Kaseya® Automating IT

Agent Configuration and Deployment

User Guide

Kaseya 2008 SP1

September 30, 2008

About Kaseya

Kaseya is a global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

Contents

VSA Foundation Concepts

One of the unique features of the VSA is the ability to work with multiple machines or individual machines—across domains, clients, locations or any structure defined. This greatly increases the ability to create and use "best practices", increase flexibility and greatly decrease the amount of time it takes to complete tasks. Your understanding of the foundation concepts discussed below will greatly streamline your successful deployment and management of machines using the VSA.

Details for the topics discussed in this document can be found in the online user assistance system. User assistance is context sensitive. Please refer to it from within the VSA application.

Review the following VSA foundation concepts before configuring agents for the first time.

Agents

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

- A K icon displays in the icon tray of the remote machine. This can be a custom image or removed altogether.
- Each installed agent is assigned a unique VSA machine ID / group ID. Machine IDs can be created automatically at agent install time or individually prior to agent installation.
- Each installed agent uses up one of the available licenses purchased by the service provider.
- Agents are typically installed using packages created using Agent > Deploy Agents inside the VSA.

Machine IDs vs Agents

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

> Note: Machine ID templates are discussed in Configuring Agent Settings *(page 6)*.

Machine ID/Group ID

Each agent installed on a managed machine is assigned a unique machine ID/group ID name. All machine IDs are associated with a group ID and optionally a subgroup ID. Typically a group ID represents a single customer account. Subgroup IDs typically represent a location or network within a

group ID. For example, the full identifier for an agent installed on a managed machine could be defined as `jsmith.acme.chicago`. In this case `chicago` is a subgroup ID defined within the group ID called `acme`. Only a master administrator, or administrators authorized by a master administrator, can create group IDs. Any administrator can create subgroup IDs. Group IDs and subgroup IDs are created using the System > Machine Groups > Create/Delete page.

Group and Sub-Group Example 1:

Groups:
- Sales
- Marketing
- Accounting
- Production
- IT
- Administration

Sub-Groups:
- Servers
- Desktops
- Notebooks
- Power Users
- Standard Users
- Mobile Users

Group and Sub-Group Example 2:

Groups:
- Client 1
- Client 2
- Client 3
- Client 4

Sub-Groups:
- Sales
- Marketing
- Administration
- Accounting

Machine ID / Group ID Filter

The Machine ID / Group ID filter is available on all tabs and functions. It allows you to limit the machines displayed on *all* function pages. Once filter parameters are specified, click the green arrow icon to apply filter settings to *all* function pages. By default, the Machine ID / Group ID filter displays all machine IDs in `<All Groups>` managed by the currently logged in administrator.
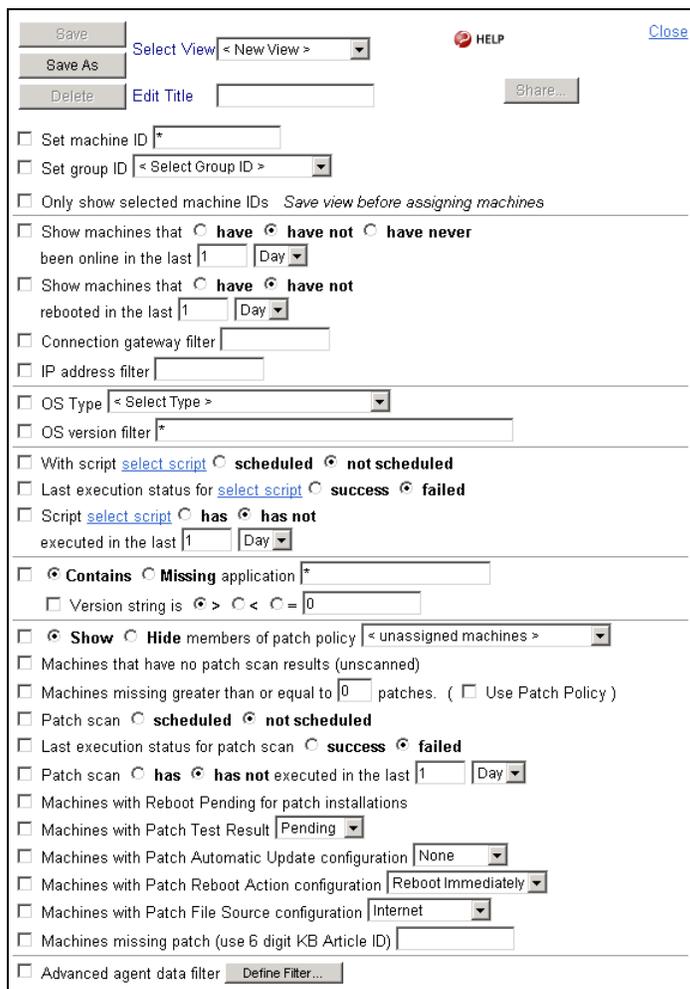
> Note: Even if an administrator selects `<All Groups>`, only groups the administrator is granted access to using System > Group Access are displayed.

