtuellen KACE SMA auf einem VMware ESX- oder VMware ESXi-Server

Sie können die virtuelle KACE SMA auf einem Hostsystem mit dem vSphere®-Client von VMware oder vSphere Web Client installieren.

Vor der Installation der virtuellen KACE SMA installieren Sie den vSphere-Client von VMware oder vSphere Web Client auf Ihrem Hostsystem. Führen Sie den vSphere-Client auf einem Computer aus, der sich im selben Netzwerk wie der gewünschte Host befindet, da der Import über ein WAN nicht funktioniert.

1. Um die virtuelle KACE SMA herunterzuladen, gehen Sie auf <https://support.quest.com/kace-systems-management-appliance/download-new-releases>. Ihre Kundenanmeldeinformationen erhalten Sie vom Quest Softwaresupport unter <https://support.quest.com/contact-support>.
2. Laden Sie im Bereich Virtuelle Appliance die komprimierte OVF(Open Virtualization Format)-Datei auf Ihr vSphere-Client-System herunter.
3. Extrahieren Sie die Dateien.
4. Starten Sie das vSphere-Client-Programm und klicken Sie anschließend auf **Datei > OVF-Vorlage bereitstellen**.
5. Wechseln Sie zu dem Ordner, in dem Sie die Dateien extrahiert haben, und wählen Sie die OVF-Datei aus.  
  
Der Installationsassistent wird angezeigt und informiert Sie über die verschiedenen Installationsoptionen.
6. Wählen Sie die Komponenten aus, die für Ihre Implementierung erforderlich sind (Rechenzentrum, Datenspeicher usw.).
7. Klicken Sie auf **Fertig stellen**.
8. Bestätigen Sie die Appliance-Einstellungen. Überprüfen Sie, ob das Netzwerk gültig ist, und überprüfen Sie alle anderen erforderlichen Einstellungen.

## Einschalten der Appliance und Anmelden bei der Administratorkonsole

Beim ersten Einschalten der Appliance können Sie sich über einen beliebigen Computer in Ihrem LAN bei der KACE SMA **Administratorkonsole** anmelden, vorausgesetzt ein DHCP-Server ist verfügbar, um der Appliance eine IP-Adresse zuzuweisen. So können Sie den Setup-Assistenten zum Konfigurieren der anfänglichen Netzwerkeinstellungen verwenden.

Wenn kein DHCP-Server verfügbar ist, können Sie die anfänglichen Netzwerkeinstellungen mithilfe der **Befehlszeilenkonsole** konfigurieren. Siehe [Anfängliche Netzwerkeinstellungen manuell konfigurieren \(optional\)](#).



Die für die Datums- und Uhrzeitinformationen verwendeten Gebietsschemaformate, die bei Ihrer ersten Anmeldung in der **Administratorkonsole** angezeigt werden, sind durch Ihre Browsereinstellungen festgelegt. Informationen zum Ändern der Spracheinstellungen finden Sie im **Administratorhandbuch** der Appliance: [Zugriff auf das Administratorhandbuch und die Onlinehilfe](#).

1. Starten Sie den virtuellen Computer, um die Appliance zu starten. Dieser Vorgang dauert 5 bis 10 Minuten.

Der **Befehlszeilenkonsole**-Anmeldebildschirm wird angezeigt und zeigt die DHCP-Netzwerkeinstellungen der Appliance an.

2. Öffnen Sie auf einem beliebigen mit Ihrem LAN verbundenen Computer einen Browser und rufen die auf dem Befehlszeilenkonsole-Anmeldebildschirm angezeigte URL auf. Zum Beispiel `http://<eindeutiger_KACE_SMA_Appliance_Name>.local/admin`.

Die Seite Softwareübertragungsvereinbarung wird angezeigt.

3. Stimmen Sie der Vereinbarung zu.

Der Assistent für die Ersteinrichtung wird angezeigt.

4. Stellen Sie sicher, dass Sie über die erforderlichen Informationen für die Konfiguration der Appliance verfügen und klicken Sie dann auf **Weiter**.
5. Überprüfen Sie die Informationen auf der Seite Diagnosekonsole für Zweifaktor-Authentifizierung, erfassen Sie den geheimen Schlüssel und die Offline-Tokens und bewahren Sie sie gemäß den Anweisungen an einem sicheren Ort auf.
6. Geben Sie auf der Seite Lizenzierungs- und Administratoreinstellungen folgende Informationen an:

Option	Beschreibung
<b>Lizenzschlüssel</b>	Der Lizenzschlüssel, den Sie in der <b>Begrüßungs</b> -E-Mail von Quest erhalten haben. Wenn Sie keinen Lizenzschlüssel besitzen, wenden Sie sich an den <b>Quest Softwaresupport</b> unter <a href="https://support.quest.com/contact-support">https://support.quest.com/contact-support</a> .
<b>Name der Firma</b>	Der Name Ihrer Firma oder Gruppe.
<b>E-Mail-Adresse des Administrators</b>	Die E-Mail-Adresse, an die Sie Kommunikation von Quest erhalten möchten.
<b>Kennwort</b>	<p>Das Kennwort für das Standardkonto <b>admin</b>. Mit diesem Konto melden Sie sich bei der <b>Administratorkonsole</b> der Appliance an. Das Standardkonto <b>admin</b> ist zu diesem Zeitpunkt das einzige Konto der Appliance. Wenn Sie das Kennwort für dieses Konto vergessen, muss das System möglicherweise auf die Werkseinstellungen zurückgesetzt werden, was einen Datenverlust zur Folge haben kann.</p> <p><b>i</b> Wenn Sie über mehrere KACE SMA oder KACE SDA (Systembereitstellung) Appliances verfügen, empfiehlt Quest, für alle Appliances dasselbe Kennwort für das <b>admin</b>-Konto zu verwenden. Dadurch können Sie die Appliances später verknüpfen. Weitere Informationen hierzu finden Sie im <b>Administratorhandbuch</b> der Appliance: <a href="#">Zugriff auf das Administratorhandbuch und die Onlinehilfe</a>.</p>

## Option

## Beschreibung

### Zweifaktor-Authentifizierung

Wenn Sie mehr Sicherheit für die Benutzer bereitstellen möchten, die sich bei der Appliance anmelden, setzen Sie diese Option auf Aktiviert. Diese Funktion fügt einen zusätzlichen Schritt beim Anmeldevorgang hinzu. Sie vertraut auf die Google Authenticator-App, um Verifizierungscode zu generieren. Die App generiert in regelmäßigen Abständen einen neuen sechsstelligen Code. Wenn diese Option aktiviert ist, werden die Endbenutzer bei jeder Anmeldung aufgefordert, den aktuellen Verifizierungscode einzugeben.



Wenn Sie diese Funktion aktivieren, stellen Sie sicher, dass die Uhr des KACE SMA-Servers und diejenige des Geräts, auf dem Google Authenticator ausgeführt wird, korrekt sind. Der Google Authenticator verlässt sich auf die aktuelle Zeit, um das Token zu erstellen. Wenn die Zeit auf dem Server nicht mit der auf den Geräten synchronisiert ist, auf denen Google Authenticator ausgeführt wird, kann die Validierung von Tokens fehlschlagen, was zur Sperrung von Konten führen kann.

7. Befolgen Sie die Bildschirmanweisungen, um die Ersteinrichtung abzuschließen.

Sobald die Ersteinrichtung abgeschlossen ist, wird die Appliance neu gestartet und die **Administratorkonsole**-Anmeldeseite wird angezeigt.



Wenn Sie die IP-Adresse der Appliance ändern, wechseln Sie zu der neuen IP-Adresse, um die Anmeldeseite aufzurufen.

8. Melden Sie sich bei der Administratorkonsole an und verwenden Sie dazu die Anmelde-ID admin und das Kennwort, das Sie bei der Ersteinrichtung festgelegt haben.

Wenn die Zweifaktor-Authentifizierung auf der Seite Lizenzierungs- und Administratoreinstellungen im Assistenten für die Ersteinrichtung aktiviert wurde, wird die Seite Zweifaktor-Authentifizierung konfigurieren angezeigt.

9. **Nur Zweifaktor-Authentifizierung.** Befolgen Sie die Anweisungen auf der Seite Zweifaktor-Authentifizierung konfigurieren, um einen Google Authenticator-Verifizierungscode mit Ihrem Smartphone zu erstellen, um einen Google Authenticator-Verifizierungscode den Google Authenticator-Code ein und klicken Sie auf **Konfiguration fertig stellen**. Bei jeder nachfolgenden Anmeldung wird ein neuer Verifizierungscode benötigt.

Um diesen Schritt zu überspringen, klicken Sie auf **Weiter**. Sie können diesen Schritt nur innerhalb eines zuvor konfigurierten Übergangszeitfensters überspringen. Weitere Informationen finden Sie im Administratorhandbuch:

Die **Administratorkonsole** wird angezeigt und die Appliance kann verwendet werden.

## Anfängliche Netzwerkeinstellungen manuell konfigurieren (optional)

Wenn kein DHCP-Server verfügbar ist und Sie sich nicht bei der **Befehlszeilenkonsole** der Appliance anmelden können, können Sie die anfänglichen Netzwerkeinstellungen mithilfe der **Administratorkonsole** manuell konfigurieren.

1. Starten Sie den virtuellen Computer, um die Appliance zu starten. Dieser Vorgang dauert 5 bis 10 Minuten.


Der **Befehlszeilenkonsole**-Anmeldebildschirm wird angezeigt.

2. Geben Sie an der Eingabeaufforderung Folgendes ein:



Anmeldename: konfig

Kennwort: konfig

3. Wählen Sie die Sprache, die für die Befehlszeilenkonsole verwendet werden soll. Mit den Pfeiltasten können Sie zwischen den Feldern wechseln.
4. Konfigurieren Sie die folgenden Netzwerkeinstellungen. Mit der Nach-rechts- bzw. der Nach-links-Taste können Sie Optionen in den Feldern auswählen. Mit der Nach-oben- bzw. Nach-unten-Taste können Sie zwischen den Feldern wechseln.

