

Quest®



Solução de gerenciamento de sistemas KACE® 11.1

## **Notas da versão**



# Sumário

<b>Notas de versão da Solução de gerenciamento de sistemas Quest® KACE® 11.1</b> .....	<b>3</b>
Sobre a Solução de gerenciamento de sistemas KACE 11.1.....	3
Novos recursos.....	3
Aprimoramentos.....	5
Problemas resolvidos.....	6
Problemas conhecidos.....	10
Requisitos do sistema.....	12
Licenciamento do produto.....	12
Instruções de instalação.....	12
Preparar para a atualização.....	13
Atualizar o servidor da Solução de gerenciamento de sistemas KACE usando uma atualização anunciada.....	14
Carregar e aplicar uma atualização manualmente.....	14
Tarefas pós-atualização.....	15
Verificar conclusão com êxito.....	15
Verificar configurações de segurança.....	15
Mais recursos.....	16
Globalização.....	16
Sobre nós.....	16
Recursos de suporte técnico.....	17
Avisos legais.....	17

# Notas de versão da Solução de gerenciamento de sistemas Quest® KACE® 11.1

---

Este documento fornece informações sobre a Solução de gerenciamento de sistemas KACE versão 11.1.

## Sobre a Solução de gerenciamento de sistemas KACE 11.1

A Solução de gerenciamento de sistemas KACE é uma solução virtual desenvolvida para automatizar o gerenciamento de dispositivos, a implantação de aplicativos, a aplicação de patches, o gerenciamento de ativos e o gerenciamento de tíquetes do Service desk. Para obter mais informações sobre a série da Solução de gerenciamento de sistemas KACE, acesse <https://www.quest.com/products/kace-systems-management-appliance/>. Esta versão contém uma série de novos recursos, problemas resolvidos e melhorias de segurança.



**NOTA:** Este é o único documento traduzido para esta versão, no entanto, as variantes traduzidas não incluem informações sobre como resolver problemas, aprimoramentos e problemas conhecidos. Outros guias, como o *Guia do administrador* e a ajuda no produto, ainda não foram traduzidos, e os documentos da versão 10.2 estão incluídos.

## Novos recursos

Esta versão da Solução de gerenciamento de sistemas KACE inclui os seguintes recursos.

### Comunicações do dispositivo

- **Adições da bandeja do sistema do agente do KACE:** Mais funcionalidades adicionadas ao ícone do agente na bandeja do sistema, como abrir links. Os administradores do sistema podem especificar até dez links para aparecer no novo item de menu Atalhos. Esse item de menu só aparece quando um ou mais links são especificados nas configurações de comunicação do agente, na seção Atalhos do ícone Status do agente.

Links URI (Uniform Resource Identifier, identificador uniforme de recurso) padrão são suportados, como URLs HTTP, SSH e FTP. Clicar neste link faz com que o sistema inicie o aplicativo associado ao recurso selecionado. Por exemplo, ao clicar em um link do tipo HTTP, seu sistema abre o link no navegador padrão.

- **Inventário Hyper-V:** As informações de inventário e os comandos de dispositivos relacionados foram adicionados nesta versão para os dados do Virtual Machine Manager e do MS Hyper-V, para dispositivos

gerenciados por agente. Os detalhes do inventário incluem uma lista de máquinas virtuais e hosts do Hyper-V para inventário. Isso é semelhante ao recurso de inventário VMware criado na versão 10.0.

- **Atualizações de suporte do sistema operacional:** A solução agora é compatível com as seguintes versões de SO em dispositivos gerenciados por agente:
  - MS Windows 10 20H2
  - MS Windows Server 2019 20H2
  - macOS 11.0
    - Ao se conectar ao **Console do usuário** usando HTTPS de um sistema macOS 11.0, a solução não pode determinar o KUID (identificador exclusivo) do agente associado a esse sistema. Isso afeta a lista *Meus dispositivos* e as instalações da biblioteca de software. A causa raiz desse problema é o novo requisito para o macOS 11.0 de que todas as configurações de confiança do certificado devem ser aprovadas pelo usuário. Esse problema também faz com que a seguinte entrada apareça no `konea.log` no agente:

```
|ERROR|ssl_darwin.go:107:AddCertAsTrustedRoot |
SecTrustSettingsSetTrustSettings failed|{kbin"err":"A autorização foi
negada, pois a interação do usuário não foi possível."}
```
    - O dispositivo é compatível com aplicação de patches de sistema operacional para esta versão. Aplicação de patches do aplicativo estão disponíveis. Aplicação de patches no nível do SO para dispositivos macOS 11.0 estão disponíveis com o KACE Cloud Mobile Device Manager (MDM), se você tiver uma assinatura.

