

Quest®



Appliance de gestion des systèmes KACE® 13.0

Notes de publication



Table des matières

Notes de publication de l'appliance de gestion des systèmes Quest® KACE® 13.0	3
À propos de l'appliance de gestion des systèmes KACE 13.0.....	3
Nouvelles fonctionnalités.....	3
Améliorations.....	4
Problèmes résolus.....	5
Resolved Service Desk issues.....	6
Resolved API issues.....	7
Resolved Reporting issues.....	7
Resolved Server issues.....	7
Resolved KACE Agent issues.....	8
Problèmes recensés.....	9
Configuration requise.....	9
Licence du produit.....	10
Instructions d'installation.....	10
Préparation de la mise à jour.....	10
Mise à jour du serveur de l'appliance de gestion des systèmes KACE à partir d'une mise à jour annoncée.....	12
Téléchargement et application manuelle d'une mise à jour.....	12
Tâches à effectuer après la mise à jour.....	13
Vérification du bon déroulement de la mise à jour.....	13
Vérification des paramètres de sécurité.....	13
Ressources supplémentaires.....	14
Globalisation.....	14
Qui nous sommes.....	15
Ressources du support technique.....	15
Mentions légales.....	15

Notes de publication de l'appliance de gestion des systèmes Quest® KACE® 13.0

Ce document fournit des informations sur la version 13.0 de l'appliance de gestion des systèmes KACE.

À propos de l'appliance de gestion des systèmes KACE 13.0

L'appliance de gestion des systèmes KACE est conçue pour automatiser la gestion des périphériques, le déploiement d'applications, l'application des correctifs, la gestion du parc informatique et la gestion des tickets du Service Desk. Pour plus d'informations sur la série d'appliances de gestion des systèmes KACE, consultez la page <https://www.quest.com/products/kace-systems-management-appliance/>. Cette version contient de nouvelles fonctions, des résolutions de problèmes et des améliorations relatives à la sécurité.

Nouvelles fonctionnalités

Cette version de l'appliance de gestion des systèmes KACE comprend les fonctionnalités suivantes.

- **Notifications pratiques de l'utilisateur** : L'appliance est désormais livrée avec une large gamme de configurations de notification prédéfinies. Plusieurs catégories disponibles se concentrent sur les aspects spécifiques de votre environnement, tels que la sécurité ou l'application de correctifs. Lorsque vous examinez les notifications déclenchées, les couleurs de l'arrière-plan indiquent la gravité de l'alerte : information (bleu), avertissement (jaune), avertissement (rouge). Certaines notifications incluent des liens pratiques qui vous permettent d'accéder à l'objet associé à la notification. Par exemple, si vous voyez un avis d'expiration de licence, le lien dans la notification vous dirige directement vers l'instance de licence qui est sur le point d'expirer.



REMARQUE: Les informations de la section Alerte de la page *Détails du Tableau de bord* sont déplacées dans le volet Notification.

- **Désinstallation simplifiée du logiciel** : Vous pouvez désormais ajouter ou supprimer rapidement un élément du catalogue de logiciels d'une installation gérée à l'aide de la page *Détails sur le catalogue de logiciels*.
- **Intégration de Let's Encrypt pour une gestion simplifiée des certificats** : Let's Encrypt est une autorité de certification (CA) gratuite, automatisée et ouverte. Lorsque vous obtenez un certificat de Let's Encrypt, leurs serveurs valident que vous contrôlez les noms de domaine de ce certificat à l'aide d'un défi. Un compte Let's Encrypt doit être enregistré dans le cas peu probable où le certificat expire.
- **Intégration de l'authentification Google Workspace** : L'appliance peut authentifier les utilisateurs à l'aide des informations d'identification Google Workspace à partir de cette version. Ce processus est

exploité dans les inventaires, la distribution, la rédaction de scripts, ainsi que dans le Service Desk. Les composants gérés par l'appliance suivants peuvent être authentifiés via l'API Google :

