

Quest®



# KACE® Systems Management Appliance 11.0

## Setup Guide for Hyper-V Platforms



# Table of Contents

Setting up the appliance.....	4
Before you begin.....	4
Import the virtual KACE SMA in to a Microsoft Hyper-V server and configure settings.....	4
Power-on the appliance and log in to the Administrator Console.....	6
Configure initial network settings manually (optional).....	8
Configuring backup integration services.....	12
Virtual NIC configuration.....	13
Accessing the Administrator Guide and online Help.....	14
Scheduling training.....	14
About us.....	15
Technical support resources.....	15
Configuration de l'appliance.....	17
Avant de commencer.....	17
Importation de l'appliance virtuelle KACE SMA dans un serveur Microsoft Hyper-V et configuration des paramètres.....	17
Mettre l'appliance sous tension et se connecter à la Console d'administration.....	19
Configurer les paramètres réseau initiaux manuellement (facultatif).....	22
Configuration des services d'intégration de sauvegarde.....	27
Configuration de la carte réseau virtuelle.....	28
Accès au Guide de l'administrateur et à l'aide en ligne.....	29
Programmation des formations.....	29
Einrichten der Appliance.....	30
Vorbereitung.....	30
Importieren der virtuellen KACE SMA in einen Microsoft Hyper-V-Server und Konfigurieren der Einstellungen.....	30
Einschalten der Appliance und Anmelden bei der Administratorkonsole.....	32
Anfängliche Netzwerkeinstellungen manuell konfigurieren (optional).....	35
Konfiguration von Backup-Integrationsdiensten.....	40
Virtuelle NIC-Konfiguration.....	41
Zugriff auf das Administratorhandbuch und die Onlinehilfe.....	42
Zeitplanung für Schulungen.....	42
アプライアンスのセットアップ.....	44
はじめに.....	44
Microsoft Hyper-Vサーバへの仮想KACE SMAのインポートと設定の構成.....	44
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.....	46
手動による初期ネットワーク設定の構成 ( オプション ) .....	48
バックアップ統合サービスの設定.....	53
仮想 NIC の構成.....	54
管理者ガイドおよびオンラインヘルプへのアクセス.....	55
トレーニングのスケジュール設定.....	55
Configuração do equipamento.....	57
Antes de começar.....	57
Importar o KACE SMA virtual para um servidor Microsoft Hyper-V e definir as configurações.....	57
Ligue a solução e faça login no Console do administrador.....	59
Definir as configurações iniciais de rede manualmente (opcional).....	61
Como configurar os serviços de integração de backup.....	66

Configuração de NIC virtual.....	67
Acessar o Guia do administrador e a Ajuda on-line.....	68
Programação de treinamento.....	69
Configuración del dispositivo.....	70
Antes de comenzar.....	70
Importe el SMA virtual de KACE a un servidor de Microsoft Hyper-V y configure los ajustes.....	70
Encienda el dispositivo e inicie sesión en la Consola del administrador.....	72
Configure los ajustes de red iniciales de forma manual (opcional).....	74
Configuración de los servicios de integración de las copias de seguridad.....	79
Configuración de NIC virtual.....	81
Acceso a la Guía para el administrador y la ayuda en línea.....	82
Programación de la capacitación.....	82
Legal notices.....	83

# Setting up the appliance

This guide explains how to set up the virtual KACE Systems Management Appliance (SMA) on Microsoft® Hyper-V® 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 DMZ (demilitarized zone) or screened subnet. A DMZ adds an additional layer of security to a LAN (local area network).
5. Configure the backup integration services for the virtual appliances running on Hyper-V. For more information, see [Configuring backup integration services](#).



Failing to configure backup integration services properly may cause MySQL database file corruption.

## Import the virtual KACE SMA in to a Microsoft Hyper-V server and configure settings

Hyper-V Manager is the built-in virtual machine management tool that you use to import the virtual KACE KACE SMA.

- Do not configure the virtual machine with the Legacy Network Adapter.

- In Hyper-V Manager, keep the default setting to enable Hyper-V Time Synchronization Service.
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 VHD bundle to your Hyper-V host system.
  3. Extract and verify the integrity of the files.
  4. In Hyper-V Manager, right-click the host and click Import Virtual Machine.  
The Import Virtual Machine window appears.
  5. Browse to the location of the extracted VHD bundle.
  6. In Settings, select Copy the virtual machine (create a new unique ID) and Duplicate all files so the same virtual machine can be imported again.
  7. Click Import.

The virtual KACE SMA appears in the Virtual Machines list.

8. Edit the virtual machine's settings to connect the virtual network adapter to your Hyper-V host's virtual switch.
9. Choose a static MAC address for the virtual machine:



Quest recommends using a static MAC address because Hyper-V might randomly assign a new MAC address to the virtual machine if a dynamic MAC address is used. Since the KACE SMA runs on FreeBSD®, the guest operating system must be restarted to detect the change to the network interface, and this can cause erratic network behavior.

- a. Go to the Advanced Features section of the virtual machine's Network Adapter settings.
  - b. Select Static under MAC address.
  - c. Specify a valid unique MAC address for your environment. Typically, you can use the current MAC address.
  - d. Click Apply.
10. Disable virtual machine queue (VMQ) for the virtual machine:



VMQ is a packet filtering technology in Hyper-V designed to reduce overhead of packet routing with supported hardware and guest operating systems. However, it is not supported by the Intel® e1000 virtual NIC (network interface controller) used by the KACE SMA, and this can cause poor network performance. Some physical adapters are known to have performance issues with VMQ as well. Therefore, Quest recommends disabling VMQ.

- a. Go to the Hardware Acceleration section of the virtual machine's Network Adapter settings.
- b. Clear the check box next to Enable virtual machine queue.
- c. Click Apply.

Power-on the appliance.

# 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 Welcome email from Quest. If you do not have a license key, contact Quest Software Support 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.

Option	Description
Password	<p>The password for the default admin account, which is the account you use to log in to the appliance Administrator Console. The default admin account is the only account on the appliance at this time. If you forget the password for this account, the system might have to be reset to factory defaults which can result in loss of data.</p> <p> 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: <a href="#">Accessing the Administrator Guide and online Help</a>.</p>

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> <p> 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.</p>
---------------------------	--

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

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

 If you changed the appliance IP address, go to the new address to display the login page.

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

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

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

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

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



When you log in to the virtual KACE SMA, make sure that Automatically synchronize with an internet time server is disabled on the Date and Time Settings that are accessed through Settings > Control Panel.



## Configure initial network settings manually (optional)



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

1. Power on the virtual machine to boot the appliance. This takes 5 to 10 minutes.  
The Command Line Console login screen appears.
2. At the prompts, enter:  
Login: konfig  
Password: konfig
3. Choose the language to use for the Command Line Console. Use the up- and down-arrow keys to move between fields.
4. Configure the following network settings. Use the right- and left-arrow keys to select options in a field; use the up- and down-arrow keys to move between fields.

Option	Description
KACE SMA DNS Hostname	Enter the hostname of the appliance. The default is k1000, but Quest recommends to change this name to a more unique value during initial setup. Leaving the appliance name unchanged can cause problems when additional KACE SMA appliances are introduced.



Option	Description
	<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>
Automatically generate server name	<p>Select this check box to enable the system to generate the KACE SMA web server name using this format: Hostname.Domain. For example: &lt;unique_KACE_SMA_appliance_name&gt;.example.com. Clear this check box to enter a custom web server name.</p>
KACE SMA Web Server Name	<p>Enter the fully qualified domain name of the appliance. This is the Hostname concatenated with Domain. 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>
DHCP	<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>
Manual IPv4 Configuration	<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>
SLAAC	<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>

Option	Description
Manual IPv6 Configuration	<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> <p> The IPv6 address is optional. The IPv4 address is required whether or not an IPv6 address is available.</p>
Disable IPv6	<p>Select this option if you want to disable an IPv6 address for the appliance. This is the default setting.</p>
SMTP Server	<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>
SSH Enabled	<p>(Optional) Select this option to enable SSH (secure) access to the appliance Administrator Console. Quest recommends that you enable SSH during the initial setup. When the setup is complete, you can change the setting in the Administrator Console as needed.</p>
Proxy	<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
License Key	The license key you received in the Welcome email from Quest. If you do not have a license key, contact Quest Software Support at <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 admin account, which is the account you use to log in to the appliance Administrator Console. The default admin account is the only account on the appliance at this time. If you forget the password for this account, the system might have to be reset to factory defaults which can result in loss of data.</p> <p> 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: <a href="#">Accessing the Administrator Guide and online Help</a>.</p>
Two-Factor Authentication	If you want to provide stronger security for users logging into the appliance, set this to Enabled. This feature adds an extra step to the login process. It relies on the Google Authenticator app to generate verification codes. The app generates a new six-digit code at regular intervals. When enabled, end users will be

Option	Description
	<p data-bbox="548 239 1029 295">prompted for the current verification code each time they log in.</p> <div data-bbox="560 303 1029 569" style="border-left: 1px solid black; padding-left: 10px;"> <p data-bbox="560 311 1029 569"><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 validation may fail, which may result in the account lockouts.</p> </div>

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.

**i** If you changed 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.

## Configuring backup integration services

Configuring backup integration services appropriately for KACE Systems Management Appliance (SMA) virtual machines running on Hyper-V prevents MySQL database file corruption.

KACE SMA virtual machine running on Hyper-V is incorrectly configured for virtual machine (VM) backup, resulting in some MySQL database file corruption inside the appliance, rendering the appliance unusable until Technical Support is contacted to resolve the issue, by restoring the database from the most current, non-corrupted database backup.

This is caused by the Hyper-V live virtual machine backup feature, that facilitates zero down time backup of live virtual machines. For more information, visit [https://technet.microsoft.com/en-us/library/dn531031\(v=ws.12\).aspx](https://technet.microsoft.com/en-us/library/dn531031(v=ws.12).aspx).

However, Microsoft does not yet support the Hyper-V live backup feature for any version of FreeBSD virtual machines running on Hyper-V, which includes Hyper-V VMs of the KACE SMA products, since they are based on FreeBSD. For more information, visit [https://technet.microsoft.com/library/dn848318\(ws.12\).aspx](https://technet.microsoft.com/library/dn848318(ws.12).aspx).

If correctly configured, when a backup is taken of a VM that does not support live backup, the Hyper-V server takes the VM offline (placed into the saved state) for the duration of the backup process, and then restores the VM to its previous state after the backup process is done. While the VM has to be taken offline, resulting in downtime for the VM, the backup should be able to complete without adversely affecting the VM's contents. For more information, visit <https://technet.microsoft.com/en-us/library/dn798286.aspx>.

Since Microsoft does not support live backups of the FreeBSD operating system that the KACE appliances run on, it is important to configure the appropriate Integration Services settings of the KACE SMA Hyper-V VMs that prevent Hyper-V from attempting to perform live backups of the VM. When the VM's Integration Services settings are not properly configured, some customers have experienced file corruption inside of the KACE SMA which causes it to not function correctly, resulting in needing to contact Technical Support to correct the problem.

