Dell KACE™ K1000 Systems Management Appliance 7.0

Release Notes

November 2016

These release notes document provides information about the K1000 Systems Management Appliance version 7.0.

Topics:

About K1000 Systems Management Appliance 7.0

K1000 Systems Management Appliance is a physical or virtual appliance designed to automate device management, application deployment, patching, asset management, and Service Desk ticket management. For more information about K1000 series appliances, go to http://software.dell.com/products/kace-k1000-systems-management-appliance/.

New features and enhancements

The following K1000 Systems Management Appliance modules include new features and enhancements in this release:

- Location improvements on page 10
- Cross-appliance reporting on page 10
- Agent-based device management on page 11
- Agentless device management on page 11
- Monitoring on page 13
- Security and configuration on page 13
- API support on page 14

IMPORTANT: In this release, the AMP protocol and AMPAgent service, are replaced with the Konea service and protocol. For more information, see Agent-based device management on page 11.

For complete information about these features, see the *Administrator Guide*.

To find out more about the new features in this release, watch the video tutorials available on our Support site: https://support.quest.com/k1000-systems-management-appliance/kb/video-articles?k=what%27s+new.

Service Desk and User Console

The Service Desk and User Console include the following new features and enhancements:

- Queue configuration on page 2
- Workflow process on page 3
- Workflow approvals on page 4

Queue configuration

This release includes the following queue configuration features:

- **Validation of queue SMTP settings**. Queue SMTP settings include a user name, password, server name, and port number. Failing to provide this information could prevent emails from being sent to specific users. A validation process is added in this release to ensure that these values are added when the SMTP settings are enabled.
- **Ability to display comments on the New Ticket page**. The *Queue Customization* page now allows you to indicate if you want to display comments and attachments on the ticket page. You can select or clear this option as required:
  - **Display comments in tickets**: By default, this option is only turned on for the existing queues that do not display the Summary field on the ticket page.
  - **Display attachments in tickets**: By default, this option is turned on for new and existing queues.
- **Adding comments to a ticket results in email notifications**. Email notifications are sent when a comment is added to a ticket, after using the **Save** or **Apply** button on the ticket page.
- **Enhanced ticket input form customization** . The *Layout Ticket Fields* section on the *Queue Customization* page is updated to give full control to Administrators over the visibility and placement of the fields appearing on the *New Ticket* page.

- **Ticket layout previews.** While customizing the ticket layout, administrators now have the ability to preview how a specific ticket layout is displayed in different modes before the changes are saved(*New Ticket* page: Administrator, *New Ticket* page: User, *Ticket Detail* page: Administrator, *Ticket Detail* page: User).
- **Ability to display sub-categories when filtering or reporting on a parent category**. Selecting a parent category through a custom view, search or report results in displaying all tickets from the parent category and all related sub-categories.

Workflow process

This release includes the following process features:

- **Process improvements**.
  - The new *Create Process Template* wizard is added in this release to allow you to create process templates. Use a process template (previously known as *process*) when you want to create process tickets that contain related tasks.
  - The wizard provides an intuitive workflow for specifying approval and ticket workflows and notifications. If you choose to use the process status workflow instead of the ticket workflow, the associated parent ticket automatically advances through various process-specific states. If you choose not to select this option and use ticket workflows, you must create custom ticket rules to achieve an approval and notification functionality, as required.
  - Process steps can be hidden from end users, if needed.
  - Process owners and submitters have the ability to cancel a process at any time so that no further work is done on this process. A process cancellation is recorded in the process ticket history.
  - The *All Tickets by Process Status* and *My Tickets by Process Status* views are added to the *Tickets* page.
- **Updates to the Tickets page**.
  - The *Process* column on the *Tickets* page indicates if a ticket is based on a process template (*Yes* or *No*).
  - The *Process Type* and *Ticket Type* columns are added to the *Tickets* page. For process-based ticket, the *Status* column displays the related process status.
  - New out-of-the-box system views are added in this release: *By Process Type* and *By Process Status*.

  Updates to the Custom View and Advanced Search. These views now include the process Status and Type options. You can use them to search for specific process type or status.
- **Updates to the Process Templates**.
  - The following columns are added to *Process Templates* list: *Process Type* and *Approval Required* (*Yes* or *No*).
  - The column *All Users* is renamed to *Visibility*. It displays *All Users* or the appropriate comma-separated label names.
  - The column *Status* is renamed to *Enabled*. It is set to *Yes* or *No*.
  - The *Description* column is removed from the list.
  - When configuring a process template, Administrators can automatically configure either the child ticket owner or submitter as the parent ticket owner or submitter, so that they can set the default users on a process dynamically, based upon how the initial parent ticket was submitted.

