Kaseya

Audit

User Guide

Version R94

English

December 12, 2016

Copyright Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Contents

Audit Overview

Audit

Agents can be scheduled to automatically audit the hardware and software configurations of their managed machines on a recurring basis. Agents report the information back to the Kaseya Server so you can access it using the VSA even when managed machines are powered down. Audits enable you to examine configurations before they develop into serious problems. The system maintains three types of audits for each machine ID:

- **Baseline audit** - The configuration of the system in its original state. Typically a baseline audit is performed when a system is first set up.
- **Latest audit** - The configuration of the system as of the last audit. Once per week is recommended.
- **System Info** - All DMI / SMBIOS data of the system as of the last system info audit. This data seldom changes and typically only needs to be run once.

The VSA detects changes in a machines's configuration by comparing the latest audit to the baseline audit. The latest audit record is stored for as many days as you specify.

Most of the agent and managed machine data displayed by function pages and Info Center > Reporting > Reports are based on the latest audit. The **Machine Changes** report compares a machine ID's latest audit to a baseline audit. Two alert types specifically address changes between a baseline audit and the latest audit: **Application Changes** and **Hardware Changes**. Collected audit information includes:

- All hardware, including CPUs, RAM, PCI cards, and disk drives.
- All installed software, including licenses, version numbers, full path, and description.
- System Information from DMI and SMBIOS including PC make, model, serial number, mother board type, and over **40** other pieces of information describing the PC and its configuration.
- OS info with version number and service pack build.
- Current network settings including local IP address, gateway IP address, DNS, WINS, DHCP, and MAC address.

Functions	Description
View Assets *(page 2)*	Provides a consolidated view of all "assets" managed by the VSA.
Manage Credentials *(page 5)*	Specifies credentials by organization and machine group.
Credential Log *(page 6)*	Provides an audit log of the VSA users who create, modify and delete credentials.
Run Audit *(page 7)*	Schedules latest, system, and baseline audits of machine IDs.
Audit Summary *(page 8)*	Displays data returned by audits of machines
Configure Column Sets *(page 10)*	Configures columns sets for the Audit Summary page.
Machine Summary *(page 10)*	Displays detailed information about a single managed machine.
System Information *(page 13)*	Shows DMI / SMBIOS data collected.
Installed Applications *(page 15)*	Shows a list of executable (.exe) files on selected managed machines.
Add/Remove *(page 16)*	Shows the Add or Remove Programs list from a managed machine.

Software Licenses *(page 16)*	Shows a list of vendor license codes found on selected managed machines.
Documents *(page 17)*	Stores files associated with a machine ID.

View Assets

Audit > Asset > View Assets

The Audit > **View Assets** page is populated by **Discovery** scans of networks and domains.The **View Assets** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#10649.htm)* page provides a consolidated view of all "assets" managed by the VSA. Types of assets include:

- **Agent managed machines and mobile devices** - Computers and mobile devices that have an agent installed on them are always considered managed assets and display on this page for as long as the agent is installed on them.
- **Devices promoted to an asset** - When an agent cannot be installed on a discovered device, the device can still be "promoted" to a managed asset and display on this page. For example, a router or printer may still require monitoring, even if an agent cannot be installed on the machine. There are many different types of non-agent device types that can be managed by the VSA: routers, switchers, printers, firewalls, etc. The **Make Asset** button on the Discovery > Discovered Devices page enables you to "promote" a device to an asset. When you do the device begins displaying on this page. You can "demote" a asset using the **Demote Asset to Device** on this page. When you do, the asset is removed from this page.

All managed assets are assigned a machine group and organization. **Scoping rules** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#4578.htm)* and **view filtering** *(http://help.kaseya.com/webhelp/EN/VSA/9040000/index.asp#214.htm)* features within the VSA depend on this assignment.

- Multiple credentials can be defined for each asset. For agent assets, one of the credentials can be designated an agent credential and optionally used by **Policy Management** as an agent credential.
- **Service Desk** tickets can be optionally associated with assets listed on this page.

Actions

- **View** - Displays a popup window of information collected about a selected device. Different views, based on the type of probe used to collect the information, can be selected using the **Probe Type** drop-down list:
  - `NMAP Probe` - The standard method of discovering a device on a network, using the **Discovery** module.
  - `Machine Audit` - The audit performed on a machine installed with an agent.
  - `vPro` - The inventory of hardware attributes returned by a **vPro audit** *(http://help.kaseya.com/webhelp/EN/KDIS/9040000/index.asp#11552.htm)*.
  - `Merge View` - Merges all methods of data collection into one consolidated view. The default view.
- **Demote Asset to Device** - Removes a selected device as an managed asset. Computers and mobile devices that have agents installed on them cannot be demoted.
- **Change Group** - Changes the organization and machine group assigned to an asset.
- **Refresh** - Refreshes the page.

