Virtual System Administrator 4.7.0.0

HELP System Documentation

Help for Kaseya Virtual System Administrator
Version 4.7.0.0

Kaseya
185 Berry Street, Suite 5050
San Francisco, CA 94107
Ph: (415) 694-5700 x103
www.kaseya.com

Table of Contents

Help Home

Virtual System Administrator
HELP

Download a PDF version of Help. You must have Acrobat Reader installed on your system to view the PDF file.

Read Me First

Quick Start Guide

Feature Tabs

Audit
Monitor
Remote Cntl
Agent
Scripts
Ticketing
Reports
System

General Information

Browser Settings
Deploy Agents
Using Scripts
Technical Support
Logging on...
Single-User Interface
Agent Icon
Console Features
Specifying Accounts
IF-THEN-ELSE Script Definitions
Toolbox
Logging off...
Administrator Notes Database
Status Monitor

Welcome!

Online Help can be used to assist you in becoming familiar with the various functions of the system, or to refresh expert users on various commands and features. Before logging in, Internet Explorer should be able to accept cookies and JavaScript enabled.

Some things to keep in mind as you navigate Online Help:

- Selecting a feature tab from the table above shows you all of its available functions.
- Selecting one of the functions displays in-depth information about that function.
- Clicking HELP while using the system displays a context-sensitive help on the currently selected function..
- After logging in, you will be reminded if there are any Agents under your control that are out of date and need to be updated. You can disable this feature by selecting the appropriate checkbox in the reminder window.

To return to this page, click HELP HOME from any Assistant page. Selecting the Show me link in a Assistant page opens up a popup window without transporting you to a new page. Click on the popup window to clear it and return to the Assistant page you are currently viewing.

Since Online Help is viewed using Internet Explorer, the navigation shortcuts you already know can be used:

Alt + **Back Arrow** (or **Backspace**) = Back one page
Alt + **Forward Arrow** = Forward one page
F5 = Refresh the browser window

Minimum System Requirements	Defines minimum system requirements for both client and servers components.
Configure Server	Check list used to verify your server is set up and configured correctly.
Deploy Agents	Shows you the easiest and quickest ways to deploy agents and start managing PCs in minutes. Click here to download and install the default Agent.
Asset Inventory & Audit	Maintain accurate list of hardware and software installed on each managed machine. Alert sent when audit detects any change.
Remote Control	View, operate, and send files to managed machines as if they were right in front of you. Reach managed machines through firewalls or behind NAT gateways without opening new ports.
Patch Management & Software Install	Deploy software updates and new software installations to an entire organization with a single click. Monitor each managed machine and alerts you when a new OS patch is available.
System Monitoring	Monitoring provides instant notification of system problems and changes. Monitors NT event logs, system resources, and configuration changes.
Trouble Ticketing	Both users and administrators can access the integrated trouble ticketing system.
Browser Settings	Defines requires browser settings to operate the system.
Technical Support	How to contact technical support for assistance.
Help Home	Open the online help system.

Configure Server

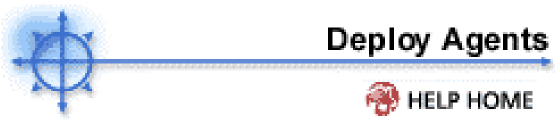
The server is the heart of the system. Administrators access all functions through this server's web interface. The agents, on all managed machines, connect to this server to get any instructions/tasking orders.

Your server must be accessible to both administrators and agents.

Administrators and agents need to be able to connect back to the server from anywhere on the internet. Verify your server meets the following requirements:

1. **Public server name/IP address** - Define a public IP address for your server. If your server is behind a gateway on a private network, your VSA may be using the private IP address. Long term it is better to use a name instead of an IP address. Using a name lets you change the IP address without having to re-configure any agents. Set the name/IP address of the VSA in the Server Info function under the System tab.
2. **Open required ports at the firewall** - Administrators access the VSA through the web interface (typically port **80**). Agents connect to the server on a separate port (default port **5721**). Both these port must be opened at your firewall for TCP/IP traffic. The agent port (5721) must be open for both inbound and outbound.
3. **Verify localhost access for the web server** - Several VSA services depend on localhost access. Typically localhost access can be enabled by:
   - Open the IIS Enterprise Manager
   - Right click the Default Web Site and select Properties
   - Click the Web Site tab
   - Verify the IP Address field is set to (All Unassigned)
4. **Specify the alert email sender address** - The VSA sends alerts via email. Emails are sent from your server using the built-in SMTP service. You can set the address these emails come from to any valid email address in the Server Info function under the System tab. The default email address is vsa@kaseya.com.

Deploy Agents



The system manages remote machines with the Agent. Each agent gets an account on the VSA. Accounts can be created automatically at agent install time or individually prior to agent installation. Deploy Agents using one of the following methods:

1. **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 a Agent is already on this machine.
2. **Email** KcsSetup.exe to all users on the network. The automatic install package can carry an Administrator credential for your network so users do not need to be logged on as an Administrator to successfully install the Agent.
3. **Download the default agent from http://your_vsa_address/dl.asp.** The default agent has all the default account settings specified by a master administrator. The first time an agent installed with this package checks in, the VSA automatically creates a new account for that machine.
4. **Manually** install KcsSetup.exe on each machine.

Automatic Install Package

These installs automatically create accounts on the VSA the first time the agent checks in. Using the Automatic Install Wizard, you can specify the machine ID naming conventions used to create new accounts. The wizard also allows you to specify a silent install and set any agent parameter.

The easiest way to deploy agents in LAN environments is to run the automatic install package via a login script. Install packages may also be emailed or otherwise sent to remote machines and executed manually.

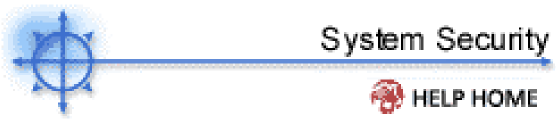
Individual Install Package

Individual install packages contain all settings for an *existing* machine account. Use Individual Install packages to install re-install agents on existing accounts or to load agents for accounts that already exist. Click the Create button under the Agent tab to download install packages for a specific account.

Minimum System Requirements

Up to date Minimum System Requirements are always available on our web site at
http://www.kaseya.com/sup1/min_requirements.phtml

System Security



We designed the system with comprehensive security throughout. Our design team brings over 50 years of experience designing secure systems for government and commercial applications. We applied this experience to uniquely combine ease of use with high security.

The platform's architecture is central to providing maximum security. The agent initiates all communications back to the server. Since the agent will **not** accept any inbound connections, it is virtually impossible for a third party application to attack the agent from the network. **The system does not need any input ports opened** on client machines. This lets the agent do its job in virtually any network configuration without introducing any susceptibility to inbound port probes or new network attacks.

The VSA protects against man-in-the-middle attacks by encrypting all communications between the agent and server with **256-bit RC4** using a key that rolls every time the server tasks the agent (typically at least once per day). Since there are no plain-text data packets passing over the network, there is nothing available for an attacker to exploit.

Administrators access the VSA through a web interface after a secure logon process. The system never sends passwords over the network and never stores them in the database. Only each administrator knows his or her password. The client side combines the password with a random challenge, issued by the VSA server for each session, and hashes it with SHA-1. The server side tests this result to grant access or not. The unique random challenge protects against a man-in-the-middle attack sniffing the network, capturing the random bits, and using them later to access the VSA.

The web site itself is protected by running the Hotfix Checker tool on the VSA server every day. The VSA sends alerts to the master administrator when new IIS patches are available. The helps you keep the VSA web server up to the latest patch level with a minimum of effort. Finally, for maximum web security, the VSA web pages fully support operating as an SSL web site.

Browser Settings

Enabling Browser Cookies and JavaScript

When connecting to the console, you will enter the default login page. Internet Explorer 5.0 or greater must have cookies and JavaScript enabled in order to proceed:

To enable cookies in Internet Explorer 5

Cookies are enabled by default in Internet Explorer. However, if cookies are turned off, you may need to enable them.

1. Click on the **Tools** menu.
2. Select **Internet Options**.
3. Switch to the **Security** tab.
4. Click on **Internet** in the **Select a Web** content zone.
5. Press the **Custom Level** button.
6. Scroll down to the **Cookies** section.
7. In *Allow cookies that are stored on your computer,* select the **Enable** radio button.
8. In *Allow per-session cookies,* select the **Enable** radio button.
9. Press **OK**.

To enable cookies in Internet Explorer 6

1. Click on the **Tools** menu.
2. Select **Internet Options**.
3. Switch to the **Privacy** tab.
4. Select a privacy setting no greater than **Medium High** (i.e. the setting must not be High nor Block All Cookies).
5. Press **OK**.

To enable JavaScript in Internet Explorer

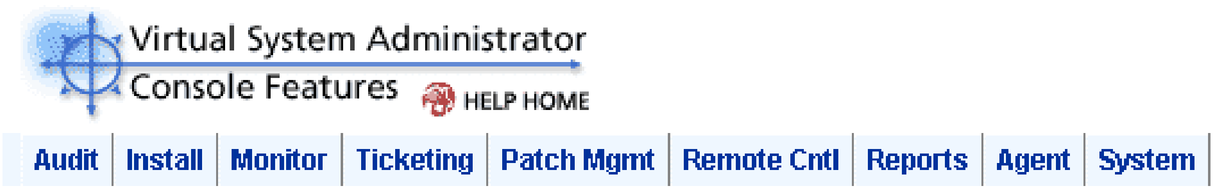
1. Click on the **Tools** menu.
2. Select **Internet Options**.
3. Switch to the **Security** tab.
4. Click on **Internet** in the **Select a Web** content zone.
5. Press the **Custom Level** button.
6. Scroll down to the **Scripting** section.
7. In *Scripting of Java applets*, enable the **Custom**, **High safety**, **Low safety**, or **Medium safety** radio button, depending on the security requirements of the machine running the .
8. Press **OK**.

Log in by:

1. Enter the administrator name and password.
2. Press login. For initial login, use the master administrator account name and password entered during installation.

Note: To prevent unauthorized access after making configuration changes, log off or close the session by terminating the browser application.

Console Features



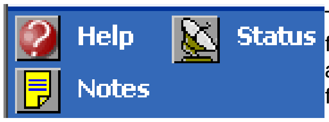
All of the features of the system can be accessed through the feature tabs located at the top of the console window. Within each feature tab are the core functions that allow administrators to perform a variety of tasks on remote client machines and the Server. Each feature tab is easily accessible by simply clicking it. Furthermore, each of the feature tabs' functions can be accessed via the left-hand navigation bar on each feature tab page.

Note: The System tab is viewable and accessible only by a master administrator.

Console Features:

- Specifying User Accounts
- Login
- Log Off
- Toolbox
- Help Home
- Single-User Interface

Toolbox



The Toolbox provides the administrator with a common area to access frequently used commands and functions. The Toolbox is accessible from any feature tab, giving administrators convenient access to frequently used features of the VSA.

Notes

Administrator Notes Database provides a place to record and retrieve what previous administrator actions were performed on each machine. Learn more...

Scripts

Brings up the script editor. Develop your own scripts to automate actions on multiple client machines. Learn more...

Status

Brings up the status monitor window. The status monitor continuously monitors selected machines, notifying you when they go online or offline. Learn more...

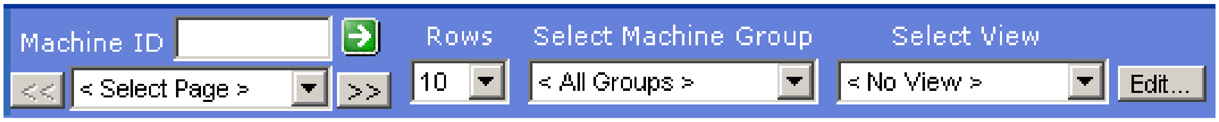
Help

Brings up the online help system you are in now.

Select Machines

The Select Machines area is available on all feature tabs and functions. It allows administrators to easily select an individual or group of client machines. Machine accounts are identified by a machine ID, which is part of a group ID.

By default, the Select Machines filter displays all machine IDs in all groups managed by the logged in administrator.



Note: Only a master administrator can create top level group IDs. Any administrator can create subgroups. Create Machine Groups with the Create/Delete function under the System tab.

Filtering a client machine list

Filtering the client machine list allows administrators to view machines under their control. Along with the **Rows** dropdown menu, administrators can control the number of client machines displayed in the list. Views let you further refine the filter based on attributes contained on each machine (like operating system type).

Machine ID

Enter the machine ID of the user account being filtered. For multiple accounts, wildcards are acceptable. For example, searching all machine IDs within a group ID can be accomplished be entering an asterisk (*) in the machine ID field.

Select Page

When more machines are selected than can be displayed on a single page (as defined by the **Rows** dropdown control), this control lets you quickly locate a machine. The << and >> buttons go to the previous and next page in the sequence. The drop down control alphabetically lists the first machine ID from each page of data. To locate any machine quickly select the page based on machine ID.

Rows

Select the number of accounts displayed on each account page.

Select Machine Group

Select the group ID to be filtered. Select "<All Groups>" to search for machine IDs across all group IDs managed by the logged in administrator.

Select View

Views let you refine the list of machines you wish to work on at one time. In addition to sorting based on machine group, views let you sort by attributes found on the machine (such as operating system type).

Once the filter parameters are specified, click green arrow button to initiate the filter. Results will be displayed in the client machine list.

Logoff

Log Off the system

Once configuration changes to user accounts have been made, click the **Log Off** link to prevent unauthorized access to the server and return to the logon page. The **Log Off** link is located in the upper right-hand corner of the window and is accessible from any feature tab and function.

For increased security, it is recommended that administrators log off and terminate all browser sessions when not administering the server.

Machine Summary Interface

Single-User Interface

HELP HOME

How do I access the single-user interface?

To access the single-user interface:

- Simply click the Agent status icon next to the client machine ID in any VSA console window:

  Agent status icons- *

*Shown only in the Remote Control function page.

Simply click the Agent status icon next to the client machine ID in any VSA console window:

Agent status icons- *

The single-user interface allows administrators to single out and perform tasks and functions solely to one client machine. At a glance, administrators can view a client machine's Agent profile, audit information, PCI hardware and disk information, scheduled scripts, script history, installed applications, and network access information. The breadth of the information shown is controlled by an administrator: they can select the information they want to view by customizing the single-user interface layout.

The following elements are displayed in the single-user interface:

Agent Profile Displays information about the Agent on the client machine. The same information is listed in the Edit Profile function of the Agent feature tab.

Audit Information IP Address, Computer Name, Subnet Mask, OS, Version and Build, Default Gateway, Connection Gateway, RAM ,MAC Address, CPU ,DHCP Server, DNS Server, and Primary and Secondary WINS Servers.

Disk Volumes Drive letter, Type, Format, Free Space, Total Size, and Labe**l**

PCI & Disk Hardware Type, Vendor, and Product name. Provides the same functionality as the PCI & Disk H/W function in the Audit feature tab.

Script Scheduler The same script scheduling interface used to schedule existing scripts.

Script History Script History, Last Execution time, and the Admin that scheduled the script.

Installed Applications Lists all the applications installed on the client machine. Provides the same functionality as the Installed Apps function in the Audit feature tab.

Network Access Provides the same functionality as the Network Access function in the Protect feature tab.

These elements can be re-ordered by pressing Layout. The Network Access function requires Installed Applications to appear directly above it. You will not be able to save the display order if Network Access is not preceded by Installed Applications.

Home Tab

The Home tab contains summary information (the dashboard) as well as links to the quick start guide. After the dashboard links, you can completely customize the all the links appearing in this list.

To access the Assistant, click Assistant from any function page.

The following functions are available in the Homefeature tab:

Functions	Description
View Dashboard	Displays system summary information at a glance.
Layout	Specify which items appear in the dashboard and the order the items appear.
Custom Links	Write files to all selected remote machines and maintain them.

Home > View Dashboard

The dashboard gives you a quick view of system health, highlighting the tasks and items you need to work on first. In addition to viewing total system status at a glance, you can **managed tasks** and send **message** to other administrators. Customize the dashboard display with the Layout function.

Alerts

Displays all alerts sent relating to all machine IDs that match the current machine ID / group ID filter. The display lists the most recent alerts first. By default, alerts generated within the **last 24 hours** are highlighted in **red**. Alerts generated within the **last week** display in **yellow**. The color coding lets you quickly distinguish alerts you may not have examined yet.

Agent Status

Summarizes the online status of all machine IDs that match the current machine ID / group ID filter. Gives you an at-a-glance count of how many machine are **online**, have **users logged into** them, have not been online for **more than 30 days**, and how many **total machines** on match the current filter.

Patch Status

Pie chart highlighting machines missing patches. The chart displays either with or without applying the Patch Approval policy. Click the **Use Policy** button to apply the Patch Approval policy when generating the pie chart. Click Hide Policy to generate the pie chart without the patch approval policy (to show all missing patches including those denied by patch approval). Clicking on any pie segment opens a sub window listing all machine IDs that make up that pie segment.

NOTE: The Patch Approval policy incurs a significant performance penalty. If you have a lot of machine IDs this pie chart takes a long time to generate when using the patch approval policy.

Operating Systems

Pie chart showing the mix of operating systems in use by the machines matching the current machine ID / group ID filter. Clicking on any pie segment opens a sub window listing all machine IDs that make up that pie segment.

Tickets

Lists recent tickets issued against the selected machine IDs.

Tasks

Place to create, edit, and monitor tasks for yourself or other administrators. Use this section to keep track of tasks you need to perform. A pop up window alerts you when new tasks are created for you have been added to your task list. Addition pop ups occur when the task becomes past due. You may elect to have the system remind you again later of a past due task, buy clicking a **snooze** button.

Messages

Place to create and monitor messages between you and other administrators. Use this section to send messages to other administrators and view messages sent to you from other administrators (you can also send yourself messages). A pop up window alerts you when new arrive.

Home > Layout

Each dashboard item appears as a vertical section. Layout control lets you view/hide each item and set the order, from top to bottom, they appear. To display an item, simply check the box next to the item.

Three items have addition customization control: **Alert, Tickets, and Messages**. All three display time dependent data. To make it easy to quickly distinguish new item from old items, you can specify different highlight colors from data rows depending on how recently the data item was generated.

Highlight the most recent items in red. All items created in the last N days are shown in red.

Items created in the last <enter number here> days

Highlight the next most recent items in yellow. All items that are older than the red highlight date but more recent than the number entered here are shown in yellow.

Items created in the last <enter number here> days

Disable highlighting by setting the number of days to zero.

The number of rows shows for **Alerts** and **Tickets** may also be customized.

Audit Tab

The system automatically audits each managed machine on a recurring basis (once per day is the default). Audit maintains a comprehensive picture of the current software and hardware configuration. Collected audit information includes:

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

The audit can assist an administrator in troubleshooting since it enables them to observe events prior to a problem. The Agent automatically records configurations and reports the information back to the Server so you can access it even when managed machines are powered down.

To access the Assistant, click Assistant from any function page.