- **Découverte et inventaire des appareils Google Workspace** : Cela inclut à la fois les Chromebooks et les appareils mobiles gérés par un domaine Google Workspace (anciennement *G Suite*).
- **E-mail entrant en attente du Service Desk** : Inclut les comptes de messagerie qui font partie d'un compte Google Workspace ou d'un compte Gmail public.
- **Analyse antivirus sur les pièces jointes du Service Desk** : L'appliance inclut désormais une fonction de détection des logiciels malveillants pour les pièces jointes du Service Desk. Ce processus automatisé vérifie que les listes de définitions de virus sont mises à jour régulièrement. Toutes les pièces jointes sont analysées avant d'être ajoutées aux tickets. Gérez les fichiers en quarantaine via la page *Quarantaine antivirus*. Utilisez cette page pour consulter et gérer les pièces jointes du Service Desk en quarantaine. Une notification s'affiche lorsqu'une menace est détectée, avec un lien vers l'appareil associé au fichier. Vous pouvez également créer des notifications lorsque des types spécifiques de menaces sont détectés ou en fonction de leur changement d'état.
- **Distribution des pièces jointes du Service Desk par e-mail** : L'appliance peut désormais envoyer des pièces jointes au ticket au lieu de fournir des liens vers les fichiers. Vous pouvez également ajouter des pièces jointes aux modèles d'e-mail si nécessaire.



REMARQUE: La configuration minimale requise pour l'exécution d'un système 13.0 (ou pour la mise à niveau depuis un système 12.1) a été modifiée. Un espace de 8 Go minimum est requis pour le fonctionnement de l'appliance. En outre, la surveillance est désormais prise en charge pour les appareils macOS 12.0 gérés. Pour plus de détails, voir les *Caractéristiques techniques*.

Améliorations

La liste ci-dessous répertorie les améliorations apportées à cette version.

Enhancement	Issue ID
Agent support for Windows 10 22H2.	K1A-3959
Agent support for Red Hat Enterprise Linux 9.	K1A-3945
Agent support for Windows 11 22H2.	K1A-3944
Support for Microsoft System Center Virtual Machine Manager and Hyper-V 2022.	K1A-3931
Agent support for Raspbian Linux 11 (Bullseye).	K1A-3923
Agentless support for macOS 13 Ventura.	K1A-3922
Agent support for macOS 13 Ventura.	K1A-3921
Agent support for Ubuntu 22 LTS.	K1A-3913
Konea module security enhancements.	K1A-3909
Linux package upgrades: Ability to pull repository information from the <code>sources.list.d</code> directory.	K1A-3903
Added DirectX version to inventory data.	K1A-3898

Enhancement	Issue ID
Agentless support for Red Hat Enterprise Linux 9.	K1-33030
Agentless support for Windows 11 22H2.	K1-33028
Agentless support for Raspbian Linux 11 (Bullseye).	K1-32835
Added logical disks to Dell Data Protection Encryption inventory on Windows.	K1-32746
Migrated Google OAuth support for Google Workspace Integration.	K1-32682
Added ticket history for deleted Service Desk tickets.	K1-32646
Agentless support for openSUSE Leap 15.4.	K1-32604
Agentless support for Fedora 35 and 36.	K1-32603
Agentless support for Ubuntu 22 LTS.	K1-32602
Ability to limit system generated approval workflow comments to owners only.	K1-32547
Added ability to create a managed uninstall directly from the SW Catalog Detail Page using a Add Managed Uninstall button.	K1-32530
The TLS 1.2 ciphers are adjusted to provide the highest possible security rating while maintaining client compatibility.	K1-32476
Added a link to the Microsoft Defender Advanced Threat Protection console to the Microsoft Defender section on the <i>Device Detail</i> page, when applicable.	K1-32422
<i>My Recent Sessions</i> pop-up includes country, if available.	K1-32412
Updated User Notification system to forward new notifications to push server.	K1-32277
Added ability to remove incoming SMTP capability from appliance.	K1-32096
Removed framesets from the Administrator Console , System Administration Console , and User Console .	K1-30094
Drop-down fields (<i>Category</i> , <i>Impact</i> , <i>Priority</i> , and <i>Status</i>) can be left blank when required	K1-22073

Problèmes résolus

Cette section contient les problèmes résolus dans cette version :

Resolved Service Desk issues

The following is a list of server issues resolved in this release.