Table Columns

- **Asset Name** - The name of the asset. Typically this is the device name combined with VSA machine group and organization assigned to the asset.

- **Device Type** - The type of device: computers, mobile devices, routers, switchers, printers, firewalls, etc
- **Computer Agent** - If checked, the asset is a computer and has an agent installed on it.
- **Mobile Agent** - If checked, the asset is a mobile device and has an agent installed on it.
- **Probes** - Click this link to display the list of methods used to probe this computer or device.
- **Monitoring** - If checked, this asset is monitored.
- **Patching** - If checked, this asset is managed by Patch Management.
- **Auditing** - If checked, this asset is audited on a recurring basis.
- **Backing Up** - If checked, this asset is being backed up.
- **Security** - If checked, this asset has antivirus protection.
- **Ticket Count** - Displays the number of open tickets for this asset.
- **Alarm Count** - Displays the number of alarms generated by this asset.
- **Domain / Workgroup** - The domain or workgroup this asset is member of, if any.
- **SNMP Active** - If checked, this asset is SNMP-enabled.
- **Network** - Click this link to display the list of networks this asset is a member of.
- **Device Name** - The network name of a computer or device. If no network name is available, the IP address of the device displays.

Credentials tab

This tab specifies credentials by individual asset. These can be referenced by a VSA user when accessing a machine or device. Optionally include a note with each credential. Use the **Manage Credentials** *(page 5)* page to specify credentials by organization and machine group.

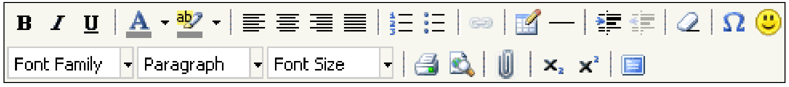
Agent Credentials

If the asset is an agent machine, a credential can be optionally used as the **source credential for an agent credential in a Policy Management policy** *(http://help.kaseya.com/webhelp/EN/KPM/9040000/index.asp#8158.htm)*. If multiple credentials are defined for a machine, then the most local level defined has precedence: by individual machine, by machine group, or by organization. At any one level, only one managed credential can be designated the source credential for an agent credential.

Actions

- **New / Edit** - Specifies a credential.
  - **Description** - A one line description for the credential.
  - **Username** - The username.
  - **Password** - The password.
  - **Domain** - The domain of the credential, if one exists.
  - **Set as agent credential** - Only one credential for this asset can be designated the source credential for an agent credential.
    - ✓ **Create account** - Check to create a new user account on the managed machine.
    - ✓ **as Adminstrator** - Check to create the new user account with administrator privileges.
    - ✓ **Local user account** - Select this option to use a credential that logs into this machine locally, without reference to a domain.
    - ✓ **Use machine's current domain** - Create a credential using the domain name this machine is a member of, as determined by the latest audit.

- ✓ **Specified domain** - Use the domain specified above.
- ➢ **Notes** - Optionally include a note with the credential. Use the edit toolbar to add images and special formatting to the text. *Images must be uploaded rather than copied and pasted in.*



- ✓ 🔗 - Hyperlink selected text. You may need to reset links copied and pasted from another source.
- ✓ ▦ - Insert a table.
- ✓ — - Insert a horizontal line as a percentage of the width, or set a fixed width in pixels.
- ✓ ⇥ - Indent text.
- ✓ ⇤ - Outdent text.
- ✓ ⌫ - Remove formatting.
- ✓ Ω - Insert a symbol.
- ✓ ☺ - Insert an emoticon.
- ✓ 🔍 - Preview the display of text and images.
- ✓ 📎 - Upload a file or image.
- ✓ x_2 - Set selected text to subscript.
- ✓ x^2 - Set selected text to superscript.
- ✓ ▣ - Toggle full screen mode for editing and viewing.

- **View** - Displays the properties of a selected credential.
- **Delete** - Deletes a select credential.

Table Columns

- **Type** - The type of credential.
  - ➢ 🔑 - This is an agent credential.
  - ➢ (blank) - This is *not* an agent credential.
- **Name** - The VSA name of this credential.
- **Username** - The username of the credential.
- **Domain** - The domain of the credential, if one is required.
- **Agent Credential** - If checked, this is the agent credential.
- **Create Account** - Created the account if it does not already exist.
- **as Administrator** - Created the account is an administrator-level account.

vPro tab

Audit > View Assets > vPro tab

The Audit > View Assets > **vPro** tab displays hardware information about vPro-enabled machines discovered by enabling a vPro scan using the Edit Network dialog, then scanning the network. This information is only available if a machine's vPro credential is specified when scanning a network.