- It is now possible to differentiate between various process types when managing and reporting on tickets, such as Change Records and Service Requests.
- The *Ticket Detail* page for the parent ticket associated with a process includes the *Process Type* and *Process Status* fields.
- Process owners can move the process to a Completed status at any time, to indicate that the process is completed successfully, even if all of the approvals or child tickets may not be updated properly in the system.
- When a new process-based ticket is created, the first step is to view the process name and description. The contents of this page allow HTML/Markdown content and hyperlinks, as configured for the process. This page can be hidden, when required, by clearing the **Display process description page while creating new process requests** check box on the *Publish Options* page of the *Create Process Template* wizard. When you click *Continue* on the process name and description page, the *New Ticket* page appears, allowing you to specify the parent ticket details.
- Administrators can configure automatic email notifications for different events within the task workflow in order to control the notification recipients and content for each event in the process life cycle.
- A set of email templates is available for process-related email notifications. These templates are available for selection in the *Create Process Template* wizard. A separate template needs to be created for each process event: Process Submitted, Approval Required, Approval Timed Out, Approval Received, Approval Rejected, Process Cancelled, and Process Complete.
- New email tokens are added in this release to support process-related email notifications: `$process_description`, `$process_name`, `$process_status`, and `$process_type`.

Workflow approvals

This release includes the following workflow approval features:

- **Flexible approval scenarios**. Process-based tickets can have various approval scenarios. For example, you can create process tickets that require no approvals, one, or more approvals. The process workflow starts when all applicable approvals are received. The following procedure illustrates a typical workflow:

  1 A user creates a new process-based ticket.

  2 A parent ticket is created.

  3 If any approvals are required:

    a Approval requests are sent to the approvers.

    b If approval reminders are enabled:

      - Approval reminders are sent to the approvers according to the specified schedule.

c If any approvals time out, or if any approvals are rejected:

- The process closes with the appropriate status.

d When all approval responses are received, and all approvals are granted before the time-out period ends:

- The process advances and all Stage 1 tickets are created.

4 If approvals are not required:

- The process advances and all Stage 1 tickets are created.

- **Approval configuration**.
  - Various approval scenarios that are supported, including:
    - No approval
    - Single-level approval
    - Group-level approval
    - Sequential approval

      NOTE: Each stage in the sequence can be single- or group-level approval.

  - Administrators can override approval requirement to ensure that the process can continue in case one or more of its approvers are unavailable, or may not be able to provide the necessary approval before the time-out period. This action can only be performed for processes in the Approval Pending status. It is not available for processes that are already timed out and closed due to approval denial.
  - Administrators can configure approval time-outs to specify the amount of time each ticket approver has to approve or decline a process-based ticket.
- **Approval notifications**.
  - Notifications are sent to approvers when an approval is required, allowing them to approve or reject the process and provide additional information about their action.
  - Administrators can specify a notification recurrence period for every approver.
  - All approvers are notified if their approval is no longer required due to another approval being received before they had the opportunity to approve.
- **Changes to process-based tickets**.
  - The parent process ticket inherits its status from the approval status workflow and the states of the child tickets (if applicable). If the process does not contain any child tickets, all approvals are received, the process status is set to *In Progress*, and it can be completed or cancelled by the process owner.
  - Approval-related information is displayed on the related ticket pages to ticket owners and approvers.
  - Approval-related information can optionally be displayed to non-owners.
  - A history record is created for a process ticket each time an approval is provided or timed out.

Patching and security

This release includes the following patching and security features:

- **Configuration of default patch detect and deploy time-out values**. Administrators can adjust the default patch detect and deploy time-out values, within a reasonable range.
- **Disable the patching of all devices**. The *All Devices* check box is added to the *Patch Schedule Detail* page. Selecting this option prevents technicians from inadvertently configuring a patch deployment schedule to all devices on the network, that can potentially lead to unexpected consequences, such as rebooting production systems.
- **Patching schedules**. Administrators can now schedule patching jobs using a desired schedule, as required. You can run a patch job based on a particular day of the week within a month (for example, second Wednesday of every month).

Asset Management and Inventory

This Asset Management and Inventory include the following new features and enhancements:

- Device archive on page 6
- Asset barcodes on page 6
- Associate Software Catalog titles with Managed Installations on page 7
- User portal and software downloads on page 8
- Software license management improvements on page 8

Device archive

This release includes the following device asset archiving features.