Resolved Service Desk issues

Resolved issue	Issue ID
A new ticket from email could show a blank title and summary.	K1-33146
Ticket did not get created when more than one address was added in the To or CC field using Gmail OAuth.	K1-32862
The ticket title from the email subject field in some cases was encoded twice in UTF-8.	K1-32781
Ticket <i>Reassign To</i> owner ticket counts included closed state tickets .	K1-32750
<i>Ticket List Queue</i> drop-down was empty when user Locale is set to French (France)	K1-32739
When logging in, a blank screen sometimes appeared, requiring a page reload.	K1-32711
Ticket search did not return CC-ed user or submitter's tickets if user was not a valid submitter for the queue.	K1-32699
User downloads approval request ticket <i>Summary</i> field was blank.	K1-32694
Physical to virtual backup migration preserved any physical card network settings.	K1-32692
Tickets made from templates did not always show parent info on the ticket list.	K1-32680
The <i>Patch Schedules</i> list page could be slow to load.	K1-32575
Asset History entries could be missing from configuration.	K1-32554
Updating ticket category field through email failed if category name contained underscore.	K1-32553
Tickets: Commentor not added to CC list when only clicking Save or Apply Changes .	K1-32533
Single quote in ticket title was not displayed correctly in email sent from <i>Ticket Detail</i> page.	K1-32514
Service Desk Reporting: Approver information was not shown on parent process tickets.	K1-32496
Default Custom View caused Submitter Ticket History link to redirect to inaccurate list page results.	K1-32481

Resolved issue	Issue ID
Service Desk: Closing ticket on list page with Satisfaction Survey required resulted in an error.	K1-32454
Process approval timeout did not calculate as expected.	K1-32452
Queue email addresses in the To field was copied in the CC list (when using SMTP).	K1-32417
The timestamp on Service Desk announcements were not updating after modification	K1-32237
Updating ticket custom field through email by label name failed if label name contained space and underscore.	K1-31767



REMARQUE: The *Ticket Detail* page allows the browser to auto-complete the Title field when creating new tickets, if KB article suggestions are disabled. However, if a password manager is linked to the browser, the browser's auto-complete option is typically disabled.

Resolved API issues

The following is a list of API issues resolved in this release.

Resolved API issues

Resolved issue	Issue ID
Get owned queues API returned incorrect queue count.	K1-33322
The appliance API <code>GET /api/inventory/machines/</code> did not include <code>gateway_ip</code> <code>gateway_ipv6</code> .	K1-32675

Resolved Reporting issues

The following is a list of reporting issues resolved in this release.

Resolved Reporting issues

Resolved issue	Issue ID
An SQL error could be seen when generating report from archived ticket list advanced search.	K1-32644
Reporting: Special characters were incorrectly displayed in PDF reports generated in foreign language browser.	K1-32541
Scheduled XLS reported error with The file format and extension of <code><filename.xls></code> don't match.	K1-17412

Resolved Server issues

The following is a list of server issues resolved in this release.

Resolved server issues

Resolved issue	Issue ID
Could not save Managed Install with empty <i>Devices</i> field when logged-in user's role had Device Scope Label applied.	K1-32771
When logging in, a blank screen sometimes displayed, requiring a page reload.	K1-32711
Physical to virtual backup migration preserved any physical card network settings.	K1-32692
Restoring backup from the setup wizard did not always correctly set the DB time-zone.	K1-32688
The <i>Patch Schedule</i> list page may be slow to load.	K1-32575
FileVault encryption was missing Conversion Status/Percentage and Encryption Status/Type.	K1-32568
Asset History entries could be missing from configuration.	K1-32554
Computer Inventory: Inventory failed when unknown characters existed in Machine Process.	K1-32551
Patch Download: Failed payload download shows updated when last payload succeeded.	K1-32540
Attachments of type <code>.eml</code> or <code>.msg</code> were missing from tickets submitted by email.	K1-32111
Monitoring: Log Profile alerts did not create tickets.	K1-21174



REMARQUE: The option **Enable webserver compression** is removed from **Settings > Control Panel > Security Settings** in this release.

Resolved KACE Agent issues

The following is a list of KACE Agent issues resolved in this release.

