Table of Contents:

◇ Machine Status
◇ Install Agents
◇ LAN Discovery
◇ Configure Agents
◇ Upgrade Version
Introduction

Kaseya Virtual System Administrator (hereafter VSA) allows for remote and automatic management of computers and network devices both individually and in groups that may be spanned across domains, clients, locations or any other structure. This greatly facilitates increased automation based on the ability to create and use "best practices" and greatly decreases the amount of time it takes to complete routine maintenance tasks. To achieve this, VSA provides for configuration and installation of a Kaseya agent on each of the managed machines. As depicted in Fig. 2.1, a Kaseya agent (hereafter agent) is a software that is installed on a managed machine with the sole purpose of carrying out the tasks assigned by VSA user. Agents are fully configurable to further facilitate automation and remote control. Agents are installed as system services using packages that define expected behavior. Each installed agent represents only one computer and uses up one of the available agent licenses. Understanding the agent foundation concepts will greatly streamline the successful management of machines using VSA.

Agent Grouping

VSA organizes managed computers (and therefore the agents they host) within an organization into a hierarchy. This hierarchy places each computer at a unique position that clearly identifies the position of the computer (either logical or physical) within the organization. This way, an organization is divided into a number of relevant groups, each group is optionally divided into subgroups, which could in turn have its own subgroups. The last subgroup contains the actual computers that are members of that group or subgroup. While for any organization, one can arrive at multiple valid organizational hierarchies, existence of only one hierarchy is sufficient for unique identification of managed machines. Within this hierarchy, machines, groups, and organizations, are respectively assigned MachineIDs, GroupIDs and OrganizationIDs. It is this combination of MachineID, GroupID, and OrganizationID that uniquely identifies each machine because each agent in installed on only one managed computer. Unique identification of managed computers will therefore yield unique identification of their installed agents.

Note that 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 the entire machine IDs in that organization. A larger organization may have many machine groups and subgroups, usually organized by their location or network.

Fig. 2.2 shows an example of an organization structure. In this structure, a single organization has various groups and each group has its own set of machines. Agents are installed on each of these machines and each agent is assigned a unique machine ID to distinguish them from each other.
An organization can have multiple sub organizations and groups can have subgroups as shown in Fig. 2.3 and Fig. 2.4.

Agent Filtering

VSA enables the filtering of agents to limit the number of machines displayed on all function pages to those that are screened at the moment. There are three ways to filter agents: MachineID, Machine Group and View. By default VSA displays all machine IDs in all groups with no views as shown in Fig. 2.5.

Note: Even if VSA user selects "<All Groups>" only groups the user is granted access to will be displayed.
Portions of this page are labeled in the figure. A brief description for each label is provided below.

1. **Machine ID**: If a specific machine ID needs to be searched, the machine ID or only its beginning letters are entered in this field as shown in the Fig. 2.5 above and the Apply button is clicked. Make sure that the appropriate Machine group is selected. If you are not sure of the machine group the machine ID belongs to, select “<All Groups>”.

2. **Machine Groups**: Machine groups can be selected from the dropdown box. For example, if “ABC” is an organization with machine groups such as “Sales” and “Marketing,” the groups are listed as:

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABC</td>
<td>Lists all machine IDs under the ABC organization</td>
</tr>
<tr>
<td>ABC.Sales</td>
<td>Lists all machine IDs under the ABC organization/Sales group.</td>
</tr>
<tr>
<td>ABC.Marketing</td>
<td>Lists all machine IDs under the ABC organization/Marketing group.</td>
</tr>
</tbody>
</table>

3. **Views**: Views provide more flexibility for filtering of the agents by allowing users to define filters based on specific characteristics of the machines that are hosting the agents as shown in Fig. 2.6 and Fig. 2.7. Any number of views can be created and shared with other administrators. A new view can be created by clicking on Edit button to the right of the Views drop-down list as shown in Fig. 2.5 and then configuring attributes of the new view from the View definition window shown in Fig. 2.6-1 and Fig. 2.6-2.
The View definitions window lets you further refine a machine ID / machine group filter based on attributes contained on each machine as shown in the figure above. The available options in the View definitions window are explained below:

**View by Machine ID**
- **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** – A view needs to be saved 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.

**View by Network Status and Address**
- **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 KServer, 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.
  
  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.
  
  Example: 66.221.11.* matches all IP addresses from 66.221.11.1 through 66.221.11.254.

**View by Operating System**
- **OS Type** - Check to only list machines that match the selected operating system as reported using the Audit > Name/OS Info.
- **OS Version** - Check to only list machines that match the OS version string as reported using Audit > Name/OS Info. Use this filter to identify machines by service pack.

**View Machines Based on Procedure History/Status**
- **With agent procedure scheduled/not scheduled** - Check to only list machines that have the specified agent procedure either scheduled to run or not.
- **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.

**View Machines by Application**
- **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.
View Machines by Patch Update
- 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 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 (identified by the patch’s 6 digit KB Article ID) - Check to only list machines missing a specific patch.

View Machines by Agent Data
- Advanced Agent Data Filter - Check and click the Define Filter button to further refine the view using the Filter Aggregate Table.

Advanced agent data filter options are shown in Fig. 2.7. Advanced filtering lets you design complex searches to isolate data to just those values that is to be searched. The fields are self explanatory and depending on the requirement the values can be entered in the appropriate fields to filter the data.

Fig. 2.7: Advanced agent data filter
## Agent Functions Overview

Fig. 2.8 shows the available functions in the agent module. The list of agent functions and a brief description of their use is listed in the table below. In the following sections, each function is explained in detail.

![Agent Functions](image)

### Fig. 2.8
**Agent Functions**

<table>
<thead>
<tr>
<th>Section</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Machine Status</td>
<td>Displays active user accounts, IP addresses and last check-in times.</td>
</tr>
</tbody>
</table>
| 2.1.1    | Agent Status   | 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 |
<p>| 2.1.2    | Agent Logs     | Specifies how long to store log data.                                                                                                                                                                          |
| 2.1.3    | Log History    | Specifies event log types and categories included in event logs.                                                                                                                                              |
| 2.1.4    | Event Log Settings | Creates machine ID accounts and/or install packages for installing agents on single machines.                                                                                                                  |
| 2.2      | Install Agents | Deletes machine ID accounts.                                                                                                                                                                                   |
| 2.2.1    | Create         | Renames existing machine ID accounts.                                                                                                                                                                           |</p>
<table>
<thead>
<tr>
<th>2.2.4</th>
<th>Change Group</th>
<th>Reassigns machines to a different machine group or subgroup.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.5</td>
<td>Deploy Agents</td>
<td>Creates agent install packages for installing agents on multiple machines.</td>
</tr>
<tr>
<td>2.3</td>
<td>LAN Discovery</td>
<td>Uses an existing agent on a managed machine to periodically scan the local area network for any and all new devices connected to that LAN since the last time LAN Watch ran.</td>
</tr>
<tr>
<td>2.3.1</td>
<td>LAN Watch</td>
<td>Installs the agent on a remote system and creates a new machine ID / group ID account for any new PC detected by LAN Watch.</td>
</tr>
<tr>
<td>2.3.2</td>
<td>Install Agents</td>
<td>Displays the results of the latest LAN Watch scan.</td>
</tr>
<tr>
<td>2.3.3</td>
<td>View LAN</td>
<td>Lists all computers listed in an Active Directory when LAN Watch runs on a system hosting Active Directory. Installs agents on AD machines.</td>
</tr>
<tr>
<td>2.3.5</td>
<td>View AD Users</td>
<td>Lists all Active Directory users discovered by LAN Watch when LAN Watch runs on a system hosting Active Directory. Creates VSA users from AD users.</td>
</tr>
<tr>
<td>2.3.6</td>
<td>View vPro</td>
<td>Displays hardware information about vPro-enabled machines discovered while running LAN Watch.</td>
</tr>
<tr>
<td>2.4</td>
<td>Configure Agents</td>
<td>Mass copies settings from one machine account to other machine accounts.</td>
</tr>
<tr>
<td>2.4.1</td>
<td>Copy Settings</td>
<td>Imports and exports agent settings, including scheduled agent procedures, assigned monitor sets, and event sets, as XML files.</td>
</tr>
<tr>
<td>2.4.3</td>
<td>Suspend</td>
<td>Suspends all agent operations, such as agent procedures, monitoring, and patching, without changing the agent's settings.</td>
</tr>
<tr>
<td>2.4.4</td>
<td>Agent Menu</td>
<td>Customizes the agent menu on managed machines.</td>
</tr>
<tr>
<td>2.4.5</td>
<td>Check-In Control</td>
<td>Controls agent check-in frequency on agent machines.</td>
</tr>
<tr>
<td>2.4.6</td>
<td>Working Directory</td>
<td>Sets the path to a directory used by the agent to store working files.</td>
</tr>
<tr>
<td>2.4.7</td>
<td>Edit Profile</td>
<td>Edits machine account information.</td>
</tr>
<tr>
<td>2.4.8</td>
<td>Portal Access</td>
<td>Sets up accounts to allow machine users remote control access to their own machines.</td>
</tr>
<tr>
<td>2.4.9</td>
<td>Set Credential</td>
<td>Sets a logon credential for the agent to use in Patch Management, the Use Credential procedure command, Kaseya Endpoint Security, and Desktop Policy and Migration.</td>
</tr>
</tbody>
</table>
2.1 Machine Status

2.1.1 Agent Status

The Agent Status page provides a summary view of a wide variety of agent data. Any data pertaining to the agent can be obtained by selecting the appropriate data column. The data columns are fully customizable and can be selected according to the requirements. Fig. 2.9 shows a general view of the agent status page. Portions of this page are labeled in the figure. A brief description for each label is provided below.