Since Microsoft automatically defaults all new Hyper-V VMs to have the Backup Integration Service enabled, if you created a Hyper-V VM for the KACE SMA, follow the instructions below to correctly configure this service for FreeBSD, to prevent the above database file corruption.

Disabling the live backup feature on KACE SMA Hyper-V VMs is recommended.

To disable the Backup Integration Service, in the VM Settings dialog box, under Management > Integration Services, clear the Backup (volume checkpoint) check box, and click Apply. This setting may have a different name, such as Backup (volume shadow copy), depending on the Windows version of the Hyper-V server.



To change this setting, you must first shut down the VM.



After the Backup setting is disabled, if Windows fails to first take the VM offline (by changing the state of the VM to saved) during the backup process, and MySQL corruption in the KACE appliance continues to occur during VM backup, put the VM into shutdown or saved state before performing a VM backup.

For additional information about this issue, visit <https://support.quest.com/kace-systems-management-appliance/kb/195580>.

## Virtual NIC configuration

Erratic network behavior, including poor performance, agent disconnects, interface freezing, and complete network unavailability is observed with a virtual KACE Systems Deployment Appliance (SDA) running on Hyper-V.

By default, two problematic network settings are enabled in Hyper-V for all guest virtual machines (VMs). These settings are a Dynamic MAC address and VMQ (virtual machine queue).

When configured with a Dynamic MAC address, Hyper-V may randomly assign a new MAC address to the guest VM. Since the KACE appliances run on FreeBSD, the OS must be restarted to detect the change to the network interface.

VMQ is a packet filtering technology in Hyper-V that reduces the overhead of packet routing with supported hardware and guest operating systems. However, it is not supported by the Intel E1000 virtual NIC used by the KACE appliances, and this can cause poor network performance. Some Broadcom physical adapters are known to have performance issues with VMQ as well.

To resolve this issue, it is recommended to disable both the dynamic MAC address (by choosing a static MAC) and VMQ, on all Hyper-V hosted virtual KACE appliances.

To disable the dynamic MAC address, in the VM Settings dialog box, under Network Adapter > Advanced Features, select the Static check box, and specify a valid, unique MAC address for your environment. Then, click Apply.

**i** Typically, this can be left as the current MAC address, that is already assigned dynamically.

**i** To switch a dynamic MAC address to a static one, and the other way around, you must first shut down the VM.

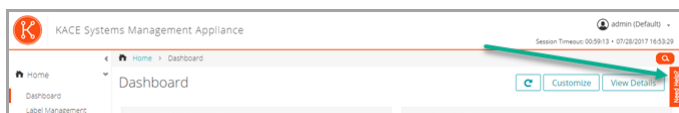
To disable VMQ, in the VM Settings dialog box, under Network Adapter > Hardware Acceleration, clear the Enable virtual machine queue check box, and click Apply.

**i** While this setting can be changed without shutting down the VM, it is recommended to change it while the VM is offline.

For additional information about this issue, visit <https://support.quest.com/kace-systems-management-appliance/kb/153445>.

## 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 Microsoft® HyperV®. 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. Déterminez 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. Déterminez 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 une zone DMZ (zone démilitarisée) ou un sous-réseau filtré. La zone DMZ permet d'ajouter un niveau de sécurité supplémentaire à un réseau LAN (Local Area Network).
5. Configurez les services d'intégration de sauvegarde pour les appliances virtuelles s'exécutant sur Hyper-V. Pour plus d'informations, voir [Configuration des services d'intégration de sauvegarde](#).



Ne pas configurer les services d'intégration de sauvegarde peut corrompre les fichiers de base de données MySQL.

## Importation de l'appliance virtuelle KACE SMA dans un serveur Microsoft Hyper-V et configuration des paramètres

Le gestionnaire Hyper-V est l'outil de gestion de machine virtuelle intégré qui permet d'importer l'appliance virtuelle KACE KACE SMA.

- Ne configurez pas la machine virtuelle avec la carte réseau virtuelle héritée.
  - Dans le gestionnaire Hyper-V Manager, conservez le paramètre par défaut afin d'activer l'option Service Synchronisation date/heure Microsoft Hyper-V.
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 groupement VHD compressé sur votre système hôte Hyper-V.
  3. Extrayez les fichiers et vérifiez leur intégrité.
  4. Dans le gestionnaire Hyper-V, cliquez avec le bouton droit sur l'hôte, puis cliquez sur Importer l'ordinateur virtuel.

La fenêtre Importer l'ordinateur virtuel s'affiche.

5. Accédez à l'emplacement du groupement VHD extrait.
6. Dans les Paramètres, sélectionnez Copier l'ordinateur virtuel (créer un ID unique) et Dupliquer tous les fichiers de manière à ce que le même ordinateur virtuel puisse être réimporté.
7. Cliquez sur Importer.

L'appliance virtuelle KACE SMA s'affiche dans la liste Machines virtuelles.

8. Modifiez les paramètres de la machine virtuelle pour connecter la carte réseau virtuelle à votre commutateur virtuel hôte Hyper-V.
9. Sélectionnez une adresse MAC statique pour la machine virtuelle :



Quest recommande l'utilisation d'une adresse MAC statique. En effet, si vous utilisez une adresse MAC dynamique, Hyper-V risque d'attribuer aléatoirement une nouvelle adresse MAC à la machine virtuelle. Étant donné que l'appliance KACE SMA est exécutée sous FreeBSD®, vous devez redémarrer le système d'exploitation invité afin de détecter les modifications apportées à l'interface réseau, ce qui peut entraîner une défaillance du réseau.

- a. Rendez-vous dans la section Fonctionnalités avancées des paramètres Carte réseau de la machine virtuelle.
  - b. Sélectionnez Statique sous Adresse MAC.
  - c. Indiquez une adresse MAC unique valide pour votre environnement. Vous pouvez généralement utiliser votre adresse MAC actuelle.
  - d. Cliquez sur Appliquer.
10. Désactivez VMQ (Virtual Machine Queue) pour la machine virtuelle :



VMQ est une technologie de filtrage de paquets dans Hyper-V conçue pour réduire la surcharge de travail liée au routage des paquets sur le matériel et les systèmes

d'exploitation invités pris en charge. Cependant, cette technologie n'est pas prise en charge par la carte réseau virtuelle Intel® e1000 utilisée par l'appliance KACE SMA, ce qui peut nuire aux performances du réseau. VMQ entraîne également des problèmes de performances pour certaines cartes réseau physiques. Quest vous recommande donc de désactiver VMQ.

- a. Rendez-vous dans la section Accélération du matériel des paramètres Carte réseau de la machine virtuelle.
- b. Décochez la case Activer la file d'attente de la machine virtuelle.
- c. Cliquez sur Appliquer.

Mettez l'appliance sous tension.

## 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'appliance, 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
Clé de licence	Saisissez la clé de licence que vous avez reçue dans le courrier électronique de bienvenue envoyé par Quest. Si vous ne disposez d'aucune clé de licence, contactez le Support Quest Software à l'adresse <a href="https://support.quest.com/contact-support">https://support.quest.com/contact-support</a> .
Nom de l'entreprise	Nom de votre entreprise ou organisation.
E-mail de l'administrateur	Adresse e-mail à laquelle vous souhaitez recevoir les communications de Quest.
Mot de passe	<p>Mot de passe du compte admin par défaut, qui est le compte que vous utilisez pour vous connecter à la Console d'administration de l'apppliance. Le compte admin 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.</p> <div style="border-left: 1px solid #0070C0; padding-left: 10px; margin-top: 10px;"> <p><b>i</b> 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 de l'apppliance : <a href="#">Accès au Guide de l'administrateur et à l'aide en ligne</a>.</p> </div>
Authentification bifactorielle	Si vous voulez fournir une sécurité accrue aux utilisateurs se connectant à l'apppliance, 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

## Option

## Description

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'apppliance redémarre, puis la page de connexion à la Console d'administration s'affiche.



Si vous avez modifié l'adresse IP de l'apppliance, 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'apppliance.




Lorsque vous vous connectez à l'apppliance KACE SMA, vérifiez que l'option Synchroniser automatiquement avec un serveur de temps Internet est désactivée dans les Paramètres de date et d'heure accessibles via Paramètres > Panneau de configuration.



# 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
Nom d'hôte DNS du KACE SMA	<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><b>i</b> 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>
Générer automatiquement le nom du serveur	<p>Cochez cette case pour permettre au système de générer le nom du serveur Web KACE SMA au format suivant : Nom d'hôte.Domaine. Exemple : &lt;unique_KACE_SMA_appliance_name&gt;.example.com. Décochez cette case pour saisir un nom de serveur Web personnalisé.</p>

Option	Description
Nom du serveur Web du KACE SMA	<p>Saisissez le nom de domaine complet de l'appliance. Il s'agit du Nom d'hôte concaténé avec le Domaine. 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>
DHCP	<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>
Configuration IPv4 manuelle	<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="560 932 1023 1011" style="border-left: 1px solid black; padding-left: 10px;"> <p> L'adresse IPv4 est requise, qu'une adresse IPv6 soit disponible ou non. L'adresse IPv6 est facultative.</p> </div>
SLAAC	<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>
Configuration IPv6 manuelle	<p>Sélectionnez cette option si vous souhaitez spécifier manuellement l'adresse IPv6. Si vous sélectionnez cette option, vous devez spécifier l'adresse IPv6, la longueur du préfixe et la passerelle par défaut pour l'appliance.</p>

Option	Description
Désactiver IPv6	 L'adresse IPv6 est facultative. L'adresse IPv4 est requise, qu'une adresse IPv6 soit disponible ou non.  Sélectionnez cette option si vous souhaitez désactiver une adresse IPv6 pour l'appliance. Il s'agit du paramètre par défaut.
Serveur SMTP	(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'appliance de communiquer directement avec le serveur SMTP. En outre, le serveur de messagerie doit être configuré pour permettre le relai du courrier électronique de l'appliance sans authentification. Si vous ne fournissez pas les informations du serveur SMTP, l'appliance KACE SMA envoie les e-mails par le biais de son serveur SMTP interne.
SSH activé	(Facultatif) Sélectionnez cette option pour activer l'accès SSH (sécurisé) à la Console d'administration de l'appliance. 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 Console d'administration si nécessaire.
Proxy	(Facultatif) Saisissez les informations concernant le serveur proxy.   L'appliance 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'appliance à la liste des exceptions du serveur proxy.