Resolved KACE Agent issues

Resolved issue	Issue ID
macOS installer prompted user to install Rosetta on Mac with Apple silicon (M1/M2) chip.	K1A-3942
Agents were going offline after failing to update the Konea certificate after it had expired.	K1A-3934
Process names could be reported incorrectly in inventory for Linux.	K1A-3914
Offline Scripts looping due to DST change.	K1A-3906

Problèmes recensés

L'existence des problèmes suivants est connue à la date de cette publication.



REMARQUE: L'inventaire des appareils Ubuntu 21.04 sans agent échoue pour les utilisateurs dont le shell par défaut n'est pas en bash.

Known issue	Issue ID
Agentless inventory of macOS 12 incorrectly shows two volumes mounted to '/'.	K1-33162
Manually provisioning an SNMP device from <i>Discovery Results</i> page shows missing settings when SNMP walk is selected and that walk failed.	K1-33154
Nmap discovery type with TCP or UDP port scan options selected does not return opened ports.	K1-33005
Device Actions can sometimes fail when accessing them through a direct URL.	K1-32305
Login field does not update after user authenticates through SAML and the mapping was changed.	K1-32304
Large metering data can cause page to load slowly.	K1-32249
Schedule info does not show correctly after disabling a Linux Package Upgrade Schedule.	K1-30725
Managed Install snooze time is ignored. Snooze option does not reappear until next inventory interval.	K1-20832
Managed Install attempts used up during inventory when user alert is snoozed.	K1-20826

Configuration requise

La version minimale requise pour installer l'appliance de gestion des systèmes KACE 13.0 est la version 12.1. Si votre appliance exécute une version antérieure, vous devez d'abord effectuer la mise à jour vers la version indiquée avant de procéder à l'installation.

La version minimale requise pour effectuer la mise à niveau de l'agent KACE est la version 11.0. Nous vous recommandons de toujours utiliser la même version de l'agent et de l'appliance de gestion des systèmes KACE.

À partir de la version 12.0 de l'appliance, les versions antérieures de l'agent KACE, telles que la version 11.1, doivent être signées spécifiquement pour la version de votre appliance. Par exemple, si vous utilisez l'agent KACE 11.1 avec la version 12.1 de l'appliance, vous devez obtenir et installer le fichier KBIN KACE Agent 11.1 signé avec la clé d'appliance 12.1. Vous pouvez télécharger les fichiers KBIN KACE Agent signés à partir de la page *Téléchargements de logiciels* de l'appliance de gestion des systèmes KACE.



REMARQUE: Le package RPM de l'agent KACE peut être installé sur les appareils SUSE Linux gérés uniquement lorsque le package `libxslt-tools` est installé avant le package de l'agent.

Pour vérifier le numéro de version de l'appliance, connectez-vous à la page **Console d'administration** et cliquez sur **Besoin d'aide**. Dans le panneau Aide qui s'affiche, en bas, cliquez sur le bouton entouré « i ».

Avant de procéder à la mise à niveau vers la version 13.0 ou d'installer cette version, vérifiez que votre système répond aux exigences minimales. Ces exigences figurent dans les spécifications techniques de l'appliance de gestion des systèmes KACE.

- Pour les appliances virtuelles : rendez-vous sur <https://support.quest.com/technical-documents/kace-systems-management-appliance/13.0-common-documents/technical-specifications-for-virtual-appliances/>.
- Pour KACE en tant que service : rendez-vous sur <https://support.quest.com/technical-documents/kace-systems-management-appliance/13.0-common-documents/technical-specifications-for-kace-as-a-service/>.

Licence du produit

Aucune licence supplémentaire n'est requise si vous possédez une licence de produit de l'appliance de gestion des systèmes KACE.

Si vous utilisez l'appliance de gestion des systèmes KACE pour la première fois, vous trouverez les informations relatives à la licence dans le guide d'installation de l'appliance. Rendez-vous sur [Ressources supplémentaires](#) pour accéder au guide approprié.

i **REMARQUE:** les licences de produit correspondant à la version 13.0 doivent être utilisées exclusivement sur les appliances de gestion des systèmes KACE qui exécutent la version 13.0 ou une version ultérieure. Les licences correspondant à la version 13.0 ne peuvent être utilisées avec des appliances exécutant une version antérieure, comme la version 12.0.