Option	Beschreibung
<b>KACE SMA DNS-Hostname</b>	<p>Geben Sie den Hostnamen der Appliance ein. Die Standardeinstellung ist k1000, aber Quest empfiehlt, den Namen während der Ersteinrichtung zu ändern. Wird der Gerätenamen nicht geändert, kann es zu Problemen kommen, wenn zusätzliche KACE SMA Geräte hinzugefügt werden.</p> <p> Wenn mehrere KACE SMA Geräte mit identischen Namen zum selben Netzwerk gehören, haben diese dieselbe IP-Adresse. Dies kann bei diesen Geräten zu Problemen führen.</p>
<b>Servernamen automatisch generieren</b>	<p>Aktivieren Sie dieses Kontrollkästchen, damit das System den Namen des KACE SMA Webservers im folgenden Format generiert: <b>Hostname.Domain</b>. Beispiel:</p>

Option	Beschreibung
<b>KACE SMA Webservername</b>	<p data-bbox="558 245 1012 368">&lt;eindeutiger_KACE_SMA_Appliance Name&gt;.beispiel.com. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie einen benutzerdefinierten Webservernamen eingeben möchten.</p> <p data-bbox="558 400 1012 727">Geben Sie den vollständig qualifizierten Domainnamen der Appliance ein. Hierbei handelt es sich um den mit der <b>Domain</b> verknüpften <b>Hostnamen</b>. Beispiel: &lt;eindeutiger_KACE_SMA_Appliance Name&gt;.beispiel.com. Geräte stellen über diesen Namen eine Verbindung mit der Appliance her. Quest empfiehlt, dass Sie dem DNS-Server einen statischen IP-Adresseintrag für die Appliance hinzufügen. Wenn Sie ein SSL-Zertifikat verwenden, muss der Hostname vollständig und gültig sein und demjenigen auf dem Zertifikat entsprechen.</p>
<b>DHCP</b>	<p data-bbox="558 756 1012 1007">(Optional) Wählen Sie diese Option, wenn Sie DHCP (Dynamic Host Configuration Protocol) verwenden möchten, um die IPv4-Adresse und andere Informationen zur Netzwerkkonfiguration für die Appliance automatisch zu beziehen. Wenn Sie diese Option wählen, müssen Sie keine Einstellungen für die statische IP-Adresse, die Domain, die Subnetzmaske, den Standard-Gateway und den primären bzw. sekundären DNS-Server angeben.</p>
<b>Manuelle IPv4-Konfiguration</b>	<p data-bbox="558 1035 1012 1158">Legen Sie die IPv4-Adresse fest und geben Sie die statische IP-Adresse, die Domain, die Subnetzmaske, das Standard-Gateway und die primären bzw. sekundären DNS-Einstellungen für die Appliance an.</p> <div data-bbox="566 1174 583 1222" style="border-left: 1px solid black; padding-left: 5px; margin-left: 10px;"> <p data-bbox="566 1174 1012 1286"><b>i</b> Die IPv4-Adresse ist unabhängig von der Verfügbarkeit einer IPv6-Adresse erforderlich. Die IPv6-Adresse ist optional.</p> </div>
<b>SLAAC</b>	<p data-bbox="558 1308 1012 1455">Wählen Sie diese Option aus, wenn Sie SLAAC (Stateless Address Autoconfiguration – zustandslose Adressenautokonfiguration) verwenden möchten, die im Rahmen von IPv6 verfügbar ist, um die Netzwerkeinstellungen der Appliance zu konfigurieren. Mit SLAAC</p>

Option	Beschreibung
<b>Manuelle IPv6-Konfiguration</b>	<p>können Geräte ihre eigenen IPv6-Adressen basierend auf dem Präfix auswählen, das von der verbundenen Schnittstelle mitgeteilt wird.</p> <p>Wählen Sie diese Option, wenn Sie die IPv6-Adresse manuell angeben möchten. Wenn Sie diese Option auswählen, müssen Sie IPv6-Adresse, Präfixlänge und Standard-Gateway für die Appliance angeben.</p> <p> Die IPv6-Adresse ist optional. Die IPv4-Adresse ist unabhängig von der Verfügbarkeit einer IPv6-Adresse erforderlich.</p>
<b>Deaktivieren Sie IPv6.</b>	<p>Wählen Sie diese Option, wenn Sie die IPv6-Adresse für die Appliance deaktivieren möchten. Dies ist die Standardeinstellung.</p>
<b>SMTP-Server</b>	<p>(Optional) Geben Sie den Hostnamen oder die IP-Adresse eines externen SMTP-Servers an, beispielsweise smtp.gmail.com. Externe SMTP-Server müssen die anonyme (nicht authentifizierte) Übermittlung ausgehender E-Mails unterstützen. Vergewissern Sie sich, dass es Ihre Netzwerkrichtlinien der Appliance gestatten, den SMTP-Server direkt zu kontaktieren. Der E-Mail-Server muss zudem für die Weiterleitung von E-Mails von der Appliance ohne Authentifizierung konfiguriert sein. Wenn Sie keine SMTP-Serverinformationen angeben, sendet die KACE SMA E-Mails über ihren internen SMTP-Server.</p>
<b>SSH aktiviert</b>	<p>(Optional) Wählen Sie diese Option, um den sicheren Zugriff (SSH) auf die <b>Administratorkonsole</b> der Appliance zu aktivieren. Quest empfiehlt, SSH während der Ersteinrichtung zu aktivieren. Wenn die Einrichtung abgeschlossen ist, können Sie diese Einstellung bei Bedarf über die <b>Administratorkonsole</b> ändern.</p>
<b>Proxy</b>	<p>(Optional) Geben Sie die Informationen des Proxy-Servers ein.</p> <p> Die Appliance unterstützt Proxy-Server mit bereichsbasierter Standardauthentifizierung, für die</p>

Option	Beschreibung
	Benutzernamen und Kennwörter erforderlich sind. Verwendet Ihr Proxy-Server eine andere Authentifizierungsmethode, fügen Sie die IP-Adresse der Appliance zur Ausnahmeliste des Servers hinzu.
5.	<p>Verschieben Sie den Cursor mithilfe der Nach-unten-Taste auf Speichern und drücken Sie dann die <b>Eingabetaste</b>.</p> <p>Die Appliance wird neu gestartet.</p>
6.	<p>Öffnen Sie auf einem beliebigen mit Ihrem LAN verbundenen Computer einen Browser und rufen die Administratorkonsole-URL der Appliance auf. Zum Beispiel <code>http://&lt;eindeutiger_KACE_SMA_Appliance_Name&gt;.local/admin</code>.</p> <p>Die Seite Softwareübertragungsvereinbarung wird angezeigt.</p>
7.	<p>Stimmen Sie der Vereinbarung zu.</p> <p>Der Assistent für die Ersteinrichtung wird angezeigt.</p>
8.	<p>Stellen Sie sicher, dass Sie über die erforderlichen Informationen für die Konfiguration der Appliance verfügen und klicken Sie dann auf <b>Weiter</b>.</p>
9.	<p>Überprüfen Sie die Informationen auf der Seite Diagnosekonsole für Zweifaktor-Authentifizierung, erfassen Sie den geheimen Schlüssel und die Offline-Tokens und bewahren Sie sie gemäß den Anweisungen an einem sicheren Ort auf.</p>
10.	<p>Geben Sie auf der Seite Lizenzierungs- und Administratoreinstellungen folgende Informationen an:</p>

Option	Beschreibung
<b>Lizenzschlüssel</b>	Der Lizenzschlüssel, den Sie in der <b>Begrüßungs</b> -E-Mail von Quest erhalten haben. Wenn Sie keinen Lizenzschlüssel besitzen, wenden Sie sich an den <b>Quest Softwaresupport</b> unter <a href="https://support.quest.com/contact-support">https://support.quest.com/contact-support</a> .
<b>Name der Firma</b>	Der Name Ihrer Firma oder Gruppe.
<b>E-Mail-Adresse des Administrators</b>	Die E-Mail-Adresse, an die Sie Kommunikation von Quest erhalten möchten.
<b>Kennwort</b>	Das Kennwort für das Standardkonto <b>admin</b> . Mit diesem Konto melden Sie sich bei der <b>Administratorkonsole</b> der Appliance an. Das Standardkonto <b>admin</b> ist zu diesem Zeitpunkt das einzige Konto der Appliance. Wenn Sie das Kennwort für dieses Konto vergessen,



## Option

## Beschreibung

muss das System möglicherweise auf die Werkseinstellungen zurückgesetzt werden, was einen Datenverlust zur Folge haben kann.



Wenn Sie über mehrere KACE SMA oder KACE SDA (Systembereitstellung) Appliances verfügen, empfiehlt Quest, für alle Appliances dasselbe Kennwort für das **admin**-Konto zu verwenden. Dadurch können Sie die Appliances später verknüpfen. Weitere Informationen hierzu finden Sie im **Administratorhandbuch** der Appliance: [Zugriff auf das Administratorhandbuch und die Onlinehilfe](#).

## Zweifaktor-Authentifizierung

Wenn Sie mehr Sicherheit für die Benutzer bereitstellen möchten, die sich bei der Appliance anmelden, setzen Sie diese Option auf Aktiviert. Diese Funktion fügt einen zusätzlichen Schritt beim Anmeldevorgang hinzu. Sie vertraut auf die Google Authenticator-App, um Verifizierungscodes zu generieren. Die App generiert in regelmäßigen Abständen einen neuen sechsstelligen Code. Wenn diese Option aktiviert ist, werden die Endbenutzer bei jeder Anmeldung aufgefordert, den aktuellen Verifizierungscode einzugeben.



Wenn Sie diese Funktion aktivieren, stellen Sie sicher, dass die Uhr des KACE SMA-Servers und diejenige des Geräts, auf dem Google Authenticator ausgeführt wird, korrekt sind. Der Google Authenticator verlässt sich auf die aktuelle Zeit, um das Token zu erstellen. Wenn die Zeit auf dem Server nicht mit der auf den Geräten synchronisiert ist, auf denen Google Authenticator ausgeführt wird, kann die Validierung von Tokens fehlschlagen, was zur Sperrung von Konten führen kann.

11. Befolgen Sie die Bildschirmanweisungen, um die Ersteinrichtung abzuschließen.

Sobald die Ersteinrichtung abgeschlossen ist, wird die Appliance neu gestartet und die **Administratorkonsole**-Anmeldeseite wird angezeigt.



Wenn Sie die IP-Adresse der Appliance ändern, wechseln Sie zu der neuen IP-Adresse, um die Anmeldeseite aufzurufen.

12. Melden Sie sich bei der Administratorkonsole an und verwenden Sie dazu die Anmelde-ID admin und das Kennwort, das Sie bei der Ersteinrichtung festgelegt haben.

Wenn die Zweifaktor-Authentifizierung auf der Seite Lizenzierungs- und Administratoreinstellungen im Assistenten für die Ersteinrichtung aktiviert wurde, wird die Seite Zweifaktor-Authentifizierung konfigurieren angezeigt.

13. **Nur Zweifaktor-Authentifizierung.** Befolgen Sie die Anweisungen auf der Seite Zweifaktor-Authentifizierung konfigurieren, um einen Google Authenticator-Verifizierungscode mit Ihrem Smartphone zu erstellen. Geben Sie in das Feld Verifizierungscode den Google Authenticator-Code ein und klicken Sie auf **Konfiguration fertig stellen**. Bei jeder nachfolgenden Anmeldung wird ein neuer Verifizierungscode benötigt.

Um diesen Schritt zu überspringen, klicken Sie auf **Weiter**. Sie können diesen Schritt nur innerhalb eines zuvor konfigurierten Übergangszeitfensters überspringen. Weitere Informationen finden Sie im Administratorhandbuch:

Die **Administratorkonsole** wird angezeigt und die Appliance kann verwendet werden.