#### Aplicação de patches

- **Atualizações de pacote Linux:** O dispositivo agora permite automatizar o processo de instalação e gerenciamento de atualizações de pacotes do Linux que mantém o SO Linux atualizado em seus dispositivos gerenciados Linux RedHat, SUSE, Ubuntu, CentOS e Raspbian. Essas atualizações melhoram o desempenho geral de seus dispositivos gerenciados Linux e os protegem contra possíveis vulnerabilidades.

Use esse recurso para criar programações de atualização que permitam detectar atualizações de pacotes ou detectar e atualizar todos os pacotes aplicáveis. É possível analisar a lista de atualizações de pacotes disponíveis após uma ação de agendamento somente detecção, para cada tipo de Linux.

O processo de atualização se baseia na suposição de que seus dispositivos gerenciados Linux apontam para os repositórios de pacotes apropriados. Somente os pacotes que incluem atualizações de segurança são identificados. A solução não tenta detectar nem atualizar todos os pacotes nem todo o SO para a versão mais recente.



**NOTA:** O Raspbian Linux não faz distinção entre atualizações regulares e de segurança. Detectar e atualizar pacotes para dispositivos gerenciados Raspbian resulta na instalação de todos os pacotes atualizados nesses dispositivos.

- **Integração com o novo catálogo de atualização de hardware da Dell:** A partir desta versão, o equipamento usa uma nova versão do catálogo de hardware da Dell. O processo de detecção e implantação de atualizações de hardware é muito semelhante ao usado para a aplicação de patches em dispositivos. Comece criando atualizações de programação para detectar, implantar ou detectar e implantar atualizações de hardware. É possível revisar a lista de atualizações da Dell disponíveis na página do catálogo. Esta página lista as atualizações para as quais existem arquivos de assinatura na solução.
  - Este recurso requer a versão mais recente do agente do KACE para ser executado em dispositivos gerenciados Dell.
  - Os dados existentes relacionados às atualizações de hardware da Dell, como histórico de programação, não são migrados de versões anteriores do dispositivo.
  - Os relatórios de usuário associados às atualizações de hardware da Dell e criados com uma versão anterior do dispositivo não são migrados para a versão 11.1.

## Infraestrutura

- **Oval para Linux e Mac:** Nesta versão, a solução estende o suporte Oval além do exclusivo para MS Windows, usando a maior e melhor seleção de dados CVE do mundo.
- **Alertas de renovação de licença:** Quando a manutenção da solução expira, alguns recursos, como suporte a patches, ficam indisponíveis. Isso faz com que um alerta de erro seja exibido no Painel inicial. Para renovar sua licença, acesse <https://support.quest.com/contact-us/renewals>.

## Service desk

- **Hierarquia de categorias de tíquetes do Service Desk:** O Console do administrador foi aprimorado para permitir a simplificação da configuração de categorias e subcategorias para o Service Desk. É possível criar e editar categoria de tíquete e nós de subcategoria usando um widget de árvore. A exibição em árvore permite que você entenda melhor e gerencie as relações entre as categorias. É possível adicionar facilmente novos nós de categoria, renomear, excluir ou classificá-los, conforme necessário. Uma função de pesquisa também está disponível para localizar rapidamente uma categoria ou subcategoria específica.
- **Capacidade de especificar o prefixo do tíquete do Service Desk:** A partir desta versão, é possível usar um prefixo diferente para cada fila para organizar o fluxo de trabalho do Service Desk e associá-las a categorias aplicáveis, como `HELP`: para Helpdesk ou `HDREQ`: para requisições de hardware e software.
- **Suporte ao Microsoft 365 GCC High Service:** Suas credenciais OAuth do MS Office 365 agora permitem que você especifique o tipo de locatário do Azure AD e o URL do endpoint para adquirir tokens para a nuvem nacional associada ao seu ambiente. Ao selecionar um OAuth do Office 365 para e-mails de entrada do Service Desk, é possível apontar para um serviço de API do Microsoft 365 aplicável, como Microsoft 365 GCC, Microsoft 365 GCC High e outros. O Microsoft 365 GCC High em particular é usado em ambientes de alta segurança.

# Aprimoramentos

Veja a seguir uma lista de melhorias implementadas nesta versão.