- **Archiving devices**. Administrators can archive device assets that are no longer in use. When you archive a device asset, that device is no longer included in the node license count for the K1000 appliance. Archived assets are also not listed in active inventory views or reports. Device assets marked for archiving are automatically archived after a configured time period, as specified in the *General Settings*. The default period is three days. This allows administrators to revert the device from being marked from archiving, if needed.
- **Reporting features**. The *Archive* column can be added to reports to indicate if a device is archived, pending an archive, or not archived. The Advanced Search of the *Assets* list page also allows you to filter on the *Archive Completed*, *Pending* and *Not Archived* status.
- **Ability to archive MIA devices**. You can enable the archival of MIA (missing in action) asset devices on the MIA Settings page.

Asset barcodes

This release includes the following asset barcode features:

- **Adding barcodes to assets**. A barcode allows you to create device association or to quickly retrieve device details. Barcodes can be added to asset records either by scanning them with the K1000 GO Mobile Application Scanning, by entering them manually, or by importing them from a CSV (comma-separated values) file. Standard

barcode formats are supported, such as UPC-A, Code 11, UPC-E, and others. For more information, visit https://support.software.dell.com/kb/212519.

- **Ability to scan barcodes and manage assets with the K1000 GO mobile application**.
  - The main home screen is also updated to include the **Scripting**, **Assets**, **Create Ticket**, and **Scan Barcode** buttons, providing access to these features.
  - The *Asset* home screen, added to the K1000 GO mobile application in this release, contains the **Scan Barcode** command, that allows you to scan a barcode, and associate it with an asset.
  - Scanning a barcode on an asset allows you to create a new asset, to track new inventory as it comes into the organization. An asset can have one more barcodes, as needed.
  - Location, barcode, and Service Desk ticket information appear on the asset detail page. Device inventory details are accessible from the *Assets* list page.
  - Technicians who need to find information on an asset to which they do not have direct access can search for assets and view or edit the asset information.
  - The level of user permissions controls access to the links to the asset and barcode scanning features:
    - The **Assets** and **Scan Barcode** buttons on the main home screen and the **Assets** sidebar link are only enabled for users with read and write permissions.
    - Editing asset details is only enabled for users with write permissions.
    - User with hidden access do not have access to the asset and barcode scanning features.

- **Search capabilities**. Administrators can search for a device barcode to quickly retrieve inventory information about the associated device asset.
- **Access restrictions**. Administrators can restrict access to the barcode scanning features.
- **Reporting features**. You can use the reporting wizard to report on certain attributes associated with a barcode and identify devices that are not scanned during a specific period of time.
- **Bulk uploads**. You can perform bulk uploads of multiple barcodes instead of manually entering the required information.
- **Tracking changes**. The appliance tracks changes made to the barcode field. Appliance technicians can use this information to understand important aspects like the first or last time an asset is physically scanned.
- **Searching for Dell service tags**. Appliance administrators can search the barcode field and have the appliance search for both the internal barcode syntax and the Dell service tag value in order to find a match.

Associate Software Catalog titles with Managed Installations

This release includes the following Software Catalog and Managed Installation feature:

- **Uploading and associating files with Managed Installations or the Software Catalog**. You can now associate one or more installation files with Software Catalog items. You can also choose a Software Catalog title when creating a Managed Installation.

User portal and software downloads

This release includes the following user portal and software download features:

- **Improvements to User Downloads**.
  - Administrators can display additional information about Software Catalog titles on the *User Downloads Detail* page.
  - When a user downloads a software title from the Software Catalog, the software is deployed to the device assigned to the user. If multiple devices are assigned to the user, the user can choose from the list of their assigned devices. The user's primary device is the default option.
  - The *User Downloads Detail* page makes a clear distinction between three types of software downloads: *Download* (*Cataloged* or non-cataloged *Software*), *Install* (*Managed Install* or *Default Installation*), or *Script*.
  - User installations are now queued immediately through the Run Now action.
  - The *Download History* page in the User Console displays a final status of a self-service software installation, providing an accurate history of software installed through the User Console.
  - Software installation requests for an Mac OS® system automatically execute and install after being downloaded without end-user interaction.
- **New user profile window**. The *My Profile* window, accessible by clicking the user name in the upper-right corner, lists the devices assigned to the user.
- **My Devices page**. The *My Device* page is replaced with the *My Devices* page. This page displays a list of all devices associated with the users and their inventory information.

Software license management improvements

This release includes the following software license management feature:

Administrators have a better control over how upgrade and downgrade rights are managed for the software licenses by being able to associating the versions and editions with these entitlements.

Distribution and scripting

The distribution and scripting components include the following new features and enhancements:

- Run Now for Managed Installations on page 8
- User Downloads enhancements with Managed Installations on page 9

Run Now for Managed Installations

Appliance administrators now have the option to force a Managed Installation to run immediately rather that wait for the next inventory interval, or to manually force the inventory to run on selected devices, to quickly distribute required software.