## Zugriff auf das Administratorhandbuch und die Onlinehilfe

Um Hilfe zur Verwendung der **Administratorkonsole** zu erhalten, klicken Sie auf den Hilfelink in der oberen rechten Ecke der Oberfläche, um die kontextbezogene Hilfe aufzurufen. Klicken Sie auf die Links in den Themen der kontextbezogenen Hilfe, um auf das Haupthilfesystem zuzugreifen.



## Zeitplanung für Schulungen

Um Sie bei der Verwendung der Appliance zu unterstützen, bietet Quest ein Schulungsprogramm mit dem Titel "QuickStart" an. Dieses Programm bietet Remote-Unterstützung, sodass Ihre Lösung schnell einsatzbereit gemacht werden kann, um die Bereitstellung, Verwaltung, Sicherung und Wartung Ihrer mit dem Netzwerk verbundenen Geräte zu beschleunigen.

Um mehr über dieses Programm zu erfahren, rufen Sie einen der folgenden Links auf:

- **KACE Systemverwaltungs-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>

Senden Sie für die Registrierung eine Anfrage an:

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

## Über uns

Quest entwickelt Softwarelösungen, die sich die Vorteile neuer Technologien bei einer immer komplexer werdenden IT-Infrastruktur zu Nutze machen. Von der Datenbank- und Systemverwaltung über Active Directory- und Office 365-Verwaltung bis hin zur Erhöhung der Widerstandskraft gegen Cyberrisiken unterstützt Quest Kunden bereits jetzt bei der Bewältigung ihrer nächsten IT-Herausforderung. Weltweit verlassen sich mehr als 130.000 Unternehmen und 95 % der Fortune 500-Unternehmen auf Quest, um proaktive Verwaltung und Überwachung für die nächste Unternehmensinitiative bereitzustellen, die nächste Lösung für komplexe Microsoft-Herausforderungen zu finden, und der nächsten Bedrohung immer einen Schritt voraus zu sein. Quest Software. Wo die Zukunft auf die Gegenwart trifft. Weitere Informationen hierzu finden Sie unter [www.quest.com](http://www.quest.com).

## Ressourcen für den technischen Support

Der technische Support steht Quest Kunden mit gültigem Servicevertrag sowie Kunden mit Testversionen zur Verfügung. Auf das Quest Support Portal können Sie unter <https://support.quest.com/de-de/> zugreifen.

Im Support-Portal finden Sie Tools zur Selbsthilfe, mit denen Probleme rund um die Uhr schnell und selbständig gelöst werden können. Das Support-Portal bietet folgende Möglichkeiten:

- Einreichen und Verwalten einer Serviceanfrage
- Anzeigen von Knowledge Base-Artikeln
- Registrieren für Produktbenachrichtigungen
- Herunterladen von Software und technischer Dokumentation
- Anzeigen von Anleitungsvideos
- Teilnehmen an Community-Diskussionen
- Online Chatten mit Supporttechnikern
- Anzeigen von Services, die Sie bei Ihrem Produkt unterstützen können


# アプライアンスのセットアップ

このガイドでは、仮想 KACE システム管理アプライアンス (SMA) を VMware® ESX® または VMware ESXi™ ホストシステムにセットアップする方法について説明します。仮想 KACE SMA では専用のハードウェアを必要としません。

追加マニュアルについては、<https://support.quest.com/kace-systems-management-appliance/technical-documents> に進みます。

## はじめに

アプライアンスを設定する前に、いくつかの作業を行っていただく必要があります。

1. 仮想KACE SMAをQuestの営業担当から購入します ( <https://www.quest.com/company/contact-us.aspx> )。
2. DHCP サーバーを使用して IP アドレスをアプライアンスに自動的に割り当てるか、アプライアンスの静的 IP アドレスを取得するかを決定します。
3. アプライアンスの静的 IP アドレスを取得する場合は、社内の DNS (ドメインネームシステム) サーバーの A レコードに、アプライアンスのホスト名を入力します。「A」レコードは「MX」レコードのホスト名を定義します。これにより、ユーザーはサービスデスクにEメールチケットを送信できるようになります。アプライアンスのホスト名は、デフォルトでは「k1000」ですが、初期セットアップ中にこの名前をより固有な値に変更することをお勧めします。  
 アプライアンス名を変更しないままにしておくと、追加のKACE SMAアプライアンスが導入されたときに問題が発生することがあります。同じネットワークに属する同一の名前を持つ複数のKACE SMAアプライアンスは、同じIPアドレスを持ちます。このため、これらのアプライアンスに関する問題が発生することがあります。
4. スプリットDNSを使用するかどうか決定します。スプリット DNS は、リバースプロキシを使用してアプライアンスをインターネットに接続する場合や、アプライアンスを境界ネットワークやスクリーンサブネットに配置する場合に便利です。DMZでは、LAN (ローカルエリアネットワーク) に新たなセキュリティレイヤが追加されます。

## VMware ESXまたはVMware ESXiサーバへの仮想KACE SMAのインストール

VMware vSphere®クライアントまたはvSphere Webクライアントがインストールされているホストシステムに、仮想KACE SMAをインストールすることができます。

仮想KACE SMAをインストールする前に、VMware vSphereクライアントまたはvSphere Webクライアントをホストシステムにインストールする必要があります。WANを介してのインポートは使用できないため、指定されたホストと同じネットワーク上のコンピューターでvSphereクライアントを実行します。

1. 仮想KACE SMAをダウンロードするには、<https://support.quest.com/kace-systems-management-appliance/download-new-releases>にアクセスします。ログイン資格情報の入

手方法については、Quest Software サポート (<https://support.quest.com/contact-support>) までお問い合わせください。

2. 仮想アプライアンス セクションから、OVF ( Open Virtualization Format ) 圧縮ファイルを vSphere クライアントシステムにダウンロードします。
3. ファイルを解凍します。
4. vSphere クライアントプログラムを起動し、ファイル > OVF テンプレートの展開 の順にクリックします。
5. ファイルの解凍先フォルダを参照し、OVFファイルを選択します。  
インストールウィザードが起動し、インストールに関する選択肢が表示されます。
6. 実装に必要なコンポーネント ( データセンター、データストアなど ) を選択します。
7. 終了 をクリックします。
8. アプライアンスの設定を確認します。ネットワークが有効かどうかを確認し、その他の必要な設定についても確認します。

## アプライアンスの電源投入と管理者コンソールへのログイン

最初にアプライアンスの電源をオンにするとき、LAN 上の任意のコンピュータから KACE SMA 管理者コンソールにログインできます。ただし、アプライアンスにIPアドレスを割り当てるための DHCP サーバーが必要です。それによって、セットアップウィザードを使用して、初期ネットワーク設定を構成できます。

DHCPサーバーがない場合は、コマンドラインコンソールを使用して、初期ネットワーク設定を構成できます。詳細については、「[手動による初期ネットワーク設定の構成 \( オプション \)](#)」を参照してください。



使用しているブラウザの設定に基づいて、初回ログイン時に管理者コンソールに表示される日付と時刻情報に使用されるロケール形式が決定されます。言語設定の変更の詳細については、アプライアンスの『[Administrator Guide](#)』 ( 管理者ガイド ) を参照してください：[管理者ガイドおよびオンラインヘルプへのアクセス](#)。

1. 仮想マシンの電源をオンにして、アプライアンスを起動します。起動まで5~10分かかります。  
コマンドラインコンソールのログイン画面が表示され、アプライアンスのDHCPネットワーク設定を示します。
2. LANに接続されている任意のコンピューター上でブラウザを開き、コマンドラインコンソールのログイン画面に表示されているURLにアクセスします。例：[http://<一意のKACE\\_SMAアプライアンス名>.local/admin](http://<一意のKACE_SMAアプライアンス名>.local/admin)。  
ソフトウェア取引契約書 ページが表示されます。
3. 契約書に同意します。  
初期セットアップ ウィザードが表示されます。

4. アプライアンスの設定に必要な情報がすべてそろっていることを確認したら、次へ をクリックします。
5. 指示に従って、表示される 診断コンソールの 2 要素認証 ページの情報を確認し、シークレットキーとオフライントークンを安全な場所に記録します。
6. ライセンスと管理者の設定 ページで、以下の情報を入力します。

オプション	説明
ライセンスキー	Questからの案内のEメールに記載されているライセンスキーです。ライセンスキーがない場合は、 <b>Quest Software サポート</b> ( <a href="https://support.quest.com/contact-support">https://support.quest.com/contact-support</a> ) お問い合わせをください。
会社名	会社またはグループの名前です。
管理者Eメール	Questからの連絡の宛先となるEメールアドレスです。
パスワード	<p>デフォルトの <b>admin</b> アカウントのパスワードです。このアカウントは、アプライアンスの管理者コンソールにログインするために使用します。この時点でデフォルトの <b>admin</b> アカウントがアプライアンス上で唯一のアカウントになります。このアカウントのパスワードを忘れると、システムを出荷時のデフォルト状態にリセットすることが必要になる場合があり、データロスが発生します。</p> <div style="border-left: 1px solid black; padding-left: 10px; margin-top: 10px;"> <p><b>i</b> 複数のKACE SMAまたはKACE SDA (システム導入) アプライアンスを使用する場合、Questでは、すべてのアプライアンスの<b>admin</b>アカウントに同じパスワードを使用することをお勧めします。これにより、後でアプライアンス同士をリンクすることが可能になります。詳細については、アプライアンスの『<b>Administrator Guide</b>』(管理者ガイド)を参照してください：<a href="#">管理者ガイドおよびオンラインヘルプへのアクセス</a>。</p> </div>

- 2 要素認証
 

アプライアンスにログインしているユーザーのセキュリティをより強力にするには、この設定を有効にします。この機能では、ログインプロセスにステップが 1 つ追加されます。これは、Google Authenticator アプリケーションに依存して検証コードを生成します。このアプリは、定期的に新しい 6 桁のコードを生成しま

す。有効にすると、エンドユーザーはログインするたびに現在の検証コードを要求されます。



この機能を有効にする場合は、KACE SMA サーバのクロック、および Google Authenticator を実行しているデバイスが正確であることを確認してください。Google Authenticator は、現在の時刻に依存してトークンを作成します。サーバのクロックが Google Authenticator を実行しているデバイスのクロックと同期されていない場合、トークンの検証が失敗し、アカウントのロックアウトが発生する可能性があります。

7. 画面の指示に従って、初期セットアップを完了します。

初期セットアップが完了すると、アプライアンスが再起動し、管理者コンソールのログインページが表示されます。



アプライアンスの IP アドレスを変更する場合は、新しいアドレスにアクセスして、ログインページを表示します。

8. ログイン ID 「admin」と、初期セットアップ中に選択したパスワードを使用して、管理者コンソールにログインします。

初期セットアップウィザードのライセンスと管理者の設定 ページで 2 要素認証が有効になっている場合は、2 要素認証の設定 ページが表示されます。

9. **2 要素認証のみ。** 2 要素認証の設定 ページの指示に従い、スマートフォンを使用して Google Authenticator の検証コードを生成します。検証コード フィールドに、Google Authenticator のコードを入力し、**設定を完了** をクリックします。その後はログインのために新しい検証コードが要求されます。