Instructions d'installation

Vous pouvez appliquer cette version à partir d'une mise à jour annoncée ou en téléchargeant et en appliquant manuellement un fichier de mise à jour. Pour obtenir des instructions, reportez-vous aux rubriques suivantes :

- [Préparation de la mise à jour](#)
- [Mise à jour du serveur de l'appliance de gestion des systèmes KACE à partir d'une mise à jour annoncée](#)
- [Téléchargement et application manuelle d'une mise à jour](#)
- [Tâches à effectuer après la mise à jour](#)

i **REMARQUE:** afin de garantir la précision de la découverte des logiciels et du nombre d'installations pour les appareils exécutant un logiciel en particulier, à partir de la version 7.0 de l'appliance de gestion des systèmes KACE, le catalogue de logiciels se réinstallera après chaque mise à niveau.

Préparation de la mise à jour

Avant de procéder à la mise à jour du serveur de l'appliance de gestion des systèmes KACE, suivez ces recommandations :

- **IMPORTANT : Activation du démarrage du BIOS existant :**

Un problème dans le démarrage du BIOS UEFI peut être déclenché lors d'une mise à niveau. Pour l'éviter, vous devez vous assurer que le démarrage du BIOS existant est activé. L'appliance doit être hors tension avant de procéder à un changement de mode. En outre, pour les machines virtuelles basées sur ESX, assurez-vous que la version matérielle est la version 13 ou une version ultérieure.

Avant d'appliquer la mise à niveau de l'appliance, vous devez vous assurer que la mémoire cache de votre navigateur est vide et que le port 52231 est disponible de votre navigateur vers l'appliance. Les utilisateurs travaillant à domicile peuvent avoir besoin de configurer leur pare-feu d'entreprise pour permettre les communications sur le port 52231.

- **Vérifiez la version du serveur de l'appliance de gestion des systèmes KACE :**

La version minimale requise pour installer l'appliance de gestion des systèmes KACE 13.0 est la version 12.1. Si votre appliance exécute une version antérieure, vous devez d'abord effectuer la mise à jour vers la version indiquée avant de procéder à l'installation.

Pour vérifier le numéro de version de l'appliance, connectez-vous à la page **Console d'administration** et cliquez sur **Besoin d'aide**. Dans le panneau Aide qui s'affiche, en bas, cliquez sur le bouton entouré « i ».

- **Vérifiez la version de votre agent KACE.**

La version minimale requise pour effectuer la mise à niveau de l'agent KACE est la version 11.0. Nous vous recommandons de toujours utiliser la même version de l'agent et de l'appliance de gestion des systèmes KACE.

À partir de la version 12.0 de l'appliance, les versions antérieures de l'agent KACE, telles que la version 11.1, doivent être signées spécifiquement pour la version de votre appliance. Par exemple, si vous utilisez l'agent KACE 11.1 avec la version 12.1 de l'appliance, vous devez obtenir et installer le fichier KBIN KACE Agent 11.1 signé avec la clé d'appliance 12.1. Vous pouvez télécharger les fichiers KBIN KACE Agent signés à partir de la page *Téléchargements de logiciels* de l'appliance de gestion des systèmes KACE.



REMARQUE: Le package RPM de l'agent KACE peut être installé sur les appareils SUSE Linux gérés uniquement lorsque le package `libxslt-tools` est installé avant le package de l'agent.

- **Effectuez une sauvegarde avant de commencer.**

Sauvegardez votre base de données et vos fichiers, et enregistrez vos sauvegardes sur un support extérieur au serveur de l'appliance de gestion des systèmes KACE, pour pouvoir y accéder ultérieurement. Pour des instructions sur la sauvegarde de votre base de données et de vos fichiers, consultez le document **Administrator Guide** (Guide de l'administrateur) à l'adresse <https://support.quest.com/technical-documents/kace-systems-management-appliance/13.0-common-documents/administrator-guide/>.

- **Appliances installées avant la version 7.0.**

Pour les appliances initialement installées avant la version 7.0 qui n'ont pas été réimaginees (appliances physiques) ou réinstallées (virtuelles), Quest Software recommande fortement d'exporter, de recréer (une installation d'image ou de machine virtuelle à partir d'un fichier OVF) et réimporter la base de données avant de mettre à niveau vers la version 13.0. Pour plus d'informations, rendez-vous sur <https://support.quest.com/kace-systems-management-appliance/kb/111810/how-to-re-image-the-k1000-appliance>.