User Downloads enhancements with Managed Installations

This release includes the following user download features:

- **User Downloads Detail page improvements**. The *User Downloads Detail* page allows you to choose an existing Managed Installation. Selecting this option instructs the installation process to use the configuration options associated with the selected Managed Installation.
- **Deprecation of Microsoft® ActiveX® device actions**. ActiveX device actions are removed from the sample actions. Any existing ActiveX device actions will continue to work (if the browser supports them).

User management improvements

This release includes the following user management features:

- **General user management improvements**.
  - A user record allows multiple email addresses.
  - A default role can be configured for a user.
  - Appliance administrators can search for a user based on an extended set of user attributes (such as manager, additional email addresses, device associations, and new custom fields).
  - Appliance technicians can filter the list of users based on their hierarchal relationships, and to navigate up and down the relationship tree in order to see the associated assets at specific levels.
  - Appliance administrators can configure an LDAP import to automatically set the manager for a user based on a given attribute.
  - Appliance administrators can inspect the user hierarchy to easily identify and navigate the corporate structure when handling escalations and approval requests.
  - This release allows you to make bulk updates to existing users to quickly and easily make changes to user records without having to perform multiple changes to individual records.
  - The domain a user belongs to now appears on the *Users* and *User Detail* pages.
- **New user profile page**. The *My Profile* page allows every user to quickly change their password, review the devices and assets assigned to them, and any Service Desk tickets that they created. Users with administrative-level permissions can also edit some additional parameters, such as their name, email, manager, and locale. They can also access the *User Detail* page to review additional information about their account, and to make any changes, as needed.
- **Device/user integration**.
  - Appliance administrators can enable user accounts to reference multiple devices, and to specify a primary device.
  - Appliance technicians can assign devices to specific individuals when allocating company resources. Appliance administrators can assign devices to users in bulk.
  - The appliance matches users with a device based on the user-specific inventory and their Active Directory credentials. This allows administrators to easily identify the users of specific devices.

- When a device is associated with a user or a domain, that information is displayed on the *Devices* and *Device Detail* pages.
- Appliance administrators can use the *Advanced Search* to identify the devices with specific user, location, and department attributes.
- User-related device attributes are now available in the report wizard.

Location improvements

This release includes the following location features:

- **New Locations and Location Detail pages**.
  - The *Locations* list page contains a list of your physical locations. A location entity represents a physical site that contains one or more of your assets and users. You can add, move, or delete location entities, as needed.
  - Appliance administrators can search for specific location attributes on the *Location* list page, to quickly find a specific location.
  - Appliance administrators can make bulk updates to the existing locations, to quickly and easily make changes to the location records, without having make changes to individual locations.
  - The *Location Detail* page is added in this release. In addition to a set of expected fields, such as *Name*, *Description*, or *Address*, this page can include custom fields. Administrators can view and edit these custom fields, as needed.
  - By default, any records that include a location field have that field set to `Unassigned`.
- **Changes to the Device Detail page**. Appliance technicians can manually assign devices to specific locations using the *Device Detail* page, when allocating company resources.
- **Changes to the Users and User Detail pages**.
  - The *Users* list page displays the location associated with each user record.
  - Appliance administrators can associate locations to users in bulk, to quickly and easily make changes to user records without having to make changes to individual users.
  - The *Users* list page can be filtered to only show users associated with specific locations.
  - Appliance technicians can manually assign users to locations.
- **Changes to the Assets list page**. The *Assets* list page can be filtered to display only the assets associated with specific locations.

Cross-appliance reporting

This release includes the following cross-appliance reporting features:

- **New linked report pages**.

- A linked report contains consolidated information from multiple appliances.
- The *Linked Reports* list and *Edit Linked Report* wizard are added to the K1000 systemui.
- When linked reporting is enabled, each linked appliance has access to the Federation API settings, and is granted the Administrator role, you can run linked reports.

- **Scheduling linked reports**.
  - Administrators can stop a report from running on a remote appliance, for example, if data is no longer needed, or after detecting a problem with the same report, while running on another linked appliance.
  - You can schedule the appliance to run linked reports and send them to administrators at specified times and intervals.
  - Administrators can schedule a linked report to run at a different time for each server that is part of the linked report, in order to capture a specific type of information.