Types of hardware information returned by the vPro machine include:

- Agent check-in status, if the vPro machine has an agent installed
- Computer Information
- Motherboard Asset Information
- BIOS Information
- Processor Information

- RAM Information
- Hard Drive Information

> **Note:** The **vPro** module provides **vPro management features** *(http://help.kaseya.com/webhelp/EN/VPRO/9040000/index.asp#10070.htm)*.

Manage Credentials

Audit > Asset > Manage Credentials

The **Manage Credentials** page specifies credentials by organization and machine group. These can be referenced by a VSA user when accessing a machine or device. Optionally include a note with each credential. Use the **View Assets** *(page 2)* page to specify credentials by individual machine or device.

Agent Credentials

If the asset is an agent machine, a credential can be optionally used as the **source credential for an agent credential in a Policy Management policy** *(http://help.kaseya.com/webhelp/EN/KPM/9040000/index.asp#8158.htm)*. If multiple credentials are defined for a machine, then the most local level defined has precedence: by individual machine, by machine group, or by organization. At any one level, only one managed credential can be designated the source credential for an agent credential. A managed credential is created when a user runs the **Systems Management Configuration Setup Wizard** *(http://help.kaseya.com/webhelp/EN/VPRO/9040000/index.asp#10070.htm)* for an organization.

Middle Panel Columns

Rows are sorted by organization, then machine group, then machine ID.

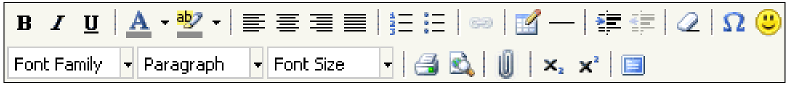
- **(Level)** - Identifies the row as an organization, a machine group or a machine ID.
- **Name** - The name of the organization, machine group or machine ID.
- **Credentials** - Displays a key if at least one credential is specified for that row.

Right Panel Actions

Select an organization or machine group before performing these actions.

- **New / Edit** - Specifies a credential.
  - **Description** - A one line description for the credential.
  - **Username** - The username.
  - **Password** - The password.
  - **Domain** - The domain of the credential, if one exists.
  - **Set as agent credential** - Only one credential for this organization or machine group can be designated the source credential for an agent credential.
    - ✓ **Create account** - Check to create a new user account on the managed machine.
    - ✓ **as Adminstrator** - Check to create the new user account with administrator privileges.
    - ✓ **Local user account** - Select this option to use a credential that logs into this machine locally, without reference to a domain.
    - ✓ **Use machine's current domain** - Create a credential using the domain name this machine is a member of, as determined by the latest audit.

- ✓ **Specified domain** - Use the domain specified above.
- ➢ **Notes** - Optionally include a note with the credential. Use the edit toolbar to add images and special formatting to the text. *Images must be uploaded rather than copied and pasted in.*



- ✓ 🔗 - Hyperlink selected text. You may need to reset links copied and pasted from another source.
- ✓ ▦ - Insert a table.
- ✓ — - Insert a horizontal line as a percentage of the width, or set a fixed width in pixels.
- ✓ ⇥ - Indent text.
- ✓ ⇤ - Outdent text.
- ✓ ⌫ - Remove formatting.
- ✓ Ω - Insert a symbol.
- ✓ 🙂 - Insert an emoticon.
- ✓ 🔍 - Preview the display of text and images.
- ✓ 📎 - Upload a file or image.
- ✓ x_2 - Set selected text to subscript.
- ✓ x^2 - Set selected text to superscript.
- ✓ ▣ - Toggle full screen mode for editing and viewing.

- **Delete** - Deletes a select credential.

Table Columns

- **Username** - Username of the credential.
- **Password** - Password of the credential.
- **Domain** - Domain of the credential, if applicable.
- **Inherited From** - The level the credential is inherited from. Credentials can be inherited from a higher level organization or machine group.
- **Agent** - If checked, this is the agent credential.
- **Description** - The VSA name for the credential.
- **Notes** - Notes about the credential.

Credential Log

Audit > Asset > Credential Log

The **Credential Logs** page provides an audit log of the VSA users who create, modify and delete credentials on the **View Assets** *(page 2)* and **Manage Credentials** *(page 5)* pages.

- **Event ID**
- **Event Name**
- **Message**
- **Admin**
- **Event Date**

Run Audit

Audit > Collect Data > Run Audit

The **Run Audit** page performs audits of the hardware and software configuration of manage machines.

Audits

Agents can be scheduled to automatically audit the hardware and software configurations of their managed machines on a recurring basis. Agents report the information back to the Kaseya Server so you can access it using the VSA even when managed machines are powered down. Audits enable you to examine configurations before they develop into serious problems. The system maintains three types of audits for each machine ID:

- **Baseline audit** - The configuration of the system in its original state. Typically a baseline audit is performed when a system is first set up.
- **Latest audit** - The configuration of the system as of the last audit. Once per week is recommended.
- **System Info** - All DMI / SMBIOS data of the system as of the last system info audit. This data seldom changes and typically only needs to be run once.