この手順をスキップするには、**設定をスキップ** をクリックします。このステップは、設定されている移行ウィンドウでのみバイパスできます。詳細については、『管理者ガイド』を参照してください。

管理者コンソールが表示され、アプライアンスが使用可能になります。

## 手動による初期ネットワーク設定の構成 (オプション)

DHCPサーバがないためアプライアンスのコマンドラインコンソールにログインできない場合は、管理者コンソールを使用して、初期ネットワーク設定を手動で構成することができます。

1. 仮想マシンの電源をオンにして、アプライアンスを起動します。起動まで5~10分かかります。

コマンドラインコンソールのログイン画面が表示されます。

2. プロンプトで、次のように入力します。

ログイン : konfig

パスワード : konfig

3. コマンドラインコンソールで使用する言語を選択します。上矢印キーと下矢印キーを使用してフィールド間を移動します。
4. 以下のネットワーク設定を構成します。フィールド内のオプションを選択するには、右矢印キーと左矢印キーを使用します。フィールド間を移動するには、上矢印キーと下矢印キーを使用します。

## オプション

## 説明

### KACE SMA DNSホスト名

アプライアンスのホスト名を入力します。デフォルトは「k1000」ですが、初期セットアップ中にこの名前をより固有な値に変更することをお勧めします。アプライアンス名を変更しないままにしておく、追加のKACE SMAアプライアンスが導入されたときに問題が発生することがあります。



同じネットワークに属する同一の名前を持つ複数のKACE SMAアプライアンスは、同じIPアドレスを持ちます。このため、これらのアプライアンスに関する問題が発生することがあります。

### 自動的に生成されたサーバ名

このチェックボックスをオンにすると、次のフォーマットを使用して、KACE SMAウェブサーバ名をシステムで生成できます。ホスト名.ドメイン。例：<一意のKACE\_SMAアプライアンス名>.example.com。このチェックボックスをオフにすると、カスタムのウェブサーバ名を入力できます。

### KACE SMAウェブサーバ名

アプライアンスの完全修飾ドメイン名を入力します。完全修飾ドメイン名とは、ホスト名とドメインを連結した値です。例：<一意のKACE\_SMAアプライアンス名>.example.com。デバイスは、この名前を使用してアプライアンスに接続します。Questでは、DNSサーバに、アプライアンスの静的IPアドレスのエントリを追加することをお勧めします。SSL証明書を使用する場合、証明書と同じ完全修飾ホスト名を使用する必要があります。

### DHCP

(オプション) このオプションは、DHCP (動的ホスト構成プロトコル) を使用して、アプラ



## オプション

## 説明

	<p>イアンスの IPv4 アドレスおよびその他のネットワーク設定情報を自動的に取得するときに選択します。このオプションを選択すると、静的 IP アドレス、ドメイン、サブネットマスク、デフォルトゲートウェイ、プライマリ DNS、およびセカンダリ DNS の設定を入力する必要がなくなります。</p>
手動 IPv4 設定	<p>IPv4 アドレスを指定して、アプライアンスの静的 IP アドレス、ドメイン、サブネットマスク、デフォルトゲートウェイ、プライマリ DNS、またはセカンダリ DNS 設定を入力します。</p> <p><b>i</b> IPv4 アドレスは、IPv6 アドレスが使用可能であるかどうかに関わらず必要です。IPv6 アドレスはオプションです。</p>
SLAAC	<p>アプライアンスのネットワーク設定を構成するために、IPv6 により提供される、SLAAC (ステートレスアドレス自動設定) を使用する場合は、このオプションを選択します。SLAAC では、デバイスは接続済みのインターフェイスから通知されたプレフィックスに基づいて独自の IPv6 アドレスを選択できます。</p>
手動 IPv6 設定	<p>IPv6 アドレスを手動で指定する場合は、このオプションを選択します。このオプションを選択した場合は、アプライアンスの IPv6 アドレス、プレフィックス長、デフォルトゲートウェイを指定する必要があります。</p> <p><b>i</b> IPv6 アドレスはオプションです。IPv4 アドレスは、IPv6 アドレスが使用可能であるかどうかに関わらず必要です。</p>
IPv6 を無効にする	<p>アプライアンスの IPv6 アドレスを無効にする場合は、このオプションを選択します。これはデフォルトの設定です。</p>
SMTPサーバ	<p>(オプション) 外部 SMTP サーバのホスト名または IP アドレスを指定します (「smtp.gmail.com」など)。外部 SMTP サーバでは、匿名 (認証なし) のアウトバウンド E メール転送を許可する必要があります。ネットワークポリシーで、アプライアンスが SMTP サーバに直接問い合わせられることを確認します。また、メールサーバは、アプライアンスからの Eメールのリレーを、認証なしで許可するように設定する必要があります。SMTPサーバ情</p>

## オプション

## 説明

### SSHを有効にする

報を入力しなかった場合、KACE SMAは使用する社内のSMTPサーバにEメールを送信します。

(オプション) このオプションを選択すると、アプライアンスの管理者コンソールへのSSH (セキュア) アクセスが有効になります。Questでは、アプリケーションの初期セットアップ中に、SSHを有効にすることをお勧めします。セットアップが完了したら、管理者コンソールで必要に応じて設定を変更できます。

### プロキシ

(オプション) プロキシサーバーの情報を入力します。



アプライアンスでは、ユーザー名とパスワードを要求する、基本的なレムベースの認証を使用したプロキシサーバーをサポートしています。プロキシサーバーが他の種類の認証を使用する場合は、プロキシサーバーの例外リストにアプライアンスのIPアドレスを追加してください。

5. 下矢印キーを使用してカーソルを 保存 に移動し、EnterキーまたはReturnキーを押しません。

アプライアンスが再起動します。

6. LANに接続されている任意のコンピューター上でブラウザを開き、アプライアンスの管理者コンソールのURLにアクセスします。例: `http://<一意のKACE_SMAアプライアンス名>.local/admin`。

ソフトウェア取引契約書 ページが表示されます。

7. 契約書に同意します。

初期セットアップ ウィザードが表示されます。

8. アプライアンスの設定に必要な情報がすべてそろっていることを確認したら、次へ をクリックします。
9. 指示に従って、表示される 診断コンソールの 2 要素認証 ページの情報を確認し、シークレットキーとオフライントークンを安全な場所に記録します。
10. ライセンスと管理者の設定 ページで、以下の情報を入力します。

## オプション

## 説明

### ライセンスキー

Questからの案内のEメールに記載されているライセンスキーです。ライセンスキーがない場合は、**Quest Software サポート** (<https://>

## オプション

## 説明

	<a href="https://support.quest.com/contact-support">support.quest.com/contact-support</a> ) にお問い合わせください。
会社名	会社またはグループの名前です。
管理者Eメール	Questからの連絡の宛先となるEメールアドレスです。
パスワード	<p>デフォルトの <b>admin</b> アカウントのパスワードです。このアカウントは、アプライアンスの管理者コンソールにログインするために使用しません。この時点でデフォルトの <b>admin</b> アカウントがアプライアンス上で唯一のアカウントになります。このアカウントのパスワードを忘れると、システムを出荷時のデフォルト状態にリセットすることが必要になる場合があり、データロスが発生します。</p> <p><b>i</b> 複数のKACE SMAまたはKACE SDA (システム導入) アプライアンスを使用する場合、Questでは、すべてのアプライアンスの<b>admin</b>アカウントに同じパスワードを使用することをお勧めします。これにより、後でアプライアンス同士をリンクすることが可能になります。詳細については、アプライアンスの『<b>Administrator Guide</b>』(管理者ガイド)を参照してください：<a href="#">管理者ガイドおよびオンラインヘルプへのアクセス</a>。</p>

## 2 要素認証

アプライアンスにログインしているユーザーのセキュリティをより強力にするには、この設定を有効にします。この機能では、ログインプロセスにステップが1つ追加されます。これは、Google Authenticator アプリケーションに依存して検証コードを生成します。このアプリは、定期的に新しい6桁のコードを生成します。有効にすると、エンドユーザーはログインするたびに現在の検証コードを要求されます。

**i** この機能を有効にする場合は、KACE SMA サーバのクロック、および Google Authenticator を実行しているデバイスが正確であることを確認してください。Google Authenticator は、現在の時刻に依存してトークンを作成します。サーバのクロックが Google Authenticator を実行しているデバイス

のクロックと同期されていない場合、トークンの検証が失敗し、アカウントのロックアウトが発生する可能性があります。

11. 画面の指示に従って、初期セットアップを完了します。

初期セットアップが完了すると、アプライアンスが再起動し、管理者コンソールのログインページが表示されます。



アプライアンスの IP アドレスを変更する場合は、新しいアドレスにアクセスして、ログインページを表示します。

12. ログイン ID 「admin」と、初期セットアップ中に選択したパスワードを使用して、管理者コンソールにログインします。

初期セットアップウィザードのライセンスと管理者の設定 ページで 2 要素認証が有効になっている場合は、2 要素認証の設定 ページが表示されます。

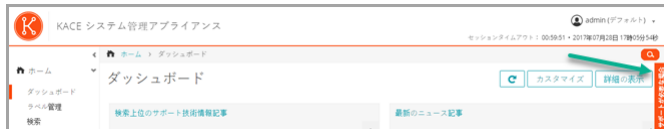
13. **2 要素認証のみ。** 2 要素認証の設定 ページの指示に従い、スマートフォンを使用して Google Authenticator の検証コードを生成します。検証コード フィールドに、Google Authenticator のコードを入力し、**設定を完了** をクリックします。その後はログインのたびに新しい検証コードが要求されます。

この手順をスキップするには、**設定をスキップ** をクリックします。このステップは、設定されている移行ウィンドウでのみバイパスできます。詳細については、『管理者ガイド』を参照してください。

管理者コンソールが表示され、アプライアンスが使用可能になります。

## 管理者ガイドおよびオンラインヘルプへのアクセス

管理者コンソールの使用のヘルプを表示するには、インターフェースの右上隅にあるヘルプリンクをクリックして、コンテキスト依存ヘルプを開きます。メインのヘルプシステムにアクセスするには、コンテキスト依存ヘルプのトピック内のリンクをクリックします。



## トレーニングのスケジュール設定

Quest では、アプライアンスの使用に役立てていただけるように、QuickStart と呼ばれるトレーニングプログラムを提供しています。このプログラムは、ネットワーク接続されたデバイスのプ

ロビジョニング、管理、セキュリティ保護、およびサービスを開始するために、ソリューションを迅速に導入して実行するためのリモートアシスタンスを提供します。

このプログラムの詳細については、次のリンクのいずれかをご覧ください。

- **KACEシステム管理アプライアンス** : <https://support.quest.com/kace-systems-management-appliance/professional-services/332>
- **KACE 資産管理アプライアンス** : <https://support.quest.com/kace-asset-management-appliance/professional-services/331>

登録するには、次の場所でリクエストを送信してください。

- **KACEシステム管理アプライアンス** : <https://www.quest.com/register/113381>
- **KACE 資産管理アプライアンス** : <https://www.quest.com/register/113379>