The following functions are available in the Audit feature tab:

Run Audit	The Run Audit function used in conjunction with the Reports feature tab can be used to generate reports about usage trends and client machine configurations, which can be helpful in isolating faults and other software- or hardware-related problems.
System Info	Shows DMI / SMBIOS data collected
Installed Apps	Shows a list of executable (.exe) files on selected client machines.
SW Licenses	Shows a list of vendor license codes found on selected client machines.
Name/OS Info	Shows the Windows Networking computer name, operating system, and operating system version in use on the client machine(s).
IP Info	Shows the Machine.Group ID, IP address, subnet mask, default gateway, and connection gateway in use on the client machine(s).
DNS/DHCP	Shows the Machine.Group ID, DNS Server, DHCP server, and primary and secondary WINS servers in use on the client machine(s).
Disk Volumes	Shows the Machine.Group ID, types of drives with corresponding drive letters, and free space and total space on physical and logical drives in use on the client machine(s).
PCI & Disk H/W	Shows information about PCI, disk drives, and disk controller cards installed on client machines.

CPU/RAM	Shows the Machine.Group ID, CPU, quantity and speed of CPUs, and RAM as reported in use on the client machine(s)
Printers	Lists all printers available to the Machine ID.
Machine Summary	Organize the layout of the single machine interface.

Audit > Run Audit

Show me an explanation of the items on this page.

Audit collects the current state of both the hardware and software on a managed machine. The system maintains two audits for each machine: **baseline audit** and **latest audit**. Typically, you run a baseline audit once when a system is in a known working state. Then schedule latest audit to run every day to always have the latest audit information available for any machine. Reports provide detailed comparisons between baseline and latest audits, giving you a clear view of any changes on a machine.

When an agent checks into the KServer for the first time, both a baseline and latest audit are run on the machine. Audit collects all hardware and software information about the machine and stores it in the KSErver's database for retrieval any time.

What is a latest audit?

A latest audit contains current information about a client machine's hardware and software configuration. Typically you would schedule a latest audit collection to run daily.

What is a baseline audit?

A baseline audit contains the same information as a latest audit. Baseline audit information only updates when a new baseline audit runs. You would typically only run a baseline audit when a managed machine is in a known good state. Reports let you compare this known good state to the latest audit and quickly identify any system changes.

How do I cancel a previously scheduled audit?

To cancel a previously scheduled audit, select the client machine whose audit you wish to cancel, then press the **Cancel** button. The **Next Audit** column information will be removed.

Why should I disable PCI & Disk Audit?

The agent uses a driver to query the PCI bus during the audit. Only disable the driver if you suspect a driver conflict on the managed machine. The agent can not audit PCI hardware cards if this driver is disabled.

Explanation of items on this page

The system maintains current data on each managed machine by auditing each machine on a recurring basis. The KServer detects changes in a machines's configuration by comparing audit results to a **Baseline** audit and issuing alerts, were desired, or publishing Reports.

The following elements are displayed in the **Run Audit** function:

Latest Audit

Select this radio button and press Schedule to run a **Latest Audit** of all selected machines. Run Latest Audit to capture the state of machines on a frequent basis, such as daily. Reports use latest audit information for the majority of data listed.

Baseline Audit

Select this radio button and press Schedule to run a **Baseline Audit** of all selected machines. Run a Baseline Audit to capture the state of machines in a known good working condition. Reports compare the Baseline Audit information against the **Latest Audit** information to quickly highlight changes and identify the source of problems.

System Info

Select this radio button and press Schedule to collect **System Info** of all selected machines. System Info displays all DMI / SMBIOS data collected for each managed machine. This data virtually never changes and typically only needs to be run once.

Schedule

Pressing Schedule tasks each checked machine to perform an audit at the specified time. The audit is automatically repeated at the recurring interval you set. **Stagger by** setting lets you spread the audit time out when running several machines.

Note: Schedule Latest Audit by *unchecking* both Baseline Audit and System Info

Cancel

Press Cancel to stop the recurring audit on all selected machines.

Run recurring

To execute a script indefinitely at a regular interval, check the Run recurring checkbox and enter the interval time in day(s) or hour(s).

Note: If the interval is at least one day, then the recurring script runs at the scheduled time every interval. If the interval is less than one day, the interval is added to the last execution time of the script.

Stagger by

Scheduling a the same script to run at the same time on multiple machines my excessively load your server and/or internet connection. To automatically spread out the execution times, enter the number of minutes to stagger the script start time by. Clicking Schedule with multiple machine IDs selected, sets the execution time for the first machine at the scheduled time. It schedules the second machine at that time plus stagger minutes, and so on.

Skip if offline

Checking this box to only allow the script to run at the scheduled time of day (15 minute window). If the machine is offline at the scheduled time, then the script will not execute at all. If recurring is set, then the script is rescheduled to run at the next appointed time.

Remind me when accounts need audit scheduled

Check this box (the default) to pop up a warning message when audits have not been scheduled on a machine. The warning pops up every time you show the Run Audit function.

Machine.Group ID/System Info

Top line shows the machine ID of the managed machine. Bottom line shows when the last System Info collection ran. If a System Info collection is pending, the time displays in red text.

Latest Audit/Baseline Audit

Top line shows when Latest Audit data was last collected. Bottom line shows when Baseline Audit data was last collected. If the baseline audit is pending, the time displays in red text.

Next Audit/Recurring Interval

Shows the time of the next scheduled latest audit and its execution frequency. If the latest audit is pending, the time displays in red text.

PCI & Disk Audit

Enable/Disable the hardware audit driver for an agent. Only disable the driver if you suspect a driver conflict on the managed machine. The agent can not audit PCI hardware cards if this driver is disabled.

Check-in status

The check-in status of the machines shown in the client machine list is indicated by the icon shown to the left of the client machine ID. The icons and their status are as follows:

OK **Agent has checked in**

⚑ **Agent has not recently checked in**

⚑ **Agent has never checked in**

Audit > System Info

Show me an explanation of the items on this page.

System Info displays all DMI / SMBIOS data collected for each managed machine. System Info collection, like Baseline Audit, is automatically scheduled and run once after creating a new machine account. System Info data rarely changes so running once is usually sufficient. To collect fresh System Info again, check the box in front of each requested managed machine and then click the Schedule button. Missing data or data not available for a particular machine may be entered manually by the administrator.

When is System Info collected?

System Info runs once each time a collection is scheduled. Collection is automatically scheduled after creating a new machine account. To collect fresh System Info again, check the box in front of each requested managed machine and then click the Schedule button.

When would I Cancel a System Info collection?

Cancel a pending collection if collection is causing a problem on the remote machine.

How can I display more data?

Click the Show More button to display any or all of the data items collected by System Info. Available items are defined here.

Explanation of items on this page

Schedule

System Info runs once each time a collection is scheduled. Collection is automatically scheduled after creating a new machine account. To collect fresh System Info again, check the box in front of each requested managed machine and then click the Schedule button.

Cancel

Cancels scheduled System Info Collection tasks on selected machines.

Run recurring

To execute a script indefinitely at a regular interval, check the Run recurring checkbox and enter the interval time in day(s) or hour(s).

Note: If the interval is at least one day, then the recurring script runs at the scheduled time every interval. If the interval is less than one day, the interval is added to the last execution time of the script.

Stagger by

Scheduling a the same script to run at the same time on multiple machines my excessively load your server and/or internet connection. To automatically spread out the execution times, enter the number of minutes to stagger the script start time by. Clicking Schedule with multiple machine IDs selected, sets the execution time for the first machine at the scheduled time. It schedules the second machine at that time plus stagger minutes, and so on.

Skip if offline

Checking this box to only allow the script to run at the scheduled time of day (15 minute window). If the machine is offline at the scheduled time, then the script will not execute at all. If recurring is set, then the script is rescheduled to run at the next appointed time.

Show More

Define the list of data displayed on **System Info**. The list below defines each available data item.

Automatic Collection

Symbol indicates the data item is automatically collected and updated each time collection runs. *Click this icon to toggle to Manual Collection mode*.

Manual Collection

Symbol indicates the data item is manually input by the administrator. These items are **not** updated each time collection runs. *Click this icon to toggle to Automatic Collection mode*.

Edit Value

Edit any System Info data by clicking this icon. Edit Value only appears by items set to **Manual Collection**.

System Info Data Items

System Info collects each of the items listed below. You may display any and all of them by clicking the Show More button.

Manufacturer - system manufacturer

Product Name - system product name

System Version - product version number

System Serial Number - system serial number

Chassis Serial Number - serial number on the enclosure

Chassis Asset Tag - asset tag number on the enclosure

External Bus Speed - motherboard bus speed

Max Memory Size - max memory size the motherboard can hold

Max Memory Slots - total number of memory module slots available

Chassis Manufacturer - manufacturer of the enclosure

Chassis Type - enclosure type

Chassis Version - enclosure version number

Motherboard Manufacturer - motherboard manufacturer

Motherboard Product - motherboard product ID

Motherboard Version - motherboard version number

Motherboard Serial Num - motherboard serial number

Processor Family - processor type installed

Processor Manufacturer - processor manufacturer

Processor Version - processor version ID

CPU Max Speed - max processor speed supported

CPU Current Speed - speed processor is currently running at

On Board Devices - table of motherboard based devices (like video or ethernet)

Port Connectors - table of all the connections available on the chassis

Memory Devices - table of memory modules installed on the motherboard

System Slots - table indicating status of each available card slot

Audit > Installed Apps

Installed Apps lists all applications found during the last audit on the selected machine. Click the machine ID of choice to view the installed applications on a client machine. Shortly, the list of applications installed on the client machine will be displayed in the browser window. Adjust the display size and type of data shown with the following controls:

Explanation of items on this page

Row Selector

To enhance performance the VSA limits the number of applications listed per page. Select the set of applications you wish to view with the drop down control .

Filter button

The filter fields on the bottom of the Filter dialog box allows administrators to narrow down their search by entering filter criteria. By default, the (*) wildcard is used, which lists all files. For example, if an administrator is looking for a particular application that starts with the letter 'A', simply type the letter 'A' in the Application field, click Save, and the application list will update accordingly. The NOT checkbox masks the criteria listed in the filter field. For example, typing 'A' in the Application filter field and checking the NOT checkbox will display all applications that do NOT start with the letter 'A'.

To view the application filter, click here.

Full column width

Column data is limited to fit in the allotted space for each column. Hovering over shortened data displays the full data as a tool tip. To view all the data check this box.

Rows/page

Selects the number of applications displayed per page. Selecting "All" displays all applications for the selected machine. All applications may take a long time to display.

Machine.Group ID

Lists the client machines according to the Specify Accounts criteria.

The following information is displayed by default:

Application

Lists the filename of the application.

Version

Lists the version number of the application.

Product Name

Lists the product name of the application.

Description

Lists a brief description of the application as reported in the Properties dialog box of the executable file.

Directory Path

Lists the absolute directory path where the application file is located.

File Size

Lists the size (Kbytes) of the application file.

Last Modified

Lists the modification date of the application file.

Audit > SW Licenses

Show me an explanation of the items on this page.

Displays all the Software Licenses found on this machine. Each vendor stores an application's license key differently so all applications may not be found. To display licenses for any machine, simply click on the machine name.
The VSA displays duplicate license keys, found on more than one machine, in red text.

What information is displayed here?

Displays all the Software Licenses found on each machine. Vendors store application's license key differently so all applications may not be found. To display licenses for any machine, simply click on the machine name.

When are SW License codes collected?

Software licenses are re-collected with each audit. You do not need to do anything special to collect this information.

Why are some lines displayed in red?

If duplicate license codes are found on different machine they are displayed in red text.

Explanation of items on this page

Publisher

Software publisher of the application (e.g. Microsoft).

Title

Name of the application.

License

License code associated with this application.

Audit > Name/OS Info

Show me an explanation of the items on this page.

Name/OS Info displays the Microsoft Windows Networking computer name, operating system, and version information for specified user accounts.

How do I find out computer name and operating system information about a client machine?
Information shown in this function is collected when a Latest Audit is performed.

By going to the Name/OS Info function of the Audit tab, you can obtain the computer name, operating system, and operating system version information. To see all administered machines in all groups, enter an asterisk (*) in the Machine ID field of the Specify Accounts area.

A client machine needs to have performed a Latest Audit recently in order for the Name/OS Info information to be up to date.

Information shown in this function is collected when a Latest Audit is performed.

By going to the Name/OS Info function of the Audit tab, you can obtain the computer name, operating system, and operating system version information. To see all administered machines in all groups, enter an asterisk (*) in the Machine ID field of the Specify Accounts area.

A client machine needs to have performed a Latest Audit recently in order for the Name/OS Info information to be up to date.

Explanation of items on this page
The following elements are displayed in the Name/OS Info function:

Machine.Group ID
Lists the client machines according to the Specify Accounts criteria.

Computer Name
Lists the name of the computer as reported and used by Windows Networking.

Operating System
Lists the operating system name used by the client machine.

Version
Lists the version number of the operating system in use by the client machine.

Check-in status
The check-in status of the machines shown in the client machine list is indicated by the icon shown to the left of the client machine ID. The icons and their status are as follows:

OK **Agent has checked in**

⚑ **Agent has not recently checked in**

⚑ **Agent has never checked in**

Related Info

Audit > IP Info

Show me an explanation of the items on this page.

IP Info displays IP address, subnet mask, default gateway (internal) and connection gateway (external) information for selected user accounts.

> **Note: Connection gateway is the public IP address the outside world sees when a machine connections from a private LAN behind a NAT gateway. Typically that IP address is the address on the WAN side of the NAT gateway.**

How do I view IP and gateway information about client machines?

Information shown in this function is collected when a Latest Audit is performed.

By going to the IP Info function of the Audit tab, you can obtain IP address and gateway information. To see all administered machines in all groups, enter an asterisk (*) in the Machine ID field of the Specify Accounts area.

A client machine needs to have performed a Latest Audit recently in order for the IP Info information to be up to date.

Information shown in this function is collected when a Latest Audit is performed.

By going to the IP Info function of the Audit tab, you can obtain IP address and gateway information. To see all administered machines in all groups, enter an asterisk (*) in the Machine ID field of the Specify Accounts area.

A client machine needs to have performed a Latest Audit recently in order for the IP Info information to be up to date.

Explanation of items on this page

The following elements are displayed in the IP Info function:

Machine.Group ID

Lists the client machines according to the Specify Accounts criteria.

IP Address

Lists the IP address assigned to the client machine.

Subnet Mask

Lists the subnet mask that the IP address belongs to.

Default Gateway/Connection Gateway

Lists the default and connection gateway in use by the client machine.

MAC Address

Lists the Media Access Control (MAC) address of the machine listed, which uniquely identifies each node on a network.

Check-in status

The check-in status of the machines shown in the client machine list is indicated by the icon shown to the left of the client machine ID. The icons and their status are as follows:

Agent has checked in

Agent has not recently checked in

Agent has never checked in

Related Info

Audit > DNS/DHCP

Show me an explanation of the items on this page.

DNS/DHCP displays DNS servers, DHCP server, Primary and Secondary WINS server information for specified user accounts.

How do I view the DNS, DHCP and WINS information about an individual client machine or group of client machines?

Information shown in this function is collected when a Latest Audit is performed.

By going to the DNS/DHCP function of the Audit tab, you can obtain DNS, DHCP and WINS information. To see all administered machines in all groups, enter an asterisk (*) in the Machine ID field of the Specify Accounts area.

A client machine needs to have performed a Latest Audit recently in order for the DNS/DHCP information to be up to date. If a function is not used on the client machine, **not available** is shown. For example, **Secondary WINS** servers are often not utilized.

Information shown in this function is collected when a Latest Audit is performed.

By going to the DNS/DHCP function of the Audit tab, you can obtain DNS, DHCP and WINS information. To see all administered machines in all groups, enter an asterisk (*) in the Machine ID field of the Specify Accounts area.

A client machine needs to have performed a Latest Audit recently in order for the DNS/DHCP information to be up to date. If a function is not used on the client machine, **not available** is shown. For example, **Secondary WINS** servers are often not utilized.

Explanation of items on this page

The following elements are displayed in the DNS/DHCP function:

Machine.Group ID

Lists the client machines according to the Specify Accounts criteria.

DNS Server

Displays the DNS servers in use by the client machine.

DHCP Server

Displays the DHCP servers in use by the client machine.

Primary/Secondary WINS

Displays the primary and, if used, the secondary WINS servers in use by the client machine.

Check-in status

The check-in status of the machines shown in the client machine list is indicated by the icon shown to the left of the client machine ID. The icons and their status are as follows:

🟩 **Agent has checked in**

🟨 **Agent has not recently checked in**

🟥 **Agent has never checked in**

Related Info

Audit > Disk Volumes

Show me an explanation of the items on this page.

Disk Volumes displays drive letter, drive type (fixed, removable, or CD-ROM), free space, and total size of drive information for specified user accounts.

How do I get information about PCI devices and disk volumes used by a client machine?

Information shown in this function is collected when a Latest Audit is performed.

By going to the **Disk Volumes** function of the **Audit tab**, you can obtain information about PCI devices in use by a client machine. To see all administered machines in all groups, enter an asterisk (*) in the Machine ID field of the Specify Accounts area.

The drive letters used by the media is reported in the **Drive** column along with the **Label**, **Type**, **Format**, **Free Space**, and **Total Size**.

The different types of media, along with free space and total size, reported by the sytem are:

- Removable (ZIP, floppy)
- Fixed (hard disk)
- Network (share drives, network drives)
- CD-ROM (CD-ROM, DVD-ROM, Optical drive)

A client machine needs to have performed a Latest Audit recently in order for the Disk Volumes information to be up to date.

Explanation of items on this page

The following elements are displayed in the Storage Devices function:

Machine.Group ID

Lists the client machines according to the Specify Accounts criteria.

Drive

Lists the drive letter in use by the client machine for the selected drive.

Label

Lists the name given to the volume. In Windows, this value can be set and viewed by right-clicking the volume in any Explorer window and selecting **Properties**.

Type

Lists the type of drive in use by the client machine. The different types are:

- **Removable** Examples include a ZIP drive, tape drive, optical drive, etc.
- **Fixed** Standard non-removable hard drives.
- **CD-ROM** CD-ROM, CD-RW and DVD-ROM drives, all reported as CD-ROM drives.
- **Network** Mapped network drives accessible from the client machine.

Format

Lists the formatting applied to the volume. Formats that can be read by the system are: **NTFS**, **FAT32**, **FAT**, and **CDFS**.

Free Space

Lists the available free space (megabytes) as reported from removable and network drives.

Total Size

Lists the total storage capacity (megabytes) of the removable or network drive.

Check-in status

The check-in status of the machines shown in the client machine list is indicated by the icon shown to the left of the client machine ID. The icons and their status are as follows:

🟩 **Agent has checked in**

🟨 **Agent has not recently checked in**

🟥 **Agent has never checked in**

Audit > PCI & Disk H/W

Show me an explanation of the items on this page.

How do I get information about the PCI devices used by a client machine?
Information shown in this function is collected when a Latest Audit is performed.

By going to the PCI & Disk H/W function of the Audit tab, you can obtain information about network cards, controller cards multimedia cards, hard disk controllers and other devices installed on a client machine. To view all machines administered in all groups, enter an asterisk (*) in the Machine ID field of the Specify Accounts area.

The different types of devices reported by the system are:

- Network cards
- Graphics cards
- Multimedia (sound) cards
- Hard disk controller cards
- CD-ROM and hard disk vendor information

A client machine needs to have performed a Latest Audit recently in order for the **PCI & Disk H/W** information to be up to date.

Information shown in this function is collected when a Latest Audit is performed.

By going to the **PCI & Disk H/W** function of the **Audit tab**, you can obtain information about network cards, controller cards multimedia cards, hard disk controllers and other devices installed on a client machine. To view all machines administered in all groups, enter an asterisk (*) in the Machine ID field of the Specify Accounts area.