The VSA detects changes in a machines's configuration by comparing the latest audit to the baseline audit. The latest audit record is stored for as many days as you specify.

Most of the agent and managed machine data displayed by function pages and Info Center > Reporting > Reports are based on the latest audit. The **Machine Changes** report compares a machine ID's latest audit to a baseline audit. Two alert types specifically address changes between a baseline audit and the latest audit: **Application Changes** and **Hardware Changes**.

Actions

- **Schedule Audit** - Click **Schedule Audit** or **Reschedule Audit** to display the **Scheduler** window, which is used throughout the VSA to schedule a task. Schedule a task once or periodically. Each type of recurrence—Once, Hourly, Daily, Weekly, Monthly, Yearly—displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence. *Not all options are available for each task scheduled.* Options can include:
  - **Baseline Audit**, **Latest Audit** or **System Information** - Type of audit.
  - **Schedule will be based on the timezone of the agent (rather than server)** - If checked, time settings set in the Scheduler dialog reference the local time on the agent machine to determine when to run this task. If blank, time settings reference server time, based on the server time option selected in System > Preferences. Defaults from the System > Default Settings page.
  - **Distribution Window** - Reschedules the task to a randomly selected time no later than the number of periods specified, to spread network traffic and server loading. For example, if the scheduled time for a task is 3:00 AM, and the distribution window is 1 hour, then the task schedule will be changed to run at a random time between 3:00 AM and 4:00 AM.
  - **Skip if offline** - If checked and the machine is offline, skip and run the next scheduled period and time. If blank and the machine is offline, run the task as soon as the machine is online again. Applies only to recurring schedules, a 'Once' schedule always executes the next time the agent is online.
  - **Power up if offline** - Windows only. If checked, powers up the machine if offline. Requires Wake-On-network or vPro and another managed system on the same network.
  - **Exclude the following time range** - **Applies only to the distribution window.** If checked, specifies a time range to exclude the scheduling of a task within the distribution window. Specifying a time range outside of the distribution window is ignored by the scheduler.
- **Reschedule Audit** - Populates the scheduler with the values of a pending schedule so you can make adjustments.
- **Run Audit Now** - Schedules an audit to run immediately.
- **Cancel Audit** - Cancels a scheduled audit.

Remind me when accounts need audit scheduled

If checked, displays a pop up warning message if audits have not been scheduled for one or more machine IDs. The warning displays each time you select **Run Audit**. Applies to each VSA user individually.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent Quick View window.

🟢 Online but waiting for first audit to complete
🟢 Agent online
🔵 Agent online and user currently logged on.
🟡 Agent online and user currently logged on, but user not active for 10 minutes
● Agent is currently offline
▣ Agent has never checked in
◐ Agent is online but remote control has been disabled
🛑 The agent has been suspended
🔵 An agent icon adorned with a red clock badge is a temporary agent.

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Machine.Group ID

The top line shows the machine ID. The bottom line displays the last time a System Info audit was performed. Overdue date/time stamps display as red text with yellow highlight. Pending and completed date/time stamps display as black text.

System Information / Latest Audit / Baseline Audit

Each column displays the last time that type of audit was performed. Overdue date/time stamps display as red text with yellow highlight. Pending and completed date/time stamps display as black text.

Next Audit

Displays the time of the next scheduled Latest Audit. Overdue date/time stamps display as red text with yellow highlight. Pending and completed date/time stamps display as black text.

Recurring Interval

Displays the recurring interval for latest audits.

Audit Summary

Audit > View Group Data > Audit Summary

The Audit > **Audit Summary** page provides a view of the data returned by audits of machines using the **Run Audit** *(page 7)* page. The columns of audit data shown on this page are individually selectable and filterable. User-defined sets of columns can also be selected. Columns sets are defined using the **Configure Column Sets** *(page 10)* page. Additional data not shown in the **Audit Summary** page is provided using the **Machine Summary** *(page 10)* page. This table supports selectable columns, column sorting, column filtering and flexible columns widths.

Columns of audit data, in the default order they display in this page, include:

- **Machine ID** - The name identifying the machine within the VSA. Typically based on the computer name.