## 当社について

Quest は、複雑化する IT 環境において、新しいテクノロジーの利点を現実のものにするソフトウェアソリューションを生み出しています。データベースとシステム管理から Active Directory と Office 365 の管理、サイバーセキュリティの回復力まで、Quest はお客様の次の IT の課題を今すぐ解決できるように支援します。世界中で、130,000 社以上の企業と Fortune 500 企業の 95% が、次の企業イニシアチブのプロアクティブな管理と監視を実施し、複雑なマイクロソフトの課題に対応する次のソリューションを見つけ、次の脅威に先んじるために、Quest を頼りにしています。Quest Software。今「次」に備える。詳細に関しては、「[www.quest.com](http://www.quest.com)」を参照してください。

## テクニカルサポートのリソース

Quest の有効なメンテナンス契約をお持ちのお客様、および試用版をお持ちのお客様は、テクニカルサポートをご利用いただけます。Quest サポート ポータルは、<https://support.quest.com> からアクセスできます。

サポートポータルは、問題を迅速に自身で解決するのに使用できるセルフヘルプツールを提供しており、毎日24時間アクセスできます。このサイトでは、以下の操作を実行できます。

- サービスリクエストの送信と管理
- サポート技術情報記事の表示
- 製品情報への登録
- ソフトウェアと技術文書のダウンロード
- 説明ビデオの再生
- コミュニティの討論への参加
- サポートエンジニアとのオンラインチャット
- 製品のサポートサービスの表示

# Configuração do equipamento

**Este guia explica como configurar a Solução de gerenciamento de sistemas KACE (SMA) virtual nos sistemas host VMware® ESX® ou VMware ESXi™. O KACE SMA virtual não requer hardware dedicado.**

Para obter a documentação adicional, vá para <https://support.quest.com/kace-systems-management-appliance/technical-documents>.

## Antes de começar

Antes de configurar a solução, há algumas ações preliminares que você precisa realizar.

1. Compre uma licença do KACE SMA virtual com o departamento de vendas da Quest em <https://www.quest.com/company/contact-us.aspx>.
2. Decida se utilizará um servidor DHCP para atribuir automaticamente um endereço IP ao equipamento, ou para obter um endereço IP estático para o equipamento.
3. Se você obter um endereço IP estático para a solução, insira o nome de host da solução no registro A do seu servidor DNS (Domain Name System) interno. O registro A define o nome do host para o registro MX e isto permite que usuários enviem tiquetes por e-mail para o Service Desk. Por padrão, o nome do host da solução é k1000, mas a Quest recomenda a alteração desse nome para um mais exclusivo durante a configuração inicial.



Não alterar o nome da solução pode causar problemas quando soluções adicionais do KACE SMA forem introduzidas. Várias soluções do KACE SMA com nomes idênticos e pertencentes à mesma rede terão o mesmo endereço IP, o que pode causar problemas para essas soluções.

4. Decida se utilizará um DNS dividido. Isso pode ser útil se a solução se conectar à Internet utilizando um proxy reverso ou colocar a solução em uma rede de perímetro ou sub-rede filtrada. Uma DMZ adiciona uma camada adicional de segurança a uma LAN (Local Area Network, Rede de Área Local).

## Instalar o KACE SMA virtual em um servidor VMware ESX ou VMware ESXi

É possível instalar o KACE SMA virtual em um sistema host que tenha o VMware vSphere® Client ou o vSphere Web Client instalado.

Antes de instalar o KACE SMA virtual, é necessário instalar o VMware vSphere Client, ou o vSphere Web Client no seu sistema host. Execute o cliente do vSphere em um computador que esteja na mesma rede que o host designado porque a importação por WAN não funciona.

1. Para baixar o KACE SMA virtual, acesse <https://support.quest.com/kace-systems-management-appliance/download-new-releases>. Para obter suas credenciais de login do cliente, entre em contato com o Suporte ao software da Quest em <https://support.quest.com/contact-support>.

2. Na seção **Appliance virtual**, faça o download do arquivo OVF (Open Virtualization Format) compactado para o sistema do vSphere Client.
3. Extraia os arquivos.
4. Inicie o programa vSphere Client clique em **Arquivo > Implantar modelo de OVF**.
5. Navegue até a pasta na qual você extraiu os arquivos e selecione o arquivo OVF.  
O assistente de instalação é exibido e oferece as opções de instalação.
6. Selecione os componentes exigidos por sua implementação: centro de dados, repositório de dados e assim por diante.
7. Clique em **Concluir**.
8. Confirme as configurações da solução. Verifique se há uma rede válida e outras configurações necessárias.

## Ligue a solução e faça login no Console do administrador

Quando o equipamento for ligado pela primeira vez, você poderá fazer login no **Console do administrador** do KACE SMA de qualquer computador em sua LAN, desde que um servidor DHCP esteja disponível para atribuir um endereço IP a ele. Isso permite o uso do assistente de configuração para definir as configurações iniciais de rede.

Se um servidor DHCP não estiver disponível, você poderá definir as configurações iniciais de rede usando o **Console da linha de comando**. Consulte [Definir as configurações iniciais de rede manualmente \(opcional\)](#).



A configuração do navegador determinará os formatos de local usados para as informações de data e hora exibidas no **Console do administrador** ao fazer o login pela primeira vez. Para obter mais informações sobre como alterar as configurações de idioma, consulte o **Guia do Administrador** do equipamento: [Acessar o Guia do administrador e a Ajuda on-line](#).

1. Ligue a máquina virtual para inicializar a solução. Isso pode levar de 5 a 10 minutos.  
A tela de login do **Console da linha de comando** é exibida e mostra as configurações de DHCP da rede da solução.
2. Em qualquer computador conectado à sua LAN, abra um navegador e vá para o URL exibido na tela de login do Console da linha de comando. Por exemplo, `http://<unique_KACE_SMA_appliance_name>.local/admin`.  
A página Acordo de transação de software será exibida.
3. Aceite o acordo.  
O assistente de Configuração inicial será exibido.
4. Verifique se você possui as informações necessárias para configurar a solução e depois clique em **Avançar**.

- Confira as informações na página Autenticação de dois fatores do Console de diagnóstico que será exibida e registre a chave secreta e os tokens off-line em um local seguro, conforme instruído.
- Na página Configurações do administrador e licenciamento, forneça as seguintes informações:

Opção	Descrição
<b>Chave de licença</b>	A chave de licença recebida no e-mail de <b>boas-vindas</b> da Quest. Se você não tem uma chave de licença, entre em contato com o <b>Suporte ao software da Quest</b> em <a href="https://support.quest.com/contact-support">https://support.quest.com/contact-support</a> .
<b>Nome da empresa</b>	O nome de sua empresa ou grupo.
<b>E-mail do administrador</b>	O endereço de e-mail em que você deseja receber as comunicações da Quest.
<b>Senha</b>	<p>A senha para a conta de <b>administrador</b> padrão, que é a conta usada para fazer o login no <b>Console do administrador</b> da solução. A conta de <b>administrador</b> padrão é a única conta na solução nesse momento. Caso você esqueça a senha para essa conta, pode ser necessário reiniciar o sistema de volta aos padrões de fábrica, o que pode resultar em perda de dados.</p> <div style="border-left: 1px solid black; padding-left: 10px; margin-left: 20px;"> <p><b>i</b> Se houver várias soluções KACE SMA ou KACE SDA (Implantação de sistemas) a Quest recomenda usar a mesma senha para a conta de <b>administrador</b> em todas as soluções. Isso permitirá vincular as soluções posteriormente. Para obter mais informações, consulte o <b>Guia do administrador</b> da solução: <a href="#">Acessar o Guia do administrador e a Ajuda on-line</a>.</p> </div>
<b>Autenticação de dois fatores</b>	Se você deseja fornecer mais segurança para os usuários que fizerem login no equipamento, defina essa opção como Ativado. Esse recurso adiciona uma etapa adicional para o processo de login. Depende do aplicativo Google Authenticator para gerar códigos de verificação. O aplicativo gera um novo código de seis dígitos em intervalos regulares. Quando ativado, o código de verificação atual será solicitado aos usuários finais sempre que eles fizerem o login.



## Opção

## Descrição



Se você ativar esse recurso, certifique-se de que o relógio do servidor KACE SMA esteja correto, bem como o dispositivo que executa o Google Authenticator. O Google Authenticator depende da hora atual para criar o token. Se o relógio do servidor não estiver sincronizado com os dos dispositivos que executam o Google Authenticator, a validação do token pode falhar, o que pode resultar em bloqueios de contas.

7. Siga as instruções na tela para concluir a configuração inicial.

Quando a configuração inicial for concluída, a solução será reiniciada e a página de login do **Console do administrador** exibida.



Se você alterar o endereço IP da solução, acesse o novo endereço para exibir a página de login.

8. Faça login no Console do administrador usando a ID de login admin e a senha escolhida durante a configuração inicial.

Se a Autenticação de dois fatores tiver sido ativada na página Configurações do administrador e licenciamento no assistente Configuração inicial, a página Configurar a autenticação de dois fatores será exibida.

9. **Apenas Autenticação de dois fatores.** Siga as instruções na página Configurar autenticação de dois fatores para gerar um código de verificação do Google Authenticator usando seu smartphone. No campo Código de verificação, digite o código do Google Authenticator, e clique em **Concluir configuração**. Um novo código de verificação é obrigatório em cada login subsequente.

Para ignorar essa etapa, clique em **Ignorar configuração**. Você só pode ignorar essa etapa durante uma janela de transição configurada. Para obter mais informações, consulte o Guia do administrador.

O **Console do administrador** será exibido e a solução estará pronta para uso.

# Definir as configurações iniciais de rede manualmente (opcional)

Se um servidor DHCP não estiver disponível e não for possível fazer login na **Console da linha de comando** da solução, você poderá definir as configurações iniciais de rede manualmente usando a **Console do administrador**.

1. Ligue a máquina virtual para inicializar a solução. Isso pode levar de 5 a 10 minutos.


A tela de login do **Console da linha de comando** será exibida.



2. Na solicitação, insira:

Login: konfig

Senha: konfig


3. Escolha o idioma a ser usado no Console da linha de comando. Use as teclas de seta para cima e seta para baixo para percorrer os campos.
4. Defina as seguintes configurações de rede. Use as teclas de seta direita e esquerda para selecionar opções em um campo; use as teclas de seta para cima e para baixo para se movimentar entre os campos.