The different types of devices reported by the system are:

- Network cards
- Graphics cards
- Multimedia (sound) cards
- Hard disk controller cards
- CD-ROM and hard disk vendor information

A client machine needs to have performed a Latest Audit recently in order for the **PCI & Disk H/W** information to be up to date.

Explanation of items on this page

Machine.Group ID
Lists the client machines according to the Specify Accounts criteria.

Type
Lists the type of device installed on the client machine. This can include network interface cards, graphics cards, sounds cards, hard disks, and CD-ROM drives.

Vendor
Lists the manufacturer of the device installed on the client machine.

Product
Lists the device installed in the client machine.

Check-in status
The check-in status of the machines shown in the client machine list is indicated by the icon shown to the left of the client machine ID. The icons and their status are as follows:

🟩 **Agent has checked in**

🟨 **Agent has not recently checked in**

🟥 **Agent has never checked in**

Audit > CPU/RAM

Show me an explanation of the items on this page.

How do I find out what type, speed and quantity of CPU a client machine has?

Information shown in this function is collected when a Latest Audit is performed.

By going to the CPU/RAM function of the Audit tab, you can obtain CPU, CPU speed, quantity and RAM information. To see all administered machines in all groups, enter an asterisk (*) in the Machine ID field of the Specify Accounts area.

A client machine needs to have performed a Latest Audit recently in order for the CPU/RAM information to be up to date.

Information shown in this function is collected when a Latest Audit is performed.

By going to the CPU/RAM function of the Audit tab, you can obtain CPU, CPU speed, quantity and RAM information. To see all administered machines in all groups, enter an asterisk (*) in the Machine ID field of the Specify Accounts area.

A client machine needs to have performed a Latest Audit recently in order for the CPU/RAM information to be up to date.

How do I find out how much RAM a client machine has?

Information shown in this function is collected when a Latest Audit is performed.

By going to the CPU/RAM function of the Audit tab, you can obtain RAM information. To see all administered machines in all groups, enter an asterisk (*) in the Machine ID field of the Specify Accounts area.

The amount of RAM reported may be slightly different than the actual physical RAM in the machine. This is the RAM information as reported by the operating system, and is normal.

Information shown in this function is collected when a Latest Audit is performed.

By going to the CPU/RAM function of the Audit tab, you can obtain RAM information. To see all administered machines in all groups, enter an asterisk (*) in the Machine ID field of the Specify Accounts area.

The amount of RAM reported may be slightly different than the actual physical RAM in the machine. This is the RAM information as reported by the operating system, and is normal.

Explanation of items on this page

CPU/RAM displays the CPU type, number of CPUs, CPU speed, and total physical RAM as reported by the client machine during an audit.

The following elements are displayed in the CPU/RAM function:

Machine.Group ID

Lists the client machines according to the Specify Accounts criteria.

CPU

Lists the manufacturer and model of the CPU as reported by the client machine. If a client machine has more than one CPU, the manufacturer and model is displayed for each one.

Quantity (Qty.)

Lists the number of CPUs used in the client machine.

Speed

Lists the clock speed (megahertz) of the client machine. If a client machine has more than one CPU, the speed is displayed for each one.

Note: Due to rounding, the listed speed of the processor may not be the advertised speed, as specified by its manufacturer.

RAM

Lists the amount of physical random access memory available (megabytes) as reported by the client machine.

Check-in status

The check-in status of the machines shown in the client machine list is indicated by the icon shown to the left of the client machine ID. The icons and their status are as follows:

OK **Agent has checked in**

🟨 **Agent has not recently checked in**

🟥 **Agent has never checked in**

Related Info

Audit > Printers

Show me an explanation of the items on this page.

What information is displayed on this page.

Printers list all printers mounted for the currently logged on user at the time the last audit ran.

The list of printers do not match those on the machine. Why?

Printers are mounted on a per users basis. Therefore, the printers listed are those of the user who is logged on at the time of the audit. If no user is logged in, the printers of the Administrator account are reported.

Explanation of items on this page

The following elements are displayed in the Printers function:

Machine.Group ID

Lists the client machines according to the Specify Accounts criteria.

Printers

Lists the name of each printer found during the last audit.

Note: Printers are mounted on a per users basis. Therefore, the printers listed are those of the user who is logged on at the time of the audit. If no user is logged in, the printers of the Administrator account are reported.

Port

Name of the port this printer is connected to.

Model

Lists the model name reported by the manufacturer of each printer found.

Audit > Machine Summary

The Machine Summary interface displays collected information for a single machine at a time. You can access a unique page for every machine ID simply by clicking the agent status icon to the left of every machine ID on any function in the system.

Agent status icons- *

*Shown only in the Remote Control function page.

The Machine Summary page groups similar data types together into tabs. Click any tab to view the details for the selected machine ID.

Machine Info

Displays the following information about the machine collected during audit:

- Computer Name
- Operating System
- OS Version
- RAM size
- CPU type

The second block of data displays network configuration data for this machine.

- IP Address
- Subnet Mask
- Default Gateway
- Connection Gateway
- MAC Address
- DHCP Server
- DNS Server
- Primary WINS
- Secondary WINS

Installed Applications

Lists all applications reported during the latest audit.

System Info

System Information collected during the latest audit.

Disk Volumes

Lists all fixed and removable disk drives found during the latest audit. Reports free space and total space of fixed disk drives.

PCI & Disk Hardware

List all PCI devices found during the latest audit. Also list make and model of each disk drive found.

Printers

Lists all printers mounted for the user logged on during the latest audit. If no one was logged in, then printers for the Administrator account are reported.

Pending Scripts

Lists all scripts scheduled to run on the selected machine. Through this interface you can modify the schedules and/or schedule new scripts to run. A summary history of recent scripts that ran is shown below the pending script list.

Agent Logs

View the captured log data for the machine ID here. Change to any log by selecting the desired log from the drop down control. Logs include:

- Alert Log
- Agent Log
- Configuration Changes

- Network Statistics
- Application Event Log
- Security Event Log
- System Event Log
- Script Log

Alerts

Modify the settings for any alert assigned to this machine ID

Patch Status

Displays all patch configuration data for this machine ID. Can also show either the Machine Update or Patch History data set for this machine. With Machine Update, you can schedule and deploy patches to this machine.

Remote Control

Initiate a remote control, FTP, or Chat session with the machine ID. You can also specify the default remote control package to use, pre-install or un-install the package, or reset a password on the remote machine.

Agent Settings

Modify the check-in control, profile, or log settings for this machine ID.

Audit > File Access

Show me an explanation of the items on this page.

The Agent can protect any file on client machines from unauthorized access by a rogue application or user. Any application can be approved or denied access to the file. Additionally, specifying "Ask user to approve unlisted" opens a dialog box and asks the user to approve the application accessing the file. This method effectively learns which applications to approve or deny as you go.

The file can be **referenced by file name and/or a portion of the full path**. For example, adding a file named *protectme.doc* to the list, protects on occurrences of *protectme.doc* in any directory on any drive. Adding *myfolder\protectme.doc* protects all occurrences of the file in any directory named *myfolder*.

Note: You may also block operating system access to the protected file. This prevents the file from being renamed, moved, or deleted therefore completely locking down the file from tampering.

Note: Granting access to explorer.exe and/or cmd.exe allows operating system access to a file.

Add

To protect a file from access by rouge applications, enter the filename and click the add button. This open a new dialogue window into which you can select applications to approve for access to that file.

Note: The Browse... button is there solely for your convenience in quickly finding a file path. It can not browse the file system on a remote machine.

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

Filename to access control - Spot to edit the path to the controlled file

New... - Add in a new application to give access to this file. You can manually enter the application or use the Search... button to select an application from the audit list.

Remove - Removes an application from the approved access list

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 - Automatically blocks an application from accessing the file. Select this option if you are already sure of which files need access and which do not.

Delete

Remove an application from the protection list by clicking the Delete 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.

Explanation of items on this page

The following elements are displayed in the File Access function:

Machine.Group ID

List the Machine ID of all machines that match the Specify Accounts filter. Each Machine ID is a link. **Clicking the machine ID name displays the list of applications found by audit for that machine ID.** Use this to quickly browse for application names on to approve or deny file access to.

Filename

Filename of the file to be protected. Click the Edit icon next to any filename to change the path for that filename.

Approved Apps

List of all applications protected for each machine ID.

Ask User Approval

Check mark appears if **Ask user to approve unlisted** is set for this machine ID.

Check-in status

The check-in status of the machines shown in the client machine list is indicated by the icon shown to the left of the client machine ID. The icons and their status are as follows:

OK Agent has checked in

⚑ Agent has not recently checked in

⚑ Agent has never checked in

Audit > Network Access

Show me an explanation of the items on this page.

What is Network Protection?

Network Protection allows you to monitor and control access on a per application and per machine basis. Use it to collect bandwidth utilization consumed by each managed machine on your network. The network access function lets you approve or deny network access on a per application basis. Use the Network Statistics report to view network bandwidth utilization versus time. Drill down and identify peak bandwidth consumers by clicking on the graph's data points. See which application and which machine use bandwidth at any point in time.

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 agent can not monitor network statistics or block network access if this driver is disabled.

How do I approve/deny applications from accessing the network?

The system allows administrators to control access to the network by individual applications. Applications can be permanently denied access to the network; users can also be notified when an unlisted application accesses the network, permitting or denying that application network access.

To approve network access to an application:

1. Click the client machine link from the **Machine.Group ID** column whose applications you wish to approve network access to.
A list of applications installed on the client machine will be displayed. Since the list may be large, you can control the applications displayed by using the application filter, which is accessed by pressing Filter , located at the top of the application.

2. In the applications list, select the application(s) that you wish to approve access to the network.

3. Select the **Ask user to approve unlisted** radio button, then press Apply.

4. Press Approve apps.

The application(s) selected in the application list are added to the **Approved Apps** column.

To deny network access to an application:

1. Perform steps 1-3, as shown above.

2. Press deny apps.

The application(s) selected in the application list are added to the **Denied Apps** column.

In approving application access to the network and selecting the **Ask use to approve unlisted** radio button, the user will be notified when an application attempts to access the network that is not on the application list for their machine. The user has four responses that they can enter for the given application:

- **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.

The system allows administrators to control access to the network by individual applications. Applications can be permanently denied access to the network; users can also be notified when an unlisted application accesses the network, permitting or denying that application network access.

To approve network access to an application:

1. Click the client machine link from the **Machine.Group ID** column whose applications you wish to approve network access to. A list of applications installed on the client machine will be displayed. Since the list may be large, you can control the applications displayed by using the application filter, which is accessed by pressing Filter , located at the top of the application.
2. In the applications list, select the application(s) that you wish to approve access to the network.
3. Press Approve apps.

The application(s) selected in the application list are added to the **Approved Apps** column.

To deny network access to an application:

1. Perform steps 1-2, as shown above.
2. Press deny apps.

The application(s) selected in the application list are added to the **Denied Apps** column.

Notify user when app blocked

Clicking Enable notifies the user when an application attempts to access the network that is not on the application list for their machine. Use the function to build up the access list based on normal usage. This lets you see which applications on your system are accessing the network and when.

The user has four responses that they can enter for the given application:

- **Always** Allows the application access to the network indefinitely. Users will not be prompted again.
- **Yes** Allows the application access to the network for the duration of the session. Users will be prompted again.
- **No** Denies the application access to the network for the duration of the session. Users will be prompted again.
- **Never** Denies the application access to the network indefinitely. Users will not be prompted again.

Enable / Disable driver 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 can not monitor network statistics or block network access if this driver is disabled.

NOTE: Changing the state of the drive does not take effect until the selected machine is next reboot.

Explanation of items on this page

The following elements are displayed in the Network Access function:

Machine.Group ID

Lists the client machines according to the Specify Accounts criteria.

Notify User

An X in this column indicates that the client machine user will be notified when an application has been denied network access. To remove this notification:

1. Select the client machine that is to have the notification removed by selecting the checkbox next the machine ID.
2. Unselect the *Notify use when app is blocked* (make sure it is checked).
3. Press Apply.

To notify the user when a application has been denied:

1. Select the client machine that is to have the notification removed by selecting the checkbox next the machine ID.
2. Select the *Notify use when app is blocked* (make sure it is unchecked).
3. Press Apply.

Enable Driver

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

Approved Apps

If all applications are approved for network access, then *Approve All Unlisted* is shown in the Approved Apps column. Specific applications can be added to the list by selecting the checkbox next to the application in the application list, then pressing Approve Apps. If an application is specifically listed in the Approved Apps column, all unlisted applications that attempt to access the network can be set to behave in the following ways by responding to the Internet Access Attempted dialog box:

- **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.

Denied Apps

Applications listed in the **Denied Apps** column are not allowed to access the network.

The following functions can be applied in conjunction with the settings applied in the previous functions:

Unlisted Action

Identifies how each machine ID reacts when an application that is not specifically listed tries to connect to the network.

- **Ask** - Asks the user each time an unlisted application accesses the internet.
- **Approve** - Allows access for all unlisted application.
- **Deny** - Denies access to any unlisted application.

Check-in status

The check-in status of the machines shown in the client machine list is indicated by the icon shown to the left of the client machine ID. The icons and their status are as follows:

OK **Agent has checked in**

🟨 **Agent has not recently checked in**

🟥 **Agent has never checked in**

Audit > Application Blocker

Show me an explanation of the items on this page.

Prevent any application from running on a machine. Applications listed here are blocked when a user double clicks them or tries to run the application at all.

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.

Note: Blocked application may not be renamed, moved, or deleted from the system.

Add

To block an application from running on a machine, the application's filename and click the add button.

Delete

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

Explanation of items on this page

The following elements are displayed in the File Access function:

Machine.Group ID

List the Machine ID of all machines that match the Specify Accounts filter. Each Machine ID is a link. **Clicking the machine ID name displays the list of applications found by audit for that machine ID.** Use this to quickly browse for application names on to approve or deny file access to.

Application Location

Filename of the application to be blocked.

Check-in status

The check-in status of the machines shown in the client machine list is indicated by the icon shown to the left of the client machine ID. The icons and their status are as follows:

OK **Agent has checked in**

⚑ **Agent has not recently checked in**

⚑ **Agent has never checked in**

Feature Tab > Scripts

You may create customized installation packages to deploy to active user account machines. Or create any general purpose script to modify files and/or the registry on any machine ID. Use the Scripts tab feature to organize customized scripts. The scripts facility provides:

- Installation of applications via administrator-defined scripts
- Support for all standard installation programs
- The Packager captures system changes resulting from product installations, desktop optimization, and customizations. It "packages" them in one convenient self-extracting file ready for automated distribution

To access the Assistant, click Assistant from any function page.

The following functions are available in the Install feature tab:

Functions	Description
Patch Deploy	Use this wizard tool to create scripts to deploy patches to managed machines.
Application Deploy	Use this wizard tool to create scripts to deploy third party install packages (setup.exe) to managed machines.
Packager	An external application that allows administrators to create installation packages deployable on administered client machines.
Get File	View and manage files uploaded to the VSA from remote machines by a Get File script command.
Distribute File	Write files to all selected remote machines and maintain them.
Scripts Status	Shows the status of scripts executed on client machines, machine.group ID, time of the last executed script, results of the executed script, and the number of times the script has been executed.
Distribution	Minimize network traffic and server loading by executing scripts evenly throughout the day

Scripts > Patch Deploy

Patch Deploy is a wizard tool to automatically create a script to distribute and apply Microsoft patches. The wizard walks you through a step by step process resulting in a script you can schedule to deploy a patch to any managed machine.

Step 1: Enter 6-digit knowledge base article number

Microsoft Publishes a vast assortment of information about its operating system in the **Microsoft Knowledge Base**. Each article in the Knowledge Base is identified with a 6-digit Q number (e.g. Q324096. All Microsoft patches have an associated knowledge base article number.

Entering the article number is optional. Leave it blank if you do not know it.

Step 2: Select the operating system type

Sometimes patches are specific to certain operating system. If the patch you are trying to deploy applies to a specific OS only, then select the appropriate operating system from the drop down control. When the wizard creates the patch deploy script, it will restrict execute of the script to only those machines with the selected OS. This prevents inadvertent application of operating system patches to the wrong OS.

Step 3: Download the patch

This step is just a reminder to fetch the patch from Microsoft. Typically there is a link to the patch on the knowledge base article describing the patch.

Step 4: How do you want to deploy the patch?

The patch needs to execute on the managed machine to install. The wizard generated script tells the remote machine where to get the patch file to execute. The Patch Deploy Wizard asks you in step 4 if you want to "*Send the patch from the VSA server to the remote machine and execute it locally*" or "*Execute the patch from a file share on the same LAN as the remote machine*."

Pushing the patch down to each machine from the VSA may be bandwidth intensive. If you are patching a multiple machines on a LAN no internet bandwidth is used to push out the patch. Each machine on the LAN can execute the patch file directly from a common file share.

Step 5: Select the patch file *or* Specify the UNC path to the patch stored on the same LAN as the remote machine.

If "*Send the patch from the VSA server to the remote machine and execute it locally*" was selected, then the patch must be on the VSA server. Select the file from the drop down list.

If the patch file does not appear in the list then it is not on the VSA server. Click the Back button and upload the file to the VSA by clicking the first here link.

If "*Execute the patch from a file share on the same LAN as the remote machine*" was selected, then the patch must be on the remote file share prior to running the patch deploy script. The specified path to the file must be in **UNC format** such as \\computername\dir\.

If the file is not already on the remote file share, you can put it their via FTP. Click the Back button and then the second here link which takes you to FTP.

Step 6: Specify the command line parameters needed to execute this patch silently.

To deploy a patch silently you need to add the appropriate command line switches used when executing the patch. Each knowledge base article lists the parameters for silent install. Typical switch settings are **/q /m /z**

Command line parameters are optional. Leave it blank if you do not know it.

Step 7: Name the script

The new script appears under the Install Tab. Master administrators can specify a shared script or private script. Standard Administrators can only create private scripts.

Step 8: Reboot the machine after applying the patch.

Check this box to automatically reboot the managed machine after applying the patch. The default setting is to **not** reboot.

Scripts > Application Deploy

Application Deploy is a wizard tool to automatically create a script to distribute vendor installation packages (typically setup.exe). The wizard walks you through a step by step process resulting in a script you can schedule to deploy an application to any managed machine.

Step 1: How do you want to deploy the application?

The application needs to execute on the managed machine to install. The wizard generated script tells the remote machine where to get the patch file to execute. The Patch Deploy Wizard asks you in step 4 if you want to "*Send the installer from the VSA server to the remote machine and execute it locally*" or "*Execute the installer from a file share on the same LAN as the remote machine*."

Pushing the patch down to each machine from the VSA may be bandwidth intensive. If you are patching a multiple machines on a LAN no internet bandwidth is used to push out the patch. Each machine on the LAN can execute the patch file directly from a common file share.

Step 2: Select the application install file *or* Specify the UNC path to the installer stored on the same LAN as the remote machine.

If "*Send the installer from the VSA server to the remote machine and execute it locally*" was selected, then the installer file must be on the VSA server. Select the file from the drop down list.

If the installer file does not appear in the list then it is not on the VSA server. Click the here link to upload the file to the server.

If "*Execute the installer from a file share on the same LAN as the remote machine*" was selected, then the installer file must be on the remote file share prior to running the application deploy script. The specified path to the file must be in **UNC format** such as \\computername\dir\.

If the file is not already on the remote file share, you can put it their via FTP. Click the here link to start FTP.