- **Current User** - Logon name of the machine user currently logged into the machine (if any).
- **Last Reboot Time** - Time of the last known reboot of the machine.
- **Last Checkin Time** - Most recent time when a machine checked into the Kaseya Server.
- **Group ID** - The group ID portion of the machine ID.
- **First Checkin Time** - Time when a machine first checked into the Kaseya Server.
- **Time Zone** - The time zone used by the machine.
- **Computer Name** - The name assigned the machine by users of the machine.
- **Domain/Workgroup** - The workgroup or domain the computer belongs to.
- **DNS Computer Name** - The fully qualified DNS computer name identifying the machine on the network. The DNS computer name typically comprises the computer name plus the domain name. For example: `jsmithxp.acme.com`. Displays only the computer name if the machine is a member of a workgroup.
- **Operating System** - Operation system type the machine is running.
- **OS Version** - Operation system version string.
- **CPU Type** - Processor make and model.
- **CPU Speed** - Clock speed of the processor.
- **CPU Count** - The number of CPUs.
- **RAM (MB)** - Megabytes of RAM on the machine.
- **Agent Version** - Version number of the Kaseya agent loaded on the machine.
- **Last Logged In User** - Logon name of the last person to log into the machine.
- **Primary/Secondary KServer** - IP address / name the machine uses to communicate with the Kaseya Server.
- **Quick Checkin Period** - Quick check in time setting in seconds.
- **Contact Name** - Machine user name entered in Edit Profile.
- **Contact Email** - Email address entered in Edit Profile.
- **Contact Phone** - Phone number entered in Edit Profile.
- **Manufacturer** - System manufacturer.
- **Product Name** - System product name.
- **System Version** - Product version number.
- **System Serial Number** - System serial number.
- **Chassis Serial Number** - Serial number on the enclosure.
- **Chassis Asset Tag** - Asset tag number on the enclosure.
- **External Bus Speed** - Motherboard bus speed.
- **Max Memory Size** - Max memory size the motherboard can hold.
- **Max Memory Slots** - Total number of memory module slots available.
- **Chassis Manufacturer** - Manufacturer of the enclosure.
- **Chassis Type** - Enclosure type.
- **Chassis Version** - Enclosure version number.
- **Motherboard Manufacturer** - Motherboard manufacturer.
- **Motherboard Product** - Motherboard product ID.
- **Motherboard Version** - Motherboard version number.
- **Motherboard Serial Num** - Motherboard serial number.
- **Processor Family** - Processor type installed.
- **Processor Manufacturer** - Processor manufacturer.
- **Processor Version** - Processor version ID.
- **CPU Max Speed** - Max processor speed supported.
- **CPU Current Speed** - Speed processor is currently running at.
- **IPv4 Address** - IP address assigned to the machine, in version 4 format.

- **IPv6 Address** - IP address assigned to the machine, in version 6 format.
- **Subnet Mask** - Networking subnet assigned to the machine.
- **Default Gateway** - Default gateway assigned to the machine.
- **Connection Gateway** - IP address seen by the Kaseya Server when this machine checks in. If the machine is behind a DHCP server, this is the public IP address of the subnet.
- **Country** - The country associated with the Connection Gateway.
- **MAC Address** - MAC address of the LAN card used to communicate with the Kaseya Server.
- **DNS Server** - IP address of the DNS server assigned to the machine.
- **DHCP Server** - The IP address of the DHCP server used by this machine.
- **Primary/Secondary WINS** - WINS settings.
- **Free Space** - The free data storage space in gigabytes.
- **Used Space** - The used data storage space in gigabytes.
- **Total Size** - The total data storage space in gigabytes.
- **Number of Drives** - The number of drives on the machine.
- **Portal Access Logon** - Logon name given to a machine user for logging into the Kaseya Server.
- **Portal Access Remote Control** - Enabled if this machine user can log in and get remote control access *to their own machine from another machine*. Disabled if access is denied.
- **Portal Access Ticketing** - Enabled if this machine user can log in and enter trouble tickets. Disabled if access is denied.
- **Portal Access Chat** - Enabled if this machine user can *initiate* chat sessions with a VSA user. Disabled if access is denied.

Configure Column Sets

Audit > View Group Data > Configure Column Sets

The **Configure Columns Sets** page defines columns sets that can be used to select a set of columns in the Audit > **Audit Summary** *(page 8)* table. The column set filter is on the right side of the **Audit Summary** table.

Actions

- **New** - Create a new column set.
- **Edit** - Edit a selected column set.
- **Delete** - Delete a selected column set.

Select a Column Set

Select an existing column set in the middle panel of this page. When more rows of data are selected than can be displayed on a single page, click the ‹ and › buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data using the *sort order of the selected column on that page*.

Machine Summary

Audit > View Individual Data > Machine Summary

- *Similar information is provided using Info Center > Reporting > Machine Summary.*

Machine Summary

The **Machine Summary** page allows users to perform tasks and functions solely for one managed machine. A series of tabbed property sheets provided access to various categories of information about the managed machine.

Actions

You may wish to edit both custom field values and the data collected for a machine during a system audit. Edits to system audit data will be overwritten by subsequent system audits, unless you remove these system audit fields from automatic collection. Edited system audit fields and custom fields can both be selected using the Filter Aggregate Table page and the Aggregate Table report. You can also automate changes to the values of data items by running the updateSystemInfo() command in an agent procedure.