Opção	Descrição
<b>Nome do host DNS do KACE SMA</b>	<p>Digite o nome de host da solução. O padrão é k1000, mas a Quest recomenda a alteração desse nome para um mais exclusivo durante a configuração inicial. Não alterar o nome da solução pode causar problemas quando soluções adicionais do KACE SMA forem introduzidas.</p> <p> Várias soluções do KACE SMA com nomes idênticos e pertencentes à mesma rede terão o mesmo endereço IP, o que pode causar problemas para essas soluções.</p>
<b>Gerar automaticamente nome do servidor</b>	<p>Marque essa caixa de seleção para permitir que o sistema gere o nome do servidor da Web do KACE SMA utilizando este formato: <b>Nome de host.Domínio</b>. Por exemplo: &lt;nome_único_da_solução_KACE_SMA&gt;.example.com. Desmarque essa caixa de seleção para inserir um nome do servidor da Web personalizado.</p>
<b>Nome do servidor da Web do KACE SMA</b>	<p>Digite o nome do domínio totalmente qualificado da solução. Este é o <b>Nome do host</b> concatenado ao <b>Domínio</b>. Por exemplo: &lt;nome_único_da_solução_KACE_SMA&gt;.example.com. Os dispositivos se conectam à solução usando esse nome. A Quest recomenda que você adicione uma entrada de endereço IP estático para a solução do servidor DNS. Se você usa um certificado SSL, o nome de host deve ser totalmente qualificado e corresponder ao nome no certificado.</p>

Opção	Descrição
<b>DHCP</b>	<p>(Opcional) Selecione essa opção para usar DHCP (Dynamic Host Configuration Protocol) e obter automaticamente o endereço IPv4 e outras informações de configuração da rede do equipamento. Se você selecionar essa opção, você não precisa fornecer as configurações de endereço IP estático, domínio, máscara de sub-rede, gateway padrão, DNS primário e DNS secundário.</p>
<b>Configuração IPv4 manual</b>	<p>Especifique o endereço IPv4 e forneça o endereço IP estático, o domínio, a máscara de sub-rede, o gateway padrão, o DNS primário ou as configurações de DNS secundário para o equipamento.</p> <p> O endereço IPv4 é necessário quer um endereço IPv6 esteja disponível ou não. O endereço IPv6 é opcional.</p>
<b>SLAAC</b>	<p>Marque essa opção se quiser usar o SLAAC (Stateless Address Auto-Configuration, Configuração automática de endereço sem estado), oferecido por IPv6, para definir as configurações de rede do equipamento. A SLAAC permite que os dispositivos selecionem seus próprios endereços IPv6 com base no prefixo que é anunciado a partir de sua interface conectada.</p>
<b>Configuração IPv6 manual</b>	<p>Selecione essa opção se quiser especificar manualmente o endereço IPv6. Se você selecionar essa opção, é preciso especificar o endereço IPv6, o comprimento do prefixo e o gateway padrão da solução.</p> <p> O endereço IPv6 é opcional. O endereço IPv4 é necessário quer um endereço IPv6 esteja disponível ou não.</p>
<b>Desative o IPv6</b>	<p>Selecione essa opção se quiser desativar um endereço IPv6 do equipamento. Essa é a configuração padrão.</p>
<b>Servidor SMTP</b>	<p>(Opcional) Especifique o nome de host ou o endereço IP de um servidor SMTP externo, como smtp.gmail.com. Os servidores SMTP externos devem permitir o transporte de e-</p>

## Opção

## Descrição

	<p>mail de saída anônimo (não autenticado). Certifique-se de que as políticas de rede da empresa permitam que a solução contate o servidor SMTP diretamente. Além disso, o servidor de e-mail deve estar configurado para permitir a transferência de e-mails da solução sem autenticação. Se você não fornecer as informações do servidor SMTP, o KACE SMA envia um e-mail utilizando seu servidor SMTP interno.</p>
<b>SSH habilitado</b>	<p>(Opcional) Selecione esta opção para ativar o acesso SSH (seguro) ao <b>Console do administrador</b> da solução. A Quest recomenda que você habilite o SSH durante a configuração inicial. Quando a configuração estiver completa, você pode alterar as definições no <b>Console do administrador</b> conforme necessário.</p>
<b>Proxy</b>	<p>(Opcional) Digite as informações do servidor proxy.</p> <p> A solução suporta servidores proxy que utilizam autenticação básica baseada em domínio, que requer nome de usuário e senha. Se seu servidor proxy utiliza um tipo diferente de autenticação, adicione o endereço IP da solução à lista de exceções do servidor proxy.</p>

- Use a seta para baixo para mover o cursor para Salvar e pressione **Enter** ou **Retornar**.  
O equipamento é reiniciado.
- Em qualquer computador conectado à sua LAN, abra um navegador e vá para o URL do Console do administrador da solução. Por exemplo, `http://<unique_KACE_SMA_appliance_name>.local/admin`.  
A página Acordo de transação de software será exibida.
- Aceite o acordo.  
O assistente de Configuração inicial será exibido.
- Verifique se você possui as informações necessárias para configurar a solução e depois clique em **Avançar**.
- Confira as informações na página Autenticação de dois fatores do Console de diagnóstico que será exibida e registre a chave secreta e os tokens off-line em um local seguro, conforme instruído.

10. Na página Configurações do administrador e licenciamento, forneça as seguintes informações:

Opção	Descrição
<b>Chave de licença</b>	A chave de licença recebida no e-mail de <b>boas-vindas</b> da Quest. Se você não tem uma chave de licença, entre em contato com o <b>Suporte ao software da Quest</b> em <a href="https://support.quest.com/contact-support">https://support.quest.com/contact-support</a> .
<b>Nome da empresa</b>	O nome de sua empresa ou grupo.
<b>E-mail do administrador</b>	O endereço de e-mail em que você deseja receber as comunicações da Quest.
<b>Senha</b>	<p>A senha para a conta de <b>administrador</b> padrão, que é a conta usada para fazer o login no <b>Console do administrador</b> da solução. A conta de <b>administrador</b> padrão é a única conta na solução nesse momento. Caso você esqueça a senha para essa conta, pode ser necessário reiniciar o sistema de volta aos padrões de fábrica, o que pode resultar em perda de dados.</p> <p><b>i</b> Se houver várias soluções KACE SMA ou KACE SDA (Implantação de sistemas) a Quest recomenda usar a mesma senha para a conta de <b>administrador</b> em todas as soluções. Isso permitirá vincular as soluções posteriormente. Para obter mais informações, consulte o <b>Guia do administrador</b> da solução: <a href="#">Acessar o Guia do administrador e a Ajuda on-line</a>.</p>
<b>Autenticação de dois fatores</b>	<p>Se você deseja fornecer mais segurança para os usuários que fizerem login no equipamento, defina essa opção como Ativado. Esse recurso adiciona uma etapa adicional para o processo de login. Depende do aplicativo Google Authenticator para gerar códigos de verificação. O aplicativo gera um novo código de seis dígitos em intervalos regulares. Quando ativado, o código de verificação atual será solicitado aos usuários finais sempre que eles fizerem o login.</p> <p><b>i</b> Se você ativar esse recurso, certifique-se de que o relógio do servidor KACE SMA esteja correto, bem como o dispositivo que executa o Google</p>

## Opção

## Descrição

Authenticator. O Google Authenticator depende da hora atual para criar o token. Se o relógio do servidor não estiver sincronizado com os dos dispositivos que executam o Google Authenticator, a validação do token pode falhar, o que pode resultar em bloqueios de contas.

11. Siga as instruções na tela para concluir a configuração inicial.

Quando a configuração inicial for concluída, a solução será reiniciada e a página de login do **Console do administrador** exibida.



Se você alterar o endereço IP da solução, acesse o novo endereço para exibir a página de login.

12. Faça login no Console do administrador usando a ID de login admin e a senha escolhida durante a configuração inicial.

Se a Autenticação de dois fatores tiver sido ativada na página Configurações do administrador e licenciamento no assistente Configuração inicial, a página Configurar a autenticação de dois fatores será exibida.

13. **Apenas Autenticação de dois fatores.** Siga as instruções na página Configurar autenticação de dois fatores para gerar um código de verificação do Google Authenticator usando seu smartphone. No campo Código de verificação, digite o código do Google Authenticator, e clique em **Concluir configuração**. Um novo código de verificação é obrigatório em cada login subsequente.

Para ignorar essa etapa, clique em **Ignorar configuração**. Você só pode ignorar essa etapa durante uma janeça de transição configurada. Para obter mais informações, consulte o Guia do administrador.

O **Console do administrador** será exibido e a solução estará pronta para uso.

# Acessar o Guia do administrador e a Ajuda on-line

Para obter ajuda usando o **Console do administrador**, clique no ícone de Ajuda no canto direito superior da interface para abrir a Ajuda contextual. Para acessar o sistema principal da Ajuda, clique nos links nos tópicos de Ajuda contextual.



# Programação de treinamento

Para ajudá-lo a começar a usar a solução, a Quest oferece um programa de treinamento chamado QuickStart. Este programa oferece assistência remota para ajudar a preparar rapidamente a solução para uso e começar o provisionamento, o gerenciamento, a proteção e a manutenção de seus dispositivos conectados à rede.

Para saber mais sobre o programa, acesse um dos seguintes links:

- **Solução de gerenciamento de sistemas KACE:** <https://support.quest.com/kace-systems-management-appliance/professional-services/332>
- **Solução de gerenciamento de ativos KACE:** <https://support.quest.com/kace-asset-management-appliance/professional-services/331>

Para se registrar, envie uma solicitação em:

- **Solução de gerenciamento de sistemas KACE:** <https://www.quest.com/register/113381>
- **Solução de gerenciamento de ativos KACE:** <https://www.quest.com/register/113379>

## Sobre nós

A Quest cria soluções de software que tornam reais os benefícios da nova tecnologia em um cenário de TI cada vez mais complexo. Desde o gerenciamento de banco de dados e de sistemas até o gerenciamento do Active Directory e do Office 365 e a resiliência da segurança cibernética, a Quest ajuda os clientes a resolver seu próximo desafio de TI imediatamente. Em todo o mundo, mais de 130.000 empresas e 95% das empresas da Fortune 500 confiam na Quest para oferecer gerenciamento e monitoramento proativos para a próxima iniciativa empresarial, encontrar a próxima solução para desafios complexos da Microsoft e ficar à frente da próxima ameaça. Quest Software. Onde o futuro encontra o presente. Para obter mais informações, visite [www.quest.com](http://www.quest.com).

## Recursos de suporte técnico

O suporte técnico está disponível para clientes da Quest com um contrato de manutenção válido e clientes que estão usando versões de teste. Acesse o Portal de suporte da Quest em <https://support.quest.com>.

O Portal de suporte oferece ferramentas de autoajuda que podem ser usadas para solucionar problemas de forma rápida e independente, 24 horas por dia, 365 dias por ano. O Portal de suporte permite:

- Enviar e gerenciar uma solicitação de serviço
- Consultar artigos da Base de conhecimento
- Inscrever-se para receber notificações de produtos

- Fazer download de software e documentação técnica
- Assistir a vídeos de instruções
- Participar de discussões da comunidade
- Conversar com os engenheiros de suporte on-line
- Consultar os serviços disponíveis para ajudá-lo com o seu produto.



# Configuración del dispositivo

En esta guía se explica cómo configurar el dispositivo virtual de administración de sistemas (SMA) KACE en los sistemas host VMware® ESX® o VMware ESXi™. El SMA virtual de KACE no requiere hardware dedicado.