Aprimoramento	ID do problema
Windows Installer now preserves the <code>NoHooks</code> <code>userinit</code> registry setting during upgrade.	K1A-2393
Managed Installation can continue if the Agent disconnects.	K1A-2392
KACE Agent no verifies the Konea tunnel and alerts the server if broken.	K1A-2384
The user is alerted when reboot is pending and patching operations are skipped as a result.	K1A-2381
11.1 KACE macOS agents use PKG installer file rather than DMG disk image.	K1A-2374
API access can now be restricted through the <i>Access Control List Details</i> page.	K1-30596
This version includes the ability to sort by custom ticket fields in KACE GO.	K1-30562
SAML-enabled systems can now be locked down to allow access only to SAML-authenticated users and the local <code>admin</code> user.	K1-30246

<b>Aprimoramento</b>	<b>ID do problema</b>
This version includes an option to reject SAML users who do not already have an account on the appliance.	K1-30211
<i>Approval Status</i> column is added to the <i>Quarantine</i> list and <i>Quarantine Detail</i> pages.	K1-30105
In the <i>General Settings</i> page, an option is added to indicate interest in participation in a future Beta program.	K1-30071
The appliance now includes the ability to select an Azure AD <i>GCC High account</i> during the creation of credentials for a Office365 OAuth account, and to set the URL endpoint for a .us domain.	K1-22281
In the email notification text editor, the <b>\$</b> button now allows insertion of tokens.	K1-22082
Added the ability to select a <i>single-tenant</i> Azure AD account type during the creation of credentials for a Office365 OAuth account.	K1-21914
User's manager can now be reset to <i>Unassigned</i> either manually through the <b>Console do administrador</b> , or during LDAP import with an empty manager mapped field.	K1-19328
Discovery schedules for devices associated with an Active Directory server, now include a new option for enabling the appliance to use a secure port for LDAP communication, <b>Use Secure LDAP (LDAPS)</b> . This check box is available in the <i>Active Directory</i> section on the <i>Discovery Schedule Detail</i> page, when you select <b>Active Directory</b> as the <i>Discovery Type</i> .	N/A
Access Control List restrictions can be now applied based on sub-domains. You can specify the sub-domain name on the <i>Access Control List</i> page, in the <i>IP Address/Domain</i> column of the <i>Allow List</i> .	N/A

## Problemas resolvidos

Veja a seguir uma lista dos problemas resolvidos nessa versão.

### Resolved Service Desk issues

<b>Problema resolvido</b>	<b>ID do problema</b>
Creating a Service Desk process template that included a separator could result in an error when used from the User Portal.	K1-30698
<i>Time Closed</i> , <i>Time Stalled</i> and <i>Time Opened</i> are not updated for a parent ticket with approvals.	K1-30685
When copying text from a Word application to a ticket, the formatting could not be retained.	K1-30545
When duplicating a process, the ticket template was not duplicated.	K1-30460

<b>Problema resolvido</b>	<b>ID do problema</b>
Tickets with very long summary fields could result in an error when the <i>Tickets</i> list page loads.	K1-23726
Default ticket template is not set when creating a new ticket by email.	K1-23422
Unexpected rendering behavior (scrolling) could be seen when viewing ticket details when multiple categories and sub-categories are present.	K1-22645
In the Service Desk list view, <i>Time Open</i> and <i>Time Opened</i> are renamed to <i>Time Since Last Opened</i> and <i>Last Opened</i> , respectively.	K1-22630
Emails sent with display names with a comma or multi-language character to a Service Desk queue through POP3 was not handled correctly, in some cases.	K1-22610
Image was broken using several variables in email templates.	K1-21347
<i>Email On Event</i> ticket notification emails were formatted differently than Custom Ticket Rule emails.	K1-21198
Default value was not displayed on ticket detail page for drop-down fields with <i>Always Required</i> option.	K1-21187
Service Desk: Token emails from Gmail to Gmail leaved behind empty spaces.	K1-21186
When a ticket is submitted by email with embedded dark colors, the text was hidden if the <b>Console do administrador</b> is also set to a dark theme.	K1-21147
Process parent ticket did not close if child tickets were closed from <i>Tickets</i> list view.	K1-21143
Service Desk email notifications broke if templates exceeded character limits.	K1-21118
Advanced Search: Filters did not work as expected when using Unassigned Owner.	K1-21116
Advanced Search in <i>Tickets</i> list: Filters did not work as expected when using <i>Status</i> and <i>Process Status</i> .	K1-21107
Populating a Service Desk ticket multi-selection custom field with double quotes in the select value resulted in unexpected behavior.	K1-21094
Ticket attachment links sent in email notifications did not work as expected in some cases.	K1-19964

#### Resolved KACE Agent issues

<b>Problema resolvido</b>	<b>ID do problema</b>
CentOS receives all updates with the Linux Update feature. The security filter is not available for the Linux Package Upgrades page.	K1A-3810
KACE Agent 11.0 failed to download file from HTTPS source, impacting use of replication shares that are accessed through the HTTPS protocol.	K1A-2330

