Agent

User Guide

Version R95

English

July 8, 2021

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."

©2019 Kaseya. All rights reserved. | www.kaseya.com

Contents

Contents

Agent Overview

Agent

Functions in the **Agent** module allow users to create, edit, and delete machine IDs, customize the appearance of the machine's agent icon in the system tray, control agent check-in frequency, and update the version of agent software that resides on managed machines.

> **Note:** If you're new to agent installation, see the **Agent Configuration and Deployment** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/EN_AgentDeployment_R95.pdf#zoom=70&navpanes=0)* quick start guide.

Functions	Description
Manage Agents *(page xi)*	Displays agent properties and performs a number of functions on multiple agents. • Update Agents • Delete Agents • Rename (Agents) • Change Group (Agents) • Working Directory • Suspend/Resume (Agents) • Set Credentials
Agent Logs *(page xv)*	Displays logs of: • Agent system and error messages • Execution of agent procedures, whether successful or failed. • Configuration changes made by a user. • Send/receive data for applications that access the network. • Application, System, and Security event log data collected from managed machine. • Alarm log • Remote control log • Log monitoring
Log History *(page xvi)*	Specifies how long to store log data.
Event Log Settings *(page xvi)*	Specifies event log types and categories included in event logs.
Screen Recordings *(page xx)*	Lists session recordings.
Automatic Update *(page xx)*	Updates agents to the latest version automatically.
Manage Packages *(page xxi)*	Creates agent install packages for installing agents on multiple machines.
Create *(page xxxiv)*	Creates machine ID accounts and/or install packages for installing agents on single machines.
Delete *(page xxxviii)*	Deletes machine ID template accounts.
Rename *(page xxxvii)*	Renames existing machine ID template accounts.
Change Group *(page*	Reassigns templates to a different machine group or

xxxix)	subgroup.
Set Credential *(http://help.kaseya.com/webhelp/EN/vsa/9050000/352.htm)*	Sets credential for a machine ID template.
Copy Settings *(page xl)*	Mass copies settings from one machine account to other machine accounts.
Import / Export *(page xli)*	Imports and exports agent settings, including scheduled agent procedures, assigned monitor sets, and event sets, as XML files.
Agent Menu *(page xlii)*	Customizes the agent menu on managed machines.
Check-In Control *(page xliv)*	Controls agent check-in frequency on agent machines.
Edit Profile *(page xlvii)*	Edits machine account information.
Portal Access	Sets up accounts to allow machine users remote control access to their own machines.
LAN Cache *(page li)*	Designates a machine to act as a file source for other machines on the same LAN.
Assign LAN Cache *(page liv)*	Assigns machines to, and removes machines from, a selected LAN Cache machine.
File Access *(page lvi)*	Prevents unauthorized access to files on managed machines by rogue applications or users.
Network Access *(page lvii)*	Lets you approve or deny network access on a per application basis.
Application Blocker *(page lx)*	Application blocker prevents any application from running on a managed machine.
Application Logging *(page lxi)*	Displays a log of Agent module activity.
Configuration *(page lxi)*	Configures and enables the Live Connect on Demand feature.
Dashboard *(page lxii)*	Provides a dashboard view of temporary agent session metrics.

Agent - Video Overview

Agents

The VSA manages machines by installing a software client called an **agent** on a managed machine. The agent is a system service that does not require the user to be logged on for the agent to function and does not require a reboot for the agent to be installed. The agent is configurable and can be totally invisible to the user. The sole purpose of the agent is to carry out the tasks requested by the VSA user. Once installed:

- An agent icon—for example the agent icon—displays in the system tray of the managed machine. **Agent icons** *(page iii)* can be custom images or removed altogether.

- Each installed agent is assigned a unique VSA machine ID / group ID / organization ID. Machine IDs can be created automatically at agent install time or individually prior to agent installation.
- Each installed agent uses up one of the available agent licenses purchased by the service provider.
- Agents are typically installed using packages created using Agent > **Deploy Agents** *(page xxi)* inside the VSA.
- **Multiple agents** *(page xxx)* can be installed on the same machine, each pointing to a different server.
- A check-in icon displays next to each machine ID in the VSA, displaying the overall status of the managed machine. For example, the ● check-in icon indicates an agent is online and the user is currently logged on.
- Clicking a check-in icon displays a single machine interface for the managed machine called Live Connect. **Live Connect** provides instant access to comprehensive data and tools you need to work on that one machine.
- Hovering the cursor over a check-in icon displays an agent Quick View window immediately. You can view agent properties, quick launch selected agent procedures, or launch **Live Connect** from the agent **Quick View** window.

Agent Icons

Once installed on a machine, the agent displays an icon in the computer's system tray. This icon is the machine user's interface to the agent. The icon may be disabled at the discretion of the VSA user using the Agent > **Agent Menu** *(page xlii)* page.

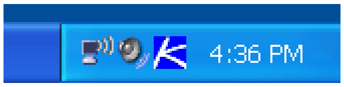
The icon can only be displayed to one user at a time. By default, it will only be displayed for the *console session* user but there is an optional switch (-remote) available to allow it to be displayed for a *single* terminal session (RDP) user. If enabled, the icon will be displayed for the first user that logs into the machine, whether they are on the console or a terminal session. See **this KB article** *(https://helpdesk.kaseya.com/hc/en-gb/articles/229011388-Adding-the-remote-tag-for-KaUsrtsk-exe-on-Windows-Agents)* for instructions how to apply the switch.

The user that the icon is displayed to will be reported as the logged in user in the VSA console.

> **Note:** You can fully customize agents icon using System > Site Customization. See Creating Custom Agent Icons. This includes unique icons for MacOS and Linux machines.

Agent Icon Background is Blue

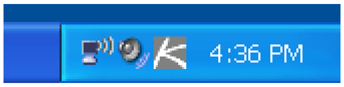
When the agent is running and **successfully checking into the VSA**, the agent icon's background is **blue**.



> **Note:** Double clicking the agent icon displays the Portal Access Welcome Page.

Agent Icon Background is Grey

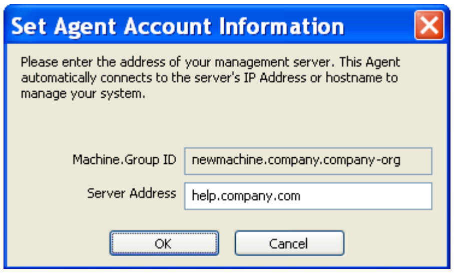
A running agent that can **not** check into the VSA displays a **gray icon**. This indicates that either the network connection is down or the agent is pointed at the wrong address for the VSA.



If the agent icon is gray check the following:

1. Verify this machine has internet access.

2. Check to see if there is a firewall blocking the **outbound** port used by the agent to connect to the VSA. The default is port 5721.
3. Verify this machine account's **Check-in Control** *(page xliv)* settings are correct.
4. Manually set the VSA server address in the agent by right clicking the agent menu, selecting **Set Account...**, and filling in the form with the correct address.


Set Agent Account Information

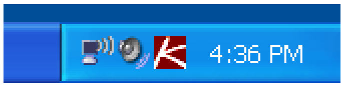
Please enter the address of your management server. This Agent automatically connects to the server's IP Address or hostname to manage your system.

Machine.Group ID: newmachine.company.company-org

Server Address: help.company.com

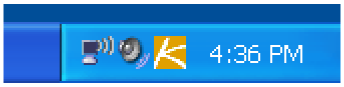
Agent Icon Background is Red

The agent icon turns **red** when a machine user manually disables remote control. VSA users prevent anyone from remote controlling their machine by selecting **Disable Remote Control** when they right click the agent menu.



Agent Icon Background Flashes between White and Blue

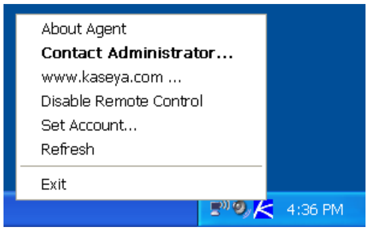
The agent icon **flashes** between a white background and its normal background when a *message is waiting* to be read. Clicking the icon displays the message.



> **Note:** See Remote Control > Send Message for an explanation of how to set up the sending of messages.

Agent Menu Options

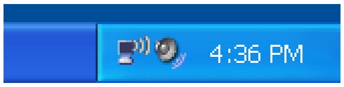
Right clicking the agent icon pops up a menu of options available to the machine user.



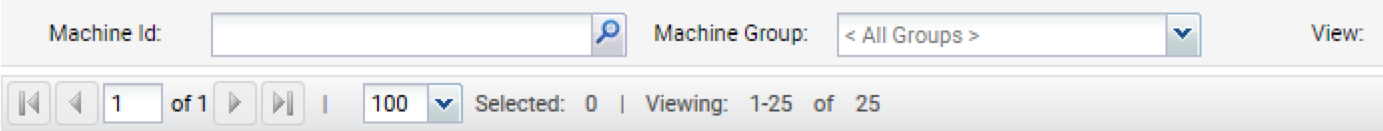
> **Note:** See Agent > **Agent Menu** *(page xlii)* for a description of how to turn these options on or off.

Disabling the Agent Menu

VSA users may completely **disable the agent menu** *(page xlii)* and remove the icon from the machine's desktop.



Machine ID / Machine Group Filter



Machine Id: | Machine Group: < All Groups > | View:

1 of 1 | 100 | Selected: 0 | Viewing: 1-25 of 25

The Machine ID / Machine Group filter is available on all tabs and functions. It allows *you*—rather than an administrator—to limit the machines displayed on *all* function pages. The **View Definitions** window lets you further refine a machine ID / machine group filter based on attributes contained on each machine—for example, the operating system type. Once filter parameters are specified, click the **Apply** button to apply filter settings to *all* function pages. By default, the Machine ID / Group ID filter displays all machine IDs in `<All Groups>` managed by the currently logged on VSA user.

> **Note:** Even if a VSA user selects `<All Groups>`, only groups the VSA user is granted access to using System > User Security > Scopes are displayed.

- **Machine ID** - Limits the display of data on *all* function pages by machine ID string. Include an asterisk (*) wildcard with the text you enter to match multiple records. For example, entering the string `ABC*` limits the display of machine IDs on all function pages to machine IDs that start with the letters `ABC`.

  Filters the display of machines by machine ID. Enter the *beginning* of a string to find all machine IDs that match that string. Include an asterisk at the beginning of a string to find all devices that match that string anywhere in the machine ID. For example, entering the string `*ABC` matches all machine IDs that include ABC anywhere in their machine ID.
- **Apply** - Click the **Apply** button to apply filter settings to all function pages.
- **Machine Group** - Limits the display of data on all function pages by group ID or organization. An organization with only *one machine group* only displays the machine group in the **Machine Group** drop-down list, not the organization. Organizations with *multiple machine groups* display both the organization and all machine groups for that organization. This allows the organization to be optionally selected to include all the machine groups.
- **View** - Change views by selecting a different view definition. The **View Definitions** window lets you further refine a machine ID / machine group filter based on attributes contained on each machine—for example, the operating system type.
- **New** - Create new view.
- **Edit...** - Click to display the **View Definitions** *(page v)* page.
- **Reset** - Clears all filtering.
- **Go to** - 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 and click |◀ and ▶| buttons to go to the last page. The drop-down list alphabetically lists the first record of each page of data.
- **Show** - Select the number of machines I Ds displayed on each page.
- **Viewing** - Shows the machine count, based on filter settings.

View Definitions

Machine ID / Group ID Filter > Edit...

The **View Definitions** window lets you further refine a machine ID / machine group filter based on attributes contained on each machine—for example, the operating system type. You can create and name multiple views. View filtering is applied to *all* function pages by selecting a **View** from the drop-down list on the **machine ID / machine group filter** *(page v)* panel and clicking the **Apply** 🔍 icon. Options are organized by sections that can be expanded and collapsed as needed. When an option is set the section remains expanded.

Header Options

- **Save** - Save the selected view.
- **Save As** - Save the selected view view to a new name.
- **Delete** - Delete the selected view.
- **Cancel** - Cancel changes.
- **Share...** - You can share a view with selected VSA users and user roles or make the view public for all VSA users and user roles.
- **Help** - Redirects you to help page.
- **Select View** - Select a view.
- **Edit Title** - Edit the title of a view.

To Create or Edit a New View

1. Click the **Edit...** button to the right of the **View** drop-down list in the machine ID / group ID filter panel to open the **View Definitions** editor.
2. Click the **Save As** button and enter a name for a new view.
3. Enter the desired filter specifications.
4. Click the **Save** button.

Machine Filter

- **Set machine ID** - Checking this box overrides any value set for the **Machine ID** field on the Machine ID / Group ID filter panel with the value entered here. The Machine ID field on the Machine ID / Group ID filter panel is disabled to prevent inadvertent changes while displaying a view with **Set machine ID** selected.
- **Set group ID** - Checking this box overrides the **Group ID** filter on the Machine ID / Group ID filter panel with the value entered here. The Group ID field on the Machine ID / Group ID filter panel is disabled to prevent inadvertent changes while displaying a view with **Set group ID** selected.
- **Only show selected machine IDs** - Save a view first before selecting machines IDs using this option. Once the view is saved, a **<N> machines selected** link displays to the right of this option. Click this link to display a **Define Collection** window, which allows you to create a view using an arbitrary collection of machine IDs.

Machine Status

- **Show machines that have / have not / never been online in the last N periods** - Check to list those machines whose agents have checked into the Kaseya Server, or not, within the specified period of time. Use the **never** option to filter machine ID template accounts, because these accounts never check in.
- **Show machines that are suspended / not suspended** - Check to list machines that are suspended or are not suspended.
- **Show machines that have/have not rebooted in the last N periods** - Check to list machines that have not rebooted in the specified number of periods.
- **Machines with Credential status** - Check to list machines with the selected credential status.
- **Connection gateway filter** - Check to only list machines that have a connection gateway matching the specified filter. Include an asterisk (*) wildcard with the text you enter to match multiple records. For example `66.221.11.*` matches all connection gateway addresses from `66.221.11.1` through `66.221.11.254`.
- **IP address filter** - Check to only list machines that have an IP address matching the specified filter. Include an asterisk (*) wildcard with the text you enter to match multiple records. For example `66.221.11.*` matches all IP addresses from `66.221.11.1` through `66.221.11.254`.

OS Info

- **OS Type** - Check to only list machines that match the selected operating system as reported by a Latest Audit.
- **OS Version** - Check to only list machines that match the OS version string as reported by a Latest Audit. Use this filter to identify machines by **service pack**.

Agent Procedure

- **With agent procedure scheduled/not scheduled** - Check to only list machines that have the specified agent procedure either scheduled to run or not.

> **Note:** *Click the* **select agent procedure** *link to specify the agent procedure by name.*

- **Last execution status success/failed** - Check to only list machines that have already executed the selected agent procedure. Select the appropriate radio button to list machines that successfully executed the agent procedure or failed to execute the agent procedure.
- **Agent procedure has/has not executed in the last N days** - Check to only list machines that have or have not executed the agent procedure in the specified period of time.

Applications

- **Contains/Missing application** - Check to only list machines that have, or don't have, an application installed using the specified filter. Include an asterisk (*) wildcard with the text you enter to match multiple records.
- **Version string is > < = N** - Check to further refine the application filter with a version number greater than, less than or equal to a specified value.
- **Show Machines with the following module installed**
  - **Anti-Malware**
  - **Antivirus**

Add-On Modules

- Filter machines based on whether they have had client software installed for selected add-on modules.

Label

- **Show machines with all or any of the following labels** - Filters machines using **all** or **any** of the selected labels.
- A series of keys in a machine's local registry is checked to identify whether the machine can be "labeled" a certain type of machine. Examples of labels include: `DNS Server`, `Domain Controller`, `POP3 Server`, `SMTP Server`, and `SQL Server`. Labeling is automatic. Each agent machine is checked periodically, typically once an hour, for configuration changes that may affect the labeling of the machine.

Software Management Views

- **machines with Approved Patches** - Show/Hide machines with Vulnerabilities which have been approved (marked ready).
- **machines with Pending Review patches** - Show/Hide machines with Vulnerabilities which are Pending Review
- **machines with Rejected patches** - Show/Hide machines with Vulnerabilities which have been rejected
- **machines with Suppressed patches** - Show/Hide machines with Vulnerabilities which have been suppressed
- **members of scan profile** - Show/Hide machines assigned with specific scan profile
- **members of over-ride profile** - Show/Hide machines assigned with specific over-ride profile
- **members of deployment** - Show/Hide machines assigned with specific deployment profile

- **members of 3rd party software profile** - Show/Hide machines assigned with specific third party profile
- **members of alert profile** - Show/Hide machines assigned with specific alert profile
- **Machines which are fully patched** - Show/Hide machines which are fully patched
- **Software Management Scan Scanned/Not Scanned** - Check scan status of machines wtihin x days
- **Software Management Deployment Deployed/NotDeployed** - Check deployment status of machines wtihin x days
- **Machines with Reboot pending** - Check for list of machines with reboot pending
- **Machines with user logged in and Reboot Action Configuration** - Check for list of machines with user logged in and specific Reboot strategy
- **Machines with user NOT logged in and Reboot Action Configuration** - Check for list of machines with user not logged in and specific Reboot strategy
- **Software Management Status** - Check for list of machines which are suspended or active in Software Management module.
- **Last Deployment Status** - Check for list of machines which list machines that have successful or failed deployments (Present)
- **Windows Automatic Update** - Check to only list machines where Windows Automatic Update is disabled or is not disabled.
- **Machines with Windows service WUAUSERV not running** - Check list of machines with Windows WUASERV service not running
- **Machines with Pending Actions** - List of machines with the following pending actions: Error - Scan tasks - Deployment tasks
- **Machines missing a specific patch (use KB Article ID - digits only)** - Check to only list machines missing a specific patch.
- **Machines with installed patch (use KB Article ID - digits only)** - Check to only list machines with an installed patch identified by KB Article.
- **Filter by CVE Codes** - List of machines where Vulnerabilities matching various CVE codes will be populated.
- **Filter by CVSS Base Score** (Technical Preview access only) - List of machines where Vulnerabilities meet a certain value of CVSS base score. < > and = operators are supported in this function.
- **Machines missing greater than or equal to 'N' approved patches: Machines missing greater than or equal to N patches** - Check to only list machines missing a specified number of Microsoft patches.

