KACE® as a Service 7.1

Setup Guide

Table of Contents

Legal notices

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Trademarks

Legend

	A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
	A WARNING icon indicates a potential for property damage, personal injury, or death.
	An information icon indicates supporting information.

Updated - February 2017

Software Version - 7.1

Setting up the appliance

This guide explains how to get started with the hosted version of KACE as a Service, which runs within the Dell Cloud. In this guide you will find requirements, feature descriptions, and instructions for using the hosted appliance. For information about setting up other versions of the KACE Systems Management Appliance, and for additional documentation, see https://documents.quest.com.

Before you begin

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

1. Purchase a license for K1 as a Service from Quest sales at https://www.quest.com/company/contact-us.aspx. After you purchase a license, Quest sends you onboarding details, including a static IP address for the appliance, in a Welcome email. Have this email available when you begin.

   > Some K1 as a Service features require a VPN connection. To add a VPN connection to your purchase at any time, contact Quest sales at https://www.quest.com/company/contact-us.aspx.

2. In the A record of your internal DNS (domain name system) server, enter the appliance's hostname. 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 you should change it during initial setup.
3. Ensure that your network and firewall settings allow outbound access to K1 as a Service on the following ports. These ports should also be open on devices, including desktops and servers, that will have the K1000 Agent software installed:
   - 80: Used for appliance web-based consoles and Agent communications over HTTP
   - 443: Used for appliance web-based consoles and Agent communications over HTTPS
   - 52230: Used for communications between the appliance and Agents
4. Obtain a registered domain name for the K1 as a Service appliance. This is REQUIRED to generate an SSL certificate signing request from the appliance and use port 443 (HTTPS) for Agent communications. Quest reserves the right to turn off access to port 80 (HTTP) within 30 days. For more information, see https://support.quest.com/kb/114757.

K1 as a Service feature exceptions

All functionality of the K1000 Administrator Console can be configured to be used within the Dell Cloud. However, some features require direct access to your network, which is established using a site-to-site VPN connection. VPN connections leverage the shared K1 as a Service network, and a single VPN connection usually is sufficient to enable the functionality for a single company. In some cases, however, additional VPN connections might be necessary, and dedicated network

bandwidth might be required. For more information, see Using VPN connections and network resources.

Administrator Console features that require a VPN connection

The following Administrator Console features require a VPN connection:

- Server monitoring using Agentless device management.
- Wake On LAN.
- Network Discovery, including IP Scan, Active Directory® scan, and NMAP scan.
- K1000 Agent provisioning from the appliance. See Provisioning the K1000 Agent to managed devices.
- Importing and exporting resources (file sharing is blocked by the Dell Cloud firewall).
- FTP access to backup files (FTP access is blocked by the Dell Cloud firewall).
- Application packages and script dependencies must be uploaded using HTTP. Large package uploads could timeout on slower network connections. Packages larger than 2 GB must be distributed using an alternate download location from an internal file server.
- LDAP user and device labels.
- LDAP user authentication.
- LDAP user import.
- Active Directory single sign on for the Administrator Console and User Console.
- Email forwarding, used for Service Desk tickets and other email communications.

User Console feature exceptions

The User Console is the interface that makes software library and Service Desk features available to end users. The following User Console features are not supported in the cloud:

- Automatic software installations from the User Console (downloads are supported).
- The My Computer tab within the User Console.

Log in to the Administrator Console

Log in to the Appliance Administrator Console to begin using K1 as a Service.

Your browser setting determines the language displayed in the Administrator Console the first time you log in. For information about changing the language settings, go to the appliance Administrator Guide: Accessing the Administrator Guide and online Help.

1. Open a web browser and enter the Administrator Console URL you received in your Welcome email from Quest.

   The Software Transaction Agreement page appears.

2. Accept the agreement.

   The Initial Setup wizard appears.

3. Verify that you have the information required to configure the appliance, then click Next.
4. 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. Include the dashes. If you do not have a license key, contact Quest Software Support at https://support.quest.com/contact-support.
Company Name	The name of your company or group.
Administrator Email	The email address where you want to receive communications from Quest.
Password	The password for the default admin account, which is the account you use to log in to the appliance Administrator Console. The default admin account is the only account on the appliance at this time. If you forget the password for this account, the system might have to be reset to factory defaults which can result in loss of data. If you have multiple K1000 or K2000 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, go to the appliance Administrator Guide: Accessing the Administrator Guide and online Help.

5. Follow the onscreen 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.

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

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

Configure network settings

Your appliance is configured with a static IP address, subnet mask, and gateway. These settings cannot be changed. However, you must change the appliance hostname and web server name to match your DNS settings, and you can configure additional network settings to match your requirements.

1. In the Administrator Console, go to the appliance Control Panel:
   - If the Organization component is not enabled on the appliance, click Settings.
   - If the Organization component is enabled on the appliance, select System in the drop-down list in the top-right corner of the page, then click Settings.
2. Click Network Settings.

   The Network Settings page appears.
3. Configure the following network settings.

Option	Description
DNS Hostname	Enter the hostname of the appliance. The default is your static IP address.
Web Server	Enter the fully-qualified domain name of the appliance. This is the Hostname concatenated with Domain. For example: kbox.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. The default is your static IP address.
IP Address	The email address where you want to receive communications from Quest.
Static IP Address	Enter the static IP address of the appliance.
Domain	Enter the domain that the appliance is on. For example, example.com.

Option	Description
Subnet Mask	Enter the subnet (network segment) that the appliance is on. The default is 255.255.255.0.
Default Gateway	Enter the network gateway for the appliance.
Primary DNS	Enter the IP address of the primary DNS server the appliance uses to resolve hostnames. The default is 8.8.8.8.
Secondary DNS	(Optional) Enter the IP address of the secondary DNS server the appliance uses to resolve hostnames. The default is 4.2.2.2.
Proxy Configuration	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.
Email Configuration	To enable the appliance to send and receive email, select Enabled, then specify the following settings: • SMTP Server: Specify the host name or IP address of an SMTP server, such as smtp.gmail.com. This enables email notifications. The SMTP server must allow anonymous (nonauthenticated) 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. • Port: Enter the port number to use for the SMTP server. For standard SMTP, use port 25. For secure SMTP, use port 587. • Login: Enter the username for an account that has SMTP server access, such as <your_account_name>@gmail.com. • Password: Enter the password of the specified server account.

Option	Description
	• Enable Service Desk POP3 Server: Select the check box to use POP3 email for Service Desk ticket email. After POP3 is enabled, you can specify the POP3 server settings on Service Desk Queue Detail pages.

4. Click Save.

   The appliance restarts.

Configure the SNMP community string

Change the SNMP community string to d35kt0pEn6. This enables Quest to proactively manage the virtual infrastructure of the appliance and correct issues with disk space and virtual processors as they arise.

1. In the Administrator Console, go to the appliance Control Panel:
   - If the Organization component is not enabled on the appliance, click Settings.
   - If the Organization component is enabled on the appliance, select System in the drop-down list in the top-right corner of the page, then click Settings.
2. In the upper section of the page, select Enable SNMP monitoring.
3. Specify the following SNMP Community String: d35kt0pEn6, then click Save.

Enable SSL

You must enable secure communications between the appliance and managed devices, and you can use the appliance Administrator Console to generate an SSL certificate.

Obtain a registered domain name to be used for the appliance. This is required to generate an SSL certificate signing request using the appliance Administrator Console.

1. In the Administrator Console, go to the appliance Control Panel:
   - If the Organization component is not enabled on the appliance, click Settings.
   - If the Organization component is enabled on the appliance: Select System in the drop-down list in the top-right corner of the page, then click Settings.
2. Click Security Settings.

   The Security Settings page appears.
3. In the SSL section toward the bottom of the page, select Enable SSL.
4. Click Generate SSL Certificate.

5. Provide the configuration information, then click Save.
6. Copy all of the certificate request text, including the lines "-----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST-----" and everything in between, then send it to the person who provides your company with web server certificates. Your Private Key appears in the Private Key field. It is deployed to the appliance when you upload a valid certificate and later click Deploy.
7. Click Create Self-Signed Cert.

   The SSL certificate is generated. Self-signed certificates are converted to PEM files, named kbox.pem, and they are placed in K1000 Agent data folders.

   If you create a self-signed certificate, you need to deploy that certificate to all Agent-managed devices.
8. Click Deploy to deploy the certificate and enable SSL on the appliance.
9. Click OK to restart the appliance.

Best practices

Follow the guidelines and recommendations in this section when using K1 as a Service.

Using VPN connections and network resources

If you are using the traditional Agent-server communication between the K1 as a Service appliance and your managed devices, installing the Agent on managed devices is all that is required for communication. However, if you are using a VPN connection, it is your responsibility to complete the network handshake from your environment to K1 as a Service. The K1 as a Service team can provide recommendations, such as the appropriate IP addresses and ports to allow, and it is essential to have your network administrator involved in the setup process. Dell configures the appropriate connections for the Dell side, and you need to ensure connection from your side to complete the setup successfully.

In addition, some K1 as a Service features require a VPN connection to be used in the cloud, and a single VPN connection is usually sufficient for a single company. For example, you can use a single VPN connection even if you have remote locations provided that those locations can route traffic through the main corporate site where the VPN connection exists. All K1000 Agent traffic is routed through the VPN and then to the appliance through the VPN connection. If remote locations cannot see the main corporate site, or if you want each site to have a direct VPN link to the appliance, you need to purchase a VPN connection for each site. For more information about features that require VPN connections, see K1 as a Service feature exceptions.

Pricing for K1 as a Service is based upon shared network bandwidth. To purchase additional network resources, or to purchase VPN connections, contact Quest sales at https://www.quest.com/company/contact-us.aspx.

Using VPN connections with multiple domains

K1 as a Service is designed to be used with a single domain and a single VPN connection. If you have multiple domains, you can manage devices (inventory) on other domains using the appliance, but features that require VPN access are available only to a single domain. For example, you can authenticate to a single Active Directory environment for Identity Access Management, but you cannot authenticate to more than one domain. Agent traffic from the domain with the VPN connection is routed through the VPN connection, whereas Agent traffic for other domains connects to the appliance using standard Internet access. For more information about features that require VPN connections, see K1 as a Service feature exceptions.

About the appliance IP address

K1 as a Service is configured for a single IP address. The IP address is assigned by Quest and that address cannot be changed. You must create a Host (A) record in your internal DNS (domain name system) server for the appliance's static IP address, and you can create multiple A (host) records across multiple networks or domains to point to your appliance. If you need to use more than one public IP address for your network, you must purchase a separate instance of K1 as a Service. Multiple instances of K1 as a Service cannot share any data or database information. For more information, contact Quest sales at https://www.quest.com/company/contact-us.aspx.

About network settings

By default, all network protocols and their associated services are disabled except for AMP (Agent Messaging Protocol, used by the K1000 Agent), HTTPS, and HTTP. These protocols are used for the appliance user interfaces and K1000 Agent communications. When the K1000 Agent software is provisioned to a device, the Agent first uses port 52230 to establish the AMP connection. For all other traffic, the Agent always attempts to connect to the appliance using HTTPS over port 443 for encrypted communications if SSL is enabled. Otherwise, the Agent uses HTTP over port 80.

Provisioning the K1000 Agent to managed devices

The K1000 Agent is an application that can be installed on devices to enable device management and inventory reporting through the K1 as a Service appliance. To provision the Agent software to devices directly from the appliance, you must have a VPN connection. However, there are alternative methods for deploying Agent software without VPN connectivity:

- Manually download and install the Agent on devices: You can download the K1000 Agent and include it in the gold image used to image new devices. For more information, see: https://support.quest.com/kb/112151 .

- Install the Agent using Windows Group Policy (GPO). For more information, go to https://support.quest.com/kb/133776.
- Install the Agent using another management system: If the Quest solution is replacing another systems management solution, you can deploy the Agent using the distribution methods of the system being replaced prior to its decommission and cleanup.

Configuring K1000 Agent communication settings

Agents installed on managed devices periodically communicate with the appliance to report inventory, update scripts, and perform other tasks. You can configure the Agent settings, including the interval at which the Agents check in, messages displayed to users, and log retention time. If you have multiple organizations, you can configure Agent settings for each organization separately. For more information, see the K1000 Administrator Guide: Accessing the Administrator Guide and online Help.

About server monitoring

Version 6.3 of K1 as a Service introduces server monitoring, which provides basic performance and application monitoring for servers in inventory. You can enable monitoring for servers using the K1000 Agent, and for servers using Agentless management, and setup depends upon your IT department policies. Server monitoring is available for up to five servers using a standard K1 as a Service license, and you can obtain a license to increase that number.

If you enable monitoring for Agent-managed servers, alert information is transmitted over port 443 in addition to the existing Agent communication protocol. If you enable monitoring for servers using Agentless management, the appliance uses SSH or Telnet to connect to the server, read the logs, check for alerts, and display the alerts in the K1000 Administrator Console. Because VPN access is required for the use of SSH and Telnet, a VPN connection is required for Agentless server monitoring.

About file distribution (packages) and Replication Shares

With K1 as a Service, every site is a remote site. Quest strongly recommends that you configure Replication Shares for each site to optimize bandwidth usage on the remote office Internet connections. Replication Shares are devices that keep copies of files for distribution, such as Managed Installations, patches, scripts, and Dell Updates.

With Samba file sharing turned off, file uploads to the appliance are limited to 2 GB. For files that exceed 2 GB, use an alternate download location to stage the files inside the corporate network.

An alternate download location can be any network location that has all the files required to install a particular application. You can distribute packages from alternate download locations including a UNC address or DFS source. The CIFS and SMB protocols, Samba servers, and file server

appliances are supported. You specify the location when you create a Managed Installation. For more information, see the Distribution section of the K1000 Administrator Guide: Accessing the Administrator Guide and online Help.

About bandwidth usage and dedicated network bandwidth

K1 as a Service uses a shared cloud network. To reduce the bandwidth requirements of the shared network, Dell strongly recommends the use of Replication Shares. If your appliance causes bandwidth issues on the shared network, you might be required to set up Replication Shares or purchase dedicated network bandwidth. For more information, contact Quest sales at https://quest.com/company/contact-us.aspx.

About data protection and security

The Dell Cloud Data Centers and Quest appliances have a Highly Available infrastructure and provide all the necessary protection and security for your appliance. For more information about appliance security settings, see the configuration section of the K1000 Administrator Guide: Accessing the Administrator Guide and online Help.

Using backup files

Backup files are used to restore your K1 as a Service appliance in the event of a data loss, or to preserve settings during upgrades, and Quest automatically makes offboard copies of the most recent nightly backup file for disaster recovery.

You can access backup files using the Administrator Console. If the files become too large to download using HTTP, you can access them using FTP. See Back up the appliance and enable FTP access. If network bandwidth is limited, consider using file distribution to download large backup files. See About file distribution (packages) and Replication Shares.

Restoring any type of backup file destroys the data currently configured in the appliance server. Quest recommends that you offload any backup files or data that you want to keep before you restore settings.

Back up the appliance and enable FTP access

You can enable Quest to copy daily and monthly backup files to a local high-speed storage area by enabling FTP access and setting the FTP password to sepgetbxf as described in this section. FTP access requires a VPN connection.

1. In the Administrator Console, go to the appliance Control Panel:
    - If the Organization component is not enabled on the appliance, click Settings.

- If the Organization component is enabled on the appliance, select System in the drop-down list in the top-right corner of the page, then click Settings.

2. Click Security Settings.

   The Security Settings page appears.

3. In the top section, specify the following settings:

Option	Description
Enable backup via FTP	Select this check box to enable FTP access to backup files.
Make FTP writable	Select this check box to use FTP to upload backup files.
New FTP user password	Type the following password: sepgetbxf.

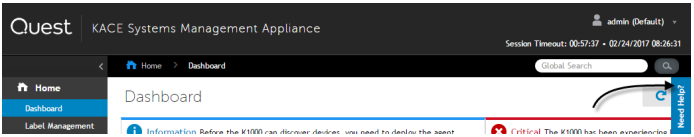
If the FTP user password is set, the backup server automatically copies daily and monthly backup files to a local high-speed storage area. For more information about managing backups, see the maintenance section of the K1000 Administrator Guide: Accessing the Administrator Guide and online Help.

Using K1000 GO

K1000 GO is an app that provides access to Service Desk tickets, inventory information, and application deployment features from smartphones and tablets. The app also enables users to submit Service Desk tickets, view the status of submitted tickets, and read Knowledge Base articles from their mobile devices. You can download K1000 GO from the Apple® App Store℠ for iOS devices, or from the Google® Play™ Store for Android™ devices. For more information, see the K1000 Administrator Guide: Accessing the Administrator Guide and online Help.

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.



About Dell Managed Services

If you are interested in a fully outsourced IT solution, Dell Managed Services is available to manage your appliance for you. For more information, contact Quest sales at https://www.dell.com/support/contents/ca/en/calca1/category/Contact-Information.

Scheduling training

To help you begin using the appliance, Quest provides a fixed number of online training sessions called JumpStart.

To understand the scope of your JumpStart purchase, review the JumpStart Datasheet at https://support.quest.com/kace-systems-management-appliance/training/152/kace-k1000-management-appliance-jumpstart-program.

To schedule training, email the Quest training team at mailto: KaceTraining@quest.com. Additional training sessions can be purchased separately as needed.