- 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'apppliance. 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'apppliance, 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
Clé de licence	Saisissez la clé de licence que vous avez reçue dans le courrier électronique de bienvenue envoyé par Quest. Si vous ne disposez d'aucune clé de licence, contactez le Support Quest Software à l'adresse <a href="https://support.quest.com/contact-support">https://support.quest.com/contact-support</a> .
Nom de l'entreprise	Nom de votre entreprise ou organisation.
E-mail de l'administrateur	Adresse e-mail à laquelle vous souhaitez recevoir les communications de Quest.
Mot de passe	Mot de passe du compte admin par défaut, qui est le compte que vous utilisez pour vous connecter à la Console d'administration de l'apppliance. Le compte admin 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
Authentification bifactorielle	<p data-bbox="636 240 969 293">de l'apppliance : <a href="#">Accès au Guide de l'administrateur</a> et à <a href="#">l'aide en ligne</a>.</p> <p data-bbox="551 316 1025 600">Si vous voulez fournir une sécurité accrue aux utilisateurs se connectant à l'apppliance, 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.</p> <p data-bbox="568 619 1025 927">  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. </p>
11. Suivez les instructions affichées à l'écran pour finaliser la configuration initiale.	<p data-bbox="143 986 1025 1034">Une fois la configuration initiale terminée, l'apppliance redémarre, puis la page de connexion à la Console d'administration s'affiche.</p>
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.	<p data-bbox="154 1054 994 1102">  Si vous avez modifié l'adresse IP de l'apppliance, utilisez la nouvelle adresse pour afficher la page de connexion. </p> <p data-bbox="143 1193 1025 1262">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.</p>
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.

## Configuration des services d'intégration de sauvegarde

La configuration appropriée des services d'intégration de sauvegarde pour les machines virtuelles de l'appliance de gestion des systèmes KACE s'exécutant sur Hyper-V empêche la corruption des fichiers de la base de données MySQL.

La machine virtuelle KACE SMA s'exécutant sur Hyper-V n'est pas correctement configurée pour la sauvegarde de machine virtuelle (VM). Cela cause des problèmes de corruption des fichiers de la base de données MySQL dans l'appliance, rendant l'appliance inutilisable jusqu'à ce que le support technique soit contacté pour résoudre le problème en restaurant la base de données à partir de la sauvegarde de base de données non corrompue la plus récente.

Ce phénomène est provoqué par la fonctionnalité sauvegarde en direct de la machine virtuelle d'Hyper-V qui facilite la sauvegarde sans interruption des machines virtuelles en direct. Pour plus d'informations, visitez le site [https://technet.microsoft.com/en-us/library/dn531031\(v=ws.12\).aspx](https://technet.microsoft.com/en-us/library/dn531031(v=ws.12).aspx).

Cependant, Microsoft ne prend actuellement pas en charge la fonctionnalité sauvegarde en direct pour les versions de machines virtuelles FreeBSD s'exécutant sur HyperV, dont les machines virtuelles HyperV des produits KACE SMA qui utilisent FreeBSD. Pour plus d'informations, visitez le site [https://technet.microsoft.com/library/dn848318\(ws.12\).aspx](https://technet.microsoft.com/library/dn848318(ws.12).aspx).

S'il est correctement configuré, lors de la sauvegarde d'une machine virtuelle ne prenant pas en charge la sauvegarde en direct, le serveur Hyper-V met la machine virtuelle hors ligne (placée dans l'état sauvegardé) pendant le processus de sauvegarde, puis restaure la machine virtuelle à son état précédent lorsque le processus de sauvegarde est terminé. Bien que la mise hors ligne de la machine virtuelle entraîne l'indisponibilité de celle-ci, la sauvegarde devrait se terminer sans affecter de manière négative le contenu de la machine virtuelle. Pour plus d'informations, visitez le site <https://technet.microsoft.com/en-us/library/dn798286.aspx>.

Étant donné que Microsoft ne prend pas en charge les sauvegardes en direct du système d'exploitation FreeBSD exécuté sur l'appliance KACE, il est important de configurer les paramètres de services d'intégration appropriés des machines virtuelles Hyper-V KACE SMA qui empêchent l'Hyper-V de tenter d'effectuer des sauvegardes en direct de la machine virtuelle. Lorsque les paramètres de services d'intégration de la machine virtuelle ne sont pas correctement configurés, certains clients ont connu des corruptions de fichiers au sein du KACE SMA qui ont entraîné son fonctionnement incorrect. Le support technique a dû être contacté pour résoudre le problème.

Microsoft activant automatiquement par défaut le service d'intégration de sauvegarde sur toutes les nouvelles machines virtuelles HyperV, si vous créez une machine virtuelle HyperV sur l'appliance KACE SMA, suivez les instructions ci-dessous pour configurer correctement ce service

pour FreeBSD, afin d'empêcher la corruption de fichiers de la base de données mentionnée ci-dessus.

Il est recommandé de désactiver la fonctionnalité de sauvegarde en direct sur les machines virtuelles Hyper-V KACE SMA.

Pour désactiver le service d'intégration de sauvegarde, dans la boîte de dialogue Paramètres de la machine virtuelle, sous Gestion > Services d'intégration, décochez la case Sauvegarde (point de contrôle de volume), puis cliquez sur Appliquer. Ce paramètre peut avoir un autre nom, comme Sauvegarde (copie masquée), selon la version Windows du serveur Hyper-V.



Pour modifier ce paramètre, vous devez d'abord arrêter la machine virtuelle.



Une fois le paramètre de sauvegarde désactivé, si Windows ne parvient pas à mettre hors ligne la machine virtuelle en premier lieu (en modifiant l'état de la machine virtuelle sur sauvegardé) pendant le processus de sauvegarde et si la corruption MySQL dans l'appliance KACE se poursuit pendant la sauvegarde de la machine virtuelle, mettez la machine virtuelle en état arrêt ou sauvegardé avant d'effectuer la sauvegarde de la machine virtuelle.

Pour des informations supplémentaires sur ce problème, rendez-vous sur <https://support.quest.com/kace-systems-management-appliance/kb/195580>.

## Configuration de la carte réseau virtuelle

La défaillance du réseau, comprenant des performances faibles, un agent déconnecté, le blocage de l'interface et l'indisponibilité totale du réseau, est observée sur l'appliance virtuelle de déploiement des systèmes KACE s'exécutant sur l'Hyper-V.

Par défaut, deux paramètres du réseau problématiques sont activés dans l'Hyper-V pour toutes les machines virtuelles invitées. Ces paramètres sont Adresse MAC dynamique et VMQ (file d'attente de la machine virtuelle).

Lorsqu'il est configuré avec une adresse MAC dynamique, l'Hyper-V peut attribuer aléatoirement une nouvelle adresse MAC à la machine virtuelle invitée. Étant donné que les appliances KACE sont exécutées sous FreeBSD, le système d'exploitation doit être redémarré afin de détecter les modifications apportées à l'interface réseau.

VMQ est une technologie de filtrage de paquets dans Hyper-V qui réduit la surcharge de travail liée au routage des paquets sur le matériel et les systèmes d'exploitation invités pris en charge. Cependant, cette technologie n'est pas prise en charge par la carte réseau virtuelle Intel E1000 utilisée par les appliances KACE, ce qui peut nuire aux performances du réseau. VMQ entraîne également des problèmes de performances pour certaines cartes réseau physiques Broadcom.

Pour résoudre ce problème, il est conseillé de désactiver l'adresse MAC dynamique (en choisissant une adresse MAC statique) et VMQ sur toutes les appliances virtuelles KACE hébergées sur Hyper-V.

Pour désactiver l'adresse MAC dynamique, dans la boîte de dialogue Paramètres de la machine virtuelle, sous Carte réseau > Fonctionnalités avancées, cochez la case Statique et spécifiez une adresse MAC unique valide pour votre environnement. Cliquez ensuite sur Appliquer.



Généralement, vous pouvez laisser l'adresse MAC actuelle qui est déjà attribuée de manière dynamique.



Pour passer d'une adresse MAC dynamique à une adresse MAC statique, et vice versa, vous devez d'abord arrêter la machine virtuelle.

Pour désactiver VMQ, dans la boîte de dialogue Paramètres de la machine virtuelle, sous Carte réseau > Accélération du matériel, décochez la case Activer la file d'attente de la machine virtuelle, puis cliquez sur Appliquer.

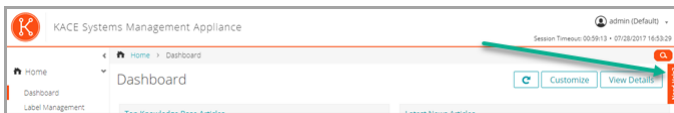


Bien que ce paramètre puisse être modifié sans arrêter la machine virtuelle, il est préférable de le modifier lorsque la machine virtuelle est hors ligne.

Pour des informations supplémentaires sur ce problème, rendez-vous sur <https://support.quest.com/kace-systems-management-appliance/kb/153445>.

## 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>

# Einrichten der Appliance

In diesem Handbuch wird erklärt, wie Sie die virtuelle KACE Systemverwaltungs-Appliance (SMA) auf Microsoft® Hyper-V® 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.



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 oder durch Hinzufügen zu einer DMZ (demilitarisierte Zone) oder zu einem überwachten Subnetz hergestellt wird. Durch eine DMZ wird ein LAN (lokales Netzwerk) um eine zusätzliche Sicherheitsebene erweitert.
5. Konfigurieren Sie die Sicherungsintegrationsdienste für die Virtual Appliances, die auf Hyper-V ausgeführt werden. Weitere Informationen finden Sie unter [Konfiguration von Backup-Integrationsdiensten](#).



Die falsche Konfiguration der Sicherungsintegrationsdienste kann zu einer Beschädigung der MySQL-Datenbankdatei führen.

## Importieren der virtuellen KACE SMA in einen Microsoft Hyper-V-Server und Konfigurieren der Einstellungen

Hyper-V-Manager ist das integrierte Verwaltungstool für virtuelle Computer zum Importieren der virtuellen KACE KACE SMA.

- Konfigurieren Sie den virtuellen Computer nicht mit dem Legacy-Netzwerkadapter.
  - Lassen Sie im Hyper-V-Manager die Standardeinstellung unverändert, um den Hyper-V-Zeitsynchronisierungsdienst zu aktivieren.
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 Abschnitt Virtuelle Appliance das komprimierte VHD-Bundle auf das Hyper-V-Hostsystem herunter.
  3. Extrahieren Sie die Dateien und überprüfen Sie deren Integrität.
  4. Klicken Sie im Hyper-V-Manager mit der rechten Maustaste auf den Host und klicken Sie dann auf Virtuellen Computer importieren.

Das Fenster Virtuellen Computer importieren wird angezeigt.

5. Navigieren Sie zum Speicherort des extrahierten VHD-Bundles.
6. Aktivieren Sie unter Einstellungen die Optionen Virtuellen Computer kopieren (neue eindeutige ID erstellen) und Alle Dateien duplizieren, sodass derselbe virtuelle Computer erneut importiert werden kann.
7. Klicken Sie auf Importieren.

Die virtuelle KACE SMA wird in der Liste der virtuellen Computer angezeigt.