Patch Management

- **Show/Hide members of patch policy** - Checking this box works together with the machine ID and group ID filters to only list specific machines belonging (**Show**) or not belonging (**Hide**) to a specific patch policy.
- **Machines that have no patch scan results (unscanned)** - Check to only list machines that have not been scanned for missing patches.
- **Machines missing greater than or equal to N patches** - Check to only list machines *missing* a specified number of Microsoft patches.
- **Use Patch Policy** - Check to only list machines missing a specified number of *approved missing* Microsoft patches.
- **Patch scan schedule / not schedule** - Check to only list machines with either a patch scheduled or not scheduled.
- **Last execution status for patch scan success / failed** - Check to only list machines whose patch scan succeeded or failed.
- **Patch scan has / has not executed in the last <N> <periods>** - Check to only list machines whose patch scan has or has not executed within a specified time period.
- **Machines with Reboot Pending for patch installations** - Check to only list machines with a reboot pending for patch installations.
- **Machines with patch installation failures** - Check to only list machines with patch installation failures.

- **Machines with Windows service WUAUSERV not running** - Check to only list machines with Windows service WUAUSERV not running.
- **Machines with Patch Test Result** - Check to only list machines with the selected patch test result.
- **Machines with Patch Automatic Update configuration** - Check to only list machines with the selected Automatic Update configuration.
- **Machines with Patch Reboot Action configuration** - Check to only list machines with the selected Reboot Action configuration.
- **Machines with Patch File Source configuration** - Check to only list machines with the selected patch File Source configuration.
- **Machines missing a specific patch (use KB Article ID - digits only)** - Check to only list machines missing a specific patch.
- **Machines with installed patch (use KB Article ID - digits only)** - Check to only list machines with an installed patch identified by KB Article.
- **Machines being used as file share** - Check to only list machines configured as a file share using File Source.
- **Machines with file share located at select a machine** - Check to only list machines using a file share that was configured using File Source.
- **Machines with patch scan source set to online but offline scan ran last** - Check to only list machines with a Default Scan Source set to online but ran an offline scan most recently.
- **Default patch scan source Offline/Online**. - Check to only list machines using an offline or online default patch scan source.
- **Windows Automatic Update Disabled/Not Disabled** - Check to only list machines where Windows Automatic Update is disabled or is not disabled.

Monitoring

- **Only show machines with monitorset assigned <Select a Monitorset>** - Select to list all machines assigned this monitor set.
- **Only show machines with monitorset assigned <Select a SNMPset>** - Select to list all machines assigned this SNMP set.

Advanced Filtering

- **Advanced Agent Data Filter** - Check and click the **Define Filter...** button to further refine the view using the **Filter Aggregate Table** *(page ix)*.

> **Warning:** You must enter a **space character** to separate the operator from the data in a filter entry. For example, the filter entry `>= 500` includes a space character just after the equal sign.

Filter Aggregate Table

Machine ID / Group ID Filter > Edit... > Define Filter...

The **Filter Aggregate Table** lists over 75 agent and managed machine attributes that can be used to further refine a view definition using **advanced filtering** *(page x)*.

> **Note:** Collections provide an alternate method of selecting machine IDs for a **view definition** *(page v)*, regardless of whether they share any attributes.

User Defined Attributes

You can add user defined attributes to the **Filter Aggregate Table** using the Audit > System Information page, then create view definitions that select machine IDs based on these user defined attributes.

Advanced Filtering

Advanced filtering lets you design complex searches to isolate data to just those values you want. Enter filter strings into the same edit fields you enter filter text.

> **Warning:** You must enter a space character to separate the operator from the data in a filter entry. For example, the filter entry `>= 500` includes a space character just after the equal sign.

Advanced filtering supports the following operations:

White Space

To search for white space in a string, include an asterisk for white space.

For example: `Microsoft*Office` OR `Adobe*`

Nested operators

All equations are processed from left to right. Use parenthesis to override these defaults.

For example: `(("* adobe " OR *a*) AND *c*) OR NOT *d* AND < m`

AND

Use the logical AND operator to search for data that must contain multiple values but can appear in different places in the string.

For example: `Microsoft* AND *Office*` returns all items that contain both Microsoft and Office in any order.

OR

Use the logical OR operator to search for data that may contain multiple values but must contain at least one.

For example: `*Microsoft* OR *MS*` returns all items that contain either Microsoft and MS in any order.

NOT

Search for a string not containing the match data.

For example: `NOT *Microsoft*` returns all non-Microsoft applications.

For example: `NOT *Windows* AND NOT *update*` returns all items that do not contain either the strings `Windows` or `update`.

<, <= (Less than or less than or equal to)

Performs a string comparison to return all data whose value is less than the entered value.

For example: `< G*` returns all applications starting with a letter less than `G`.

For example: `< 3` returns the values `2`, `21` and `287`.

> **Note:** Dates may also be tested for but must be in the following format: `YYYYMMDD HH:MM:SS` where `YYYY` is a four digit year, `MM` is a two digit month (01 to 12), `DD` is a two digit day (01 - 31), `HH` is a two digit hour (00 - 23), `MM` is a two digit minute (00 - 59), and `SS` is a two digit second (00 - 59). `HH:MM:SS` is optional. Date and time are separated with a space.
>
> For example: `< 20040607 07:00:00` or `< "20040607 07:00:00"` returns all dates earlier than 7:00 on 7 June 2004. *Ensure a space exists after the < operator.*

>, >= (Greater than or greater than or equal to)

Performs a string comparison to return all data whose value is more than the entered value.

For example: `> G*` returns all applications starting with a letter greater than `G`.

For example: `> 3` returns the value `3`, `3abc` and `30.129.101.76`.

Agent Ver

Returns all machines using a specified **agent version** *(page xi)*. For example, agent version 6.2.1.1 is specified as `6020101`

Manage Agents

Agent > Agents > Manage Agents

The **Manage Agents** page consolidates a number of agent functions all in one page.

Agent Properties and Column Sets

The page can display a wide variety of **agent properties** *(page xiii)*. You can use selectable columns, column sorting, column filtering and flexible columns widths to adjust the display of agent properties. You can also create named "column sets" to save a preferred display of data. Column and filter selections apply to each VSA user individually. You can click the cell of any column and copy its value to your clipboard.

Maintenance

A gear ⚙ icon provides access to three maintenance functions.

- **Export** - Exports agent data to a csv file. Only data or columns currently displayed are exported—for all agents, selected agents or just the current page of agents.
- **Refresh** - Refreshes the table.
- **Reset** - Resets the display of table columns to the default.

Actions

Select one or more agents before selecting any of the following actions. In many cases an additional dialog displays.

Manage menu

- **Update Agents** - Updates selected agents with the latest version of the agent software. Updating the agent software makes no changes to the agent settings you have defined for each agent. Optionally
  - **Force update even if agent is at version x.x.x.x** - If checked, machines selected for update are updated with new files to replace the agent files on the managed machine, even if the agent version is currently up to date. This performs a "clean" installation of the agent files.
  - **Agent procedure to run after update** `<select agent procedure>` - Select an agent procedure to run immediately after an agent update completes. This lets you re-apply customizations to an agent that may be lost after an agent update. Typically these customizations involve hiding or renaming agent identifiers on managed machines so as to prevent users from recognizing the agent is even installed.
- **Cancel Update** - Cancels a pending update on selected managed machines.
- **Delete Agents** - Deletes three different combinations of *machine ID accounts* and *agents*.
  - **Uninstall agent first at next check-in** - Uninstall the agent from the machine **and** remove the machine ID account from the Kaseya Server. The account is not deleted until the next time the agent successfully checks in.

  - **Delete account now without uninstalling the agent** - Leave the agent installed **and** remove the machine ID account from the Kaseya Server. Once the agent checks in next time the agent GUID would be changed.

    > **Note:** All the files and folders associated to the agent would be deleted.

  - **Uninstall the agent and keep the account** - Uninstall the agent from the machine **without** removing the machine ID account from the Kaseya Server.
- **Cancel Delete** - Cancels a pending delete on selected managed machines.
- **Rename**
  - **Rename account** - Renames an existing machine ID account. You can also assign the machine to a different machine group. Renaming an agent only changes how the name is displayed in the VSA.
  - **Merge offline account <Offline Machine ID> into <Select Machine ID> Delete <Offline Machine ID> after merge** - Use merge to combine log data from two different accounts into the same machine. This could be necessary if an agent was uninstalled and then re-installed with a different account name. Merge combines the accounts as follows:
    - ✓ Log data from both accounts are combined.
    - ✓ Baseline Audit data from the old offline account replaces any baseline data in the selected account.
    - ✓ Alert settings from the selected account are kept.
    - ✓ Pending agent procedures from the selected account are kept. Pending agent procedures from the old offline account are discarded.
    - ✓ The old account is deleted after the merge.

    > **Note:** Since the machine can only be active on a single account, only offline accounts are provided in the drop-down list to merge with.

- **Change Group** - Assigns multiple agents to a different machine group. Machines currently offline are assigned the next time they check in. Changing the machine group may trigger automated actions. For example, **Policy Management** *(http://help.kaseya.com/webhelp/EN/KPM/9050000/index.asp#8138.htm)* may apply different policies, based on the the assigned machine group.
- **Working Directory** - Sets the path to a directory on the managed machine used by the agent to store working files. Depending on the task at hand, the agent uses several additional files. The server transfers these files to a working directory used by the agent on the managed machine. For selected machine IDs you can change the default working directory from `C:\kworking` to any other location. You can approve this directory in security programs, such as virus checkers, to allow operations such as remote control from being blocked. A working directory can be written to using a getVariable() command in agent procedures. A **Set System Default Working Directory** button displays for master users.

  > **Warning: Do not delete files and folders in the working directory.** The agent uses the data stored in the working directory to perform various tasks.

- **Suspend/Resume** - Suspends/resumes all agent operations, such as agent procedures, monitoring, software management, and patching, without changing the agent's settings. When suspended, a machine ID displays a suspended icon next to it. While a machine ID account is suspended the managed machine displays a gray agent icon in the system tray. You can filter the display of machine IDs on any agent page using the **Show machines that are suspended/not suspended** option in **View Definitions** *(page v)*.

Credentials menu

- **Set Credentials** - Registers an *agent credential* used by an agent to perform user level tasks on a managed machine. A credential is the logon name and password used to authenticate a user or process's access to a machine or network or some other resource. Most agent tasks do not require an agent credential.
  - ➢ **Username** - Enter the username for the credential. Typically this a user account.
  - ➢ **Password** - Enter the password associated with the username above.
  - ➢ **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. This makes it easier to **Select All** and rapidly set a common username/password on multiple machines, even if selected machines are members of different domains.
  - ➢ **Specify Domain** - Manually specify the domain name to use for this credential in the **Specify** field.
- **Test Credentials** - Verifies whether an agent credential works.
- **Clear Credentials** - Removes the agent credential from all checked machine IDs.

Deploy Agent - Downloads the current VSA user's default package to the user's local machine..

Columns Sets menu

- **New** - Create a new column set. Add agent property columns to display when this column set is selected in the Manage Agents page.
- **Edit** - Edit a selected column set.
- **Delete** - Delete a selected column set.
- **Manage** - Displays a dialog of all columns sets. You can add, edit or delete column sets from this dialog.

Manage Agents - Video Overview

Agent Properties

Agent > Agents > Manage Agents

The **Manage Agents** *(page xi)* pages displays the following agent properties.

- **Machine ID** - Machine ID label used throughout the system.
- **Current User** - Logon name of the machine user currently logged into the machine (if any).
- **Quick Checkin Period** - Quick check in time setting in seconds.
- **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 machine's organization ID and group ID, in that order.
- **First Checkin Time** - Time when a machine first checked into the Kaseya Server.
- **Timezone** - The time zone used by the machine.
- **Computer Name** - Computer name assigned to the machine.
- **Domain/Workgroup** - The workgroup or domain the computer belongs to.
- **Agent GUID** - A unique identifier for a machine ID.group ID account and its corresponding agent.
- **Working Dir** - The directory on the managed machine the agent uses to store temporary files.
- **DNS Computer Name** - The fully qualified DNS computer name for the machine, which 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.

- **IP Address** - IP address assigned to the machine, in version 4 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.
- **IPv6 Address** - IP address assigned to the machine, in version 6 format.
- **MAC Address** - MAC address of the LAN card used to communicate with the Kaseya Server.
- **DNS Server 1, 2** - IP address of the DNS servers assigned to the machine.
- **DHCP Server** - The IP address of the DHCP server used by this machine.
- **Primary/Secondary WINS** - WINS settings.
- **CPU Type** - Processor make and model.
- **CPU Speed** - Clock speed of the processor.
- **CPU Count** - The number of CPUs.
- **RAM Size** - MBytes of RAM on the machine.
- **Agent Version** - Version number of the Kaseya agent loaded on the machine. To filter by this column, enter the format `9030004` instead of `9.3.0.4`.
- **Last Logged In User** - Logon name of the last person to log into the machine.
- **Portal Access Login** - Logon name given to a machine user for logging into the Kaseya Server.
- **Portal Access Remote Cntl** - 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.
- **Primary/Secondary KServer** - IP address / name the machine uses to communicate with the Kaseya Server.
- **Contact Name** - Machine user name entered in **Edit Profile** *(page xlvii)*.
- **Contact Email** - Email address entered in Edit Profile.
- **Contact Phone** - Phone number entered in Edit Profile.
- **Contact Notes** - Notes entered in Edit Profile.
- **VDI** - Displays a green check if the /v agent **install switch** *(page xxviii)* is used to install an agent to an existing agent account.
- **Reverse Group ID** - The machine's group ID and organization ID, in that order.
- **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.
- **Transition Time**
- **Timezone Offset** - The time zone used by the machine.
- **Tool Tip Notes** - Special instructions specified for this agent in the Agent > **Edit Profile** *(page xlvii)* page.
- **Show Tool Tip** - Displays the index number for the icon badge set for this agent in the Agent > **Edit Profile** page.
- **Agent Info** - Displays pending tasks assigned by the **Manage Agents** page.

Agent Logs

Agent > Agents > Agent Logs

The **Agent Logs** page displays log data related to managed machines. There are corresponding log reports for each type of log provided.

> **Note:** The system automatically limits the number of log entries per log type per machine to 1000. Once the limit has been reached, log entries exceeding the limit are archived, if archiving is enabled, and deleted from the system. The archive option is set in **Log History** *(page xvi)*.

Select a machine.

- **Machine ID** - Click the hyperlink of a machine ID to list all logs for that machine ID.

Select one of the following tabs to display that log.

- **Diagnostic Logs**
  - **Endpoints** - Lists endpoint logs generated by the agent for this machine. Click the link of any log type to display the list of available logs for that agent.
- **Technician Logs**
  - **KRC** - Displays a log of remote control sessions using Kaseya Remote Control.
  - **Classic Remote Control** - Displays a log of remote control sessions using the Remote Control module.
  - **Live Connect** - Displays a log of Live Connect sessions.
- **Agent Admin Logs**
  - **Agent** - Displays a log of agent, system, and error messages.
  - **Configuration Changes** - Displays VSA settings changes for the selected machine.
  - **Procedure History** - Displays a log of successful/failed agent procedures.
  - **Events** - Displays event log data collected by Windows. Not available for Win9x. Only event logs that apply to the selected machine display in the event log drop-down list.
    - ✓ A ⚠ indicates a log entry classified as a warning.
    - ✓ A ❗ indicates a log entry classified as an error.
    - ✓ A ℹ indicates a log entry classified as informational.

  Select a log entry, then click the **Setup Event Log Monitor** to create a new event set criteria based on that log entry. The new event set criteria can be added to any new or existing event set. The new or changed event set is immediately applied to the machine that served as the source of the log entry. Changing an existing event set affects all machines assigned to use that event set. The monitor wizard icon displays in:

- ✓ Agent > Agent Logs
- ✓ Live Connect > Event Viewer
- ✓ Live Connect > Agent Data > Event Log

See Monitor > Event Log Alerts for a description of each field shown in the wizard.

- **Agent Monitoring Logs**
  - **Alarm Log** - Lists all alarms triggered for the selected machine. This tab includes three action buttons you can select for a single alarm.
    - ✓ **Delete Alarm** - Deletes the alarm.
    - ✓ **Change Alarm State** - Toggles the alarm state between `Open` and `Closed`.
    - ✓ **Create/Edit Ticket** - Creates or edits a ticket associated with this alarm.
  - **Actions** - The log of alert conditions that have occurred and the corresponding actions, if any, that have been taken in response to them.