1. **Select Columns**: Select columns can be used to specify which columns are to be displayed in the agent status window. Fig. 2.10 shows the Column Select window. The ordering of the column data can be rearranged using the up and down arrow buttons.

   **Example**: Display the Machine ID, Current user, Last Reboot Time, Last Check in Time, Group ID & Time Zone.

   1. Select *Machine ID* in the Not Displayed window. Click Add >>
   2. Select *Current User* in the Not Displayed window. Click Add>>
   3. Select *Last Reboot* time in the Not Displayed window. Click Add>>
   4. Select *Last Check* in time in the Not Displayed window. Click Add>
   5. Select *Group ID* in the Not Displayed window. Click Add>>
   6. Select *Time Zone* in the Not Displayed window. Click Add>>

Once all the options are selected and added to the Displayed window, the Apply button must be clicked to apply the desired settings.
VSA provides a wide variety of agent data that can be displayed in the Agent status page according to the requirements. The list of column data along with a brief description that can be selected is listed below.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine ID</td>
<td>Machine ID label used throughout the system.</td>
</tr>
<tr>
<td>Group ID</td>
<td>The group ID portion of the machine ID.</td>
</tr>
<tr>
<td>Last Checkin Time</td>
<td>Most recent time when a machine checked into the KServer.</td>
</tr>
<tr>
<td>First Checkin Time</td>
<td>Time when a machine first checked into the KServer.</td>
</tr>
<tr>
<td>Last Reboot Time</td>
<td>Time of the last known reboot of the machine.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>The time zone used by the machine.</td>
</tr>
<tr>
<td>Computer Name</td>
<td>Computer name assigned to the machine.</td>
</tr>
<tr>
<td>Domain/Workstation</td>
<td>The workgroup or domain the computer belongs to.</td>
</tr>
<tr>
<td>Agent GUID</td>
<td>A globally unique identifier for a machine ID, group ID account and its</td>
</tr>
<tr>
<td></td>
<td>corresponding agent.</td>
</tr>
<tr>
<td>DNS Computer Name</td>
<td>The fully qualified DNS computer name for the machine, which comprises</td>
</tr>
<tr>
<td></td>
<td>the computer name plus the domain name. For example: jsmithxp.acme.com.</td>
</tr>
<tr>
<td></td>
<td>Displays only the computer name if the machine is a member of a workgroup.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Operation system type the machine is running.</td>
</tr>
<tr>
<td>OS Version</td>
<td>Operation system version string.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address assigned to the machine.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Networking subnet assigned to the machine.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Default gateway assigned to the machine.</td>
</tr>
<tr>
<td>Connection Gateway</td>
<td>IP address seen by the KServer when this machine checks in. If the</td>
</tr>
<tr>
<td></td>
<td>machine is behind a DHCP server, this is the public IP address of the</td>
</tr>
<tr>
<td></td>
<td>subnet.</td>
</tr>
<tr>
<td>Country</td>
<td>The country associated with the Connection Gateway.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC address of the LAN card used to communicate with the KServer.</td>
</tr>
<tr>
<td>DNS Server 1, 2</td>
<td>IP address of the DNS servers assigned to the machine.</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>The IP address of the DHCP server used by this machine.</td>
</tr>
<tr>
<td>Primary/Secondary WINS</td>
<td>WINS settings.</td>
</tr>
<tr>
<td>CPU Type</td>
<td>Processor make and model.</td>
</tr>
<tr>
<td>CPU Speed</td>
<td>Clock speed of the processor.</td>
</tr>
<tr>
<td>CPU Count</td>
<td>The number of CPUs.</td>
</tr>
<tr>
<td>RAM Size</td>
<td>MBytes of RAM on the machine.</td>
</tr>
<tr>
<td>Agent Version</td>
<td>Version number of the Kaseya agent loaded on the machine.</td>
</tr>
<tr>
<td>Current User</td>
<td>Logon name of the machine user currently logged into the machine (if any).</td>
</tr>
<tr>
<td>Last Logged In User</td>
<td>Logon name of the last person to log into the machine.</td>
</tr>
<tr>
<td>Portal Access Logon</td>
<td>Logon name given to a machine user for logging into the KServer.</td>
</tr>
<tr>
<td>Portal Access Remote Control</td>
<td>Enabled if this machine user can log in and get remote control access to</td>
</tr>
<tr>
<td></td>
<td>their own machine from another machine. Disabled if access is denied.</td>
</tr>
<tr>
<td><strong>Portal Access Ticketing</strong></td>
<td>Enabled if this machine user can log in and enter trouble tickets. Disabled if access is denied.</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Portal Access Chat</strong></td>
<td>Enabled if this machine user can initiate chat sessions with a VSA user. Disabled if access is denied.</td>
</tr>
<tr>
<td><strong>Primary/Secondary KServer</strong></td>
<td>IP address / name the machine uses to communicate with the KServer.</td>
</tr>
<tr>
<td><strong>Quick Checkin Period</strong></td>
<td>Quick check in time setting in seconds.</td>
</tr>
<tr>
<td><strong>Contact Name</strong></td>
<td>Machine user name entered in Edit Profile.</td>
</tr>
<tr>
<td><strong>Contact Email</strong></td>
<td>Email address entered in Edit Profile.</td>
</tr>
<tr>
<td><strong>Contact Phone</strong></td>
<td>Phone number entered in Edit Profile.</td>
</tr>
<tr>
<td><strong>Contact Notes</strong></td>
<td>Notes entered in Edit Profile.</td>
</tr>
<tr>
<td><strong>Manufacturer</strong></td>
<td>System manufacturer.</td>
</tr>
<tr>
<td><strong>Product Name</strong></td>
<td>System product name.</td>
</tr>
<tr>
<td><strong>System Version</strong></td>
<td>Product version number.</td>
</tr>
<tr>
<td><strong>System Serial Number</strong></td>
<td>System serial number.</td>
</tr>
<tr>
<td><strong>Chassis Serial Number</strong></td>
<td>Serial number on the enclosure.</td>
</tr>
<tr>
<td><strong>Chassis Asset Tag</strong></td>
<td>Asset tag number on the enclosure.</td>
</tr>
<tr>
<td><strong>External Bus Speed</strong></td>
<td>Motherboard bus speed.</td>
</tr>
<tr>
<td><strong>Max Memory Size</strong></td>
<td>Max memory size the motherboard can hold.</td>
</tr>
<tr>
<td><strong>Max Memory Slots</strong></td>
<td>Total number of memory module slots available.</td>
</tr>
<tr>
<td><strong>Chassis Manufacturer</strong></td>
<td>Manufacturer of the enclosure.</td>
</tr>
<tr>
<td><strong>Chassis Type</strong></td>
<td>Enclosure type.</td>
</tr>
<tr>
<td><strong>Chassis Version</strong></td>
<td>Enclosure version number.</td>
</tr>
<tr>
<td><strong>Motherboard Manufacturer</strong></td>
<td>Motherboard manufacturer.</td>
</tr>
<tr>
<td><strong>Motherboard Product</strong></td>
<td>Motherboard product ID.</td>
</tr>
<tr>
<td><strong>Motherboard Version</strong></td>
<td>Motherboard version number.</td>
</tr>
<tr>
<td><strong>Motherboard Serial Num</strong></td>
<td>Motherboard serial number.</td>
</tr>
<tr>
<td><strong>Processor Family</strong></td>
<td>Processor type installed.</td>
</tr>
<tr>
<td><strong>Processor Manufacturer</strong></td>
<td>Processor manufacturer.</td>
</tr>
<tr>
<td><strong>Processor Version</strong></td>
<td>Processor version ID.</td>
</tr>
<tr>
<td><strong>CPU Max Speed</strong></td>
<td>Max processor speed supported.</td>
</tr>
<tr>
<td><strong>CPU Current Speed</strong></td>
<td>Speed processor is currently running at.</td>
</tr>
<tr>
<td><strong>vPro Host Name</strong></td>
<td>The name of the vProenabled machine set by vPro configuration.</td>
</tr>
<tr>
<td><strong>vPro-Computer Name</strong></td>
<td>The name of the vPro-enabled machine set by the operating system.</td>
</tr>
<tr>
<td><strong>vPro-Model</strong></td>
<td>The model of the vPro-enabled machine.</td>
</tr>
<tr>
<td><strong>vPro-Manufacturer</strong></td>
<td>The manufacturer of the vPro-enabled machine.</td>
</tr>
<tr>
<td><strong>vPro-Version</strong></td>
<td>The version of the vPro-enabled machine.</td>
</tr>
<tr>
<td><strong>vPro-Serial Number</strong></td>
<td>The serial number of the vPro-enabled machine.</td>
</tr>
<tr>
<td><strong>vPro-Asset Number</strong></td>
<td>An asset management identifier assigned to the vPro-enabled machine.</td>
</tr>
<tr>
<td><strong>vPro-Motherboard Manufacturer</strong></td>
<td>The manufacturer of the motherboard of the vPro-enabled machine.</td>
</tr>
<tr>
<td><strong>vPro-Motherboard Version</strong></td>
<td>The version number of the motherboard of the vPro-enabled machine.</td>
</tr>
</tbody>
</table>
### 2. Filter
Filter is used for displaying selective information of rows in the paging area. For example, to search for the machine ID "pc1.cec.fiu-johndoe", enter "pc1*" in the text box in the window as shown in the Fig. 2.11 next to Machine ID.