Step 3: What kind of installer is this?

The wizard need to know what kind of installer was used by your software vendor to create the install package. The VSA provides a small utility to automatically identify all supported installer types. Download and run kInstId.exe to automatically identifies the installer type. Supported installer types are:

- Windows Installer - used to deploy MSI file types
- Wise Installer
- Installshield - Package For The Web
- Installshield - Multiple Files

Step 4: Name the script

The new script appears under the Install Tab. Master administrators can specify a shared script or private script. Standard Administrators can only create private scripts.

Step 5: Reboot the machine after installing the application.

Check this box to automatically reboot the managed machine after running the install. The default setting is to **not** reboot.

Scripts > Packager

How does Packager work?

Packager evaluates the state of the source machine before and after an installation and/or resource change. The Packager compiles the differences into a single executable file - the Package - that can be distributed via scripts to any managed machine.

Each Package is OS dependent. To deploy to multiple OS's, you need to build a Package for each OS. During installation, Packager checks the target machine's operating system and does not continue if the Package is being deployed on an OS different than the source OS.

Packager picks up everything you do to a machine between the time you take the first snapshot and create the Package. Be careful what additional tasks you perform on the source machine as any system changes will be rolled into the Package.

For best results, we recommend you create a Package on a representative machine; that is, a machine that closely resembles the client machine(s) on which the Package will be deployed.

What if installation fails?

Packager has complete rollback capability. The rollback executable and associated restore files are located in the Agent directory on the target machine in the directory C:\Program Files\Kaseya\KPackage.

Creating a Package:

1. Download and execute the Packager application.
2. Packager takes a snapshot of the source system.
3. Install any application and/or resource on the source system.
4. Execute Packager again. Packager records the changes in the source system and creates a Package.
5. Distribute the Package any way you choose. You can e-mail it, or store it on a server where a custom script can perform a silent installation on any managed machine.

Scripts > Get File

Use the Get File function to access files uploaded from a remote machine when scripts execute either the Get File or Get File In Directory Path commands.

The VSA stores uploaded files in a unique directory for each machine ID. Clicking the Machine ID displays the uploaded files for that machine. Each file is displayed as a link. Click any filename to access that file.

Remove uploaded files from the VSA by clicking the delete icon ❌ next to the file.

As an option in the Get File script command, existing copies of uploaded files will be renamed with a .bak extension prior to the next upload of the file. This allows you to examine both the latest version of the file and the previous version. For example, your script executes the following Get File command (Exported with *Export Script...* in the script editor):

```
Get File
  Parameter 1 : c:\temp\info.txt
  Parameter 2 : news\info.txt
  Parameter 3 : 2
     OS Type : 0
```

Parameter 3 : 2 indicates Save existing version, get file, and send alert if file changed. The first time the above script statement executes on a remote machine the agent sends c:\temp\info.txt to the server and the VSA stores it. The second time the above statement executes, the VSA renames the original copy of news\info.txt to news\info.txt.bak then uploads a fresh copy and saves it as news\info.txt.

Also as an option, an email alert can be sent when a change in the uploaded file has been detected (compared to the last time the same file was uploaded).

The Get File command must have either the *Overwrite existing file and send alert if file changed* setting or the *Save existing version, get file, and send alert if file changed* setting selected.

Why would I use Get File instead of FTP?

If all you want to do is get a file from a remote machine as a one-time event then **FTP** is the simplest way. **Get File** is designed to support automated checks on a large number of remote machines simultaneously.

Use Get File in conjunction with a script to perform some automated task on a set of remote machines. For example, if you have a utility that reads out some information unique to your managed computers you can write a script to do the following:

1. Send the utility to the remote machine (using either the **Write File** script command or the **Distribute File** function.
2. Execute the utility using either the script command **Execute DOS Command** or **Execute File** and pipe the output to a text file (results.txt)
3. Upload the file to the server using the **Get File** command.

To perform continuous health checks on the remote machine, run the script on a recurring schedule and activate **Get File Changes alerts**. The VSA instantly notifies you of any changes to the results.

How do I get files from remote machines?

Any script executing a **Get File** or **Get File In Directory Path** command writes the file to the directory viewable from this function. You have to write a script to put files into this directory.

I see files present that I did not upload. Where did they come from?

Other administrators or a VSA system function like Hot Fix Check fetched these files. Any script executing a **Get File** command writes the file to the directory viewable from this function.

Scripts > Distribute File

Show me an explanation of the items on this page.

The **Distribute File** function sends files stored on your VSA server to remote machines. It is ideal for mass distribution of configuration files, such as virus foot prints, or maintaining the latest version of executables on all machines. The VSA checks the integrity of the file every full check-in. If the file is ever deleted, corrupted, or an updated version is available on the VSA, the VSA sends down a new copy prior to any script execution. Use it in conjunction with recurring scripts to run batch commands on remote machines.

The script command "Write File" performs the same action as Distribute File. Each time a script executes the "Write File" command, the agent checks to see if the file is already there or not. If not, the file is written. "Write File" is better than Distribute File for sending executable files you plan to run on remote machines via scripts.

How often are the files written to the remote machines?

Files are only written if they are missing from or corrupted on the remote machine.

One of the first steps in every Agent's full check-in process is to validate the integrity of all files in the **Distribute File** list. if the file was never there or was deleted the VSA sends down a copy of the file to the remote machine.

If the file is present, it is compared to the same file on the VSA server. If the file is corrupted, or an updated version is available on the VSA, the VSA sends down a new copy.

Where do the files in the drop down list come from?

These are the same files you see when accessing Managed Files... from inside the script editor. Private files are listed with **(Priv)** in front of the filename.

Click the **Managed Files... link** on the **Distribute File** page to add or remove files from this list.

When I cancel a file distribution is the file deleted?

Files are not deleted from either the server or remote machines by clicking **Cancel** or **Cancel All**.

Cancelling a file distribution just removes it from the Distribute File list for the selected machine. The Agent no longer performs Integrity checking on that file during a full check-in.

Another administrator has set up file distribution on several machines. Why can't I see them in the list?

The only files listed are private managed files or shared managed files. If another administrator chooses to distribute a private file you will not see it.

Master Administrators see all file distributions. Instead of the (Priv) prefix, (*admin name*) is listed.

Explanation of items on this page

Select server file

Select a file to distribute to remote machines from this list. All your shared and private files from the Script Editor's Managed Files... function appear in this list.

Specify full path and filename to store file on remote machine.

Enter a location to write the file at for the selected remote machines. The **Browse...** button is there as a convenience to more easily locate correct paths. Click it to get the standard Windows file browser dialog.

REMEMBER: Clicking the Browse... button allows you to browse directories on your own machine, NOT the remote machines.

Manage Files... link

Clicking the Manage Files... link opens a new window with the script editor's **Manage Files** function. Go here to add, update, or remove files stored on the VSA server.

Distribute

Click the Distribute button to tell the VSA to start distribution management of the file selected in

Select server file and write it to the location specified in **Specify full path and filename to store file on remote machine**. This effects all checked remote machines.

Cancel

Click the Cancel button to remove the distribution of the file selected in **Select server file** from all checked remote machines.

WARNING: *Cancel* and *Cancel All* do NOT delete the file from either the remote machines or the server. These functions simply stop the integrity check and update process from occurring at each full check-in.

Cancel All

Cancel All removes all file distributions from all checked remote machines.

Removing and modifying individual distributions

To the left of each distribution item listed, are two icons. Clicking these icons takes action on only that single listed item. Click ✗ to cancel that file distribution. Click 📋 to edit the destination path on the remote machine.

Scripts > Scripts Status

The Scripts function allows administrators to view the status of a script on selected client machines. Administrators can, at a glance, find out what time a script was executed and whether it was successfully executed. Pending scripts listed first in **dark red**.

The following elements are displayed in the Scripts function:

Machine.Group ID

Lists the client machines according to the Specify Accounts criteria.

Select Script To Display Its Current Status

Select a script in the dropdown menu to view its current execution status on client machines. If the selected script has been executed on the selected client machine, its status is displayed and the following information about the script shown:

- **Last Execution Time**

  Displays the date and time the script was last executed.

- **Last Execution Status**

  Displays the results of the executed script.

  - **Scheduling Admin**

    Displays the administrator who scheduled the script.

Check-in status

The check-in status of the machines shown in the client machine list is indicated by the icon shown to the left of the client machine ID. The icons and their status are as follows:

OK **Agent has checked in**

🟨 **Agent has not recently checked in**

🟥 **Agent has never checked in**

More detailed information about scripts can be learned by going to the Using Scripts section.

Related Info

Scripts > Distribution

Scripts can cause excessive network loading by pushing large files between the server and agent. Performing these operations with hundreds of agents simultaneously may cause unacceptable network loading levels.

Use this function to spread network traffic and server loading by executing scripts evenly throughout the day or a specific block of time in a day.

The system plots a histogram for each script currently scheduled to run at a recurring interval. Setting the histogram period to match the recurring interval of the script **counts how many machines execute the script in a specific time interval**. Peaks in the histogram visually highlight areas where a lot of machines are trying to execute the script at the same time. Use the controls, described below, to reschedule the script such that the network loading is spread evenly over time. **Only machines matching the current Machine ID/Group ID/View filter are counted in the histogram.**

Reschedule selected script evenly through the histogram period

Pick this radio control to reschedule selected scripts running on all machines matching the machine ID/group ID/view filter. Script execution times are adjusted such that no machine executes the script at the same time. Execute times are **staggered evenly across the entire histogram period**.

Reschedule selected script evenly between <start time> and <end time>

Pick this radio control to reschedule selected scripts running on all machines matching the machine ID/group ID/view filter. Script execution times are adjusted such that no machine executes the script at the same time. Execute times are **staggered evenly beginning with the start time and ending with the end time**.

Distribute

Click this button to reschedule all script execute start times for all machines set to execute that script on a recurring basis.

NOTE: The script recurring interval is replaced with the histogram period.

Replot

Refreshes the display with the a histogram period.

Histogram Plots

Each script with any machines set to execute them recurring display a histogram. Above the histogram is:

- Script name - name of the script. Check to box to select this script for distribution.
- Peak - number of machines executing the script at a specific time when the most machines are executing at the same time.
- Total - total number of machines executing the script on a recurring basis.

Skip if offline

Checking this box to only allow the script to run at the scheduled time of day (15 minute window). If the machine is offline at the scheduled time, then the script will not execute at all. If recurring is set, then the script is rescheduled to run at the next appointed time.

Creating Silent Installs

Assistant

HELP HOME

Creating Silent Installs

Most vendors provide either a single file (when downloaded from the web) or set of files (when distributed on a CD). Executing the installer file (typically named **setup.exe**) installs the vendor's application on any operating system.

Vendors typically use one of three applications to create install packages: **InstallShield**, **Windows Installer**, or **Wise Installer**.

Silent Installs with InstallShield

InstallShield has a record mode that captures answers to all dialog boxes in the installation script. The **Acrobat 4.05 script** under the **Install Tab** is an example of this technique. Define the Managed Variable **<FileServer>** to point to the location of the acrobat setup.exe file. InstallShield requires the recorded iis file to be on the same machine as the local machine. The first step in the script writes out that file (stored on the VSA).

Create a custom install package by following these steps:

1. Verify the install package was made with InstallShield.
   a. Launch the install package
   b. Look in window's the title bar. **InstallShield Wizard** appears at the end of the title.
2. Launch the install package in record mode from a command prompt.
   a. Install package is a **single** file. Run **`setup.exe /a /r /f1c:\temp\record.iss`**. `setup.exe is the name of the install package. c:\temp\record.iss` is the full path filename to save the recorded output.
   b. Install package is a **set** of files. Run **`setup.exe /r /f1c:\temp\record.iss`**. `setup.exe is the name of the install package. c:\temp\record.iss` is the full path filename to save the recorded output.
3. Deploy the install package with the recorded dialog box responses. Write both the vendor's install package and `record.iss` to each managed machine or a file server accessible by each machine.
4. Execute the install package with silent mode command line parameters using the Execute File script function.
   a. Install package is a **single** file. Run **`setup.exe /s /a /s /f1c:\temp\record.iss`**. `setup.exe is the name of the install package. c:\temp\record.iss` is the full path filename location of the recorded settings.
   b. Install package is a **set** of files. Run **`setup.exe /s /f1c:\temp\record.iss`**. `setup.exe is the name of the install package. c:\temp\record.iss` is the full path filename location of the recorded settings.

Silent Installs with Windows Installer

Windows Installer does not have a record mode. As such it can only silently install the "**Typical**" install configuration. To silently install a Windows Installer package write a script to perform the following:

1. Write the vendor's install package to each managed machine or a file server accessible by each machine.
2. run the install package with the **/q** parameter using the Execute File script function.

Silent Installs with Wise Installer

Wise Installer does not have a record mode. As such it can only silently install the "**Typical**" install configuration. To silently install a Wise Installer package write a script to perform the following:

1. Write the vendor's install package to each managed machine or a file server accessible by each machine.
2. run the install package with the **/s** parameter using the Execute File script function.

Assistant

Assist Packager

Show me an explanation of the items on this page.

How do I deploy the software vendor's install package?

Most vendors provide either a single file (when downloaded from the web) or set of files (when distributed on a CD). Executing the installer file (typically named **setup.exe**) installs the vendor's application on any operating system.

Deploy the vendor's install package by writing a script to do the following:

1. Write the file or files to a location accessible by the remote machine (either the machine itself or a file server accessible by the remote machine).
2. Execute the installer on the remote machine.

Note: Using the vendor's installer typically requires users to answer questions during the install process. See Creating Silent Installs to create a package that does not require any user interaction.

Information on creating custom scripts...

What does the Packager do?

Each package is OS dependent. To deploy to multiple OS's, you need to build a package for each OS. During installation, Packager checks the OS and does not continue if the package is being deployed on an OS different than the source OS.

Close all applications before running Packager. This prevents open applications from modifying the system during package creation.

Packager picks up everything you do to a machine between the time you take the first snapshot and create the package. Be careful what additional tasks you perform on the source machine as any system changes will be rolled into the package.

What if installation fails? The Packager has complete rollback capability. The Rollback executable and associated restore files are located in the Agent directory on the target machine in the directory C:\Program Files\Kaseya\KPackage.

How do I create a Package?

1. Download and execute the Packager application.
2. The Packager takes a snapshot of the source system.
3. Install any application and/or resource on the source system.
4. Execute the Packager application again. The Packager records the changes in the source system and creates a Package file.
5. Distribute the Package file any way you like. You can e-mail it, or store it on a server where a custom script can perform a silent installation on any managed machine.

Information on creating custom scripts...

Monitor Tab

The Monitoring tab contains functions related to monitoring of Machines and SNMP Devices.
The following functions are available in the Monitoring feature tab:

Functions	Description
View Console	Multiple monitoring views to display summary of monitoring status.
Layout Console	Administrators can customize the View Console page.
Alarm Summary	List of alarms for monitored machines.
Suspend Alarms	Suspend alarm notifications for specific Machine IDs.
Live Connect	Real time view of monitor counter objects.
Monitor Lists	Configure the monitor list objects for monitoring.
Update Lists By Scan	Scan machines for monitor counters and services.
Monitor Sets	Configure monitor sets.
SNMP Sets	Configure SNMP monitor sets.
Add SNMP Object	Manage SNMP MIB objects.
Alerts	Configure monitor alerts for machines.
Assign Monitoring	Assign, remove and manage alarms of monitor sets on machines.
Monitor Log	View monitor log data in chart and table format.
System Check	Assign, remove and manage alarms for system checks on machines.
SNMP Community	Install and Remove SNMP Community settings for machines. Allowing for SNMP Device monitoring.
LAN Watch	Scan network range for specifice SNMP enabled devices.
Assign SNMP	Assign, remove and manage alarms of SNMP monitor sets on devices.
SNMP Log	View SNMP log data in chart and table format.
Set SNMP Values	Set SNMP values on the specified device.

Monitor > View Console

The console gives you a quick view of monitoring health, highlighting the alarms and items you need to work on first. In addition to viewing system monitoring at a glance, you can put each monitoring item in it's own browser window and customize the window position. Customize the console display with the Layout function. Alarm icons will be used in views to display current alarm status. By default if a machine has any open alarms it will display a **red** monitoring icon, if no alarms are open a **green** monitoring icon will display. If there are no alarms and a trending alarm is open an **orange** monitoring icon will display.

Alarm Status

Displays all alarms relating to all machine IDs that match the current machine ID / group ID filter. The display lists the most recent alarms first. By default, alarms generated within the **last 24 hours** are highlighted in **red**. Alarms generated within the **last week** display in **yellow**. The color coding lets you quickly distinguish alerts you may not have examined yet. The color coding is customizable. Each alarm contains a link to **Open or Close** alarm, create or view **Ticket** associated to this alarm**,** a icon link to display monitor log information if it applies and an expand icon to display alarm information.

Group Alarm Status

Summarizes the alarm status of all Group IDs/machine IDs that have monitoring assigned. Monitoring includes Agent Monitoring, Alerts, SNMP Monitoring and System Checks. Each Group IDs/Machine IDs will collect alarms in the Group Alarm Column assigned within the Define Monitor Set function. Gives you an at-a-glance status of the of how many open alarms for the selected view. By clicking the **Machine ID/SNMP Device ID** link the Monitor Set Status view will be opened in a new browser window.

Monitor Set Status

Displays all monitoring objects relating to all machine IDs that match the current machine ID / group ID filter. Displaying an expandable view of each Machine IDs monitor set objects. These monitoring objects include Agent Monitoring, Alerts, SNMP Monitoring and System Checks. Each Monitoring level will display the monitoring icons to give you a current status of the object selected.

Parent Machine ID/SNMP Device objects display total summary of the status of all the monitoring objects for that machine. Containing a link to Monitoring Summary, and the ability to expand all monitoring objects by clicking the expand all icon.

Agent Monitoring objects display a summary of the alarm status, link to Quick Status Charts, link to Monitor Log, link to Live Connect and a link to Alarm Summary that contains the number of open alarms.

Alert Monitoring and System Check Monitoring objects display a summary of the alarm status, and a link to Alarm Summary that contains the number of open alarms.

SNMP Monitoring objects display a summary of the alarm status, link to SNMP Log and a link to Alarm Summary that contains the number of open alarms.

Monitor Status Chart

Bar Chart showing the number of alarms created for the selected time interval and machines matching the current machine ID / group ID filter.

Machines Online Chart

Chart showing the percentage of machines online for the machines matching the current machine ID / group ID filter.

Top 'N' Daily Monitor Alarm Chart

Bar Chart showing the number of alarms created for the **TOP "N" machines** for the selected time interval and machines matching the current machine ID / group ID filter. The chart will show up to 10 machines and it will select the machines with the most alarms.

Monitor > Layout

Each View Console item appears as a vertical section. Layout control lets you view/hide each item and set the order, from top to bottom, they appear. To display an item, simply check the box next to the item.

Four items have addition customization controls: **Monitor Set Status, Alarm Status, Chart Total Monitor Alarms and Chart Top N Monitor Alarms**.

Alarm sounds can be turned on for the **Monitor Set Status, Alarm Status** items**.**

The **Chart Total Monitor Alarms** and **Chart Top N Monitor Alarms** background and title colors are customizable. Each chart parameter is customizable, this includes the chart time interval and the number of machines in the **Top N Monitor Alarms** chart.