    > **Note:** A counter value of -998 in the monitor logs indicates the monitor set is returning no data. Check that the the `Performance Logs & Alerts` service in Windows is running. This is a pre-requisite for monitoring of performance counters.

  - **Network Stat** - Displays a log of send/receive data for network applications.

    > **Note:** This log requires the Agent > **Network Access** *(page lvii)* driver be enabled. This driver inserts itself into the TCP/IP stack to measure TCP/IP-protocol-based network traffic by application. The driver is *disabled* by default.

  - **Monitoring** - Displays Log Monitoring entries.
- **Events per Page** - Select the number of rows displayed per page.
- **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 and click ⏮ and ⏭ buttons to go to the last page. The drop-down list alphabetically lists the first record of each page of data.

Log History

Agent > Agents > Log History

The **Log History** page determines the number of days to store log data in the database on a per log basis for each machine ID. Log data is displayed using **Agent Logs** *(page xv)* or printed to a report using Info Center > Reporting > Logs. This page also determines whether agent log data is subsequently archived to text files located on a network directory. The directory is specified using System > Server Management > Configure. Changes made using this page take effect at the next agent check-in and display in red text until then.

- **Log Settings** can also be maintained using the **Agent Settings** tab of Live Connect (Classic) > Agent Data or the Machine Summary page.
- System > System Preferences > Check-in Policy can restrict the number of days users can keep log entries, to avoid placing undue stress on servers running the Kaseya Server service.
- These settings default from the agent install package. Agent install packages are created using Agent > **Manage Package** *(page xxi)*.

Estimating Database Sizing Requirements

The more data you log, the larger your database grows. Database sizing requirements can vary, depending on the number of agents deployed and the level of logging enabled. To estimate database sizing requirements for log data, create a dump of your database's `nteventlog` table. Determine how much data is being logged per day, then use that to predict the amount of extra space required to extend the log retention period.

Set days to keep log entries, check to archive to file

Set the number of days to keep log data for each type of log. Check the checkbox for each log to archive log files past their cutoff date.

- **Configuration Changes** - The log of configuration changes made by each user.
- **Network Statistics** - The log of incoming and outgoing packet count information and the application or process transmitting and/or receiving such packets. This information can be viewed in detail using Agent > **Agent Logs** *(page xv)* > Network Statistics.
- **Agent Procedure Log** - Displays a log of successful/failed agent procedures.
- **Legacy Remote Control Log** - Displays a log of remote control sessions using the Remote Control module.
- **Kaseya Remote Control Log** - Displays a log of remote control sessions using Kaseya Remote Control.
- **Alarm Log** - The log of all alarms issued.
- **Monitor Action** - The log of alert conditions that have occurred and the corresponding actions, if any, that have been taken in response to them.
- **SYS log** - The 'log monitoring' log.
- **Agent Uptime Log** - Logs the uptime history of agents. Number of days must be set to 1 or greater for accurate last reboot time collection. See **Collecting last reboot times for the agent** *(https://helpdesk.kaseya.com/entries/35994418)* and **Reboot Now button remains and/or end user reports ongoing patch reboot nag after reboot** *(https://helpdesk.kaseya.com/entries/33901207)*.

> **Note:** All agent log archives listed above are stored in the directory specified by the System > Server Management > Configure > **Log file archive path** field.

Set days to keep monitoring logs for all machines

The following monitoring log settings are applied system-wide.

- **Event Log** - The log of all events. The events collected are specified in more detail using Agent > **Event Log Settings** *(page xviii)*.
- **Monitor Log** - The log of data collected by monitoring sets.
- **SNMP Log** - The log of all data collected by SNMP sets.
- **Agent Log** - The log of agent, system, and error messages

> **Note:** Monitoring data log archives—identified on the Agent > **Log History** *(page xvi)* page—are stored in the `<KaseyaRoot>\UserProfiles\@dbBackup` directory. This is to improve performance on systems where the database is on a different server. All other agent log archives are stored in the directory specified by the System > Configure > **Log file archive path** field.

Set All Days

Click **Set All Days** to set all "day" fields to the same setting.

Select All Archive / Unselect All Archive

Click the **Select All Archive** link to check all archive checkboxes on the page. Click the **Unselect All Archive** link to uncheck all archive checkboxes on the page.

Update

Click **Update** to update selected machine IDs with agent log settings.

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.

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.

● Agent is currently offline

🔵 User Logged In and Agent is Active

🟡 User Logged In and Agent is Inactive

🟢 User Not Logged In and Agent is online

🟢 User Not Logged In and Agent is Idle

🛑 The agent has been suspended

▣ Agent has never checked in

Machine.Group ID

The list of Machine.Group IDs displayed is based on the **Machine ID / Group ID filter** *(page v)* and the machine groups the user is authorized to see using System > User Security > Scopes.

Event Log Settings

Agent > Agents > Event Log Settings

The **Event Log Settings** page specifies the combination of event log types and categories that are collected by the VSA.

> **Note:** Alerts can be separately specified for events using Monitoring > Event Log Alerts. **If NO or ALL event logs types and categories are collected for a machine, then event log alerts are generated for that machine. If SOME event log types and categories are collected for a machine, then event log alerts are generated only for those event log types.**

To specify **Event Log Settings**:

1. Click an event log type in the **Event Log Types** list box. Hold down the [Ctrl] key to click multiple event log types.
2. Click **Add >** to add event log types to the **Assigned Event Types** list box. Click **<< Remove** or **<< Remove all** to remove event log types from the **Assigned Event Types** list box.
3. Check one or more event categories: **Error, Warning, Information, Success Audit, Failure Audit, Critical, Verbose**.
4. Select one or more machine IDs.
5. Click **Update** or **Replace** to apply these settings to selected machine IDs.

Global Event Log Black Lists

Each agent processes all events, however events listed on a "black list" are *not* uploaded to the VSA server. There are two black lists. One is updated periodically by Kaseya and is named `EvLogBlkList.xml.` The second one, named `EvLogBlkListEx.xml`, can be maintained by the service provider and is not updated by Kaseya. Both are located in the `\Kaseya\WebPages\ManagedFiles\VSAHiddenFiles` directory. Alarm detection and processing operates regardless of whether entries are on the collection blacklist.

Flood Detection

If 1000 events—not counting black list events—are uploaded to the Kaseya Server by an agent *within one hour*, further collection of events of that log type are stopped for the remainder of that hour. A new event is inserted into the event log to record that collection was suspended. At the end of the hour, collection automatically resumes. This prevents short term heavy loads from swamping your Kaseya Server. Alarm detection and processing operates regardless of whether collection is suspended.

Update

Adds event log types listed in the **Assigned Event Types** list box to the set of event log types already assigned to selected machine IDs.

Replace

Replaces all event log types assigned to selected machine IDs with the event log types listed in the **Assigned Event Types** list.

Clear All

Clears all event log types assigned to selected machine IDs.

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.

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.

● Agent is currently offline

🔵 User Logged In and Agent is Active

🟡 User Logged In and Agent is Inactive

🟢 User Not Logged In and Agent is online

🟢 User Not Logged In and Agent is Idle

🔴 The agent has been suspended

▣ Agent has never checked in

Machine.Group ID

The list of Machine.Group IDs displayed is based on the **Machine ID / Group ID filter** *(page v)* and the machine groups the user is authorized to see using System > User Security > Scopes.

Delete Icon

Click the delete icon ✕ to delete this record.

Edit icon

Click the edit icon 📝 next to a machine ID to automatically set header parameters to those matching the selected machine ID.

Assigned Categories

The event categories stored by the VSA for this machine ID and event log:

- Error
- Warning
- Information
- Success Audit
- Failure Audit
- Critical
- Verbose

Screen Recordings

Agent > Agents > Screen Recordings

The **Screen Recordings** page lists selected Kaseya Remote Desktop session recordings. Recordings can be set by policy using the Remote Control > User Role Policy and Machine Policy pages. See Recording KRC Sessions.

Storage Limit

Each partition is allocated a fixed storage space, using the System > Server Management > Storage Configuration page. Recordings are automatically removed, based on the **Length of time to keep logs** setting on this page.

Actions

Select a machine.

- **(View)** - Click the link of a listed `*.webm` video recording file to download it. Run the `*.webm` file in your preferred browser.
- **Delete** - Delete a selected row.

File Grid

A list of screen recording files is displayed for the selected machine:

- **File Name** - Comprised of VSA user that recorded the session and date/time the recording started in server time. Click on the hyperlink to download the recording.

> **Note:** *Logged in user's time zone offset from System > User Settings > Preferences is not applied.*

- **Date Created** - Date/time the screen recording was uploaded to the VSA server (typically the time the recording was finished), displayed as logged in user's time zone.
- **Expiration Date** - Date/time the screen recording will be deleted from the VSA server, displayed as logged in the user's time zone.

Automatic Update

Agent > Agents > Automatic Update

- *This page only displays for master role users.*

The **Automatic Update** page enables you to update agents to the latest version automatically. Scheduling is staggered to avoid bandwidth issues.

1. Check **Enable Automatic Updates**.
2. Enter the number of agents to update during each recurring interval.
3. Enter the number and type of recurring intervals.
4. Click **Save Auto Update Settings** to start scheduling agent updates automatically to the latest version.

Settings

- **Enable Automatic Updates** - If checked, automatic updates are enabled.
- **Update Agents** - The number of agents to update during each recurring interval.
- **Recurring Interval** - The number of time periods to wait between update sessions.
- **Recurrence Type** - `minutes`, `Hourly`, `Daily`

Manage Packages

Agent > Packages > Manage Packages

The **Manage Packages** page creates and distributes an agent install package to *multiple* machines.

> **Note:** You can quickly create agent packages for any machine group using the **Deploy Agent URL** link on the System > Manage > General tab or Machine Groups tab.

Agent Install Packages

Agents are installed on managed machines using an **agent install package**. An agent install package contains all the settings you prefer an agent to work with on a target machine.

The Agent > **Manage Packages** page displays the agent install packages that are available in your VSA. A `Default Install` package is provided with the VSA. You might see other agent install packages already created and listed on this page.

An agent install package is created using the **Create Agent Package** wizard. The wizard copies agent settings from an *existing* machine ID or machine ID template and generates an install package called `KcsSetup.` All settings and pending agent procedures from the machine ID you copy from—except the machine ID, group ID, and organization ID—are applied to every new machine ID created with the package.

Updating the Agent Software

An agent install package always downloads a `KcsSetup.exe` that uses the latest version of the agent software available. Once the `KcsSetup.exe` file is created, its version of the agent software remains fixed within the exe. Consider replacing `KcsSetup.exe` files that were created a while ago, then stored in network locations or added to CDs for ease of distribution. Similarly, the version of agent software installed on machines always remains fixed, until you update them using the **Manage Agents** *(page xi)* page.

> **Note:** See the PDF quick start guide, ***Agent Configuration and Deployment*** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/EN_AgentDeployment_R95.pdf#zoom=70&navpanes=0).*

Actions

- **Create** - Creates a new **Creating an Agent Install Package** *(page xxii)*.
- **Edit** - Edits a selected **Creating an Agent Install Package** *(page xxii)*.
- **Delete** - Deletes a selected agent install package.
- **Share** - Shares a selected agent agent install package. See Legacy Share Options.
- **Settings**
  - **Set as Default Install Package**
  - **Show on Download Page** - Adds the select agent install package to the **Download Page**. Machine users can use your VSA's `dl.asp` page—formatted as `http://<YourVSAaddress>/dl.asp`—to download agents without having to log into your VSA.
  - **Remove from Download Page**
- **Download Page** - Displays the `dl.asp` download page shown to machine users.
- Click the link underneath the **Name** of an install package to display a download link you can copy to your clipboard or into an email message. Anyone who receives an email with that link can click it to install the agent package.
- Click the **Download Package** link for an install package to immediately download that package to your local machine.

Additional Topics

- **Creating an Agent Install Package** *(page xxii)*
- **Manually Installing the Agent** *(page xxiii)*
- **Automating the Installation of the Agent** *(page xxiv)*
- **Configuring Agent Settings** *(page xxv)*
- **Agent Install Command Line Switches** *(page xxviii)*
- **Install Issues and Failures** *(page xxix)*
- **Installing Multiple Agents** *(page xxx)*
- **Installing Linux Agents** *(page xxxii)*
- **Supported Linux Functions** *(page xxxiii)*
- **Supported MacOS Functions** *(page xxxiii)*

Actions

- **Click to download default Agent** - Click this link to download the current VSA user's default package directly from this page.
- **Users can download agents from** - Paste this hyperlink into an email message. The *unique ID number* ensures that when the link is clicked in the email message, the default install package is selected and downloaded. Set a different install package as the default to display the link for that install package.
- **Manage packages from all administrators** - Check to display all packages created by all VSA users. Once a hidden package is displayed, you can use the package or make the package public. This option only displays for master role users.

Table Columns

- **Set Default** - Specify your own default install package by selecting the radio button to the left of the package name in the **Set Default** column.
- **Delete Icon** - Click the delete icon ✗ to remove a package from the paging area. If you created the package, then this also deletes the package from the system and removes it for all VSA users.
- **Edit Icon** - Click the edit icon 📝 next to a package to change parameters for that package using the **Create Agent Package** wizard.
- **Package Name** - Lists the name of the package.
- **Public Package** - Public package rows display with a brown background. Private package rows display with a gray background.
- **Share** - Click **Share** to share a private package with other users, user roles or to make the package public.
- **List on dl.asp** - Click the **dl.asp** link in the column header to display the web page machine users see when they install an agent on their machine. Check a box in this column to include its package in the list of available download packages on the **dl.asp** page.
- **Description** - Displays the description of the package.

Creating an Agent Install Package

On the Agent > **Manage Packages** *(page xxi)* page, click **Create** to start the **Create Agent Pack** wizard. The wizard is a 7 step process.

> **Note:** To save changes to an existing agent package that is not shared `Master` users can **Take Ownership** of the agent package using the **Share** button.

1. Specify how the machine id is assigned.
   - ➢ Prompt the user to enter a machine ID.

- ➢ Use the computer name as the machine ID.
- ➢ Set the user name of the currently logged on user as the machine ID.
- ➢ Specify a fixed machine ID for this install package.

2. Specify how the group id is assigned
   - ➢ **Existing Group** - Select an existing group ID from a drop-down list.
   - ➢ **Domain Name** - Uses the user's domain name.
   - ➢ **New Group** - Specify a new group ID. This option only displays for master role users.
   - ➢ **Prompt User** - Asks user to enter a group ID. This option only displays for master role users.
3. Optionally specify installer options using **command line switches** *(page xxviii)*. This includes the ability to install silently without any task bars or dialog boxes.
4. Optionally select a machine from the **Agents** list to copy settings from. This is oftentimes a machine ID template account. All copied settings and pending agent procedures—except the organization ID, machine ID, and group ID—are applied to every new machine ID created with the package.

   If **Do Not Copy Settings** is checked, default agent settings are used. If unchecked, click **Select Copy Agent** to select the agent or agent template account to copy settings from.
5. Select the operating system you are creating the install package for: `Windows`, `Mac - Intel`, or `Linux`.
6. For Mac packages, optionally bind a user logon credential to the install package. Fill in the Administrator Credential form to securely bind user rights to the install package.
   - ➢ Users without administrator rights can install the package successfully without having to enter an administrator credential.
   - ➢ If the administrator credential is left blank and the user does not have administrator rights to install software, the install package prompts the user to enter an administrator credential during the install. **If the package is also silent `KcsSetup` will fail without any dialog messages explaining this.**
7. Provide a name and description for the install package for easy reference later. This name displays on the **Manage Packages** page and the `dl.asp` download page.
8. Optionally set the new install package as the default install package.
9. Optionally show the install package on the download page.

Manually Installing the Agent

Manually Downloading Install Packages from the Manage Packages Page

The **Manage Packages** page provides three types of links for downloading agent install packages:

- Click the link underneath the **Name** of an install package to display a download link you can copy to your clipboard or into an email message. Anyone who receives an email with that link can click it to install the agent package.
- Click the **Download Package** link for an install package to immediately download that package to your local machine.
- Select an install package and click the **Download Page** to display a download link you can use to download the package to your local machine.

Any of these methods downloads the same `KcsSetup` file used to install the agent.

Installing an Agent Using the Download Page (on premises only)

The following is the fastest way to install an agent manually.

> **Note:** The `dl.asp` download page is available to install partition 1 agents in an on-premise VSA, whether or not tenants are created using the Tenant Management module. The `dl.asp` page is not available in any partition in SaaS environments.

1. Log on to any machine you want to install an agent on.
2. Enter the following URL in the browser of that machine:

   `http://<YourVSAaddress>/dl.asp`
3. Click the `Default Install` package to begin installation of the agent on that machine.
   - If other install packages are listed, select your preferred install package.
   - Once the install starts you may have to confirm the installation to ensure it completes.
4. Logon to your VSA:

   `http://<YourVSAaddress>`
5. Within the VSA, select the Agent > **Manage Agents** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#250.htm)* page.

You should see a new machine account listed on this page for the agent you just created.