- **Edit Machine Data** - Edits the data collected for a machine by a system audit. You can also edit the values for custom fields.
- **Edit Automatic Collection** - Uncheck items to prevent data from being overwritten by subsequent system audits. Used in conjunction with the **Edit Machine Data** dialog.
- **Bulk Edit Custom** - Changes the values of custom fields for multiple machines.
    1. Select multiple machine rows.
    2. Click the **Bulk Edit Custom** button.
    3. Select a custom field from the **Custom field to modify** drop-down list.
    4. Choose a replacement value by:
        - ✓ Selecting an existing replacement value from the drop-down list, or...
        - ✓ Entering the replacement value manually.

You can maintain an unlimited number of custom fields of information about managed machines. Custom fields can be maintained on both the **Summary** tab and the Hardware > **Summary** tab of this page. Custom fields can also be maintained on the Audit > **System Information** *(page 13)* page. Custom fields are supported in views, procedures, and reports. Custom reports do not support more than 40 custom fields.

- **New Custom Field** - Creates a new custom field.
- **Rename Custom Field** - Renames a custom field.
- **Delete Custom Field** - Deletes a custom field.

Select a Machine

Select a machine in the middle panel to display data for that machine. When more rows of data are selected than can be displayed on a single page, click the ‹ and › buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data using the *sort order of the selected column on that page*.

Summary

- **Collections** - Displays the collections a machine is a member of. Defined using the **Only show selected machine IDs** option in View Definitions.
- **Name/OS Information** - Displays the name, operating system and OS version.
- **System Information** - Displays the manufacturer of system, the product name, version and serial number.
- **Network Information** - Displays network configuration settings.
- **CPU/RAM Information** - Displays CPU and RAM specifications.
- **Custom Fields** - Displays custom fields and values assigned by the user to this machine.

Software

- **System Information -** Lists system hardware attributes and related information.

- **Software Licenses** - Lists all software licenses found for a selected machine ID. Duplicate license keys found on more than one machine display in red text. Clicking the number link next to the title of a duplicate license lists the machine IDs using the duplicate license.
- **Installed Applications** - Lists all the applications installed on the managed machine.
- **Add/Remove** - Displays programs listed in Add/Remove window of Windows machines.
- **Startup Apps** - Displays programs that start automatically when a user logs on.
- **Security Products** - Identifies the install status of antivirus products registered with a Windows machine's *Windows Security Center*. Windows 7 and later later calls the *Windows Security Center* the *Action Center*.

Hardware

- **Summary**
  - **System Information -** Lists system hardware attributes and related information.
  - **Network Information** - Displays network configuration settings.
  - **Chassis** - The chassis manufacturer, type, version, serial number and asset tag.
  - **Motherboard** - The motherboard manufacturer, product, version, serial number and external bus speed.
  - **CPU/RAM Information** - Displays CPU and RAM specifications.
  - **Custom Fields** - Displays custom fields and values assigned by the user to this machine.
- **Printers -** Lists the printers and ports a machine can direct print jobs to.
- **PCI & Disk Hardware** - Displays type, vendor, and product names.
- **Disk Volumes** - Displays disk volume information.
- **Disk Partitions** - Displays the partitions on each disk volume.
- **Disk Shares** - Displays shared folders.

Agent

- **Settings** - Displays information about the agent on the managed machine:
  - **Agent version**
  - **Current User**
  - **Last check-in**
  - **Last reboot**
  - **First time check-in**
  - **Patch Policy Membership** - Defined using Patch Management > Membership: Patch Policy
  - **View Definition Collections** - Defined using the **Only show selected machine IDs** option in View Definitions.
  - **Working Directory** - Can also be defined using Agent > Manage Agents.
  - **Check-In Control** - Can also be defined using Agent > Check-In Control.
  - **Edit Profile** - Can also be defined using Agent > Edit Profile.
  - **Agent Logs and Profiles** - Can also be defined using Agent > Log History.
- **Logs** - Displays the logs available for a machine: Alarm Log, Monitor Action Log, Agent Log, Configuration Changes, Network Statistics, Event Log, Agent Procedure Log, Remote Control Log, Log Monitoring.
  - **Pending Procedures** - Displays pending procedures for a machine and the procedure history for that machine. Includes the execution date/time, status and user who scheduled the procedure.

Patch Status

- Displays `Missing` and `Pending` Microsoft patches and schedules missing patches. If a machine belongs to a patch policy, missing patches may be further identified as `Denied (Pending Approval)`. The user can manually override the denied patch policy by scheduling the patch.
  - ➢ Click the **Schedule** button to schedule a selected missing patch.
  - ➢ Click the **Cancel** button to cancel a selected pending patch.
  - ➢ Click the **Show History** link to display the history of patches installed on the managed machine.