**Note:** "*" asterisk wildcard can be used with the text you enter to match multiple records.

### 3. Reset filter
The Reset filter is used to clear all the filter settings. This option is not displayed by default. It is only displayed if the advanced filter is selected. The advanced filter can be used by selecting Filter.

### Check-In Status
Once a machine ID is created for an agent, check-in icon displays next to each machine ID account in VSA. These icons indicate the agent check-in status of each managed machine. These icons appear in most of the modules in VSA and it is important to remember the icons to quickly determine the status of the agent on a particular machine. Below is a list of all icons and a brief explanation of the status they indicate.

- ![Agent icon](image)
  - Agent is Online but waiting for first audit to complete.
- ![Agent icon](image)
  - Agent is online.
- ![Agent icon](image)
  - Agent is online and user currently logged on. Icon displays a tool tip showing the logon name.
- ![Agent icon](image)
  - Agent is online and user currently logged on, but user not active for 10 minutes.
- ![Agent icon](image)
  - Agent is currently offline.
- ![Agent icon](image)
  - Agent has never checked in.
- ![Agent icon](image)
  - Agent is online but remote control has been disabled
- ![Agent icon](image)
  - Agent has been suspended

### 2.1.2 Agent Logs
The **Agent Logs** page displays the log data for each of the managed machines. For each type of log a corresponding log report is provided. This helps to identify the events that occurred with a corresponding managed machine. The events along with the time are displayed in this window as shown in Fig. 2.12.
Note: The system automatically limits the number of log entries per log type per machine to 1000. Once the limit has been reached, if archiving is enabled, and deleted from the system, log entries exceeding the limit are archived. The archive option is set in Agent > Log History.

Portions of this page are labeled in the figure. A brief description for each label is provided below.

1. Selecting Machine ID: Select the machine ID for which you want to see the log information.

2. Select Log: Select Log allows you to choose the appropriate log information to be displayed for the selected machine ID. The types of log that are available are:

- **Alarm Log**: Lists all alarms triggered for the selected machine.
- **Monitor Action Log**: The log of alarm conditions* that have occurred and the corresponding actions, if any has been taken in response to them.
- **Agent Log**: Displays a log of agent, system, and error messages.
- **Configuration Changes**: Displays VSA settings changes for the selected machine.
- **Network Statistics**: Displays a log of send/receive data for network applications.
- **Event Logs**: Displays event log data collected by Windows. It is not available for Win9x. Only event logs that apply to the selected machine display in the event log drop-down list.
- **Agent Procedure Log**: Displays a log of successful/failed agent procedures.
- **Remote Control Log**: Displays a log of successful/failed remote control sessions.
- **Log Monitoring**: Displays Log monitoring entries.

Alarm Condition:
An alarm condition exists when a machine’s performance succeeds or fails to meet pre-defined criteria.

![Fig. 2.12: Agent Logs](image1)

![Fig. 2.13: Events per page](image2)
3. **Events per page:** Events per page allow you to specify the number of rows that can be displayed in the agent logs page.

   **Example:** Selecting "10" from the drop down menu as shown in Fig. 2.13 below would display 10 rows of events.

4. **Filter:** Filter option is used to restrict the amount of data displayed. The Event log filter has different event categories. You can specify a different advanced filter for each event category and column of data displayed. After populating the options, click Apply. By default Apply Event Log filter is selected. If the option is not selected, the filters are not applied.

5. **Start Date / End Date / Refresh:** This option allows you to filter the log data by specifying the date range. Click Refresh to see the new filtered data.

### 2.1.3 Log History

The Log History page (Fig. 2.14) determines the number of days to store the log on a per log basis for each machine ID. These settings are set as default from the agent install package (see section 2.2 for details). This page also determines whether agent log data is subsequently archived to text files located on a network directory.

- Log data is displayed using Agent logs or printed to a report using **Info Center > Reporting > Logs**.
- **System > Check-in-Policy** can restrict the number of days users can keep log entries, to avoid placing undue stress on servers running the KServer service.

### Log File Locations

Monitoring data log archives are stored in the `<KaseyaRoot>\UserProfiles\dbBackup` directory. This is to improve performance on systems where the log 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.

Portions of this page are labeled in the figure. A brief description for each label is provided below.

1. **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.

   - **Agent Log** - The log of agent, system, and error messages.
   - **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 > Network Statistics.

- **Agent Procedure Log** - Displays a log of successful/failed agent procedures.
- **Remote Control Log** - Displays a log of remote control events.
- **Alarm Log** - The log of all alarms issued.
- **Monitor Action** - The log of alarm conditions that have occurred and the corresponding actions, if any that have been taken in response to them.
- **SYS log** - The log of all system check external systems.

2. **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
- **Monitor Log** - The log of data collected by monitoring sets.
- **SNMP Log** - The log of all data collected by SNMP sets.

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

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

### 2.1.4 Event Log Settings

An Event Log service runs on Windows operating systems (Not available with Win9x) and it enables event log messages to be issued by Window based programs and components. These events are stored in event logs located on each machine. The event logs of managed machines stored in the KServer database, serve as the basis of alerts and reports, and be archived.

The Event Log Settings page as shown below in Fig. 2.15 specifies the event log types and categories included in Agent > Log History. The list of event log types available on this page can be updated using Monitor > Update lists by scan.

Portions of this page are labeled in the figure. A brief description for each label is provided below.

1. **Event log types**: Depending on the operating system, the event log types available include but are not limited to:
   - Application log
   - Directory Service
   - DNS Server
   - Internet Explorer
   - Security
   - System
2. **Event categories**: The event categories stored by VSA for this machine ID and event log:
   - Error
   - Warning
   - Information
   - Success Audit
   - Failure Audit
   - Critical - Applies only to Vista.
   - Verbose - Applies only to Vista.

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

4. **Replace**: Replaces all event log types assigned to selected machine IDs with the event log types listed in the *Assigned Event Logs* list.

5. **Clear All**: Clears all event log types assigned to select machine IDs.

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>>* or *Add all>>* 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.

**Flood Detection**

If 1000 events, not counting black list events are uploaded to the KServer 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 KServer. Alarm detection and processing operates regardless of whether collection is suspended.

2.2 Install Agents

2.2.1 Create

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

- **Machine ID templates** - In this case, no install package needs to be created, since agent templates are not intended for installation to a machine.
- **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.

**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 an agent template. Agent 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 or Macintosh operating systems, or to automatically choose the type of operating system of the downloading computer.

Machine ID templates
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.

The following operations can be performed with the help of agent templates.

• Create machine ID templates using Agent > Create.
• Import a machine ID template using Agent > Import/Export.
• Deploy an agent install package on an agent template using Agent > Deploy Agents.
• Copy selected settings from agent templates to existing machine ID accounts using Agent > Copy Settings.
• Identify the total number of agent template accounts in your VSA using System > Statistics.
• Configure settings for the agent template using the standard VSA functions
• Separate agent templates are recommended for Windows and Macintosh machines.
• Alternatively a package can be created that selects the appropriate OS automatically and copy settings from a template that includes an agent procedure that uses OS specific steps.

Fig. 2.16: Copy Settings while creating machine ID

1. Select a machine ID from the paging area as shown in Fig. 2.16 above by clicking on the radio button next to it.
2. Click on Set. You can notice that the machine ID that was selected appears under Copy new ac-
count settings from as shown in the figure above.

3. Enter the name of the machine ID in the New machine ID field and click Create.

Note: If you do not include a machine ID to copy from and click Create, a new, usable machine ID account is created using KServer defaults. You can copy settings between existing machine ID accounts at any time using Agent > Copy Settings.

Fig. 2.17 below shows the general view and all the available functions that are supported on the Create page.

1. New Machine ID: Enter a unique name for the new machine ID you are creating.

2. 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.

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

4. Set/Clear new accounts created in group ID <GroupID> copy settings from <Machine ID>: For each group ID you can specify a different default machine ID to copy settings from.
   - Select a machine ID to copy settings from by clicking the radio button next to any machine ID listed in the paging area.
   - Select a group ID from the group ID drop-down list.
   - 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.
   - Click the link to remove this assignment.

5. 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.
   - 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.
   - Click 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.
   - Click the Clear link to remove this assignment.

2.2.2 Delete

The Delete page (Fig. 2.18) 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 KServer. The account is not deleted until the next time the agent success-
fully checks in.

- **Delete account now without uninstalling the agent**: Leave the agent installed and remove the machine ID account from the KServer.
- **Uninstall the agent and keep the account**: Uninstall the agent from the machine without removing the machine ID account from the KServer.

Portions of this page are labeled in the figure. A brief description for each label is provided below.

1. **Machine.Group ID**: The list of Machine.Group IDs is displayed based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

2. **Select Uninstall/Delete option**: Make a choice of uninstall/delete depending on the requirement.

3. **Delete Accounts**: Delete accounts option deletes/uninstall the machine ID that was selected depending on the option selected.

4. **Clean Database**: Removing a machine account using this Delete page marks the machine account for deletion. Actual deletion usually occurs during off hours to preserve resources during working hours. There are some cases where it is useful to purge machine accounts immediately. For example, your KServer may exceed the agent license count. Click **Clean Database** to immediately purge machine accounts that are already marked for deletion.

5. **Select old accounts that have not checked in since <date>**: Click the **Select old** hyperlink to check all machine IDs in the paging area that have not checked in since the specified date. This is an easy way to identify and remove obsolete machine IDs.