The **Alarm Status** display has time dependent data for monitor alarms. To make it easy to quickly distinguish new item from old items, you can specify different highlight colors from data rows depending on how recently the data item was generated.

Highlight the most recent items in red. All items created in the last N days are shown in red.

Items created in the last <enter number here> days

Highlight the next most recent items in yellow. All items that are older than the red highlight date but more recent than the number entered here are shown in yellow.

Items created in the last <enter number here> days

Disable highlighting by setting the number of days to zero.

The number of rows shows for **Alarms** may also be customized.

Monitor > Alarm Summary

Alarm Summary view displays alarms for all machine IDs that match the current machine ID / group ID filter. Each row displays summary data for a single alarm. You can further filter listed alarms with any field in the **Alarm Filter** section. The alarms are sorted by alarm date/time with the most current alarms displaying first.

Alarm Filters

The following are additional filters for alarms:

1. **Alarm ID** - A specific alarm ID can be searched for.
2. **Monitor Type** - Alarms for monitor types of Counter, Process, Service, SNMP, Alert or System Check can be searched for.
3. **Alarm State** - Alarms or state Open or Closed can be searched for.
4. **Alarm Type** - Alarms of type Alarm or Trending can be searched for.

Update Alarms

Clicking the **Update** button will apply the selected alarm status and notes to the selected alarms.

Deleting Alarms

Clicking the **Delete** button will delete the selected alarms.

Select All/Unselect All

Select All will select all all alarms on all alarm pages. Unselect All will unselect selected alarms on all alarm pages. For individual alarms, select the checkbox next to the alarm ID.

ID

System generated unique ID for each alarm. The plus/minus icon can be clicked to display specific alarm information.

Machine.Group ID

Lists the agent machines the alarm is assigned to.

Machine.Group ID

Lists the agent machines the alarm is assigned to.

State

Current state of alarm, can be **Open** or **Closed**. The data will display as a link, if the administrator clicks the link the state of the alarm clicked will change. For example, if the administrator clicks the Open link on a specific alarm it's state will change from **Open** to **Closed**.

Alarm Date

Date and Time the alarm was created.

Type

Type of monitor object which includes: Counter, Process, Service, SNMP, Alert and System Check.

Ticket

A ticket can be created from an alarm. If no ticket has been generated for an alarm a link to create a new ticket is displayed New Ticket.... This link can be clicked and a new ticket will be created for this alarm. If a ticket has been generated for the alarm a link with the Ticket ID will display allowing the administrator to view that ticket.

Name

Name of the monitoring object.

Monitor > Suspend Alarms

Allows the user to specify a recurring duration of time period during which all Alarms will be suppressed. This allows for a defined window of time to be set

so upgrade and maintenance activity can take place without generating Alarms. **The Agent is still collecting data, but will not generate corresponding alarm**s.

Schedule

Specify a time of day to restore the image. Remember, the restore will reboot the machine and restore the image without warning the user first.

Run recurring

Schedule selected machines to suspend Alarms on a repeating scheduled basis.

Suspend alarms

Select a duration of time during which the Alarms will be suspended.

Monitor > Live Connect

Live Connect displays current monitor counter log information at a faster check in rate of up to every 3 seconds. Live connect works with all Monitor Counters objects that return numeric values. Each specific live connect is placed in a new window to allow for multiple views.

Machine Picker

Machine IDs are displayed as links to be selected for live connect.

Monitor Set

Each monitor set applied to the Machine ID selected will be displayed in the select list.

Refresh Rate

Value from 3 to 60 will be the interval which live connect will gather data.

Select Counter

List of links containing all monitor counters within the monitor set selected. When the counter link is clicked a new window will open displaying the live connect chart.

Live Connect Window

A new window will be created for each live connect counter object. Each window will display a bar chart with 75 data points containing the value of the counter object for the **Refresh Rate** specified. The new data will be displayed on the far right of the chart and the data will move from right to left as it ages.

Each Bar within the chart will display in a specific color which is determined by the alarm and warning thresholds of the Monitor Set Counter object. The bar will display **RED** if alarming, **YELLOW** if within warning threshold and **GREEN** if not alarming or in warning threshold.

Monitor > Monitor Lists

This operation allows the user to edit any of the lists used in creating Monitor or SNMP Sets.

Note: The Counter Objects, Counters, Instances and Services lists can be initially populated with the Update Lists by Scan feature. Additionally these lists, as well as Services, Processes can be populated with the import of a Monitor Set . MIB OIDs can be populated with the Add SNMP Object feature or the import of a SNMP Set.

Counter Objects

Presents a list (or opportunity to add a list) of Counter Objects required by the edit Monitor Set feature. That feature uses the PerfMon combination of Object/Counter/Instance to collect counter information. **Counter Objects are the primary reference (the user needs to create this record first) before adding a Counter or Instance (both secondary records).**

Counters

Presents a list (or opportunity to add a list) of Counters required by the edit Monitor Set feature. That feature uses the PerfMon combination of Object/Counter/Instance to collect counter information. **Counters are a secondary reference (the user needs to create a Counter Object record first) and the entry will ask the user to select the Counter Object that the Counter is associated to.**

Instances

Presents a list (or opportunity to add a list) of Instances required by the edit Monitor Set feature. That feature uses the PerfMon combination of Object/Counter/Instance to collect counter information. **Instances are a secondary reference (the user needs to create a Counter Object record first) and the entry will ask the user to select the Counter Object that the Instance is associated to.**

Note: Although it is required by the use of Windows PerfMon that a Counter Object have at least one Counter associated, it is not required that an Instance be available.

Services

Presents a list (or opportunity to add a list) of Windows Services required by the edit Monitor Set feature to monitor the activity of a Windows Service. This list can also be populated with the execution of the Update Lists By Scan feature OR the import of a Monitor Set.

Processes

Presents a list (or opportunity to add a list) of Windows Processes required by the edit Monitor Set feature when monitoring for the transition of a process (equivalent to an application) to or from a 'Running' state. This list is NOT populated via the Update Lists by Scan feature.

MIB OIDs

Presents a list (or opportunity to add a list) of SNMP MIB Objects required by the edit SNMP Sets feature to monitor the activity of a SNMP Agents . This list can be populated with the import of a SNMP Set OR the execution of the Add SNMP Object feature. MIB Objects are references to values that can be monitored on SNMP Agents (for example: the MIB Object of 'sysUptime' returns how much time has passed since the device was powered-up.)

SNMP Devices

Presents a list (or opportunity to add a list) of SNMP Devices that are used in the 'Auto Deployment' of SNMP Sets. The user will select from this list, if they want a particular SNMP Set to be automatically deployed once the LAN Watch discovers SNMP Agent it 'thinks' corresponds to the item selected from this list (see the next paragraph on SNMP Services).

SNMP Services

Presents a list (or opportunity to add a list) of SNMP Services that are used in determining what type of SNMP device responding to the LAN Watch function. An SNMP Agent will respond to the LAN Watch function by saying what 'sysServices' it provides. From this number and the devices it is related to in the SNMP Devices list, the system interprets what type of SNMP Device has been discovered. This table comes 'seeded' with information on basic devices. System updates (or customers themselves) may update this table form time to time.

'VCR' buttons ('<<' or '>>')

Page the list of results.

Page 'Drop Down' list

Presents a list of the first record of each page, allowing the user to directly 'page' to the desired records.

Delete Icon

Will delete, with confirmation' the selected record.

Edit Icon

Will open up the Edit interface.

Save Button

Will save any changes.

Cancel Button

Will ignore any changes and return to the list of records.

Monitor > Update Lists By Scan

This operation allows the user to scan one or more machines under management and return lists of counter categories, counters, instances and services to select from when creating or editing a monitor set.

Scan

Executes a scan on the selected machines that will gather available categories, counters, instances and services from the selected machines.

Cancel

Will cancel a scan that is in a pending status.

Select All

Selects (checks) all of the listed machines.

Un-select ALL

Removes the selection (checks) from all of the listed machines.

Machine Group ID

The name and group of the machine that can be selected.

Status

This will indicate whether a scan is pending or when the last scan was completed.

Monitor > Monitor Sets

This operation allows the user to add, import or modify a Monitor Set. **Not all monitor sets will be available for editing, since the creator of a Monitor Set may only have shared the use of the monitor set but not the view or editing of the set.**

Open

Opens the Define Monitor Set function in the edit mode of the Monitor Set feature.

Add

Opens the a form that asks the user to:

1. **Name** the Monitor Set
2. **Describe** the Monitor Set
3. **Select the Group Alarm Column** from the list of column names that are displayed in the Group Alarm Status window under View Console.

Save (button) Opens the Define Monitor Set function in the edit mode of the Monitor Set feature with the Monitor Set and Description already saved and populated.

Import

Opens the Import Monitor Set function of the Monitor Set feature.

VCR Buttons ('<<' and '>>')

Provide paging through the list of monitor sets. If there are more than one page of Monitor Sets a **paging 'drop down' list** appears for rapid navigation to a specific page.

Monitor > SNMP Sets

This operation allows the user to add, import or modify a SNMP Set. **Not all SNMP Sets will be available for editing, since the creator of a SNMP Set may only have shared the use of the set but not the view or editing of the set.**

Note: Certain Command Line functions from Net-SNMP suite of applications are used to implement SNMP v1, SNMP v2c retrieval of information from SNMP capable devices in accordance with all pertinent copyright requirements.

Open (button)

Opens the Define SNMP Set function in the edit mode of the SNMP Set feature.

Add (button)

Opens the a form that asks the user to:

1. **Name** the SNMPSet
2. **Describe** the SNMP Set
3. **Select Automatic deployment** to certain devices. If the Lan Scan /SNMP discovery detects this type of SNMP device the system will automatically deploy the create SNMP set.
4. **Select the Group Alarm Column** from the list of column names that are displayed in the Group Alarm Status window under View Console.

Save (button) Opens the Define SNMP Set function in the edit mode of the SNMP Set feature with the SNMP Set Name and Description already saved and populated.

Import (button)

Opens the Import SNMP Set function of the SNMP Set feature.

VCR Buttons ('<<' and '>>')

Provide paging through the list of SNMP Sets. If there are more than one page of SNMP Sets a **paging 'drop down' list** appears for rapid navigation to a specific page.

Monitor > Add SNMP Object

This operation allows the user load a MIB (SNMP Management Information Base) file into a 'tree view'. Once in the 'tree view' the user can select those Objects (values available to monitor) they wish to monitor via the SNMP Sets feature.

Note: This is considered a feature for advanced users because it is the goal of the system designers to provide many SNMP Sets that can be imported into the user's system with all the monitoring levels set as examples.

Load MIB (Button)

Executes a load file dialog. If the system does not have standard SNMP files that are considered required by most MIBs, it will load them automatically (these files are considered MIB II: snmp-tc, snmp-smi, snmp-conf, rfc1213, rfc1759). Once the file is loaded, the MIB Tree located at the bottom of the page can be opened and navigated to find the new Objects that the user can select. Most private vendor MIBs will be installed under the Private folder (see MIB Tree below).

Select Mib Object (step2)

Selects (checks) all of the Object 'leaves' that the user wants to be available in the SNMP Sets feature. .

Add MIB Objects (button)

Adds the Objects selected to the MIB Object list used in the SNMP Sets feature.

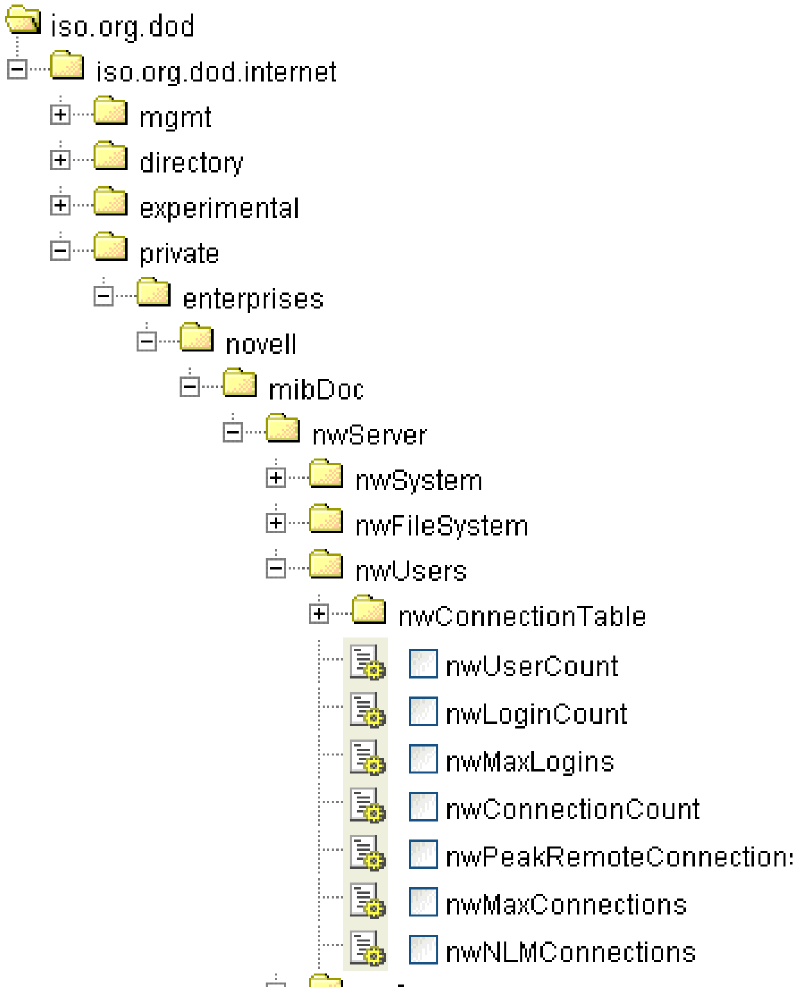
Remove MIB (button)

After selections have been made the MIB file can be removed. The size of the MIB Tree can become so large that it is hard to navigate. THis function cleans that process up.

Note: The MIB File can be loaded and removed at any time and does NOT affect any MIB Objects that have been selected for use or any MIB Objects that have already deployed to SNMP Sets.

MIB Tree

Represents all the MIB files that are currently loaded for the user to select from.



```
iso.org.dod
⊟ iso.org.dod.internet
    ⊞ mgmt
    ⊞ directory
    ⊞ experimental
    ⊟ private
        ⊟ enterprises
            ⊟ novell
                ⊟ mibDoc
                    ⊟ nwServer
                        ⊞ nwSystem
                        ⊞ nwFileSystem
                        ⊟ nwUsers
                            ⊞ nwConnectionTable
                               □ nwUserCount
                               □ nwLoginCount
                               □ nwMaxLogins
                               □ nwConnectionCount
                               □ nwPeakRemoteConnection:
                               □ nwMaxConnections
                               □ nwNLMConnections
```

Monitor > Assign Monitoring

You can assign monitor sets to any Machine that has an operating system of Windows 2000 or newer. Each monitor set assignment can include the following alarm parameters:

- Create Alarm (always checked)
- Create Ticket
- Run Script after alarm: select script on this machine ID
- Email Recipients

If you check any of these boxes the action will be performed on the monitor set for that machine when an alarm is created. You can select monitor sets from the Select Monitor Set list to apply to machine IDs. To add/edit monitor sets go to the Monitor Sets function. **You may assign more than one monitor set to the same machine.**

Apply
Applies the selected monitor set to the checked machine IDs.

Clear
Clears the selected monitor set from the checked machine IDs.

Clear All
Clears all the monitor sets from the selected machine IDs.

Create Alarm
The **Create Alarm** check box is always checked. This will create an alarm for any monitor set object that goes into alarm threshold.

Create Ticket
When an alarm is generated you can set up the system to automatically generate a new ticket at the same time the alarm is created. This new ticket will be associated to the new alarm.

Run Script after alarm
When an alarm is generated you can set up the system to automatically run a script at the same time the alarm is created. You can run the script on the machine that generated the alarm or any other machine you wish.

Email Recipients
Email address where the alarm notification is sent. You can specify a different email address for each agent machine, even if it is for the same alarm. The "From:" email address is specified in the Server Info function of the System feature tab. The alarm notification may be sent to more than one email address by putting a comma before each additional address.

Add to current list
Select this radio button to add the email address to the current list of recipients for that alarm. If the name is already on the list for a selected machine ID, then any changes to alarm settings are applied but the address list remains the same.

Replace list
Set the recipient email list for this alarm to the list entered. This over-writes any existing email list.

Remove
Remove an email address from the recipient list for all selected machines **without modifying any alarm parameters**. Use this button to quickly remove an email address for alarms without having to worry about setting up alarms parameters.

Format Email
Change the default message sent with each email alarm by clicking this button.

Select Monitor Set
Select list containing monitor sets that can be applied to Machine IDs. To add/edit monitor sets go to the Define Monitor Set function.

Add Monitor Set
When a monitor set is applied to Machine IDs, the selected monitor set will be added to the list of

current monitor sets on that Machine.

Replace Monitor Set(s)

When a monitor set is applied to Machine IDs, the selected monitor set will be added to the Machine replacing all monitor sets deployed to that Machine.

Machine.Group ID

Lists the agent machines according to the Specify Accounts criteria.

Monitor Sets

List of monitor sets that have been assigned to Machine ID.

ATSE

Assign monitoring parameters to execute when an alarm is created:

- **A** = Create Alarm
- **T** = Create Ticket
- **S** = Run Script
- **E** = Email Recipients

Email Address

List of Email Addresses to notify when an alarm is created for the specific monitor set.

Monitor > Monitor Log

The Monitor Log page displays the agent monitoring object logs in chart and table formats. A list of Machine IDs that have monitor sets applied will display to view monitor log data. If no Machine IDs display go to the Assign Monitoring function to apply monitor sets. Clicking the Machine ID will display all agent monitoring objects to view.

Machine Selection List

All machines with agent monitoring sets assigned will be displayed that match the current machine ID / group ID filter. Clicking the Machine ID will display all agent monitoring objects to view.

Select monitoring object to display information

A listing of monitoring objects to view by either chart or table. If the object can't be represented by a chart only the table view will be accessible.

View

Each row in the monitor objects list will contain a link to view the log data. If selected the chart or table will be displayed, the row selected will be changed to bold text. Only one row can be viewed at a time.

Type

Displays type of monitor object: Counter, Process or Service.

Monitor Set Name

Name of monitor set of the monitor set object.

Object Name

Name of the monitor object.

Bar Chart or Table

Radio button to display data in Bar Chart or Table format. Only monitor objects of type **Counters** can be displayed in Bar Chart format.

Bar Chart displays the last 500 data points at the sample interval rate. The background of the chart will display RED for alarm threshold, yellow for warning threshold and green. See the Define Monitor Set for more information.

Table log data will display most current values first and display alarm and warning icons on log data that falls within these thresholds. See the Define Monitor Set for more information.

Log rows per Page

Only displays for log data being displayed in Table format. Select number of rows to display per page.

Refresh

Click the refresh button to display the most current log data.

TIPS for non responsive monitors

Monitor No Values

If your monitor doesn't show any log values please verify the following.

1. For Monitor Counters check the sample interval, once a monitor set is deployed it will return values to the monitor log at the sample interval. Please wait for the sample interval plus the agent check in interval for the first value to come back.
2. If there are no values returned, check Collection Threshold for the Monitor Counter commands. If no values on the monitored machine or device meet the collection threshold they will not be inserted into the monitor log.

