Kaseya 2

Agent Deployment

User Guide

Version 7.0

English

September 3, 2014

Agreement

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

Contents

Installing Your First Agent

If you haven't installed an agent on a VSA yet, you should do so now. You can use it to experiment with the features mentioned in this document. The following is the fastest way to install an agent manually.

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 on to your VSA:
   `http://<YourVSAaddress>`
5. Within the VSA, select the Agent > **Agent Status**
   (http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#250.htm) page.
   - ➢ You should see a new machine account listed on this page for the agent you just created.

What are Agents?

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 ![icon] agent icon—displays in the system tray of the managed machine. Agent icons 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 inside the VSA.
- Multiple agents 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 ![icon] 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 launch an agent procedure, view logs or launch **Live Connect** from the agent quick view window.

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.

The Machine ID / Group ID / Organization ID Hierarchy

Each agent installed on a managed machine is assigned a unique **machine ID / group ID / organization ID**. All machine IDs belong to a machine group ID and optionally a subgroup ID. All machine group IDs belong to an organization ID. An organization typically represents a single customer account. If an organization is small, it may have only one machine group containing all the machine IDs in that organization. A larger organization may have many machine groups and subgroups, usually organized by location or network. For example, the full identifier for an agent installed on a managed machine could be defined as `jsmith.sales.chicago.acme`. In this case `sales` is a subgroup ID within the `chicago` group ID within the organization ID called `acme`. In some places in the VSA, this hierarchy is displayed in reverse order. Each organization ID has a single default machine group ID called `root`. Group IDs and subgroup IDs are created using the System > Orgs/Group/Depts/Staff > Manage > Machine Groups page.

Working With Agents on Managed Machines

Agent Icons on Managed Machines

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.

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

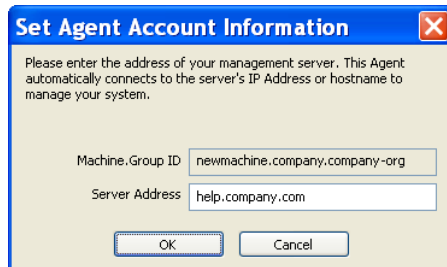### Agent Icon Background is Grey

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 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.

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.
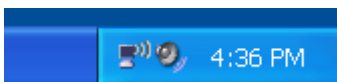
Agent Menu Options

Right clicking the agent icon pops up a menu of options available to the machine user.
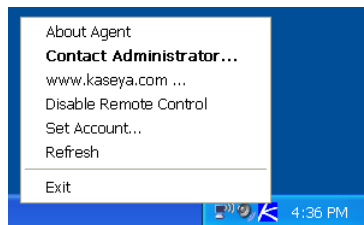
> Note: See Agent > Agent Menu for a description of how to turn these options on or off.

Disabling the Agent Menu

VSA users may completely disable the agent menu and remove the icon from the machine's desktop.

Working with Agents in the VSA

Viewing Audit Results

When an agent is first installed on a machine all the hardware and software components of the machine are inventoried and reported back to the VSA.

Wait a few minutes after the agent is installed, then navigate to the Audit > **Machine Summary** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#554.htm)* page in the VSA. This single page shows all the data returned by the audit about the machine you just installed an agent on.

Agent Status

Once an agent is installed and checks in, its corresponding "machine ID" displays on various pages throughout the VSA. A typical one is the Agent > **Agent Status** page. The **Agent Status** page provides a summary view of a wide variety of agent data.
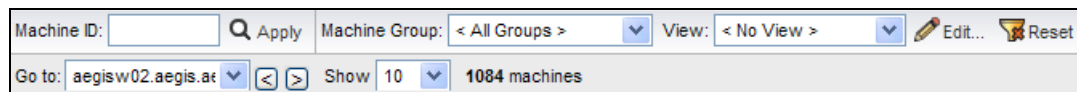
Agent Status Icons in the VSA

Once a machine ID is created, an agent check-in icon displays next to each machine ID account in the VSA. These icons indicate the agent check-in status of each managed machine. Click a check-in icon to display Live Connect. 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. Icon displays a tool tip showing the logon name.
- 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

Filtering Lists of Machine IDs

A **Machine ID / Machine Group** filter at the top of a "machine ID" page allows *you* to decide how to limit the display of all the machines IDs you are authorized to see. The **Machine ID / Machine Group** filter is displayed at the top of *all* function pages that display machine ID accounts.