6. **Last Check-In**: Displays the time the machine’s agent last checked in to the KServer. Agents that have not checked-in recently display this information in red text.

### 2.2.3 Rename

The **Rename page** renames any existing machine ID account to a new one. You can change the machine ID and/or re-assign it to a different group ID. The Rename page is shown in Fig. 2.19 and all the options supported by this module are listed below.
1. **Rename Account**: This option renames a selected machine ID account to a new one.

2. **Merge offline account <Offline Machine ID> into <Select Machine ID> Delete <Offline Machine ID> after merge**: Merge option is used 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.

The above operation can be performed as follows:
- Select **Merge offline account** option and select the machine ID from the drop down menu.
- Select a machine ID from the list of machine ID’s displayed in the paging area.
- Click **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. **New Name**: Enter the New Name for the selected machine ID.

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

5. **Machine.Group ID**: The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view. Click the radio button to the left of the machine account you wish to rename.

6. **New name at next Check in**: Lists the new name of the account the next time that agent checks in. Only pending renames are displayed here.

### 2.2.4 Change group

The Change Group page (Fig 2.20) assigns a single or multiple machine IDs belonging to one group ID to a different group ID. Machines that are currently offline are assigned to the new group ID the next time they check in.
1. **Machine.Group ID**: The list of machine.group IDs displayed is based on the machine ID / group ID filter and the machine groups the user is authorized to view.

2. **Select new group ID**: Specify the new group ID to assign to each selected machine ID from the drop down list.

3. **Move**: The Move option assigns selected machine IDs to the selected group ID.

Moving a Machine ID to a Different Group

- Select one or more machine IDs in the paging area.
- Select a group ID from the Select new group ID drop-down menu.
- Click the Move button.

### 2.2.5 Deploy Agents

The **Deploy Agent** page creates and distributes an agent install package to multiple machines. **Agent > Create** can be used to create a machine ID account and agent install package in two separate steps and apply them to a single machine. **Agent > Create** can also be used to create agent templates or re-install an agent for an existing machine ID.

**Note**: To install agents on remote machines, use **Agent > Install Agents**

**Deploy Agents Wizard**

The **Deploy Agents** install package is created using the **Configure Automatic Account Creation** wizard. The wizard copies agent settings from an existing machine ID or agent template and generates an install package called "KcsSetup". All settings and pending agent procedures from the machine ID the agent settings are copied from – except the machine ID, group ID, and organization ID – are applied to every new machine ID created with the package.

**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 is bound to the install package.

**Editing Existing Install Packages**

Typically an existing Deploy Agents install package is edited just before re-distribution. The most common changes made to an install package are:
• Pre-selecting an organization ID, group ID or sub-group ID.
• Assigning a credential, if necessary.

Once edited, the install package can be re-created and distributed to its target customer and location.

**Distribution Methods**

Once the agent install package is created, you can use the following methods to the package:

1. **Logon**
   - **Windows** - Set up an NT logon procedure to run the install package every time a user logs into the network.
   
   *Note: Windows 98 is not supported.*
   
   - **Macintosh** - Set up a Mac OS X Login Hook Procedure to run the install package every time a user logs into the network.

2. **Email**

   Email “KcsSetup” to all users on the network. Download the appropriate install package from the Deploy Agents page, and 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.

3. **LAN Watch**

   Users can discover newly added machines during a LAN Watch and subsequently install agents remotely using the Agent > Install Agents page.

4. **Active Directory**

   Run LAN Watch on an Active Directory machine. From then on, Windows agents can be installed automatically on Windows machines as soon as users log in using the Active Directory.

5. **Manual**

   You can instruct users to download an install package agent from the “http://<VSA_Address>/dl.asp” website to their target machines. If more than one install package is displayed on the website, instruct users which package should be selected. Users can execute the “KcsSetup” installer using any of the following methods:

   **Windows**
   - Double click “KcsSetup” to launch it.
   - Open a command line window (CMD) 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**
   - Double click “KcsSetup” to launch it.
   - Open a terminal process, navigate to where “KcsSetup” is located and launch “KcsSetup” followed by any desired command line switches.

**Default User Install Packages**

Each user can specify their own default install package by selecting the Set Default radio button to the left of the package name. Users can download their own default agent immediately by selecting the Click to
download default Agent link on the Deploy Agents page.

**Unique ID Number**

You can tell users which install package to download by referencing the install package’s unique ID number. (Example: http://<VSA_Address>/dl.asp?id=123). The default install package is displayed with its unique ID number in the header of the Deploy Agents page.

**Assigning New Machine IDs to Machine Group by IP Address**

Maintaining multiple agent install packages in **Agent > Deploy Agents**, one for each organization, can be time consuming. Instead some server providers use a single agent package for the unnamed organization and perform all installs using this package. **System > Naming Policy** can reassign new agents to the correct organization, group ID automatically – the first time the agents check in – based on each managed machine’s IP or connection gateway. **Agent > Copy** Settings may be scheduled afterwards, to copy specific kinds of agent settings by machine ID template to the type of machine revealed by the baseline audit. This can be automated using agent procedures.

**Automatic Account Creation**

You must have automatic account creation enabled using **System > Check-in Policy** to automatically create a machine ID account when a Deploy Agents package is installed.

**Operating System Selection**

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

**Create Package**

To create a package, click **Create Package** to start a **Configure Automatic Account Creation** wizard where you can specify all configuration parameters for the install package.

The wizard is a 7 step process:

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. 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.

Note: Silent installs, also called silent deploys, do not prompt the user for input. Silent installs may not require user input or else provide a typical configuration that serves the purposes of most users, or else provide command line parameters that enable users to configure the installation at execution.

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

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 dialogue messages explaining this.

   **Note:** Credentials are only necessary if users are installing packages on machines and do not have administrator access to their network.

7. Name the install package for easy reference later. This name displays on the Deploy Agents page and the dl.asp download page.
Chapter 2 - Agents

Sadjadi et al.

Editing the Default Install Package

The Default Install package sets the default values displayed when you create a new package. Normally the Default Install package should not be modified. The Save button is disabled by default. To enable the Save button for the Default Install package, do the following as a master role user:

1. Click the Share button next to the Default Install package.
2. Click Take Ownership.
3. Check Allow other users to modify.
4. Click Save.
5. Click the edit icon next to the Default Install package.

Note: If you delete the Default Install package, it is re-created immediately.

Fig. 2.28 below shows the Deploy Agents page and all the available functions that this module provides. They are:

1. Click to download default Agent: Click the link to download the current VSA user’s default package directly from the page.

2. Users can download agents from: The web address for the agent to download from can be provided to user to download the agent. The unique ID number ensures that when the link is clicked, the default install package is selected and downloaded.

3. Manage packages from all administrators: This option can be checked to display all packages created by all VSA users. Once a hidden package is displayed, you can use the package, make the
package public or take ownership. This option is only available to master role users.

4. **Set Default**: An agent install package can be set as default install package by selecting the radio button to the left of the package name in the *Set Default* column.

5. **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.

6. **Edit Icon**: Click the edit icon next to a package to change the parameters for that package using the Configure Automatic Account Creation wizard.

7. **Package Name**: This field displays the name of the package.

8. **Public Package**: Public package rows display with a brown background. Private package rows display with a gray background.

9. **Share**: Click *Share* to share a private package with other users, user roles or to make the package public.

10. **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.

11. **Description**: Displays the description of the package.

### 2.3 LAN Discovery

#### 2.3.1 LAN Watch

**LAN Watch** uses an existing agent on a managed machine to periodically scan the local area network for any and all new devices connected to that LAN since the last time LAN Watch ran. These new devices can be workstations and servers without agents or SNMP devices. Optionally, VSA can send an alert when a LAN Watch discovers any new device. LAN Watch effectively uses the agent as a proxy to scan a LAN behind a firewall that might not be accessible from a remote server.

**Using Multiple Machines on the Same LAN**

Typically, you do not have to run a LAN Watch on more than one machine in a scan range. Some reasons to do a LAN Watch on multiple machines within the same scan range include:

- There are multiple SNMP Communities within the same scan range and therefore there are multiple machines with different SNMP Community Read values.
- There are multiple vPro-enabled credentials required.
- There are different alert configurations required.
- The user wishes to have redundant SNMP monitoring

**LAN Watch and Install Agents using Windows or Macintosh**

Both Windows and Macintosh agents can discover Windows and Macintosh machines on the same LAN using LAN Watch.

**Agent > Install Agents** can only install agents on:

- Windows machines if the LAN Watch discovery machine was a Windows machine.
Macintosh machines if the LAN Watch discovery machine was a Macintosh machine.

The generic view of the LAN Watch page is shown in Fig. 2.29 below. The options that are available for this module are:

![Fig. 2.29: LAN Watch](image)

1. **Schedule**: Click **Schedule** to display the Scheduler window, which is used throughout VSA to schedule a task. Schedule a task once or periodically. Each type of recurrence - Once, Hourly, Daily, Weekly, Monthly, Yearly - displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence. Not all options are available for each scheduled task. Options include:
   - Distribution Window - Reschedules the task to a randomly selected time no later than the number of periods specified, to spread network traffic and server loading.
   - Skip if offline - If checked and the machine is offline, skip and run during the next scheduled period and time. If blank and the machine is offline, run the task as soon as the machine is online again.
   - Power up if offline – It is available for Windows only. If checked, powers up the machine if offline. Requires Wake-On-LAN or vPro and another managed system on the same LAN.
   - Exclude the following time range - If checked, specifies a date/time range to not perform the task.