8. Bearbeiten Sie die Einstellungen des virtuellen Computers, um eine Verbindung zwischen dem virtuellen Netzwerkadapter und dem virtuellen Switch des Hyper-V-Hosts herzustellen.
9. Wählen Sie eine statische MAC-Adresse für die virtuelle Maschine aus:



Quest empfiehlt die Verwendung einer statischen MAC-Adresse, da Hyper-V eine neue MAC-Adresse möglicherweise zufällig an die virtuelle Maschine vergibt, wenn eine dynamische MAC-Adresse verwendet wird. Da die KACE SMA unter FreeBSD® ausgeführt wird, muss das Gastbetriebssystem neu gestartet werden, um die Änderung der Netzwerkschnittstelle zu erkennen. Das kann zu fehlerhaftem Netzwerkverhalten führen.

- a. Navigieren Sie zum Abschnitt Erweiterte Funktionen in den Einstellungen Netzwerkadapter der virtuellen Maschine.
  - b. Wählen Sie Statisch bei der MAC-Adresse aus.
  - c. Geben Sie eine gültige, eindeutige MAC-Adresse für Ihre Umgebung an. Normalerweise können Sie die aktuelle MAC-Adresse verwenden.
  - d. Klicken Sie auf Übernehmen.
10. Deaktivieren Sie Warteschlange für virtuelle Computer (VMQ) für die virtuelle Maschine:



VMQ ist eine Paketfiltertechnologie in Hyper-V für die Verringerung des Mehraufwands beim Paketrouting in Verbindung mit unterstützter Hardware und unterstützten Gastbetriebssystemen. VMQ wird jedoch nicht von der Netzwerk-

Interface-Steuereinheit (NIC) Intel® e1000 unterstützt, die für die KACE SMA eingesetzt wird. Daher kann es zu schlechter Netzwerkleistung kommen. Außerdem sind bei einigen physischen Adaptern Leistungsprobleme in Verbindung mit VMQ bekannt. Daher empfiehlt Quest die Deaktivierung von VMQ.

- a. Navigieren Sie zum Abschnitt Hardwarebeschleunigung in den Einstellungen Netzwerkadapter der virtuellen Maschine.
- b. Deaktivieren Sie das Kontrollkästchen neben Warteschlange für virtuelle Maschinen aktivieren.
- c. Klicken Sie auf Übernehmen.

Schalten Sie die Appliance ein.

## 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
Lizenzschlüssel	Der Lizenzschlüssel, den Sie in der Begrüßungs-E-Mail von Quest erhalten haben. Wenn Sie keinen Lizenzschlüssel besitzen, wenden Sie sich an den Quest Softwaresupport unter <a href="https://support.quest.com/contact-support">https://support.quest.com/contact-support</a> .
Name der Firma	Der Name Ihrer Firma oder Gruppe.
E-Mail-Adresse des Administrators	Die E-Mail-Adresse, an die Sie Kommunikation von Quest erhalten möchten.
Kennwort	<p>Das Kennwort für das Standardkonto admin. Mit diesem Konto melden Sie sich bei der Administratorkonsole der Appliance an. Das Standardkonto admin 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> 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: <a href="#">Zugriff auf das Administratorhandbuch und die Onlinehilfe</a>.</p>
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 Verifizierungs-codes zu generieren. Die App generiert in regelmäßigen Abständen einen neuen sechsstelligen Code. Wenn diese

## Option

## Beschreibung

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 geändert haben, wechseln Sie zu der neuen 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. 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.



Überprüfen Sie bei der Anmeldung an der virtuellen KACE SMA, ob Automatisch mit einem Internetzeitserver synchronisieren in den Datum- und Uhrzeiteinstellungen deaktiviert ist. Auf diese Einstellungen greifen Sie über Einstellungen > Systemsteuerung zu.

# 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
KACE SMA DNS-Hostname	<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>
Servernamen automatisch generieren	<p>Aktivieren Sie dieses Kontrollkästchen, damit das System den Namen des KACE SMA Webservers im folgenden Format generiert: Hostname.Domain. Beispiel: &lt;eindeutiger_KACE_SMA_Appliance Name&gt;.beispiel.com. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie einen benutzerdefinierten Webservernamen eingeben möchten.</p>

Option	Beschreibung
KACE SMA Webservername	<p>Geben Sie den vollständig qualifizierten Domainnamen der Appliance ein. Hierbei handelt es sich um den mit der Domain verknüpften Hostnamen. 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>
DHCP	<p>(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>
Manuelle IPv4-Konfiguration	<p>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>
SLAAC	<p>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 können Geräte ihre eigenen IPv6-Adressen basierend auf dem Präfix auswählen, das von der verbundenen Schnittstelle mitgeteilt wird.</p>
Manuelle IPv6-Konfiguration	<p>Wählen Sie diese Option, wenn Sie die IPv6-Adresse manuell angeben möchten. Wenn Sie</p>



Die IPv4-Adresse ist unabhängig von der Verfügbarkeit einer IPv6-Adresse erforderlich. Die IPv6-Adresse ist optional.

Option	Beschreibung
	<p>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>
Deaktivieren Sie IPv6.	<p>Wählen Sie diese Option, wenn Sie die IPv6-Adresse für die Appliance deaktivieren möchten. Dies ist die Standardeinstellung.</p>
SMTP-Server	<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>
SSH aktiviert	<p>(Optional) Wählen Sie diese Option, um den sicheren Zugriff (SSH) auf die Administratorkonsole 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 Administratorkonsole ändern.</p>
Proxy	<p>(Optional) Geben Sie die Informationen des Proxy-Servers ein.</p> <p> Die Appliance unterstützt Proxy-Server mit bereichsbasierter Standardauthentifizierung, für die Benutzernamen und Kennwörter erforderlich sind. Verwendet Ihr Proxy-Server eine andere Authentifizierungsmethode, fügen</p>

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

## Option

## Beschreibung



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 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.

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 geändert haben, wechseln Sie zu der neuen 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.

## Konfiguration von Backup-Integrationsdiensten

Die Konfiguration der Sicherungsintegrationsdienste für die entsprechenden virtuellen Maschinen der KACE Systemverwaltungs-Appliance (SMA) auf Hyper-V verhindert die Beschädigung der MySQL-Datenbankdateien.

Die virtuelle Maschinen der KACE SMA auf Hyper-V ist für die Sicherung der virtuellen Maschine (VM) falsch konfiguriert, was zur Beschädigung einiger MySQL-Datenbankdateien innerhalb der Appliance führt. Somit kann die Appliance bis zur Kontaktaufnahme mit dem technischen Support für die Lösung des Problems durch Wiederherstellen der Datenbank aus dem neusten, nicht beschädigten Datenbank-Backup nicht genutzt werden.

Dies wird durch die Hyper-V Funktion Live-Sicherung von virtuellen Maschinen verursacht, die Sicherung von virtuellen Live-Maschinen ohne Ausfallzeiten unterstützt. Weitere Informationen finden Sie unter [https://technet.microsoft.com/en-us/library/dn531031\(v=ws.12\).aspx](https://technet.microsoft.com/en-us/library/dn531031(v=ws.12).aspx).

Jedoch unterstützt Microsoft die Hyper-V Funktion Live-Sicherung noch nicht für alle Versionen der virtuellen FreeBSD Maschinen auf Hyper-V, die Hyper-V VMs von KACE SMA Produkten umfassen, da diese auf FreeBSD basieren. Weitere Informationen finden Sie unter [https://technet.microsoft.com/library/dn848318\(ws.12\).aspx](https://technet.microsoft.com/library/dn848318(ws.12).aspx).

Bei ordnungsgemäßer Konfiguration wird eine VM, bei der die Funktion „Live-Backup“ nicht unterstützt wird, vom Hyper-V-Server beim Erstellen einer Sicherung für die Dauer des Sicherungsvorgangs offline (in den Status gesichert) geschaltet. Nach Abschluss des Sicherungsvorgangs wird die VM wieder auf ihren vorherigen Status zurückgesetzt. Während die VM offline geschaltet werden muss, was zu einer Ausfallzeit für die VM führt, sollte das Backup, ohne die Inhalte der VM zu beeinträchtigen, abgeschlossen werden können. Weitere Informationen finden Sie unter <https://technet.microsoft.com/en-us/library/dn798286.aspx>.

Da Microsoft Live-Sicherung für das Betriebssystem FreeBSD, auf die KACE Appliances ausgeführt werden, nicht unterstützt, ist es wichtig, die entsprechenden Einstellungen der



Integrationservices von KACE SMA Hyper-V VMs zu konfigurieren, die verhindern, dass Hyper-V Live-Sicherungen der VM durchführt. Sofern die VM-Einstellungen Integrationservices nicht ordnungsgemäß konfiguriert wurden, wurden bei einigen Kunden die Dateien in der KACE SMA beschädigt, wodurch diese nicht ordnungsgemäß funktionierte und zur Behebung des Problems der technische Support kontaktiert werden musste.

Da Microsoft den Backup-Integrationservice aller neuen Hyper-V VMs standardmäßig aktiviert, befolgen Sie beim Erstellen einer Hyper-V VM für die KACE SMA die nachfolgenden Anweisungen für die ordnungsgemäße Konfiguration dieses Dienstes für FreeBSD, um die Beschädigung der obigen Datenbank zu vermeiden.

Es wird empfohlen, die Funktion Live-Sicherung auf KACE SMA Hyper-V VMs zu deaktivieren.

Um den Backup-Integrationsdienst im Dialogfeld VM-Einstellungen unter Verwaltung > Integrationsdienste auszuschalten, deaktivieren Sie das Kontrollkästchen Backup (Volume-Prüfpunkt) und klicken auf Übernehmen. Diese Einstellung kann je nach Windows-Version des Hyper-V-Servers eine andere Bezeichnung haben, wie beispielsweise Backup (Volume-Schattenkopie).



Um diese Einstellung zu ändern, müssen Sie zuerst die VM herunterfahren.



Wenn die Backup-Einstellung deaktiviert ist und Windows die VM nicht offline setzen kann (indem der Status der VM auf gesichert geändert wird), setzen Sie während des Backup-Prozesses, und wenn die MySQL-Beschädigung der KACE-Appliance während des VM-Backups fortbesteht, die VM auf den Status Herunterfahren oder gesichert, bevor Sie ein VM-Backup ausführen.

Weitere Informationen zu diesem Problem finden Sie unter <https://support.quest.com/kace-systems-management-appliance/kb/195580>.

## Virtuelle NIC-Konfiguration

In einer virtuellen KACE Systems Deployment Appliance (SDA) auf Hyper-V wird fehlerhaftes Netzwerkverhalten, einschließlich schlechter Leistung, Trennung des Agenten, Einfrieren von Schnittstellen und die vollständige Nichtverfügbarkeit des Netzwerks, beobachtet.

In Hyper-V sind für alle virtuellen Gast-Maschinen (VMs) zwei problematische Netzwerkeinstellungen standardmäßig aktiviert. Diese Einstellungen sind eine Dynamische MAC-Adresse und VMQ (Warteschlange virtueller Maschinen).