Agent-based device management

The agent-based device management is improved to include the following new feature:

- **AMP Agent replaced with KONEA**. Prior to this release, the K1000 Agent connected to the server using the AMP protocol, implemented by AMPAgent. In this version, the AMP protocol and AMPAgent service are replaced with the Konea service and protocol. Konea provides optimized real-time communications for systems-management operations. Unlike AMPAgent, Konea does not require proprietary ports to be open on the network.

  IMPORTANT: While securing the Agent's connection, Konea is designed to be "sticky" to the first certificate it downloads from the appliance during the initial connection. If the appliance is restored or replaced, or if any other operation causes a new Konea certificate to be generated, all existing Agent instances will be orphaned, as they will not trust the appliance with the new certificate.

- **Blacklisting improvements**. Users can no longer bypass the blacklist policy by simply changing the name of a blacklisted executable. Starting in this version, the appliance uses the file description together with the original file name to determine whether an executable is part of a blacklisted application.

Agentless device management

The agentless device management is improved to include the following new features and enhancements:

- AirWatch integration on page 11
- Inventory and tracking of virtual host assets on page 12

AirWatch integration

This release includes the following AirWatch features:

- **General VMware® AirWatch® integration features**.

- AirWatch is an enterprise-level mobility management platform that allows management of different device types. The appliance can be integrated with AirWatch to discover devices managed with AirWatch.
- AirWatch-specific values are stored in the K1000 database as part of device inventory.
- Each device from a third-party AirWatch environment takes up an asset license.
- Appliance administrators can configure a discovery schedule to include AirWatch devices.
- Communication between an AirWatch solution and the appliance is carried over a secure connection.

- **Collecting and viewing AirWatch data**.
  - Appliance technicians can collect inventory data (about devices, applications, user/data metrics, and status) from an AirWatch environment that is integrated with the inventory and asset views, to gain a collective view of the company assets.
  - This feature also allows you to view inventory information about the integrated AirWatch mobile devices, and to summarize and analyze the related asset information.
  - For any AirWatch-displayed device, the user interface clearly indicates that the information about that device came from an AirWatch source.
  - Devices provisioned and inventoried through AirWatch integration have the *Mobile Information* group of fields on the *Device Details* page populated with relevant mobile and location information, as applicable.

Inventory and tracking of virtual host assets

The inventory and tracking of virtual host assets improved to include the following features:

- **Collecting and viewing VMware data**.
  - The appliance can collect inventory information about ESXi hosts through a vCenter. VMware-specific inventory information is included in the device details, reports, and the object history.
  - For each physical server, a view of each virtual machine's resource consumption is available, allowing you to quickly predict potential bottlenecks and to optimize under- and over-utilized assets. Administrators can view and report on the relationships between ESXi hosts and their guest systems which improves the asset management functionality.
  - For each virtual machine, administrators can see its CPU, memory and datastore usage, allowing them to quickly find the highest consumers of the host's resources and prevent related problems.
  - Inventoried VMware devices have the VMware asset type.
  - Administrators can adjust the connection time-out for collecting data from a VMware environment, as some connections may require more time.

Monitoring

SNMP trap receiver

This release includes the following SNMP trap receiver features:

- **New SNMP trap receiver**.
  - The SNMP trap receiver alerts the administrators of SNMP notifications being sent from SNMP devices such as printers, routers, switches, and so on.
  - The trap receiver reads and parses all received traps and generates alerts when it receives specific traps.
  - The trap receiver can use MIB files to translate SNMP traps into human-readable messages. Uploaded MIB files are backed up and available when the appliance is restored from a backup.
  - A new monitoring profile is added for SNMP devices.
  - SNMP trap log files rotate every night together with other appliance log files.

Security and configuration

The security and configuration aspects of the K1000 appliance are improved in this release with the following enhancements:

- FreeBSD 10.3 upgrade on page 13
- Root password security on page 13
- TLS 1.2 support on page 14
- SHA-1 updated to SHA-256 on page 14
- Use of secure algorithms on page 14

FreeBSD 10.3 upgrade

The K1000 Systems Management Appliance includes a number of third-party components, including FreeBSD.

In this release FreeBSD is updated to version 10.3. This version includes a number of new features, including the support of the TLS (Transport Layer Security) 1.2 protocol. For more information, seeTLS 1.2 support on page 14

Root password security

This release includes the following root password security features:

- **Two-Factor Authentication (2FA)**. Enabling SSH access to the appliance and creating a tether allows the KACE Support team to log in to the back-end of the K1000 appliance using the appliance root password together with an access token. This feature allows you to control access to the appliance back-end by providing the KACE

Support team with access tokens, when required. Each token can be used only once. Every time a token is used it expires, and must be replaced. You must maintain a list of current tokens.