2. **Cancel**: Click **Cancel** to stop the scheduled scan. Cancel also deletes all records of the devices identified on a LAN from VSA. If you re-schedule LAN Watch after clicking Cancel, each device on the LAN is re-identified as though for the first time.

3. **Scan IP Range**: Set the minimum and maximum IP addresses to scan here. Selecting a machine ID to scan, by checking the box next to that machine’s name, automatically fills in the minimum and maximum IP range based on that machine’s IP address and subnet mask.

   **Note**: LAN Watch does not scan more than 2048 IP addresses. If the subnet mask of the machine running LAN Watch specifies a larger IP range, LAN Watch limits it to 2048 addresses. LAN Watch only detects addresses on the local subnet to the machine you run LAN Watch from. For example, with a subnet mask of 255.255.255.0, there can be no more than 253 other devices on the local subnet.

4. **Enable SNMP**: If checked, scan for **SNMP devices** within the specified Scan IP Range. SNMP Devices are network devices such as printers, routers, firewalls, servers and UPS devices that can’t support the installation of an agent. But a VSA agent installed on a managed machine on the same network as the device can read or write to that device using simple network management protocol (SNMP). Read/write instructions are communicated using a set of object variables. Collectively, the set of object variables made available by a device is called its Management Information Base or MIB. The objects within a MIB are therefore referred to as MIB objects.

5. **Read Community Name / Confirm**: LAN Watch can only identify SNMP devices that share the same SNMP community read value as the managed machine performing the LAN Watch. Enter the
value in the Read Community Name and Confirm text boxes.

**Note:** Community names are case sensitive. Typically the default read community name value is public, but may be reset by an administrator to Public, PUBLIC, etc.

6. **Enable vPro:** This option is available in Windows only. If checked, identifies vPro-enabled machines within the specified Scan IP Range. The machine does not need to be a vPro machine to discover vPro machines using LAN Watch. If a vPro machine is used as the LAN Watch discovery machine, it cannot discover itself.

7. **Enable Alerts:** If Enable Alerts is checked and a new device is discovered by LAN Watch, an alert is sent to all email addresses listed in Email Recipients. LAN Watch alerts and email recipients can also be specified using the Monitor > Alerts page.

**Note:** Machines that have not been connected to the LAN for more than 7 days and then connect are flagged as new devices and will generate an alert.

8. **Email Recipients:** If alerts are enabled, enter the email addresses where alert notifications are sent. You can specify a different email address for each managed machine, even if it is for the same event. The From email address is specified using System > Outbound Email.

9. **Ignore devices seen in the last <N> days:** Enter the number of days to suppress alerts for new devices. This prevents creating alerts for devices that are connected to the network temporarily.

10. **Run Script:** If the option is checked and an alarm condition is encountered, an agent procedure is run. You must click the Select agent procedure link to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking this machine ID link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

11. **Skip alert if MAC address matches existing agent:** Checking this box suppresses alerts if the scan identifies that the MAC address of a network device belongs to an existing managed machine with an agent on it. Otherwise a managed machine that was offline for several days and comes back online triggers an unnecessary alert during a LAN Watch.

12. **Machine.Group ID:** The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

13. **IP Range Scanned:** The IP addresses that are scanned by the selected machine ID when LAN Watch runs.

14. **Last Scan:** This timestamp shows when the last scan occurred. When this date changes, new scan data is available to view.

15. **Primary DC:** This is available for Windows only. If a primary domain controller icon is displayed, this machine ID is a primary domain controller. If checked, performing a scan on a primary domain controller running Active Directory enables you to “harvest” the users and computers throughout a domain. You can subsequently install VSA agents automatically on computers listed in Active Directory and create VSA users and VSA users based on Active Directory administrator credentials.

16. **SNMP Active:** If the SNMP icon is displayed, SNMP devices are included in the scheduled scan.

17. **vPro Active:** This option is available for windows only. If the vPro icon is displayed, vPro machines are included in the schedule scan.

18. **Alert Active:** If checked LAN Watch alerts are enabled for this scan.
2.3.2 Install Agents

The Install Agents page installs the agent on a remote system and creates a new machine ID / group ID account for any new machine detected by LAN Watch. Install Agents remotely installs the packages created using Agents > Deploy Agents. A list of machines with scan results is displayed when this page is first displayed. Clicking any machine ID displays a table listing all machines with a host name. Machines without an agent display in red text.

There are two methods of selecting machines to install agents on:

1. A list of machines is displayed on this page that have run LAN Watch. Clicking any LAN Watch machine displays a listing of all discovered machines. Machines without an agent display in red text.
2. You can also install an agent by entering an IP address or host name that you know the discovery machine has access to, even if it’s not listed on the page.

Using the Same Operating System for Discovery and Agent Installs

Windows, Macintosh, and Linux agents can discover Windows, Macintosh, and Linux machines on the same LAN using LAN Watch. Agent > Install Agents can only install agents on:

• Windows machines if the LAN Watch discovery machine was a windows machine.
• Macintosh machine if the LAN Watch discovery machine was a Macintosh machine.
• Linux machines if the LAN Watch discovery machine was a Linux machine.

Note: Macintosh agent install packages require a credential when using Agent > Install Agent, or when installing agents using the /s “silent install” switch.

Note: For Linux machines, the root username alone without a hostname or domain must be used.

Installing Agents on Selected Machines

1. Enter a administrator credential for the machines you’ve selected.
   - If the target machine is on a domain, the administrator credential must include the domain. The username field must be in the form domain\administrator or administrator@domain. If the target machine is not on a domain, then the administrator credential must include the hostname in the form hostname\administrator. For Linux machines, the root username alone without a hostname or domain must be used.
2. Select an agent install package. The selected agent install package must be appropriate for:
   - Windows machines if the LAN Watch discovery machine was a Windows machine.
   - Macintosh machines if the LAN Watch discovery machine was a Macintosh machine.
   - Linux machines if the LAN Watch discovery machine was a Linux machine.
3. Click Install.

Kconnect and SSH

The following technologies are used by Agent > Install Agents to install agents on remote systems after a LAN Watch scan is run on the discovery machine.

• Kconnect enables the installation of agent packages on remote target systems running a Windows operating system.
• SSH (aka Secure Shell) is a network protocol that allows data to be exchanged using a secure channel between two networked devices. This protocol is primarily used on Unix-based systems, including Mac OS X and Linux.
  - Mac OS X 10.3.9 and above machines must have SSH Remote Login in System Preferences > Sharing > Remote Login enabled to support the remote install of Macintosh agents using Install Agents.
  - On Linux sshd must be installed and enabled. This is not enabled by default in some Linux distributions.
• A valid credential set with administrator rights is required to successfully install an agent remotely.
Note: 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. The installer overwrites installation if it detects an agent is already installed on a machine if the \r switch is present in the installer package. The \r switch overrides the \eswitch if both switches are included in the agent package.

Running Kconnect
When Install Agent is run, Kconnect.exe is downloaded from the KServer into the c:\kworking directory and run using the following command line. You don’t have to create this command line. Install Agent does it for you.

c:\kworking\kconnect \hostname -u “adminname” -p “password” -c -f -d “c:\kworking\kcsetup.exe” > c:\kworking\LANIlnsAipAddr.txt

The terms hostname and ipAddr refer to the remote machine. If the agent is on a drive other than C: then the working files are referenced to the same drive the agent is installed on.

Kconnect Error Messages
If a remote Windows agent installation fails for any reason, the KServer passes back the results reported by Kconnect.exe. Typically, Kconnect.exe is simply reporting OS errors that it received trying to execute a call.

Typical Reasons for Install Failure
For a general agent install issues and failures refer Agents > Deploy Agents > Install issues and failures. Additional issues and failure related to remote installation of agents using Install Agents include:

- File and Printer Sharing Not Enabled - Verify File and Printer Sharing is enabled on the target machine’s firewall if the target machine’s firewall is on.
- Blocked by Network Security Policy
  - Windows - Kconnect.exe connects to the remote PC through the RPC service and runs as a local account. Remote access to this service is controlled by a Local or Domain Security Setting. Open Local Security Policy (part of Administrative Tools). Open Local Policies\Security Options\Network access: Sharing and security model for local accounts. The policy must be set to Classic for Kconnect.exe to operate across the network.
  - Macintosh - SSH can be blocked by client management network policies, which are configured using Server Admin in Mac OS X 10.4 and later.
- Failure to Connect - The RPC service is not available on the target machine. For example, XP Home does not support RPC. This prevents anything from remotely executing on that box. On Windows XP you can turn this service on by opening Windows Explorer and selecting Tools - Folder Option... - View tab. Scroll to the bottom of the list and uncheck Use simple file sharing. The XP default configurations are as follows:
  - XP Pro on a domain - RPC enabled by default. Use simple file sharing is unchecked.
  - XP Pro in a工作组 - RPC disabled by default. Use simple file sharing is checked.
  - XP Home - RPC disabled always. Use simple file sharing is not available.
- Network Path Not Found - If you get a message saying that the network path could not be found, it means that the admin$ share is not available on that machine. The admin$ share is a default share that windows creates when it boots, it is possible to turn this off via the local security policy, or domain policy. If you want to check the shares on that remote machine you can use Kconnect.exe to retrieve a list for you. Type kconnect \ “net share”. Check that the admin$ share exists and points to c:\windows or c:\winnt on older operating systems.
- Blocked by Anti-Virus Program - Some anti-virus programs may classify Kconnect.exe and SSH as security threats and block its execution.
- Invalid Credential - The credential must have administrator rights on the local machine. The agent requires administrator rights to install successfully.
  - If the target machine is on a domain, the administrator credential must include the domain. The username field must be in the form domain\administrator or administrator@domain. If the target machine is not on a domain, then the administrator credential must include the hostname in the form hostname\administrator. For Linux machines, the root username alone without a hostname or domain must be used.
  - On Vista, 7, and 2008 machines, ensure User Account Control (UAC) is disabled for the
administrator rights credential being used.
• Mac OS - Macintosh agent install packages require a credential when using Agent > Install Agent, or when installing agents using the /s “silent install” switch.
• Linux - Linux machines credentials must use the root user on the Install Agents page. Embedding a root credential in the agent install package is unnecessary for Linux agent install packages used on the Install Agents page.