Monitor Not Responding

If a monitor isn't responding the log will display a message within the graph and in the table listing stating the **Monitor Not Responding**. There can be several reasons for no response from the monitor;

1. If all values returned to the Monitor Counter, Service, Process are **Not Responding, Service**

Does Not Exist or Process Stopped the monitor object doesn't exist on the agent.

- **Counters:** With windows counters, you may deploy a counter that doesn't exist on the specific operating system on the agent machine. Use the Update Lists By Scan function in the Monitor Tab to pull all specific monitor counters and services from a specific machine. Connect to the agent machine, select the RUN COMMAND within the start menu, type in **perfmon.exe** click OK**,** create a new Counter Log, and check for the existence of the monitor counters, objects and instances for the specific monitor counter that isn't responding.
- **Services:** If you deploy a monitor service to a machine that doesn't contain that service your log will contain a message that states **Service Does Not Exist**.
- **Processes:** If you deploy a monitor process to a machine that doesn't contain that process your log will contain a message that states **Process Stopped**.

Monitor > System Check

You can assign System Checks to any Machine ID. System Checks will create an alarm if the specified check fails. Each System Check assignment can include the following alarm parameters:

- Create Alarm (always checked)
- Create Ticket
- Run Script after alarm: select script on this machine ID
- Email Recipients

If you check any of these boxes the action will be performed on the System Check for that machine when an alarm is created. **You may assign more than one System Check to the same machine.**

Apply
Applies the selected System Check to the checked machine IDs.

Clear
Clears all System Checks from the checked machine IDs.

Create Alarm
The **Create Alarm** check box is always checked. This will create an alarm for any monitor set object that goes into alarm threshold.

Create Ticket
When an alarm is generated you can set up the system to automatically generate a new ticket at the same time the alarm is created. This new ticket will be associated to the new alarm.

Run Script after alarm
When an alarm is generated you can set up the system to automatically run a script at the same time the alarm is created. You can run the script on the machine that generated the alarm or any other machine you wish.

Email Recipients
Email address where the alarm notification is sent. You can specify a different email address for each agent machine, even if it is for the same alarm. The "From:" email address is specified in the Server Info function of the System feature tab. The alarm notification may be sent to more than one email address by putting a comma before each additional address.

Add to current list
Select this radio button to add the email address to the current list of recipients for that alarm. If the name is already on the list for a selected machine ID, then any changes to alarm settings are applied but the address list remains the same.

Replace list
Set the recipient email list for this alarm to the list entered. This over-writes any existing email list.

Remove
Remove an email address from the recipient list for all selected machines **without modifying any alarm parameters**. Use this button to quickly remove an email address for alarms without having to worry about setting up alarms parameters.

Format Email
Change the default message sent with each email alarm by clicking this button.

System Check Parameters
Select a System Check Type:

- **Web Server -** Enter URL to Poll at a selected time interval.
- **DNS Server -** Enter DNS address (name or IP) to poll at a selected time interval.
- **Port Connection -** Enter address (name or IP) to connect to and port number to connect to at a selected time interval.
- **Ping -** Enter address (name or IP) to ping at a selected time interval.
- **Custom -** Enter path to a custom program with parameters to run at a selected time interval.

Add (System Check)

Add System Check to selected Machine IDs.

Replace (System Check)

Add System Check to selected Machine IDs over-writing all System Checks.

Replace (System Check)

Remove selected System Check from selected Machine IDs.

Edit Icon

Load the selected System Check into the System Check Parameters to allow the administrator to update and re-apply.

Machine.Group ID

Lists the agent machines according to the Specify Accounts criteria.

ATSE

System Check parameters to execute when an alarm is created:

- **A** = Create Alarm
- **T** = Create Ticket
- **S** = Run Script
- **E** = Email Recipients

Email Address

List of Email Addresses to notify when an alarm is created for the specific monitor set.

Type

System Check Type: Web Server, DNS Server, Port Connection, Ping and Custom.

Interval

Reoccurring time interval System Check is executed.

Monitor > SNMP Community

SNMP Community sets and applies the Read Community value to a selected machine(s), so that the selected machine can have access to the SNMP agents. This is the first step in collecting SNMP monitor data. The Read Community value is simply a password for allowing read access to SNMP Agents. The default Read Community value is 'public'.

Note: Once the Community Read values (password) has been applied to a machine that will act as the collector of SNMP data, the next step is to schedule a LAN Watch to discover SNMP devices within an IP address range.

Note: If there are multiple Read Community Names, each will have to be assigned to a different machine. That machine will then have the duty of scanning and attaining SNMP data for the community read name that was applied to it.

Set Community
Applies the value the user has set in the Read Community Name field to the machine or machines that have been selected.

Remove
Removed the Read Community Name that had been applied to the machine or machines that have been selected.

Read Community Name
Enter the value of the SNMP Community read password.

Confirm
Enter the SNMP Community read password again for confirmation.

Select All
Selects (checks) all of the listed machines.

Un-select ALL
Removes the selection (checks) from all of the listed machines.

Machine Group ID
The name and group of the machine that can be selected

Community Set
This will indicate whether the machine has a Read Community value applied, or if the machine needs to have the agent updated.

Monitor > LAN Watch

LAN Watch periodically scans the local area network **of the designated Client** for any and all new devices connected to that the LAN since the last time LAN Watch ran. Optionally, the VSA sends an **alert** when LAN Watch discovers any new device. LAN Watch effectively uses the Client as a proxy to scan a LAN behind a firewall that would not normally be accessible from a remote server. **Additionally, the LAN Watch looks for and identifies if any new device is SNMP aware (responds to SNMP requests).**

NOTE: The user will only be presented with machines that have already applied the SNMP Community value.

There are reasons to do a LAN Watch on multiple machines within a scan range: 1.) There are multiple SNMP Communities within the scan range and therefore there have been multiple machines with different SNMP Community Read values. 2.) The user wishes to have redundant SNMP Monitoring.

What does LAN Watch do?

LAN Watch periodically checks the local area network looking for any and all new devices connected to the LAN since the last time LAN Watch ran. Optionally, the VSA sends an **alert** when LAN Watch discovers any new device. Additionally, if the machine the LAN Watch has been scheduled on has had a SNMP Community Read value applied, it will discover any new SNMP aware devices in the same scan range.

Is it necessary to run LAN Watch for SNMP Devices on more than one machine on the same LAN?

There are only two reasons to do a SNMP LAN Watch on multiple machines within a scan range: 1.) There are multiple SNMP Communities within the scan range and therefore there have been multiple machines with different SNMP Community Read values. 2.) The user wishes to have redundant SNMP Monitoring.

NOTE: LAN Watch will not scan more than 65,536 IP addresses. If the specified IP address range is larger than 65,536 then LAN Watch will truncate it to 65,536 addresses.

How long does a LAN Watch scan take?

The scanner pings every IP address in the specified range. If a device exists at that address, the response comes back right away. The scanner times out after 200ms if no device exists at that address. If you scan the **maximum range of 65,536** addresses, the scan may take up to **3.6 hours** to complete if very few of the addresses reply to the ping.

NOTE: The system automatically adjusts the recurring interval to be longer than the maximum scan time as defined by number of IP addresses at 200ms per address.

What triggers a LAN Watch alert?

An email alert is sent to all email addresses listed in Email Recipients when a new device is discovered by LAN Watch.

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

Explanation of items on this page

Scan Button

Click Scan to schedule a recurring LAN Watch scan on each machine selected (with the check box) from the list of displayed machine IDs. The scan runs every interval that you set (default is 1 day).

NOTE: LAN Watch will not scan more than 65,536 IP addresses. If the subnet mask of the machine running LAN Watch specifies a larger IP range, LAN Watch will truncate it to 65.536 addresses.

Cancel Button

Click Cancel to stop the scheduled scan from running any more. Cancel also deletes all records of the devices identified on a LAN from the VSA. If you re-schedule LAN Watch, after clicking Cancel, each device on the LAN will generate a new alert.

Scan 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**.

Alert when new device appears on LAN

Checking this box sends an alert to all email addresses listed in Email Recipients when a new device is discovered by LAN Watch.

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

Email Recipients

Email address where the event notification is sent. You can specify a different email address for each client machine, even if it is for the same event. The "From:" email address is specified in the Server Info function of the System feature tab.

Machine.Group ID

Lists the client machines according to the Specify Accounts criteria.

IP Range

The IP addresses that will be scanned by the selected Client when LAN Watch runs.

Last Scan

Timestamp showing when the last LAN Watch scan ran on a machine. When this date changes, new LAN Watch data has been processed and is available for viewing

Recurring Interval

The time interval used to determine how often LAN Watch runs.

Alert Active

A check mark appears if LAN Watch alerts are enabled for this scan. If checked, then an email alert is sent every time LAN Watch discovers a new device on the LAN. Email notification addresses may be viewed and/or edited in the Alerts function.

Monitor > Assign SNMP

SNMP Monitoring is managed by a specific Machine ID(SNMP Relay) that will perform SNMP Commands on the Devices. Machines with an SNMP Community applied will show up in the Machine ID list. To add a machine as a SNMP Relay go to the SNMP Community function. By clicking the machine (SNMP Relay) a list of SNMP Devices will be displayed, if no Devices are displayed go the the LAN Watch function to scan for new devices.

SNMP Sets can be applied to a any device with the following parameters.

- Create Alarm (always checked)
- Create Ticket
- Run Script after alarm: select script on this machine ID
- Email Recipients

If you check any of these boxes the action will be performed on the monitor set for that device when an alarm is created. You can select monitor sets from the Select Monitor Set list to apply to machine IDs. To add/edit monitor sets go to the SNMP Sets function. **You may assign more than one monitor set to the same device.**

Apply

Applies the selected monitor set to the checked device(s).

Clear

Clears the selected monitor set from the checked devices(s)

Clear All

Clears all the monitor sets from the selected device(s).

Create Alarm

The **Create Alarm** check box is always checked. This will create an alarm for any monitor set object that goes into alarm threshold.

Create Ticket

When an alarm is generated you can set up the system to automatically generate a new ticket at the same time the alarm is created. This new ticket will be associated to the new alarm.

Run Script after alarm

When an alarm is generated you can set up the system to automatically run a script at the same time the alarm is created. You can run the script on the machine that generated the alarm or any other machine you wish.

Email Recipients

Email address where the alarm notification is sent. You can specify a different email address for each device, even if it is for the same alarm. The "From:" email address is specified in the Server Info function of the System feature tab. The alarm notification may be sent to more than one email address by putting a comma before each additional address.

Add to current list

Select this radio button to add the email address to the current list of recipients for that alarm. If the name is already on the list for a selected device, then any changes to alarm settings are applied but the address list remains the same.

Replace list

Set the recipient email list for this alarm to the list entered. This over-writes any existing email list.

Remove

Remove an email address from the recipient list for all selected machines **without modifying any alarm parameters**. Use this button to quickly remove an email address for alarms without having to worry about setting up alarms parameters.

Format Email

Change the default message sent with each email alarm by clicking this button.

Select Monitor Set

Select list containing monitor sets that can be applied to device(s). To add/edit monitor sets go to the Define SNMP Set function.

Add Monitor Set

When a monitor set is applied to device(s), the selected monitor set will be added to the list of current monitor sets on that Machine.

Replace Monitor Set(s)

When a monitor set is applied to device(s), the selected monitor set will be added to the device replacing all monitor sets deployed to that device.

Name

List of SNMP devices generated for the specific Mahcine ID by the LAN Watch function.

Device IP

IP Address of device.

MAC Address

MAC Address of device.

SNMP Info

SNMP Device information.

SNMP Sets

List of monitor sets that have been assigned to the device.

ATSE

Assign monitoring parameters to execute when an alarm is created:

- **A** = Create Alarm
- **T** = Create Ticket
- **S** = Run Script
- **E** = Email Recipients

Email Address

List of Email Addresses to notify when an alarm is created for the specific monitor set.

Monitor > SNMP Log

The SNMP Log page displays the SNMP monitoring object logs in chart and table formats. A list of Machine IDs that have SNMP monitor sets applied will display to view monitor log data. When clicking the Machine ID all devices will display for the Machine SNMP Relay. If no Machine IDs display go to the SNMP Community function to assign a new SNMP Machine Relay machine. If no devices display for the selected machine go to the LAN Watch function. When clicking a specific device a list of SNMP Monitor objects will display to view log data.

SNMP monitor objects can contain multiple instances and be viewed together within one Chart or Table. For example, a network switch may have 12 ports, each is an instance and can contain log data. All 12 instances can be combined in one Chart or Table. SNMP Bar Charts are in 3D format to allow for multiple instance viewing.

Machine / Device Selection List

All machines assigned to SNMP Monitoring will be displayed that match the current machine ID / group ID filter. Clicking the Machine ID will display all devices assigned to this machine ID. Click the device to display all snmp monitor objects assigned to the device.

Select monitoring object to display information

A listing of monitoring objects to view by either chart or table. If the object can't be represented by a chart only the table view will be accessible.

View

Each row in the monitor objects list will contain a link to view the log data. If selected the chart or table will be displayed, the row selected will be changed to bold text.

Remove

Remove data from Chart or Table.

View All

If the SNMP monitor object has multiple instances, clicking the view all link will display all data for every instance.

Remove All

If the SNMP monitor object has multiple instances, clicking the remove all link remove all data displaying for each instance.

Monitor Set Name

Name of monitor set of the monitor set object.

GET Object Name

Name of the monitor object.

Description

Description of monitor object.

Bar Chart or Table

Radio button to display data in Bar Chart or Table format. Only monitor objects of type **Counters** can be displayed in Bar Chart format.

Bar Chart displays the last 500 data points at the sample interval rate. The background of the chart will display RED for alarm threshold, yellow for warning threshold and green. See the Define Monitor Set for more information.

Table log data will display most current values first and display alarm and warning icons on log data that falls within these thresholds. See the Define Monitor Set for more information.

Display Last

Bar Charts will log data for the last interval selected. This interval will be split up into 500 data elements for each bar to display in the chart. For example, if you selected **Display Last** 500 minutes, each bar in the chart would represent 1 minute.

Save View

The administrator can save custom views for each monitor object. The next time this monitor object is selected the saved information will be loaded.

Log rows per Page

Only displays for log data being displayed in Table format. Select number of rows to display per page.

Refresh

Click the refresh button to display the most current log data.

TIPS for non responsive monitors

Monitor No Values

If your monitor doesn't show any log values please verify the following.

1. If there are no values returned, check Collection Threshold for the SNMP Get commands. If no values on the monitored machine or device meet the collection threshold they will not be inserted into the monitor log.
2. The log value sample interval is determined by the number of SNMP commands within the SNMP Probe.   The more SNMP Get commands the larger the sample interval. Check all devices within the SNMP Probe, if some are returning values then you SNMP Get Command isn't compatible, see step 3.

Monitor Not Responding

If a monitor isn't responding the log will display a message within the graph and in the table listing stating the **Monitor Not Responding**. There can be several reasons for no response from the monitor;

1. If a SNMP Get command is incompatible with the device a Not Responding message will be displayed for the log value. Either the command isn't compatible or the SNMP MIB for that device hasn't been loaded onto the SNMP Probe machine. You will need to run those SNMP GET commands from the SNMP Probe machine from SNMP directory is located in the Agent Temp Directory \usr\bin to validate the results.

Monitor > Set SNMP Values

This operation allows the user to change SNMP Objects that have been identified as 'Read Write' capable. The user will require the masked input of the Community Read/Write value (password).

Note: The user will only see the machines that have been set up as SNMP Probes by applying the Read Community value via the SNMP Community feature.

Machine ID (list)

Select the Machine that has been set up as the SNMP Probe for the SNMP device of interest.

SNMP Device (list)

Select the specific SNMP Device of interest.

Create (button)

Opens a edit form to prepare the SNMP Write execution and add all required fields.

Cancel

Ignores any data changes and returns the form to the Create step.

Execute SNMPSet

Prepares a script that executes a SNMPSet against the selected SNMP Device

Ticketing Tab

The Ticketing tab contains functions related to the built in trouble ticketing system. The trouble ticketing system sends email alerts to designated administrators and users on ticket creation, changes, and resolutions. The system organized trouble tickets by machine ID. All trouble tickets **must** be assigned to a machine ID. You may wish to create extra machine accounts to hold trouble tickets of a global nature, such as general network problems.

To access the Assistant, click Assistant from any function page.

The following functions are available in the Ticketing feature tab:

Functions	Description
View Summary	Define email alerts on a per machine basis.
View Ticket	View and manage files uploaded to the VSA from remote machines by a Get File script command.
Delete/Archive	Permanently delete tickets or move tickets into archival storage.
Notify Policy	Write files to all selected remote machines and maintain them.
Access Policy	Automates execution of and collection of information from Microsoft's Hotfix Checker tool.
Due Date Policy	Define default due date for new tickets based on field values and email subject lines.
Edit Fields	Define, modify, or create trouble ticket categories. Each ticket is assigned to a particular category.
Email Reader	Setup automatic polling of email to generate new ticket entries.
Email Mapping	Defines default field values for new tickets received via email. Separate email maps may be defined for email addresses or domains.
User Profiles	Allows administrators to edit machine account information.
User Access	Set up accounts to allow users remote control access to their own machines

Ticketing > View Summary

View Summary lists all the trouble tickets assigned to machine IDs selected in Specify Accounts. Each row displays summary data for a single ticket. You can further sort and filter listed tickets with any field list type drop down control.

The **View Summary** page gives you a quick view of all the tickets you are currently working on. New tickets, or new notes in existing tickets, are clearly highlighted in one of two way.

1. **By Date** - tickets with new notes entered in the last 1 day are highlighted in red. New notes entered in the last 7 days are highlighted in yellow. You can adjust these times and colors by clicking Change Highlight link.
2. **Read Flag** - Each ticket is flagged to indicate if the administrator has viewed all the notes in the ticket. Once viewed, the ticket is marked as read with 🗒. If another administrator or user adds or modifies a note, the flag for you is switched back to unread showing 🟨.

Why don't I see a particular trouble ticket?

Standard administrators only have access to trouble tickets of machine IDs that are in group IDs they have access rights to. Users only have access to trouble tickets for their machine ID.

The View Summary function only displays trouble tickets belonging to machine IDs that match the Specify Accounts filter.

The View Summary function can **filter** the list of trouble tickets to only those that match the Category, Status, and Priority drop down control.

The **Search** function will not display a ticket if none of the notes contain the words being searched for.

NOTE: The system does not delete tickets when deleting machine IDs. The ticket summary chart includes tickets matching the Machine ID and Group ID filters. Because no machine data exists for deleted Machine IDs, Views are not applied to this table.

Open Tickets, Past Due, Hold Tickets, Total Tickets

Shows the number of tickets open, past due, and on hold for all tickets matching the Specify Accounts filter.

Note: Ticket counts are not effected by the Category, Status, or Priority controls.

Fields...

Allows each administrator or users to organize the columns displayed in the table. Clicking the **Fields...** button opens a dialog in a new browser window. There, you can select which columns to show or hide and also the order in which columns are displayed. You can show/hide any of the following columns:

- ID - unique ID number automatically assigned to each trouble ticket.
- Machine ID - trouble ticket applies to this machine.
- Category - type of problem this trouble ticket discusses
- **Assignee - Name of the administrator responsible for solving this problem.**
- Status - Open, Hold, Closed
- Priority - High, Normal, Low
- Creator - person who created this trouble ticket (administrator, user name, or machine ID).
- Last Modified Date - last time any note was added to this ticket
- Creation Date - time when the ticket was first entered
- Due Date - ticket due date
- Resolution Date - date the ticket was closed

List Fields

Each field of type **list**, such as category, status, or priority, are shown as drop down controls. Selecting any value from the drop down displays only those tickets matching the selected field value.