Bei Konfiguration mit einer dynamischen MAC-Adresse kann Hyper-V der Gast-VM willkürlich eine neue MAC-Adresse zuweisen. Da die KACE Appliances auf FreeBSD aufgeführt werden, muss das Betriebssystem neu gestartet werden, damit die Änderung der Netzwerkschnittstelle erkannt wird.

VMQ ist eine Paketfiltertechnologie in Hyper-V, die den Mehraufwand beim Paketrouting in Verbindung mit unterstützter Hardware und unterstützten Gastbetriebssystemen verringert. VMQ wird jedoch nicht von der virtuellen NIC Intel E1000 unterstützt, die für die KACE eingesetzt wird. Daher kann es zu schlechter Netzwerkleistung kommen. Außerdem sind bei einigen physischen Broadcom-Adaptoren Leistungsprobleme in Verbindung mit VMQ bekannt.

Um dieses Problem zu lösen, wird empfohlen, sowohl die dynamische MAC-Adresse (durch Auswahl einer statischen MAC-Adresse) als auch VMQ zu deaktivieren, und zwar auf allen über Hyper-V gehosteten virtuellen KACE Appliances.

Um die dynamische MAC-Adresse im Dialogfeld VM-Einstellungen unter Netzwerkadapter > Erweiterte Funktionen zu deaktivieren, aktivieren das Kontrollkästchen Statisch und geben eine gültige, eindeutige MAC-Adresse für Ihre Umgebung an. Klicken Sie dann auf Übernehmen.

- Dieses kann normalerweise die aktuelle MAC-Adresse bleiben, die bereits dynamisch zugewiesen wurde.
- Um eine dynamische MAC-Adresse auf eine statische zu ändern und umgekehrt, müssen Sie zuerst die VM herunterfahren.

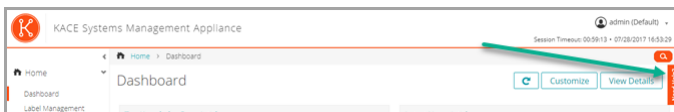
Um VMQ zu deaktivieren, löschen Sie im Dialogfeld VM-Einstellungen unter Netzwerkadapter > Hardware-Beschleunigung, das Kontrollkästchen Warteschlange für virtuelle Computer aktivieren und klicken auf Übernehmen.

- Diese Einstellung kann zwar ohne Herunterfahren der VM geändert werden, es wird jedoch empfohlen, diese Änderung durchzuführen, während die Maschine offline ist.

Weitere Informationen zu diesem Problem finden Sie unter <https://support.quest.com/kace-systems-management-appliance/kb/153445>.

## 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>

# 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 Microsoft® Hyper-V® 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DMZ ( 非武装地帯 ) 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。
5. Hyper-V で実行されている仮想アプライアンスのバックアップ統合サービスを設定します。詳細については、「[バックアップ統合サービスの設定](#)」を参照してください。



バックアップ統合サービスを正しく設定できないと、MySQL データベースファイルの破損が発生する可能性があります。

## Microsoft Hyper-Vサーバへの仮想KACE SMAのインポートと設定の構成

Hyper-Vマネージャーは、仮想KACE SMAをインポートする際に使用する、ビルトイン仮想マシン管理ツールです。

- レガシーネットワークアダプタを使って、仮想マシンを設定しないでください。

- Hyper-V Manager で、デフォルト設定を維持して Hyper-V Time Synchronization Service ( Hyper-V 時刻の同期サービス ) を有効にします。
- 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、VHD 圧縮バンドルを Hyper-V ホストシステムにダウンロードします。
- 3. ファイルを解凍し、整合性を確認します。
- 4. Hyper-Vマネージャーでホストを右クリックして、仮想マシンのインポート をクリックします。

仮想マシンのインポート ウィンドウが表示されます。

- 5. 解凍したVHDバンドルの場所を参照します。
  - 6. 「設定」で、「仮想マシンをコピーする ( 新しい一意なIDを作成する ) 」および「すべてのファイルを複製し、同じ仮想マシンを再度インポートできるようにする」を選択します。
  - 7. インポート をクリックします。
- 仮想KACE SMAが 仮想マシン リストに表示されます。
- 8. 仮想マシンの設定を編集して、仮想ネットワークアダプタをHyper-Vホストの仮想スイッチに接続できるようにします。
  - 9. 仮想マシンの静的 MAC アドレスを選択します。

**i** Quest では静的 MAC アドレスを使用することをお勧めします。これは、動的 MAC アドレスを使用すると、Hyper-V によって仮想マシンに新しい MAC アドレスがランダムに割り当てられる可能性があるためです。KACE SMAは FreeBSD®上で実行されるため、ゲストオペレーティングシステムを再起動して、ネットワークインタフェースの変更を検出する必要があります。これによって誤ったネットワーク動作が発生する場合があります。

- a. 仮想マシンの ネットワーク アダプタ 設定の 高度な機能 セクションに移動します。
  - b. MAC アドレス の下で 静的 を選択します。
  - c. 使用する環境に有効な一意の MAC アドレスを指定します。通常は現在の MAC アドレスを使用できます。
  - d. 適用 をクリックします。
- 10. 仮想マシンの仮想マシンキュー ( VMQ ) を無効にします。

**i** VMQ は、サポートされるハードウェアおよびゲストオペレーティングシステムによるバケットルーティングのオーバーヘッドを削減するために設計された、Hyper-V のバケットフィルタリング技術です。ただし、KACE SMAが使用するIntel® e1000仮想NIC ( ネットワークインタフェースコントローラ ) でサポートされていないため、ネットワークパフォーマンスが低下する可能性があります。一部の物理アダプタでも VMQ によるパフォーマンスの問題があることが分かっています。このため、Quest では VMQ を無効にすることをお勧めしています。

- a. 仮想マシンの ネットワーク アダプタ 設定の ハードウェア アクセラレータ セクションに移動します。
- b. 仮想マシンキューを有効にする の隣のチェックボックスをオフにします。
- c. 適用 をクリックします。

アプライアンスの電源をオンにします。

## 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分かかりません。

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`。

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

## オプション

## 説明

	い場合は、Quest Software サポート ( <a href="https://support.quest.com/contact-support">https://support.quest.com/contact-support</a> ) お問い合わせ 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 admin 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 admin 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admin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『Administrator Guide』 ( 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。

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 アドレスを変更した場合は、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。



仮想 KACE SMA にログインするときは、日付と時刻の設定 (設定 > コントロール パネル からアクセス) で、自動的にインターネット時刻サーバーと同期する が無効になっていることを確認してください。

## 手動による初期ネットワーク設定の構成 (オプション)

DHCPサーバー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分かかりません。

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。

### 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

## オプション

## 説明

	びセカンダリ DNS の設定を入力する必要がなくなります。
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。</p>
SSHを有効にする	<p>( 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</p>

## オプション

## 説明

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、基本的なレル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キーを押します。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://support.quest.com/contact-support>) 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

デフォルトの admin 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 admin 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。



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 admin 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『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](#)

## 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。

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 アドレスを変更した場合は、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。

## バックアップ統合サービスの設定

Hyper-Vで実行されているKACE Systems Management Appliance ( SMA ) 仮想マシンにバックアップ統合サービスを適切に設定することで、MySQLデータベースファイルの破損を防ぐことができます。

Hyper-Vで実行されているKACE SMA仮想マシンが仮想マシン ( VM ) のバックアップに正しく設定されていないと、アプライアンス内部で一部のMySQLデータベースファイルが破損し、テクニカルサポートに連絡を取り、破損していない最新のデータベースバックアップからデータベースを復元して問題を解決するまでアプライアンスが使用できなくなります。

これは、ライブ仮想マシンのダウンタイムなしバックアップを容易化する、Hyper-Vの ライブ仮想マシンバックアップ 機能が原因です。詳細については、[https://technet.microsoft.com/en-us/library/dn531031\(v=ws.12\).aspx](https://technet.microsoft.com/en-us/library/dn531031(v=ws.12).aspx)を参照してください。

ただし、Microsoftは、Hyper-Vで動作するFreeBSD仮想マシンのどのバージョンに対しても、Hyper-V ライブバックアップ 機能は未サポートであり、これには、FreeBSDベースであるKACE SMA製品のHyper-V VMも含まれます。詳細については、[https://technet.microsoft.com/library/dn848318\(ws.12\).aspx](https://technet.microsoft.com/library/dn848318(ws.12).aspx)を参照してください。

正しく設定した場合、ライブバックアップをサポートしないVMのバックアップを取った場合、Hyper-Vサーバはバックアップ処理中VMを ( 保存済み 状態にして ) オフラインにし、バックアップ処理の完了後、VMを元の状態に復元します。VMをオフラインにする必要がある間は、VMでダウンタイムが発生するため、VMのコンテンツに悪影響を及ぼさずにバックアップを完了する必要があります。詳細については、<https://technet.microsoft.com/en-us/library/dn798286.aspx>を参照してください。

Microsoftが、KACEアプライアンスが動作するFreeBSDオペレーティングシステムのライブバックアップをサポートしないため、Hyper-VがVMのライブバックアップの実行を試行しないように

する、KACE SMA Hyper-V VMの統合サービスを適切に設定するのが重要です。VMの統合サービスが正しく設定されていない場合、KACE SMAの内部でファイルの破損が発生して、正しく動作しない原因になり、問題を修正してもらうためにテクニカルサポートへの連絡が必要になる可能性があります。

Microsoft は自動的にすべての新しい Hyper-V VM のバックアップ統合サービスをデフォルトで有効にするため、KACE SMA に Hyper-V VM を作成した場合は、下の手順に従って、FreeBSD 向けのこのサービスを正しく設定して、上記のデータベースファイルの破損を回避します。

KACE SMA Hyper-V VMでライブバックアップ機能を無効にすることをお勧めします。

バックアップ統合サービスを無効にするには、VM の設定 ダイアログボックスの 管理 > 統合サービス の下で、バックアップ ( ポリウムチェックポイント ) チェックボックスをオフにして、適用 をクリックします。この設定は、Hyper-V サーバの Windows のバージョンにより、バックアップ ( ポリウムシャドウコピー ) など、名前が異なる場合があります。



この設定を変更するには、最初に VM をシャットダウンする必要があります。



バックアップ設定を無効にした後、バックアップ処理中にまず Windows が ( VM の状態を保存済みに変更して ) VM をオフラインにするのに失敗し、VM のバックアップ中に引き続き KACE アプライアンスでの MySQL の破損が発生する場合は、VM のバックアップを実行する前に VM をシャットダウンまたは保存済み状態にします。

この問題の追加情報については、<https://support.quest.com/kace-systems-management-appliance/kb/195580> にアクセスしてください。

## 仮想 NIC の構成

Hyper-Vで実行されている仮想KACEシステム導入アプライアンス ( SDA ) では、パフォーマンスの低下、エージェントの切断、インターフェースのフリーズ、およびネットワークが全く利用できないなど、不安定なネットワーク動作が確認されています。