- **2FA token generation**. Tokens are provided in the *Initial Setup Wizard*. They can be viewed and regenerated using the *Support Two-Factor Authentication* page in the appliance System Console.

TLS 1.2 support

Starting in this version, the K1000 Systems Management Appliance supports and prefers version 1.2 of the Transport Layer Security (TLS) protocol in the appliance web portals and client communication.

Versions 1.1 and 1.0 are also supported, but version 1.2 is preferred.

SHA-1 updated to SHA-256

The previous versions of the K1000 appliance used SHA-1 (Secure Hash Algorithm 1).

This version is considered as being out of date and potentially insecure. In this release, the appliance uses SHA-256.

Use of secure algorithms

Starting in this version, the appliance uses a set of newer secure algorithms such as TLS (see TLS 1.2 support on page 14), ECDHE (Elliptic Curve Diffie–Hellman) protocol, ECDSA (Elliptic Curve Digital Signature Algorithm), AES-256 (Advanced Encryption Standard with a 256-bit key size), GCM Galois/Counter Mode) operation, and SHA-384.

API support

The following APIs are added in this release:

- **Managed Installation API**. The Managed Installation API enables access to and actions on Managed Installations, machines, and files.
- **Asset Management API**. The Asset Management API allows you to view, create, update, and delete assets.
- **Inventory API**. The Inventory API allows you to manage inventory requests on a K1000 machine.
- **Scripting API**. The Scripting API allows you to manage scripts on a K1000 machine.

Resolved issues

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

Table 1. General resolved issues

Resolved issue	Issue ID
Service desk custom fields were not visible in the results of SQL queries.	ESMAS-3344

Resolved issue	Issue ID
In Microsoft Windows® 10, Microsoft changed how they report the version of the operating system. Major updates such as Windows 10 Anniversary Edition have new build numbers, but report the same name. There are some areas where specific operating system versions can be selected: • *Script Detail* page • *Software Detail* page • Wake-on-LAN settings If you previously chose a Windows 10 version, review your selection to ensure all of the Windows 10 builds are selected.	ESMEA-2550
The *Ticket Modified* date could be incorrect if Service Level Agreements (SLAs) are enabled.	K1-18730
A backup error message was incorrect if backups were disabled.	K1-18688
Scripts could not run with user credentials unless the user is logged into the agent machine.	K1-18674
On Microsoft Windows®, patching deployment did not remove temporary files.	K1-18649
The *Patching Catalog View By* menu contained the Windows 10 OS option in a wrong location.	K1-18606
An owners-only comment could be sent to the submitter if the status change was done at the same time and the changes were saved.	K1-18595
A Windows agent running multiple `explorer.exe` files resulted in duplicate user alerts.	K1-18591
Installed and *Missing* patch counts were incorrect on the *Catalog* page	K1-18504
Agent log files may overwrite previously rotated log files.	K1-18472
SCAP (Secure Content Automation Protocol) was not processing results when the benchmark file name contained more than 50 characters.	K1-18471
An error was reported when exporting software search results to a CSV (comma-separated value) file.	K1-18425
When adding a parent ticket you could only search for the first four octets.	K1-18367
When deploying a script, a wrong error could be generated about a missing label.	K1-18256
The patch *Reboot delay* setting was not honored when a patch reboot alert was allowed to time-out.	K1-18153
An error could be reported when an email attachment or body contained an *emoji*.	K1-18111
A computer device custom asset field could not link correctly on the *Asset Detail* page.	K1-18091
A computer inventory report was incorrectly sorted by current uptime.	K1-17803
Setting a ticket status from *Tickets* list page did not function correctly.	K1-17396

Resolved issue	Issue ID
A time-out action could not be set when configuring a Dell Update Schedule.	K1-17395
Assets were duplicated in Global Search Results.	K1-17364
Service Desk attachments containing the '#' symbol were not handled correctly	K1-17363
Emails to the service desk ignored embedded images if file attachments were also present	K1-17362
In the ticket archive list, an error could be reported when doing an Advanced Search by *Created*.	K1-17252
When viewing tickets by owner, closed tickets were included in the results.	K1-17235
With SSO enabled, the Samba share was only accessible by its IP address.	K1-17170
A length limit on alerts associated with scripts was not enforced, preventing alerts from being seen.	K1-17155
An Advanced Search of computer assets did not populate the Owners Name column.	K1-17154
A Dell Warranty report created with the report wizard showed duplicates and Incorrect serial numbers and warranty information.	K1-16250
Private IPs could not be associated with an asset.	K1-12370

Known issues

The following is a list of issues, including those attributed to third-party products, known to exist at the time of release.