Sort

Changes the display order of the table to **ascending** or **descending**.

Search

Search restricts the list of tickets to only tickets containing _any_ of the words in the search string. Search examines the **ticket summary** line, submitter **name**, submitter **email**, submitter **phone**, or any of the **notes**. Use the *** character as a wildcard** in the search string.

The drop down control below the search box list the **last 10 searches** you have made. Selecting any item from the list automatically re-searches for those words.

Clicking any of the ticket summary lines returned by search jumps to that ticket. Words in the ticket notes matching any search word are .

Mark All Read

Click to mark all tickets as read. New any changes or note additions inserted by other administrators reset the ticket to unread.

Merge

Merge lets you combine two tickets into one. Use Merge to combine related tickets. The resulting merged ticket contains all the notes and attachments from both tickets. Merge asks you which field values you wish to use in the ticket for all field values that are different between the two tickets. To merge ticket, **check the box for any two tickets** listed. Then click the Merge... button.

Change Highlight

Click to set and/or modify row highlighting based on date. Highlight tickets based on date in two ways. Tickets with a date within 1 day of the current time are highlighted in red. Tickets with a date within 7 days are highlighted in yellow. You can independently **adjust both the number of days and the highlight color**. To disable highlighting by date, set each number of days to zero. The highlight date may be **last modified date**, **due date**, or **creation date**.

Column Headings

Clicking any column heading resorts the table using that column as the sort criteria.

Data Table

Each row of the table lists summary data for a single ticket. To access the entire ticket click the ticket **summary** line. To toggle the state to **read** click 📒. To toggle the state to **unread** click 🗒. To completely delete a ticket from the system click ✗.

NOTE: Prevent standard administrators and users from deleting trouble tickets in Access Policy.

Ticketing > View Ticket

Create new trouble tickets, add notes to existing tickets, or modify notes in existing tickets with the **View Ticket** function. Select the ticket of interest from the Ticket ID drop down control. Edit any existing data by clicking the 📝 next to the data you wish to edit. Delete notes by clicking ✗ next to the note.

NOTE: Prevent standard administrators and users from deleting trouble tickets in Access Policy.

How do I create a new ticket?

Creating a new trouble ticket requires filling out all fields of the trouble ticket. Perform all the following steps to create a new ticket.

1. Enter a short description of the problem.
2. Specify a machine ID or a machine group ID to submit a trouble ticket for. All trouble tickets must be assigned to either a machine ID or a machine group ID. Pick the appropriate radio button to indicate if the ticket is to be associated with a machine ID or group ID. Next, click 📝 to enter a selection. A window will pop up with a list of machine Ids or group Ids and then select the radio button next to the choice desired.
3. Select a category from the Category drop down control to assign to this trouble ticket.
4. 5elect a status (Open, Hold, Closed) from the **Status** drop down control.
5. Select an administrator from the Assignee drop down control to assign to this trouble ticket
6. Select a priority (High, Normal, or Low) from the **Priority** drop down control.
7. The submitter field defaults to the email sender (if received from an email) or the administrator's email. This information can be updated if need be.
8. User name, user email and user phone will default from the user information of the user associated with the machine assigned to the ticket. This information can be updated if appropriate.
9. The creation date is automatically assigned. This will be set to the date the ticket is created.
10. Enter a due date for this trouble ticket by clicking 📝 next to **Due Date**. The default due date one week from the creation date.
11. Enter details of the problem in the **Notes** edit box. Click the Submit button to complete the ticket.

Why can't I edit a ticket?

Master administrators may disable ticket delete and edit privileges for users and standard administrators. See Access Policy.

How do I attach a file, such as a screen shot, to the trouble ticket?

Click the **Browse...** button below the note entry area. Locate the file you wish to attach on your local computer. Click the **Open** button in the browse window to upload the file to the VSA server. Once the file has been successfully uploaded tag text is automatically entered into the note in this format: <attached file:*filename.ext*>. This tag appears as a link in the notes listing for the ticket. Display/download the file at any time by clicking that link.

Ticket ID

Enter the ticket ID to view/edit an existing ticket. Leave blank to create a new trouble ticket.

Machine or ID

Each trouble ticket must be assigned to either a machine ID or group ID. Click 📝 to enter or change the ID. Clicking 📝 opens a new window with a list of available machine IDs to choose from. To choose a machine ID select **group** from the drop down control. Click the radio button to the left of the machine or group ID of interest.

Assignee

Name of the administrator responsible for solving this problem.

Fields

Master administrators can define any number of customer fields associated with each ticket (see the

Edit Fields function). When you modify any field, the system automatically inserts a note recording the change. The note may be standard or hidden depending on the access policy set for this administrator. Automatic notes may also be disabled. Three fields are mandatory and may not be deleted

NOTE: Master administrators can add, delete, or edit filed labels with the Edit Fields function. Master administrators can also define who can view and/or edit fields on a per administrator group using the Access Policy function.

Category

Assign the trouble ticket to a category with this drop down control.

Status

Drop down control specifies the status of this ticket.

- **Open** - Indicates ticket has not been resolved and is actively under investigation
- **Hold** - Indicates ticket has not been resolved but is **not** being worked on. Use hold tickets for non-critical problems whose resolution can be postponed.
- **Closed** - The ticket has been completely resolved.

Priority

Drop down control specifies the status of this ticket.

- **High** - Set to high for critical trouble tickets that need immediate attention
- **Normal** - This ticket requires normal response time.
- **Low** - Indicates this trouble ticket does not impact current operations and may be postponed until time permits.

Submitter Information

Displays the Name, Email address, and phone number associated with the machine ID for this ticket. Typically, this information corresponds to contact information for a person using that machine. Enter user information in User Profiles.

Update

This button applies any changes to text fields such as submitter information, non-list fields (strings, integers, numbers).

Note: All list fields are immediately saved in the ticket.

Last Search

This button returns you to the **View Summary** screen using the last search string entered. Use last search to quickly browse through multiple tickets returned by a key word search. Words matching any of the search words are in the displayed notes. For example, if you are searching for all tickets that dealt with DHCP:

1. Search for DHCP in View Summary.
2. Click on a ticket summary to view one of the tickets returned.
3. Quickly scan the ticket notes looking for and scan the surrounding notes.
4. If the ticket is not of interest, click the Last Search button to return to the search results.
5. Repeat the above steps until the ticket of interest is found.

Created

Time stamp indicating the date and time this trouble ticket was first created.

Age / Closed

Age lists the number of hours/days since the creation date for open and hold tickets. If the ticket has been closed then **Age** is replace with **Closed** and lists the time stamp indicating the date and time this trouble ticket was closed.

Due

Desired resolution date for this ticket. Click 📝 to edit the due date. If the due date does not match one of the defined due date policies, then the **Due Date** label is hilighed. Click the Apply button to reset the due date to the policy. If no policy matches then the system default due date is used.

Summary

Short summary description of the problem reported in this trouble ticket. Click 📝 to edit the summary.

Submit/Add

Add details about the problem here. Use this space to describe the initial problem in detail and also to add notes discussing problem investigation or resolution. Notes may be edited by clicking 📝 and/or deleted by clicking ✕ next to each note listed for this trouble ticket

Add Hidden

You can also add hidden notes, not viewable by users, to tickets. Use hidden note to record data or analysis that may be too detailed or confusing to users by useful to other administrators.

Note: Hidden notes are NEVER included in email notifications.

Browse... Click to attach file (such as screen shots of problem).

Click the **Browse...** button below the note entry area. Locate the file you wish to attach on your local computer. Click the **Open** button in the browse window to upload the file to the VSA server. Once the file has been successfully uploaded tag text is automatically entered into the note in this format: <attached file:*filename.ext*>. This tag appears as a link in the notes listing for the ticket. Display/download the file at any time by clicking that link.

Notes Table

Lists all notes relating to this trouble ticket in ascending or descending time order. Each note is time stamped and labeled with the login name of the person entering the note.

NOTE: User entered notes are labeled with the machine ID they logged in with. See User Access for details.

Ticketing > Notify Policy

Notify Policy defines when the trouble ticketing system sends out email notifications. **Multiple independent policies may be set for each group ID**. This lets you specify different email lists for different events. For example, you may wish to send email alerts to a group of administrators for ticket creations and note additions, but send email to a different list of administrators for overdue tickets. As a default, no email notifications are sent. You must enter a policy to get email notifications from the trouble ticketing system. To set a policy perform the following steps:

1. Check the box to the left of each notification event you need email notification of
2. Enter a comma separated list of email address in the **Email List** edit box.
3. Check the box to the left of all group IDs you wish to apply this notification policy to.
4. Click the **Update** button.

Note: You can NOT send notifications to the email address used to receive tickets (set in Email Reader).

Email List

Comma separated list of valid email addresses to send notification emails to.

Notification Type Checkbox

The list below describes when the trouble ticketing system sends an email notification to all addresses in the email list.

- **Ticket Creation** - Email sent at time of ticket creation.
- **Modify/Add Note** - Email sent when any note is added or changed to a ticket.
- **Overdue Ticket** - Email sent when a ticket passes its due date without being closed.
- **Assignee Change** - Email sent when a ticket is assigned to a different admin
- **Field Change** - Email sent when anyone changes any custom field in a ticket.
- **Edit Summary** - Email sent when anyone changes the summary line for a ticket.
- **Due Date Change** - Email sent when anyone changes the due date of a ticket.
- **Notify Ticket Submitter when note added** - Send alert to the email address entered for the ticket submitter, in addition to the email list for all email notification messages.
- **Include all public notes in Modify/Add notification** - Selecting this option will include **all** the notes for a ticket when a **Modify/Add Note** message is sent out.
- **Received email alerts always sent to assignee** - This option sends an email to the ticket assignee, when ever a new note is created from a received email, even if the assignee is **not** on the notification email list for this group ID.
- **Send auto response to emails creating new tickets** - This sends an automated reply message out to the person that send in an email that generated a new ticket. Automated response emails give your users an acknowledgement that there request has been received and processed by the system. Master administrators can specify the canned message sent in reply to these emails.

Ticketing > Access Policy

Access Policy determines who can edit and/or view fields in trouble tickets. **Only Master Administrators can set this policy.** Independent policies may be set for each Administrator Group and Users. Users only see trouble tickets assigned to their machine ID. Standard administrators only see tickets assigned to machine IDs that are part of group IDs they have rights to access.

Select user or administrator Group

This drop down control lists < Users > and all administrator groups. Select the group you wish to set a policy for here.

Enable ticket delete from the view summary table

Checking this box lets the selected administrator group delete entire tickets by clicking the ✗ icon on the view summary page.

Enable ticket edit to modify or remove notes.

Checking this box lets the selected administrator group edit existing notes.

Note: Adding new notes is always enabled for all administrator groups

Enable due date edit when editing trouble tickets

Checking this box lets the selected administrator group modify the ticket due date.

Enable suppress email notifications when editing trouble tickets.

Checking this box lets the selected administrator group suppress email notifications when he modifies an existing ticket.

View hidden notes.

This checkbox specifies whether or not hidden notes may be viewed by this administrator group.

Note: Hidden notes are never viewable by users.

Change hidden notes status checkbox.

This checkbox enabled the Hide checkbox at the far right edge of each ticket note. Toggling the hidden checkbox makes a note hidden or not.

Automatically insert new note with every field change

Check this box to enable automatic note insertion to record all ticket field changes.

As hidden note

Check this box to make all automatic notes added as hidden. This policy only has an effect if "Automatically insert new note with every field change" is checked.

Define access to each ticket field

Access to each field, created in Edit Fields, may be defined here. Three levels of access may be specified.

1. **Full Access** - Can view and modify this field in every ticket.
2. **View Only** - Can see but not change the value of this field.
3. **Hidden** - Hidden fields are not shown to the selected administrator group.

Due Date Policy

Set the due date for each **new ticket** based on field values. Any combination of **list fields** may be defined to set a due date. This allows you to set a ticket due date based on the urgency of the ticket and a guaranteed level of service. For example, define a new field named *Service Level* with the following list items: *Premium, Standard, Economy*. Create different due date policies for each combination such as

- Set resolution time to 1 hr when Priority = High and Service Level = Premium
- Set resolution time to 7 days when Priority = Normal and Service Level = Economy

When a new ticket gets created, the due date is set by adding the number of hours in the policy to the current time.

Default time to resolve tickets with no policy

When new tickets are created that do not match any policy, then the due date is set to this number of hours plus the current time.

Policy Name

Give the policy any name you wish

Time

When new tickets are created that match the field values in this policy, then the due date is set to this number of hours plus the current time.

Fields

A column for each defined list field contains the value for the associated policy.

Ticketing > Edit Fields

Edit Fields lets you create and/or edit fields shown on tickets. Seven field types are available. Fields are associated with the entire ticket (as opposed to each note of the ticket). Use field to hold data items you need to collect for all tickets. Three mandatory fields exist that may not be removed from the system. They are:

1. **Category** - A customizable list of trouble ticket categories (such as Printer Problem).
2. **Status** - State of the current ticket (Open, Hold, Closed)
3. **Priority** - High, Normal, Low

Field Position

Click the up/down arrows to the left of the field label to change the display position for this field in View Tickets.

Field Label

You may modify the label for any field here. Click the Update button to apply the change

Type

1. **String** - May contain any text up to 500 characters in length. Best used to hold things like problem location or other variables that do not belong in the summary line.
2. **Integer** - May contain any positive or negative integer value
3. **List** - Lets you create a drop down list of choices
4. **Number (nn.d)** - Number that always shows one digit to the right of the decimal point.
5. **Number (nn.dd)** - Number that always shows two digits to the right of the decimal point.
6. **Number (nn.ddd)** - Number that always shows three digits to the right of the decimal point.
7. **Number (nn.dddd)** - Number that always shows four digits to the right of the decimal point.

Default Value

Creating a new ticket automatically sets each field to its default value. You can specify that default value here.

Note: Default values are system wide and may not be different for different machine group IDs or administrator groups.

< Edit List >

Edit any label. Click update to have the changes take effect.

Ticketing > Email Reader

The **Email Reader** function provides a means to set-up the needed parameters to use Kaseya's automated Email Reader. The Email Reader will poll a specified email account periodically and move the contents of the email into the ticketing system. The information needed to set this up is as follows:

Email Address

Enter the email address you wish to send ticketing related notifications from here. Replies to this email address are in turn processed by the ticketing system as added notes to the relevant ticket.

Disable email reader

Check this box to prevent the email reader component from polling a server.

Host Name

The name of the Pop3 host service is needed.

Port

Provide the port number used by the Pop3 service. This is normally 110.

Use SSL

Check this box to enable SSL communications with your POP server. Your POP server must support SSL to use this feature. Typically, SSL enabled POP uses **port 995**.

Login

Provide the email account name.

Password

Provide the email account password.

Check for new emails every N minutes

The number of minutes the Email Reader should wait before polling the POP3 server for new emails.

Apply

Click this button to load the new parameters into the ticketing system.

Connect Now

Click this button to connect to the POP3 server now instead of waiting for the next polling time.

Contents of Email

The Email Reader can receive any email, with or without attachments, and add the contents to the ticketing system. Additional information can be added to the email to enhance the mapping of the email to the ticketing system. The following tags can be included in either the subject or the body of the email.

~ticid='xxx' – This tag will cause the email to have its body appended to an existing ticket rather than cause a new ticket to be created.

~username=’xxx’ – Automatically insert the value given as xxx into the Submitter Information Name field.

~useremail=’xxx’ – Automatically insert the value given as xxx into the Submitter Information Email field.

~userphone=’xxx’ – Automatically insert the value given as xxx into the Submitter Information Phone field.

~category=’xxx’ - This tag will cause the ticket created to get a specific category. The category must exist.

~priority=’xxx’ – This tag will cause the ticket created to get a specific priority. The priority must exist.

~status=’xxx’ – This tag will cause the ticket created to get a specific priority. The status must exist.

~assignee=’xxx’ – This tag will cause the ticket created to get a specific administrator assigned. The administrator must exist.

~machineid=’xxx.xxx’ – This tag will cause the ticket to have a machine id set immediately. The machine id must exist. The inclusion of this tag will cause the ticket to bypass the pending stage and go directly to the View Summary.

~fieldName='xxx' – An initial value for any defined field can be assigned a value. If the field is a list type, then the value must exist in the list.

Ticketing > Email Mapping

The Email Mapping function provides a means to set-up defaults for emails that are received and turned into tickets. A map can be created for either an individual email address or a domain (a client's domain). The email reader to build a ticket uses this information. This information will override the defaults provided in the configuration set-up. The fields entered are:

Email Map

The email address or domain to be mapped. Examples would be support@kaseya.com or kaseya.com.

Set map for unassigned emails

Check this box to specify an email map for a messages received by the ticketing system from email address not covered by any other email map.

Associate map with a machine or group

Tickets can be associated with an individual machine or a machine group. By making this selection the user is then allowed to pick a machine id or a group id..

Assignee

Name of the administrator responsible for solving this problem.

Fields

Specify the default field values entered for new tickets created when an email is received by the ticketing system.

Create

This button will create a new map.

Delete icon

Click the ✗ icon to the left of each email map to remove that map from the ticketing system.

Edit Icon

Click the 📝 icon to the left of each email map to modify the current settings for that map.

Patch Mgmt Tab

The Patch Mgmt tab contains functions related to monitoring, scanning, installing, and verifying patches to managed machines.

The following functions are available in the Patch Mgmt feature tab:

Functions	Description
Scan Machine	Schedule a recurring scan for missing patches on managed machines.
Patch Status	See at a glance, the number of missing and installed patches for each machine.
Initial Update	Automatically applies all required service packs and patches according to the Patch Approval Policy beginning at the scheduled initial update time. Rebooting the machine immediately as required.
Patch History	View patch scan results for each machine.
Patch Alert	Send an alert when a new patch becomes available for a managed machine.
Machine Update	Schedule patch deployment to an individual machine.
Patch Update	Lists only patches missing from selected machines. Manually schedule installation of missing patches to machines requiring update.
Rollback	Rollback gives you a mechanism to remove patches after they have been installed on a system. Not all patches may be uninstalled.
Automatic Update	Configure the system to automatically deploy newly discovered patches on selected machines.
Cancel Updates	Cancel any pending patch installations.
Exclude Machines	Designate machines to never show up in the Apply Update list.
Patch Approval	Defines a collections based policy for approving patches for automatic update.
Reboot Action	Determines whether or not to reboot the machine automatically after installing new patches.
File Source	Specifies where each machines gets new patch installation files from.
Patch Alert	Configures alerts generated by the patch system.
Windows Auto Update	Remotely sets the Windows Automatic Update settings on selected machines.
Pre/Post Script	Run scripts before and/or after patch initial update.
Office Source	Specify a path to MS Office installation source.

Command Line	Set the command line parameters used to install patches.
Patch Location	Specify the URL to download a patch from when the system can not automatically locate it.

Patch Mgmt > Scan Machine

Show me an explanation of the items on this page.

Use this function to schedule scans to search for missing patches on each managed machine. Scanning takes very little resources and can safely be scheduled to run at any time of day. The scanning operation will not impact users at all.

When new patches are published, your VSA server's patch database is updated with the information it needs to identify which machines may require the new patch.

How often should I scan a machine?