Knowledge Base articles

For additional information, go to the Quest Support Knowledge Base site, https://support.quest.com/systems-management-appliance/kb .

- Network ports required by the appliance: https://support.quest.com/kb/111775
- Whitelisting required for patching: https://support.quest.com/kb/111785
- Installing the K1000 Agent using Windows Group Policy: https://support.quest.com/kb/133776
- Working with backup files: https://support.quest.com/kb/111736

About us

We are more than just a name

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

Our brand, our vision. Together.

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

Contacting Quest

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

Technical support resources

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product.

Configuration de l'appliance

Ce guide explique comment utiliser la version hébergée de KACE en tant que service, exécutée dans le Cloud Dell. Vous y trouverez la configuration requise, les descriptions des fonctionnalités et des instructions concernant l'utilisation de l'appliance hébergée. Pour plus d'informations sur la configuration d'autres versions de l'appliance de gestion des systèmes KACE et pour obtenir de la documentation supplémentaire, rendez-vous sur https://documents.quest.com.

Avant de commencer

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

1. Achetez une licence K1 en tant que service auprès du service commercial Quest à l'adresse https://www.quest.com/company/contact-us.aspx. Une fois que vous avez acheté une licence, Quest vous envoie un e-mail de bienvenue contenant les détails d'intégration, notamment une adresse IP statique pour l'appliance. Assurez-vous d'avoir cet e-mail sous la main avant de commencer.

   certaines fonctionnalités de K1 en tant que service nécessitent une connexion VPN. Pour ajouter une connexion VPN à votre achat, contactez le service commercial Quest à l'adresse https://www.quest.com/company/contact-us.aspx.

2. 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 nous vous conseillons de le modifier au cours de la configuration initiale.
3. Assurez-vous que vos paramètres de réseau et de pare-feu autorisent un accès sortant vers K1 en tant que service sur les ports suivants. Ces ports doivent également être ouverts sur les périphériques, notamment les ordinateurs de bureau et les serveurs, sur lesquels le logiciel de l'agent K1000 sera installé :
   - 80 : utilisé pour les communications entre les consoles basées sur le Web de l'appliance et l'agent via HTTP
   - 443 : utilisé pour les communications entre les consoles basées sur le Web de l'appliance et l'agent via HTTPS
   - 52230 : utilisé pour les communications entre l'appliance et les agents
4. Obtenez un nom de domaine enregistré pour l'appliance K1 en tant que service. Cette étape est OBLIGATOIRE si vous souhaitez générer une requête de signature de certificat SSL et utiliser le port 443 (HTTPS) pour les communications avec l'agent. Quest se réserve le droit de désactiver l'accès au port 80 (HTTP) dans les 30 jours. Pour plus d'informations, voir https://support.quest.com/kb/114757.

Exceptions concernant les fonctionnalités de K1 en tant que service

Vous pouvez configurer toutes les fonctionnalités de la Console d'administration de l'appliance K1000 afin de les utiliser dans le Cloud Dell. Cependant, certaines fonctionnalités nécessitent un accès direct à votre réseau, établi via une connexion VPN de site à site. Les connexions VPN exploitent le réseau K1 en tant que service partagé et une seule connexion VPN suffit généralement à activer la fonctionnalité pour une seule entreprise. Toutefois, dans certains cas, des connexions VPN supplémentaires, ainsi que de la bande passante réseau dédiée, peuvent être nécessaires. Pour plus d'informations, voir Utilisation de connexions VPN et de ressources réseau.

Fonctionnalités de la Console d'administration qui nécessitent une connexion VPN

Les fonctionnalités suivantes de la Console d'administration nécessitent une connexion VPN :

- Surveillance des serveurs à l'aide de la gestion des périphériques sans agent.
- Wake-on-LAN.
- Découverte du réseau, notamment l'analyse IP, l'analyse Active Directory® et l'analyse NMAP.
- Provisioning de l'agent K1000 à partir de l'appliance. voir .
- Importation et exportation de ressources (le partage de fichiers est bloqué par le pare-feu du Cloud Dell).
- Accès FTP aux fichiers de sauvegarde (l'accès FTP est bloqué par le pare-feu du Cloud Dell).
- Les packages d'application et dépendances de script doivent être téléchargés via HTTP. Les téléchargements de packages volumineux peuvent expirer lorsque la connexion réseau est lente. Les packages de plus de 2 Go doivent être distribués via un autre emplacement de téléchargement à partir d'un serveur de fichiers interne.
- Étiquettes pour le périphérique et l'utilisateur LDAP.
- Authentification de l'utilisateur LDAP.
- Importation de l'utilisateur LDAP.

- Authentification unique Active Directory pour la Console utilisateur et la Console d'administration.
- Transfert d'e-mails, utilisé pour les tickets du Service Desk et d'autres communications par e-mail.

Exceptions concernant les fonctionnalités de la console utilisateur

La Console utilisateur est l'interface qui met les fonctionnalités de la Bibliothèque de logiciels et du Service Desk à la disposition des utilisateurs finaux. Les fonctions suivantes de la Console utilisateur ne sont pas prises en charge dans le Cloud :

- Installations automatiques de logiciels à partir de la Console utilisateur (les téléchargements sont pris en charge).
- L'onglet Mon ordinateur de la Console utilisateur.

Connexion à la Console d'administration

Connectez-vous à la Console d'administration de l'appliance à l'aide de K1 en tant que service.

Votre paramètre de navigateur détermine la langue affichée 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. Ouvrez un navigateur Web et saisissez l'URL de la Console d'administration que vous avez reçue dans votre e-mail de bienvenue de Quest.

   La page Contrat de transaction du logiciel apparaît.

2. Acceptez le contrat.

   L'assistant Installation initiale s'affiche.

3. Vérifiez que vous disposez de toutes les informations nécessaires pour configurer l'appliance, puis cliquez sur Suivant.
4. À la page Paramètres de licence et d'administrateur, fournissez les informations suivantes :

Option	Description
Clé de licence	Clé de licence que vous avez reçue dans le courrier électronique de bienvenue envoyé par Quest. N'oubliez pas d'inclure les tirets. Si vous ne disposez d'aucune clé de licence, contactez le Support Quest Software à l'adresse https://support.quest.com/fr-fr/contact-support.

Option	Description
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'appliance. Le compte admin par défaut est le seul compte défini sur l'appliance à ce stade. Si vous oubliez le mot de passe de ce compte, il vous faudra probablement rétablir les paramètres d'usine par défaut du système, ce qui peut entraîner une perte de données. Si vous disposez de plusieurs appliances K1000 ou K2000, Quest vous recommande d'utiliser un mot de passe identique pour le compte admin sur 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'appliance : Accès au Guide de l'administrateur et à l'aide en ligne.

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

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

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

6. 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.

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

Configuration des paramètres réseau

Votre appliance est configurée avec une adresse IP statique, un masque de sous-réseau et une passerelle. Vous ne pouvez pas modifier ces paramètres. Cependant, vous devez modifier le nom d'hôte de l'appliance et le nom du serveur Web afin qu'ils correspondent à vos paramètres DNS et vous pouvez configurer des paramètres réseau supplémentaires en fonction de vos besoins.

1. Dans la Console d'administration, accédez au Panneau de configuration de l'appliance :

- Si le composant Organisation n'est pas activé sur votre appliance, cliquez sur Paramètres.
- Si le composant Organisation est activé sur l'appliance, sélectionnez Système dans la liste déroulante située en haut à droite de la page, puis cliquez sur Paramètres.

2. Cliquez sur Paramètres du réseau.

   La page Paramètres du réseau s'affiche.

3. Configurez les paramètres réseau ci-dessous.

Option	Description
Nom d'hôte DNS	Entrez le nom d'hôte de l'appliance. Par défaut, il s'agit de votre adresse IP statique.
Serveur Web	Saisissez le nom de domaine complet de l'appliance. Il s'agit du Nom d'hôte concaténé avec le Domaine. Exemple : kbox.exemple.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. Par défaut, il s'agit de votre adresse IP statique.
Adresse IP	Adresse e-mail à laquelle vous souhaitez recevoir les communications de Quest.
Adresse IP statique	Entrez l'adresse IP statique de l'appliance.
Domaine	Indiquez le domaine auquel appartient l'appliance. Par exemple, exemple.com.
Masque de sous-réseau	Spécifiez le sous-réseau (segment du réseau) auquel appartient l'appliance. La valeur proposée par défaut est 255.255.255.0.
Passerelle par défaut	Indiquez la passerelle réseau de l'appliance.
DNS principal	Entrez l'adresse IP du serveur DNS principal que l'appliance utilise pour résoudre les noms d'hôte. La valeur proposée par défaut est 8.8.8.8.
DNS secondaire	(Facultatif) Spécifiez l'adresse IP ou le serveur DNS secondaire utilisé par l'appliance pour

Option	Description
	résoudre les noms d'hôte. La valeur proposée par défaut est 4.2.2.2.
Configuration 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.
Configuration des e-mails	Pour permettre à l'appliance d'envoyer et de recevoir des e-mails, sélectionnez Activé(s), puis spécifiez les paramètres suivants : • Serveur SMTP : Spécifiez le nom d'hôte ou l'adresse IP d'un serveur SMTP, comme smtp.gmail.com. Cela permet d'activer les notifications par e-mail. Le serveur SMTP doit 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 relais du courrier électronique de l'appliance sans authentification. • Port : Entrez le numéro de port à utiliser pour le serveur SMTP. Pour un serveur SMTP standard, utilisez le port 25. Pour un serveur SMTP sécurisé, utilisez le port 587. • ID de connexion : Saisissez le nom d'utilisateur d'un compte disposant de l'accès au serveur SMTP, comme <votre_nom_de_compte>@gmail.com. • Mot de passe : Saisissez le mot de passe du compte de serveur spécifié. • Activer le serveur POP3 du Service Desk : Cochez la case afin d'utiliser la messagerie POP3 pour l'envoi des tickets du Service Desk par e-mail. Une fois que le serveur POP3 est activé, vous pouvez spécifier les

Option	Description
	paramètres de celui-ci sur les pages Détails de la file d'attente du Service Desk.

4. Cliquez sur Enregistrer.

   L'appliance redémarre.

Configurer la chaîne de la communauté SNMP

Réglez la chaîne de la communauté SNMP sur d35kt0pEn6. Quest peut alors gérer de manière proactive l'infrastructure virtuelle de l'appliance et régler les problèmes liés à l'espace disque et aux processeurs virtuels dès qu'ils surviennent.

1. Dans la Console d'administration, accédez au Panneau de configuration de l'appliance :
   - Si le composant Organisation n'est pas activé sur votre appliance, cliquez sur Paramètres.
   - Si le composant Organisation est activé sur l'appliance, sélectionnez Système dans la liste déroulante située en haut à droite de la page, puis cliquez sur Paramètres.
2. Dans la section supérieure de la page, sélectionnez Activer la surveillance SNMP.
3. Spécifiez la chaîne de communauté SNMP d35kt0pEn6, puis cliquez sur Enregistrer.

Activer SSL

Vous devez activer les communications sécurisées entre l'appliance et les périphériques infogérés et vous pouvez utiliser la Console d'administration de l'appliance pour générer un certificat SSL.

Obtenez un nom de domaine enregistré à utiliser pour l'appliance. Cette étape est obligatoire si vous souhaitez générer une requête de signature de certificat SSL à l'aide de la Console d'administration de l'appliance.

1. Dans la Console d'administration, accédez au Panneau de configuration de l'appliance :
   - Si le composant Organisation n'est pas activé sur votre appliance, cliquez sur Paramètres.
   - Si le composant Organisation est activé sur l'appliance, procédez comme suit : Sélectionnez Système dans la liste déroulante située en haut à droite de la page, puis cliquez sur Paramètres.
2. Cliquez sur Paramètres de sécurité.

   La page Paramètres de sécurité apparaît.
3. Dans la section SSL au bas de la page, sélectionnez Activer SSL.

4. Cliquez sur Générer un certificat SSL.
5. Renseignez les informations de configuration, puis cliquez sur Enregistrer.
6. Copiez le texte de la demande, de la ligne "-----BEGIN CERTIFICATE REQUEST----- à la ligne -----END CERTIFICATE REQUEST-----" (incluses), puis envoyez-le à la personne chargée de fournir à votre entreprise des certificats de serveur Web. Votre clé privée s'affiche dans le champ Clé privée. Elle est déployée vers l'appliance dès que vous téléchargez un certificat valide et cliquez ensuite sur Déployer.
7. Cliquez sur Créer un certificat auto-signé.

   Le certificat SSL est généré. Les certificats autosignés sont convertis en fichiers PEM, intitulés kbox.pem, et ils sont placés dans des dossiers de données de l'agent K1000.

   Si vous créez un certificat autosigné, vous devez le déployer sur tous les périphériques gérés par l'agent.
8. Cliquez sur Déployer pour déployer le certificat et activer SSL sur l'appliance.
9. Cliquez sur OK pour redémarrer l'appliance.

Pratiques d'excellence

Suivez les consignes et les recommandations de cette section lors de l'utilisation de K1 en tant que service.

Utilisation de connexions VPN et de ressources réseau

Si vous utilisez une communication agent-serveur traditionnelle entre l'appliance K1 en tant que service et vos périphériques infogérés, il vous suffit d'installer l'agent sur les périphériques infogérés pour permettre la communication. Cependant, si vous utilisez une connexion VPN, vous devez établir la liaison réseau de votre environnement vers K1 en tant que service. L'équipe K1 en tant que service peut vous conseiller, notamment en termes d'adresses IP et de ports à autoriser, et il est important que votre administrateur réseau soit impliqué dans le processus de configuration. Dell configure les connexions adaptées côté Dell et vous devez vous charger de la connexion de votre côté pour assurer le bon déroulement de la configuration.

De plus, certaines fonctionnalités de K1 en tant que service nécessitent une connexion VPN dans le Cloud et une connexion VPN unique est généralement suffisante pour une seule entreprise. Par exemple, vous pouvez utiliser une seule connexion VPN même si vous avez des emplacements distants, à condition que ces emplacements puissent router le trafic via le site d'entreprise principal où se trouve la connexion VPN. L'ensemble du trafic de l'agent K1000 est routé via le VPN puis jusqu'à l'appliance par le biais de la connexion VPN. Si les emplacements distants ne parviennent pas à voir le site d'entreprise principal, ou si vous souhaitez que chaque site ait un lien VPN direct vers l'appliance, vous devez acheter une connexion VPN pour chaque site. Pour plus d'informations sur les fonctionnalités qui nécessitent des connexions VPN, voir Exceptions concernant les fonctionnalités de K1 en tant que service.

La tarification de K1 en tant que service est basée sur une bande passante réseau partagée. Pour acheter des ressources réseau supplémentaires, ou pour acheter

des connexions VPN, contactez le service commercial Quest à l'adresse https://www.quest.com/company/contact-us.aspx.

Utilisation de connexions VPN avec plusieurs domaines

K1 en tant que service a été conçu pour être utilisé avec un seul domaine et une seule connexion VPN. Si vous avez plusieurs domaines, vous pouvez gérer vos périphériques (inventaire) sur d'autres domaines via l'appliance, mais les fonctionnalités qui nécessitent un accès VPN ne sont accessibles qu'à un seul domaine. Par exemple, vous pouvez vous authentifier sur un environnement Active Directory pour Identity Access Management, mais vous ne pouvez pas vous authentifier sur plusieurs domaines. Le trafic de l'agent à partir du domaine avec la connexion VPN est routé via la connexion VPN, tandis que le trafic de l'agent pour les autres domaines se connecte à l'appliance via un accès Internet standard. Pour plus d'informations sur les fonctionnalités qui nécessitent des connexions VPN, voir Exceptions concernant les fonctionnalités de K1 en tant que service.

Utilisation de K1000 GO

K1000 GO est une application qui permet d'accéder aux tickets du Service Desk, aux informations d'inventaire et aux fonctionnalités de déploiement d'applications à partir d'un smartphone ou d'une tablette. L'application permet également aux utilisateurs d'envoyer des tickets au Service Desk, d'afficher l'état des tickets émis et de consulter les articles de la base de connaissances depuis leurs périphériques mobiles. Vous pouvez télécharger l'application K1000 GO à partir de l'App Store℠ d'Apple® pour les périphériques iOS ou à partir de la boutique Google® Play™ pour les périphériques Android™. Pour plus d'informations à ce sujet, consultez le Guide de l'administrateur du K1000 : Accès au Guide de l'administrateur et à l'aide en ligne.

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.

À propos de Dell Managed Services

Si vous êtes intéressé par une solution informatique entièrement externalisée, Dell Managed Services peut gérer votre appliance pour vous. Pour en savoir plus, contactez le service

commercial Quest à l'adresse https://www.dell.com/support/contents/ca/en/calca1/category/Contact-Information.

Programmation des formations

Afin de vous aider à commencer à utiliser l'appliance, Quest propose un nombre limité de sessions de formation sous la forme de l'offre JumpStart.

Pour bien comprendre le contenu des formations JumpStart, consultez la fiche récapitulative JumpStart disponible à l'adresse https://support.quest.com/kace-systems-management-appliance/training/152/kace-k1000-management-appliance-jumpstart-program.