Si la version de votre appliance a de nombreuses versions de retard, l'article suivant contient des conseils utiles concernant la mise à niveau : <https://support.quest.com/kace-systems-management-appliance/kb/155574/upgrading-a-kace-systems-management-appliance-that-is-multiple-versions-behind-upgrade-path-6-x-to-10-0->.

Les raisons pour lesquelles vous devriez réimager l'appliance sont nombreuses. La nouvelle disposition du disque, par exemple, offre une meilleure compatibilité avec la version 13.0. Elle présente également une meilleure sécurité et de meilleures performances.

Pour déterminer si votre système bénéficierait d'une telle mise à niveau, vous pouvez utiliser un fichier KBIN pour déterminer l'âge exact de votre appliance et de la disposition de son disque. Pour télécharger le fichier KBIN, consultez <https://support.quest.com/kace-systems-management-appliance/kb/210267/how-to-run-the-kace-systems-management-appliance-configuration-report>.

- **Assurez-vous que le port 52 231 est disponible.**

Avant toute mise à niveau `.kbin`, le port 52 231 doit être disponible afin que la page de la console de mise à niveau KACE soit accessible. Si la mise à niveau est lancée sans que ce port ne soit disponible, vous ne pourrez pas suivre la progression de la mise à niveau. Quest KACE vous recommande fortement d'autoriser le trafic vers l'appliance via le port 52231 depuis un système de confiance et de suivre la mise à niveau à l'aide de la Console de mise à niveau. Sans accès à la Console de mise à niveau, la mise

à niveau renvoie vers une page inaccessible qui indique dans le navigateur une expiration du délai de réponse. La personne en charge peut alors croire à un plantage du système dû à la mise à niveau, la conduisant à redémarrer alors que la mise à niveau est en réalité toujours en cours. En cas de doute sur la progression de la mise à niveau, contactez le support KACE et **ne redémarrez pas l'appliance**.

Mise à jour du serveur de l'appliance de gestion des systèmes KACE à partir d'une mise à jour annoncée

Vous pouvez effectuer la mise à jour du serveur de l'appliance de gestion des systèmes KACE en appliquant une mise à jour annoncée sur la page *Tableau de bord* ou *Mises à jour de l'appliance* de **Console d'administration**.

MISE EN GARDE: Ne redémarrez jamais le serveur de l'appliance de gestion des systèmes KACE manuellement pendant une mise à jour.

1. Sauvegardez votre base de données et vos fichiers. Pour obtenir des instructions, consultez le **Guide de l'administrateur**, <https://support.quest.com/technical-documents/kace-systems-management-appliance/13.0-common-documents/administrator-guide/>.
2. 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 :
Connectez-vous à la page Console d'administration système de l'appliance :
`http://nom_hôte_KACE_SMA/system` ou sélectionnez **Système** dans la liste déroulante figurant en haut à droite de la page, puis cliquez sur **Paramètres**.
3. Dans la barre de navigation de gauche, cliquez sur **Mises à jour de l'appliance** pour afficher la page *Mises à jour de l'appliance*.
4. Cliquez sur **Rechercher des mises à jour**.
Le journal présente les résultats de la vérification.
5. Lorsqu'une mise à jour est disponible, cliquez sur **Mise à jour**.

i **IMPORTANT:** au cours des dix premières minutes, certains navigateurs peuvent donner l'impression de se bloquer pendant la décompression et la vérification de la mise à jour. Pendant cette procédure, ne quittez pas la page, ne l'actualisez pas et ne cliquez sur aucun des boutons du navigateur de cette page car ces actions interrompraient la procédure. Une fois la mise à jour décompressée et vérifiée, la page *Journaux* s'ouvre. Ne redémarrez jamais l'appliance manuellement pendant la procédure de mise à jour.

La version 13.0 est appliquée et le serveur de l'appliance de gestion des systèmes KACE redémarre. La progression s'affiche dans la fenêtre du navigateur et dans **Console d'administration**.

6. Une fois la mise à niveau du serveur terminée, mettez à niveau tous de vos agents vers la version 13.0.

Téléchargement et application manuelle d'une mise à jour

Si vous disposez d'un fichier de mise à jour fourni par Quest, vous pouvez le télécharger manuellement pour mettre à jour le serveur de l'appliance de gestion des systèmes KACE.