Views

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

Only Show Selected Machine IDs

You can select a free-form set of *individual machine IDs within a view*. It doesn't matter which groups the machine IDs belong to, so long as the administrator is authorized to have access to those groups. This enables the administrator to view and report on logical sets of related machine IDs, such as laptops, workstations, servers, MS Exchange Servers, etc. Machines are selected within a view using the Only show selected machine IDs checkbox in View Definitions. Save a view first before selecting machines IDs using this option. Once the view is saved, a <N> machines selected link displays to the right of this option. Click this link to display a window which allows you to create a view using a free-form selection of individual machine IDs.

Configuring Agent Settings

Agent Settings

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

To provide both flexibility and automation, the VSA enables you to specify different values for the following types of agent settings on a per machine basis:

- Credential
- Agent Menu
- Check-in Control
- Temp Directory
- Logs
- User Profile - Refers to settings in Audit > Edit Profile or Ticketing > User Profiles.
- View Collections
- User Access
- Remote Control Policy
- Patch Settings
- Patch File Source
- Patch Policy Memberships
- Fixed Alerts - These all the alert types on the Monitor > Alerts page except for Event Log alerts and System alerts.
- Event Log Alerts
- Monitor Sets
- Distribute Files
- Protection
- Script Schedules

Once these settings are configured the way you want them for a single managed machine, you can create a new install package. The new package will install the same set of agent settings on any managed machine.

Machine ID Templates

Using *all* the agent settings appropriate for a working machine poses some drawbacks. For example, the credential and patch file source for a working machine *will not work* on a newly managed machine if that machine belongs to another customer.

The solution is to use machine ID templates to configure agent settings. A machine ID template is *a*

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

- Create machine ID templates using Agent > Create.
- Import a machine ID template using Agent > Import/Export. Sample templates can be downloaded from the Kaseya Support Forum and imported.
- Base an agent install package on machine ID template using Agent > Deploy Agents.
- Copy *selected* settings from machine ID templates to existing machine ID accounts using Agent > Copy Settings.
- Identify the total number of machine ID template accounts in your VSA using System > Statistics.
- Configure settings for the machine ID template using the standard VSA functions, just as you would a machine ID account with an agent.

To apply a machine ID template to a package:

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

Copying Agent Settings

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

Templates and Filtered Views

There is a corresponding relationship between machine ID templates and filtering your view of selected machines using the Only show selected machine IDs option. (This option was described earlier in VSA Foundation Concepts *(page 3)*.) For example, if you define a machine ID template called "laptops", then it's easier to apply settings to all the "laptops" you're responsible for if you have a filtered view called "laptops". Simply select the view for "laptops" and only laptops are displayed on any function page, regardless of the machine group they belong to. The same idea applies to "desktops", "workstations", Exchange servers", etc.

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

Base Templates and Audits

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

Creating Agent Install Packages

Agent Install Packages

Rapid deployment is an important feature of the VSA. Getting the system up and running as quickly as possible helps the IT group get machines under management immediately and allows for the implementation of best practices. One aspect of rapid deployment is the ability to deploy agents that are totally configured using agent install packages.

Agent install packages are created using two functions within the VSA:

- Deploy Agents - Creates and distributes an agent install package to *multiple* machines. This is the preferred method for creating agent install packages and discussed in detail in this document.
- Create - Creates a machine ID account and agent install package in two separate steps. The install package is applied to a *single* machine. You can also use Create to create machine ID templates or re-install a missing agent for an *existing* machine ID.