<b>Problema resolvido</b>	<b>ID do problema</b>
Client certificate install operation could timeout on newly provisioned Windows devices, preventing the agent from receiving any commands from the appliance until a reconnect event happened.	K1A-2329
VMM managed Hyper-V host was not added to appliance during VMM inventory when the Agent is installed on some Hyper-V hosts.	K1A-2328
Replication did work when password had an '@' symbol.	K1A-2326
macOS 11.0 (Big Sur): Installing KACE Agent with the Agent Status icon enabled resulted in warnings during installation.	K1A-2318
<code>konea.exe</code> and <code>clientidentifier.exe</code> could crash in some environments.	K1A-2291
Recurring Alert messages kept spawning new Windows on endpoint.	K1A-2289
Wake-on-LAN (WoL) through relay did not display error when the relay agent selected was down.	K1A-2285
Tokens were treated as invalid by agents (error: Agent token signed by another server) if the appliance database became out of sync with the file system.	K1-30642
SNMP inventory data from Dell servers could cause inventory to fail.	K1-30615
In the <b>Console de administração de sistema</b> , on the <i>Agent Token Detail</i> page, <i>Organization</i> is represented with its ID instead of name.	K1-29969
Offline KScripts did not run when scheduled for <i>Run on the instance/day of week</i> .	K1-21173
MSI Policy wizard script could fail to set the registry value correctly.	K1-21049
Scripting option <i>Allow run without a logged-in user</i> cleared still allowed script to run.	K1-19576
SMB URLs did not properly handle passwords with special characters.	K1-17342

#### Resolved Inventory issues

<b>Problema resolvido</b>	<b>ID do problema</b>
SNMP inventory mistakenly identified non-hex strings as hex strings, causing incorrect values in some cases.	K1-30668
Dell Warranty retrieval errors were not logged to the new <code>dell_warranty_log</code> error file.	K1-30531
Overdue Service Desk widgets included tickets that were not yet overdue.	K1-30480
In the <b>Quarantine</b> list page, it was not possible to view the details of a quarantined device.	K1-24508
Viewing script logs from the <i>Device Detail</i> page displayed blank logs.	K1-21349



Problema resolvido	ID do problema
<b>Reset Tries</b> button in <i>Windows Feature Updates Status</i> on <i>Device Detail</i> page did not always work.	K1-21172
<i>Gateway IP Address</i> was not an available column on the <i>Devices</i> list page.	K1-21131
Machine deletion could lead to software installation counts being inaccurate.	K1-20437
No history was tracked when Smart Label was edited.	K1-17612

#### Other resolved issues

Problema resolvido	ID do problema
The <i>Windows Feature Update Summary</i> page did not correctly list all updates, in some cases.	K1-30887
Knowledge Base articles with multiple labels could be hidden for users.	K1-30671
LDAP Import: Scheduled imports set to <i>None</i> could still run automatically.	K1-30666
<i>Compliance by Patch</i> and <i>Compliance by Machine</i> widgets sometimes did not display correct values.	K1-30630
Images did not appear correctly in knowledge base articles, in some cases.	K1-30565
Emails with multiple CC's sent to a Service Desk queue through a POP3 server could not be handled correctly.	K1-30533
File attachments of type .eml or .msg were missing from tickets submitted by email.	K1-30527
Managed Installation with <b>Override default installation</b> configured would show <b>Default installation</b> set after saving.	K1-30481
An error could be seen while creating custom view on the <i>Quarantine</i> page in the <b>Console de administração de sistema</b> .	K1-29978
<b>Do not associate file</b> Managed Installation option was not displayed correctly after saving.	K1-29927
In some cases, the network settings for the proxy settings were not honored by the Credential manager when using an Office365 OAuth account.	K1-29063
Access to the <b>Console do administrador</b> could be disrupted when changing an organization's virtual IP address or host name.	K1-25452
Email sent to Service Desk queues that use a multi-part MIME format could fail to parse correctly.	K1-22656
When a non-administrative queue owner attempts to retrieve the list of Service desk tickets using the API, tickets they did not submit could be omitted from the results.	K1-22653