Para obtener documentación adicional, vaya a <https://support.quest.com/kace-systems-management-appliance/technical-documents>.

## Antes de comenzar

Antes de configurar el dispositivo, hay diversas medidas preliminares que debe tomar.

1. Adquiera una licencia de SMA virtual de KACE en ventas de Quest en <https://www.quest.com/company/contact-us.aspx>.
2. Decida si desea utilizar un servidor DHCP para asignar automáticamente una dirección IP al dispositivo o para obtener una dirección IP estática para el dispositivo.
3. Si obtiene una dirección IP estática para el dispositivo, introduzca el nombre de host del dispositivo en el registro A del servidor DNS (sistema de nombres de dominio) interno. El registro A define el nombre de host para el registro MX, lo que habilita a los usuarios a enviar tickets por correo electrónico a la mesa de servicio. De manera predeterminada, el nombre de host del dispositivo es k1000, pero Quest recomienda cambiar este nombre por un valor más exclusivo durante la configuración inicial.  

i

Si no cambia el nombre del dispositivo, puede causar problemas cuando se incorporen dispositivos de SMA de KACE adicionales. Varios dispositivos de SMA de KACE con nombres idénticos que pertenezcan a la misma red tendrán la misma dirección IP, lo cual puede causarles problemas.
4. Decida si utilizará un DNS dividido. Esto resulta útil si el dispositivo se conecta a Internet mediante un proxy inverso o si coloca el dispositivo en una red perimetral o una subred filtrada. Una DMZ agrega una capa adicional de seguridad a una LAN (red de área local).

## Instale el SMA virtual de KACE en un servidor VMware ESX o VMware ESXi

Puede instalar el SMA virtual de KACE en un sistema de host que tenga instalado el cliente VMware vSphere® o el cliente web vSphere.

Antes de instalar el SMA virtual de KACE, debe instalar el cliente VMware vSphere o el cliente web vSphere en su sistema de host. Ejecute el cliente vSphere en un equipo que esté en la misma red que el host designado, la importación mediante una WAN no funciona.

1. Para descargar el SMA virtual de KACE, diríjase a <https://support.quest.com/kace-systems-management-appliance/download-new-releases>. Para obtener las credenciales de inicio de sesión como cliente, comuníquese con el Soporte de software de Quest en <https://support.quest.com/contact-support>.

2. En la sección Dispositivo virtual, descargue el archivo OVF (Open Virtualization Format) comprimido en su sistema cliente vSphere.
3. Extraiga los archivos.
4. Inicie el programa para el cliente de vSphere y haga clic en **Archivo > Implementar plantilla OVF**.
5. Vaya a la carpeta donde extrajo los archivos y seleccione el archivo OVF.  
Aparecerá el asistente de instalación y le ofrecerá opciones de instalación.
6. Seleccione los componentes que se requieren en su implementación: centro de datos, almacén de datos, etc.
7. Haga clic en **Finalizar**.
8. Confirme los ajustes del dispositivo. Busque una red válida y cualquier otro ajuste que necesite.

## Encienda el dispositivo e inicie sesión en la Consola del administrador

Quando se enciende el dispositivo por primera vez, puede iniciar sesión en la **Consola del administrador** de SMA de KACE desde cualquier computadora en su LAN, siempre que haya disponible un servidor DHCP para asignar una dirección IP al dispositivo. Esto le permite utilizar el asistente de configuración para configurar los ajustes de red iniciales.

Si no está disponible un servidor DHCP, puede configurar los ajustes de redes iniciales mediante la **Consola de la línea de comandos**. Consulte [Configure los ajustes de red iniciales de forma manual \(opcional\)](#).



Los ajustes del navegador determinan los formatos regionales que se utilizan en cuanto a la información de hora y fecha que se muestra en la **Consola del administrador** la primera vez que inicia sesión. Para obtener información acerca de cómo cambiar los ajustes de idioma, consulte la **Guía para el administrador** del dispositivo: [Acceso a la Guía para el administrador y la ayuda en línea](#).

1. Encienda la máquina virtual para arrancar el dispositivo. Este paso llevará entre 5 y 10 minutos.

Aparece la pantalla de inicio de sesión de la **Consola de la línea de comandos** y muestra los ajustes de redes DHCP del dispositivo.

2. En cualquier equipo conectado a su LAN, abra un navegador y vaya a la URL que se muestra en la pantalla de inicio de sesión de la Consola de la línea de comandos. Por ejemplo, `http://<unique_KACE_SMA_appliance_name>.local/admin`.

Aparece la página Acuerdo de transacción de software.

3. Acepte el acuerdo.

Aparece el asistente de Configuración inicial.

4. Verifique que dispone de la información requerida para configurar el dispositivo y, luego, haga clic en **Siguiente**.
5. Revise la información en la página Autenticación de dos factores de la consola de diagnóstico que aparece y registre la clave secreta y los tokens fuera de línea en una ubicación segura, tal como se indica.
6. En la página Licencias y ajustes de administrador, proporcione la siguiente información:

Opción	Descripción
<b>Clave de licencia</b>	La clave de licencia que recibió en el correo electrónico de <b>bienvenida</b> de Quest. Si no cuenta con una clave de licencia, comuníquese con <b>Soporte de software de Quest</b> en <a href="https://support.quest.com/contact-support">https://support.quest.com/contact-support</a> .
<b>Nombre de la compañía</b>	El nombre de su compañía o grupo.
<b>Correo electrónico del administrador</b>	La dirección de correo electrónico en la que desea recibir las comunicaciones de Quest.
<b>Contraseña</b>	<p>La contraseña para la cuenta de <b>administrador</b> predeterminada, que es la cuenta que utiliza para iniciar sesión en la <b>Consola del administrador</b> del dispositivo. La cuenta de administrador <b>predeterminada</b> es la única cuenta en el dispositivo en este momento. Si olvida la contraseña de esta cuenta, el sistema podría tener que reajustarse a los ajustes de fábrica que pueden resultar en pérdida de datos.</p> <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-left: 20px;"> <p><b>i</b> Si cuenta con varios dispositivos de SMA de KACE o SDA de KACE (implementación de sistemas), Quest recomienda que use la misma contraseña para la cuenta de <b>administrador</b> en todos los dispositivos. Esto le permitirá vincular los dispositivos posteriormente. Para obtener más información, consulte la <b>Guía para el administrador</b> del dispositivo: <a href="#">Acceso a la Guía para el administrador y la ayuda en línea</a>.</p> </div>
<b>Autenticación de dos factores</b>	Si desea proporcionar una mayor seguridad para los usuarios que inician sesión en el dispositivo, establezca este valor como <b>Habilitado</b> . Esta función agrega un paso adicional en el proceso de inicio de sesión. Se basa en la aplicación Google Authenticator para generar códigos de verificación. La aplicación genera un nuevo

## Opción

## Descripción

código de seis dígitos a intervalos regulares. Cuando esta opción esté habilitada, a los usuarios finales se les solicitará el código de verificación cada vez que inicien sesión.



Si habilita esta función, asegúrese de que la hora del servidor KACE SMA sea exacta, así como los dispositivos que ejecutan Google Authenticator. Google Authenticator se basa en la hora actual para crear el token. Si la hora del servidor no está sincronizada con la de los dispositivos que ejecutan Google Authenticator, la validación del token puede fallar, lo que podría ocasionar un bloqueo de la cuenta.

7. Siga las instrucciones en pantalla para completar la configuración inicial.

Cuando finaliza la configuración inicial, el dispositivo se reinicia y aparece la página de inicio de sesión de **Consola del administrador**.



Si modifica la dirección IP del dispositivo, vaya a la nueva dirección para visualizar la página de inicio de sesión.

8. Inicie sesión en Consola del administrador con la ID de inicio de sesión admin y la contraseña que eligió en la configuración inicial.

Si la autenticación de dos factores está habilitada en la página Licencias y ajustes de administrador, en el asistente de Configuración inicial, aparecerá la pantalla Configurar autenticación de dos factores.

9. **Autenticación de dos factores solamente.** Siga las instrucciones que aparecen en la página Configurar autenticación de dos factores para generar un código de verificación de Google Authenticator utilizando su teléfono inteligente. En el campo Código de verificación, escriba el código de Google Authenticator y haga clic en **Finalizar configuración**. Se necesita un nuevo código de verificación para cada inicio de sesión posterior.

Para omitir este paso, haga clic en **Omitir configuración**. Solo se puede omitir este paso durante un período de transición configurado. Para obtener más información, consulte la Guía para el administrador.

Aparece la **Consola del administrador** y el dispositivo está listo para usarse.

# Configure los ajustes de red iniciales de forma manual (opcional)

Si no está disponible un servidor DHCP y no puede iniciar sesión en el dispositivo **Consola de la línea de comandos**, puede configurar los ajustes de redes iniciales en forma manual mediante la **Consola del administrador**.

1. Encienda la máquina virtual para arrancar el dispositivo. Este paso llevará entre 5 y 10 minutos.  
Aparece la pantalla de inicio de sesión de la **Consola de la línea de comandos**.
2. En la ventana de inicio de sesión, escriba:  
Inicio de sesión: konfig  
Contraseña: konfig
3. Seleccione el idioma que se usará en la Consola de la línea de comandos. Use las teclas de flecha arriba y abajo para moverse entre los campos.
4. Configure los siguientes ajustes de redes. Use las teclas de flecha derecha e izquierda para seleccionar las opciones en un campo; use las teclas de flecha arriba y abajo para moverse entre los campos.