Executing the Agent Install Package on the Endpoint Machine

Users can execute the `KcsSetup` installer on the endpoint machine using any of the following methods:

- *Windows*
  - Double-click the `KcsSetup` to launch it.
  - Open a **command line window** and type `KcsSetup` followed by any desired **command line switches** *(page xxviii)*.
  - Select **Run...** from the **Windows Start** menu and type `KcsSetup` followed by any desired command line switches.
- *MacOS and Linux*

> **Note:** For MacOS, installing an agent from flash driver is not supported.

- Double-click `KcsSetup` to launch it.
- The full filename for a MacOS agent install package is `KcsSetup.app`. `KcsSetup.app` is downloaded as a `KcsSetup.zip` which contains `KcsSetup.app` inside a folder titled `Agent`. Click the `KcsSetup.zip` file to expand it, click the `Agent` folder, then click the `KcsSetup.app` file to execute it.

> **Note:** For MacOS, **command line switches** *(page xxviii)* can only be used when creating the agent install package.
>
> **Note:** For Linux, see **Installing Linux Agents** *(page xxxii)* for more detailed instructions.

Reinstalling Agents

The **Create** *(page xxxiv)* page enables you to re-install an agent for an existing machine ID account.

Automating the Installation of the Agent

You can use the following methods to automate the installation of agent install packages:

Logon

- **Windows** - Set up an **NT logon** procedure to run the install package every time a user logs into the network. See system requirements.

- **Apple** - Set up an **Apple OS X Login Hook Procedure** to run the install package every time a user logs into the network. See Apple KB Article **HT2420** *(http://support.apple.com/kb/HT2420)*.

Procedure

1. Create the deployment package using the Agent > **Manage Packages** wizard.
   - The `KcsSetup` installer skips installation if it detects an agent is already on a machine if the `/e` switch is present in the installer package.
   - You will probably want to select the silent install option.
   - It may be necessary to bind an administrator credential if users running the logon procedure don't have user rights.
2. Download the appropriate `KcsSetup` installer package using the `dl.asp` page and copy it to a network share which users can execute programs from.
3. Add `KcsSetup` with its network path to the logon procedure.

Email

Email `KcsSetup` to all users on the network. Download the appropriate install package from the **Manage Packages** page, then attach it to an email on your local machine. You can also copy and paste the link of the default install package into an email message. Include instructions for launching the package, as described in the **Manual** bullet below.

Discovery by Network or Domain

Use the **Discovery** module to discover machines on **Networks** *(http://help.kaseya.com/webhelp/EN/KDIS/9050000/index.asp#1944.htm)* and **Domains** *(http://help.kaseya.com/webhelp/EN/KDIS/9050000/index.asp#10750.htm)*, then install the agents on discovered machines, either manually or automatically.

Automatic Account Creation

You should be aware that *automatic account creation* is enabled using System > **Check-in Policy** to automatically create a machine ID account when an agent install package is installed. This option is enabled by default when the VSA is installed.

Assigning New Machine IDs to Machine Group by IP Address

You may choose to create a "generic" install package that adds all new machine accounts to the `unnamed` group ID. When the agent checks in the first time, the System > **Naming Policy** assigns it to the correct group ID and/or sub-group ID using the IP address of the managed machine. Agent settings can be configured afterward by policy or template. See:

- **Configuring Agent Settings Using Policies** *(page xxvi)*
- **Configuring Agent Settings Using Templates** *(page xxvii)*

Configuring Agent Settings

Agent Settings

Agent settings determine the behavior of of the agent on the managed machine. Although each agent can be configured individually, it's easier to manage machines if you adopt similar settings for each type of machine you manage. For example, laptops, desktops and servers could all have settings that are unique to that type of machine. Similarly, machines for one customer may have unique characteristics that differ from the machines used by other customers. Type of agent settings include:

- Agent Credential
- **Agent Menu** *(page xlii)*
- **Check-in Control** *(page xliv)*

- **Working Directory** *(page xi)*
- **Logs** *(page xvi)*
- **Edit Profile** *(page xlvii)*
- View Collections
- Portal Access
- Remote Control Policy
- Patch Settings
- Patch File Source
- Patch Policy Memberships
- Alerts
- Event Log Alerts
- Monitor Sets
- Distribute Files
- Scheduled Agent Procedures

Policies vs Templates

There are two general methods of maintaining agent settings on multiple machines.

- **Configuring Agent Settings Using Policies** *(page xxvi)* - This is the preferred, *dynamic* method of managing agent settings on hundreds, even thousands, of machines. Once a policy is applied to a target machine, propagation is automatic.
- **Configuring Agent Settings Using Templates** *(page xxvii)* - This is the legacy, *static* method of maintaining agent settings on multiple machines. Agent settings must be manually copied to each target machines each time you make a change.

Configuring Agent Settings Using Policies

The **Policy Management** (KPM) module in the VSA manages *agent settings by policy*. Once policies are assigned to machines, machine groups or organizations, *policies are propagated automatically*, without further user intervention.

The System Management Wizard

A policy setup wizard is located on System > Orgs/Groups/Depts/Staff > Manage > Systems Management tab.

The **Systems Management Configuration** setup wizard enables you to quickly *configure and apply machine management policies for a specific organization.* Once configured, these polices are assigned to each machine you manage on behalf of that organization. Policies govern many different aspects of machine management:

- Audit scheduling
- Monitoring
- Alerts
- Patch Management
- Routine machine maintenance using agent procedures

With policies you no longer have to manage each machine individually. You only have to assign or change the policy. A policy assignment or a change within an assigned policy is propagated within 30 minutes to all member machines without you having to schedule anything. Once applied, you can quickly determine whether managed machines are in compliance or out of compliance with their assigned policies. Compliance tracking by individual policy provides you with the information you need to deliver IT services consistently throughout the organizations you manage.

> **Note:** See the **Standard Solution Package** for a detailed explanation of each option in the **setup wizard** *(http://help.kaseya.com/webhelp/EN/SSP/9050000/index.asp#11220.htm).*

Configuring Agent Settings Using Templates

Machine ID Templates

A machine ID template is *a machine ID record without an agent*. Since an agent never checks into a machine ID template account, it is not counted against your total license count. You can create as many machine ID templates as you want without additional cost. When an agent install package is created, the package's settings are typically copied from a selected machine ID template. Machine ID templates are usually created and configured for certain types of machine. Machine type examples include desktops, Autocad, QuickBooks, small business servers, Exchange servers, SQL Servers, etc. **A corresponding install package can be created based on each machine ID template you define.**

- Create machine ID templates using Agent > **Create** *(page xxxiv)*.
- Import a machine ID template using Agent > **Import/Export** *(page xli)*.
- Base an agent install package on a machine ID template using Agent > **Manage Packages** *(page xxi)*.
- Copy *selected* settings from machine ID templates to existing machine ID accounts using Agent > **Copy Settings** *(page xl)*.
- Identify the total number of machine ID template accounts in your VSA using System > Statistics.
- Configure settings for the machine ID template using the standard VSA functions, just as you would a machine ID account with an agent.
- Separate machine ID templates are recommended for Windows, Apple and Linux machines. Alternatively you can create a package that selects the appropriate OS automatically and copy settings from a template that includes an agent procedure that uses OS specific steps.

To apply a machine ID template to a package:

1. Use the **Create Agent Package** wizard in **Manage Packages** to use the template as the source machine ID to copy settings from when creating the package to install.
2. Add additional attributes to the package using this same wizard. These additional attributes usually differ from one customer to the next and therefore cannot be usefully stored in the template.

Copying Agent Settings

Machine ID templates are initially used to create an agent install package using the template as the source to copy settings from. But even after agents are installed on managed machines, you'll need to update settings on existing machine ID accounts as your customer requirements change and your knowledge of the VSA grows. In this case use Agent > **Copy Settings** to copy these changes to any number of machines IDs you are authorized to access. Be sure to select `Do Not Copy` for any settings you do not want to overwrite. Use `Add` to copy settings without removing existing settings. Kaseya recommends making changes to a selected template first, then using that template as the source machine ID to copy changes from. This ensures that your machine ID templates remain the "master repositories" of all your agent settings and are ready to serve as the source of agent install packages and existing machine ID accounts.

Templates and Filtered Views

There is a corresponding relationship between machine ID templates and filtering your view of selected machines using the **Only show selected machine IDs** view definition option. For example, if you define a machine ID template called "laptops", then it's easier to apply settings to all the "laptops" you're responsible for if you have a filtered view called "laptops". Simply select the view for "laptops" and only laptops are displayed on any function page, regardless of the machine group they belong to. The same idea applies to "desktops", "workstations", Exchange servers", etc.

Filtered views of selected machines are particularly useful when you're getting ready to copy settings from a machine ID template to existing agents using the **Copy Settings** function described above.

Base Templates and Audits

Since you can never be sure what settings should be applied to a machine until you perform an audit on the machine, consider installing an agent package created from a "base" template that has most of the agent settings *turned off*. Once you have the audit, then you can decide which settings should go on which machine. Use the **Copy Settings** function to copy settings from the appropriate template to the new agent.

Agent Install Command Line Switches

Agent install command line switches for `KcsSetup` are case insensitive and order independent. Separate switches with an empty space. For example: `KcsSetup /e /g=root.unnamed /c`

> **Note:** For Apple agents, command line switches can only be used when creating the agent install package.

`/b` - Reboot the system after installation completes. Agent installation requires a reboot in order to load its drivers. Use this switch on packages given to users that do not have rights to shut down the computer.

`/c` - Use the computer name as the machine ID for the new account. If the computer name cannot be determined programmatically, the machine user is prompted to enter a machine ID. The exception is silent mode, `/s`, in which case the installation stops and an error is logged to the installation log.

`/d` - Use the current domain name as the group ID for the new account. If the domain name cannot be determined programmatically, the machine user is prompted to enter the group ID. The exception is silent mode, `/s`, in which case the installation stops and an error is logged to the installation log.

`/e` - Exit immediately if the installer detects that an agent is already installed. Use `/e` at the end of logon procedures. `/k` or `/r` overrides `/e`.

`/f "Publisher"` - Specifies the full name of the service provider or tenant. Windows only.

`/g=subgroup.group.org` - Specifies the group ID to use for the new account. Group ID for existing group must match how its displayed in System > Orgs/Groups/Depts/Staff > Manage > Machine Groups tab.

> **Note:** Machine ID reverses the Group ID, so it will appear as `machine.subgroup.group.org` after checking in. When selecting the group in Agent Install package, it will display as org.group.subgroup in the user interface.

`/h` - Display the help dialog box listing all the command line switches, unless the `/s` switch is set, in which case the application exits.

`/i` - Ignore non-critical errors such as incorrect or indeterminate versions of WinSock2, or indeterminate versions of the OS, and force the installation to proceed.

`/j` - Does not install an agent shortcut to the **Start > All Programs** menu. Windows only.

`/k` - Displays a dialog box asking the user if it is OK to re-install when the agent is already detected on the machine. Without this switch, the installer exits if an agent is already present.

`/m=xxx` - Specifies the machine ID to use for the new account. `xxx` must be an alpha-numeric string and can not contain spaces or any punctuation marks except period(.).

`/n = partitionId` - Specifies the partition ID of the tenant partition the installed agent/machine ID account is a member of.

`/o "Company Title"` - Specifies the company title of the service provider or tenant. Windows only.

`/p "install_path"` - Overrides the default installation path by specifying the full directory path, including drive letter, in which to install the agent.

- On Windows, by default, the agent installation creates a directory using the `%ProgramFiles%` variable path as `\<company>\<Agent-Instance-Guid>`.

- On Linux, by default, the agent installation creates a directory named `/opt/Kaseya/<Agent-Instance-Guid>`
- On Apple, the /p switch is not supported & ignored.

> **Warning:** Kaseya does not support installing agents in the `%windir%` (typically `c:\windows`) directory.

`/r` - Executes the installation program and re-installs the agent even if an agent is already on the machine.

`/s` - Runs in silent mode. Suppresses all dialog boxes.

`/t "Title"` - Specifies the title of any dialog windows shown to the machine user during installation. The default title is: `"Kaseya Agent"`.

`/u` - Uses the current machine user name as the machine ID for the new account. If the machine user name cannot be determined programmatically, the user is prompted to enter a machine ID. The exception is silent mode, `/s`, in which case the installation stops and an error is logged to the installation log.

`/v` - Associates this agent with an existing agent account in the VSA when the machine name, agent name and organization are the same for the same partition. Ignores creating a new agent account when a new MAC address is detected. Suitable for re-using existing agent accounts created for reverted VDI resources.

`/w` - Overwrites the existing configuration file with a configuration file included in the agent installation. Use with the `/r` switch to re-install an agent with new server settings. Intended for an existing agent that is attempting to connect to a server that no longer exists. A green check displays in the VDI column of the **Manage Agents** *(page xi)* page if the /v agent install switch was used to install an agent to an existing agent account.

`/x` - Disables remote control after successfully installing the agent. This option is ignored when updating or re-installing. Remote control of this machine can only occur after the user selects **Enable Remote Control** by right clicking the K icon on the system tray.

`/z “Message”` - Specifies the message shown to the user when installation completes. The exception is silent mode, `/s`, in which case the installation completes and the status message is written to the installation log. The default message is: "`The Agent has been installed successfully on your computer.`”

`/?` = Display the help dialog box listing all the command line switches, unless the `/s` switch is set, in which case the application exits. Windows only.

Linux Only Install Switches

See **Installing Linux Agents** *(page xxxii)*.

Install Issues and Failures

The following issues and failures can occur when installing agents:

- **Invalid Credential** - The credential bound to the package must have administrator rights on the local machine. The agent installs as a system service requiring full administrator privileges to install successfully. The administrator name may be a domain user of the form `domain\administrator` or `administrator@domain`. On Vista, 7, and 2008 machines, ensure User Account Control (UAC) is disabled for the administrator rights credential being used.
- **Domain Specified for a Machine Not in the Domain** - If, in step 2 of package creation in **Manage Package**, the **Domain Name** option is selected and the computer is not part of a domain, an installation package will peg the CPU at 100% during install, but eventually install.
- **Blocked by Anti-Virus Program** - Some anti-virus programs may classify the agent installation as a security threat and block its execution.

- **Blocked by Security Policy** - Local or domain security policies may prevent access to the installation directory, typically by default the `Program Files` directory.
- **Insufficient Licenses** - The agent may be prevented from checking in the first time and creating an account if there are insufficient VSA licenses available. When this happens a gray K icon appears in the system tray just after the agent is installed on the machine and never turns blue. A tooltip displays when the cursor is placed over the gray agent icon and reports "'Machine ID.Group ID' not recognized by the Kaseya Server".

MacOS

- MacOS agents cannot be deployed silently without a valid username and password.

Installing Multiple Agents

Multiple agents can be installed on the same managed machine, each checking into different VSAs. *Run the R95 agent installer from a different VSA* and you will get an additional agent.

- Applies to Windows and Linux agents. Installing multiple MacOS agents is not supported.
- A R95 agent can co-exist with other R95 agents.

Driver Usage - Windows Agents Only

If multiple agents are installed on a machine, only one agent at a time controls the drivers required to use **File Access** *(page lvi)*, **Network Access** *(page lvii)*, **Application Blocker** *(page lx)*. These functions can only be performed by the agent controlling these drivers.

- Originally the first agent installed controls the drivers.
- If the first agent controlling the drivers is uninstalled, then these drivers are uninstalled as well and these three functions cannot be performed by any agent.
- These drivers are re-installed by either of the following events:
  - Any of the existing agents on the machine are updated. The updated agent takes control of the drivers and can perform these three functions.
  - A new agent is installed. The newly installed agent takes control of these drivers and can perform these three functions.
- To determine which agent has control of the drivers, see *Registry* below.

Identifying Agents on Managed Machines

When a Kaseya agent is installed, a *unique identifier* is created for the agent comprising the Kaseya Server's 6 character customer ID and a randomly generated 14 digit number. This unique agent identifier, called the agent GUID, is used to create separate sub-folders to store agent program files, and as a sub-key for agent registry values.

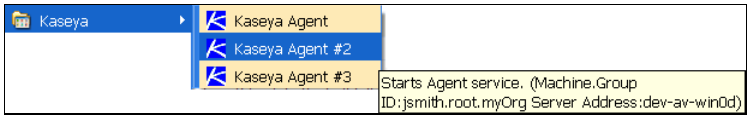
In the examples below, agents display specific information for the following placeholders:

- `<GUID>` - The agent instance GUID.
- `<company>` - The agent's install directory.
- `<serveraddress>` - The Kaseya Server address the agent checks into.
- `<machineID.groupID.orgID>` - The machine ID, group ID, and organization ID of the agent on the Kaseya Server.
- `<shortcutname>` - The name of the shortcut. Example: `Kaseya Agent #2`.

Shortcuts

When you move the mouse cursor over a Kaseya Agent shortcut—for example, a shortcut on the Windows Start Menu—a tool tip displays as:

- `Start Agent service. (machine.GroupID:<machineID.groupID.orgID> Address:<serveraddress>)`
- If you right click a shortcut, you'll also see this text in the comment field of the shortcut property page.



Starts Agent service. (Machine.Group ID:jsmith.root.myOrg Server Address:dev-av-win0d)

About Agent

Right click the K icon in the system tray of a managed machine and select the **About Agent** option to display the following information:

- Agent Version
- Server Address - `<serveraddress>`
- Product ID - `<GUID>`
- Program Title - `<shortcutname>`

Windows Agents

Add/Remove

Agents display as follows:

- `Kaseya Agent (<machineID.groupID.orgID> - <serveraddress>)`
- `Kaseya Agent #2 (<machineID.groupID.orgID> - <serveraddress>)`
- `Kaseya Agent #3 (<machineID.groupID.orgID> - <serveraddress>)`

Services

The description field of the service displays the same text shown above in the agent shortcut.