MISE EN GARDE: Ne redémarrez jamais le serveur de l'appliance de gestion des systèmes KACE manuellement pendant une mise à jour.

1. Sauvegardez votre base de données et vos fichiers. Pour obtenir des instructions, consultez le **Guide de l'administrateur**, <https://support.quest.com/technical-documents/kace-systems-management-appliance/13.0-common-documents/administrator-guide/>.
 2. Connectez-vous au site Web de Quest à l'adresse <https://support.quest.com/kace-systems-management-appliance/download-new-releases> à l'aide de vos informations d'identification, téléchargez le fichier `.kbin` du serveur de l'appliance de gestion des systèmes KACE correspondant à la version 13.0 GA (disponibilité générale) et enregistrez localement ce fichier.
 3. Dans la barre de navigation de gauche, cliquez sur **Mises à jour de l'appliance** pour afficher la page *Mises à jour de l'appliance*.
 4. Dans la section *Mettre à jour manuellement* :
 - a. Cliquez sur **Parcourir** ou sur **Sélectionner un fichier**, puis accédez au fichier de mise à jour.
 - b. Cliquez sur **Mise à jour**, puis sur **Oui** pour confirmer.
- La version 13.0 est appliquée et le serveur de l'appliance de gestion des systèmes KACE redémarre. La progression s'affiche dans la fenêtre du navigateur et dans **Console d'administration**.
5. Une fois la mise à niveau du serveur terminée, mettez à niveau tous de vos agents vers la version 13.0.

Tâches à effectuer après la mise à jour

Après la mise à jour, vérifiez que celle-ci s'est déroulée avec succès et vérifiez les paramètres selon les besoins.

Vérification du bon déroulement de la mise à jour

Pour vous assurer que la mise à jour s'est déroulée avec succès, vérifiez le numéro de version de l'appliance de gestion des systèmes KACE.

1. 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 :**
Connectez-vous à la page Console d'administration système de l'appliance :
`http://nom_hôte_KACE_SMA/system` ou sélectionnez **Système** dans la liste déroulante figurant en haut à droite de la page, puis cliquez sur **Paramètres**.
2. Pour vérifier la version actuelle, cliquez sur **Besoin d'aide** en haut à droite de la page, puis dans le panneau Aide qui s'affiche, en bas, cliquez sur le bouton entouré « i ».

Vérification des paramètres de sécurité

Afin de renforcer la sécurité, l'accès à la base de données via HTTP et FTP est désactivé pendant la mise à jour. Si vous utilisez cette méthode pour accéder aux fichiers de base de données, vous devrez modifier les paramètres de sécurité après la mise à jour.

1. 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 :**
Connectez-vous à la page Console d'administration système de l'appliance :

`http://nom_hôte_KACE_SMA/system` ou sélectionnez **Système** dans la liste déroulante figurant en haut à droite de la page, puis cliquez sur **Paramètres**.

2. Dans la barre de navigation de gauche, cliquez sur **Paramètres de sécurité** pour afficher la page *Paramètres de sécurité*.
 3. Dans la section supérieure de la page, modifiez les paramètres suivants :
 - **Activer les fichiers de sauvegarde sécurisés** : décochez cette case pour permettre aux utilisateurs d'accéder aux fichiers de sauvegarde de base de données via HTTP sans authentification.
 - **Activer l'accès à la base de données** : cochez cette case pour permettre aux utilisateurs d'accéder à la base de données sur le port 3306.
 - **Activer la sauvegarde via FTP** : cochez cette case pour permettre aux utilisateurs d'accéder aux fichiers de sauvegarde de base de données via FTP.
- !** **MISE EN GARDE:** la modification de ces paramètres n'est pas recommandée car elle réduit la sécurité de la base de données.
4. Cliquez sur **Enregistrer**.
 5. **Mises à niveau KBIN uniquement.** Renforcez l'accès par mot de passe racine (2FA) à l'appliance.
 - a. Dans Console d'administration système, cliquez sur **Paramètres > Support**.
 - b. Sur la page *Support*, sous *Outils de dépannage*, cliquez sur **Authentification à deux facteurs**.
 - c. Sur la page *Authentification à deux facteurs du support*, cliquez sur **Remplacer la clé secrète**.
 - d. Enregistrez les jetons et placez ces informations dans un endroit sûr.