Deploy Agents

The Deploy Agents install package is created using a Create Package wizard. The wizard copies agent settings from an *existing* machine ID or machine ID template and generates an install package that is always named KcsSetup.exe. All agent settings and pending scripts from the machine ID you copy from—except the machine ID and group ID—are applied to every agent installed using this package.
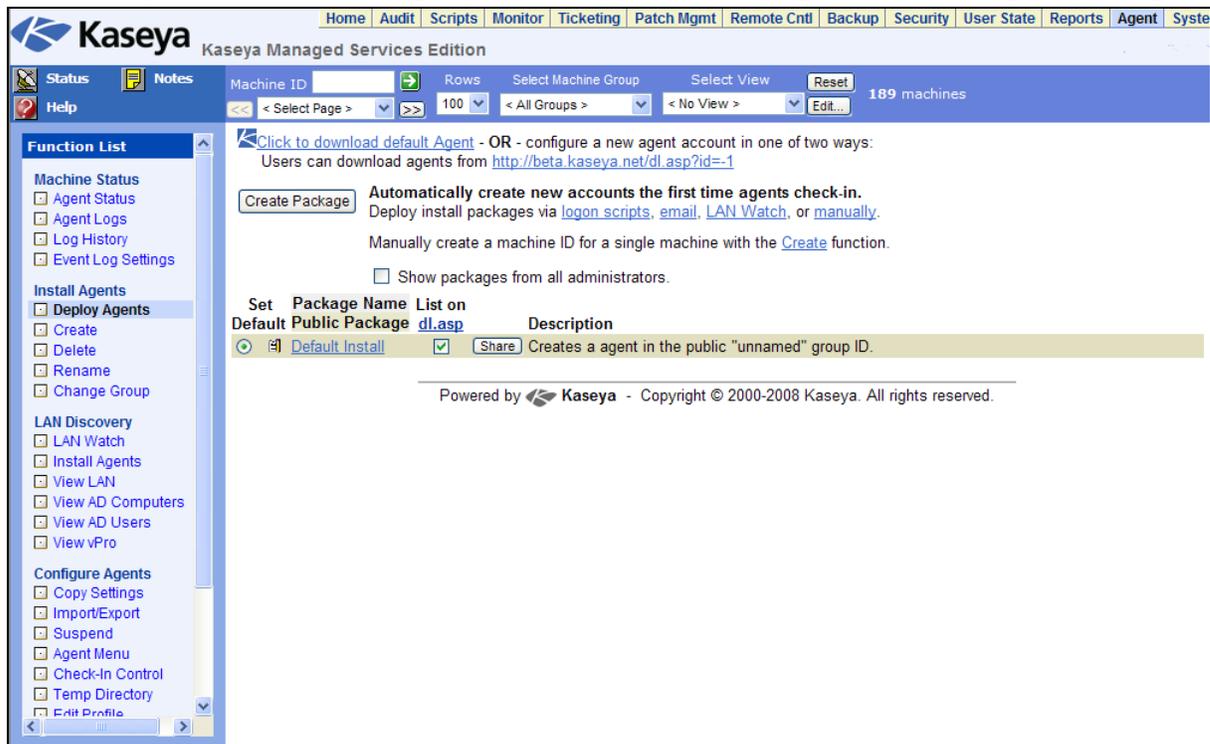
When you click the Create Package button a 7-step wizard lets you make choices about how that package should be created.

1. Define rules for naming the machine ID.
   - ➢ Prompt the user to enter a machine ID.
   - ➢ Use the computer name as the machine ID.
   - ➢ Specify the machine ID for this install package.
   - ➢ Set the user name of the currently logged on user as the machine ID.

2. Define rules for naming the group ID.
   - ➢ Prompt User - Asks user to enter a group ID. This option is only displayed to master administrators.
   - ➢ Domain Name - Uses the user's domain name.
   - ➢ Existing Group - Select an existing group ID from a drop down list.

> ➢ New Group - Specify a new group ID. This option is only displayed to master administrators.

3. Specify agent install package command line switches including the ability to install silently without any task bars or dialog boxes. These command line switches are described in the user guide and online help.

4. Specify the machine ID to copy settings and pending scripts from. All settings and pending scripts from the machine ID you copy from—except the machine ID and group ID—are applied to every agent installed using this package.

> Best Practices: Use a machine ID template as the source of your agent settings.

5. Select the operating system you are creating the install package for: `Windows` or `Macintosh`.

6. Optionally bind an administrator logon credential to the install package. Fill in the Administrator Credential form to securely bind administrator 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.