Registry

Agent registry settings displays as follows:

```
HKLM\Software\Kaseya\Agent
   DriverControl - The agent that controls driver usage.
   KES_Owned_By - The agent that manages the KES client.

HKLM\Software\Kaseya\Agent\<GUID>
   Title - <shortcutname>
   Path - C:\Program Files\<company>\<GUID>
   ServAddr - <serveraddress>
   machineID - <machineID.groupID.orgID>
   DriverControl - The agent that controls driver usage.
   KES_Owned - The agent that manages the KES client.
```

Default Agent Installation Folders

- See the `/p` switch in **Agent Install Command Line Switches** *(page xxviii)*.

Installing Linux Agents

> **Note:** See **System Requirements** *(http://help.kaseya.com/WebHelp/EN/VSA/9050000/reqs/index.asp#home.htm)* for supported Linux operating systems and browsers.

Installing Linux Agents Manually

1. From a Linux machine open a Firefox or Chrome browser in a Gnome session and log into the VSA.
2. Display the Agent > Install Agents > **Manage Packages** *(page xxi)* page.
3. Create a Linux agent install package—if one does not already exist—by clicking **Create** and stepping through the **Create Agent Package** wizard.
   - Ensure **Select Agent Type** is set to `Linux`.
4. Click the Linux agent install package you just created to begin downloading the agent.
5. Once the download is complete, locate the `KcsSetup.sh` file in the download directory of the Linux machine.

   > **Note:** If you have downloaded `KcsSetup.exe` or `KcsSetup.zip`, you have downloaded the wrong install file because the selected install package is dedicated to Windows or MacOS installs.

6. Issue the following commands as root:

   ```
   # chmod +x KcsSetup.sh
   # ./KcsSetup.sh
   ```

   The agent installs and starts. Log into your VSA and view the status of the agent.

   For further information see the install log file, located at:
   `/tmp/KASetup_<pid>.log`
   where <pid> is the process id of the `./KcsSetup.sh` execution.

   > **Note:** Run `KcsSetup.sh -V -D` for verbose terminal output.
   >
   > **Note:** Run `KcsSetup.sh -X` to save the temp files created in the /tmp file. Saving these files is useful when troubleshooting a failed install.

7. After the Linux agent is installed, log in and log out to see the Kaseya agent icon in a Gnome panel.

Installing Linux Agents after Scanning Networks

1. Schedule a Discovery > **By Agent** *(http://help.kaseya.com/webhelp/EN/KDIS/9050000/index.asp#1944.htm)* scan *using an existing Linux agent as the discovery machine*.
2. Install a Linux agent on a discovered Linux machine using one of the Discovery > Discovered Devices pages.
   - Enter `root` in the **Admin Logon** field.
   - Enter the password for the `root` user of the targeted Linux machines in the **Password** field.
   - Select an agent install package in the **Select an Agent Package to install** field.
   - Check the checkboxes next to one or more targeted Linux machines, or enter the IP address or name of a targeted Linux machine in the **undiscovered machine** field.
   - Click the **Submit** button.

   > **Note:** The **Install Agents** page does not currently distinguish between Linux and other systems. It is the installer's responsibility to select only Linux systems.

Uninstalling a Linux Agent Manually

A `<install-dir>/bin/KcsUninstaller` always gets installed with the agent and will remove the agent. Agents are typically installed to the `/opt` directory.

Issue the following commands as root:

```
# ./KcsUninstaller
```

> **Note:** Run the command `./KcsUninstaller -D -V` to uninstall the agent with verbose terminal output.

Troubleshooting Linux Agents Installs

- See the **Troubleshooting Linux Agent Installs** *(https://helpdesk.kaseya.com/entries/36223968)* community page.

Supported Linux Functions

Linux agents support the following functions:

- 'Headless' agent procedures
- Latest audits, baselines audits and system audits
- The SSH page in the legacy Remote Control module
- Selected alerts
- Monitoring of Processes
- Monitoring of SNMP
- Log Parser
- Site Customization - The **Agent Icons** tab includes a set of icons for Linux agents you can customize.
- Live Connect - See **Live Connect Requirements** *(http://help.kaseya.com/WebHelp/EN/VSA/9050000/reqs/#37313.htm)* for supported Linux versions.

See **System Requirements** *(http://help.kaseya.com/WebHelp/EN/VSA/9050000/reqs/index.asp#home.htm)*.

Supported MacOS Functions

MacOS agents support the following functions:

- Audits - selected hardware and software attributes
- Agent procedures
- Remote Control
- FTP
- SSH
- Reset Password
- Task Manager
- Live Connect
- Kaseya Remote Control
- Live Connect (Classic)
- Network scan via Discovery

> **Note:** MacOS is not currently supported for Probe Machine, but devices running macOS are discovered by the Network Discovery.

- Supported monitoring:

- SNMP monitoring
- Process monitoring in monitor sets
- System Check
- Log Parser

See **System Requirements** *(http://help.kaseya.com/WebHelp/EN/VSA/9050000/reqs/index.asp#home.htm)*.

Templates

Create

Agent > Templates > Create

The **Create** page creates a machine ID account and optionally agent install package for a *single* machine. You create the machine ID account first, then create an install package for this single machine. Typically the **Create** page applies to:

- **Machine ID templates** - In this case, no install package need be created, since machine ID templates are not intended for installation to a machine.
- **Reinstalling Agents for an Existing Account** - Because the **Create** install packages does *not automatically create a new machine ID account*, you can use the **Create** page to *re-install* agents on managed machines for *existing* accounts.
- **Secured environments** - Secured environments may require each machine be setup manually. For example, you might be required to name a new machine ID account manually and/or create an agent install package with a unique credential for a single machine. A user must be logged into a target machine locally to install the package.

> **Note:** Use Agent > **Manage Packages** *(page xxi)* to create and distribute agent install packages to *multiple* machines. The **Manage Packages** install package *automatically creates a machine ID account* when it is installed provided automatic account creation is enabled using System > Check-in Policy.
>
> **Note:** Use **Discovery** to install agents *on remote systems*.

Machine IDs vs. Agents

When discussing agents it is helpful to distinguish between the machine ID / group ID / organization ID and the agent. The machine ID / group ID / organization ID is the **account name** for a managed machine in the VSA database. The agent is the client software installed on the managed machine. A one-to-one relationship exists between the agent on a managed machine and its account name on the VSA. Tasks assigned to a machine ID by VSA users direct the agent's actions on the managed machine.

Agent License Counts

The following events affect agent license counts:

- An "unused" agent license is changed to "used" if a machine ID account is created and the agent installed.
- If the agent is deleted but not the account, the agent license is still considered "used".
- If the account is deleted, regardless of what happens to the agent, the agent license goes back to "unused".
- If an account is created, but the agent is not yet installed the first time, the account is called a machine ID template. Machine ID template accounts are not counted as "used" until you install the agent.

Including Credentials in Agent Install Packages

If necessary, an agent install package can be created that includes an administrator credential to access a customer network. Credentials are only necessary if users are installing packages on machines and *do not have administrator access* to their network. The administrator credential is encrypted, never available in clear text form, and bound to the install package.

Operating System Selection

Agent packages can be created to install agents on machines running either Windows, Apple, or Linux operating systems, or to automatically choose the type of operating system of the downloading computer.

Machine ID Templates

A machine ID template is *a machine ID record without an agent*. Since an agent never checks into a machine ID template account, it is not counted against your total license count. You can create as many machine ID templates as you want without additional cost. When an agent install package is created, the package's settings are typically copied from a selected machine ID template. Machine ID templates are usually created and configured for certain types of machine. Machine type examples include desktops, Autocad, QuickBooks, small business servers, Exchange servers, SQL Servers, etc.

A corresponding install package can be created based on each machine ID template you define.

- Create machine ID templates using Agent > **Create** *(page xxxiv)*.
- Import a machine ID template using Agent > **Import/Export** *(page xli)*.
- Base an agent install package on a machine ID template using Agent > **Manage Packages** *(page xxi)*.
- Copy *selected* settings from machine ID templates to existing machine ID accounts using Agent > **Copy Settings** *(page xl)*.
- Identify the total number of machine ID template accounts in your VSA using System > Statistics.
- Configure settings for the machine ID template using the standard VSA functions, just as you would a machine ID account with an agent.
- Separate machine ID templates are recommended for Windows, Apple and Linux machines. Alternatively you can create a package that selects the appropriate OS automatically and copy settings from a template that includes an agent procedure that uses OS specific steps.

Predefined Alerts

If you create a machine ID account using Agent > **Create** *and do not copy settings from any other machine*, then several typical alerts are created for the machine ID account by default.

Copy new account settings from

Click a radio button next to any machine ID listed in the paging area. Agent settings are copied from this machine ID.

> **Note:** If you don't include a machine ID to copy from and click **Create**, a new, usable machine ID account is created using Kaseya Server defaults.

New Machine ID

Enter a unique name for the new machine ID you are creating.

> **Note:** Machine ID names cannot include special characters such as: s: /[,[]#&%\'\"\/\:*?<>|]/g,"-".

Group ID

Select an existing group ID for the new machine ID you are creating. The default is `root.unnamed`. Group IDs are created by a VSA user using System > Orgs / Groups / Depts > Manage.

Create

Click **Create** to create the new machine ID for the selected group ID.

Set/Clear New accounts created in group ID <Group ID> copy settings from <Machine ID>

For each group ID you can specify a different default machine ID to copy settings from.

1. Select a machine ID to copy settings from by clicking the radio button next to any machine ID listed in the paging area.
2. Select a group ID from the group ID drop-down list.
3. Click the **Set** to ensure that new machine IDs you create for the selected group ID will copy settings from the selected default machine ID.
4. Click the **Clear** link to remove this assignment.

Set/Clear Accounts created in *unassigned* group IDs copy settings from <Machine ID>

This option specifies the default machine ID to copy settings from if no default machine ID is set for a group ID. This option only displays for master role users.

1. Select a machine ID to copy settings from by clicking the radio button next to any machine ID listed in the paging area. Initially this value is set to *unassigned*.
2. Click the **Set** to ensure that new machine IDs created without a group default machine ID copy settings from the master role user's default machine ID. Initially this value is set to *unassigned*.
3. Click the **Clear** link to remove this assignment.

Entering Contact Information

When you enter contact information on this page for a new machine ID account, then create the new machine ID account by clicking the **Create** button, these same contact information fields populate the Agent > **Edit Profile** *(page xlvii)* page. Contact information includes:

- **Contact Email** - Enter the email address of the individual using the managed machine.
- **Auto** - Check **Auto** to automatically populate the **Contact Email** field with an email address that uses the following format: `machineid@groupid.com`. This feature assumes you are creating machine IDs and group IDs that conform to user email addresses.
- **Contact Name** - Enter the name of the individual using the managed machine.
- **Contact Phone** - Enter the phone number of the individual using the managed machine.
- **Admin Email** - Enter the email address of the individual responsible for providing IT support for the managed machine.

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.

⚪ Agent is currently offline

🔵 User Logged In and Agent is Active

🟡 User Logged In and Agent is Inactive

🟢 User Not Logged In and Agent is online

🟢 User Not Logged In and Agent is Idle

🛑 The agent has been suspended

▣ Agent has never checked in

Copy Settings

Click a radio button next to any machine ID listed in the paging area. Machine ID settings are copied from this machine ID.

Download / Email Agent Installation

Click a machine ID link to create and distribute an install package for an existing machine ID account using the **Download Agent** wizard.

> **Note:** An install package created using this page is for a specific machine ID account. Use **Manage Packages** *(page xxi)* to create install packages for *multiple* machines.

1. Select the operating system you are creating the install package for: `Windows`, `MacOS`, or `Linux`.
2. Optionally bind a user logon credential to the install package. Fill in the Administrator Credential form to securely bind user rights to the install package.
   - Users without user rights can install the package successfully without having to enter an administrator credential.
   - If the administrator credential is left blank and the user does not have user rights to install software, the install package prompts the user to enter a administrator credential during the install.
3. Select the method of distribution.
   - **Download** - Download the install package immediately to the machine you are currently using. The install package is always called `KcsSetup`.
   - **Email** - Email a text message that contains a link to download the install package.

Type

The type of operating system used by the managed machine:

- Windows
- Macintosh
- Linux

First Checkin

Lists the time that each agent checked into the Kaseya Server for the first time.

Rename

Agent > Templates > Rename

The **Rename** page renames machine ID template accounts.

Procedure

1. Select a machine ID in the paging area.
2. Click one of the following radio buttons:
   - **Rename account** - Select this option to rename a selected machine ID account.
   - **Merge offline account <Offline Machine ID> into <Select Machine ID> Delete <Offline Machine ID> after merge** - Use merge to combine log data from two different accounts into the same machine. This could be necessary if an agent was uninstalled and then re-installed with a different account name. Merge combines the accounts as follows:
     - ✓ Log data from both accounts are combined.
     - ✓ Baseline Audit data from the old offline account replaces any baseline data in the selected account.
     - ✓ Alert settings from the selected account are kept.
     - ✓ Pending agent procedures from the selected account are kept. Pending agent procedures from the old offline account are discarded.
     - ✓ The old account is deleted after the merge.

> **Note:** Since the machine can only be active on a single account, only offline accounts are provided in the drop-down list to merge with.

3. Optionally enter in a **New Name** for the machine ID account.
4. Optionally select a different **Group ID** for the machine ID account.
5. Click the **Rename** button.

Rename

Click **Rename** to change the name of a selected machine ID account, using the options previously selected.

New Name

Enter the **New Name** for the selected machine ID.

Group ID

Select the **Group ID** to assign to the selected machine ID account. The default leaves the group ID unchanged.

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.

● Agent is currently offline

🔵 User Logged In and Agent is Active

🟡 User Logged In and Agent is Inactive

🟢 User Not Logged In and Agent is online

🟢 User Not Logged In and Agent is Idle

🛑 The agent has been suspended

▣ Agent has never checked in

Machine.Group ID

The list of Machine.Group IDs displayed is based on the **Machine ID / Group ID filter** *(page v)* and the machine groups the user is authorized to see using System > User Security > Scopes. Click the radio button to the left of the machine account you wish to rename.

New Name at Next Check-in

Lists the new name the account will be renamed to the next time that agent checks in. Only pending renames are displayed here.

Delete

Agent > Templates > Delete

The **Delete** page deletes machine ID template accounts.

> **Note:** To delete agent accounts use the Agent > **Manage Agents** page.

Deleting Templates

1. Select the Agent > **Delete** page.
2. Select one or more machine ID template accounts.
3. Click **Delete**.

4. Optionally click the **Clean Database** button. Deleting a machine account initially marks it for deletion. Actual deletion usually occurs during off hours to reserve resources during working hours. Click **Clean Database** to immediately purge machine accounts that are already marked for deletion.

Change Group

Agent > Templates > Change Group

The **Change Group** page assigns machine ID template accounts to different machine groups.

> **Note:** *Create a new machine group ID or sub group ID using System > User Security > Scopes.*

Moving a Machine ID to a Different Group

1. Select one or more machine ID templatesin the paging area.
2. Select a group ID from the **Select new group ID** drop-down menu.
3. Click the **Move** button.

Set Credential

Agent > Templates > Set Credential

The **Set Credential** page sets a credential for a machine ID template.

- **Username** - Enter the username for the credential. Typically this a user account.
- **Password** - Enter the password associated with the username above.
- **Domain**
  - **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. This makes it easier to **Select All** and rapidly set a common username/password on multiple machines, even if selected machines are members of different domains.
  - **Specify domain** - Manually specify the domain name to use for this credential.

Actions

- **Apply** - Assign the credential to all checked machine IDs. Machine IDs with assigned credentials display the username and domain in the associated table columns.
- **Clear** - Remove the credential from all checked machine IDs.
- **Auto Refresh Table** - Refreshes the table.

Configure Agents

Copy Settings

Agent > Configure Agents > Copy Settings

The **Copy Settings** page copies selected settings from a single source machine ID to multiple machine IDs. You can copy settings *from only one source* machine ID or template at a time. But you can copy different types of settings from different source machine IDs or templates in succession.

Copy Settings and Templates

Machine ID templates are initially used to create an agent install package using the template as the source to copy settings from. But even after agents are installed on managed machines, you'll need to update settings on existing machine ID accounts as your customer requirements change and your knowledge of the VSA grows. In this case use Agent > **Copy Settings** to copy these changes to any number of machines IDs you are authorized to access. Be sure to select `Do Not Copy` for any settings you do not want to overwrite. Use `Add` to copy settings without removing existing settings. Kaseya recommends making changes to a selected template first, then using that template as the source machine ID to copy changes from. This ensures that your machine ID templates remain the "master repositories" of all your agent settings and are ready to serve as the source of agent install packages and existing machine ID accounts.

Copy

Click **Copy** to select a source machine. Once you select the source machine a second window displays the types of settings you can copy.

By selecting only certain types of settings to copy, you can avoid overwriting customer specific settings you want to keep, such as the `Patch File Source`, which is different for each customer.

Select the `Add` option to add settings to target machines without replacing existing settings.