**SSH Not Installed or Enabled** - Mac OS X 10.3.9 and above machines must have SSH Remote Login in System Preferences > Sharing > Remote Login enabled to support the remote install of Macintosh agents using Install Agents. On Linux sshd must be installed and enabled. This is not enabled by default in some Linux distributions.

**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 > Deploy Agents page.
3. Click the Click to download default Agent hyperlink to begin downloading the the default agent install package. A Linux agent install package will download.

   **Note:** Alternately, you can create your own Linux package by pressing Create Package and stepping through the wizard.

4. 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 Macintosh installs.

5. 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.

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

**Installing Linux Agents Using LAN Watch and Install Agents**

1. Schedule a LAN Watch scan using an existing Linux agent as the discovery machine.
2. Install a Linux agent on a discovered Linux machine, using the Install Agents page.
   • 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.

**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.

**Fig. 2.30** below shows the generic view of the Install agents page. The options available on this page are listed and explained below.

1. **Admin Logon Name:** The administrator name used to remotely access the selected machine. The Admin Logon Name must have administrator rights on the remote selected machine. Multiple accounts may have administrator rights on the same machine. Your domain administrator account may be different than the local administrator account. To ensure you are using the domain account, enter the logon name using the domain administrator format. If the domain is left off, the local account will be used.

2. **Password:** The password associated with the Admin Logon Name.

3. **Install:** Click Install to schedule an installation of the selected install package on all selected machines.

4. **Cancel:** Click Cancel to cancel execution of this task on selected managed machines.

5. **Select a Windows Agent Package to Install:** Select the agent package to remotely install on selected machines. These packages are created using Agents > Deploy Agents.

6. **IP address to install an undiscovered machine:** Enter an IP address to install agent on that machine.

**Note:** This feature allows you to install agent on a machine using the IP address within the network only.
7. **Hide devices that match the MAC address of existing machine IDs:** Check this box to hide all machines on a LAN with a MAC address matching the MAC address of an existing machine ID / group ID account.

8. **Hide devices that match the computer names of existing machine in <machine ID>:** Check this box to hide machines that have a common computer name in this same group ID. A LAN Watch may discover a managed machine with a second device using a different MAC ID then the one used to report to the KServer. For example, the same managed machine may connect to the internet using direct connection and have a second wireless connection with a different MAC ID. Checking this box hides the second device from this list so that you don’t assume you’ve found a new unmanaged machine.

9. **Host Name:** The host name of each device on the LAN discovered by the latest LAN Watch scan.

10. **IP Address:** The private IP address of each device discovered by the latest LAN Watch scan.

11. **MAC Address:** The MAC address of each device discovered by the latest LAN Watch scan.

12. **Vendor:** The system manufacturer.

13. **Last Seen:** The time each device was last detected by the latest LAN Watch scan.

### 2.3.3 View LAN

The **View LAN** (Fig 2.31) page displays the results of the latest LAN Watch scan run on a machine ID. Only machine IDs with returned scan data can be selected. Click any machine ID to display a table listing all machines and devices found by LAN Watch run on that machine ID. Data only displays in the host name column for machines, not devices. Paging rows can be sorted by clicking column heading links.

1. **Host Name:** The host name of each device on the LAN discovered by the latest LAN Watch scan. A host name only displays for computers. Hubs, switches, routers, or other network appliances do not return a host name.

2. **IP Address:** The private IP address of each device discovered by the latest LAN Watch scan.

3. **MAC Address:** The MAC address of each device discovered by the latest LAN Watch scan.

4. **Vendor:** The system manufacturer.

5. **Last Seen:** The time each device was last detected by the latest LAN Watch scan.

6. **SNMP Info:** SNMP identifying information
2.3.4 View AD Computers

The View AD Computers page shows all computers listed in an Active Directory* when LAN Watch runs on a system hosting Active Directory. Active Directory is a directory service used to store information about the network resources across a domain. Its main purpose is to provide central authentication and authorization services for Windows based computers. An Active Directory structure is a hierarchical framework of objects. The objects fall into three broad categories: resources (e.g. printers), services (e.g. e-mail) and users (user accounts and groups). The AD provides information on the objects, organizes the objects, controls access and sets security. VSA can reference information stored in Active Directory during a LAN Watch. View AD Computers can be used to install agents automatically on computers listed in the Active Directory by policy at computer startup.

Using this method has the following benefits:

• This policy ensures an agent is always present on a machine at every reboot, even if the agent is subsequently removed by a user.
• Agents can be deployed to an entire AD network even if VSA user does not know the local credentials for each computer.
• A LAN Watch scan performed by an AD machine discovers all computers that are members of a domain, whether the machines are online or not.

Summary View
The summary view of View AD Computers lists all domain controllers that have run LAN Watch for all machine groups.

• Discovered By: Lists the machine ID.group ID names of domain controllers that have performed a LAN Watch scan.
• Computers Found: Lists the number of computers, with or without agents, listed in the domain controller directory.
• Agents Installed: Lists the number of computers with agents that are also listed in the domain controller’s directly.

Details View
The details view of View AD Computers displays computers listed in active directory services hosted on computers that have run LAN Watch within a specified machine group.

Installing Agents on Active Directory Computers
You can associate an install package with an AD computer. This installs an agent package when the AD computer reboots, unless the agent is already installed. You can specify the agent package installed for each AD computer.

As shown in Fig. 2.32, to associate an install package with an AD computer:

1. Check Show Details as shown in Fig. 2.32 below to display the Canonical Name* of discovered computers in the paging area.
2. Select an agent package from the Select an Agent Package to install drop-down list.
3. Click Install Agent Policy.
4. Optionally click Update Agent Policies to copy a changed agent install package to the AD computer. The updated install package replaces the copy on the AD computer.
5. Optionally select an AD computer and click Cancel to un-associate an install package with an AD computer.

Canonical Name: The primary name for an object in DNS. Each object can also have an unlimited number of aliases.
2.3.5 View AD Users

The View AD Users page lists all AD users discovered by LAN Watch when LAN Watch runs on a system hosting Active Directory.

Using View AD Users:
- Agents can be automatically installed on each machine an AD user logs onto.
- VSA users logons can be created based on AD user logons.
- Portal Access logons can be created based on AD user logons.
- Contact information can be extracted from AD users and applied to the contact information for machine IDs.

Summary View
The summary view of View AD Computers lists all domain controllers that have run LAN Watch for all machine groups.

- **Discovered By**: Lists the machine ID, group ID names of domain controllers that have performed a LAN Watch scan.
- **Computers Found**: Lists the number of computers, *with or without agents*, listed in the domain controller directory.
- **Agent Installed**: Lists the number of computers *with agents* that are also listed in the domain controller’s directory.

Details view
The details view of View AD Users displays a list of Active Directory users on domain controllers that ran LAN Watch within a specified machine group.

Installing agents on any machine an AD User logs onto
You can associate an install package with an AD User. This installs an agent package on any machine an AD user logs onto, unless the agent is already installed. Even if the agent is subsequently removed from a machine, the agent will be re-installed the next time the AD user logs on. You can specify the agent package installed for each AD user.

As shown in Fig. 2.33, to associate an install package with an AD User:
1. Select AD users listed in the Logon Name column of the paging area as shown in Fig. 2.33.
2. Select an agent package from the Select an Agent Package to Install drop-down list.
3. Click Install Agent Policy.
4. Optionally click Update Agent Policies to copy a changed agent install package to the AD user’s computer. The updated install package replaces the copy on the AD user’s computer.
5. Select an AD user and click Cancel to un-associate an install package with an AD user.
Creating VSA Users Based on AD Users

VSA users created using this method log onto VSA using their AD domain, user name, and password. This means users only have to maintain credentials in a single location, the Active Directory.

Note: If a VSA staff record is created based on an AD user, VSA staff record can only be changed in AD and not within VSA but can be done only in Active Directory. An AD user can only be associated with either a VSA user logon or a machine user logon but not both.

As shown in Fig. 2.34, to create a new VSA user based on an AD user:
1. Select an AD users listed in the Logon Name column of the paging area as shown in Fig. 2.34.
2. Select a user role from the Select Role drop-down list.
3. Select a scope from the Select Scope drop-down list.
4. Click Create User.

You can confirm the creation of the new VSA user using System > Users. VSA user names based on AD users are formatted as follows: <domainname>|<username>.

Creating Portal Access Logons Based on AD Users

Portal Access logons can be created based on AD users. VSA users created using this method can log onto VSA Portal Access menu using their AD domain, user name, and password. This means credentials only have to be maintained in a single location, the Active Directory.
As shown in Fig. 2.35, to create a new Portal Access logon based on an AD user:
1. Click the unassigned link for an AD user listed in the Assigned To column of the paging area as shown in Fig. 2.35.
2. Select a machine ID, group ID account in the popup window. The popup window closes.
3. Select the checkbox for this same AD user in the left most column.
4. Click Create Machine Logon.