Ressources supplémentaires

Des informations supplémentaires sont disponibles parmi les sources suivantes :

- Documentation du produit en ligne (<https://support.quest.com/kace-systems-management-appliance/13.0/technical-documents>)
 - **Spécifications techniques** : informations concernant les exigences minimales d'installation et de mise à niveau vers la dernière version du produit.
Pour les appliances virtuelles : rendez-vous sur <https://support.quest.com/technical-documents/kace-systems-management-appliance/13.0-common-documents/technical-specifications-for-virtual-appliances/>.
Pour KACE en tant que service : rendez-vous sur <https://support.quest.com/technical-documents/kace-systems-management-appliance/13.0-common-documents/technical-specifications-for-kace-as-a-service/>.
 - **Guides d'installation** : instructions d'installation des appliances virtuelles. Rendez-vous sur <https://support.quest.com/kace-systems-management-appliance/13.0/technical-documents> pour accéder à la documentation relative à la version la plus récente.
 - **Guide de l'administrateur** : instructions concernant l'utilisation de l'appliance. Rendez-vous sur <https://support.quest.com/technical-documents/kace-systems-management-appliance/13.0-common-documents/administrator-guide/> pour accéder à la documentation relative à la version la plus récente.

Globalisation

Cette section contient des informations concernant l'installation et le fonctionnement de ce produit dans les configurations autres qu'en langue anglaise utilisées, par exemple, par des personnes extérieures à l'Amérique du Nord. Cette section ne remplace pas les informations relatives aux plateformes et configurations prises en charge que vous retrouverez dans d'autres parties de la documentation du produit.

Cette version est au format Unicode et est compatible avec tous les jeux de caractères. Dans cette version, tous les composants du produit doivent être configurés afin d'utiliser les mêmes codages de caractères, ou des codages compatibles, et ils doivent être installés de manière à utiliser les mêmes options locales et régionales. Cette version peut être utilisée dans les régions suivantes : Amérique du Nord, Europe Occidentale et Amérique Latine, Europe Centrale et Orientale, Asie Orientale, Japon.

La version est disponible dans les langues suivantes : allemand, espagnol, français, japonais, portugais (Brésil).

Qui nous sommes

Quest crée des solutions logicielles qui rendent tangibles les avantages des nouvelles technologies, dans un environnement IT de plus en plus complexe. De la gestion des bases de données et des systèmes à la gestion d'Active Directory et d'Office 365, en passant par la résilience de la cybersécurité, Quest aide ses clients à relever, dès maintenant, leur prochain défi IT. Dans le monde entier, plus de 130 000 entreprises, dont 95 % des entreprises du classement Fortune 500, comptent sur Quest pour assurer une gestion et un suivi proactifs de leur prochaine initiative, pour trouver la solution aux prochains défis complexes de Microsoft et pour garder une longueur d'avance sur la prochaine menace. Quest Software. Quand le présent rencontre le futur. Pour plus d'informations, visitez le site www.quest.com.

Ressources du support technique

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

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

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

Mentions légales

© 2022 Quest Software Inc. ALL RIGHTS RESERVED.

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

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

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

Brevets

Chez Quest Software, nous sommes fiers de notre technologie avancée. Des brevets et des brevets en attente peuvent s'appliquer à ce produit. Pour obtenir les informations les plus récentes sur les brevets applicables à ce produit, visitez notre site Web à l'adresse <https://www.quest.com/legal>.

Trademarks

Quest, the Quest logo, Join the Innovation, and KACE are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. All other trademarks and registered trademarks are property of their respective owners.

Légende

-  **MISE EN GARDE:** une icône MISE EN GARDE indique un risque de dommage causé au matériel ou de perte de données si les instructions ne sont pas respectées.
-  **IMPORTANT, REMARQUE, CONSEIL, MOBILE ou VIDÉO:** une icône d'information indique la présence de renseignements supplémentaires.

Notes de publication de l'appliance de gestion des systèmes KACE

Date de mise à jour : octobre 2022

Version logicielle - 13.0