The types of agent settings you can copy include:

- Credential
- Agent Menu
- Checkin Control
- Working Directory
- Logs
- Machine Profile - Refers to settings in Audit > **Edit Profile** *(page xlvii)*.
- View Collections
- Portal Access
- Remote Control Policy
- Patch Settings
- Patch File Source
- Patch Policy Memberships
- Fixed Alerts - These are all the alert types on the Monitor > Alerts page except for `Event Log` alerts and `System` alerts.
- Event Log Alerts
- Monitor Sets
- Distribute Files
- Protection
- Agent Procedure Schedules

Select Machine ID

Click the **Select Machine ID** link to specify which machine ID to copy settings from.

Spread agent procedure schedules when copying to multiple machines

You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the scan on each machine ID is staggered by 5 minutes. For example, machine 1 runs at 10:00, machine 2 runs at 10:05, machine 3 runs at 10:10,

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.

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.

● Agent is currently offline
◉ User Logged In and Agent is Active
◉ User Logged In and Agent is Inactive
● User Not Logged In and Agent is online
◔ User Not Logged In and Agent is Idle
✋ The agent has been suspended
▣ Agent has never checked in

Machine.Group ID

The list of Machine.Group IDs displayed is based on the **Machine ID / Group ID filter** *(page v)* and the machine groups the user is authorized to see using System > User Security > Scopes.

Status

Shows the machine name that settings were copied from and the time they were copied.

Import / Export

Agent > Configure Agents > Import / Export

The **Import / Export** page imports and exports machine ID account settings as XML files, including scheduled agent procedures, assigned monitor sets and event sets. Log data is not included in the import or export. You can use **Import / Export** to migrate machine ID account settings, including machine ID templates, from one Kaseya Server to the next.

- When importing an XML file ensure the encoding of the file is ISO-8859-1.
- See **Copy Settings** *(page xl)* for a list of the types of settings associated with a machine ID account.
- For the latest instructions on migrating an existing Kaseya Server to a new machine see *Moving the Kaseya Server* section in the latest **Kaseya Server installation instructions** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/Install/index.asp#home.htm)*.
- Sample templates for specific types of machines can be imported and are available on the Kaseya forum in our **Kaseya Connections** website at **http://community.kaseya.com** *(http://community.kaseya.com)*.

To Export Machine ID Settings

1. Click the **select the machine** link. A machine selection dialog box displays.
2. Optionally filter the display of the machine IDs listed using the machine ID / group ID filter.

3. Click a machine ID link to export. The machine ID you selected now displays on the **Import / Export** page.
4. Click **Export**. The page displays an XML statement of the agent settings being exported.
5. Export the XML statement by:
   - Copying the XML text to the clipboard.
   - Right-clicking the **Download** link and selecting the **Save Target As** option to save the XML text as an XML file on your local computer.

To Import Machine ID Settings

1. When importing an XML file ensure the encoding of the file is ISO-8859-1.
2. Click **Browse** to select an XML file representing the settings of a machine ID account. Typically these XML files are created by exporting them from another Kaseya Server.
3. Click **Import**. A set of additional options displays.
4. Accept or specify the name of the machine ID. A new one is created if this name doesn't already exist in the Kaseya Server.
5. Accept or select a different group ID.
6. Optionally check the box next to **Replace existing data if this machine ID already exists**.
7. Optionally change the email notification address for all alerts defined for this machine ID account.
8. Click **Finish** to complete the import.

Agent Menu

Agent > Configure Agents > Agent Menu

The **Agent Menu** page specifies the options that display in the agent menu of a user's machine. The user displays the agent menu by right-clicking the agent icon in the system tray of the managed machine. This page can also *prevent* the agent icon from displaying on the user's machine. Changes made using this page take effect at the next agent check-in and display in red text until then.

Note: See **Agent Icons** *(page iii)* for a general explanation of how agent icons display on the user's machine.

Hiding the Agent Icon on the User's Machine

To hide the agent icon altogether:

1. Select one or more machine IDs.
2. Uncheck the **Enable Agent Icon** checkbox.
3. Click **Update**.

All of the other checkbox settings will become dimmed, indicating that all agent menu options have been disabled.

Preventing the User from Terminating the Agent Service on the User's Machine

If the **Exit** option is enabled on a user's managed machine, the user can terminate the agent service on the managed machine by selecting this option. When the agent service is stopped, the managed machine displays as offline to VSA users and can no longer receive commands from the Kaseya Server.

To remove the **Exit** option from agent menus on managed machines:

1. Select one or more machine IDs.
2. Uncheck the **Exit** checkbox.
3. Click **Update**.

Checkboxes

- **Enable Agent Icon** - Check to display the agent icon in the system tray of the managed machine. Uncheck to hide the agent icon and prevent the use of agent menu options.
- **About <Agent>** - Check to enable the machine user to click this option to display the About box for the installed agent. The default option label `Agent` can be customized.
- **Contact Administrator Menu** - Check to enable the machine user to click this option to contact an administrator. The label `Contact Administrator...` can be customized.
  - **User Logon page** - Displays the User Portal page for this machine.
  - `use <mid> for machine ID, <gid> for group ID, <guid> for agent GUID` - Displays a custom URL. Use the variables provided to construct a URL to a custom website you have created to administrate machines. For example: `http://www.yourcompany.com/?agentguid=<guid>` could display a website page you have created specific to an agent guid. Alternatively you could use the `<gid>` variable to construct a shared URL for all machines using the same machine group.
- **Company URL Menu / URL** - Check to enable the machine user to click this option to display the URL specified in the corresponding URL field.
- **Disable Remote Control** - Check to enable the machine user click this option to *disable* remote control on the user's managed machine.
- **Set Account...** - Check to enable the machine user to click this option to display their machine ID.group ID.organization ID and to change the Kaseya Server address the agent checks into. The new IP address you enter must point to a working VSA, or else the IP address change will not take effect.
- **Refresh** - Check to enable the machine user to initiate an immediate full check-in.
- **Exit** - Check to enable the machine user to terminate the agent service on the managed machine.

Update

Click **Update** to apply agent menu settings to selected machine IDs.

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.

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.

● Agent is currently offline

🔵 User Logged In and Agent is Active

🟡 User Logged In and Agent is Inactive

🟢 User Not Logged In and Agent is online

🟢 User Not Logged In and Agent is Idle

⛔ The agent has been suspended

▣ Agent has never checked in

Machine.Group ID

The list of Machine.Group IDs displayed is based on the **Machine ID / Group ID filter** *(page v)* and the machine groups the user is authorized to see using System > User Security > Scopes.

ACObSRx

This column summarizes the agent menu options enabled for a machine ID. **ACObSRx** applies to the keyboard shortcuts that are used to access each option in the agent menu.

A letter indicates that option displays in the agent menu. A "-" indicates that menu option does not display in the agent menu.

A = **A**bout Agent

C = **C**ontact User

O = Launches the URL specified in the URL field. The agent displays the text listed in the field to the left of the URL field.

b = Disa**b**le Remote Control

S = **S**et Account...

R = **R**efresh

x = E**x**it

About Title

The text appended to the label for the **About** option on the agent menu. For example, if the About Title is `Agent` then the label of the **About** option displays as `About Agent`.

Contact Title

The text displayed on the agent menu for contacting a VSA user.

Custom Title

The text displayed on the agent menu for contacting a custom URL.

Contact URL

The URL to display when the `Contact Administrator...` option is selected by the machine user. The default URL is the Portal Access page. A different URL can be entered.

Custom URL

The URL to display when this agent menu option is selected by the user.

Check-In Control

Agent > Configure Agents > Check-In Control

The **Check-In Control** page specifies when and where each agent should check in with a Kaseya Server. You can specify the primary and secondary Kaseya Server names/IP addresses used by the agent to check in, the bandwidth consumed by an agent to perform tasks and the check-in period.

- The agent only checks into the primary server but not the secondary server, unless the primary server goes offline.
- The primary and secondary Kaseya Server values and the minimum and maximum check-in periods are subject to the policies set using System > Check-in Policy. This prevents users from selecting settings that place undue stress on servers running the Kaseya Server service.
- Changes made using this page take effect at the next agent check-in and display in red text until then.
- **Check-in Control** information can also be maintained using the **Agent Settings** tab of the **Live Connect** *(page xxxvii)* and Machine Summary pages.

Secondary Server Limitations

Legacy remote control functions are relayed through the primary Kaseya Server address. When an agent checks into the secondary Kaseya Server address, legacy remote control sessions do not connect because they are directed to the wrong VSA relay server address. All other functions, including Kaseya Remote Control functions, are supported and scheduled by the secondary Kaseya Server in the same manner as the primary Kaseya Server address.

Migrating Agents from one Kaseya Server to Another

You may decide for performance or logistical reasons to migrate managed machines to a new Kaseya Server. For instructions, see **How to migrate agents to another VSA instance** *(https://helpdesk.kaseya.com/entries/100409247)*.

Changing the Port used by Agents to Check into the Kaseya Server

1. Set the **Primary** Port to the **new** port.
2. Set the **Secondary** Port to the **old** port.
3. Wait for the new settings to take effect on all the agents.
4. Display the System > Configure page. Enter the new port number in the **Specify port Agents check into server with** edit box and click the **Change Port** button.

> **Note:** If any agents have not migrated to the new port before you switch the Kaseya Server, you will have to manually change the port at the managed machine. Right click the agent icon in the system tray to display the agent menu on the managed machine and select the **Set Account...** option. Enter the server address and port. For example, `192.168.1.7:1234`.

Primary KServer

Enter the IP address or fully qualified host name of the machine ID's primary Kaseya Server. This setting is displayed in the **Primary Kaseya Server** column.

Kaseya agents initiate all communication with the Kaseya Server. For this reason the agents must always be able to reach the domain name or IP (Internet Protocol) address assigned to the Kaseya Server. Choose an IP address or domain name which can be resolved from all desired network(s), both on the local LAN and across the internet.

> **Best Practices:** Although a public IP address may be used, Kaseya recommends using a **domain name server (DNS)** name for the Kaseya Server. This practice is recommended as a precaution should the IP address need to change. It is easier to modify the DNS entry than redirecting orphaned agents.

Primary Port

Enter the port number of either the primary Kaseya Server or a virtual system server. This setting is displayed in the **Primary KServer** column.

> **Warning:** Do NOT use a *computer name* for your server. The agent uses standard WinSock calls to resolve a fully qualified host name into an IP address, which is used for all agent connections. Resolving a computer name into an IP address is done by NETBIOS, which may or may not be enabled on each computer. NETBIOS is an optional last choice that the Windows will attempt to use to resolve a name. Therefore, only fully qualified names or IP addresses are supported.

Secondary KServer

Enter the IP address or fully qualified host name of the machine ID's secondary Kaseya Server. This setting is displayed in the **Secondary KServer** column. The agent only checks into the primary server but not the secondary server, unless the primary server goes offline.

Secondary Port

Enter the port number of either the secondary Kaseya Server or a virtual system server. This setting is displayed in the **Secondary KServer** column.

Check-In Period

Enter the time interval for an agent to wait before performing a quick check-in with the Kaseya Server. A check-in consists of a check for a recent update to the machine ID account. If a recent update has been set by a VSA user, the agent starts working on the task at the next check-in. This setting is displayed in the **Check-In Period** column. The minimum and maximum check-in periods allowed are set using System > Check-in Policy.

> **Best Practices:** The agent maintains a persistent connection to the Kaseya Server. As a result, quick check-in times do not effect response times from the agent. The quick check-in time sets the maximum time to wait before re-establishing a dropped connection. Setting all your machine's quick check-in time to 30 seconds guarantees each agent recovers from a dropped connection within 30 seconds, assuming connectivity is successful.

Bind to Kserver

If checked, the agent is bound to a **unique Kaseya Server ID**. Bound agents cannot check-in successfully unless the unique Kaseya Server ID they are bound to using the Agent > **Check-in Control** *(page xliv)* page matches the unique ID assigned to the Kaseya Server using the System > Configure > **Change ID** option. Prevents IP address spoofing from redirecting agent check-ins. A lock 🔒 icon in the paging areas shows the agent is bound. To *unbind* agents, select machines IDs, ensure **Bind to Kserver** is unchecked and click **Update**. The lock 🔒 icon no longer displays for selected machines.

Bandwidth Throttle

Limit the agent to consuming a maximum amount of bandwidth on the system with this control. By default the agent shares bandwidth with all other running applications so you typically do not need bandwidth throttle enabled. Disable bandwidth throttle by entering a 0.

Warn if multiple agents use same account

The Kaseya Server can detect if more than one agent is connecting to the Kaseya Server and using the same machine ID.group ID.Organization ID. This problem could be caused by installing an agent install package pre-configured with the machine ID on more than one machine. Check this box to receive notifications of more than one agent using the same account each time you log into the Kaseya Server as a user.

Warn if agent on same LAN as KServer connects through gateway

If you are managing machines that share the same LAN as your Kaseya Server then you may get this alert. By default all agents connect back to the Kaseya Server using the external name/IP address. TCP/IP messages from these agents travel through your internal LAN to your router, and then back to the Kaseya Server. Some routers do a poor job of routing internal traffic back through themselves. Check this box to receive a notification when the Kaseya Server detects an agent may be on the same LAN but connecting through the router.

> **Note:** Agents on the same LAN as the Kaseya Server should specify the internal IP address shared by both the agent and the Kaseya Server on the **Check-In Control** *(page xliv)* page.

Update

Click **Update** to update all selected machine IDs with the options previously selected.

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.

⚪ Agent is currently offline

🔵 User Logged In and Agent is Active

🟡 User Logged In and Agent is Inactive

🟢 User Not Logged In and Agent is online

🟢 User Not Logged In and Agent is Idle

- 🛑 The agent has been suspended
  - ▣ Agent has never checked in

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 list of Machine.Group IDs displayed is based on the **Machine ID / Group ID filter** *(page v)* and the machine groups the user is authorized to see using System > User Security > Scopes.

Edit Profile

Agent > Configure Agents > Edit Profile

The **Edit Profile** page maintains contact information, the language preference for the agent menu on the user's machine and notes about each machine ID/group ID account. Profile information can be maintained in three other places:

- The contact information in the **Edit Profile** page can be automatically populated when a new account is created using the Agent > **Create** *(page xxxiv)* page.
- VSA users and machine users can both maintain contact information using the Home > **Change Profile** tab in the Live Connect (Classic) or Portal Access (Classics) window.
- VSA users only can maintain notes and contact information using the **Agent Settings** tab of the Live Connect (Classic) and Machine Summary pages.

To change user accounts settings:

1. Select a machine ID in the paging area.
2. Enter **Notes**, **Admin Email**, **Contact Name**, **Contact Email** and **Contact Phone** information.
3. Press **Update**.

Special Instructions

Enter any notes about a machine ID account. Helpful information can include the machine's location, the type of machine, the company, or any other identifying information about the managed machine. These special instructions display when you hover the cursor over an agent status icon with a badge. The Quick View window displays the **Special Instructions** text in the bottom of the window.

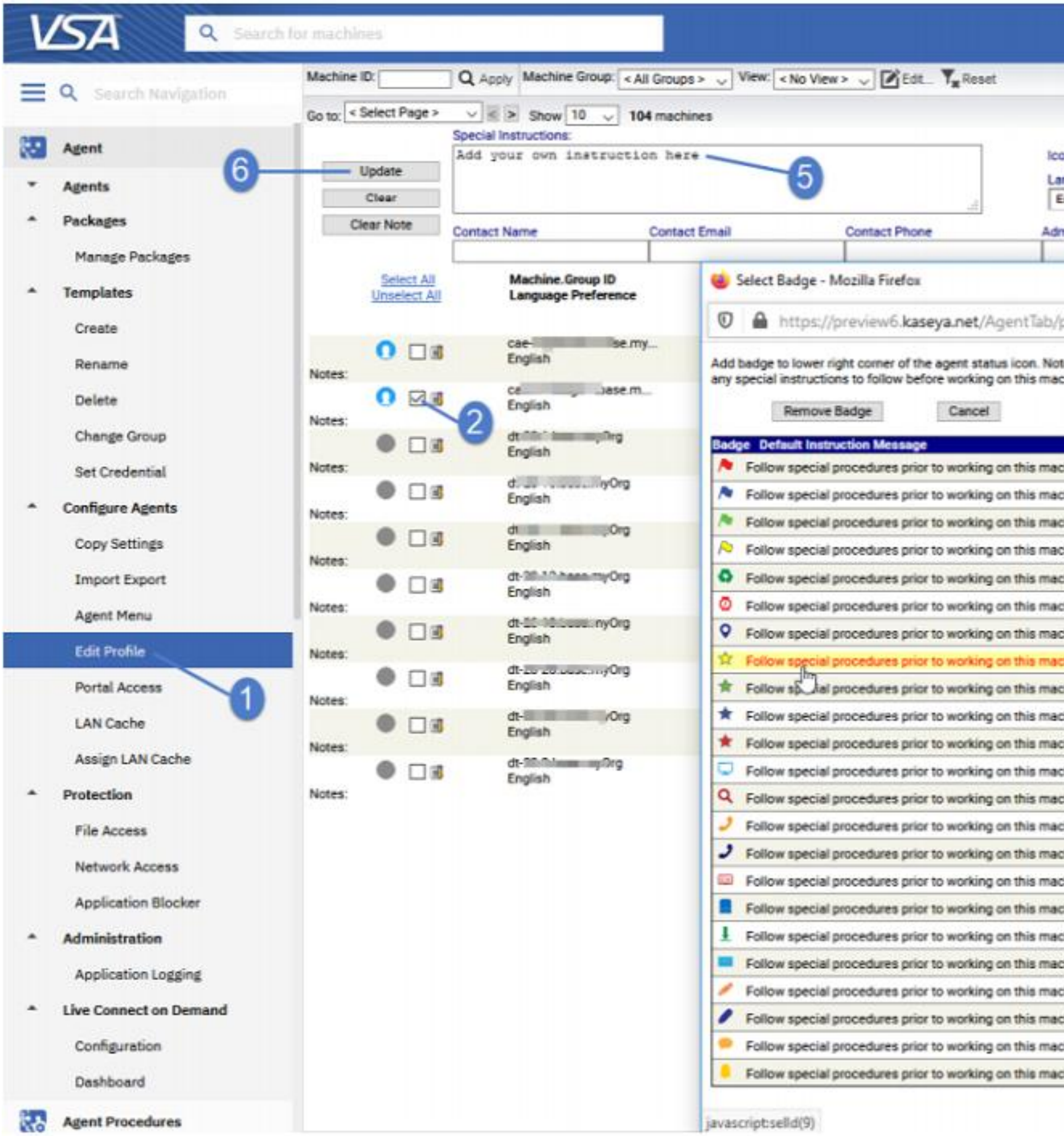
Icon Badge

Add *badges* to the lower right corner of agent status icons, such as ⭐☎🔍. These badges display everywhere the agent icon displays in the user interface. For example, you could mark a machine with a ☎ badge to indicate the customer requires a phone call before anyone works on that machine. Or mark a server with a ⏰ badge because you should not do anything to it until after hours.