Problema resolvido	ID do problema
SFTP- and FTP-specific <i>Offboard Backup Transfer Settings</i> fields containing backslashes caused offboard backup failure.	K1-22608
The <i>Object History</i> page sometimes failed to load when it contained Windows Feature Update data.	K1-21575
Agent upstream tunnel client certificate validation failed when an aging konea certificate was archived.	K1-21354
In KACE GO it was not possible to accept barcode searches that have embedded spaces or new line characters.	K1-21195
SAML LDAP attribute mapping option could cause authentication failures.	K1-21193
Asset import did not change Assignee information.	K1-21185
Code can now be saved in the <i>Notes</i> field of KScripts.	K1-21184
Monitoring: Create Ticket in Profile configuration did not select proper queue ID.	K1-21175
Search on <i>Device Issues</i> page did not function as expected.	K1-21169
SAML: Editing SP Metadata for <code>NameIDFormat</code> did not save changes.	K1-21139
Unexpected behavior observed when trying to map and update <i>Manager</i> field using SAML.	K1-21102
Default role for new users did not always honor the role chosen in <i>Settings</i> .	K1-21082
<i>Alternate location</i> for Managed Installation was not used behind a replication share.	K1-21016
Location was unassigned on asset when a new or previously removed device connects.	K1-20468
The <b>Generate Self-Signed Certificate</b> button was incorrectly enabled before the configuration information was saved in the SSL wizard.	K1-18300

## Problemas conhecidos

No momento desta versão, sabe-se que os seguintes problemas existem.

Problema conhecido	ID do problema
KACE Agent for SUSE 11.1 requires <code>libxslt</code> to be installed in order to install. This is a newly introduced dependency.	K1A-3813
Disk Usage history is not recorded by a macOS KACE Agent of an APFS file system.	K1A-3805

Problema conhecido	ID do problema
The appliance reports the MS Windows 10 build number 20H2 through its technical release version of 2009.	K1A-3803
Dell Updates: Custom View does not report any results when Smart Label is a criteria.	K1-31860
Email attachments in .eml and .msg file format are marked as <i>discarded</i> if subject contains slashes '/	K1-31786
Linux package upgrades: <i>Deploy All</i> can push some updates that change system configuration which requires manual reconfiguration, such as on Ubuntu 18.04LTS (Desktop version with UI).	K1-31770
KACE GO: Non-admin queue owners cannot to set ticket device/asset to arbitrary device.	K1-31764
Windows Feature Update (WFU) schedule fails when using a deployment type of <i>Detect and Stage</i> type and the Agent version is 10.2.	K1-31743
Wake-on-LAN (WoL) options are not present in the <b>Choose Action</b> menu on the <i>Device Detail</i> page for supported devices.	K1-31729
Duplicating patch schedule from list of schedules does not work as expected.	K1-31714
Duplicating Dell Updates schedule from list of schedules does not work as expected.	K1-31713
Users with no queue permissions cannot see tickets they are CC-ed on.	K1-31710
Downloading status count is not displayed in <i>Patch Schedules</i> list page.	K1-31066
<i>Managed Installation Detail</i> page incorrectly shows that PKG files cannot be used.	K1-30820
Patching step with reboot in <i>Task Chain</i> shows Failed status.	K1-30812
Patch schedule with On-Demand Deploy ends Task Chain task when staging is completed.	K1-30811
Patch schedule information is not showing correctly after disabling a patch schedule.	K1-30733
Schedule information is not showing correctly after disabling a Linux package upgrade schedule.	K1-30725
Pasting an image into a knowledge base article causes other pasted images to reset alignment and justification.	K1-30721
Package download process incorrectly updates offline <i>Last Modified</i> instead of <i>Last Update</i> status.	K1-30588
Invalid filters (Smart Labels) can be saved, resulting in Smart Labels that never populate.	K1-20268

# Requisitos do sistema

A versão 11.0 é a versão mínima obrigatória para a instalação da Solução de gerenciamento de sistemas KACE 11.1. Se a solução estiver sendo executada em uma versão anterior, é necessário atualizar para a versão indicada antes de continuar a instalação.

A versão mínima obrigatória para atualizar o agente do KACE é 10.2. Recomendamos executar a versão mais recente do agente com a Solução de gerenciamento de sistemas KACE 11.1.



**NOTA:** O pacote RPM do agente do KACE pode ser instalado em dispositivos gerenciados SUSE Linux somente quando o pacote `libxslt-tools` é instalado antes do pacote do agente.

Para verificar o número da versão da solução, faça login no **Console do administrador** e clique em **Need Help** (Precisa de ajuda?). No painel de ajuda que é exibido, na parte inferior, clique no botão circulado "i".

Antes de atualizar ou instalar a versão 11.1, certifique-se de que seu sistema atende aos requisitos mínimos. Esses requisitos estão disponíveis nas especificações técnicas da Solução de gerenciamento de sistemas KACE.

- Para soluções virtuais: Acesse <https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/technical-specifications-for-virtual-appliances/>.
- Para KACE como um serviço: Acesse <https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/technical-specifications-for-kace-as-a-service/>.