Pour programmer une formation, envoyez un courrier électronique à l'équipe chargée des formations Quest à l'adresse mailto: KaceTraining@quest.com. Des sessions de formation supplémentaires peuvent être achetées séparément selon vos besoins.

Articles de la base de connaissances

Pour plus d'informations, rendez-vous sur le site de la base de connaissances du support Quest, https://support.quest.com/systems-management-appliance/kb .

- Ports réseau requis par l'appliance : https://support.quest.com/kb/111775
- Liste blanche nécessaire à l'application de correctifs : https://support.quest.com/kb/111785
- Installation de l'agent K1000 à l'aide de la stratégie de groupe Windows : https://support.quest.com/fr-fr/kb/133776
- Utilisation des fichiers de sauvegarde : https://support.quest.com/kb/111736

Qui nous sommes

Nous avons bien plus à offrir qu'un nom

Nous voulons que vos technologies de l'information en fassent plus pour vous. Pour cette raison, nous développons des solutions logicielles communautaires allégeant vos tâches d'administration, afin que vous puissiez vous consacrer davantage aux innovations de votre entreprise. Nous pouvons vous aider à moderniser votre centre de données et à accélérer votre migration vers le cloud, tout en vous fournissant l'expertise, la sécurité et l'accessibilité dont vous avez besoin pour développer vos activités basées sur l'exploitation de données. En ajoutant à cela la volonté de Quest que la communauté internationale rejoigne ses initiatives innovantes, ainsi que l'engagement de notre entreprise en matière de satisfaction client, nous continuons de proposer des solutions qui changent la vie de nos utilisateurs et laissent derrière elles un héritage dont nous pouvons être fiers. Nous changeons la donne en devenant une toute nouvelle entreprise de développement de logiciels. En tant que partenaire, nous travaillons sans relâche pour nous assurer que vos technologies de l'information sont créées à votre image et avec votre participation. Tel est notre défi, et nous le relèverons ensemble. Rejoignez-nous dans notre nouvelle quête. Rejoignez l'innovation.

Notre marque, notre vision. Ensemble.

Notre logo illustre nos valeurs : innovation, communauté et soutien. À elle seule, la lettre Q raconte une grande partie de notre histoire. Il s'agit d'un cercle parfait, qui témoigne de notre engagement envers les performances et la précision technologiques. Le creux de la lettre symbolise l'élément sans lequel notre communauté et le nouveau visage de Quest ne sauraient être complets. Et la pièce manquante du puzzle n'est autre que vous.

Contacter Quest

Pour des questions commerciales ou d'autres demandes, rendez-vous sur www.quest.com/company/contact-us.aspx ou appelez le + 1-949-754-8000.

Ressources du support technique

Ce portail propose des outils d'auto-dépannage qui vous permettront de résoudre des problèmes rapidement et sans aide extérieure, 24 h/24 et 365 j/an. Le portail du support technique vous permet de :

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

Einrichten der Appliance

In diesem Handbuch werden die ersten Schritte mit der gehosteten Version von KACE als Service, die innerhalb der Dell Cloud ausgeführt wird, beschrieben. In diesem Handbuch finden Sie Anforderungen, Beschreibungen und Anleitungen für die Verwendung der gehosteten Appliance. Weitere Informationen zum Einrichten von anderen Versionen der KACE Systemverwaltungs-Appliance sowie zusätzliche Dokumentation finden Sie unter https://documents.quest.com.

Vorbereitung

Vor dem Einrichten der Appliance müssen Sie einige Vorbereitungen treffen.

1. Erwerben Sie eine Lizenz für K1 als Service bei Quest Sales über https://www.quest.com/company/contact-us.aspx. Nachdem Sie eine Lizenz erworben haben, sendet Quest Ihnen in einer E-Mail die Onboarding-Details, einschließlich einer statischen IP-Adresse für die Appliance. Halten Sie diese E-Mail bereit, wenn Sie beginnen.

   Einige Funktionen von K1 als Service erfordern eine VPN-Verbindung. Um zusätzlich eine VPN-Verbindung zu erwerben, können Sie sich jederzeit an Quest Sales unter https://www.quest.com/company/contact-us.aspx wenden.

2. Geben Sie im A-Datensatz Ihres internen DNS-Servers (Domain Name System) den Hostnamen der Appliance ein. Der A-Datensatz definiert den Hostnamen für den MX-Datensatz. Dadurch können Benutzer E-Mail-Tickets an den Service Desk senden. Der voreingestellte Hostname des Geräts ist k1000. Sie können ihn jedoch während der Ersteinrichtung ändern.
3. Stellen Sie sicher, dass Ihre Netzwerk- und Firewall-Einstellungen den ausgehenden Zugriff auf K1 als Service an den folgenden Ports ermöglichen. Diese Ports sollten auch auf Geräten, einschließlich Desktops und Servern, offen sein, auf denen die K1000 Agenten-Software installiert werden soll:
   - 80: Wird für die webbasierten Konsolen der Appliance und die Agentenkommunikation über HTTP verwendet.
   - 443: Wird für die webbasierten Konsolen der Appliance und die Agentenkommunikation über HTTPS verwendet.
   - 52230: Wird für die Kommunikation zwischen der Appliance und den Agenten verwendet.
4. Beschaffen Sie sich einen eingetragenen Domainnamen für die K1 als Service Appliance. Dies ist ERFORDERLICH, um eine Signieranforderung für das SSL-Zertifikat von der Appliance aus zu erstellen und Port 443 (HTTPS) für die Agentenkommunikation zu verwenden. Quest behält sich das Recht vor, innerhalb von 30 Tagen den Zugriff auf Port 80 (HTTP) zu deaktivieren. Weitere Informationen hierzu finden Sie unter https://support.quest.com/kb/114757.

Funktionsausnahmen K1 als Service

Sämtliche Funktionalität der K1000 Administratorkonsole kann für die Verwendung innerhalb der Dell Cloud konfiguriert werden. Einige Funktionen erfordern jedoch den direkten Zugriff auf Ihr Netzwerk, der über eine VPN-Verbindung von Standort zu Standort hergestellt wird. VPN-Verbindungen nutzen das gemeinsame K1 als Service Netzwerk – eine einzelne VPN-Verbindung reicht hierbei für gewöhnlich aus, um die Funktionalität für ein einzelnes Unternehmen zu aktivieren. In einigen Fällen sind jedoch möglicherweise zusätzliche VPN-Verbindungen sowie dedizierte Netzwerkbandbreite erforderlich. Weitere Informationen hierzu finden Sie unter Verwenden von VPN-Verbindungen und Netzwerkressourcen.

Administratorkonsole-Funktionen, die eine VPN-Verbindung erfordern

Die folgenden Funktionen der Administratorkonsole erfordern eine VPN-Verbindung:

- Serverüberwachung mithilfe der Geräteverwaltung ohne Agenten-Software
- Wake-On-LAN
- Netzwerkerkennung einschließlich IP-, Active Directory®- und NMAP-Scan
- K1000 Agenten-Provisionierung von der Appliance Siehe Provisionierung des K1000 Agenten auf verwalteten Geräten.
- Importieren und Exportieren von Ressourcen (Dateifreigabe wird von der Dell Cloud-Firewall blockiert)
- FTP-Berechtigung für Sicherungsdateien (FTP-Zugang wird von der Dell Cloud-Firewall blockiert)
- Anwendungspakete und Skriptabhängigkeiten müssen über HTTP hochgeladen werden. Große Pakete können bei langsamen Netzwerkanschlüssen ein Timeout verursachen. Pakete von mehr als 2 GB müssen über eine alternative Download-Quelle von einem internen Dateiserver verteilt werden.
- LDAP-Benutzer- und -Gerätelabel
- LDAP-Benutzerauthentifizierung
- LDAP-Benutzerimport
- Einmalige Active Directory-Anmeldung für die Benutzerkonsole und Administratorkonsole
- E-Mail-Weiterleitung, die für Service Desk Tickets und andere E-Mail-Kommunikationen verwendet wird

Funktionsausnahmen der Benutzerkonsole

Die Benutzerkonsole ist die Schnittstelle, die Funktionen der Softwarebibliothek und des Service Desk für Enduser verfügbar macht. Die folgenden Funktionen der Benutzerkonsole werden in der Cloud nicht unterstützt:

- Automatische Softwareinstallationen über die Benutzerkonsole (Downloads werden unterstützt)
- Die Registerkarte Arbeitsplatz in der Benutzerkonsole

Anmelden bei der Administratorkonsole

Melden Sie sich bei der Administratorkonsole der Appliance an, um K1 als Service zu verwenden.

> Die Sprache, in der Ihnen die Administratorkonsole bei Ihrer ersten Anmeldung angezeigt wird, ist durch Ihre Browsereinstellungen festgelegt. Informationen zum Ändern der Spracheinstellungen finden Sie im Administratorhandbuch der Appliance: Zugriff auf das Administratorhandbuch und die Onlinehilfe.

1. Öffnen Sie einen Webbrowser und geben Sie die URL der Administratorkonsole an, die Sie in der Begrüßungs-E-Mail von Quest erhalten haben.

   Die Seite Softwareübertragungsvereinbarung wird angezeigt.

2. Stimmen Sie der Vereinbarung zu.

   Der Assistent für die Ersteinrichtung wird angezeigt.

3. Stellen Sie sicher, dass Sie über die erforderlichen Informationen für die Konfiguration der Appliance verfügen und klicken Sie dann auf Weiter.
4. 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 (mit Bindestrichen). Wenn Sie keinen Lizenzschlüssel besitzen, wenden Sie sich an den https://support.quest.com/de-de/contact-support unter Quest Softwaresupport.
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

Option	Beschreibung
	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. Wenn Sie über mehrere K1000 oder K2000 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.

5. Befolgen Sie die Anweisungen auf dem Bildschirm, um 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.

6. 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.

Die Administratorkonsole wird angezeigt und die Appliance kann verwendet werden.

Konfigurieren der Netzwerkeinstellungen

Ihre Appliance ist mit einer statischen IP-Adresse, einer Subnetzmaske und einem Gateway konfiguriert. Diese Einstellungen können nicht geändert werden. Sie müssen allerdings den Hostnamen und den Webservernamen der Appliance an Ihre DNS-Einstellungen anpassen und können zusätzliche Netzwerkeinstellungen entsprechend Ihren Anforderungen konfigurieren.

1. Navigieren Sie in der Administratorkonsole zur Systemsteuerung der Appliance:
   - Wenn die Organisationskomponente auf der Appliance nicht aktiviert ist, klicken Sie auf Einstellungen.
   - Wenn in der Appliance die Organisationskomponente aktiviert ist, wählen Sie rechts oben auf der Seite aus der Dropdown-Liste die Option System aus und klicken dann auf die Registerkarte Einstellungen.
2. Klicken Sie auf Netzwerkeinstellungen.

Die Seite Netzwerkeinstellungen wird angezeigt.

3. Konfigurieren Sie die folgenden Netzwerkeinstellungen.

Option	Beschreibung
DNS-Hostname	Geben Sie den Hostnamen der Appliance ein. Die Standardeinstellung ist Ihre statische IP-Adresse.
Webserver	Geben Sie den vollständigen Domainnamen der Appliance ein. Hierbei handelt es sich um den mit der Domain verknüpften Hostnamen. Beispiel: kbox.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. Die Standardeinstellung ist Ihre statische IP-Adresse.
IP-Adresse	Die E-Mail-Adresse, an die Sie Kommunikation von Quest erhalten möchten.
Statische IP-Adresse	Geben Sie die statische IP-Adresse der Appliance ein.
Domain	Geben Sie die Domain ein, in der sich die Appliance befindet. Zum Beispiel beispiel.com.
Subnetzmaske	Geben Sie die Subnetzmaske (Netzwerksegment) der Appliance ein. Der Standardwert lautet 255.255.255.0.
Standard-Gateway	Geben Sie das Netzwerk-Gateway für die Appliance ein.
Primärer DNS	Geben Sie die IP-Adresse des primären DNS-Servers ein, den die Appliance zur Auflösung von Hostnamen verwendet. Der Standardwert lautet 8,8.8,8.
Sekundärer DNS	(Optional) Geben Sie die IP-Adresse des sekundären DNS-Servers ein, den die Appliance zur Auflösung von Hostnamen verwendet. Der Standardwert lautet 4,2.2,2.

Option	Beschreibung
Proxy-Konfiguration	Die Appliance unterstützt Proxy-Server mit bereichsbasierter Standardauthentifizierung, für die Benutzernamen und Kennwörter erforderlich sind. Verwendet Ihr Proxy-Server eine andere Authentifizierungsmethode, fügen Sie die IP-Adresse der Appliance zur Ausnahmeliste des Servers hinzu.
E-Mail-Konfiguration	Damit die Appliance E-Mails senden und empfangen kann, wählen Sie Aktiviert aus und legen dann die folgenden Einstellungen fest: • SMTP-Server: Geben Sie den Hostnamen oder die IP-Adresse eines SMTP-Servers an, beispielsweise smtp.gmail.com. Dadurch werden E-Mail-Benachrichtigungen aktiviert. Der SMTP-Server muss 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. • Port: Geben Sie die Nummer des für den SMTP-Server zu verwendenden Ports ein. Für Standard-SMTP verwenden Sie Port 25. Für sicheres SMTP verwenden Sie Port 587. • Anmeldename: Geben Sie den Benutzernamen für ein Konto ein, das über SMTP-Serverzugriff verfügt. Beispiel: <Ihr_Kontoname>@gmail.com. • Kennwort: Geben Sie das Kennwort für das angegebene Serverkonto ein. • Service Desk-POP3-Server aktivieren: Aktivieren Sie das Kontrollkästchen, um POP3-E-Mail für Service Desk-Ticket-E-Mails zu verwenden. Nach der

Option	Beschreibung
	Aktivierung von POP3 können Sie die Einstellungen des POP3-Servers auf den Seiten Warteschlangen-Detail des Service Desks angeben.

4. Klicken Sie auf Speichern.

   Die Appliance wird neu gestartet.

Konfigurieren der SNMP-Communityzeichenfolge

Ändern Sie die SNMP-Communityzeichenfolge in d35KT0pEn6. Das ermöglicht Quest das proaktive Management der virtuellen Infrastruktur der Appliance und die sofortige Korrektur von Problemen mit Speicherplatz und virtuellen Prozessoren.

1. Navigieren Sie in der Administratorkonsole zur Systemsteuerung der Appliance:
   - Wenn die Organisationskomponente auf der Appliance nicht aktiviert ist, klicken Sie auf Einstellungen.
   - Wenn in der Appliance die Organisationskomponente aktiviert ist, wählen Sie rechts oben auf der Seite aus der Dropdown-Liste die Option System aus und klicken dann auf die Registerkarte Einstellungen.
2. Wählen Sie im oberen Bereich der Seite SNMP-Überwachung aktivieren aus.
3. Geben Sie die folgende SNMP-Communityzeichenfolge an: D35KT0pEn6 und klicken Sie dann auf Speichern.

Aktivieren von SSL

Sie müssen die sichere Kommunikation zwischen der Appliance und verwalteten Geräten aktivieren. Mit der Administratorkonsole der Appliance können Sie ein SSL-Zertifikat generieren.

Beschaffen Sie sich einen eingetragenen Domainnamen, der für die Appliance verwendet werden soll. Dies ist erforderlich, um eine Signieranforderung für das SSL-Zertifikat mit der Administratorkonsole der Appliance generieren zu können.

1. Navigieren Sie in der Administratorkonsole zur Systemsteuerung der Appliance:
   - Wenn die Organisationskomponente auf der Appliance nicht aktiviert ist, klicken Sie auf Einstellungen.
   - Wenn die Organisationskomponente auf der Appliance aktiviert ist: Wählen Sie rechts oben auf der Seite aus der Dropdown-Liste die Option System aus und klicken Sie dann auf Einstellungen.

2. Klicken Sie auf Sicherheitseinstellungen.

   Die Seite Sicherheitseinstellungen wird angezeigt.
3. Wählen Sie im Abschnitt "SSL" unten auf der Seite Aktivieren von SSL aus.
4. Klicken Sie auf SSL-Zertifikat generieren.
5. Geben Sie die Konfigurationsinformationen an und klicken Sie dann auf Speichern.
6. Kopieren Sie den gesamten Zertifikatanfragetext, einschließlich der Zeilen "-----BEGIN CERTIFICATE REQUEST----- und -----END CERTIFICATE REQUEST-----" sowie des gesamten Texts zwischen diesen Zeilen. Senden Sie diesen Text an die Person, die für Ihre Firma Webserverzertifikate bereitstellt. Ihr privater Schlüssel wird im Feld Privater Schlüssel angezeigt. Er wird in der Appliance bereitgestellt, sobald Sie ein gültiges Zertifikat hochgeladen und dann auf Bereitstellen geklickt haben.
7. Klicken Sie auf Selbstsigniertes Zertifikat erstellen.

   Das SSL-Zertifikat wird erzeugt. Selbstsignierte Zertifikate werden zu PEM-Dateien konvertiert, als kbox.pem benannt und im Datenordner des K1000 Agenten gespeichert.

   Wenn Sie ein selbstsigniertes Zertifikat erstellen, müssen Sie es auf allen vom Agenten verwalteten Geräten bereitstellen.
8. Klicken Sie auf Bereitstellen, um das Zertifikat bereitzustellen und SSL in der Appliance zu aktivieren.
9. Klicken Sie auf OK, um die Appliance neu zu starten.