Machine ID:	Q Apply	Machine Group:	< All Groups >	∨	View:	< No View >	∨	✎ Edit...	🗑 Reset
Go to: aegisw02.aegis.ae ∨	⟨<⟩ ⟨>⟩	Show	10 ∨	**1084** machines					

Once filter parameters are specified, click the Apply icon Q to apply filter settings to *all* function pages. By default, the **Machine ID / Machine Group** filter displays all machine IDs in `<All Groups>` managed by the currently logged in user.

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

View Definitions

The View Definitions window lets you further refine a machine ID / group ID filter based on attributes contained on each machine—for example, the operating system type. Views provide users flexibility for machine management and reporting. View filtering is applied to *all* function pages by selecting a view from the **Select View** drop-down list on the machine ID / group filter panel and clicking the Apply icon 🔍 . Any number of views can be created and shared with other users. Views are created by clicking the **Edit** button to the right of the **Views** drop-down list.

Live Connect

Live Connect is a web-based, single-machine user interface. You can access **Live Connect** by Ctrl+clicking the agent icon 🌐, or by clicking **Live Connect** button in Quick View. **Live Connect** enables you to perform tasks and functions solely for one managed machine. A menu of tabbed property sheets provide access to various categories of information about the managed machine.

Quick View

Hovering the cursor over a check-in icon displays an agent **Quick View** window immediately. You can launch an agent procedure, view logs or launch **Live Connect** from the agent **Quick View** window. You can use agent badges to display **Special Instructions** text in the bottom of the the **Quick View** window.
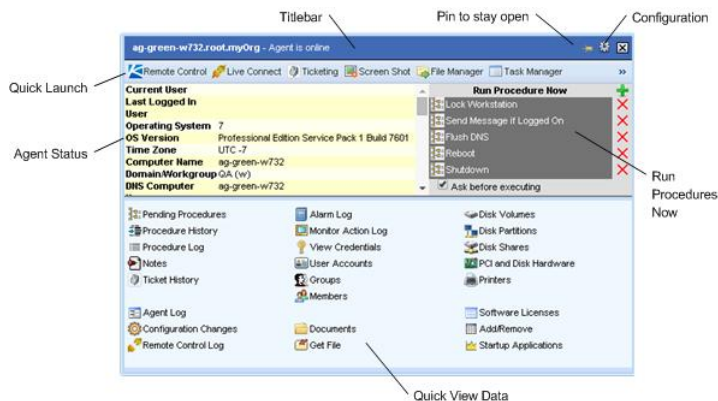

Agent Badges

Add *badges* to the lower right corner of agent status icons, such as ![badge1] ![badge2] ![badge3]. These badges display everywhere the agent icon displays in the user interface. For example, you could mark a machine with a ![badge] badge to indicate the customer requires a phone call before anyone works on that machine. Or mark a server with a ![badge] badge because you should not do anything to it until after hours.

Select one or more machines on the Agent > Edit Profile page, then click the **Icon Badge** link at the top of the page and select one of the available badges. You can define a **Special Instructions** text message for each badge. Click the **Update** button to assign the badge to selected machines.

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.

Creating Agent Install Packages

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 > **Deploy Agents** 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 **Configure Automatic Account Creation** 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.

Create an Agent Install Package

On the Agent > Deploy Agents page, click **Create Package** to start the **Configure Automatic Account Creation** wizard. The wizard is a 7 step process.

1. Define rules for naming the machine ID.
    - ➢ 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. Define rules for naming the group ID.
    - ➢ **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. Specify agent install package command line switches including the ability to install silently without any task bars or dialog boxes.
4. Specify the machine ID to copy settings and pending agent procedures from. 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.

> **Note:** The statement `Copy settings from unknown.root.unnamed if nothing selected` is based on the machine ID or template selected by the Default Install package.

5. Select the operating system you are creating the install package for: `Automatically choose OS of downloading computer:` `Windows`, `Macintosh`, or `Linux.`
6. 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.**

> **Administrator Credentials** - 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.

7. Name the install package for easy reference later. This name displays on the **Deploy Agents** page and the `dl.asp` download page.