Table 2. General issues

Known issue	Issue ID
An asset owner may only be set to *Unassigned* on the *Assets* or *Devices* list page.	K1-18955
Monitoring for Microsoft Windows® Server 2016 is not yet fully supported.	K1-18929
The *Patch Schedule* page lists devices that do not support patching in the Patch Tasks list (for example, Linux®).	K1-18926
The *Disable Duplicate Device Detection* option on the *Agent Settings* page is not supported under the 7.0 agent.	K1-18923
Software Catalog installation counts may be wrong after a restore is done. **Workaround**: To update the counts, select *Force Update*.	K1-18910
SNMP Inventory Configuration changes are not properly reflected in the object history.	K1-18909
The online help for Two-Factor Authentication is misleading. For more information, see Root password security on page 13.	K1-18901

Known issue	Issue ID
If a location report is started from the *Location List* page, only top-level locations are listed. **Workaround**: For a complete report including children, please use the *Reporting Wizard* under Reporting.	K1-18882
User password changes are not tracked in the object history.	ESMP-4423
When running the diagnostic utility *Services*, `z.kmsgr.sh` is indicated as `FAILED` erroneously, if the *Enable pre-7.0 Agent Support* system setting is cleared.	ESMP-4388
If ticket approvers are deleted, any subsequent ticket creation using that process will fail, yet still create the ticket.	ESMAS-3291
Google® Android™ tablet users running an old version of the OS (lower than 5.1) might fail to get push notifications sent to their tablet.	ESMAS-3237

System requirements

The minimum version required for installing K1000 7.0 is 6.4 SP3 (6.4.120822). If your appliance is running an earlier version, you must update to the listed version before proceeding with the installation. To check the appliance version number on K1000 6.3 or earlier, log in to the Administrator Console, then click **About K1000** at the bottom left of the page.

NOTE: In version 7.0, the *About K1000* link is located in the *Help* panel. Click the question mark in the upper-right corner of the page, and then click About K1000 at the bottom-right corner of the window that appears.

Before upgrading to or installing version 7.0, make sure that your system meets the minimum requirements. These requirements are available in the K1000 technical specifications.

- For physical appliances: Go to http://documents.software.dell.com/k1000-systems-management-appliance/7.0/technical-specifications-for-physical-appliances/.
- For virtual appliances: Go to http://documents.software.dell.com/k1000-systems-management-appliance/7.0/technical-specifications-for-virtual-appliances/.
- For K1000 as a Service: Go to http://documents.software.dell.com/k1000-systems-management-appliance/7.0/technical-specifications-for-k1000-as-a-service/.

Product licensing

If you currently have a K1000 product license, no additional license is required.

If you are using K1000 for the first time, see the appliance setup guide for product licensing details. Go to More resources on page 21 to view the appropriate guide.

NOTE: Product licenses for version 7.0 can be used only on K1000 appliances running version 6.3 or later. Version 7.0 licenses cannot be used on appliances running earlier versions of the K1000, such as 6.0.

Installation instructions

You can apply the Service Pack using an advertised update or by manually uploading and applying an update file. For instructions, see the following topics:

Prepare for the update

Before you begin

Before you update your K1000 server, follow these recommendations:

- **Verify your K1000 server version**: The minimum version required for installing this release is 6.4.120822. If your appliance is running an earlier version, you must update to the listed version before proceeding with the installation.

  NOTE: In version 7.0, the *About K1000* link is located in the *Help* panel. Click the question mark in the upper-right corner of the page, and then click About K1000 at the bottom-right corner of the window that appears.

- **Back up before you start**: Back up your database and files and save your backups to a location outside the K1000 server for future reference. For instructions on backing up your database and files, see the *K1000 Administrator Guide*, http://documents.software.dell.com/kace-k1000/7.0/administrator-guide/.

Update the K1000 server using an advertised update

You can update the K1000 server using an update that is advertised on the *Dashboard* page or on the *Appliance Updates* page of the Administrator Console.

CAUTION: Never manually reboot the K1000 server during an update.

Procedure

1 Back up your database and files. For instructions, see the *K1000 Administrator Guide*, http://documents.software.dell.com/kace-k1000/7.0/administrator-guide/.

2 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: Log in to the K1000 systemui: `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.

3 On the left navigation bar, click **Appliance Updates** to display the *Appliance Updates* page.

4 Click **Check for updates**.
Results of the check appear in the log.

5 When an update is available, click **Update**.
Version 7.0 is applied, and the K1000 server restarts multiple times. Progress appears in the Administrator Console.

Upload and apply an update manually

If you have an update file from Dell KACE, you can upload that file manually to update the K1000 server.