Best Practices

Befolgen Sie die Richtlinien und Empfehlungen in diesem Abschnitt bei der Verwendung von K1 als Service.

Verwenden von VPN-Verbindungen und Netzwerkressourcen

Wenn Sie eine herkömmliche Agenten-Server-Kommunikation zwischen der K1 als Service Appliance und Ihren verwalteten Geräten verwenden, ist für die Kommunikation lediglich die Installation des Agenten auf den verwalteten Geräten erforderlich. Wenn Sie jedoch eine VPN-Verbindung verwenden, unterliegt es Ihrer Verantwortung, den Netzwerk-Handshake zwischen Ihrer Umgebung und K1 als Service zu konfigurieren. Beim K1 als Service Team erhalten Sie Empfehlungen, wie z. B. zu den zuzulassenden IP-Adressen und Ports. Das Mitwirken des Netzwerkadministrators beim Setup-Vorgang ist hierbei unverzichtbar. Dell konfiguriert die entsprechenden Verbindungen auf Dell Seite. Sie müssen wiederum die Verbindung auf Ihrer Seite konfigurieren, um die Einrichtung erfolgreich abzuschließen.

Darüber hinaus erfordern einige K1 als Service Funktionen die Verwendung einer VPN-Verbindung in der Cloud. Hierbei reicht für gewöhnlich eine VPN-Verbindung für ein einzelnes Unternehmen. Sie können beispielsweise eine einzige VPN-Verbindung verwenden, selbst wenn Sie über Remote-Standorte verfügen – vorausgesetzt, dass diese Standorte Datenverkehr über den Hauptunternehmensstandort umleiten können, an dem die VPN-Verbindung vorhanden ist.

Sämtlicher K1000 Agentenverkehr wird über das VPN und daraufhin über die VPN-Verbindung an die Appliance geleitet. Wenn die Remote-Standorte den Hauptunternehmensstandort nicht erkennen können oder wenn Sie es bevorzugen, dass jeder Standort über eine direkte VPN-Verbindung zur Appliance verfügt, müssen Sie für jeden Standort eine VPN-Verbindung erwerben. Informationen zu den Funktionen, die eine VPN-Verbindung erfordern, finden Sie unter Funktionsausnahmen K1 als Service.

Die Preisgestaltung für K1 als Service basiert auf der gemeinsamen Netzwerkbandbreite. Um weitere Netzwerkressourcen oder VPN-Verbindungen zu erwerben, wenden Sie sich unter https://www.quest.com/company/contact-us.aspx an Quest Sales.

Verwenden von VPN-Verbindungen mit mehreren Domains

K1 als Service wurde für die Verwendung mit einer einzelnen Domain und einer einzelnen VPN-Verbindung entwickelt. Wenn Sie über mehrere Domains verfügen, können Sie Geräte (Inventar) in anderen Domains zwar mithilfe der Appliance verwalten, jedoch sind Funktionen, die einen VPN-Zugriff erfordern, nur für eine einzige Domain verfügbar. Sie können sich beispielsweise für die Identitätszugriffsverwaltung bei einer Active Directory-Umgebung authentifizieren, jedoch nicht bei mehr als einer Domain. Der Agentenverkehr von der Domain mit der VPN-Verbindung wird über die VPN-Verbindung geleitet, während der Agentenverkehr für andere Domains über den standardmäßigen Internetzugriff eine Verbindung mit der Appliance herstellt. Informationen zu den Funktionen, die eine VPN-Verbindung erfordern, finden Sie unter Funktionsausnahmen K1 als Service.

Informationen zur IP-Adresse der Appliance

K1 als Service ist für eine einzelne IP-Adresse konfiguriert. Die IP-Adresse wird von Quest zugewiesen und kann nicht geändert werden. Sie müssen einen Host-Datensatz (A) in Ihrem internen DNS (Domain Name System) für die statische IP-Adresse der Appliance erstellen und können dann verschiedene A-Datensätze (für Hosts) über mehrere Netzwerke und Domains hinweg erstellen, um Ihre Appliance zuzuweisen. Wenn Sie mehr als eine öffentliche IP-Adresse für Ihr Netzwerk benötigen, müssen Sie eine separate Instanz von K1 als Service erwerben. Mehrere Instanzen von K1 als Service können nicht über gemeinsame Daten oder Datenbankinformationen verfügen. Wenden Sie sich für weitere Informationen unter https://www.quest.com/company/contact-us.aspx an Quest Sales.

Informationen zu Netzwerkeinstellungen

Standardmäßig sind alle Netzwerkprotokolle und ihre zugeordneten Dienste deaktiviert. Hiervon ausgenommen sind AMP (Agenten-Messaging-Protokoll, das vom K1000 Agenten verwenden wird), HTTPS und HTTP. Diese Protokolle werden für die Benutzeroberflächen der Appliance und die K1000 Agentenkommunikationen verwendet. Wenn die K1000 Agenten-Software auf einem Gerät bereitgestellt wird, verwendet der Agent zunächst Port 52230, um eine AMP-Verbindung herzustellen. Bei jeglichem anderen Datenverkehr versucht der Agent zunächst, über HTTPS

und Port 443 eine verschlüsselte Verbindung zur Appliance herzustellen, sofern SSL aktiviert ist. Andernfalls verwendet der Agent HTTP über Port 80.

Provisionierung des K1000 Agenten auf verwalteten Geräten

Der K1000 Agent ist eine Anwendung, die auf Geräten installiert werden kann, um die Geräteverwaltung und Inventarberichte über die K1 als Service Appliance zu ermöglichen. Um die Agenten-Software direkt von der Appliance auf Geräten bereitzustellen, müssen Sie über eine VPN-Verbindung verfügen. Es gibt jedoch alternative Methoden zur Bereitstellung der Agenten-Software ohne VPN-Verbindung:

- Manuelles Herunterladen und Installieren des Agenten auf Geräten: Sie können den K1000 Agenten herunterladen und in dem Gold Image integrieren, das für die Abbildung neuer Geräte verwendet wird. Weitere Informationen finden Sie unter: https://support.quest.com/kb/112151 .
- Installieren des Agenten mithilfe einer Windows Gruppenrichtlinie (GPO) Weitere Informationen hierzu finden Sie unter https://support.quest.com/de-de/kb/133776.
- Installieren des Agenten mithilfe eines anderen Verwaltungssystems: Wenn die Quest Lösung eine andere Systemverwaltungslösung ersetzen soll, können Sie den Agenten mithilfe der Verteilungsmethoden des zu ersetzenden Systems bereitstellen, bevor Sie dieses entfernen und das System bereinigen.

Konfigurieren der Kommunikationseinstellungen für den K1000 Agenten

Agenten, die auf verwalteten Geräten installiert sind, kommunizieren regelmäßig mit der Appliance, um Inventarinformationen zu melden, Skripte zu aktualisieren und andere Aufgaben auszuführen. Sie können die Agenteneinstellungen einschließlich des Anmeldeintervalls der Agenten, der Meldungen für Benutzer sowie der Dauer der Aufbewahrung des Protokolls konfigurieren. Wenn Sie mehrere Organisationen haben, können Sie die Agenten-Einstellungen für jede Organisation individuell anpassen. Weitere Informationen finden Sie im K1000-Administratorhandbuch: Zugriff auf das Administratorhandbuch und die Onlinehilfe.

Informationen zur Serverüberwachung

Version 6.3 von K1 als Service führt die Serverüberwachung ein, die eine grundlegende Leistungs- und Anwendungsüberwachung für Server im Inventar bietet. Sie können die Überwachung für Server, die den K1000 Agenten verwenden, sowie für Server mit Verwaltung ohne Agenten-Software aktivieren. Die Einrichtung hängt von den Richtlinien Ihrer IT-Abteilung ab. Die Serverüberwachung ist unter Verwendung einer K1 als Service Standardlizenz für bis zu fünf Server verfügbar. Sie können eine zusätzliche Lizenz erwerben, um diese Anzahl zu erhöhen.

Wenn Sie die Überwachung für mithilfe von Agenten verwaltete Server aktivieren, werden Warnungsinformationen zusätzlich zum vorhandenen Agentenkommunikationsprotokoll über Port 443 übertragen. Wenn Sie die Überwachung für Server mit Verwaltung ohne Agenten-Software aktivieren, verwendet die Appliance SSH oder Telnet, um eine Verbindung zum Server herzustellen, die Protokolle zu lesen, nach Warnungen zu suchen und die Warnungen in der K1000 Administratorkonsole anzuzeigen. Da für die Verwendung von SSH und Telnet ein VPN-Zugang erforderlich ist, wird für die Serverüberwachung ohne Agenten-Software eine VPN-Verbindung benötigt.

Informationen zur Dateiverteilung (Pakete) und zu Replikationsfreigaben

Mit K1 als Service ist jeder Standort ein Remote-Standort. Quest empfiehlt dringend, die Replikationsfreigaben für jeden Standort zu konfigurieren, um die Bandbreitennutzung der Internetverbindungen des Remote-Standorts zu optimieren. Replikationsfreigaben sind Geräte, die Kopien von Dateien für die Verteilung aufbewahren, wie z. B. verwaltete Installationen, Patches, Skripte und Dell Aktualisierungen.

Wenn die Samba Dateifreigabe deaktiviert ist, wird die Größe von Uploads zur Appliance auf 2 GB beschränkt. Verwenden Sie für Dateien von mehr als 2 GB eine alternative Download-Quelle, um die Dateien innerhalb des Unternehmensnetzwerks bereitzustellen.

Eine alternative Download-Quelle kann jeder beliebige Netzwerkspeicherort sein, an dem sich alle erforderlichen Dateien zur Installation einer bestimmten Anwendung befinden. Sie können Pakete von alternativen Download-Quellen bereitstellen, beispielsweise von einer UNC-Adresse oder einer DFS-Quelle. Die CIFS- und SMB-Protokolle, Samba-Server und Dateiserver-Appliances werden unterstützt. Sie müssen den Speicherort angeben, wenn Sie eine verwaltete Installation erstellen. Weitere Informationen finden Sie im K1000-Administratorhandbuch im Abschnitt zur Verteilung: Zugriff auf das Administratorhandbuch und die Onlinehilfe.

Informationen zur Bandbreitennutzung und dedizierten Netzwerkbandbreite

K1 als Service verwendet ein gemeinsames Cloudnetzwerk. Um die Bandbreitenanforderungen des gemeinsamen Netzwerks zu reduzieren, empfiehlt Dell dringend die Verwendung von Replikationsfreigaben. Wenn Ihre Appliance Bandbreitenprobleme im gemeinsamen Netzwerk verursacht, müssen Sie möglicherweise Replikationsfreigaben einrichten oder dedizierte Netzwerkbandbreite erwerben. Wenden Sie sich für weitere Informationen unter https://quest.com/company/contact-us.aspx an Quest Sales.

Informationen zur Datensicherheit

Die Dell Cloud Rechenzentren und Quest Appliances verfügen über eine hoch verfügbare Infrastruktur und bieten den erforderlichen Schutz für Ihre Appliance. Weitere Informationen zu den Sicherheitseinstellungen der Appliance finden Sie im Konfigurationsabschnitt im K1000-Administratorhandbuch: Zugriff auf das Administratorhandbuch und die Onlinehilfe.

Verwenden von Sicherungsdateien

Sicherungsdateien werden verwendet, um Ihre K1 als Service Appliance im Falle eines Datenverlusts wiederherzustellen oder um Einstellungen während Upgrades zu bewahren. Quest erstellt zum Zwecke der Notfallwiederherstellung automatisch externe Kopien der letzten Sicherungsdatei.

Sie können über die Administratorkonsole auf Sicherungsdateien zugreifen. Werden die Dateien zu groß für einen HTTP-Download, können Sie über FTP darauf zugreifen. Siehe Sichern der Appliance und Aktivieren des FTP-Zugriffs. Wenn die Netzwerkbandbreite beschränkt ist, sollten Sie in Betracht ziehen, größere Sicherungsdateien mithilfe der Dateiverteilung herunterzuladen. Siehe Informationen zur Dateiverteilung (Pakete) und zu Replikationsfreigaben.

Durch das Wiederherstellen jeglicher Sicherungsdateien werden die aktuell auf dem Appliance-Server gespeicherten Daten gelöscht. Quest empfiehlt, zunächst eine externe Sicherung aller Sicherungsdateien oder Daten durchzuführen, die Sie aufbewahren möchten, bevor Sie die Einstellungen wiederherstellen.

Sichern der Appliance und Aktivieren des FTP-Zugriffs

Sie können einstellen, dass Quest tägliche und monatliche Sicherungsdateien in einen lokalen High-Speed-Speicherbereich kopiert, indem Sie den FTP-Zugriff aktivieren und das FTP-Kennwort wie in diesem Abschnitt beschrieben auf sepgetbxf festlegen. Der FTP-Zugriff erfordert eine VPN-Verbindung.

1. Navigieren Sie in der Administratorkonsole zur Systemsteuerung der Appliance:
   - Wenn die Organisationskomponente auf der Appliance nicht aktiviert ist, klicken Sie auf Einstellungen.
   - Wenn in der Appliance die Organisationskomponente aktiviert ist, wählen Sie rechts oben auf der Seite aus der Dropdown-Liste die Option System aus und klicken dann auf die Registerkarte Einstellungen.
2. Klicken Sie auf Sicherheitseinstellungen.

   Die Seite Sicherheitseinstellungen wird angezeigt.
3. Geben Sie im oberen Abschnitt folgende Einstellungen an:

Option	Beschreibung
Sicherung über FTP aktivieren	Aktivieren Sie dieses Kontrollkästchen, um den FTP-Zugriff auf Sicherungsdateien zu aktivieren.

Option	Beschreibung
Schreibschutz für FTP aufheben	Aktivieren Sie dieses Kontrollkästchen, um FTP für das Hochladen von Sicherungsdateien zu verwenden.
Neues FTP-Benutzerkennwort	Geben Sie folgendes Kennwort ein: sepgetbxf.

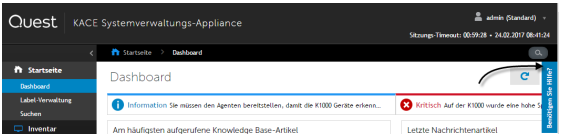
Wenn das FTP-Benutzerkennwort festgelegt wurde, kopiert der Sicherungsserver automatisch tägliche und monatliche Sicherungsdateien in einen lokalen High-Speed-Speicherbereich. Weitere Informationen zur Verwaltung von Sicherheitskopien finden Sie im Serviceabschnitt im K1000-Administratorhandbuch: Zugriff auf das Administratorhandbuch und die Onlinehilfe.

Verwenden von K1000 GO

K1000 GO ist eine App, die über Smartphones oder Tablets Zugriff auf Service Desk-Tickets, Inventarinformationen sowie Funktionen für die Anwendungsbereitstellung bietet. Mit der App können Benutzer auf ihrem Mobilgerät auch Service Desk-Tickets senden, den Status von gesendeten Tickets anzeigen und Knowledge Base-Artikel lesen. Sie können K1000 GO für iOS Geräte aus dem Apple® App Store℠ oder für Android™ Geräte aus dem Google® Play™ Store herunterladen. Weitere Informationen finden Sie im K1000-Administratorhandbuch: Zugriff auf das Administratorhandbuch und die Onlinehilfe.

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.



Informationen zu Dell Managed Services

Wenn Sie an einer vollständig ausgelagerten IT-Lösung interessiert sind, stehen Ihnen die Dell Managed Services für die Verwaltung Ihrer Appliance zur Verfügung. Wenden Sie sich für weitere Informationen unter https://www.dell.com/support/contents/ca/en/calca1/category/Contact-Information an Quest Sales.

Zeitplanung für Schulungen

Um Sie bei der Verwendung der Appliance zu unterstützen, bietet Quest eine feste Anzahl an Onlineschulungssitzungen mit dem Titel „JumpStart“ an.

Informationen zu den Inhalten Ihres JumpStart Pakets finden Sie im JumpStart Datenblatt unter https://support.quest.com/kace-systems-management-appliance/training/152/kace-k1000-management-appliance-jumpstart-program.

Wenn Sie Schulungstermine festlegen möchten, wenden Sie sich per E-Mail unter mailto:KaceTraining@quest.com an das Quest Schulungsteam. Falls erforderlich, können zusätzliche Schulungssitzungen separat erworben werden.

Knowledge Base-Artikel

Weitere Informationen finden Sie auf der Knowledge Base-Seite des Quest Softwaresupports unter https://support.quest.com/systems-management-appliance/kb .