# Licenciamento do produto

Se você possui atualmente uma licença de produto da Solução de gerenciamento de sistemas KACE, não é necessária nenhuma licença adicional.

Se você estiver usando a Solução de gerenciamento de sistemas KACE pela primeira vez, consulte o guia de configuração da solução para obter os detalhes de licenciamento do produto. Acesse [Mais recursos](#) para exibir o guia correto.



**NOTA:** As licenças de produto da versão 11.1 podem ser usadas apenas na Solução de gerenciamento de sistemas KACE versão 11.1 ou mais recente. As licenças da versão 11.1 não podem ser usadas em soluções que executam versões anteriores da solução, como a 10.0.

# Instruções de instalação

Você pode aplicar esta versão usando uma atualização anunciada ou carregando e aplicando um arquivo de atualização manualmente. Para obter instruções, consulte os seguintes tópicos:

- [Preparar para a atualização](#)
- [Atualizar o servidor da Solução de gerenciamento de sistemas KACE usando uma atualização anunciada](#)
- [Carregar e aplicar uma atualização manualmente](#)
- [Tarefas pós-atualização](#)



**NOTA:** Para garantir a precisão da descoberta do software e instalar contagens para dispositivos que executam um software específico, a partir da versão 7.0 da Solução de gerenciamento de sistemas KACE, o catálogo de software é reinstalado a cada atualização.

# Preparar para a atualização

Antes de atualizar seu servidor da Solução de gerenciamento de sistemas KACE, siga estas recomendações:

- **Verifique a versão do servidor da Solução de gerenciamento de sistemas KACE:**

A versão 11.0 é a versão mínima obrigatória para a instalação da Solução de gerenciamento de sistemas KACE 11.1. Se a solução estiver sendo executada em uma versão anterior, é necessário atualizar para a versão indicada antes de continuar a instalação.

Para verificar o número da versão da solução, faça login no **Console do administrador** e clique em **Need Help** (Precisa de ajuda?). No painel de ajuda que é exibido, na parte inferior, clique no botão circulado "i".

- **Verifique a versão do seu agente do KACE.**

A versão mínima obrigatória para atualizar o agente do KACE é 10.2. Recomendamos executar a versão mais recente do agente com a Solução de gerenciamento de sistemas KACE 11.1.



**NOTA:** O pacote RPM do agente do KACE pode ser instalado em dispositivos gerenciados SUSE Linux somente quando o pacote `libxslt-tools` é instalado antes do pacote do agente.

- **Faça um backup antes de iniciar.**

Faça backup do banco de dados e dos arquivos e salve os backups em um local fora do servidor da Solução de gerenciamento de sistemas KACE para usar como referência. Para instruções sobre como realizar o backup do banco de dados e dos arquivos, consulte **Guia do administrador**, <https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-guide/>.

- **Soluções instaladas antes da versão 7.0.**

Para soluções inicialmente instaladas antes da versão 7.0 cuja imagem não foi recriada (soluções físicas) ou reinstalada (virtuais), a Quest Software recomenda a exportação, a recriação (uma imagem ou uma instalação de máquina virtual com base em um arquivo OVF) e a reimportação do banco de dados antes de atualizar para a versão 11.1. Para obter informações completas, visite <https://support.quest.com/kace-systems-management-appliance/kb/111810/how-to-re-image-the-k1000-appliance>.

Se a versão da solução estiver muitas versões atrás, o seguinte artigo conterà dicas úteis relacionadas à atualização: <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->.

Há muitos motivos pelos quais você deve recriar a imagem da solução. O novo layout de disco, por exemplo, oferece melhor compatibilidade com a versão 11.1. Ele também apresenta segurança e desempenho melhores.

Para determinar se o sistema se beneficiaria dessa atualização, você pode usar um arquivo `KBIN` para determinar a idade exata da sua solução e o layout do disco. Para baixar o `KBIN`, visite <https://support.quest.com/kace-systems-management-appliance/kb/210267/how-to-run-the-kace-systems-management-appliance-configuration-report>.

- **Certifique-se de que a porta 52231 esteja disponível.**

Antes de qualquer atualização de `.kbin`, a porta 52231 deve estar disponível para que a página do Console de Atualização do KACE fique acessível. Se a atualização for iniciada sem disponibilizar essa porta, você não poderá monitorar o andamento da atualização. A Quest KACE recomenda enfaticamente permitir o tráfego até a solução pela porta 52231 proveniente de um sistema confiável e monitorar a atualização no Console de Atualizações. Sem acesso ao Console de Atualização, a atualização é redirecionada para uma página inacessível que aparece no navegador como tempo limite. Isso pode levar alguém a acreditar que a atualização travou o sistema, fazendo com que essa pessoa reinicie o computador quando, na verdade, a atualização ainda está em andamento. Se não tiver certeza sobre o andamento da atualização, entre em contato com o Suporte KACE e **não reinicialize a solução**.