デフォルトでは、すべてのゲスト仮想マシン ( VM ) に対して問題のある2つのネットワーク設定がHyper-Vで有効になっています。これらの設定は、動的 MAC アドレスとVMQ ( 仮想マシンキュー ) です。

動的 MAC アドレスを使用して構成されている場合、Hyper-V はゲスト VM に新しい MAC アドレスをランダムに割り当てます。KACE アプライアンスが FreeBSD で実行されているため、ネットワークインターフェイスの変更を検出するには OS を再起動する必要があります。

VMQ は、サポートされるハードウェアおよびゲストオペレーティングシステムによるパケットルーティングのオーバーヘッドを削減するために設計された、Hyper-V のパケットフィルタリング技術です。ただし、KACE アプライアンスが使用する Intel E1000 仮想 NIC でサポートされていないため、ネットワークパフォーマンスが低下する可能性があります。一部の Broadcom 物理アダプタでも VMQ によるパフォーマンスの問題があることが分かっています。

この問題を解決するには、すべての Hyper-V ホスト型仮想 KACE アプライアンスで、動的 MAC アドレス ( 静的 MAC で選択 ) および VMQ の両方を無効にすることを推奨します。

動的 MAC アドレスを無効にするには、VM の 設定 ダイアログボックスの ネットワーク アダプタ > 高度な機能 で、静的 チェックボックスを選択して、環境に対して有効な一意の MAC アドレスを指定します。次に、適用 をクリックします。



通常、これによりすでに動的に割り当てられている現在の MAC アドレスとして残すことができます。



動的 MAC アドレスを静的 MAC アドレスに切り替えるには ( またはその逆を実行するには )、最初に VM をシャットダウンする必要があります。

VMQ を無効にするには、VM の 設定 ダイアログボックスの ネットワークアダプタ > ハードウェア アクセラレータ で、仮想マシンキューを有効にする チェックボックスを選択解除して、適用 をクリックします。

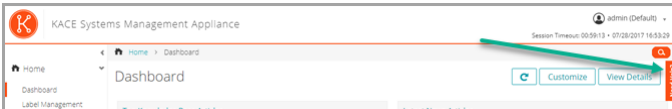


この設定は VM をシャットダウンせずに変更することができますが、VM がオフラインのときに変更することを推奨します。

この問題の追加情報については、<https://support.quest.com/kace-systems-management-appliance/kb/153445> にアクセスしてください。

## 管理者ガイドおよびオンラインヘルプへのアクセス

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>



# Configuração do equipamento

Este guia explica como configurar a Solução de gerenciamento de sistemas KACE (SMA) virtual nos sistemas host Microsoft® Hyper-V®. 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 tíquetes 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 DMZ (Demilitarized Zone, Zona desmilitarizada) ou sub-rede filtrada. Uma DMZ adiciona uma camada adicional de segurança a uma LAN (Local Area Network, Rede de Área Local).
5. Configure os serviços de integração de backups para os equipamentos virtuais executados no Hyper-V. Para obter mais informações, consulte [Como configurar os serviços de integração de backup](#).



Deixar de configurar corretamente serviços de integração de backup pode fazer com que o arquivo do banco de dados MySQL seja corrompido.

## Importar o KACE SMA virtual para um servidor Microsoft Hyper-V e definir as configurações

O Gerenciador Hyper-V é a ferramenta de gerenciamento de máquina virtual integrada que você utiliza para importar o KACE SMA virtual.

- Não configure a máquina virtual com o Adaptador de rede legado.
  - No Gerenciador Hyper-V, mantenha a configuração padrão para habilitar o Serviço de sincronização de horário do Hyper-V.
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 pacote VHD compactado para o seu sistema host Hyper-V.
  3. Extraia e verifique a integridade dos arquivos.
  4. No Gerenciador Hyper-V Manager, clique com o botão direito do mouse em host e clique em Importar máquina virtual.

A janela Importar máquina virtual será exibida.

5. Navegue até o local do pacote VHD extraído.
6. Em Configurações, selecione Copiar a máquina virtual (criar uma nova ID exclusiva) e Duplicar todos os arquivos de modo que a mesma máquina virtual seja novamente importada.
7. Clique em Importar.

A solução KACE SMA virtual é exibida na lista Máquinas virtuais.

8. Edite as configurações da máquina virtual para conectar o adaptador de rede virtual ao switch virtual do seu host Hyper-V.
9. Escolha um endereço MAC estático para a máquina virtual:



A Quest recomenda o uso de um endereço MAC estático, pois o Hyper-V pode atribuir aleatoriamente um novo endereço MAC para a máquina virtual se um endereço MAC dinâmico for usado. Como o KACE SMA é executado no FreeBSD®, o sistema operacional convidado deve ser reiniciado para detectar a alteração na interface de rede, o que pode resultar em um comportamento irregular da rede.

- a. Acesse a seção Recursos avançados das configurações do Adaptador de rede da máquina virtual.
  - b. Selecione Estático em Endereço MAC.
  - c. Especifique um endereço MAC único válido para o ambiente. Geralmente, você pode usar o endereço MAC atual.
  - d. Clique em Aplicar.
10. Desabilite a fila de máquina virtual (VMQ) da máquina virtual:



VMQ é uma tecnologia de filtragem de pacotes no Hyper-V concebida para reduzir a sobrecarga no roteamento de pacotes com hardware suportado e sistemas operacionais convidados. No entanto, não é suportado pelo NIC (controlador de interface de rede) virtual Intel® e1000 usado pelo KACE SMA, o que pode resultar em um baixo desempenho da rede. Alguns adaptadores físicos também são

conhecidos por terem problemas de desempenho com VMQ. Portanto, a Quest recomenda desativar o VMQ.

- a. Acesse a seção Aceleração de hardware das configurações do Adaptador de rede da máquina virtual.
- b. Desmarque a caixa de seleção ao lado de Habilitar fila de máquina virtual.
- c. Clique em Aplicar.

Ligue a solução.

## 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 na 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.
5. 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.
6. Na página Configurações do administrador e licenciamento, forneça as seguintes informações:

Opção	Descrição
Chave de licença	A chave de licença recebida no e-mail de boas-vindas da Quest. Se você não tem uma chave de licença, entre em contato com o Suporte ao software da Quest em <a href="https://support.quest.com/contact-support">https://support.quest.com/contact-support</a> .
Nome da empresa	O nome de sua empresa ou grupo.
E-mail do administrador	O endereço de e-mail em que você deseja receber as comunicações da Quest.
Senha	<p>A senha para a conta de administrador padrão, que é a conta usada para fazer o login no Console do administrador da solução. A conta de administrador 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 administrador em todas as soluções. Isso permitirá vincular as soluções posteriormente. Para obter mais informações, consulte o Guia do administrador da solução: <a href="#">Acessar o Guia do administrador e a Ajuda on-line</a>.</p>
Autenticação de dois fatores	<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 Authenticator. O Google Authenticator depende da hora atual para criar o</p>

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 alterou 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.



Ao fazer login no KACE SMA virtual, verifique se Sincronizar automaticamente com um servidor de horário da Internet está desativado nas Configurações de data e hora acessadas em Configurações > Painel de controle.


## 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
Nome do host DNS do KACE SMA	<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> <div style="border-left: 1px solid black; padding-left: 10px; margin-top: 10px;">  <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> </div>
Gerar automaticamente nome do servidor	<p>Marque essa caixa de seleção para permitir que o sistema gere o nome do servidor da Web do KACE SMA utilizando este formato: Nome de host.Domínio. 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>
Nome do servidor da Web do KACE SMA	<p>Digite o nome do domínio totalmente qualificado da solução. Este é o Nome do host concatenado ao Domínio. 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>
DHCP	<p>(Opcional) Selecione essa opção para usar DHCP (Dynamic Host Configuration Protocol) e obter automaticamente o endereço IPv4 e</p>

Opção	Descrição
Configuração IPv4 manual	<p>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> <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>
SLAAC	<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>
Configuração IPv6 manual	<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 do equipamento.</p> <p> O endereço IPv6 é opcional. O endereço IPv4 é necessário quer um endereço IPv6 esteja disponível ou não.</p>
Desative o IPv6	<p>Selecione essa opção se quiser desativar um endereço IPv6 do equipamento. Essa é a configuração padrão.</p>
Servidor SMTP	<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-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</p>

Opção	Descrição
SSH habilitado	<p>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> <p>(Opcional) Selecione esta opção para ativar o acesso SSH (seguro) ao Console do administrador 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 Console do administrador conforme necessário.</p>
Proxy	<p>(Opcional) Digite as informações do servidor proxy.</p> <div style="border-left: 1px solid #0070C0; padding-left: 10px; margin-left: 20px;"> <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> </div>
<ol style="list-style-type: none"> <li>5. Use a seta para baixo para mover o cursor para Salvar e pressione Enter ou Retornar. O equipamento é reiniciado.</li> <li>6. Em qualquer computador conectado à sua LAN, abra um navegador e vá para o URL do Console do administrador da solução. Por exemplo, <code>http://&lt;unique_KACE_SMA_appliance_name&gt;.local/admin</code>. A página Acordo de transação de software será exibida.</li> <li>7. Aceite o acordo. O assistente de Configuração inicial será exibido.</li> <li>8. Verifique se você possui as informações necessárias para configurar a solução e depois clique em Avançar.</li> <li>9. 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.</li> <li>10. Na página Configurações do administrador e licenciamento, forneça as seguintes informações:</li> </ol>	



Opção	Descrição
Chave de licença	<p>A chave de licença recebida no e-mail de boas-vindas da Quest. Se você não tem uma chave de licença, entre em contato com o Suporte ao software da Quest em <a href="https://support.quest.com/contact-support">https://support.quest.com/contact-support</a>.</p>
Nome da empresa	O nome de sua empresa ou grupo.
E-mail do administrador	O endereço de e-mail em que você deseja receber as comunicações da Quest.
Senha	<p>A senha para a conta de administrador padrão, que é a conta usada para fazer o login no Console do administrador da solução. A conta de administrador 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>
Autenticação de dois fatores	<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>

**i** Se houver várias soluções KACE SMA ou KACE SDA (Implantação de sistemas) a Quest recomenda usar a mesma senha para a conta de administrador em todas as soluções. Isso permitirá vincular as soluções posteriormente. Para obter mais informações, consulte o Guia do administrador da solução: [Acessar o Guia do administrador e a Ajuda on-line](#).

**i** 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.

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 alterou 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 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.

## Como configurar os serviços de integração de backup

Configurar os serviços de integração de backup adequadamente para as máquinas virtuais com Solução de gerenciamento de sistemas KACE (SMA) sendo executadas no Hyper-V impede danos nos arquivos do banco de dados MySQL.

A máquina virtual KACE SMA que está sendo executada no Hyper-V está incorretamente configurada para backup de máquina virtual (VM), resultando em algum dano no arquivo de banco de dados MySQL dentro da solução, tornando a solução inutilizável até que o Suporte Técnico seja acionado para resolver o problema, restaurando o banco de dados para o backup de banco de dados mais atual e livre de danos.