Manually Installing the Agent

Manually Downloading Install Packages from the Deploy Agent Page

The **Deploy Agent** page provides three types of links for downloading agent install packages:
- **Click the "download default agent" link** - Each user has his or her own default agent install package. Click this link to download your own user default agent.
- **Click a "package" link** - The complete list of available agent install packages displays on the **Deploy Agents** page. Click any of these links to download the agent install package.
- **Click the "dl.asp" link** - The `dl.asp` web page lists all publicly available agent install packages. Click any package listed on the dl.asp web page to download it.

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

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 `KcsSetup` to launch it.
  - ➢ Open a **command line window** and type `KcsSetup` followed by any desired command line switches.
  - ➢ Select **Run...** from the **Windows Start** menu and type `KcsSetup` followed by any desired command line switches.
- *Macintosh and Linux*
  - ➢ Double click `KcsSetup` to launch it.
  - ➢ The full filename for a Macintosh 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 Macintosh, command line switches can only be used when creating the agent install package.
>
> Note: For Linux, see Installing Linux Agents for more detailed instructions.

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 > **Deploy Agents** 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 **Deploy Agents** 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/7000000/index.asp#1944.htm) and **Domains** *(http://help.kaseya.com/webhelp/EN/KDIS/7000000/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 10)*
- **Configuring Agent Settings Using Templates** *(page 10)*

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 managed 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:

- Credential
- Agent Menu
- Check-in Control
- Working Directory
- Logs
- Edit Profile
- 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 10)* - 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 10)* - 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 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/7000000/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.
- ▪ Import a machine ID template using Agent > Import/Export.
- ▪ Base an agent install package on a machine ID template using Agent > Deploy Agents.
- ▪ Copy *selected* settings from machine ID templates to existing machine ID accounts using Agent > Copy Settings.
- ▪ 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 Package** wizard in **Deploy Agent** 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 Functions

Once agents are installed you can maintain them using a variety of additional functions. The complete list of functions provided by the **Agent** module in the VSA includes:

Functions	Description
Agent Status	Displays active user accounts, IP addresses and last check-in times.
Agent Logs	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	Specifies how long to store log data.
Event Log Settings	Specifies event log types and categories included in event logs.
Deploy Agents	Creates agent install packages for installing agents on multiple machines.
Create	Creates machine ID accounts and/or install packages for installing agents on single machines.
Delete	Deletes machine ID accounts.
Rename	Renames existing machine ID accounts.
Change Group	Reassigns machines to a different machine group or subgroup.
Copy Settings	Mass copies settings from one machine account to other machine accounts.
Import / Export	Imports and exports agent settings, including scheduled agent procedures, assigned monitor sets, and event sets, as XML files.
Suspend	Suspends all agent operations, such as agent procedures, monitoring, and patching, without changing the agent's settings.
Agent Menu	Customizes the agent menu on managed machines.
Check-In Control	Controls agent check-in frequency on agent machines.
Working Directory	Sets the path to a directory used by the agent to store working files.
Edit Profile	Edits machine account information.
Portal Access	Sets up accounts to allow machine users remote control access to their own machines.
Set Credential	Sets a logon credential for the agent to use in Patch Management, the useCredential() procedure command, Endpoint Security, and Desktop Management.
LAN Cache	Designates a machine to act as a file source for other machines on the same LAN.
Assign LAN Cache	Assigns machines to, and removes machines from, a selected LAN Cache machine.
Update Agent	Updates the agent software on managed machines.
File Access	Prevents unauthorized access to files on managed machines by rogue applications or users.
Network Access	Lets you approve or deny network access on a per application basis.
Application Blocker	Application blocker prevents any application from running on a managed machine.

Learning More

PDFs are available to help you quickstart your implementation of **Virtual System Administrator™**. They can be downloaded from the **first topic in the VSA online help** *(http://help.kaseya.com/webhelp/EN/VSA/7000000)*.

If you're new to **Virtual System Administrator™** we recommend the following quickstart guides:

1. Getting Started
2. User Administration
3. Agent Configuration and Deployment
4. Remote Control Tools
5. Monitoring Configuration
6. Custom Reports

The following resources are also available.

Kaseya University

See **Kaseya University** *(http://university.kaseya.com)* for training options.

Index

A

C

I

L

M

W