Opción	Descripción
<b>Nombre de host DNS de SMA de KACE</b>	<p>Escriba el nombre de host del dispositivo. El nombre predeterminado es k1000, pero Quest recomienda cambiar este nombre por un valor más exclusivo durante la configuración inicial. Si no cambia el nombre del dispositivo, puede causar problemas cuando se incorporen dispositivos de SMA de KACE adicionales.</p> <p><b>i</b> Varios dispositivos de SMA de KACE con nombres idénticos que pertenezcan a la misma red tendrán la misma dirección IP, lo cual puede causarles problemas.</p>
<b>Generar automáticamente el nombre del servidor</b>	<p>Seleccione esta casilla para permitir que el sistema genere el nombre de servidor web de SMA de KACE con este formato: <b>Nombre de host.Dominio</b>. Por ejemplo: &lt;unique_KACE_SMA_appliance_name&gt;.example.com. Desactive esta casilla para introducir un nombre de servidor web personalizado.</p>
<b>Nombre del servidor web de SMA de KACE</b>	<p>Escriba el nombre completo del dominio del dispositivo. Este es el <b>Nombre de host</b> junto con el <b>Dominio</b>. Por ejemplo: &lt;unique_KACE_SMA_appliance_name&gt;.example.com. Los clientes se conectan al dispositivo mediante este nombre. Quest recomienda agregar al servidor DNS una entrada de dirección IP</p>

Opción	Descripción
	estática para el dispositivo. Si usa un certificado SSL, el nombre de host debe estar completo y debe coincidir con el nombre que aparece en el certificado.
<b>DHCP</b>	(Opcional) Seleccione esta opción para utilizar el DHCP (protocolo de configuración dinámica de host) y obtener automáticamente la dirección IPv4 y otra información de configuración de red del dispositivo. Si selecciona esta opción, no es necesario que proporcione la dirección IP estática, el dominio, la máscara de subred, la puerta de enlace predeterminada, los ajustes de DNS primario o de DNS secundario.
<b>Configuración manual de IPv4</b>	<p>Especifique la dirección IPv4 y proporcione la dirección IP estática, el dominio, la máscara de subred, la puerta de enlace predeterminada, el DNS primario o los ajustes de DNS secundario del dispositivo.</p> <div data-bbox="568 767 583 810" style="border-left: 1px solid black; padding-left: 5px;">  La dirección IPv4 es obligatoria, sin importar si hay una dirección IPv6 disponible. La dirección IPv6 es opcional. </div>
<b>SLAAC</b>	<p>Seleccione esta opción si desea utilizar SLAAC (configuración automática sin estado de direcciones), que ofrece IPv6, para configurar los ajustes de redes del dispositivo. SLAAC permite a los dispositivos seleccionar sus propias direcciones IPv6 en función del prefijo que se anuncia desde su interfaz conectada.</p>
<b>Configuración manual de IPv6</b>	<p>Seleccione esta opción si desea especificar manualmente la dirección IPv6. Si selecciona esta opción, debe especificar la dirección IPv6, la longitud del prefijo y la puerta de enlace predeterminada del dispositivo.</p> <div data-bbox="568 1246 583 1289" style="border-left: 1px solid black; padding-left: 5px;">  La dirección IPv6 es opcional. La dirección IPv4 es obligatoria, sin importar si hay una dirección IPv6 disponible. </div>
<b>Deshabilitar IPv6</b>	<p>Seleccione esta opción si desea deshabilitar una dirección IPv6 para el dispositivo. Esta es la configuración predeterminada.</p>

Opción	Descripción
<b>Servidor SMTP</b>	(Opcional) Especifique el nombre de host o la dirección IP de un servidor SMTP externo, como smtp.gmail.com. Los servidores SMTP externos deben permitir el transporte de correos electrónicos de salida anónimos (no autenticados). Asegúrese de que las políticas de red permitan que el dispositivo se comuniquen con el servidor SMTP directamente. Además, el servidor de correo debe estar configurado para confiar en el correo electrónico proveniente del dispositivo sin autenticación. Si no proporciona la información del servidor SMTP, el SMA de KACE envía correos electrónicos usando su servidor SMTP interno.
<b>SSH habilitado</b>	(Opcional) Seleccione esta opción para habilitar el acceso SSH (seguro) a la <b>Consola del administrador</b> del dispositivo. Quest recomienda que habilite SSH durante la configuración inicial. Cuando la instalación haya finalizado, puede cambiar la configuración en la <b>Consola del administrador</b> según sea necesario.
<b>Proxy</b>	De manera opcional, puede escribir información sobre el servidor proxy. <div style="border-left: 1px solid black; padding-left: 10px; margin-left: 20px;"> <p><b>i</b> El dispositivo es compatible con servidores proxy que usan autenticación básica, basada en dominios y que requiere de nombres de usuarios y contraseñas. Si el servidor proxy usa un tipo diferente de autenticación, agregue la dirección IP del dispositivo a la lista de excepciones del servidor proxy.</p> </div>
<ol style="list-style-type: none"> <li>5. Use la tecla de flecha abajo para mover el cursor hasta Guardar y luego presione <b>Ingresar</b> o <b>Regresar</b>. Se reinicia el dispositivo.</li> <li>6. En cualquier equipo conectado a su LAN, abra un navegador y vaya a la URL de la Consola del administrador del dispositivo. Por ejemplo, <code>http://&lt;unique_KACE_SMA_appliance_name&gt;.local/admin</code>. Aparece la página Acuerdo de transacción de software.</li> <li>7. Acepte el acuerdo.</li> </ol>	

Aparece el asistente de Configuración inicial.

8. Verifique que dispone de la información requerida para configurar el dispositivo y, luego, haga clic en **Siguiente**.
9. Revise la información en la página Autenticación de dos factores de la consola de diagnóstico que aparece y registre la clave secreta y los tokens fuera de línea en una ubicación segura, tal como se indica.
10. En la página Licencias y ajustes de administrador, proporcione la siguiente información:

Opción	Descripción
<b>Clave de licencia</b>	La clave de licencia que recibió en el correo electrónico de <b>bienvenida</b> de Quest. Si no cuenta con una clave de licencia, comuníquese con <b>Soporte de software de Quest</b> en <a href="https://support.quest.com/contact-support">https://support.quest.com/contact-support</a> .
<b>Nombre de la compañía</b>	El nombre de su compañía o grupo.
<b>Correo electrónico del administrador</b>	La dirección de correo electrónico en la que desea recibir las comunicaciones de Quest.
<b>Contraseña</b>	<p>La contraseña para la cuenta de <b>administrador</b> predeterminada, que es la cuenta que utiliza para iniciar sesión en la <b>Consola del administrador</b> del dispositivo. La cuenta de administrador <b>predeterminada</b> es la única cuenta en el dispositivo en este momento. Si olvida la contraseña de esta cuenta, el sistema podría tener que reajustarse a los ajustes de fábrica que pueden resultar en pérdida de datos.</p> <p><b>i</b> Si cuenta con varios dispositivos de SMA de KACE o SDA de KACE (implementación de sistemas), Quest recomienda que use la misma contraseña para la cuenta de <b>administrador</b> en todos los dispositivos. Esto le permitirá vincular los dispositivos posteriormente. Para obtener más información, consulte la <b>Guía para el administrador</b> del dispositivo: <a href="#">Acceso a la Guía para el administrador y la ayuda en línea</a>.</p>
<b>Autenticación de dos factores</b>	Si desea proporcionar una mayor seguridad para los usuarios que inician sesión en el dispositivo, establezca este valor como <b>Habilitado</b> . Esta función agrega un paso adicional en el proceso de inicio de sesión. Se basa en la aplicación



## Opción

## Descripción

Google Authenticator para generar códigos de verificación. La aplicación genera un nuevo código de seis dígitos a intervalos regulares. Cuando esta opción esté habilitada, a los usuarios finales se les solicitará el código de verificación cada vez que inicien sesión.



Si habilita esta función, asegúrese de que la hora del servidor KACE SMA sea exacta, así como los dispositivos que ejecutan Google Authenticator. Google Authenticator se basa en la hora actual para crear el token. Si la hora del servidor no está sincronizada con la de los dispositivos que ejecutan Google Authenticator, la validación del token puede fallar, lo que podría ocasionar un bloqueo de la cuenta.

11. Siga las instrucciones en pantalla para completar la configuración inicial.

Cuando finaliza la configuración inicial, el dispositivo se reinicia y aparece la página de inicio de sesión de **Consola del administrador**.



Si modifica la dirección IP del dispositivo, vaya a la nueva dirección para visualizar la página de inicio de sesión.

12. Inicie sesión en Consola del administrador con la ID de inicio de sesión admin y la contraseña que eligió en la configuración inicial.

Si la autenticación de dos factores está habilitada en la página Licencias y ajustes de administrador, en el asistente de Configuración inicial, aparecerá la pantalla Configurar autenticación de dos factores.

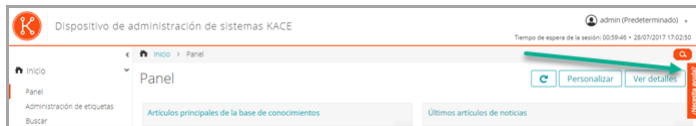
13. **Autenticación de dos factores solamente.** Siga las instrucciones que aparecen en la página Configurar autenticación de dos factores para generar un código de verificación de Google Authenticator utilizando su teléfono inteligente. En el campo Código de verificación, escriba el código de Google Authenticator y haga clic en **Finalizar configuración**. Se necesita un nuevo código de verificación para cada inicio de sesión posterior.

Para omitir este paso, haga clic en **Omitir configuración**. Solo se puede omitir este paso durante un período de transición configurado. Para obtener más información, consulte la Guía para el administrador.

Aparece la **Consola del administrador** y el dispositivo está listo para usarse.

# Acceso a la Guía para el administrador y la ayuda en línea

Para obtener ayuda a través de la **Consola del administrador**, haga clic en el vínculo de Ayuda en la esquina superior derecha de la interfaz para abrir la ayuda contextual. Para acceder al sistema de ayuda principal, haga clic en los vínculos incluidos en los temas de ayuda contextual.



## Programación de la capacitación

Para ayudarlo a comenzar a usar el dispositivo, Quest proporciona un programa de capacitación denominado QuickStart. En este programa se proporciona asistencia remota para ayudarlo a poner en marcha su solución rápidamente y comenzar el aprovisionamiento, la gestión, la protección y el mantenimiento de sus dispositivos conectados a la red.

Para obtener más información acerca de este programa, visite uno de los siguientes vínculos:

- **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>

Para registrarse, envíe una solicitud a:

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

## Acerca de nosotros

Quest crea soluciones de software que hacen reales los beneficios de las nuevas tecnologías en un panorama de TI cada vez más complejo. Desde administración de bases de datos y de sistemas hasta administración de Active Directory y Office 365 y resistencia a la seguridad cibernética, Quest ayuda a los clientes a resolver su próximo desafío de TI ahora. En todo el mundo, más de 130 000 empresas y el 95 % de la lista Fortune 500 confían en Quest para disfrutar de administración y monitoreo proactivos en la próxima iniciativa empresarial, encontrar la siguiente solución para los desafíos complejos de Microsoft y mantenerse a la vanguardia ante la próxima amenaza. Quest Software. Donde convergen el futuro y el presente. Para obtener más información, visite [www.quest.com](http://www.quest.com).

## Recursos del soporte técnico

El soporte técnico se encuentra disponible para los clientes de Quest con un contrato válido de mantenimiento y para los clientes que poseen versiones de prueba. Puede acceder al portal del Soporte de Quest en <https://support.quest.com>.

El portal de soporte proporciona herramientas de autoayuda que puede utilizar para resolver problemas de forma rápida e independiente, las 24 horas al día, los 365 días del año. El portal de soporte le permite:

- Enviar y gestionar una solicitud de servicio
- Consultar los artículos de la base de conocimientos
- Suscribirse a las notificaciones de productos
- Descargar documentación del software y técnica
- Ver videos de procedimientos
- Participar en debates de la comunidad
- Chatear en línea con ingenieros de soporte
- Ver servicios para ayudarlo con su producto

# Legal notices

---

## © 2022 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.

## Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <https://www.quest.com/legal>.

## Trademarks

Quest, the Quest logo, Join the Innovation, and KACE are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/>

trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

## Legend



**A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**



An information icon indicates supporting information.

KACE Systems Management Appliance Setup Guide for VMware Platforms

Updated - October 2022

Software Version - 13.0