Remote Control

- Displays the status of remote control sessions for the managed machine: Remote Control, FTP, and Chat. The VSA user can set the remote control package to use during a remote control session.

Documents

- Lists documents uploaded to the Kaseya Server for a managed machine. You can upload additional documents. Provides the same functionality as Audit > **Documents** *(page 17)*.

Users

- **Accounts** - Lists all user accounts for the managed machine.
- **Groups** - Lists all user groups for the managed machine.
- **Members** - Identifies the users belonging to each user group for the managed machine.

System Information

Audit > View Individual Data > System Information

- *Similar information is provided using Info Center > Reporting > Reports > Inventory.*

The **System Info** page displays all DMI / SMBIOS data collected by the system info audit for a selected machine ID.

Actions

You may wish to edit both custom field values and the data collected for a machine during a system audit. Edits to system audit data will be overwritten by subsequent system audits, unless you remove these system audit fields from automatic collection. Edited system audit fields and custom fields can both be selected using the Filter Aggregate Table page and the Aggregate Table report. You can also automate changes to the values of data items by running the updateSystemInfo() command in an agent procedure.

- **Edit Machine Data** - Edits the data collected for a machine by a system audit. You can also edit the values for custom fields.
- **Edit Automatic Collection** - Uncheck items to prevent data from being overwritten by subsequent system audits. Used in conjunction with the **Edit Machine Data** dialog.
- **Bulk Edit Custom** - Changes the values of custom fields for multiple machines.
  1. Select multiple machine rows.
  2. Click the **Bulk Edit Custom** button.
  3. Select a custom field from the **Custom field to modify** drop-down list.
  4. Choose a replacement value by:
     - ✓ Selecting an existing replacement value from the drop-down list, or...

- ✓ Entering the replacement value manually.

You can maintain an unlimited number of custom fields of information about managed machines. Custom fields can also be maintained on the Audit > **Machine Summary** *(page 10)* page. Custom fields are supported in views, procedures, and reports. Custom reports do not support more than 40 custom fields.

- **New Custom Field** - Creates a new custom field.
- **Rename Custom Field** - Renames a custom field.
- **Delete Custom Field** - Deletes a custom field.

Select a Machine

Select a machine in the middle panel to display data for that machine. When more rows of data are selected than can be displayed on a single page, click the < and > buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data using the *sort order of the selected column on that page*.

Displayed Data

- System Information
  - **Manufacturer** - system manufacturer
  - **Product Name** - system product name
  - **System Version** - system version number
  - **System Serial Number** - system serial number
- Network Information
  - **IPv4 Address** - IP version 4 address assigned to the machine.
  - **IPv6 Address** - IP version 6 address assigned to the machine.
  - **Subnet Mask** - Networking subnet assigned to the machine.
  - **Default Gateway** - Default gateway assigned to the machine.
  - **Connection Gateway** - IP address seen by the Kaseya Server when this machine checks in. If the machine is behind a DHCP server, this is the public IP address of the subnet.
  - **Country** - The country associated with the Connection Gateway.
  - **MAC Address** - MAC address of the LAN card used to communicate with the Kaseya Server.
  - **DHCP Server** - The IP address of the DHCP server used by this machine.
  - **DNS Server 1, 2** - IP address of the DNS servers assigned to the machine.
- Chassis
  - **Chassis Manufacturer** - manufacturer of the enclosure
  - **Chassis Type** - enclosure type
  - **Chassis Version** - enclosure version number
  - **Max Memory Slots** - total number of memory module slots available
  - **Chassis Serial Number** - serial number on the enclosure
  - **Chassis Asset Tag** - asset tag number on the enclosure
- Motherboard
  - **Motherboard Manufacturer** - motherboard manufacturer
  - **Motherboard Product** - motherboard product ID
  - **Motherboard Version** - motherboard version number
  - **Motherboard Serial Num** - motherboard serial number
  - **External Bus Speed** - motherboard bus speed
- CPU/RAM Information
  - **Processor Manufacturer** - processor manufacturer

  - **Processor Family** - processor type installed
  - **Processor Version** - processor version ID
  - **CPU Max Speed** - max processor speed supported
  - **CPU Current Speed** - speed processor is currently running at
  - **CPU** - Processor make and model.
  - **Quantity** - The number of CPUs.
  - **Speed** - Clock speed of the processor.
  - **RAM** - MBytes of RAM on the machine.
  - **Max Memory Size** - maximum memory size the motherboard can hold
  - **Max Memory Slots** - Total number of memory module slots available.
- **Custom Fields** - Displays custom fields and their values.
- **On Board Devices** - Lists motherboard based devices (like video or ethernet).
- **Port Connectors** - Lists all the connections available on the chassis.
- **Memory Devices** - Lists memory modules installed on the motherboard.
- **System Slots** - Displays the status of each available card slot.