# Atualizar o servidor da Solução de gerenciamento de sistemas KACE usando uma atualização anunciada

Você pode atualizar o servidor da Solução de gerenciamento de sistemas KACE usando uma atualização anunciada na página *Painel* ou na página *Atualizações da solução* do **Console do administrador**.

**! CUIDADO:** Nunca reinicie o servidor da Solução de gerenciamento de sistemas KACE manualmente durante uma atualização.

1. Faça o backup do seu banco de dados e arquivos. Para obter instruções, consulte o **Guia do administrador** em <https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-guide/>.
2. 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: Faça login no **Console de administração de sistema da solução**: `http://KACE_SMA_hostname/system`, ou selecione **Sistema** na lista suspensa no canto superior direito da página e clique em **Configurações**.
3. Na barra de navegação esquerda, clique em **Atualizações da solução** para exibir a página *Atualizações da solução*.
4. Clique em **Verifique atualizações**.

Os resultados da verificação aparecem no registro.

5. Quando uma atualização estiver disponível, clique em **Atualizar**.

**i IMPORTANTE:** Durante os primeiros dez minutos, alguns navegadores talvez pareçam estar paralisados enquanto a atualização estiver sendo descomprimida e verificada. Não saia da página nem a atualize ou clique em outros botões do navegador durante esse tempo, porque essas ações interrompem o processo. Depois que a atualização for descomprimida e verificada, a página *Registros* aparece. Não reinicialize manualmente a solução durante nenhuma parte do processo de atualização.

Quando a versão 11.1 é aplicada, o servidor da Solução de gerenciamento de sistemas KACE reinicia. O andamento aparece na janela do navegador e no **Console do administrador**.

6. Quando a atualização do servidor estiver concluída, atualize todos os seus agentes para a versão 11.1.

## Carregar e aplicar uma atualização manualmente

Se tiver um arquivo de atualização da Quest, é possível carregá-lo manualmente para atualizar o servidor da Solução de gerenciamento de sistemas KACE.

**! CUIDADO:** Nunca reinicie o servidor da Solução de gerenciamento de sistemas KACE manualmente durante uma atualização.

1. Faça o backup do seu banco de dados e arquivos. Para obter instruções, consulte o **Guia do administrador** em <https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-guide/>.
2. Usando suas credenciais de login de cliente, faça login no site da Quest em <https://support.quest.com/kace-systems-management-appliance/download-new-releases>, faça o download do arquivo `.kbin` do

servidor da Solução de gerenciamento de sistemas KACE referente à versão 11.1 GA (disponibilidade geral) e salve o arquivo localmente.

3. Na barra de navegação esquerda, clique em **Atualizações da solução** para exibir a página *Atualizações da solução*.
4. Na seção *Atualizar manualmente*:
  - a. Clique em **Procurar** ou **Escolher arquivo** e localize o arquivo de atualização.
  - b. Clique em **Atualizar** e em **Sim** para confirmar.

Quando a versão 11.1 é aplicada, o servidor da Solução de gerenciamento de sistemas KACE reinicia. O andamento aparece na janela do navegador e no **Console do administrador**.

5. Quando a atualização do servidor estiver concluída, atualize todos os seus agentes para a versão 11.1.

## Tarefas pós-atualização

Após a atualização, verifique se ela foi bem-sucedida e se as configurações são necessárias.

### Verificar conclusão com êxito

Verifique se a conclusão foi bem-sucedida visualizando o número de versão da Solução de gerenciamento de sistemas KACE.

1. 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: Faça login no Console de administração de sistema da solução: `http://KACE_SMA_hostname/system`, ou selecione Sistema na lista suspensa no canto superior direito da página e clique em Configurações.**
2. Para verificar a versão atual, clique em **Precisa de ajuda?** no canto direito superior da página e, no painel de ajuda que aparece na parte inferior, clique no botão circulado "i".

### Verificar configurações de segurança

Para aumentar a segurança, o acesso ao banco de dados através de HTTP e FTP é desativado durante a atualização. Se você usar esses métodos para acessar os arquivos do banco de dados, altere as configurações de segurança após a atualização, conforme necessário.