- Von der Appliance benötigte Netzwerkports: https://support.quest.com/kb/111775
- Für Patching erforderliches Whitelisting: https://support.quest.com/kb/111785
- Installieren des K1000 Agenten mithilfe einer Windows Gruppenrichtlinie: https://support.quest.com/de-de/kb/133776
- Arbeiten mit Sicherungsdateien: https://support.quest.com/kb/111736

Über uns

Mehr als nur ein Name

Wir befinden uns auf einer Mission: Informationstechnologie soll Sie bei Ihrer Arbeit noch weiter entlasten. Das ist der Grund dafür, dass wir Community-orientierte Softwarelösungen konzipieren, die Sie unterstützen und dafür sorgen, dass Sie weniger Zeit mit IT-Verwaltung aufwenden müssen und mehr Zeit für Unternehmensinnovationen haben. Wir helfen Ihnen bei der Modernisierung Ihres Rechenzentrums, bringen Sie schneller in die Cloud und bieten Ihnen das Know-how, die Sicherheit und die Barrierefreiheit, die Sie für das Wachstum Ihres datenorientieren Unternehmens benötigen. Zusammen mit der Einladung von Quest an die globale Community, Teil ihrer Innovation zu sein, und mit unserem entschlossenen Engagement, die Kundenzufriedenheit sicherzustellen, bieten wir weiterhin Lösungen an, die für unsere Kunden heute einen wirklichen Unterschied machen, und wir blicken auf ein Erbe zurück, auf das wir stolz sein können. Wir stellen uns dem Status Quo und entwickeln uns zu einem neuen Software-Unternehmen. Als Ihr Partner arbeiten wir auch unerlässlich daran, dass Ihre Informationstechnologie für Sie und von Ihnen konzipiert wird. Das ist unsere Mission, und wir bringen Sie gemeinsam zu Ende. Willkommen bei einem neuen Quest. Wir möchten Sie zur Innovation einladen.

Unsere Marke, unsere Vision. Gemeinsam.

Unser Logo zeigt unsere Geschichte: Innovation, Community und Support. Ein wichtiger Teil dieser Geschichte beginnt mit dem Buchstaben Q. Dabei handelt es sich um einen perfekten Kreis, der unsere Verpflichtung zu technologischer Präzision und Stärke widerspiegelt. Der Freiraum im Q selbst symbolisiert unsere Anforderung, die neue Community, das neue Quest um das fehlende Stück, nämlich Sie, zu ergänzen.

Kontaktaufnahme mit Quest

Für Vertriebs- oder andere Anfragen, besuchen Sie www.quest.com/company/contact-us.aspx oder wenden sich unter +1 949 754 8000 telefonisch an uns.

Ressourcen für den technischen Support

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

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

アプライアンスのセットアップ

このガイドでは、Dell Cloud 内で実行するホスト型バージョンである、サービスとしての KACE の使用を開始する方法について説明します。このガイドには、ホスト型アプライアンスを使用するための要件、機能説明、および操作手順が記載されています。これ以外のバージョンの KACE システム管理アプライアンスのセットアップの詳細、およびその他のマニュアルについては、https://documents.quest.com を参照してください。

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. サービスとしての K1 のライセンスを Quest の営業担当から購入します (https://www.quest.com/company/contact-us.aspx) 。ライセンスを購入すると、アプライアンスの静的 IP アドレスをはじめとする開始作業の詳細を記載した案内の E メールが Quest から送信されます。作業を開始するときは、この E メールを用意してください。

   サービスとしての K1 の一部の機能には VPN 接続が必要です。VPN 接続を任意の時点で購入に追加するには、Quest の営業担当にお問い合わせください (https://www.quest.com/company/contact-us.aspx) 。

2. 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変更する必要があります。
3. 使用するネットワークおよびファイアウォールの設定で、サービスとしての K1 へのアウトバウンドアクセスが次のポートで許可されることを確認します。これらのポートは、デスクトップとサーバーを含めた、K1000 エージェントソフトウェアがインストールされるデバイスでも開かれている必要があります。
   - 80：アプライアンスのウェブベースのコンソールおよび HTTP によるエージェント通信に使用します。
   - 443：アプライアンスのウェブベースのコンソールおよび HTTPS によるエージェント通信に使用します。
   - 52230：アプライアンスとエージェントとの間の通信に使用します。
4. サービスとしての K1 アプライアンスに使用する登録済みのドメイン名を取得します。これは、アプライアンスから SSL 証明書署名要求を生成して、エージェント通信にポート 443 (HTTPS) を使用するために必要です。Quest は、ポート 80 (HTTP) へのアクセスを 30 日以内に無効にする権利を保有します。詳細については、https://support.quest.com/kb/114757を参照してください。

サービスとしての K1 の機能の例外

K1000 管理者コンソールのすべての機能は Dell Cloud 内で使用するために設定できます。ただし、一部の機能はネットワークへの直接アクセスを必要とし、その確立にはサイト間の VPN 接続を使用します。VPN 接続は、サービスとしての K1 の共有ネットワークを利用します。通常は、企業 1 社の機能を有効にするには 1 つの VPN 接続で十分です。ただし、場合によっては、追加の VPN 接続が必要になり、専用ネットワーク帯域幅が要求されることがあります。詳細については、を参照してください。

VPN 接続を必要とする管理者コンソール機能

次に挙げる管理者コンソール機能には、VPN 接続が必要です。

- エージェント不要デバイス管理を使用するサーバー監視
- Wake on LAN
- ネットワーク検出 (IP スキャン、Active Directory® スキャン、NMAP スキャンを含む)
- アプライアンスからの K1000 エージェントのプロビジョニング。詳細については、を参照してください。
- リソースのインポートおよびエクスポート (ファイル共有は Dell Cloud ファイアウォールによってブロックされます)
- バックアップファイルへの FTP アクセス (FTP アクセスは Dell Cloud ファイアウォールによってブロックされます)
- アプリケーションパッケージおよびスクリプトの依存関係は、HTTP を使用してアップロードする必要があります。より速度の遅いネットワーク接続では、サイズの大きいパッケージのアップロードがタイムアウトする可能性があります。2 GB を超えるパッケージは、代替のダウンロード場所を使用して、内部ファイルサーバーから配布する必要があります。
- LDAP ユーザーラベルおよびデバイスラベル
- LDAP ユーザー認証
- LDAP ユーザーのインポート
- 管理者コンソールおよびユーザーコンソールに対する Active Directory シングルサインオン
- E メール転送 (サービスデスクチケットおよびその他の E メール通信に使用します)

ユーザーコンソール機能の例外

ユーザーコンソールは、エンドユーザーがソフトウェアライブラリとサービスデスクの機能を利用できるようにするためのインタフェースです。次に示すユーザーコンソール機能は、クラウドではサポートされていません。

- ユーザーコンソールからのソフトウェアの自動インストール（ダウンロードはサポートされます）
- ユーザーコンソール内の マイコンピューター タブ

管理者コンソールへのログイン

アプライアンスの管理者コンソールにログインして、サービスとしての K1 の使用を開始します。

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言語が決定されます。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. ウェブブラウザを開き、Quest から届いた案内の E メールに記載されている URL（管理者コンソール）を入力します。

   ソフトウェア取引契約書 ページが表示されます。

2. 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。

3. 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。
4. 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。ダッシュも含めてください。ライセンスキーがない場合は、Quest Software サポート（https://support.quest.com/ja-jp/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

オプション	説明
	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。 **i** 複数の K1000 または K2000 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ています。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。

5. 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。

   i 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。

6. 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。

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。

ネットワーク設定の構成

アプライアンスは、静的 IP アドレス、サブネットマスク、およびゲートウェイで設定されています。これらの設定は変更できません。ただし、アプライアンスのホスト名とウェブサーバー名は DNS 設定に合わせて変更する必要があります。また、要件に合わせて追加のネットワーク設定を構成できます。

1. 管理者コンソールで、アプライアンスの コントロールパネル に移動します。
   - アプライアンスで組織コンポーネントが有効化されていない場合は、設定 をクリックします。
   - アプライアンスで組織コンポーネントが有効になっている場合は、ページ右上隅のドロップダウンリストで システム を選択してから、設定 をクリックします。
2. 「ネットワーク設定」をクリックします。

   ネットワーク設定 ページが表示されます。

3. 以下のネットワーク設定を構成します。

オプション	説明
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、現在の静的 IP アドレスです。
Webサーバー	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：kbox.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ています。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。デフォルトは、現在の静的 IP アドレスです。
IPアドレス	Quest からの連絡の宛先となる E メールアドレスです。
静的IPアドレス	アプライアンスの静的IPアドレスを入力します。
ドメイン	アプライアンスが参加しているドメインを入力します。例：example.com。
サブネットマスク	アプライアンスが参加しているサブネット（ネットワークセグメント）を入力します。デフォルトは、255.255.255.0です。
デフォルトゲートウェイ	アプライアンスのネットワークゲートウェイを入力します。
プライマリDNS	ホスト名の解決にアプライアンスが使用するプライマリDNSサーバーのIPアドレスを入力します。デフォルトは、8.8.8.8です。
セカンダリDNS	（オプション）アプライアンスがホスト名の解決に使用するセカンダリDNSサーバーのIPアドレスを入力します。デフォルトは、4.2.2.2です。
プロキシ設定	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。

オプション	説明
設定をEメールで送信	アプライアンスを有効にして、E メールを送受信するには、有効 を選択し、次の設定を指定します。 • SMTP サーバー：SMTP サーバーのホスト名または IP アドレスを指定します（「smtp.gmail.com」など）。これにより、Eメール通知が有効化されます。SMTP サーバーでは、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サーバーに直接問い合わせられることを確認します。また、メールサーバーは、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。 • ポート：SMTPサーバーに使用するポート番号を入力します。標準的な SMTP にはポート 25 を使用します。セキュアな SMTP にはポート 587 を使用します。 • ログイン：SMTP サーバにアクセスするアカウントのユーザー名を入力します（「<your_account_name>@gmail.com」など）。 • パスワード：指定したサーバーアカウントのパスワードを入力します。 • サービスデスク POP3 サーバーを有効にする：サービスデスクチケットEメールにPOP3 Eメールを使用するには、このチェックボックスをオンにします。POP3 を有効にしたら、サービスデスクの キュー詳細 ページで POP3 サーバ設定を指定することができます。

4. 保存 をクリックします。

   アプライアンスが再起動します。

SNMP コミュニティ文字列の設定

SNMP コミュニティ文字列を「d35kt0pEn6」に変更します。これにより、Quest でアプライアンスの仮想インフラストラクチャをプロアクティブに管理し、ディスク領域や仮想プロセッサの問題が発生しても即座に修正できます。

1. 管理者コンソールで、アプライアンスの コントロールパネル に移動します。
    - アプライアンスで組織コンポーネントが有効化されていない場合は、設定 をクリックします。
    - アプライアンスで組織コンポーネントが有効になっている場合は、ページ右上隅のドロップダウンリストで システム を選択してから、設定 をクリックします。
2. ページ上部で、SNMP 監視を有効にする を選択します。
3. SNMP コミュニティ文字列として「d35kt0pEn6」を指定してから、保存 をクリックします。

SSLを有効にする

アプライアンスと管理対象デバイスとの間でセキュアな通信を有効にする必要があります。アプライアンスの管理者コンソールを使用して SSL 証明書を生成できます。

アプライアンスに使用する登録済みのドメイン名を取得します。これは、アプライアンスの管理者コンソールを使用して SSL 証明書署名要求を生成するために必要です。

1. 管理者コンソールで、アプライアンスの コントロールパネル に移動します。
    - アプライアンスで組織コンポーネントが有効化されていない場合は、設定 をクリックします。
    - アプライアンスで組織コンポーネントが有効化されている場合、ページの右上隅にあるドロップダウンリストから システム を選択し、設定 をクリックします。
2. セキュリティ設定 をクリックします。

    セキュリティ設定 ページが表示されます。
3. ページの下の方にある SSL セクションで、SSL を有効にする を選択します。
4. SSL 証明書の作成 をクリックします。
5. 設定情報を入力し、保存 をクリックします。
6. 「-----BEGIN CERTIFICATE REQUEST-----」と「-----END CERTIFICATE REQUEST-----」の行を含め、その間に記載された証明書要求テキストをすべてコピーして、会社にウェブサーバー証明書を発行する担当者に送信します。プライベートキーは、プライベートキー フィールドに表示されます。有効な証明書をアップロードし、続いて 展開 をクリックすると、アプライアンスに展開されます。
7. 自己署名証明書の作成 をクリックします。

    SSL証明書が生成されます。自己署名証明書は kbox.pem という名前の PEM ファイルに変換され、K1000 エージェントのデータフォルダに配置されます。

自己署名証明書を作成した場合は、エージェントが管理するすべてのデバイスにその証明書を展開する必要があります。

8. 展開 をクリックして証明書を展開し、アプライアンス上で SSL を有効にします。
9. OK をクリックして、アプライアンスを再起動します。

K1000 GO の使用

K1000 GO は、スマートフォンやタブレットからサービスデスクチケット、インベントリ情報、およびアプリケーション展開機能にアクセスするためのアプリケーションです。このアプリケーションにより、ユーザーは自分のモバイルデバイスから、サービスデスクチケットの送信、送信したチケットのステータスの表示、およびサポート技術情報記事の閲覧を行うこともできます。K1000 GO は、iOS デバイスでは Apple® App Store℠ から、Android™ デバイスでは Google® Play™ Store からダウンロードできます。詳細については、K1000 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。

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。

デル管理対象のサービスについて

IT ソリューションの完全なアウトソーシングをご希望の場合は、デル管理対象のサービスを利用して、アプライアンスの管理を委託できます。詳細については、Quest の営業担当（https://www.dell.com/support/contents/ca/en/calca1/category/Contact-Information）にお問い合わせください。

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、JumpStart と呼ばれるオンライントレーニングセッションを提供しています（トレーニングの使用回数には制限があります）。

ご購入になる JumpStart の範囲を確認するには、JumpStart データシート（https://support.quest.com/kace-systems-management-appliance/training/152/kace-k1000-management-appliance-jumpstart-program）を参照してください。

トレーニングのスケジュールを設定するには、Quest のトレーニングチームまで E メール（mailto: KaceTraining@quest.com）にてお問い合わせください。必要に応じて、トレーニングセッションは別途追加購入できます。

サポート技術情報記事

追加の情報については、Quest サポートのサポート技術情報サイト、https://support.quest.com/systems-management-appliance/kb を参照してください。

- アプライアンスに必要なネットワークポート： https://support.quest.com/kb/111775
- パッチ適用に必要なホワイトリストへの追加： https://support.quest.com/kb/111785
- Windows グループポリシーを使用した K1000 エージェントのインストール： https://support.quest.com/ja-jp/kb/133776
- バックアップファイルの操作： https://support.quest.com/kb/111736

当社について

名前を超える存在

当社は情報技術をより促進するための探求をしています。IT管理の時間を短縮し、ビジネス革新に時間を費やせるようにするために、コミュニティ主導のソフトウェアソリューションを構築しています。データセンターのモダナイゼーション、クラウドへの素早いアクセス、データ駆動型ビジネスを成長させるために必要な専門知識、セキュリティ、およびアクセシビリティの提供をサポートします。革新の一部となるグローバルコミュニティへの Quest の促進と、顧客満足度を確実にするための当社のコミットメントを組み合わせることで、当社はお客様に真のインパクトを与え、誇りとなるレガシーを残すソリューションを提供し続けます。当社は新しいソフトウェア企業に変化していくことで現状に挑戦しています。お客様のパートナーとして、情報技術が、お客様のために、そしてお客様により設計されるよう、継続して取り組み続けます。それこそが当社のミッションであり、一体となりこのミッションに取り組んでいます。新しい Quest にようこそ。当社とともに革新を促進させましょう。

当社のブランドとビジョンと、ともに。

当社の口ゴは、革新、コミュニティ、サポートという当社のストーリーを反映しています。このストーリーの重要な部分は、「Q」で始まります。これは技術的な精度と強度へのコミットを表している完全な円です。Q の空間は、コミュニティと新しい Quest に欠けている部分、つまりお客様に参加していただく当社の必要性を象徴しています。

Quest へのお問い合わせ

セールスまたはその他のお問い合わせについては、www.quest.com/company/contact-us.aspx を参照するか、1-949-754-8000までお電話ください。

テクニカルサポートのリソース

サポートポータルでは、迅速に独力で問題を解決するために使用できるセルフヘルプツールを年中無休（24時間体制）でご利用いただけます。サポートポータルでは次のことを行うことができます。

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

Configuração da solução

Este guia explica como começar a usar a versão hospedada do KACE como um serviço, que é executado dentro do Dell Cloud. Neste guia, você encontrará requisitos, descrições de recursos e instruções para usar a solução hospedada. Para obter informações sobre como configurar outras versões da Solução de gerenciamento de sistemas KACE, e para ver documentação adicional, consulte https://documents.quest.com.

Antes de começar

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

1. Compre uma licença do K1 como um Serviço a partir do departamento de vendas da Quest em https://www.quest.com/company/contact-us.aspx. Depois de comprar uma licença, a Quest lhe envia os detalhes contidos, incluindo um endereço IP estático para a solução, em um e-mail de boas-vindas. Tenha este e-mail disponível quando você for começar.

   Alguns recursos do K1 como um Serviço exigem uma conexão VPN. Para adicionar uma conexão VPN à sua compra a qualquer momento, entre em contato com o departamento de vendas da Quest em https://www.quest.com/company/contact-us.aspx.