Isso é realizado pelo recurso de backup de máquina virtual em tempo real do Hyper-V, que facilita o backup com tempo de inatividade zero para máquinas virtuais em tempo real. Para obter mais informações, visite [https://technet.microsoft.com/en-us/library/dn531031\(v=ws.12\).aspx](https://technet.microsoft.com/en-us/library/dn531031(v=ws.12).aspx).

No entanto, o recurso de backup em tempo real do Hyper-V ainda não é totalmente suportado pela Microsoft para qualquer versão das máquinas virtuais do FreeBSD em execução no Hyper-V, que inclui VMs Hyper-V dos produtos KACE SMA, uma vez que eles são baseados em FreeBSD. Para obter mais informações, visite [https://technet.microsoft.com/library/dn848318\(ws.12\).aspx](https://technet.microsoft.com/library/dn848318(ws.12).aspx).

Se configurado corretamente, quando um backup é realizado a partir de uma VM que não tem suporte para o backup em tempo real, o servidor Hyper-V torna a VM off-line (colocada no estado de salva) durante o processo de backup e, em seguida, restaura a VM para o seu Estado anterior após o processo de backup ser concluído. Enquanto a VM está off-line, resultando em tempo de inatividade para a VM, o backup deve ser concluído sem prejudicar o conteúdo da VM. Para obter mais informações, visite <https://technet.microsoft.com/en-us/library/dn798286.aspx>.

Como a Microsoft não oferece suporte para backups em tempo real do sistema operacional FreeBSD no qual as soluções KACE são executadas, é importante realizar as configurações adequadas em Serviços de integração das VMs KACE SMA no Hyper-V que impedem que o Hyper-V tente realizar backups em tempo real da VM. Quando as configurações de Serviços de integração não foram adequadamente configuradas, resultaram em danos nos arquivos dentro do KACE SMA do cliente, o que faz com que ele não funcione corretamente, resultando na necessidade de entrar em contato com o Suporte Técnico para corrigir o problema.

Como a Microsoft define automaticamente todas as novas VMs do Hyper-V para terem o Serviço de integração de Backup habilitado, se você criou uma VM do Hyper-V para o KACE SMA, siga as instruções abaixo para configurar corretamente este serviço para FreeBSD e evitar que os arquivos do banco de dados sejam corrompidos.

É recomendável desativar o recurso de backup em tempo real nas VMs do KACE SMA no Hyper-V.

Para desabilitar o Serviço de integração de Backup, na caixa de diálogo Configurações da VM, em Gerenciamento > Serviço de integração, desmarque a caixa de seleção Backup (ponto de verificação de volume) e clique em Aplicar. Essa configuração pode ter um nome diferente, como Backup (cópia de sombra de volume), dependendo da versão do Windows do servidor Hyper-V.



Para alterar essa configuração, primeiramente você deve desligar a VM.



Após a configuração de Backup ser desabilitada, se o Windows falhar em tornar a VM off-line (alterando o estado da VM para salva) durante o processo de backup, e os danos ao MySQL na solução KACE continuarem ocorrendo durante o backup da VM, coloque a VM no estado desligar ou salva antes de realizar um backup da VM.

Para obter mais informações sobre esse problema, acesse <https://support.quest.com/kace-systems-management-appliance/kb/195580>.

## Configuração de NIC virtual

O comportamento irregular da rede, incluindo baixo desempenho, desconexões do agente, paralisação da interface e indisponibilidade total da rede, é observado com uma Solução de implantação de sistemas KACE (SDA) sendo executada no Hyper-V.

Por padrão, duas configurações de rede problemáticas são ativadas no Hyper-V para todas as máquinas virtuais (VMs) de convidado. Essas configurações são Endereço MAC dinâmico e VMQ (fila de máquina virtual).

Quando configurado com um endereço MAC dinâmico, o Hyper-V pode atribuir aleatoriamente um novo endereço MAC para a VM do convidado. Como as soluções KACE são executadas no FreeBSD, o sistema operacional deve ser reiniciado para detectar a alteração na interface de rede.

VMQ é uma tecnologia de filtragem de pacotes no Hyper-V que reduz a sobrecarga no roteamento de pacotes com hardware suportado e sistemas operacionais convidados. No entanto, não é suportado pelo NIC virtual Intel E1000 usado pelas soluções KACE, o que pode resultar em um baixo desempenho da rede. Alguns adaptadores físicos Broadcom também são conhecidos por terem problemas de desempenho com VMQ.

Para resolver este problema, recomenda-se desabilitar o endereço MAC dinâmico (escolhendo MAC estático) e o VMQ, em todas as soluções KACE virtuais hospedadas em Hyper-V.

Para desabilitar o endereço MAC dinâmico, na caixa de diálogo Configurações da VM, em Adaptador de rede > Recursos avançados, selecione a caixa de seleção Estático e especifique um endereço MAC único válido para o ambiente. Em seguida, clique em Aplicar.



Geralmente, pode ser deixado como o endereço MAC atual, que já foi atribuído dinamicamente.



Para mudar de um endereço MAC dinâmico para um endereço MAC estático, e ao contrário, primeiramente é preciso desligar a VM.

Para desabilitar o VMQ, na caixa de diálogo Configurações da VM, em Adaptador de rede > Aceleração de hardware, desmarque a caixa de seleção Habilitar fila de máquina virtual e clique em Aplicar.

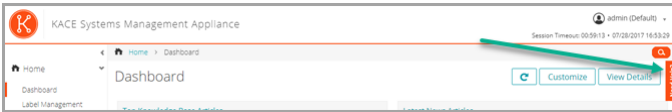


Embora essa configuração possa ser realizada sem desligar a VM, é recomendado realizar essa alteração com a VM off-line.

Para obter mais informações sobre esse problema, acesse <https://support.quest.com/kace-systems-management-appliance/kb/153445>.

## 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>

# Configuración del dispositivo

En esta guía se explica cómo configurar el dispositivo virtual de administración de sistemas (SMA) KACE en los sistemas host Microsoft® Hyper-V®. 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.



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 DMZ (zona desmilitarizada) o en una subred filtrada. Una DMZ agrega una capa adicional de seguridad a una LAN (red de área local).
5. Configure los servicios de integración de copia de seguridad de los dispositivos virtuales que se ejecutan en Hyper-V. Para obtener más información, consulte [Configuración de los servicios de integración de las copias de seguridad](#).



Si no se configuran correctamente los servicios de integración de copia de seguridad, se pueden dañar los archivos de la base de datos MySQL.

## Importe el SMA virtual de KACE a un servidor de Microsoft Hyper-V y configure los ajustes

El administrador Hyper-V es la herramienta integrada de administración de máquinas virtuales que utiliza para importar su SMA virtual de KACE.

- No configure la máquina virtual con el Adaptador de red heredado.
  - En Administrador de Hyper-V, mantenga los ajustes predeterminados para habilitar Servicio de sincronización de hora de Hyper-V.
1. Para descargar el SMA virtual de KACE, dirijase 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 paquete VHD comprimido en su sistema de host Hyper-V.
  3. Extraiga y verifique la integridad de los archivos.
  4. En el administrador Hyper-V, haga clic con el botón derecho en el host y, luego, haga clic en Importar máquina virtual.

Aparecerá la ventana Importar máquina virtual.

5. Navegue hasta la ubicación del paquete VHD extraído.
6. En Ajustes, seleccione Copiar la máquina virtual (crear un nuevo Id. único) y Duplicar todos los archivos para que la misma máquina virtual se pueda importar nuevamente.
7. Haga clic en Importar.

El SMA virtual de KACE aparece en la lista de Máquinas virtuales.

8. Edite los ajustes de la máquina virtual para conectar el adaptador de red virtual al conmutador virtual de su host Hyper-V.
9. Elija una dirección MAC estática para la máquina virtual:



Quest recomienda el uso de una dirección MAC estática, porque Hyper-V podría asignar aleatoriamente una nueva dirección MAC a la máquina virtual, si se utiliza una dirección MAC dinámica. Puesto que el SMA de KACE funciona con FreeBSD®, el sistema operativo invitado debe reiniciarse para detectar el cambio a la interfaz de red y esto puede causar un comportamiento errático de la red.

- a. Vaya a la sección Características avanzadas de los ajustes de Adaptador de red de la máquina virtual.
  - b. Seleccione Estática en Dirección MAC.
  - c. Especifique una dirección MAC única válida para su entorno. Normalmente, puede utilizar la dirección MAC actual.
  - d. Haga clic en Aplicar.
10. Deshabilite la cola de máquina virtual (VMQ) de la máquina virtual:



La VMQ es una tecnología de filtrado de paquetes en Hyper-V, diseñada para reducir la sobrecarga de enrutamiento de paquetes con sistemas operativos de invitados y de hardware compatibles. Sin embargo, no es compatible con el controlador de interfaz de red (NIC) virtual Intel® e1000 utilizado por el SMA

de KACE y esto puede causar un rendimiento deficiente de la red. Algunos adaptadores físicos son conocidos por tener problemas de rendimiento con la VMQ. Por lo tanto, Quest recomienda deshabilitar VMQ.

- a. Vaya a la sección Aceleración del hardware de los ajustes de Adaptador de red de la máquina virtual.
- b. Desactive la casilla de verificación junto a Habilitar cola de máquina virtual.
- c. Haga clic en Aplicar.

Encienda el dispositivo.

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

Cuando 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
Clave de licencia	La clave de licencia que recibió en el correo electrónico de bienvenida de Quest. Si no cuenta con una clave de licencia, comuníquese con Soporte de software de Quest en <a href="https://support.quest.com/contact-support">https://support.quest.com/contact-support</a> .
Nombre de la compañía	El nombre de su compañía o grupo.
Correo electrónico del administrador	La dirección de correo electrónico en la que desea recibir las comunicaciones de Quest.
Contraseña	<p>La contraseña para la cuenta de administrador predeterminada, que es la cuenta que utiliza para iniciar sesión en la Consola del administrador del dispositivo. La cuenta de administrador predeterminada 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> 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 administrador en todos los dispositivos. Esto le permitirá vincular los dispositivos posteriormente. Para obtener más información, consulte la Guía para el administrador del dispositivo: <a href="#">Acceso a la Guía para el administrador y la ayuda en línea</a>.</p>
Autenticación de dos factores	Si desea proporcionar una mayor seguridad para los usuarios que inician sesión en el dispositivo, establezca este valor como Habilitado. 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 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.