Installed Applications

Audit > View Individual Data > Installed Applications

- *Similar information is provided using Info Center > Reporting > Reports > Software - Software Applications Installed.*

The Installed Applications page lists all applications found during the latest audit for a selected machine ID. The list of machine IDs you can select depends on the machine ID / group ID filter and the scope you are using. This table supports selectable columns, column sorting, column filtering and flexible columns widths.

Select a Machine

Select a machine in the middle panel to display data for that machine. When more rows of data are selected than can be displayed on a single page, click the < and > buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data using the *sort order of the selected column on that page*.

The following information is displayed:

- **Application** - The filename of the application.
- **Description** - A brief description of the application as reported in the Properties dialog box of the executable file.
- **Version** - The version number of the application.
- **Manufacturer** - The manufacturer of the application.
- **Product Name** - The product name of the application.
- **Directory Path** - The absolute directory path where the application file is located.
- **File Size** - The size, in kilobytes, of the application file.
- **Last Modified** - The modification date of the application file.

> **Note:** You can filter the display of machine IDs on any agent page using the **Contains/Missing application** and **Version string is > < = N** options in View Definitions.

Select Page

When more rows of data are selected than can be displayed on a single page, click the < and >

buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data using the *sort order of the selected column on that page*.

Add/Remove

Audit > View Individual Data > Add/Remove

- Similar information is provided using Info Center > Reporting > Reports > Software.
- Alerts can be defined using Monitor > Alerts > Application Changes.

The **Add/Remove** page displays the programs listed in the **Add or Remove Programs** window of the managed machine. Information shown on this page is collected when a **Latest Audit** *(page 7)* is performed. Click a machine ID to display data for that selected machine. The list of machine IDs you can select depends on the machine ID / group ID filter and the scope you are using.

Select a Machine

Select a machine in the middle panel to display data for that machine. When more rows of data are selected than can be displayed on a single page, click the ‹ and › buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data using the *sort order of the selected column on that page*.

The following information is displayed:

- **Application Name** - The name of the application.
- **Uninstall String** - The uninstall string in the registry used to uninstall this application.

Software Licenses

Audit > View Individual Data > Software Licenses

- Similar information is provided using Info Center > Reporting > Reports > Software.

The **Software Licenses** page displays all software licenses found for a selected machine ID. The list of machine IDs displayed depends on the Machine ID / Group ID filter and machine groups the user is authorized to see using System > User Security > Scopes.

Information shown on this page is collected when a **Latest Audit** *(page 7)* is performed. Each vendor stores an application's license key differently so all application software licenses may not be collected.

Duplicate License Keys

Duplicate license keys found on more than one machine display in red text. Clicking the number link next to the title of a duplicate license lists the machine IDs using the duplicate license.

Select a Machine

Select a machine in the middle panel to display data for that machine. When more rows of data are selected than can be displayed on a single page, click the ‹ and › buttons to display the previous and next page. The drop-down list alphabetically lists the first record of each page of data using the *sort order of the selected column on that page*.

The following information is displayed:

- **Publisher** - The software publisher of the application (e.g. Microsoft).
- **Title** - The name of the application.
- **Product Key** - The product key used to activate the application during installation.
- **License** - The license code associated with the application.
- **Version** - The version of the application.

- **Date** - The version release date.

Documents

Audit > View Individual Data > Documents

- This function can also be accessed using the Documents tab of the Live Connect (Classic) > Agent Data page and the Documents tab of the Machine Summary *(page 10)* page.

The **Documents** page stores files associated with a machine ID. For example, you can upload scanned copies of purchase receipts, contract information, and configuration notes specific to a machine ID. Uploaded documents are stored in the User Profiles directory of the Kaseya Server. For example: `C:\Kaseya\UserProfiles\368905064566500\Docs`.

> **Note:** Documents are not included in the backup of the Kaseya Server database using System > Configure. A separate backup of Kaseya Server files and directories should be performed as well.
>
> **Note:** See Administrator Notes for a fast way of logging plain text notes for multiple machines without having to upload documents.

To Store a Document

1. Click a machine.group ID link. The list of machine IDs you can select depends on the machine ID / group ID filter and the scope you are using. Documents previously stored on the Kaseya Server for this machine ID display or else `No files found` displays.
2. Click **Browse** to locate a file on your local computer or LAN.
3. Click **Upload** to upload the file to the Kaseya Server.

   The added **Filename** displays, along with its file **Size** and the date/time of the **Last Upload**.

New Folder

Optionally click the **New Folder** icon and link to create a new folder to store documents in for the selected managed machine.

Edit

You can click a **Filename** link or edit icon 📝 to display a file or run the file, depending on the application the filename extension is associated with on your local machine.

Delete

Click the delete icon ✗ to delete a stored document or folder from the Kaseya Server.

Index