2. No registro A de seu servidor DNS (Domain Name System, Sistema de nome de domínio) interno, insira o nome de host da solução. 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 você deve alterá-lo durante a configuração inicial.
3. Certifique-se de que as configurações da rede e do firewall permitem acesso de saída para o K1 como um Serviço nas portas a seguir. Essas portas devem também estar abertas nos dispositivos, incluindo computadores e servidores, que terão o software do agente do K1000 instalado:
   - 80: Usado nas comunicações sobre HTTP do agente e dos consoles baseados na Web da solução
   - 443: Usado nas comunicações sobre HTTPS do agente e dos consoles baseados na Web da solução
   - 52230: Usado nas comunicações entre a solução e os agentes
4. Obter um nome de domínio registrado para a solução K1 como um Serviço. Isto é OBRIGATÓRIO para gerar uma solicitação de assinatura de certificado SSL da solução e usar a porta 443 (HTTPS) nas comunicações do agente. A Quest reserva-se o direito de desativar o acesso à porta 80 (HTTP) no prazo de 30 dias. Para obter mais informações, consulte https://support.quest.com/kb/114757.

Exceções de recursos do K1 como um serviço

Todas as funcionalidades do K1000 Console do administrador podem ser configuradas para serem usadas dentro do Dell Cloud. No entanto, alguns recursos exigem acesso direito à sua rede, o que é estabelecido usando uma conexão VPN site-a-site. As conexões VPN aproveitam o K1 compartilhado como uma rede de serviço, e uma conexão VPN normalmente é o suficiente para permitir a funcionalidade para uma única companhia. No entanto, em alguns casos, conexões VPN adicionais podem ser necessárias e uma largura de banda de rede dedicada pode ser exigidas. Para obter mais informações, consulte Usar conexões VPN e recursos de rede.

Recursos do Console do administrador que exigem uma conexão VPN

Os seguintes recursos do Console do administrador exigem uma conexão VPN:

- Monitoramento de servidor usando o gerenciamento de dispositivo sem agente.
- Wake-on-LAN.
- Descoberta de rede, incluindo varredura IP, do Active Directory® e do NMAP.
- Provisionamento de agente K1000 a partir da solução. Consulte Provisionamento do agente do K1000 para dispositivos gerenciados.
- Importar e exportar recursos (o compartilhamento de arquivos é bloqueado pelo firewall do Dell Cloud).
- Acesso do FTP aos arquivos de backup (o acesso do FTP é bloqueado pelo firewall do Dell Cloud).
- Os pacotes de soluções e dependências de script devem ser carregados usando o HTTP. Uploads de pacotes grandes podem atingir o tempo limite em conexões de rede mais lentas. Pacotes maiores de 2 GB devem ser distribuídos usando um local de download alternativo de um servidor de arquivos interno.
- Usuário LDAP e rótulos de dispositivos.
- Autenticação de usuário LDAP.
- Importação de usuário LDAP.
- Login único no Active Directory para o Console do usuário e Console do administrador.
- Encaminhamento de e-mail, usado para tíquetes do Service desk e outras comunicações por e-mail.

Exceções de recursos do Console do usuário

O Console do usuário é a interface que disponibiliza os recursos da biblioteca de software e do service desk para usuários finais. Os seguintes recursos do Console do usuário não são compatíveis com a nuvem:

- Instalações automáticas de software do Console do usuário (downloads são compatíveis).
- A guia Meu computador dentro do Console do usuário.

Fazer login no Console do administrador

Faça login na solução Console do administrador para começar a usar a K1 como um serviço.

> A configuração do navegador determinará o idioma exibido noConsole do administrador na primeira vez que você fizer login. Para obter mais informações sobre como alterar as configurações de idioma, consulte o Guia do Administrador da solução: Acessar o Guia do administrador e a Ajuda on-line.

1. Abra um navegador da Web e digite o Console do administrador URL recebido no e-mail de Boas vindas da Quest.

   A página Acordo de transação de software será exibida.

2. Aceite o acordo.

   O assistente de Configuração inicial será exibido.

3. Verifique se você possui as informações necessárias para configurar a solução e depois clique em Avançar.
4. 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. Inclua as barras. Se você não tem uma chave de licença, entre em contato com o Suporte ao software da Quest em https://support.quest.com/pt-br/contact-support.
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	A senha para a conta de administrador padrão, que é a conta usada para fazer o login na

Opção	Descrição
	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. Se houver várias soluções K1000 ou K2000, 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.

5. 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 de Console do administrador exibida.

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

6. Faça login na Console do administrador usando a ID de login admin e a senha escolhida durante a configuração inicial.

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

Definir as configurações de rede

Sua solução é configurada com um endereço IP estático, uma máscara de sub-rede e um gateway. Essas definições não podem ser alteradas. No entanto, você deve alterar o nome de host e o nome do servidor da Web da solução para que correspondam às suas configurações de DNS, e você pode configurar os parâmetros de rede adicionais para coincidir com os seus requisitos.

1. NoConsole do administrador, acesse o Painel de controle da solução:
   - Se o componente de Organização não estiver habilitado na solução, clique em Configurações.
   - Se o componente Organização estiver ativado na solução, selecione Sistema na lista suspensa no canto superior direito da página e clique na guia Configurações.
2. Clique em Configurações de rede.

   A página Configurações de rede é exibida.

3. Defina as seguintes configurações de rede.

Opção	Descrição
Nome do host DNS	Digite o nome de host da solução. O padrão é o seu endereço IP estático.
Servidor da Web	Digite o nome do domínio totalmente qualificado da solução. Este é o Nome do host concatenado ao Domínio. Por exemplo: kbox.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. O padrão é o seu endereço IP estático.
Endereço IP	O endereço de e-mail em que você deseja receber as comunicações da Quest.
Endereço IP estático	Insira o endereço IP estático da solução.
Domínio	Digite o domínio no qual a solução está. Por exemplo, example.com.
Máscara de sub-rede	Digite a sub-rede (segmento de rede) em que a solução está. O padrão é 255.255.255.0.
Gateway padrão	Digite o gateway de rede para a solução.
DNS primário	Digite o endereço IP do servidor de DNS primário que a solução usa para resolver nomes de host. O padrão é 8.8.8.8.
DNS secundário	(Opcional) Insira o endereço IP do servidor DNS secundário usado pela solução para determinar nomes de host. O padrão é 4.2.2.2.
Configuração de proxy	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.
Configuração de e-mail	Para permitir que a solução envie e receba e-mail, selecione Habilitado, e especifique as seguintes configurações:

Opção	Descrição
	• Servidor SMTP: Especifique o nome do host ou o endereço IP de um servidor SMTP, como o smtp.gmail.com. Isso permite notificações por e-mail. O servidor SMTP deve 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 servidor de e-mail deve estar configurado para permitir a transferência de e-mails da solução sem autenticação. • Porta: Insira o número da porta a ser usada para o servidor SMTP. Para SMTP padrão, use a porta 25. Para SMTP seguro, use a porta 587. • Login: Informe o nome de usuário da conta com acesso ao servidor SMTP, como <your_account_name>@gmail.com. • Senha: Insira a senha da conta de servidor especificada. • Habilitar servidor POP3 de Service desk: Marque a caixa de seleção para usar o e-mail POP3 para tíquetes de e-mail do Service desk. Depois que o POP3 for habilitado, é possível especificar as configurações do servidor POP3 nas páginas Detalhe da fila do Service desk.

4. Clique em Salvar.

   A solução é reiniciada.

Configurar a sequência da comunidade SNMP

Altere a sequência da comunidade SNMP para d35kt0pEn6. Isso permite que a Quest gerencie proativamente a infraestrutura virtual da solução e corrija problemas com o espaço do disco e processadores virtuais conforme eles surgem.

1. No Console do administrador, acesse o Painel de controle da solução:
   - Se o componente de Organização não estiver habilitado na solução, clique em Configurações.
   - Se o componente Organização estiver ativado na solução, selecione Sistema na lista suspensa no canto superior direito da página e clique na guia Configurações.
2. Na parte superior da página, selecione Ativar monitoramento SNMP.
3. Especifique a seguinte sequência da comunidade SNMP: d35kt0pEn6 e clique em Salvar.

Ativar SSL

Você deve habilitar comunicações seguras entre a solução e os dispositivos gerenciados, e pode usar a solução Console do administrador para gerar um certificado de SSL.

Obtenha um nome de domínio registrado a ser usado para a solução. Essa etapa é necessária para gerar uma solicitação de assinatura do certificado SSL usando a solução Console do administrador.

1. No Console do administrador, acesse o Painel de controle da solução:
   - Se o componente de Organização não estiver habilitado na solução, clique em Configurações.
   - Se o componente Organização estiver ativado na solução: Selecione Sistema na lista suspensa no canto superior direito da página e clique em Configurações.
2. Clique em Configurações de segurança.

   A página Configurações de segurança é exibida.
3. Na seção SSL, na parte inferior da página, selecione Habilitar SSL.
4. Clique em Gerar certificado SSL.
5. Forneça as informações de configuração e clique em Salvar.
6. Copie todo o texto de solicitação de certificado, incluindo as linhas "-----BEGIN CERTIFICATE REQUEST----- e -----END CERTIFICATE REQUEST-----” e tudo que há entre elas, e, em seguida, envie-o para a pessoa que fornece à sua empresa os certificados de servidor da web. A chave privada é exibida sob o campo Chave privada. Ele será implantado na solução quando você carregar um certificado válido e clicar em Implantar.
7. Clique em Criar certificado autoassinado.

   O certificado SSL será gerado. Os certificados autoassinados são convertidos em arquivos PEM, chamados kbox.pem e colocados nas pastas de dados do Agente do K1000.

Se você criar um certificado autoassinado, será necessário implantá-lo a todos os dispositivos gerenciados por Agentes.

8. Clique em Implantar para implantar os certificados e habilitar o SSL na solução.
9. Clique em OK para reinicializar a solução.

Práticas recomendadas

Siga as orientações e recomendações contidas nesta seção ao usar K1 como um Serviço.

Usar conexões VPN e recursos de rede

Se você estiver usando a comunicação tradicional agente-servidor entre o K1 como uma solução de Serviço e os dispositivos gerenciados, a instalação do agente nos dispositivos gerenciados é tudo o que é necessário para a comunicação. No entanto, se você estiver usando uma conexão VPN, é sua responsabilidade concluir o handshake de rede do ambiente para K1 como um Serviço. O K1 como uma equipe de Serviço pode fornecer recomendações, como os endereços IP apropriados e portas para liberar, e é fundamental que o administrador de rede esteja envolvido no processo de configuração. A Dell configura as conexões apropriadas no lado da Dell e você precisa assegurar a conexão do seu lado para concluir a configuração com sucesso.

Além disso, alguns K1 como Serviço exigem uma conexão VPN para serem usados na nuvem, e geralmente uma única conexão VPN é suficiente para uma única empresa. Por exemplo, você pode usar uma única conexão VPN, mesmo que você tenha locais remotos, desde que esses locais possam rotear o tráfego através do site corporativo principal onde a conexão VPN existe. Todo o tráfego do agente do K1000 é roteado através da VPN e, em seguida, até a solução através da conexão VPN. Se os locais remotos não puderem ver o site corporativo principal ou se você quiser que cada site tenha um link VPN direto para a solução, você precisa comprar uma conexão VPN para cada site. Para obter mais informações sobre os recursos que exigem conexões VPN, consulte Exceções de recursos do K1 como um serviço.

O preço para o K1 como um Serviço está baseado na largura de banda da rede compartilhada. Para adquirir recursos de rede adicionais ou para adquirir conexões VPN, entre em contato com o departamento de vendas da Quest em https://www.quest.com/company/contact-us.aspx.

Usar conexões VPN com múltiplos domínios

O K1 como Serviço é projetado para ser usado com um único domínio e uma única conexão VPN. Se você tiver múltiplos domínios, você pode gerenciar os dispositivos (inventário) em outros domínios usando a solução, mas os recursos que exigem acesso VPN estão disponíveis apenas para um único domínio. Por exemplo, você pode fazer a autenticação em um único ambiente do Active Directory para Identity Access Management, mas não pode fazer a autenticação em mais de um domínio. O tráfego do agente a partir do domínio com a conexão VPN é roteado através da conexão VPN, enquanto o tráfego do agente a partir de outros domínios se conecta à solução

usando o acesso padrão à Internet. Para obter mais informações sobre os recursos que exigem conexões VPN, consulte Exceções de recursos do K1 como um serviço.

Sobre o endereço IP da solução

O K1 como um Serviço é configurado com um único endereço IP. O endereço IP é atribuído pela Quest e esse endereço não pode ser alterado. Você deve criar um registro de Host (A) no seu servidor DNS (Domain Name System) interno para o endereço IP estático da solução, e você pode criar múltiplos registros A (host) através de várias redes ou domínios para apontar para a sua solução. Se você precisar usar mais de um endereço IP público na rede, terá de adquirir uma instância separada de K1 como um Serviço. Várias instâncias de K1 como um Serviço não podem compartilhar quaisquer dados ou informações de banco de dados. Para obter mais informações, entre em contato com o departamento de vendas da Quest em https://www.quest.com/company/contact-us.aspx.

Sobre as configurações de rede

Por padrão, todos os protocolos de rede e seus serviços associados estão desativados, exceto AMP (Agent Messaging Protocol, usado pelo agente do K1000), HTTPS e HTTP. Esses protocolos são utilizados nas interfaces de usuário da solução e nas comunicações do agente do K1000. Quando o software do agente do K1000 está provisionado para um dispositivo, o agente primeiro usa a porta 52230 para estabelecer a conexão AMP. Para todos os outros tipos de tráfego, o agente sempre tenta se conectar à solução usando HTTPS pela porta 443 para comunicações criptografadas se o SSL estiver ativado. Caso contrário, o agente utiliza HTTP através da porta 80.

Provisionamento do agente do K1000 para dispositivos gerenciados

O agente do K1000 é um aplicativo que pode ser instalado em dispositivos para permitir seu gerenciamento e relatório de inventário através da solução K1 com um Serviço. Para provisionar o software do agente para dispositivos diretamente da solução, você deve ter uma conexão VPN. No entanto, há métodos alternativos para implantar o software do agente sem conectividade VPN:

- Fazer download e instalar manualmente o agente nos dispositivos: Você pode baixar o agente do K1000 e incluí-lo na imagem de ouro usada para fazer a imagem de novos dispositivos. Para obter mais informações, consulte: https://support.quest.com/kb/112151 .
- Instale o agente usando a Diretiva de Grupo do Windows (GPO). Para obter mais informações, vá para https://support.quest.com/pt-br/kb/133776.
- Instale o agente usando outro sistema de gerenciamento: Se a solução Quest estiver substituindo outra solução de gerenciamento de sistemas, é possível implantar o agente

usando os métodos de distribuição do sistema que está sendo substituído antes de seu descomissionamento e limpeza.

Configurações de comunicação do agente do K1000

Agentes instalados em dispositivos gerenciados se comunicam periodicamente com a solução para reportar inventários, atualizar scripts e realizar outras tarefas. É possível configurar as definições do agente, incluindo o intervalo de conexão dos agentes, as mensagens exibidas ao usuário e o tempo de retenção de registros. Se houver várias organizações, você pode configurar definições do agente para cada organização separadamente. Para obter mais informações, consulte o Guia do administrador do K1000: Acessar o Guia do administrador e a Ajuda on-line.

Sobre o monitoramento do servidor

A versão 6.3 do K1 como um Serviço introduz o monitoramento do servidor, o qual proporciona desempenho básico e monitoramento de aplicativos para servidores no inventário. Você pode habilitar o monitoramento para servidores com o agente do K1000 e para servidores usando gerenciamento sem agente, e a configuração depende das políticas do departamento de TI. O monitoramento de servidor está disponível para até cinco servidores usando uma licença padrão do K1 como um Serviço, e você pode obter uma licença para aumentar esse número.

Se você habilitar o monitoramento de servidores gerenciados por agente, as informações de alerta serão transmitidas pela porta 443 além do protocolo de comunicação de agente existente. Se você habilitar o monitoramento para servidores usando o gerenciamento sem agentes, a solução utilizará SSH ou Telnet para se conectar ao servidor, ler os logs, verificar se há alertas e exibir os alertas no K1000Console do administrador. Como o acesso VPN é necessário para o uso do SSH e Telnet, uma conexão VPN é necessária para o monitoramento do servidor sem agente.

Sobre distribuição de arquivos (pacotes) e Compartilhamento de replicação

Com K1 como um Serviço, cada local é uma localidade remota. A Quest recomenda enfaticamente que você configure Compartilhamentos de replicação para cada localidade para otimizar o uso da largura de banda nas conexões com a Internet de escritórios remotos. Os Compartilhamentos de replicação são dispositivos que mantêm cópias de arquivos para distribuição, como, por exemplo, instalações gerenciadas, patches, scripts e atualizações da Dell.

Com o compartilhamento de arquivo Samba desligado, os uploads de arquivo para a solução são limitados a 2 GB. Para arquivos acima de 2 GB, utilize um local de download alternativo para preparar os arquivos dentro da rede corporativa.

Um local alternativo de download pode ser qualquer local de rede que possua todos os arquivos necessários para a instalação de um aplicativo específico. É possível distribuir pacotes a partir de locais de download alternativos, incluindo um endereço de UNC ou fonte DFS. Os protocolos CIFS e SMB, servidores Samba e soluções de servidores de arquivos são compatíveis. O local é

especificado ao criar uma Instalação gerenciada. Para obter mais informações, consulte a seção Distribuição do Guia do administrador do K1000: Acessar o Guia do administrador e a Ajuda on-line.