1. 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: Faça login no Console de administração de sistema da solução: `http://KACE_SMA_hostname/system`, ou selecione Sistema na lista suspensa no canto superior direito da página e clique em Configurações.**
2. Na barra de navegação esquerda, clique em **Configurações de segurança** para exibir a página *Configurações de segurança*.
3. Na parte superior da página, altere as seguintes configurações:
  - **Habilitar arquivos de backup seguros:** Desmarque esta caixa de seleção para permitir que os usuários acessem os arquivos de backup do banco de dados usando HTTP sem autenticação.
  - **Habilitar acesso ao banco de dados:** Marque esta caixa de seleção para permitir que os usuários acessem o banco de dados pela porta 3306.
  - **Habilitar backup via FTP:** Marque esta caixa de seleção para permitir que os usuários acessem os arquivos de backup do banco de dados usando FTP.



**CUIDADO:** A alteração dessas configurações diminui a segurança do banco de dados e não é recomendada.

4. Clique em **Salvar**.
5. **Apenas upgrades de KBIN.** Fortaleça o acesso à solução com senha raiz (2FA).
  - a. No Console de administração de sistema, clique em **Configurações > Suporte**.
  - b. Na página *Suporte*, em *Ferramentas de solução de problemas*, clique em **Autenticação de dois fatores**.
  - c. Na página *Suporte a autenticação de dois fatores*, clique em **Substituir chave secreta**.
  - d. Registre os tokens e coloque essas informações em um local seguro.

## Mais recursos

Informações adicionais estão disponíveis em:

- Documentação on-line do produto (<https://support.quest.com/kace-systems-management-appliance/11.1/technical-documents>)
  - **Especificações técnicas:** Informações sobre os requisitos mínimos para instalação ou atualização para a última versão do produto.  
**Para soluções virtuais:** Acesse <https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/technical-specifications-for-virtual-appliances/>.  
**Para KACE como um serviço:** Acesse <https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/technical-specifications-for-kace-as-a-service/>.
  - **Guias de configuração:** Instruções para configurar soluções virtuais. Vá para <https://support.quest.com/kace-systems-management-appliance/11.1/technical-documents> para visualizar a documentação da versão mais recente.
  - **Guia do administrador:** Instruções para utilizar a solução. Vá para <https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-guide/> para visualizar a documentação da versão mais recente.

## Globalização

Esta seção contém informações sobre a instalação e operação deste produto em configurações em idiomas diferentes do inglês, necessários para os clientes fora da América do Norte. Esta seção não substitui os materiais sobre plataformas suportadas e configurações encontradas em qualquer lugar na documentação do produto.

Esta versão é habilitada em Unicode e oferece suporte a qualquer conjunto de caracteres. Nesta versão, todos os componentes do produto devem ser configurados para usar as mesmas codificações de caracteres ou codificações compatíveis e devem ser instalados para usar as mesmas opções de localidade e região. Esta versão é direcionada para oferecer suporte a operações nas seguintes regiões: América do Norte, Europa Ocidental e América Latina, Europa Central e Leste Europeu, Extremo Oriente, Japão.

A versão está localizada nos seguintes idiomas: francês, alemão, japonês, português (Brasil), espanhol.

## Sobre nós

A Quest cria soluções de software que tornam reais os benefícios da nova tecnologia em um cenário de TI cada vez mais complexo. Desde o gerenciamento de banco de dados e de sistemas até o gerenciamento do



Active Directory e do Office 365 e a resiliência da segurança cibernética, a Quest ajuda os clientes a resolver seu próximo desafio de TI imediatamente. Em todo o mundo, mais de 130.000 empresas e 95% das empresas da Fortune 500 confiam na Quest para oferecer gerenciamento e monitoramento proativos para a próxima iniciativa empresarial, encontrar a próxima solução para desafios complexos da Microsoft e ficar à frente da próxima ameaça. Quest Software. Onde o futuro encontra o presente. Para obter mais informações, visite [www.quest.com](http://www.quest.com).

## Recursos de suporte técnico

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

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

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

## Avisos legais

© 2021 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.

## Patentes

Nós, da Quest Software, temos orgulho da nossa tecnologia avançada. Patentes em vigor e pendentes podem se aplicar a este produto. Para informações atualizadas sobre as patentes aplicáveis a este produto, acesse nosso site em <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.

## Legenda



**CUIDADO:** Um ícone de AVISO indica um potencial de danos ao hardware ou a perda de dados se as instruções não forem seguidas.



**IMPORTANTE, NOTA, DICA, MÓVEL ou VÍDEO:** Um ícone de informações indica informações de suporte.

Notas de versão da Solução de gerenciamento de sistemas KACE

Atualizado em abril de 2021

Versão do software - 11.1