- | Opción | Descripción   |
|--------|---|
|        | <p> 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.</p>  |
| 7.     | <p>Siga las instrucciones en pantalla para completar la configuración inicial.</p> <p>Cuando finaliza la configuración inicial, el dispositivo se reinicia y aparece la página de inicio de sesión de Consola del administrador.</p> <p> Si modificó la dirección IP del dispositivo, vaya a la nueva dirección para visualizar la página de inicio de sesión.</p>   |
| 8.     | <p>Inicie sesión en Consola del administrador con la ID de inicio de sesión admin y la contraseña que eligió en la configuración inicial.</p> <p>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.</p>   |
| 9.     | <p>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.</p> <p>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.</p> <p>Aparece la Consola del administrador y el dispositivo está listo para usarse.</p> |
|        | <p> Cuando inicie sesión en el SMA virtual de KACE, asegúrese de que la opción Sincronizar de forma automática con un servidor horario de Internet se encuentre desactivada en los Ajustes de fecha y hora, a los que se puede acceder a través de Ajustes &gt; Panel de control.</p>  |

## 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
Nombre de host DNS de SMA de KACE	<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>
Generar automáticamente el nombre del servidor	<p>Seleccione esta casilla para permitir que el sistema genere el nombre de servidor web de SMA de KACE con este formato: Nombre de host.Dominio. Por ejemplo: &lt;unique_KACE_SMA_appliance_name&gt;.example.com. Desactive esta casilla para introducir un nombre de servidor web personalizado.</p>
Nombre del servidor web de SMA de KACE	<p>Escriba el nombre completo del dominio del dispositivo. Este es el Nombre de host junto con el Dominio. 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.
DHCP	(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.
Configuración manual de IPv4	<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> <p> La dirección IPv4 es obligatoria, sin importar si hay una dirección IPv6 disponible. La dirección IPv6 es opcional.</p>
SLAAC	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.
Configuración manual de IPv6	<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> <p> La dirección IPv6 es opcional. La dirección IPv4 es obligatoria, sin importar si hay una dirección IPv6 disponible.</p>
Deshabilitar IPv6	Seleccione esta opción si desea deshabilitar una dirección IPv6 para el dispositivo. Esta es la configuración predeterminada.

Opción	Descripción
Servidor SMTP	(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.
SSH habilitado	(Opcional) Seleccione esta opción para habilitar el acceso SSH (seguro) a la Consola del administrador del dispositivo. Quest recomienda que habilite SSH durante la configuración inicial. Cuando la instalación haya finalizado, puede cambiar la configuración en la Consola del administrador según sea necesario.

Proxy De manera opcional, puede escribir información sobre el servidor proxy.



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.

- Use la tecla de flecha abajo para mover el cursor hasta Guardar y luego presione Ingresar o Regresar.

Se reinicia el dispositivo.

- En cualquier equipo conectado a su LAN, abra un navegador y vaya a la URL de la Consola del administrador del dispositivo. Por ejemplo, `http://<unique_KACE_SMA_appliance_name>.local/admin`.

Aparece la página Acuerdo de transacción de software.

- Acepte el acuerdo.

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
Clave de licencia	La clave de licencia que recibió en el correo electrónico de bienvenida de Quest. Si no cuenta con una clave de licencia, comuníquese con Soporte de software de Quest en <a href="https://support.quest.com/contact-support">https://support.quest.com/contact-support</a> .
Nombre de la compañía	El nombre de su compañía o grupo.
Correo electrónico del administrador	La dirección de correo electrónico en la que desea recibir las comunicaciones de Quest.
Contraseña	<p>La contraseña para la cuenta de administrador predeterminada, que es la cuenta que utiliza para iniciar sesión en la Consola del administrador del dispositivo. La cuenta de administrador predeterminada 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: 1px solid black; 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 administrador en todos los dispositivos. Esto le permitirá vincular los dispositivos posteriormente. Para obtener más información, consulte la Guía para el administrador del dispositivo: <a href="#">Acceso a la Guía para el administrador y la ayuda en línea</a>.</p> </div>
Autenticación de dos factores	Si desea proporcionar una mayor seguridad para los usuarios que inician sesión en el dispositivo, establezca este valor como Habilitado. 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.

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 modificó 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.

# Configuración de los servicios de integración de las copias de seguridad

La configuración adecuada de los servicios de integración de las copias de seguridad en máquinas virtuales con KACE Systems Management Appliance (SMA) que se ejecutan en Hyper-V evita el daño de archivos en la base de datos MySQL.

La máquina virtual con KACE que se ejecuta en Hyper-V está configurada de forma inadecuada para las copias de seguridad de la máquinas virtuales (VM), lo que puede causar que algunos archivos de la base de datos MySQL se dañen dentro del dispositivo y provoquen que el dispositivo quede inutilizable hasta que soporte técnico se comunique para solucionar el problema. La solución es restaurar la base de datos desde la copia de seguridad de la base de datos más reciente y sin archivos dañados.

Esto es provocado por la función de copias de seguridad de máquinas virtuales en vivo de Hyper-V, que no implica ningún tiempo de inactividad para las máquinas virtuales en vivo. Para obtener más información, visite [https://technet.microsoft.com/en-us/library/dn531031\(v=ws.12\).aspx](https://technet.microsoft.com/en-us/library/dn531031(v=ws.12).aspx).

Sin embargo, Microsoft aún no es compatible con la función de copias de seguridad en vivo de Hyper-V para cualquier versión de máquinas virtuales FreeBSD que se ejecutan en Hyper-V, que incluye máquinas virtuales con Hyper-V de los productos SMA de KACE, ya que se basan en FreeBSD. Para obtener más información, visite [https://technet.microsoft.com/library/dn848318\(ws.12\).aspx](https://technet.microsoft.com/library/dn848318(ws.12).aspx).

Si se configura de forma correcta, cuando una copia de seguridad se saca de una máquina virtual que no es compatible con copias de seguridad en vivo, el servidor Hyper-V cierra la sesión de la máquina virtual (puesta en el estado de guardado) durante el proceso de copias de seguridad, y luego restaura la máquina virtual a su estado anterior después de finalizar dicho proceso. Durante el cierre de sesión de la máquina virtual, que genera un tiempo de inactividad para esta, la copia de seguridad se debe completar sin afectar de manera negativa el contenido de la máquina virtual. Para obtener más información, visite <https://technet.microsoft.com/en-us/library/dn798286.aspx>.

Ya que Microsoft no es compatible con las copias de seguridad del sistema operativo FreeBSD que se ejecutan en los dispositivos KACE, es importante configurar los ajustes correctos de los servicios de integración de las máquinas virtuales de SMA de KACE con Hyper-V que evitan que Hyper-V intente realizar copias de seguridad en vivo de las máquinas virtuales. Cuando los ajustes de los servicios de integración de las máquinas virtuales no están configurados correctamente, algunos archivos de los clientes se dañan dentro de SMA de KACE, lo que provoca su mal funcionamiento. Para corregir el problema debe comunicarse con soporte técnico.

Ya que Microsoft configura automáticamente que todas las máquinas virtuales Hyper-V nuevas tengan el servicio de integración de copias de seguridad habilitado de forma predeterminada, si creó una máquina virtual con Hyper-V para SMA de KACE, siga las instrucciones que se encuentran a continuación a fin de configurar correctamente este servicio para FreeBSD y evitar que se dañen los archivos de la base de datos mencionada anteriormente.

Se recomienda deshabilitar la función de copias de seguridad en vivo en las máquinas virtuales con Hyper-V de SMA de KACE.

Para deshabilitar el servicio de integración de copias de seguridad, en el cuadro de diálogo Ajustes de la máquina virtual, en Administración > Servicios de integración, deshabilite la casilla de verificación Copias de seguridad (punto de control del volumen) y haga clic en Aplicar.



Es posible que en este ajuste haya un nombre diferente, como Copias de seguridad (copia instantánea del volumen), según la versión de Windows del servidor de Hyper-V.



Para cambiar este ajuste, primero debe apagar la máquina virtual.



Después de que se deshabilita el ajuste Copias de seguridad, si Windows no puede cerrar la sesión de la máquina virtual primero (cambio del estado de la máquina virtual a guardado) durante el proceso de respaldo, y el daño de MySQL en el dispositivo KACE sigue ocurriendo durante el respaldo de la máquina virtual, cambie el estado de la máquina virtual a apagado o guardado antes de realizar un respaldo de la máquina virtual.

Para obtener información adicional sobre este problema, visite <https://support.quest.com/kace-systems-management-appliance/kb/195580>.

## Configuración de NIC virtual

El comportamiento errático de la red, que incluye un rendimiento deficiente, desconexiones del agente, bloqueo de la interfaz e indisponibilidad completa de la red, se observa con un dispositivo virtual de implementación de sistemas (SDA) KACE que se ejecutan en Hyper-V.

De forma predeterminada, se habilitan dos ajustes de red problemáticos en Hyper-V para todas las máquinas virtuales (VM) de los invitados. Estos ajustes son dirección MAC dinámica y VMQ (cola de máquina virtual).

Cuando se configura con una dirección MAC dinámica, Hyper-V puede asignar una nueva dirección MAC al azar a la máquina virtual del invitado. Ya que los dispositivos KACE se ejecutan en FreeBSD, el SO se debe reiniciar para detectar el cambio en la interfaz de red.

La VMQ es una tecnología de filtrado de paquetes en Hyper-V que reduce la sobrecarga de enrutamiento de paquetes con sistemas operativos de invitados y de hardware compatibles. Sin embargo, esta tecnología no es compatible con el controlador de interfaz de red (NIC) virtual Intel E1000 que se utiliza en dispositivos KACE, lo que puede generar un rendimiento deficiente de la red. Se sabe que algunos adaptadores físicos Broadcom tienen problemas de rendimiento con la VMQ.

Para solucionar este problema, se recomienda deshabilitar la dirección MAC dinámica (seleccionando una MAC estática) y VMQ en todos los dispositivos virtuales KACE alojados en Hyper-V.

Para deshabilitar la dirección MAC dinámica, en el cuadro de diálogo de Ajustes de la máquina virtual, en Adaptador de red > Características avanzadas, seleccione la casilla de verificación Estática y especifique una dirección MAC única y válida para su entorno. Luego, haga clic en Aplicar.



Por lo general, esto se deja como la dirección MAC actual, que ya se asignó de forma dinámica.



Para cambiar una dirección MAC dinámica a una estática y viceversa, primero debe apagar la máquina virtual.

Para deshabilitar VMQ, en el cuadro de diálogo de Ajustes de la máquina virtual, en Adaptador de red > Aceleración del hardware, deshabilite la casilla de verificación Habilitar cola de máquina virtual y haga clic en Aplicar.

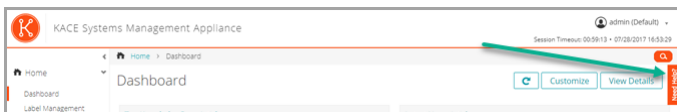


Aunque se puede cambiar este ajuste sin apagar la máquina virtual, se recomienda cambiarlo cuando se cierre la sesión de la máquina virtual.

Para obtener información adicional sobre este problema, visite <https://support.quest.com/kace-systems-management-appliance/kb/153445>.

## 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>

# Legal notices

---

© 2020 Quest Software Inc. ALL RIGHTS RESERVED.

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

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

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (<https://www.quest.com>) for regional and international office information.

## 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 Hyper-V Platforms

Updated - September 2020

Software Version - 11.0