Sobre o uso de largura de banda e largura de banda de rede dedicada

O K1 como um Serviço usa uma rede em nuvem compartilhada. Para reduzir os requisitos da largura de banda da rede compartilhada, a Dell recomenda enfaticamente o uso de Compartilhamentos de replicação. Se a solução pode provocar problemas de largura de banda na rede compartilhada, pode ser necessário configurar Compartilhamentos de replicação ou adquirir largura de banda de rede dedicada. Para obter mais informações, entre em contato com o departamento de vendas da Quest em https://quest.com/company/contact-us.aspx.

Sobre proteção de dados e segurança

Os data centers em nuvem da Dell e as soluções Quest vêm com uma infraestrutura altamente disponível e fornecem toda a proteção e segurança necessária para a solução. Para obter mais informações sobre as configurações de segurança da solução, consulte a seção de configuração do Guia do administrador do K1000: Acessar o Guia do administrador e a Ajuda on-line.

Uso dos arquivos de backup

Os arquivos de backup são usados para restaurar a solução K1 como um Serviço em caso de perda de dados ou para preservar as configurações durante upgrades, e a Quest automaticamente faz cópias externas do arquivo de backup noturno mais recente para fins de recuperação de desastres.

Você pode acessar os arquivos de backup usando o Console administrativo. Se os arquivos ficarem muito grandes para download através de HTTP, você pode acessá-las usando FTP. Consulte Fazer backup da solução e ativar o acesso de FTP. Se a largura de banda da rede for limitada, considere a possibilidade de usar uma distribuição de arquivos para baixar grandes arquivos de backup. Consulte Sobre distribuição de arquivos (pacotes) e Compartilhamento de replicação.

A restauração de qualquer tipo de arquivo de backup destruirá os dados configurados no servidor da solução. A Quest recomenda descarregar todos os arquivos de backup ou dados a serem mantidos antes de restaurar as configurações.

Fazer backup da solução e ativar o acesso de FTP

Você pode permitir que a Quest copie arquivos de backup diária e mensalmente para uma área de armazenamento local de alta velocidade, permitindo o acesso de FTP e definindo a senha de FTP para sepgetbxf, conforme descrito nesta seção. O acesso de FTP exige uma conexão VPN.

1. NoConsole do administrador, acesse o Painel de controle da solução:
   - Se o componente de Organização não estiver habilitado na solução, clique em Configurações.
   - Se o componente Organização estiver ativado na solução, selecione Sistema na lista suspensa no canto superior direito da página e clique na guia Configurações.
2. Clique em Configurações de segurança.

   A página Configurações de segurança é exibida.
3. Na seção superior, especifique as seguintes configurações:

Opção	Descrição
Habilitar backup via FTP	Marque esta caixa de seleção para permitir o acesso de FTP a arquivos de backup.
Tornar FTP gravável	Marque esta caixa de seleção para usar FTP para carregar arquivos de backup.
Senha de novo usuário do FTP	Digite a seguinte senha: sepgetbxf.

Se a senha de usuário de FTP estiver definida, o servidor de backup automaticamente copia, diariamente e mensalmente, os arquivos de backup para uma área de armazenamento local de alta velocidade. Para obter mais informações sobre o gerenciamento de backups, consulte a seção de manutenção do Guia do administrador do K1000: Acessar o Guia do administrador e a Ajuda on-line.

Usar o K1000 GO

O K1000 GO é um aplicativo que fornece acesso aos tíquetes do service desk, informações de inventário e recursos de implantação de aplicativos de smartphones e tablets. O aplicativo também permite que usuários enviem tíquetes do service desk, visualizem o status dos tíquetes enviados e leiam artigos da Base de conhecimento em seus dispositivos móveis. Você pode fazer download do K1000 GO na Apple® App Store℠ para dispositivos iOS ou na Google® Play™ Store para dispositivos Android™. Para obter mais informações, consulte o Guia do administrador do K1000: Acessar o Guia do administrador e a Ajuda on-line.

Acessar o Guia do administrador e a Ajuda on-line

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

Sobre serviços gerenciados da Dell

Se você estiver interessado em uma solução de TI completamente terceirizada, os Serviços gerenciados da Dell estão disponíveis para gerenciar a sua solução. Para obter mais informações, entre em contato com o departamento de vendas da Quest em https://www.dell.com/support/contents/ca/en/calca1/category/Contact-Information.

Programação de treinamento

Para ajudá-lo a começar a usar a solução, a Quest oferece um número fixo de sessões de treinamento on-line chamadas JumpStart.

Para entender o escopo de sua compra do JumpStart, consulte o Folheto do JumpStart em https://support.quest.com/kace-systems-management-appliance/training/152/kace-k1000-management-appliance-jumpstart-program.

Para programar um treinamento, envie um e-mail para a equipe de treinamento da Quest em mailto: KaceTraining@quest.com. Sessões de treinamento adicionais também podem ser compradas separadamente.

Artigos da Base de conhecimento

Para obter informações adicionais, acesse o site da Base de conhecimento do Suporte da Quest, https://support.quest.com/systems-management-appliance/kb .

- Portas de rede exigidas pela solução: https://support.quest.com/kb/111775
- Listas brancas necessárias para os patches: https://support.quest.com/kb/111785
- Instalar o Agente K1000 usando a Política de grupo do Windows: https://support.quest.com/pt-br/kb/133776
- Trabalhar com arquivos de backup: https://support.quest.com/kb/111736

Sobre nós

Somos mais do que um nome

Estamos em uma jornada para fazer sua tecnologia da informação trabalhar mais por você. É por esse motivo que criamos soluções de software voltadas para a comunidade que ajudam você a passar menos tempo cuidando da administração da TI e mais tempo inovando nos negócios. Ajudamos a modernizar seu data center, levamos a nuvem até você com mais rapidez e fornecemos a experiência, a segurança e a acessibilidade de que você precisa para expandir seus negócios orientados aos dados. Aliados ao convite da Quest para que a comunidade global participe dessa inovação, e ao nosso firme compromisso para garantir a satisfação do cliente, continuamos a oferecer soluções que têm um verdadeiro impacto em nossos clientes hoje e a deixar um legado do qual temos orgulho. Estamos desafiando o panorama atual transformando a nossa empresa em uma nova empresa de software. E, como seu parceiro, trabalhamos incansavelmente para garantir que sua tecnologia da informação seja projetada para e por você. Essa é a nossa missão e estamos juntos nisso. Bem-vindo à nova Quest. Você foi convidado a participar da inovação.

Nossa marca, nossa visão. Juntas.

Nosso logotipo reflete nossa história: inovação, comunidade e suporte. Uma parte importante dessa história começa com a letra Q. É um círculo perfeito, que representa nosso compromisso com a precisão e a força tecnológica. O espaço no próprio Q simboliza nossa necessidade de adicionar a parte que falta (você) à comunidade, à nova Quest.

Contato com a Quest

Para perguntas sobre vendas ou outras questões, acesse www.quest.com/company/contact-us.aspx ou ligue para 1-949-754-8000.

Recursos de suporte técnico

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

- Enviar e gerenciar uma solicitação de serviço
- Visualizar artigos da Base de conhecimento
- Inscrever-se para notificações de produtos
- Fazer download de software e documentação técnica
- Assistir a vídeos de instruções
- Participar de discussões comunitárias
- Conversar com engenheiros de suporte on-line
- Visualizar serviços para ajudá-lo com seu produto.

Configuración del dispositivo

En esta guía se explica cómo empezar a trabajar con la versión alojada de KACE como servicio, que se ejecuta desde la nube de Dell. En esta guía encontrará los requisitos, la descripción de las características y las instrucciones para utilizar el dispositivo alojado. Para obtener información sobre cómo configurar otras versiones del dispositivo de administración de sistemas KACE, y para obtener documentación adicional, consulte https://documents.quest.com.

Antes de comenzar

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

1. Adquiera una licencia para K1 como un servicio en ventas de Quest en https://www.quest.com/company/contact-us.aspx. Después de comprar una licencia, Quest le envía los detalles de la incorporación, incluida una dirección IP estática para el dispositivo, en un mensaje de correo electrónico de bienvenida. Disponga de este correo electrónico al comenzar.

   Algunas características de K1 como un servicio requieren una conexión VPN. Para agregar una conexión VPN a su compra en cualquier momento, comuníquese con ventas de Quest en https://www.quest.com/company/contact-us.aspx.

2. En el registro A del servidor DNS (sistema de nombres de dominio) interno, escriba el nombre de host del dispositivo. 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 forma predeterminada, el nombre de host del dispositivo es k1000, pero debe cambiarlo durante la configuración inicial.
3. Asegúrese de que los ajustes de la red y del firewall permitan el acceso saliente a K1 como un servicio en los siguientes puertos. Estos puertos también deben estar abiertos en los dispositivos, incluidos equipo de escritorio y servidores, que tendrán el software agente K1000 instalado:
   - 80: se usa para consolas basadas en la web de dispositivos y comunicaciones del agente a través de HTTP
   - 443: se usa para consolas basadas en la web de dispositivos y comunicaciones del agente a través de HTTPS
   - 52230: se usa para comunicaciones entre el dispositivo y los agentes
4. Obtenga un nombre de dominio registrado para el dispositivo K1 como un servicio. Esto es NECESARIO para generar una solicitud de firma de certificado SSL desde el dispositivo y utilizar el puerto 443 (HTTPS) para las comunicaciones del agente. Quest se reserva el derecho a desactivar el acceso al puerto 80 (HTTP) en un plazo de 30 días. Para obtener más información, consulte https://support.quest.com/kb/114757.

Excepciones de la característica K1 como servicio

Todas las funcionalidades de la Consola del administrador del K1000 se pueden configurar para usarse dentro de la nube de Dell. Sin embargo, algunas funciones requieren de acceso directo a la red, el cual se establece mediante una conexión VPN de sitio a sitio. Las conexiones VPN aprovechan la red compartida de K1 como servicio, y a menudo una única conexión VPN es suficiente para activar la funcionalidad para una sola empresa. Sin embargo, puede que en algunos casos se necesiten conexiones VPN adicionales y un ancho de banda de red dedicado. Para obtener más información, consulte Uso de los recursos de la red y conexiones VPN.

Funciones de la Consola del administrador que requieren una conexión VPN

Las siguientes funciones de la Consola del administrador requieren una conexión VPN:

- Supervisión de servidores mediante administración de dispositivos sin agente.
- Wake On LAN.
- Detección de redes, incluido el análisis de IP, el análisis de Active Directory® y el análisis de NMAP.
- Aprovisionamiento del agente de K1000 desde el dispositivo. Consulte Aprovisionamiento del agente de K1000 en los dispositivos administrados.
- Importación y exportación de recursos (el uso compartido de archivos está bloqueado por el firewall de la nube de Dell).
- Acceso vía FTP a los archivos de copia de seguridad (el acceso FTP está bloqueado por el firewall de la nube de Dell).
- Los paquetes de aplicaciones y las dependencias de scripts se deben cargar mediante HTTP. Las cargas de paquetes grandes podrían superar el tiempo de espera en conexiones de red lentas. Los paquetes de más de 2 GB se deben distribuir a través de una ubicación de descarga alternativa desde un servidor de archivos interno.
- Etiquetas LDAP de dispositivo y usuario.
- Autenticación de usuario LDAP.
- Importación de usuario LDAP.
- Inicio de sesión único de Active Directory para la Consola de usuario y la Consola del administrador.

- Reenvío de mensajes de correo electrónico para tickets de la mesa de servicio y otras comunicaciones por correo electrónico.

Excepciones de características de la consola de usuario

La Consola de usuario es la interfaz que permite que la biblioteca de software y las características de la mesa de servicio estén disponibles para los usuarios finales. Las siguientes funciones de la Consola de usuario no se admiten en la nube:

- Instalaciones automáticas de software desde la Consola de usuario (las descargas son compatibles).
- La ficha Mi PC dentro de la Consola de usuario.

Inicie sesión en la Consola del administrador

Inicie sesión en la Consola del administrador para comenzar a usar K1 como servicio.

> La configuración del navegador determina el idioma que se muestra en la Consola del administrador la primera vez que inicie sesión. Para obtener información sobre 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. Abra un navegador web e ingrese la URL de la Consola del administrador que recibió en el mensaje de correo electrónico de Bienvenida de Quest.

   Aparece la página Acuerdo de transacción de software.

2. Acepte el acuerdo.

   Aparece el asistente de Configuración inicial.

3. Verifique que dispone de la información requerida para configurar el dispositivo y, luego, haga clic en Siguiente.
4. 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. Incluya los guiones. Si no cuenta con una licencia, comuníquese con Soporte de software de Quest en https://support.quest.com/es-es/contact-support.

Opción	Descripción
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	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. Si cuenta con varios dispositivos K1000 o K2000, 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: Acceso a la Guía para el administrador y la ayuda en línea.

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

   Luego 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.

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

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

Configure los ajustes de redes

El dispositivo está configurado con una dirección IP estática, una máscara de subred y una puerta de enlace. Estos ajustes no se pueden cambiar. No obstante, debe cambiar el nombre de host del dispositivo y el nombre del servidor web para que coincidan con los ajustes de DNS, y puede configurar otros ajustes de red que se adapten a sus necesidades.

1. En la Consola del administrador, vaya al Panel de control del dispositivo:

- Si el componente Organización no está habilitado en el dispositivo, haga clic en Ajustes.
- Si el componente Organización está habilitado en el dispositivo, seleccione Sistema en la lista desplegable que se encuentra en la esquina superior derecha de la página y luego haga clic en Ajustes.

2. Haga clic en Ajustes de redes.

   Aparece la página Ajustes de redes.

3. Configure los siguientes ajustes de redes.

Opción	Descripción
Nombre de host DNS	Escriba el nombre de host del dispositivo. El valor predeterminado es la dirección IP estática.
Servidor web	Escriba el nombre completo del dominio del dispositivo. Este es el Nombre de host junto con el Dominio. Por ejemplo: kbox.ejemplo.com. Los clientes se conectan al dispositivo mediante este nombre. Quest recomienda agregar al servidor DNS una entrada de dirección IP 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. El valor predeterminado es la dirección IP estática.
Dirección IP	La dirección de correo electrónico en la que desea recibir las comunicaciones de Quest.
Dirección IP estática	Escriba la dirección IP estática del dispositivo.
Dominio	Escriba el dominio en el que se encuentra el dispositivo. Por ejemplo, ejemplo.com.
Máscara de subred	Escriba la subred (segmento de red) en la que se encuentra el dispositivo. El valor predeterminado es 255.255.255.0.
Puerta de enlace predeterminada	Escriba la puerta de enlace de red para el dispositivo.
DNS primario	Escriba la dirección IP del servidor DNS primario que el dispositivo usa para resolver los nombres de host. El valor predeterminado es 8,8.8,8.
DNS secundario	De manera opcional, puede escribir la dirección IP del servidor DNS secundario que el

Opción	Descripción
	dispositivo usa para resolver los nombres de host. El valor predeterminado es 4,2.2,2.
Configuración de 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.
Configuración de correo electrónico	Para habilitar el dispositivo para enviar y recibir correos electrónicos, seleccione Habilitado y, a continuación, especifique los ajustes siguientes: • Servidor SMTP: Especifique el nombre de host o la dirección IP de un servidor SMTP, como smtp.gmail.com. Esto habilita las notificaciones por correo electrónico. El servidor SMTP debe permitir el transporte de correos electrónicos salientes anónimos (no autenticados). Asegúrese de que las políticas de red permitan que el dispositivo se comunique con el servidor SMTP directamente. Además, el servidor de correo debe estar configurado para confiar en el correo electrónico proveniente del dispositivo sin autenticación. • Puerto: Escriba el número de puerto que va a usar para el servidor SMTP. Para SMTP estándar, use el puerto 25. Para SMTP seguro, utilice el puerto 587. • Inicio de sesión: Escriba el nombre de usuario para una cuenta que tenga acceso al servidor SMTP, como <su_nombre_de_cuenta>@gmail.com. • Contraseña: Escriba la contraseña de la cuenta del servidor especificada. • Habilitar servidor POP3 de la mesa de servicio. Active la casilla de verificación para utilizar el correo electrónico POP3 para el correo electrónico de ticket de la

Opción	Descripción
	Mesa de servicio. Después de habilitar POP3, puede especificar los ajustes del servidor POP3 en las páginas Detalles de la cola de la Mesa de servicio.

4. Haga clic en Guardar.

   Se reinicia el dispositivo.

Configure la cadena de comunidad SNMP

Cambie la cadena de comunidad SNMP a d35kt0pEn6. Esto le permite a Quest administrar de forma proactiva la infraestructura virtual del dispositivo y corregir los problemas de espacio en el disco y de procesadores virtuales a medida que surjan.

1. En la Consola del administrador, vaya al Panel de control del dispositivo:
   - Si el componente Organización no está habilitado en el dispositivo, haga clic en Ajustes.
   - Si el componente Organización está habilitado en el dispositivo, seleccione Sistema en la lista desplegable que se encuentra en la esquina superior derecha de la página y luego haga clic en Ajustes.
2. En la sección superior de la página, seleccione Habilitar supervisión de SNMP.
3. Especifique la siguiente cadena de comunidad SNMP: d35kt0pEn6 y, a continuación, haga clic en Guardar.