> 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.

Note: The filename of the agent install package is always `KcsSetup.exe`.

Name the install package.   Close

[<< Back] [Save]

(5) Select agent type. [Windows ▾]

(6) ☐ Securely bind administrator credentials to the install package?

Administrator Credential

Username:	[ ]
Password:	[ ]
Confirm:	[ ]
Domain:	[ ]

Successful installation may require Administrator rights. Fill in the administrator credential form to securely bind administrator rights to the install package. Users with minimal rights can then install the Agent. If the administrator credential is left blank and the user does not have rights to install software, the installer prompts for an administrator credential.

(7) **Name the install package.** Give this package a name and short description so you will remember this configuration when you use it.

Package Name

[   ]

Package description

[   ]

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 a group ID and sub-group ID. A group ID usually represents a single customer. A sub-group ID is sometimes used to represent a specific customer location.
- Assigning a credential, if necessary.

Once edited the install package can be re-created and distributed to the specific customer and location it is intended for.

Distributing Agent Install Packages

Download Methods Using Deploy Agent

The Deploy Agent page provides three types of links for downloading agent install packages:

- The administrator's *default* agent install package - Each administrator has his or her own default agent install package.
- A *selected* agent install package - First, select any package listed in the Deploy Agent page. Secondly, click this link to download this selected package using a unique index number assigned to the package.
- A `dl.asp` web page listing *all publicly available* agent install packages - Click any package listed on the `dl.asp` web page to download it.

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

Executing the Install Package

The downloaded `KcsSetup.exe` can be executed using any of the following three methods:

- Double click `KcsSetup.exe` within Windows to launch it.
- Open a command line window and type `KcsSetup.exe` followed by any desired command line switches. These switches are described in the user guide or online user assistance.
- Select Run... from the Windows Start menu and type `KcsSetup.exe` followed by any desired command line switches.

Distribution Methods

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

- Logon Scripts - Set up an NT logon script to run the install package every time a user logs into the network. The installer skips installation if it detects an agent is already on a machine.
    1. Create the deployment package using the Agent > Deploy Agents wizard.
    ✓ You will probably want to select the silent install option.
    ✓ It may be necessary to bind an administrator credential if users running the logon script don't have administrator rights.
    2. Download the `KcsSetup.exe` and copy it to a network share which users can execute programs from.
    3. Add `KcsSetup.exe` with its network path to the logon script.
- Email - Email `KcsSetup.exe` to all users on the network. Download the `KcsSetup.exe`, then attach it to an email on your local machine. You can also copy and paste the link of a `dl.asp` install package into an email message.

- LAN Watch - Administrators can discover newly added machines during a LAN Watch and subsequently install agents *remotely* using the Agent > Install Agents page. If a LAN Watch is performed using an Active Directory machine, you can also install agents to Active Directory computers using View AD Computers. Agents can also be automatically installed on each machine an Active Directory user logs onto using View AD Users.
- Manually - You can instruct users to download an install package agent from the `http://your.Kserver.com/dl.asp` website to their target machines. If more than one install package is displayed on the website, instruct them which package should be selected.

Automatic Account Creation

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

Assigning New Machine IDs to Machine Group by IP Address

You may choose to create a "generic" install package that adds all new machine accounts to the `unnamed` group ID. When the agent checks in the first time, the System > Naming Policy assigns it to the correct group ID and/or sub-group ID using the IP address of the managed machine.

Configuring Agents on an Internal LAN

If machines on an internal LAN cannot be routed to the VSA using the external host name or IP address:

1. Create an agent installation package that copies settings from an existing machine account which has its primary and secondary KServer address set to the server's *internal* IP address. The primary and secondary Kserver addresses are displayed using the Check-In Control function underneath the Agent tab.
2. If a machine account with this setting does not exist, then create a new machine ID template, with a name such as *default-internal.unnamed*, using the Agent > Create page.
3. Set the new account's primary and secondary KServer addresses to the KServer's internal IP address using the Check-In Control page.
4. Use Deploy Agents to create an installation package based on this machine ID. The installation package can then be deployed to managed machines on the internal LAN.