You can confirm the creation of the new VSA user using Agent > Portal Access.

Creating Staff Members Based on AD Users

Create staff member records based on AD users. If AD user information is changed, then VSA updates the corresponding staff member record with the AD user information. This means user information only has to be maintained in one place, the Active Directory.

As shown in Fig. 2.36, to create new VSA Portal Access logon based on an AD user:
1. Select a department from the Select Department drop-down list as shown in Fig. 2.36.
2. Select the checkbox for an AD user in the left most column.
3. Click Create Staff Member.
Chapter 2 - Agents

You can confirm the creation of the new VSA user using **System > Manage**.

**Converting Your VSA Logon to use your Domain Logon**

You can convert your own VSA logon to use your domain logon as follows:

1. Open the **System > Change Logon** page in VSA.
2. Enter your current VSA password in the **Old Password** field.
3. Enter your domain and domain logon name, formatted all in lowercase using the format domain/username, in the **Username** field.
4. Enter your domain password in the **New Password / Confirm Password** fields.

This enables you to logon to VSA using your domain logon and have your VSA logon name and password managed using Active Directory. At the same time, you can continue to use all your previous VSA share rights, procedures and other user settings.

### 2.3.6 View vPro

The **View vPro** page displays hardware information about vPro-enabled machines discovered while running LAN Watch. This information is only available if a machine’s vPro credential is specified by the LAN Watch.

Types of hardware information returned by the vPro machine include:

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

**Note:** vPro-enabled machines with a vPro credential can be powered up, powered-down or rebooted using **Remote Control > Power Management**. A vPro-enabled machine can be booted up using an ISO file using **Remote Control > Remote ISO Boot**.
Chapter 2 - Agents

2.3 Configure Agents

2.4.1 Copy Settings

The Copy Settings page copies selected settings from a single 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 might need to update settings on existing machine ID accounts as your customer requirements change and your knowledge of VSA grows. In this case, use Agent > Copy Settings to copy these changes to any number of machines IDs you are authorized to access.

It is recommended to make 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.

Procedure to copy settings

1. Click Select machine ID to select the source machine that you want to copy the settings from.

2. Select the source machine from the pop up window by selecting the appropriate group ID.
3. Once the machine ID is selected, a second pop up window screen displays the type of settings that can be copied. Select the appropriate settings according to the requirement and click Done to add settings to target machines without replacing existing settings.

4. Select the machine ID’s you want to apply the settings to and click Copy.
2.4.2 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 KServer to the next.

To Export Machine ID Settings

1. Click the select machine ID link. A machine selection pop up window displays.
2. Optionally filter the display of the machine IDs listed using the machine ID / group ID filter. Click a machine ID link to export. The machine ID you selected now displays on the Import / Export page.
3. Click Export. The page displays an XML statement of the agent settings being exported.

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

- Click Choose File and 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 KServer.
- Click Import. A set of additional options displays.
- Accept or specify the name of the machine ID. A new one is created if this name doesn’t already exist in the KServer.
- Accept or select a different group ID.
- Optionally check the box next to Replace existing data if this machine ID already exists.
- Optionally change the email notification address for all alerts defined for this machine ID account.
- Click Finish to complete the import.

2.4.3 Suspend

The Suspend page (Fig. 2.41) suspends all agent operations, such as agent procedures, monitoring, 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.

1. **Suspend**: Click Suspend to suspend agent operations on selected machine IDs.

2. **Resume**: Click Resume to resume agent operations on selected machine IDs.

3. **Machine.Group ID**: The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

4. **Suspended**: Displays Suspended if the machine ID is suspended.

### 2.4.4 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.

#### Hiding the Agent Icon on the User’s Machine

To hide the agent icon on the user’s machine, do the following:

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

All the other checkbox settings will be dimmed to indicate 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 becomes invisible to VSA users and can no longer receive commands from the KServer.

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.
The Agent Menu page is shown in Fig. 2.42 and the options available for this module are:

1. 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>** - It is the text appended to the label for the About option on the agent menu. Check to enable the machine user to click this option to display the About box for the installed agent. For example, if the About title is Agent then the label of the About option displays as Agent.

   • **<Contact Administrator>** - Check to enable the machine user to click this option to display either the user’s **Portal Access** page or a different contact URL. Portal Access is a Live Connect session initiated by the machine user. The machine user displays the Portal Access page by clicking the agent icon on the system tray of a managed machine. Portal Access contains machine user options such as changing the user’s contact information, creating or tracking trouble tickets, chatting with VSA users or remote controlling their own machine from another machine. Portal Access logons are defined using Agent > Portal Access. The function list the user sees during a Portal Access session is determined by the System > Machine Roles page. You can customize Portal Access sessions using the System > Customize: Live Connect page. The default option label Contact Administrator can be customized. The text displayed on the agent menu for contacting a VSA user.
     
     **Example:** Contact John Doe

   • **Custom Title** - The text displayed on the agent menu for contacting a custom URL.
     
     **Example:** Florida International University

   • **<Your Company 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 change the KServer address the agent checks into.

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

3. **Machine.Group ID**: The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

4. **ACOβSRx**: This column summarizes the agent menu options enabled for a machine ID. ACOβSRx 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 = About Agent  
   C = Contact 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 = Disable Remote Control  
   S = Set Account  
   R = Refresh  
   x = Exit

5. **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.

6. **Custom URL**: The URL to display when this agent menu option is selected by the user.

### 2.4.5 Check-In Control

The Check-In Control page specifies when and where each agent should check in with a KServer. Changes made using this page take effect at the next agent check-in and display in red text until then. You can specify the primary and secondary KServer names/IP addresses used by the agent to check in, the bandwidth consumed by an agent to perform tasks and the check-in period.

**Note**: The primary and secondary KServer 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 KServer service. Check-in Control information can also be maintained using the Agent Settings tab of the Live Connect and Machine Summary pages.

#### Migrating Agents from one KServer to Another

You may decide for performance or logistical reasons to migrate managed machines to a new KServer. This can be done at any time, whether or not the agents are currently checking in.

1. At the original KServer, set the Primary KServer setting to point to the new KServer address.
2. At the original KServer, point the Secondary KServer setting to the original KServer.
3. At the new KServer, set both the Primary and Secondary KServer to point to the new KServer.
4. Wait for all the agents to successfully check into the new KServer. At that time, the original KServer can be taken off-line.

#### Changing the Port used by Agents to Check into the KServer

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.
The Check-In control page is shown in Fig. 2.43. The list of all the available functions supported by this module are:

**Fig. 2.43: Checkin control**

Portions of this page are labeled in the figure. A brief description for each label is provided below.

1. **Primary KServer**: Enter the IP address or fully qualified host name of the machine ID’s primary KServer. This setting is displayed in the *Primary KServer* column. Kaseya agents initiate all communication with the KServer. For this reason the agents must always be able to reach the domain name or IP (Internet Protocol) address assigned to the KServer. 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.

   *Note: Although a public IP address may be used, Kaseya recommends using a domain name server (DNS) name for the KServer. 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.*

2. **Primary Port**: Enter the port number of either the primary KServer 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.*

3. **Secondary KServer**: Enter the IP address or fully qualified host name of the machine ID’s secondary KServer. This setting is displayed in the *Secondary KServer* column.

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

5. **Check-In Period**: Enter the time interval for an agent to wait before performing a quick check-in with the KServer. 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*.

   *Note: The agent maintains a persistent connection to the KServer. 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.*
6. **Bandwidth Throttle**: Bandwidth Throttle limits 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.

7. **Warn if multiple agents use same account**: The KServer can detect if more than one agent is connecting to the KServer 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 KServer as a user.

8. **Warn if agent on same LAN as KServer connects through gateway**: If you are managing machines that share the same LAN as your KServer then you may get this alert. By default all agents connect back to the KServer 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 KServer. Some routers do a poor job of routing internal traffic back through themselves. Check this box to receive a notification when the KServer detects an agent may be on the same LAN but connecting through the router.

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

10. **Bind to Kserver**: If checked, the agent is bound to a unique KServer ID. Bound agents cannot check-in successfully unless the unique Kserver ID they are bound to using the Agent > Check-in Control page matches the unique ID assigned to the KServer using the System > Configure page. 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.

11. **Machine.Group ID**: The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

### 2.4.6 Working Directory

The **Working Directory** page sets the path to a directory 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.

**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.

You can provide this directory in security programs, such as virus checkers, to allow operations such as Remote Control from being blocked. The general view of the Working directory page is shown in Fig. 2.44 on the next page and the options supported by this module are:
Portions of this page are labeled in the figure. A brief description for each label is provided below.

1. **Set**: Click Set to set selected machine IDs use the working directory previously entered.

2. **Set a path to a directory used by the agent to store working files**: Enter the path of the working directory used by the agent on the managed machine.

3. **Set as System Default**: Click Set as System Default to set a system-wide default for the agent working directory. This option only displays for master role users.

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

5. **Working Path**: The path of the working directory assigned to this machine ID. On a Mac OS X system, if the path name contains a space, then it must be preceded with a backslash. For example: `/tmp/name\ with\ three\ spaces`

### 2.4.7 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.
- VSA users and machine users can both maintain contact information using the **Change Profile** tab in the Live Connect or Portal Access window.
- VSA users only can maintain notes and contact information using the **Agent Settings** tab of the Live Connect 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.