Habilite SSL

Debe habilitar las comunicaciones seguras entre el dispositivo y los dispositivos administrados, y puede utilizar la Consola del administrador del dispositivo para generar un certificado SSL.

Obtenga un nombre de dominio registrado para usarlo en el dispositivo. Esto es necesario para generar una solicitud de firma de certificado SSL mediante la Consola del administrador del dispositivo.

1. En la Consola del administrador, vaya al Panel de control del dispositivo:
   - Si el componente Organización no está habilitado en el dispositivo, haga clic en Ajustes.
   - Si el componente Organización sí está habilitado en el dispositivo: Seleccione Sistema en la lista desplegable en la esquina superior derecha de la página y luego haga clic en Ajustes.
2. Haga clic en Ajustes de seguridad.

Aparece la página Ajustes de seguridad.

3. En la sección SSL hacia la parte inferior de la página, seleccione Habilitar SSL.
4. Haga clic en Generar certificado SSL.
5. Proporcione la información de configuración y luego haga clic en Guardar.
6. Copie todo el texto de la solicitud del certificado, incluidas las líneas "-----BEGIN CERTIFICATE REQUEST----- y -----END CERTIFICATE REQUEST-----", junto con todo lo que aparezca entremedio, y luego envíe la solicitud a quien provea los certificados de servidor web a su compañía. Su clave privada se muestra en el campo Clave privada. Se implementa en el dispositivo cuando carga un certificado válido y luego hace clic en Implementar.
7. Haga clic en Crear certificado autofirmado.

   Se genera el certificado SSL. Los certificados autofirmados se convierten en archivos PEM, denominados kbox.pem, y se colocan en las carpetas de datos del agente K1000.

   Si crea un certificado autofirmado, tendrá que implementar ese certificado en todos los dispositivos administrados por el agente.
8. Haga clic en Implementar para implementar el certificado y habilitar SSL en el dispositivo.
9. Haga clic en Aceptar para reiniciar el dispositivo.

Mejores prácticas

Siga las directrices y recomendaciones en esta sección cuando use K1 como un servicio.

Uso de los recursos de la red y conexiones VPN

Si está utilizando la comunicación agente-servidor tradicional entre el dispositivo K1 como servicio y sus dispositivos administrados, todo lo que se requiere para la comunicación es instalar el agente en los dispositivos administrados. Sin embargo, si está utilizando una conexión VPN, es su responsabilidad completar el protocolo de enlace de su entorno para K1 como un servicio. El equipo de K1 como un servicio puede proporcionar recomendaciones, como las direcciones IP y los puertos apropiados para autorizar, y es esencial que el administrador de red se involucre en el proceso de configuración. Dell configura las conexiones apropiadas para el lado de Dell y debe asegurarse de que la conexión de su lado complete correctamente la instalación.

Además, algunas características de K1 como un servicio requieren el uso de una conexión VPN en la nube y generalmente una única conexión VPN es suficiente para una sola empresa. Por ejemplo, puede utilizar una única conexión VPN incluso si tiene ubicaciones remotas siempre que dichas ubicaciones puedan enrutar el tráfico a través del sitio corporativo principal donde existe la conexión VPN. Todo el tráfico del agente de K1000 se envía a través de la VPN y luego al dispositivo a través de la conexión VPN. Si las ubicaciones remotas no pueden ver el sitio corporativo principal o si desea que cada sitio tenga un vínculo VPN directo al dispositivo, necesita comprar una conexión VPN para cada sitio. Para obtener más información acerca de

las características que requieren conexiones VPN, consulte Excepciones de la característica K1 como servicio.

Los precios de K1 como un servicio se basan en el ancho de banda de red compartida. Para adquirir recursos de red adicionales o conexiones VPN, comuníquese con ventas de Quest en https://www.quest.com/company/contact-us.aspx.

Uso de conexiones VPN con varios dominios

K1 como un servicio está diseñado para su uso con un dominio único y una conexión VPN única. Si tiene varios dominios, puede administrar los dispositivos (inventario) en otros dominios utilizando el dispositivo, pero las características que requieren acceso VPN solo están disponibles para un solo dominio. Por ejemplo, puede autenticarse en un único entorno de Active Directory para la administración de acceso de identidad, pero no puede autenticarse en más de un dominio. El tráfico de agente desde el dominio con la conexión VPN se enruta a través de la conexión VPN, mientras que el tráfico de agente para otros dominios se conecta al dispositivo utilizando el acceso a Internet estándar. Para obtener más información acerca de las características que requieren conexiones VPN, consulte Excepciones de la característica K1 como servicio.

Acerca de la dirección IP del dispositivo

K1 como un servicio está configurado para una única dirección IP. La dirección IP la asigna Quest y no se puede cambiar. Debe crear un registro host (A) en el servidor del sistema de nombres de dominio (DNS) interno para la dirección IP estática del dispositivo y puede crear varios registros A (host) en varias redes o dominios para señalar su dispositivo. Si necesita usar más de una dirección IP pública para su red, deberá adquirir una instancia independiente de K1 como un servicio. Varias instancias de K1 como un servicio no pueden compartir cualquier dato o información de la base de datos. Para obtener más información, comuníquese con ventas de Quest en https://www.quest.com/company/contact-us.aspx.

Acerca de los ajustes de redes

De forma predeterminada, todos los protocolos de red y sus servicios asociados están deshabilitados, excepto AMP (Agent Messaging Protocol, utilizado por el agente de K1000), HTTPS y HTTP. Estos protocolos se utilizan para las interfaces de usuario de dispositivos y en las comunicaciones del agente de K1000. Cuando el software agente de K1000 se ha aprovisionado para un dispositivo, en primer lugar el agente utiliza el puerto 52230 para establecer la conexión AMP. Para el resto del tráfico, el agente siempre intenta conectarse al dispositivo mediante HTTPS a través del puerto 443 para comunicaciones cifradas si SSL está habilitado. En caso contrario, el agente utiliza HTTP a través del puerto 80.

Aprovisionamiento del agente de K1000 en los dispositivos administrados

El agente de K1000 es una aplicación que se puede instalar en los dispositivos para permitir la administración de dispositivos y los informes de inventario a través del dispositivo K1 como un servicio. Para aprovisionar el software agente en los dispositivos directamente desde el dispositivo, debe tener una conexión VPN. Sin embargo, existen métodos alternativos para implementar el software agente sin conectividad VPN:

- Descargue e instale manualmente el agente en los dispositivos: Puede descargar el agente de K1000 e incluirlo en la imagen dorada que se utiliza para representar los dispositivos nuevos. Para obtener más información, consulte: https://support.quest.com/kb/112151 .
- Instalar el agente mediante la Directiva de grupo de Windows (GPO). Para obtener más información, visite https://support.quest.com/es-es/kb/133776.
- Instalar el agente utilizando otro sistema de administración: Si la solución Quest está reemplazando a otra solución de administración de sistemas, puede implementar el Agente mediante los métodos de distribución del sistema que se va a reemplazar antes de su retiro y limpieza.

Configuración de ajustes de comunicación del agente de K1000

Los agentes instalados en dispositivos administrados se comunican periódicamente con el dispositivo para informar el inventario, actualizar scripts y realizar otras tareas. Puede configurar los ajustes del agente, como el intervalo en el que se registran los agentes, los mensajes que se muestran a los usuarios y el tiempo de retención de registros. Si tiene varias organizaciones, puede configurar ajustes del agente para cada organización por separado. Para obtener más información, consulte la Guía para el administrador del K1000: Acceso a la Guía para el administrador y la ayuda en línea.

Acerca de la supervisión de servidores

La versión 6.3 de K1 como un servicio presenta la supervisión de servidores, que proporciona rendimiento y supervisión de aplicaciones básicos para los servidores en el inventario. Puede habilitar la supervisión de servidores con el agente de K1000 y de servidores que utilizan administración sin agente; la configuración depende de las de políticas del departamento de TI. La supervisión de servidores está disponible para un máximo de cinco servidores que utilizan una licencia estándar de K1 como un servicio. Puede obtener una licencia para aumentar esa cantidad.

Si habilita la supervisión de servidores administrados por agente, la información de la alerta se transmite a través del puerto 443, además del protocolo de comunicaciones de agente existente. Si habilita la supervisión de servidores con administración sin agente, el dispositivo utiliza SSH o

Telnet para conectarse al servidor, leer los registros, verificar las alertas y visualizar las alertas en la Consola del administrador del K1000. Puesto que se requiere acceso VPN para el uso de SSH y Telnet, se requiere una conexión VPN para la supervisión de servidores sin agente.

Acerca de la distribución de archivos (paquetes) y recursos compartidos de replicación

Con K1 como un servicio, cada sitio es un sitio remoto. Quest recomienda encarecidamente configurar recursos compartidos de replicación para cada sitio con el fin de optimizar el uso de ancho de banda en las conexiones a Internet en oficinas remotas. Los recursos compartidos de replicación son dispositivos que mantienen copias de los archivos para su distribución, tales como instalaciones administradas, parches, scripts y actualizaciones de Dell.

Con los recursos compartidos de archivo Samba desactivados, las cargas de archivos en el dispositivo están limitadas a 2 GB. Para archivos que exceden 2 GB, utilice una ubicación de descarga alternativa para guardar los archivos dentro de la red corporativa.

Una ubicación de descarga alternativa puede ser cualquier ubicación de la red que tenga todos los archivos necesarios para instalar una aplicación en particular. Puede distribuir paquetes desde ubicaciones de descarga alternativas, como una dirección UNC o un origen DFS. Admite los protocolos CIFS y SMB, los servidores Samba y los dispositivos del servidor de archivos. Especifica la ubicación cuando crea una instalación administrada. Para obtener más información, consulte la sección Distribución de la Guía para el administrador del K1000: Acceso a la Guía para el administrador y la ayuda en línea.

Acerca del uso del ancho de banda y ancho de banda de red dedicada

K1 como un servicio utiliza una red en la nube compartida. Para reducir los requisitos de ancho de banda de la red compartida, Dell recomienda encarecidamente el uso de recursos compartidos de replicación. Si el dispositivo produce problemas de ancho de banda en la red compartida, puede ser necesario configurar recursos compartidos de replicación o adquirir ancho de banda de red dedicada. Para obtener más información, comuníquese con ventas de Quest en https://quest.com/company/contact-us.aspx.

Acerca de la seguridad y protección de datos

Los centros de datos en la nube de Dell y los dispositivos Quest disponen de una infraestructura de alta disponibilidad y proporcionan toda la protección y la seguridad necesarias para el dispositivo. Para obtener más información acerca de los ajustes de seguridad de los dispositivos, consulte la sección sobre configuración de la Guía para el administrador del K1000: Acceso a la Guía para el administrador y la ayuda en línea.

Uso de archivos de copia de seguridad

Los archivos de copia de seguridad se utilizan para restaurar el dispositivo K1 como un servicio en caso de pérdida de datos o para conservar los ajustes durante una actualización; Quest hace automáticamente copias externas del archivo de copia de seguridad nocturna más reciente para la recuperación ante desastres.

Puede tener acceso a los archivos de copia de seguridad utilizando la consola del administrador. Si los archivos son demasiado grandes para descargarlos con HTTP, puede acceder a ellos mediante FTP. Consulte Hacer copia de seguridad del dispositivo y habilitar el acceso a FTP. Si el ancho de banda es limitado, considere el uso de distribución de archivos para descargar archivos de copia de seguridad grandes. Consulte Acerca de la distribución de archivos (paquetes) y recursos compartidos de replicación.

La restauración de cualquier tipo de archivo de copia de seguridad destruye todos los datos actualmente configurados en el servidor del dispositivo. Quest recomienda que descargue todos los datos o archivos de copia de seguridad que quiera conservar antes de realizar una restauración de los ajustes.

Hacer copia de seguridad del dispositivo y habilitar el acceso a FTP

Puede habilitar Quest para copiar archivos de copia de seguridad diarios y mensuales a un área de almacenamiento de alta velocidad local mediante la habilitación de acceso a FTP y la configuración de la contraseña de FTP como sepgetbxf, según se describe en esta sección. El acceso a FTP requiere una conexión VPN.

1. En la Consola del administrador, vaya al Panel de control del dispositivo:
   - Si el componente Organización no está habilitado en el dispositivo, haga clic en Ajustes.
   - Si el componente Organización está habilitado en el dispositivo, seleccione Sistema en la lista desplegable que se encuentra en la esquina superior derecha de la página y luego haga clic en Ajustes.
2. Haga clic en Ajustes de seguridad.

   Aparece la página Ajustes de seguridad.
3. En la sección superior, especifique los siguientes ajustes:

Opción	Descripción
Habilitar copia de seguridad a través del FTP	Seleccione esta casilla de verificación para habilitar el acceso de FTP a los archivos de copia de seguridad.

Opción	Descripción
Convertir el FTP en grabable	Seleccione esta casilla para utilizar FTP para cargar archivos de copia de seguridad.
Contraseña de nuevo usuario de FTP:	Escriba la siguiente contraseña: sepgetbxf.

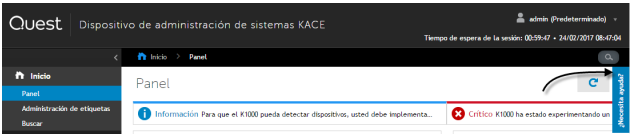
Si la contraseña de usuario de FTP está configurada, el servidor de copia de seguridad copia automáticamente los archivos de copia de seguridad diarios y mensuales a un área de almacenamiento de alta velocidad local. Para obtener más información acerca de la administración de copias de seguridad, consulte la sección sobre mantenimiento de la Guía para el administrador del K1000: Acceso a la Guía para el administrador y la ayuda en línea.

Uso de K1000 GO

K1000 GO es una aplicación que proporciona acceso a los tickets de la mesa de servicio, a información de inventario y a funciones de implementación de aplicaciones desde teléfonos inteligentes y tabletas. Además, la aplicación permite a los usuarios enviar tickets de la mesa de servicio, ver el estado de los tickets enviados y leer artículos de la base de conocimientos desde dispositivos móviles. Puede descargar K1000 GO desde Apple® App Store℠ para dispositivos iOS o desde Google Play™ para dispositivos Android™. Para obtener más información, consulte la Guía para el administrador del K1000: Acceso a la Guía para el administrador y la ayuda en línea.

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

Para obtener ayuda a través de 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.



Acerca de los servicios administrados de Dell

Si está interesado en una solución de TI completamente externa, los servicios administrados de Dell están disponibles para administrar su dispositivo por usted. Para obtener más información, comuníquese con ventas de Quest en https://www.dell.com/support/contents/ca/en/calca1/category/Contact-Information.

Programación de la capacitación

Para ayudarlo a comenzar a usar el dispositivo, Quest proporciona una cantidad fija de sesiones de capacitación en línea llamadas JumpStart.

Para comprender el alcance de la compra de JumpStart, consulte la hoja de datos de JumpStart en https://support.quest.com/kace-systems-management-appliance/training/152/kace-k1000-management-appliance-jumpstart-program.

Para programar la capacitación, envíe un correo electrónico al equipo de capacitación de Quest a mailto: KaceTraining@quest.com. Puede comprar sesiones de capacitación adicionales por separado, según las necesite.

Artículos de la base de conocimientos

Para obtener información adicional, vaya al sitio de la base de conocimientos de soporte de Quest https://support.quest.com/systems-management-appliance/kb .

- Puertos de red requeridos por el dispositivo: https://support.quest.com/kb/111775
- Listas blancas requeridas para la aplicación de parches: https://support.quest.com/kb/111785
- Instalación del agente de K1000 mediante la política de grupo de Windows: https://support.quest.com/es-es/kb/133776
- Trabajo con archivos de copia de seguridad: https://support.quest.com/kb/111736

Acerca de nosotros

Somos algo más que un nombre

Es nuestra misión hacer que su tecnología de la información trabaje arduamente para usted. Y es por eso que construimos soluciones de software impulsadas por la comunidad, que lo ayudarán a pasar menos tiempo en la administración de TI y más tiempo en la innovación empresarial. Lo ayudamos a modernizar su centro de datos, entrar más rápido a la nube y ofrecer la experiencia, seguridad y accesibilidad que necesita para hacer crecer su negocio impulsado por datos. Junto con la invitación de Quest a la comunidad mundial para ser parte de su innovación, y nuestro firme compromiso de garantizar la satisfacción del cliente, continuamos ofreciendo soluciones que tengan un verdadero impacto en nuestros clientes hoy y dejar un legado que nos llene de orgullo. Estamos desafiando al statu quo transformándonos en una nueva empresa de software. Y como su socio, trabajamos incansablemente para asegurarnos de que la tecnología de la información esté diseñada para usted y por usted. Esta es nuestra misión y estamos en esto juntos. Bienvenido al nuevo Quest. Está invitado a unirse a la innovación.

Nuestra marca, nuestra visión. Juntos.

Nuestro logo refleja nuestra historia: innovación, comunidad y apoyo. Una parte importante de esta historia comienza con la letra Q. Es un círculo perfecto que representa nuestro compromiso con la precisión y solidez tecnológica. El espacio en la propia Q simboliza nuestra necesidad de añadir la pieza faltante (usted), a la comunidad y al nuevo Quest.

Para comunicarse con Quest

Para ventas u otras consultas, visite www.quest.com/company/contact-us.aspx o llame al 1-949-754-8000.

Recursos del soporte técnico

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

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

Index