△ **CAUTION: Never manually reboot the K1000 server during an update.**

Procedure

1 Back up your database and files. For instructions, see the *K1000 Administrator Guide*, http://documents.software.dell.com/kace-k1000/7.0/administrator-guide/.

2 Using your customer login credentials, log in to the Dell Software website at https://support.software.dell.com/k1000-systems-management-appliance/download-new-releases, download the K1000 server `.kbin` file for the7.0 GA (general availability) release, and save the file locally.

3 On the left navigation bar, click **Appliance Updates** to display the *Appliance Updates* page.

4 In the *Manually Update* section:

   a Click **Browse** or **Choose File**, and locate the update file.

   b Click **Update**, then click **Yes** to confirm.

   Version 7.0 is applied, and the K1000 server restarts multiple times. The Administrator Console is unavailable until the update is complete. Progress appears in the browser window and in the Administrator Console.

Post-update tasks

After the update, verify that the update was successful and verify settings as needed.

Verify successful completion

Verify successful completion by viewing the K1000 version number.

Procedure

1 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: Log in to the K1000 systemui: `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.

2 Click the question mark in the upper-right corner of the page, and then click **About K1000** at the bottom-right corner of the window that appears, to verify the current version.

Verify security settings

To enhance security, database access over HTTP and FTP is disabled during the update. If you use these methods to access database files, change the security settings after the update as needed.

Procedure

1 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: Log in to the K1000 systemui: `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.

2 On the left navigation bar, click **Security Settings** to display the *Security Settings* page.

3 In the top section of the page, change the following settings:

- **Enable Secure backup files**: Clear this check box to enable users to access database backup files using HTTP without authentication.
- **Enable Database Access**: Select this check box to enable users to access the database over port 3306.
- **Enable Backup via FTP**: Select this check box to enable users to access database backup files using FTP.

CAUTION: Changing these settings decreases the security of the database and is not recommended.

4 Click **Save**.

5 **KBIN upgrades only**. Harden root password (2FA) access to the appliance.

a In the System Console, click **Settings** > **Support**.

b On the *Support* page, under *Troubleshooting Tools*, click **Two-Factor Authentication**.

c On the *Support Two-Factor Authentication* page, click **Replace Secret Key**.

d Record the tokens and place this information in a secure location.
If a tether is established, a token will need to be provided to KACE Support. For more information, see Root password security on page 13.

More resources

Additional information is available from the following:

- Online product documentation (http://documents.software.dell.com/ProductsAZ.aspx#K)
  - **Technical specifications**: Information on the minimum requirements for installing or upgrading to the latest version of the product.

    For physical appliances: Go to http://documents.software.dell.com/k1000-systems-management-appliance/7.0/technical-specifications-for-physical-appliances/.

    For virtual appliances: Go to http://documents.software.dell.com/k1000-systems-management-appliance/7.0/technical-specifications-for-virtual-appliances/.

For K1000 as a Service: Go to http://documents.software.dell.com/k1000-systems-management-appliance/7.0/technical-specifications-for-k1000-as-a-service/.

- **Setup guides**: Instructions for setting up physical and virtual appliances. Go to https://support.software.dell.com/k1000-systems-management-appliance/release-notes-guides to view documentation for the latest release.
- **Administrator guide**: Instructions for using the appliance. Go to http://documents.software.dell.com/k1000-systems-management-appliance/7.0/administrator-guide/ to view documentation for the latest release.

Globalization

This section contains information about installing and operating this product in non-English configurations, such as those needed by customers outside of North America. This section does not replace the materials about supported platforms and configurations found elsewhere in the product documentation.

This release is Unicode-enabled and supports any character set. In this release, all product components should be configured to use the same or compatible character encodings and should be installed to use the same locale and regional options. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan.

The release is localized to the following languages: French, German, Japanese, Portuguese (Brazil), Spanish.

About Dell

Dell listens to customers and delivers worldwide innovative technology, business solutions and services that customers trust and value. For more information, visit http://software.dell.com.

Contacting Dell

For sales or other inquiries, visit http://software.dell.com/company/contact-us.aspx or call 1-949-754-8000.

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions. To access the Support Portal, go to https://support.software.dell.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the Support Portal provides direct access to product support engineers through an online Service Request system.

The Support Portal enables you to:

- Create, update, and manage Service Requests (cases).
- View Knowledge Base articles.
- Obtain product notifications.
- Download software. For trial software, go to http://software.dell.com/trials.
- View how-to videos.
- Engage in community discussions.
- Chat with a support engineer.

Legend

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

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

KACE K1000 Systems Management Appliance Release Notes
Updated - November 2016
Software Version - 7.0