To add an agent badge

1. Select one or more machines on the Agent > Configure Agents > **Edit Profile** *(page xlvii)* page.
2. Click the **Icon Badge** link at the top of the page and select one of the available badges.

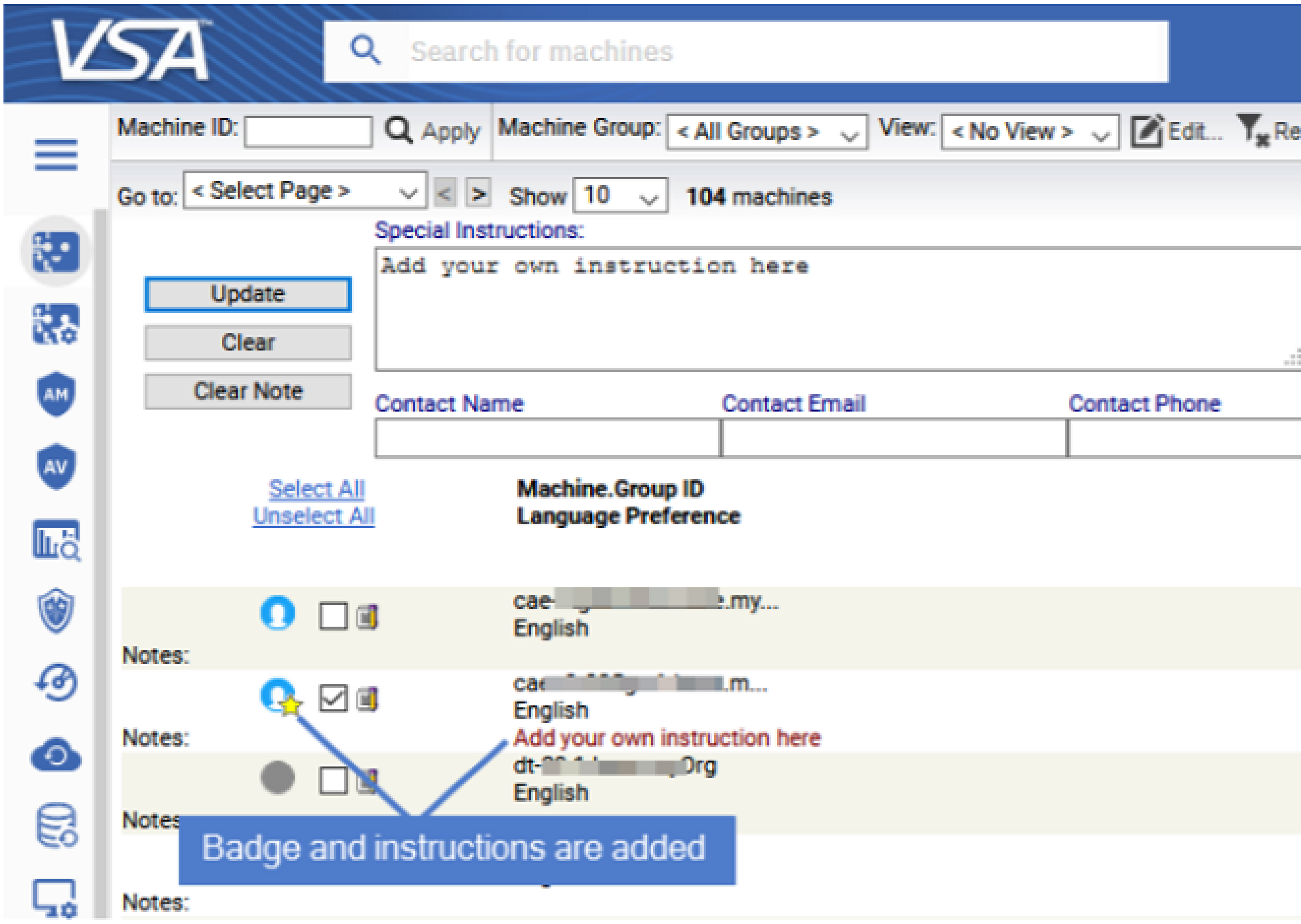
3. Add a special instructions text message for each the badge.
4. Click the **Update** button to assign the badge to selected machines.



Add badge to lower right corner of the agent status icon. Not
any special instructions to follow before working on this mac

Badge	Default Instruction Message
🚩	Follow special procedures prior to working on this mac
🚩	Follow special procedures prior to working on this mac
🚩	Follow special procedures prior to working on this mac
🚩	Follow special procedures prior to working on this mac
♻	Follow special procedures prior to working on this mac
⏻	Follow special procedures prior to working on this mac
📍	Follow special procedures prior to working on this mac
☆	Follow special procedures prior to working on this mac
★	Follow special procedures prior to working on this mac
★	Follow special procedures prior to working on this mac
★	Follow special procedures prior to working on this mac
🖵	Follow special procedures prior to working on this mac
🔍	Follow special procedures prior to working on this mac
☎	Follow special procedures prior to working on this mac
☎	Follow special procedures prior to working on this mac
✉	Follow special procedures prior to working on this mac
📘	Follow special procedures prior to working on this mac
⬇	Follow special procedures prior to working on this mac
▬	Follow special procedures prior to working on this mac
✎	Follow special procedures prior to working on this mac
✎	Follow special procedures prior to working on this mac
💬	Follow special procedures prior to working on this mac
🔔	Follow special procedures prior to working on this mac

The badge is added to the selected machines:



Special Instructions:

Add your own instruction here

Contact Name	Contact Email	Contact Phone

Machine.Group ID
Language Preference

☐ cae-[redacted].my...
English
Notes:

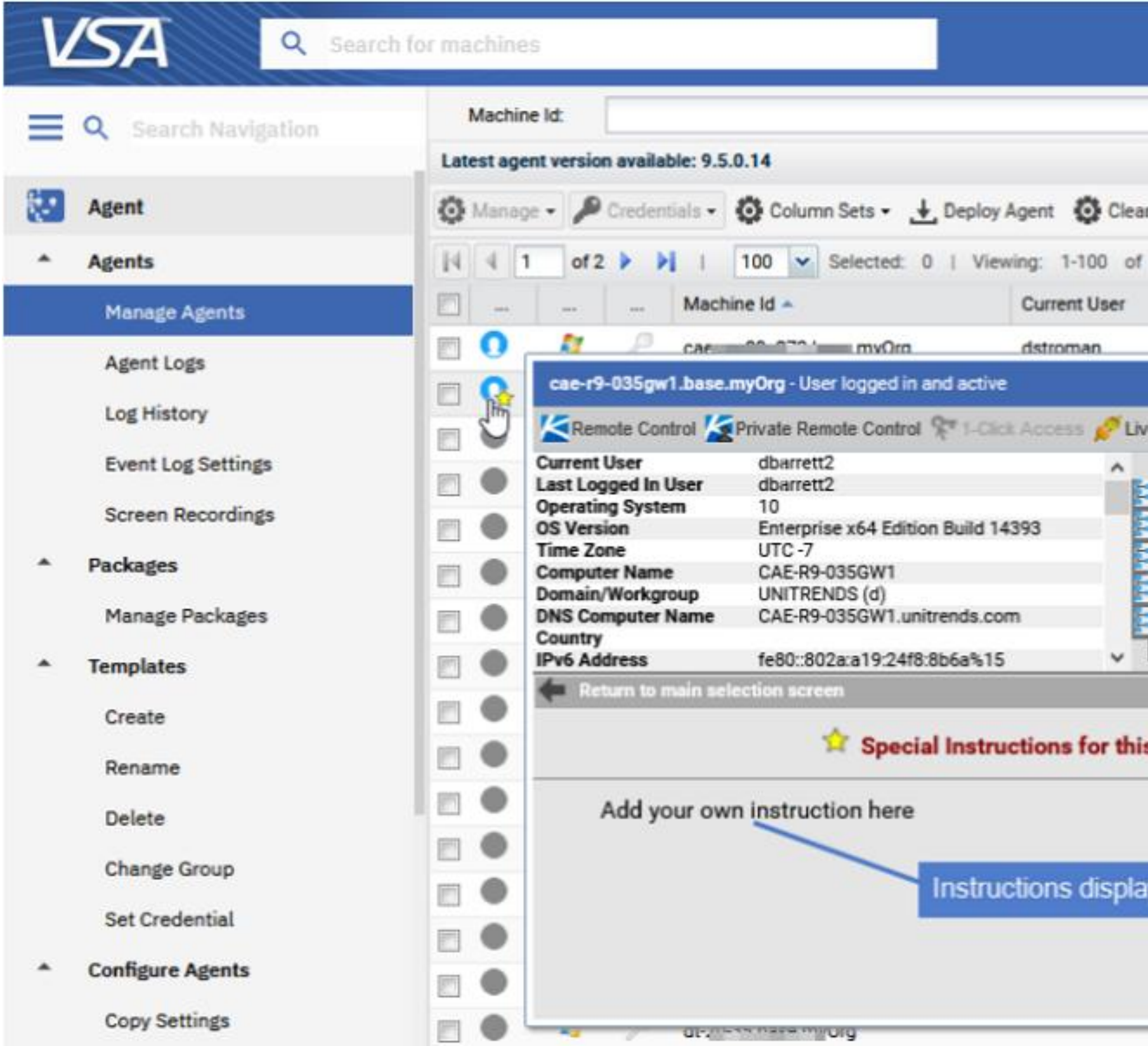
☑ ca[redacted].m...
English
Add your own instruction here
Notes:

☐ dt-[redacted]0rg
English
Notes:

Notes:

Badge and instructions are added

When you hover the cursor over an agent status icon with a badge, the Quick View window displays the special instructions text in the bottom of the window:



cae-r9-035gw1.base.myOrg - User logged in and active

Current User	dbarrett2
Last Logged In User	dbarrett2
Operating System	10
OS Version	Enterprise x64 Edition Build 14393
Time Zone	UTC -7
Computer Name	CAE-R9-035GW1
Domain/Workgroup	UNITRENDS (d)
DNS Computer Name	CAE-R9-035GW1.unitrends.com
Country	
IPv6 Address	fe80::802a:a19:24f8:8b6a%15

Special Instructions for thi

Add your own instruction here

Instructions displa

Auto assign tickets

Auto assign a ticket to this machine ID if the **Ticketing** email reader or a **Service Desk** email reader receives an email from the same email address as the **Contact Email** field of **Edit Profile**. Applies when new emails come into the **Ticketing** email reader that do not map into any of the email mappings or as described for **Service Desk** in the Ticket Associations section of the **Readers tab** *(http://help.kaseya.com/webhelp/EN/KSD/9050000/index.asp#7560.htm)* topic in online help.

> **Note:** if multiple machine IDs have the same **Contact Email** value, then only one machine ID can have this checkbox checked.

Contact Name

Enter the name of the individual using the managed machine. This setting is displayed in the **Contact Name** column.

Contact Email

Enter the email address of the individual using the managed machine. This setting is displayed in the **Contact Email** column.

Contact Phone

Enter the phone number of the individual using the managed machine. This setting is displayed in the **Contact Phone** column.

Admin Email

Enter the email address providing administrator support for this managed machine.This setting is displayed in the **Admin Email** column.

Language Preference

The language selected in the **Language Preference** drop-down list determines the language displayed by an **agent menu** *(page xlii)* on a managed machine. The languages available are determined by the language packages installed using System > Preferences.

Machine Role

The machine role to apply to selected machine IDs. Machine roles determine the Portal Access (Classic) functions available to the machine user.

Actions

- **Update** - Click **Update** to update selected machine IDs with the profile information previously entered.

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.

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.

● Agent is currently offline

● User Logged In and Agent is Active

● User Logged In and Agent is Inactive

● User Not Logged In and Agent is online

● User Not Logged In and Agent is Idle

✋ The agent has been suspended

▣ Agent has never checked in

Machine.Group ID

The list of Machine.Group IDs displayed is based on the **Machine ID / Group ID filter** *(page v)* and the machine groups the user is authorized to see using System > User Security > Scopes.

LAN Cache

Agent > Configure Agents > LAN Cache

The **LAN Cache** page designates a machine to act as a file source for other machines on the same LAN. When a LAN cache is enabled and a machine on the same LAN requests a download from the Kaseya Server for the first time, files are downloaded to the LAN cache machine, then copied to the requesting machine. From then on the file does not need to be downloaded from the Kaseya Server. Other machines—on the same LAN and using the same LAN cache—copy the file from the LAN cache machine. Doing so speeds delivery to multiple machines throughout the same LAN and reduces network bandwidth issues. The following VSA functions can use LAN Cache:

- agent procedure command getURL()
- agent procedure command writeFile()
- Patch Management > File Source
- Policy Management > Policies > Patch File Source

Warning: LAN Cache utilizes local administrator accounts to create/manage shares, and assign machines to access the shares. Since not all VSA installations are domain joined, this design utilizes pass thru authentication which is a form of password reuse. If LAN Cache is installed on a Domain Controller, the local administrator becomes a domain administrator. Installing any software onto a Domain Controller violates Microsoft best practices and introduces security risks to your environment. Kaseya recommends carefully considering your use case(s) before accepting the risk associated with creating additional domain administrator accounts, and configuring VSA to use auto-generated administrator credentials.

Background

LAN Cache configures a file source as follows:

- Automatically creates a local administrator or domain administrator account, or allows you to manually specify the credential for an existing domain administrator. Created accounts are given a unique name (`FSAdminxxxxxxxxxx` where `x` is a digit) with an automatically generated strong password. The generated password contains 15 randomly selected characters and contains at least one the following characters:
  - uppercase letters
  - lowercase letters
  - numbers (0 - 9)
  - non-alphanumeric characters
- Once the password is generated, it is compared against the admin name to ensure that no 2 character combinations in the password match any 2 character combination in the admin name. This logic ensures that the generated passwords will meet any Windows password complexity logic.
- The credentials for the account are associated with this LAN cache within Kaseya and are used when necessary instead of any assigned agent credential. *LAN Cache does not require nor support using the credential specified on the Manage Agents page.*
- Creation of the specified customer share directory on the specified fixed disk drive configured as a Windows administrative share. The directory and share are created for you without leaving the **LAN Cache** page. The directory specified for LAN cache is strictly for customer use. *Kaseya never uses this customer-specified directory/share.*
- Creation of a special Kaseya directory—always `VSAFileShare` as a sub-directory under the customer directory—on the specified fixed disk drive configured as a Windows administrative share.

Procedure - General

1. Select a LAN cache machine.
2. Assign machines to the LAN cache using the **Assign LAN Cache** *(page liv)* page.

Procedure - For writeFile() and getURL() Steps in Agent Procedures

These commands can download files from a **LAN Cache** instead of the VSA or from a URL. Files have to be larger than 4k bytes.

1. Select a LAN cache machine.

2. Assign machines to the LAN cache using the **Assign LAN Cache** *(page liv)* page.
3. *For the writeFile() command only*, upload the files you intend to download to assigned machines to the Kaseya Server using Agent Procedures > Manage Procedures > Schedule / Create > Manage Files > *Shared* folder. Files have to be larger than 4k bytes.
4. Create and run an agent procedure that includes a writeFile() or getURL() step.
   - When an agent executes the **writeFile()** or **getURL()** step of an agent procedure for the first time, it downloads the file from the KServer or the URL, then updates the assigned LAN cache with the file.
   - For subsequent requests for the same file by any agent, the file is downloaded from the LAN cache instead of from its original source.
   - To take full advantage of the caching mechanism, execute the agent procedure referencing the file on one agent first. After that agent has uploaded the file to the assigned LAN cache, execute the procedure on other agents assigned to the same LAN cache.