Fig. 2.45 below shows the general view of the Edit Profile page and the options available for this module are:
1. **Notes**: Notes about a machine ID account can be entered in this field. Helpful information can include the machine’s location, the type of machine, the company, or any other identifying information about the managed machine.

2. **Show notes as tooltip**: If checked, *Edit Profile* notes are included as part of the tooltip that displays whenever the cursor hovers over a machine ID’s check-in status icon.

3. **Auto assign tickets**: Auto assign a ticket to this machine ID if the *Ticketing > Email reader* receives an email from the same email address as the contact email. Applies when new emails come into the ticketing email reader that do not map into any of the email mappings.

   *Note: If multiple machine IDs have the same contact email, then only one machine ID can have this checkbox checked.*

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

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

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

7. **Admin Email**: Enter the email address of the individual responsible for administering support to the managed machine. This can be the machine user, but is often someone who is part of the IT staff of the company that owns the managed machine. This setting is displayed in the *Admin Email* column.

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

9. **Machine Role**: The machine role to apply to selected machine IDs. Machine roles determine the Portal Access functions available to the machine user.

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

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

2.4.8 Portal Access

A Live Connect session run by a machine user is called Portal Access. The Portal Access page defines the logon name and password, by machine ID, required to use Live Connect as a machine user remotely.

Accessing Portal Access Locally

Machine users do not have to logon to Portal Access locally. Clicking the agent icon in the system tray of their machine initiates the Portal Access session without having to logon.

Accessing the Portal Access Logon Page Remotely

A machine user can display the Portal Access logon page for their own machine from another machine as follows:

1. Browse to the http://your_KServer_address/access/ page, substituting the appropriate target KServer name for your_KServer_address in the URL text.

2. Logon by entering the user name and password assigned to the machine ID. The user name and password is specified using the Agent > Portal Access page.

The Portal Access page displays. The machine user can click any menu option as though he or she were logged in from their own managed machine. The machine user can click the desktop or file transfer menu options to initiate a remote connection to their own machine, create or view ticket, or initiate a chat, if these options are enabled by machine role.

Re-Enabling User Logons

Machine user logons follow the same System > Logon Policy as VSA user logons. If a user attempts to logon too many times with the wrong password their account will automatically be disabled. You can re-enable the logon by setting a new password or waiting for the disable account time to lapse.

The options available in Portal Access page are shown in Fig. 2.46 and listed below:

Fig. 2.46: Portal Access

1. **Logon Name**: Enter the Logon Name the user must use to log into VSA to initiate chat sessions, enter or view tickets and/or get remote access to their machine. Logon names and passwords are
case sensitive. Passwords must be at least six characters long. The Logon Name defaults to the machineID.groupID name.

2. **Create Password, Confirm Password**: Define a password for the machine user logon. Passwords must be at least 6 characters long. The machine user can change the password after VSA user assigns one.

3. **Apply**: Click Apply to apply the Portal Access logon name and password to the selected machine ID.

4. **Clear**: Permanently remove the Portal Access logon credential from the selected machine ID.

5. **Machine.Group ID**: The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

6. **Logon Name**: The Portal Access logon name assigned to this machine ID.

7. **User Web Logon**: Displays Enabled if a Portal Access logon name and password has been assigned to this machine ID. Indicates that a machine user can log into the Portal Access page for their own machine remotely using a web browser on any other machine.

### 2.5 Upgrade version

#### 2.4.9 Set Credential

The Set Credential page registers the credential required 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 a credential. Credentials are specifically required or referenced by the following:

- **Patch Management** - If a credential is defined for a machine ID, then Patch Management installs all new patches using this credential. Therefore, Set Credential should always be a user with administrator rights.
- **Patch Status** - Patch Status resets test results every time a machine ID’s Set Credential changes.
- **File Source** - File Source may require a set credential be defined for the machine ID acting as the file share.
- **Patch Alert** - Set up an alert to notify you if a machine ID’s credential is missing or invalid.
- **Office Source** - The agent must have a credential to access the alternate Office source location, in case a patch is being installed when no user is logged into the machine.
- **If-Then-Else** - The Use Credential command in the agent procedure editor requires a credential be defined in Set Credential to run successfully.
- **Image Location** - If a UNC path is specified in Image Location, a credential must be defined using Set Credential that provides access to this UNC path. Without the credential, the machine will not have access to the image location and the backup will fail.
- **View Definitions** - Includes a Machines with Credential status option that allows you to filter the display of machine IDs on any agent page by their credential status.
- **Desktop Policy and Migration** - Installing the client for this module requires a credential be defined.
Blank Passwords

Blank passwords can be used if the managed machine’s Local Security Policy allows blank passwords. On the managed machine, open the Local Security Policy tool in Administrative Tools. Navigate to Local Policies - Security Options. Look for a policy named *Accounts: Limit local account use of blank passwords to console logon only*. The default setting is enabled. Change it to disabled and a credential with a blank password will work. Fig. 2.47 below shows the generic view of the Set Credential page. The options supported by this module are listed on the next page:

![Fig 2.47: Set credential page](image)

1. **Username**: Enter the username for the credential. Typically this is a user account.

2. **Password**: Enter the password associated with the username above.

3. **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.

4. **Apply**: Assign the credential to all checked machine IDs. Machine IDs with assigned credentials display the username and domain in the associated table columns.

5. **Clear**: Remove the credential from all checked machine IDs.

6. **Test**: Click **Test** to verify whether a username/password/domain credential will work before assigning it to a machine ID.

7. **Cancel**: Click **Cancel** to cancel the testing of a username/password/domain credential.
2.5 Upgrade version

2.5.1 Update Agent

The Update Agent page (Fig. 2.48) schedules managed machines to be updated with the latest version of the agent software at the agent’s next check-in. Updating the agent software makes no changes to the agent settings you have defined for each agent.

1. **Update Agent**: Click *Update Agent* to schedule selected machines to be updated.

2. **Remind me at logon when agents need an update**: If checked, a popup window displays when VSA users logon if managed machines under their control need to be updated with the latest version of the agent software. The reminder only displays if at least one agent within VSA user’s scope requires updating. Users can disable this feature at logon time and can re-activate it by selecting this checkbox.

3. **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.

4. **After update run agent procedure <select agent procedure>**: Select an agent procedure to run immediately after an agent update completes. This capability 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.

5. **Cancel Update**: Click *Cancel Update* to cancel a pending update on selected managed machines.

6. **Machine.Group ID**: The list of machine.group IDs displayed is based on the machine ID / group ID filter and the machine groups the user is authorized to view.

7. **Agent Version**: The version of the agent software running on the managed machine. Version numbers in red indicate that the version on the agent machine is not the same as the latest version available.
8. **Update Agent Procedure**: The agent procedure assigned to run when the agent is updated.

9. **Last Update**: The date the agent was last updated on the managed machine. Since the server must wait for the managed machine to check-in, according to the check-in schedule as specified in **Agent > Check-In Control**, Pending displays in the **Last Update** column until the next check-in occurs.

## 2.6 Protection

### 2.6.1 File Access

The File Access page (Fig 2.49) 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.

![File Access Page](image.png)

**Fig 2.49: File Access**

1. **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.
- **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.

2. **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.

3. **Machine.Group ID:** The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

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

5. **Approved Apps:** Lists applications approved to access the files on the machine ID.

6. **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.

### 2.6.2 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.

**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.

The functions of the Network Access page is listed in Fig 2.50

1. **Notify user when app blocked:** Click Enable to 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.

Once this option is enabled, one of the following options must be chosen:

- 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.

2. Enable/Disable driver at next reboot: 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 cannot monitor network statistics or block network access if this driver is disabled.

Driver

This driver function needs to 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.

To determine which applications should be approved or denied network access, use the Network Statistics* report to view network bandwidth utilization versus time. It helps you analyze and identify peak bandwidth consumers by clicking the graph’s data points.

Note: Network Statistics will be covered in the Info center chapter later on. Info Center > Reports > Logs > Network Statistics Log

3. 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.

4. Machine.Group ID: The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

5. 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:
• Select machine IDs.
• Click the Enable button for Notify user when app is blocked.

To remove this notification:
• Select machine IDs that display a green checkmark in the Notify column.
• Click the Disable button for Notify user when app is blocked.

6. Enable Driver: Identifies on a per machine ID basis, which machines have the network protection driver enabled or not.

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

8. Approved Apps / Denies Apps
• 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.

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 as shown in Fig 2.51

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.

2. Since the list in the Application List (Fig 2.52) window may be large, you can control the applications displayed by clicking Filter to filter the list.
3. Check the checkboxes next to the application name you wish to approve or deny network access to.
4. You can also enter application names in the Add applications not found by audit here edit field, to identify applications not listed.
5. 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.

6. Click Approve Apps or Deny Apps (Fig 2.53). 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

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

### 2.6.3 Application Blocker

The Application Blocker (Fig 2.54) page prevents any application from running on a machine ID. Blocked applications cannot be renamed, moved, or deleted from the system.

#### 1. 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 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.

2. 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.
3. Click one or more blocked applications.
4. Click the Unblock button. The window closes.
5. The blocked application no longer displays in the Application column beside the selected machine IDs.

3. Machine.Group ID: The list of Machine,Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

4. Application: Filename of the application being blocked.

Note: If multiple agents are installed on a machine, only one agent at a time controls the drivers required to use File Access, Network Access, Application Blocker. These functions can only be performed by the agent controlling these drivers.