Agent Function List

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

Functions	Description
Agent Status	Displays active user accounts, IP addresses and last check-in times.
Agent Logs	Displays logs of: • Agent system and error messages • Execution of scripts, whether successful or failed. • Configuration changes made by an administrator. • Send/receive data for applications that access the network. • Application, System, and Security NT Event Log data collected from managed machine.
Log History	Specifies how long to store log data.
Event Log Settings	Specifies the event log types and categories included in the Log History.
Deploy Agents	Creates agent install packages for multiple machines.
Create	Creates machine accounts and/or install packages for single machines.
Delete	Allows administrators to delete machine accounts.
Rename	Renames existing machine ID accounts.
Change Group	Reassigns any number of machines to a new group ID.
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.
Install Agents	Installs the agent *on a remote system* and creates a new machine ID / group ID account for any new PC detected by LAN Watch.
View LAN	Displays the results of the latest LAN Watch scan.
View AD Computers	Lists all computers listed in an Active Directory when LAN Watch runs on a system hosting Active Directory. Installs agents on AD machines.
View AD Users	Lists all Active Directory users discovered by LAN Watch when LAN Watch runs on a system hosting Active Directory. Creates VSA administrators and users from AD users.

View vPro	Displays hardware information about vPro-enabled machines discovered while running LAN Watch.
Copy Settings	Mass copies settings from one machine account to other machine accounts.
Import / Export	Imports and exports agent settings, including script schedules, as XML files.
Suspend	Suspends all agent operations, such as scripts, monitoring, and patching, without changing the agent's settings.
Agent Menu	Customizes the agent menu on managed machines.
Check-In Control	Controls agent check-in frequency on agent machines.
Temp Directory	Sets the path to a directory used by the agent to store temporary files.
Edit Profile	Edits machine account information.
User Access	Sets up accounts to allow users remote control access to their own machines.
Set Credential	Sets a logon credential for the agent to use in Patch Management, the Use Credential script command, backups, and User State Management.
Update Agent	Updates the agent software on managed machines.

Summary

The following agent configuration and deployment summary incorporates "best practices" recommendations discussed throughout this document.

Planning

After reviewing this document and before you deploy agents, a plan should be created that identifies how the machines will be managed on a daily, weekly and monthly basis. This helps determine how they should be grouped. Although it is very easy to reassign a machine to a group or sub group, planning will help with a rapid and smoother deployment. In addition, administrator security can be defined to restrict group access.

- Users
  - ➢ Identify administrators and end users.
  - ➢ What access do they need?
- Group and Sub-Groups
  - ➢ What named grouping is needed? By department, location, client, location, user type, etc.
- Reporting
  - ➢ What is the granularity by group, sub-group, and view?
  - ➢ Who gets the reports? Who are the internal and external recipients?

Machine ID Templates and Filtered Views

- Identify the different types of machines you'll be required to support.
- Create additional machine ID templates, one for each type of machine you have identified.
- Create corresponding filtered views for each type of machine.
- Create a "base" machine ID template with most of the agent settings turned off.

Agent Configuration

Define and create agent settings, as appropriate, for each machine ID template you have defined. You don't have to have all these settings defined initially. You can update a template, then copy the template's settings to working agents repeatedly using the Copy Settings function. Be sure to select "Do Not Copy" for any agent settings you do not want to overwrite.

Package Creation

Use the package wizard in Agent > Deploy Agent to create the agent package to install. Use a machine ID template as the source of agent settings for the package.

Consider installing an agent based on a "base" template with most of the agent settings *turned off*. Once the package is installed on a new machine, review the audit for a newly managed machine first, then apply settings from the appropriate template to the new agent as appropriate using the Copy Settings function.

Consider *automating* the assignment of managed machines to groups and subgroups using the System > Naming Policy function.

Deployment

Identify locations, types of users, and machine availability. These factors determine the need for one or more methods of deployment. A domain login script is the quickest. However, not all environments use domains. LAN Watch only works with NT and higher. If you have a domain and are using Active Directory, consider using Active Directory to identify machines that should have agents installed. Remember installs can be silent and require no user interaction or reboot.

Agent Reconfiguration

When you need to reconfigure agents, make your changes to the appropriate machine ID templates first. This ensures your machine ID templates remain the "master repositories" of all your agent settings. Then filter your view of all the machines you're responsible for, by selecting a view of selected machines that corresponds to the template you have modified. Use Copy Settings to copy settings from your modified template to *all* the machines in your *filtered view*. Be sure to select "Do Not Copy" for any agent settings you do not want to overwrite.