Actions

- **Add LAN Cache** - Specifies a LAN cache on a selected machine.
  - **1. LAN Cache Name** - Enter a "friendly" name for the LAN cache as it will be displayed in **Assign LAN Cache.** It does not have to match the name of the machine. Do not specify the name of the directory or drive letter.
  - **2. Directory Name** - Enter the name of the directory only, without specifying the name of the machine or the drive letter. The directory does not have to already exist. LAN Cache will create the directory and the required share settings for you.
  - **3. Select the UNC server name resolution** - **Use Computer Name** or **Use Computer IP Address**. Specifies the UNC name resolution format used to access the share. Example: `\\computername\sharename$` or `\\10.10.10.118\sharename$`.

    > **Note:** The next step—selecting the type of credential—does not display if the System > Default Setting > **LAN Cache - Use auto-generated administrator credentials** option is set to yes.

  - **4. Select the type of LAN Cache administrator credentials to use**
    - ✓ **Use auto-generated administrator credentials** - If selected, an administrator credential is created for you when the LAN Cache is created. A local administrator credential is created unless the machine is a domain controller. If the machine is a domain controller, a domain administrator credential is created.
    - ✓ **Use an existing domain administrator credential** - If selected, enter the domain, username and password of an existing domain credential. The domain credential will not be created for you.
  - **5. Select a fixed drive on which to create the LAN Cache** - Select the drive to create the share on.
- **Remove LAN Cache** - Removes the LAN cache from a selected machine.
- **Clear Pending** - Cancels the pending creation of a LAN cache on a selected machine.
- **Test Generated Cache Credential** - Click to test the credentials used by a selected machine. The result is shown in the **Credential Test Status** column.

Columns

- **(Check-in Icon) -** 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.

- **Machine.Group ID** - A unique machine ID / group ID / organization ID name for a machine in the VSA.
- **Cache Name** - The name of the LAN cache as displayed with the VSA.
- **Cache Path** - The path specified for the LAN cache.
- **Cache UNC** - The UNC used to locate the LAN cache on the network.
- **Cache Created** - Date/time the LAN cache was created.
- **Cache Administrator** - The administrator account used to access the LAN Cache.
- **Credential Test Status** - Displays the results of testing the administrator account credentials used to access the LAN Cache. Credentials can be tested using the **Test Generated Cache Credential** button at the top of the page.

Assign LAN Cache

Agent > Configure Agents > Assign LAN Cache

The **Assign LAN Cache** page assigns machines to, and removes machines from, a selected **LAN Cache** *(page li)* machine. When a machine is assigned to a LAN cache, the LAN cache autogenerated credential is created on that machine. If the machine is a domain controller, the autogenerated credential is a domain credential.

Actions

- **Assign** - Assigns a LAN cache selected from the drop-down list to selected machines.
- **Unassign** - Unassigns a LAN cache from selected machines.
- **Clear Pending** - Cancels the pending assignment of a selected machine to a LAN cache.
- **Test Assigned LAN Cache Functionality** - Click to test the functionality of the assigned LAN cache used by a selected machine. The result is shown in the **Assigned LAN Cache** column.

Columns

- **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.
- **(Check-in Icon) -** 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.
- **Machine.Group ID** - A unique machine ID / group ID / organization ID name for a machine in the VSA.
- **Assigned LAN Cache** - Displays the LAN cache a machine is assigned to.
- **Assigned** - The date/time a machine was assigned to a LAN cache.

- **Test Status** - **Credential Test Status** - Displays the results of testing the administrator account credentials used to access the LAN Cache. Credentials can be tested using the **Test Generated Cache Credential** button at the top of the page.

> **Warning:** LAN Cache utilizes local administrator accounts to create/manage shares, and assign machines to access the shares. Since not all VSA installations are domain joined, this design utilizes pass thru authentication which is a form of password reuse. If LAN Cache is installed on a Domain Controller, the local administrator becomes a domain administrator. Installing any software onto a Domain Controller violates Microsoft best practices and introduces security risks to your environment. Kaseya recommends carefully considering your use case(s) before accepting the risk associated with creating additional domain administrator accounts, and configuring VSA to use auto-generated administrator credentials.

Set Proxy

Agent > Configure Agents > Set Proxy

For security purposes, administrators may prevent agent machines direct access to the internet and route web traffic requests and resulting downloads through proxy servers. For these environments you can use the **Set Proxy** page to specify the URL and credential used to download **Patch Management** files via a proxy server. You can then assign the proxy server configuration to one or more agents.

> **Note:** For instructions on how to configure a proxy server to support **Patch Management** downloads see **Proxy and Kaseya Patch Management**. *(https://helpdesk.kaseya.com/entries/34401486)*

Header

- **Proxy Server** - The URL of the proxy server.
- **Port** - The port of the proxy server. Defaults to 1080.

If the proxy server requires authentication, enter a username and password.

- **Username** - The username used to access the proxy server.
- **Password** - The password used to access the proxy server.

Actions

- **Apply** - Applies the proxy server configuration to one or more selected agents.
- **Clear** - Clears the proxy server configuration assigned to one or more selected agents.

Columns

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.

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.

● Agent is currently offline
🔵 User Logged In and Agent is Active
🟡 User Logged In and Agent is Inactive
🟢 User Not Logged In and Agent is online
🟢 User Not Logged In and Agent is Idle
🔴 The agent has been suspended

▣ Agent has never checked in

Machine.Group ID

The list of Machine.Group IDs displayed is based on the **Machine ID / Group ID filter** *(page v)* and the machine groups the user is authorized to see using System > User Security > Scopes.

Proxy Server

The URL of the proxy server.

Username

The username used to access the proxy server.

Protection

File Access

Agent > Protection > File Access

The **File Access** page prevents unauthorized access to files on managed machines by rogue applications or users. Any application can be approved or denied access to the file.

> **Note:** You may also block operating system access to the protected file by blocking access to `explorer.exe` and/or `cmd.exe`. This prevents the file from being renamed, moved, or deleted therefore completely locking down the file from tampering.

Multiple Agents

If **multiple agents** *(page xxx)* are installed on a machine, only one agent at a time controls the drivers required to use **File Access** *(page lvi)*, **Network Access** *(page lvii)*, **Application Blocker** *(page lx)*. These functions can only be performed by the agent controlling these drivers.

Block

To protect a file from access by rogue applications, enter the filename and click the **Block** button. This displays the **File Access** popup window.

The dialog presents the user with one of the following options:

- **Filename to access control** - Enter the **file name and/or a portion of the full path**. For example, adding a file named `protectme.doc` to the list, protects occurrences of `protectme.doc` in any directory on any drive. Adding `myfolder\protectme.doc` protects all occurrences of the file in any directory named `myfolder`.
- **New** - Add in a new application to the access list. You can manually enter the application or use the **Search...** button to select an application name.
- **Remove** - Removes an application from the approved access list
- **Search** - Select a machine ID to search the list of applications installed on that machine ID and select an application name. This list is based on the latest audit performed on that machine ID. You are not actually browsing the managed machine.
- **Ask user to approve unlisted** - Lets users approve/deny access to the file on a per application basis each time a new application tries to access that file. Use this feature to build up an access control list based on normal usage.
- **Deny all unlisted** - Blocks an application from accessing the file. Select this option if you are already sure of which files need access and which do not.

Unblock

Remove an application from the protection list by clicking the **Unblock** button. This opens a new dialog box listing all protected files for the selected machine IDs. You can remove files from just the selected machine or from all machines containing that file path.

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.

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.

- ● Agent is currently offline
- 🔵 User Logged In and Agent is Active
- 🟡 User Logged In and Agent is Inactive
- 🟢 User Not Logged In and Agent is online
- 🟢 User Not Logged In and Agent is Idle
- 🔴 The agent has been suspended
- 🟧 Agent has never checked in

Machine.Group ID

The list of Machine.Group IDs displayed is based on the **Machine ID / Group ID filter** *(page v)* and the machine groups the user is authorized to see using System > User Security > Scopes.

Filename

Filename of the file to be blocked. Click the edit icon ✎ next to any filename to change file access permissions for that filename.

Approved Apps

Lists applications approved to access the file on the machine ID.

Ask User Approval

If checked, the user of a machine ID is asked to approve file access if an unapproved application attempts to access the file.

Network Access

Agent > Protection > Network Access

The **Network Access** page lets you approve or deny **TCP/IP-protocol-based network access** on a per application basis. Users can also be notified when an unlisted application accesses the network, permitting or denying that application network access. Typically this function is used to control access to internal and external *internet* sites, but can include internal LAN traffic that also uses the TCP/IP protocol.

Driver

This function requires the driver be *enabled* to block network access and monitor network bandwidth statistics. *The driver is disabled by default*. This driver inserts itself into the TCP/IP stack to measure TCP/IP-protocol-based network traffic by application. *For Windows machines earlier than Vista, an enabled driver only takes effect after a reboot of the machine.*

Note: To determine which applications should be approved or denied network access, use the Network Statistics report to view network bandwidth utilization versus time. Drill down and identify peak bandwidth consumers by clicking the graph's data points. See which application and which machine use bandwidth at any point in time.

Warning: Applications that do not use the Windows TCP/IP stack in the standard way may conflict with the driver used to collect information and block access, especially older legacy applications.

Multiple Agents

If **multiple agents** *(page xxx)* are installed on a machine, only one agent at a time controls the drivers required to use **File Access** *(page lvi)*, **Network Access** *(page lvii)*, **Application Blocker** *(page lx)*. These functions can only be performed by the agent controlling these drivers.

To approve or deny network access to one or more applications

1. Check the checkbox next to one or more machine IDs in the **Machine.Group ID** column.
2. Click the link of *any* machine ID in the **Machine.Group ID** column. It does not have to be the machine ID you checked. This displays the **Application List** popup window, listing all applications installed on that machine ID. The list is based on the latest audit that was performed for that machine ID.
3. Since the list in the **Application List** window may be large, you can control the applications displayed by clicking **Filter** to filter the list.
4. Check the checkboxes next to the application name you wish to approve or deny network access to.
5. You can also enter application names in the **Add applications not found by audit here** edit field, to identify applications not listed.
6. Click the **Select** button to confirm your selections and close the **Application List** window. The selected applications now display at the top of the page.
7. Click **Approve Apps** or **Deny Apps**. The applications selected in the **Application List** window are added from the **Approved Apps/Denied Apps** column.

To remove approve and deny settings for one or more machine IDs

1. Check the checkbox next to one or more machine IDs in the **Machine.Group ID** column.
2. Click the **Remove Apps** button.

Network Access Options

- **Notify user when app blocked** - Notify the user when a blocked application attempts to access the network. Use this function to build up the access list based on normal usage. This lets you see which applications on your system are accessing the network and when. The machine user is prompted to select one of four responses when an application is blocked:
  - **Always** - Allows the application access to the network indefinitely. Users will not be prompted again.
  - **Yes** - Allows the application access to the network for the duration of the session. Users will be prompted again.
  - **No** - Denies the application access to the network for the duration of the session. Users will be prompted again.
  - **Never** - Denies the application access to the network indefinitely. Users will not be prompted again.
- **Enable/Disable driver** - **Enable/Disable** the network access protection driver for an agent. Applications that do not use the Windows TCP/IP stack in the standard way may conflict with this driver, especially older legacy applications. **The agent can not monitor network statistics or block network access if this driver is disabled.** *For Windows machines earlier than Vista, an enabled driver only takes effect after a reboot of the machine.*

- **Apply Unlisted Action** - An unlisted application is one that has not been explicitly approved or denied access to the network. Select the action to take when an unlisted application attempts to access the network.
  - **Ask user to approve unlisted** - A confirmation dialog box displays if an unlisted application attempts to access the network.
  - **Approve all unlisted** - The unlisted application is granted access to the network.
  - **Deny all unlisted** - The unlisted application is denied access to the network and the application is closed on the managed machine.

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.

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.

● Agent is currently offline

🔵 User Logged In and Agent is Active

🟡 User Logged In and Agent is Inactive

🟢 User Not Logged In and Agent is online

🟢 User Not Logged In and Agent is Idle

🔴 The agent has been suspended

▣ Agent has never checked in

Machine.Group ID

The list of Machine.Group IDs displayed is based on the **Machine ID / Group ID filter** *(page v)* and the machine groups the user is authorized to see using System > User Security > Scopes.

Notify User

A green checkmark ✓ in the **Notify User** column indicates that the managed machine user is notified when an application attempts to access the network that has been denied network access.

To notify the user when a application has been denied:

1. Select machine IDs.
2. Click the **Enable** button for **Notify user when app is blocked**.

To remove this notification:

1. Select machine IDs that display a green checkmark ✓ in the **Notify** column.
2. Click the **Disable** button for **Notify user when app is blocked**.

Enable Driver

Identifies on a per machine ID basis, which machines have the network protection driver enabled or not. *For Windows machines earlier than Vista, an enabled driver only takes effect after a reboot of the machine.*

Unlisted Action

Displays the **Unlisted Action** to take when an unlisted application attempts to access the network. See **Apply Unlisted Action** above.

Approved Apps / Denies Apps / Remove Apps / Remove All

These settings can only be applied once the driver is enabled.

- Approved applications are listed in the first row.

- Denied applications are listed in the second row.
- If the **Approve all unlisted** radio option is selected and applied to a machine ID, then the approved application list is replaced by the phrase `Approve All Unlisted`.
- If **Deny all unlisted** radio option is selected and applied to a machine ID, then the denied application list is replaced by the phrase `Deny All Unlisted`.
- Click **Remove Apps** to remove a selected applications from selected machines.
- Click **Remove All** to remove all applications from selected machines.

Application Blocker

Agent > Protection > Application Blocker

The **Application Blocker** page prevents any application from running on a machine ID. Blocked applications cannot be renamed, moved, or deleted from the system. **File Access** *(page lvi)* can also block applications, but **Application Blocker** is faster to configure if you simply want to block and unblock applications.

Multiple Agents

If **multiple agents** *(page xxx)* are installed on a machine, only one agent at a time controls the drivers required to use **File Access** *(page lvi)*, **Network Access** *(page lvii)*, **Application Blocker** *(page lx)*. These functions can only be performed by the agent controlling these drivers.

Block

To block an application from running on a machine:

1. Select one or more machine IDs. Only machine IDs currently matching the **Machine ID / Group ID filter** *(page v)* are displayed.
2. Enter the application's filename in the edit box.

   The application can be **referenced by file name and/or a portion of the full path**. For example, adding an application named `blockme.exe` to the list, prevents all occurrences of `blockme.exe`, on any directory or on any drive, from running. Adding `myfolder\blockme.exe` prevents occurrences of the application in any directory named `myfolder` from running.
3. Click the **Block** button.
4. The blocked application displays in the **Application** column beside the selected machine IDs.

Unblock

To unblock an application from the blocked list:

1. Select one or more machine IDs that show blocked applications in the **Application** column.
2. Click the **Unblock** button. This opens a **File Access** popup window listing all blocked applications for the selected machine IDs.

Click one or more blocked applications.

1. Click the **Unblock** button. The window closes.
2. The blocked application no longer displays in the **Application** column beside the selected machine IDs.

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.

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.

● Agent is currently offline
🔵 User Logged In and Agent is Active
🟡 User Logged In and Agent is Inactive
🟢 User Not Logged In and Agent is online
🟢 User Not Logged In and Agent is Idle
🛑 The agent has been suspended
 ▣ Agent has never checked in

Machine.Group ID

The list of Machine.Group IDs displayed is based on the **Machine ID / Group ID filter** *(page v)* and the machine groups the user is authorized to see using System > User Security > Scopes.

Application

Filename of the application being blocked.

Administration

Application Logging

Agent > Administration > Application Logging

The **Application Logging** page displays a log of **Agent** module activity by:

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

This table supports selectable columns, column sorting, column filtering and flexible columns widths.

Live Connect on Demand

Configuration

Agent > Live Connect on Demand > Configuration

The **Configuration** page configures and enables the Live Connect on Demand feature. Live Connect on Demand installs a temporary agent on machines so that Live Connect can manage a machine temporarily, up to a specified number of minutes.

Actions

- **Save Live Connect on Demand Configuration** - Saves the settings configured on this page.
- **Edit Email Template** - Edits the email template for notifying users how to install a temporary agent on their endpoint machine.

Configuration Options

- **Enable Live Connect on Demand** - If checked, temporary agents can be installed using Live Connect.
- **Use Kaseya Authorization Request Service** - Not yet enabled. If unchecked, a cloud-based server is used to authorize requests to install temporary agents on machines.
- **URL** - The authorization request service URL.
- **Remove Unused Agents after ... minutes** - Sets the initial time allowed in minutes for users to remove unused agent.
- **Automatically Remove Agents after ... hours if not closed by technician** - Sets the time allowed in hours before the temporary agent is uninstalled.
- **Machine Group** - The machine group assigned to temporary agents.
- **Badge Text** - The badge text displayed in Quick View when the cursor hovers over a temporary agent icon in the VSA.

Dashboard

Agent > Live Connect on Demand > Dashboard

The **Dashboard** page provides a dashboard view of Live Connect on Demand metrics.

- **Live Connect on Demand Sessions Created Last 24 Hours** - provides number of Live Connect on Demand Sessions in the Last 24 Hours
- **Live Connect on Demand Sessions Active -** provides active Live Connect on Demand Sessions

Configuration Options

⚙ - **Dashboard configuration** - allows to choose Live Connect on Demand metrics to view.

- ➢ Temporary Agents - Last 24 Hours;
- ➢ Temporary Agents - Active.

Index