System and network security depends on all your machines having the latest security hot fixes and patches applied. Patches are released at irregular and unpredictable intervals. To insure your machines are updated you should scan all your machines on a daily basis.

Can I scan the VSA Server itself?

To scan the VSA Server, you must install an Agent on the VSA Server. Once installed, you can scan the VSA Server just like any other managed machine. Use the Machine Update function to apply the patches manually or use the Automatic Update function to automatically apply the patches.

What is happening when the patch database is refreshed?

Product vendor information for each supported product is downloaded from the Internet at the scheduled time and recurring interval. Updates to the information is loaded into the database and distributed to each machine at its next scheduled patch scan.

Explanation of items on this page

Schedule

Scan the selected machine for new patches at the scheduled time and recurring interval.

Cancel

Cancel the scheduled patch scan.

Stagger By

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

Note: Patch Scan requires very little resources and does not impact the user or network at all when scans run. Stagger is almost never required but it is included for completeness.

Skip if machine offline

Check to only scan at the scheduled time. If machine is offline, skip and reschedule for next day at the same time. Uncheck to scan the update as soon as the machine connects after the scheduled time.

Patch > Patch Status

Patch Status gives you an at-a-glance view of the patch status for each of your managed machines. Quickly identify machines that may be missing patches or are indicating errors.

Patch Test

Most patch problems are the result of configuration and/or permissions issues. The test function exercises the entire patch deployment process without actually installing anything on the target machine or causing a reboot.

Select the machines you wish to verify patch management configuration for and click the **Test** button. The system displays test results once the test completes on each machine.

Patch Mgmt > Initial Update

Initial Update automatically applies all required service packs and patches according to the Patch Approval Policy beginning at the scheduled initial update time. Rebooting the machine immediately as required. Unlike the Automatic Update function, this is not a recurring process.

When a machine is scheduled, Initial Update will perform a patch scan to ensure the latest scan results are available. Then, updates are scheduled in successive groups. First, if required, the Windows Installer will be updated. The second group of updates consists of any operating system related service packs. After the service packs, non-security patches (Nxxxxxx) are applied. The next group is the Microsoft security patches (MSyy-xxx). Next, Office related service packs, where possible, are installed. Finally, Office related patches, where possible, are installed.

Scripts can be configured to be executed just before the Initial Update begins and/or after Initial Update completes to automate new machine preparation and setup by running scripts to perform common preparation tasks for each machine. Use the **Patch Mgmt Pre/Post Script** function to configure these scripts on a per-machine basis.

NOTE: Reboots are forced after each service pack and at the end of each patch group without warning. This is necessary to permit the re-scan and installation of the subsequent groups of patches.

NOTE: Once the Initial Update has been scheduled, the Status column will display the current processing step. When all processing has been completed, the Status column will display either “Completed - fully patched” or “Completed - remaining patches require manual processing”. If the latter is displayed, you must go to the Patch Mgmt tab, Machine Update function, and select the appropriate machine to determine why all patches were not applied. Some patches might require manual install or for the user to be logged in. In the case of patch failures, manually schedule failed patches to be reapplied. Due to occasional conflicts between patches resulting from not rebooting after each individual patch, simply reapplying the patches will typically resolve the failures.

NOTE: The Agent for the KServer will not be displayed on the Initial Update screen. Initial Update cannot be used on the KServer.

Schedule

Select a date and time and click SCHEDULE to apply all required service packs and patches on all selected machines.

Cancel

Cancel any pending patch installations.

Stagger By

You can distribute the load on your network by staggering the installation of patches. If you set the stagger for 60 minutes, then patch installation to each machine ID is staggered by 60 minutes. For example, machine 1 runs at 10:00, machine 2 runs at 11:00, and machine 3 runs at 12:00, etc.

Skip if machine offline

Check to only install the updates at the scheduled time. If machine is offline, skip and reschedule for next day at the same time. Uncheck to install the update as soon as the machine connects after the scheduled time.

Patch Mgmt > Patch History

Patch History displays the results from each patch scan. Both **installed** and **missing** patches are listed.

Usage:

Click on the machine ID you wish to view the patch history for.

Patches are grouped by product with **missing** patches listed first.

Note: If "Patch location not available" is displayed, then the VSA server does not know where it can download the patch file executable from. See the Patch Location function to remedy this.

Patch Mgmt > Machine Update

Machine Update and **Patch Update** are the primary system controls used to individually schedule patch deployment. Machine Update gives you the **single machine view**. Use it to work with a specific machine. Patch Update gives you the **patch view**. Use it to deploy a patch to all the machines that are missing a particular patch.

Usage:

- Click on the machine ID you wish to schedule patch deployment for.
- Only **missing** patches are shown. Patches are grouped by product.
- Check the box next to any/all patches you wish to deploy to the selected machine id.
- Select a time to deploy the selected patches.
- Click the **Schedule** button to install the patches at the selected time.
- Click the **Cancel** button to remove any pending patch install tasks.

Note: If you have a credential set (using the Set Credential function), that all patches are installed using the rights of that credential.

For more information on why patches fail to install click here.

Patch Mgmt > Patch Update

Show me an explanation of the items on this page.

Patch management automates the process of keeping all your machines up to date with the latest patches. You decide how and when updates are applied on a per machine basis. For each machine ID you can:

- Automatically apply all updates without any administrator interaction at all (see Automatic Update)
- Decide whether to apply a patch or not on a per patch basis.

Schedule a daily scan of each machine with the Scan Machine function. The patch status for each machine is reported up to the VSA server and used to determine which machines need a new patch.

Patch Update provides a concise view of all the patches that need to be applied across all the machines matching the Machine ID/Group ID filter. Use this function to quickly determine which patches are missing.

Note: If you have a credential set (using the Set Credential function), that all patches are installed using the rights of that credential.

Note: Patches missing from machines set for automatic update are NOT listed here. These patches are automatically applied at the Automatic Update scheduled time for each machine.

What does it mean when a patch is listed on this page?

One of more of the machines matching the Machine ID/Group ID filter needs this patch applied. To learn the details about the patch click Q number link next to the Patch ID. If, after reviewing the knowledge base article, you decide all your machines need this patch schedule the patch to be installed. It gets installed on all machines that need the patch, at the scheduled time.

Why did the patch installation fail?

Patches are downloaded (or copied from a file share) to the local machine's hard disk. Several patches, **especially service packs**, also may require significant additional local disk space to completely install. Verify the machine in question has plenty of available disk space **on the same drive as the agent is installed**.

What does "Bad Patch File" indicate?

This message indicates that the patch file failed to execute for some reason. **If you scheduled multiple patches to install as a batch, all the patches will be marked at "Bad Patch File" even if only one of them failed.** The system is reporting a script failure and can not distinguish which patch in the script caused the failure.

Note: You can determine which patch failed by looking at the Script Log for this machine. The log will indicate which patches successfully installed prior to the script failure.

Possible causes are:

- A firewall has blocked the download of the patch. The system tries to download from a URL. If the URL can not be reached the returned file may just be an HTML error message. When patch management tries to execute that file, it fails.
- The downloaded patch file is corrupt
- The patch specified in Patch Location is not correct.

What does "Missing patch location" indicate?

The patches that show up as missing are typically ones where each language requires a separate download. For these, you can enter the patch yourself for the language you are using. You can manually enter the location of the patch on Patch Location page.

What does "Install Failed" indicate?

After the patch install attempt completes (including the reboot if requested) the system re-scans the target machine. If the patch still shows missing after the re-scan, failure is reported. There are three possible reasons for patch installation to fail.

1. **No Reboot** - Several patches require a system reboot before they take effect. If your Reboot Action settings did not allow a reboot, the patch may be installed but is not effective yet (until after the reboot).
2. **Command Line Failed** - If the command line parameters set in the Command Line function are incorrect, the patch executable will typically display a dialog box on the remote machine stating there is a command line problem. This error causes patch installation to halt and the patch deployment script to terminate. The patch file remains on the remote machine and **Install Failed** is displayed. Enter the correct command line parameters for the patch and try again.

   MS Office Command Line Failed – The only command line parameter permitted for use with Microsoft Office related patches (Patch ID starts with "ODT-") is "/Q". Because MS Office patches may require the Office installation CD(s), the use of the "/Q" command line parameter might cause the patch install to fail. If an Office related patch fails, remove the "/Q" command line parameter and try again.

   NOTE: If "/Q" is not specified, Microsoft Office 2000 command line parameter will be automatically reset to blank (no command line parameter), and Microsoft Office XP and 2003 command line parameters will be automatically reset to " /INSTALL-AS-USER /DELAY-AFTER=60". These settings are enforced by the application.

Note: Command line parameters for each patch apply globally and can only be changed by a Master administrator

3. **Patch Download Blocked** - The patch file was never delivered to the machine. The system downloads the patch directly from the internet to either the server, or directly to the remote machine, depending on your File Source settings. Your firewall may be blocking these downloads. The patch file delivered to the agent having a size of only 1k or 2k bytes is an indication of this problem.
4. **Patch Location Not Correct** – The patch specified in Patch Location is not correct.

What does "User not logged in" indicate?

For the patch to be installed, a user on the machine being patched must be logged in to respond to dialogs presented to the user by the patch. The patch script automatically detects whether a user is currently logged in and will not continue if a user is not logged in. Reschedule the installation of the patch when a user is available and logged in to the machine.

What does "User not ready to install" indicate?

For the Office patch to be installed, a user on the machine being patched must be logged in to respond to dialogs presented to the user by the patch. Since Office patches occasionally require the user to insert the Office installation CD(s) during the patching process, the user is presented with the following dialog box:

Why does the IE5-IE6-EN patch still show missing after a patch update?

IE5-IE6-EN upgrades older installations of Internet Explorer to the latest version. IE does not complete its installation until **after the next time a user logs onto that machine**. Patch scans will continue to show the patch missing until someone logs onto that machine.

What does "Manual install only" indicate?

Some patches and service packs require passwords or knowledge of a customized setup that the VSA can not know. These updates must be installed manually on each machine.

The patch was scheduled to run but now it shows as unscheduled and still needs to be installed. Why?

After the patch installation completes, the machine must reboot in order for the patch to take effect. After the reboot, the machine is re-scanned and the results processed by the VSA. **This entire process can take several minutes**. After you apply a patch to a machine, please wait several minutes before checking the patch state again.

Explanation of items on this page

Schedule

Select a time and click Schedule to install the selected patch on all machines. When you schedule a patch with Apply Update the following occurs.

1. The agent on the remote machine is told to start the update process at the scheduled time.
2. The patch executable is downloaded to the remote machine (from where ever "File Source" is set for that machine ID).

3. The patch file is executed on the remote machine using the parameters specified in "Command Line". You should never have to set these switches yourself, but just in case, this capability is there.
4. After all the patches have been installed the remote machine is reboot by what ever method is specified in "Reboot Action"
5. The remote machine is rescanned automatically. It takes 2 to 3 minutes after the reboot is complete for this data to show up on the VSA.

Note: All patches are installed for each machine as a patch. If you schedule multiple patches for installation on the same machine, all the patches are installed at the same time. After all the patches have been installed the machine reboots once. This technique saves time and reboots.

Note: Service packs are always installed separately. If you are installing a service pack with other patches you will see a reboot after the service pack install and than another single reboot after all the other patches are installed.

Cancel

Cancel any pending installations of the selected patches.

Stagger By

You can distribute the load on your network by staggering the installation of patches. If you set the stagger for 5 minutes, then patch installation to each machine ID is staggered by 5 minutes. For example, machine 1 runs at 10:00, machine 2 runs at 10:05, machine 3 runs at 10:10, ...

Skip if machine offline

Check to only install the update at the scheduled time. If machine is offline, skip and reschedule for next day at the same time. Uncheck to install the update as soon as the machine connects after the scheduled time.

Patch > Rollback

Rollback gives you a mechanism to remove patches after they have been installed on a system. Not all patches may be uninstalled. The system only lists patches supporting rollback.

Rollback

Follow these steps to remove a patch from any managed machine:

1. Click the machine ID, from the list provided, that you want to remove a patch from.
2. Check the box to the left of the patch you want to uninstall.
3. Specify a time to perform the rollback operation
4. Click the Rollback button.

WARNING: Removing Windows software updates in the wrong order may cause the operating system to stop functioning. Click here for more information

Patch Mgmt > Automatic Update

Schedule

Select a time of day and *day of week* and click Schedule to apply new patches on all selected machines. To schedule automatic update for the same time every day select **Every day** from the day selector.

Note: Patch installation only occurs when a new missing patch is found by Scan Machine.

Cancel

Cancel any pending patch installations.

Stagger By

You can distribute the load on your network by staggering the installation of patches. If you set the stagger for 5 minutes, then patch installation to each machine ID is staggered by 5 minutes. For example, machine 1 runs at 10:00, machine 2 runs at 10:05, machine 3 runs at 10:10, ...

Skip if machine offline

Check to only install the update at the scheduled time. If machine is offline, skip and reschedule for next day at the same time. Uncheck to install the update as soon as the machine connects after the scheduled time.

Note: If a new patch needs to be installed, the machine is typically reboot after the installation. To restrict reboots to only occur at the scheduled time, turn "Skip if machine offline" on.

Patch Mgmt > Cancel Updates

Cancel pending patch installations on a per machine basis. Use this function to cancel **ALL** pending patch installations for the selected machine IDs.

The Apply Update function organizes on a per patch basis, while this function is per machine. User Apply Update to cancel a particular patch from all machines.

Cancel

Check the box next to any machine ID you want to cancel all pending patches for. Then click the Cancel button to remove all pending patch installations.

Show Patch List

Check this box to list all the patch ID for the pending patch installations for each machine. Unchecking this box, gives the total number of pending patches.

Patch Mgmt > Patch Approval

Patch Approval gives you control over machines set for Automatic Update. Patch Approval lets you approve a patch first before it gets generally deployed to all your managed machines. Define separate approval policies for each machine collection. For example, by setting up a separate approval policy for each of collection, you can automatically deploy a patch to all your workstations while blocking deployment to servers.

When you create a new Patch Approval policy, all patches are approved by default. You can then deny any of those patches you want to block for this collection. When new patches are released, the system automatically denies them in the policy. These are displayed as Pending Approval to distinguish them from previously denied patches. This gives you the chance to test and verify a patch in your environment before the patch automatically pushes out.

If a machine is a member of two collections and each collection has a separate policy, and if a patch is **denied by either collection** then the patch is **denied for that machine**. Note that if one collection does not have any policy set, then only the policy that is set is used.

Collection selector

Select a collection by name from the drop down control. Machines that are not a member of any collection are automatically approved.

Default Approval Status selector

Available only when the selected collection has a defined policy. Select a default approval status for this collection. This default value will be used to automatically set the approval status of newly identified patches to this value for this collection.

Remove Policy

Available only when the selected collection has a defined policy. Clicking this button will delete the current policy and automatically approve all current and all future patches for this collection.

NOTE: Clicking this button to remove this policy permanently deletes the approval policy. To enable an approval policy, you must recreate the policy.

Filter patches by Approval Status selector

Available only when the selected collection has a defined policy. Filters the list of patches in this policy based upon the selected approval status.

Approve / Deny

Available only when the selected collection has a defined policy. Clicking these buttons approves or denies the checked patches from the list.

Set Policy

Available only when the selected collection does not have a defined policy. Clicking this button will create a new patch approval policy for this collection.

Patch Groupings

To facilitate patch approval, patches are displayed in the following groupings:

- Operating System Related Service Packs
- Operating System Related Patches
- Office Related Service Packs
- Office Related Patches

Links are provided for each of these groups along with" Back to top…" links to facilitate navigation on the screen. Each grouping has "Select All" / "Unselect All" links that act only on the grouping. There are also "Select All Service Packs and All Patches" and "Unselect All Service Packs and All Patches" that act on the entire page.

Patch Mgmt > Reboot Action

This function defines what happens at the end of each patch installation. After a patch installs, the machine needs to be rebooted before the patch takes effect. This function lets you define **when** that reboot occurs.

The patch installation script runs at the scheduled time and performs the following steps:

1. Downloads (or copies from a file share) all the patch files to a local drive (same drive as the agent is installed on).
2. Executes each patch file, one at a time.
3. Performs the selected reboot action described below.

Note: Service packs are always installed separately. If a service pack is also scheduled, it installs first, the machine reboots, then any additional patches are installed.

Note: Patches will not take effect until the machine next reboots.

Warning: It is strongly recommended that the Reboot Action for the Agent on the KServer be set to "Do not reboot after update"! Automatic rebooting of the KServer can have adverse effects on other KServer processes!

Reboot immediately after update.

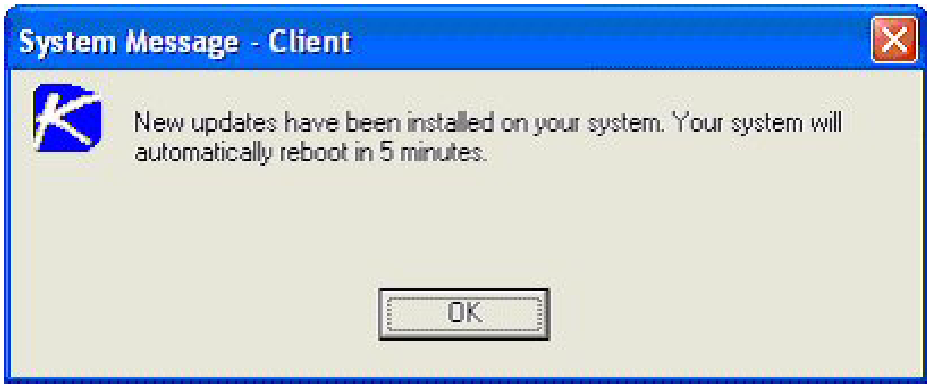
Reboots the computer immediately after install completes.

Reboot <day of week> at <time of day> after install

After the patch install completes the computer is reboot at the selected time of day and day of week. Use this setting to install patches during the day when users are logged in (to get the UNC path) and then force a reboot in the middle of the night. Selecting **every day** reboots at the next specified time of day following the patch installation.

Warn user that machine will reboot in N minutes (without asking permission).

When the patch install completes, the message below pops open warning the user and giving them N minutes (you may pick any number of minutes you like) to finish up what they are doing and save their work. If no one is currently logged in, the system reboots immediately.



System Message - Client

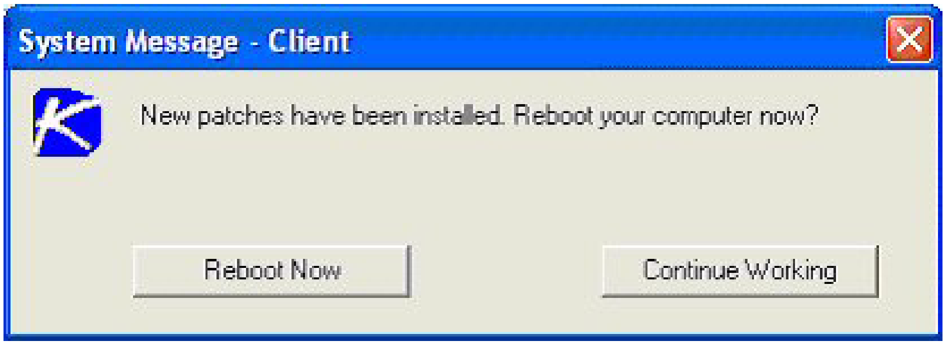
New updates have been installed on your system. Your system will automatically reboot in 5 minutes.

Skip reboot if user logged in.

Skips the reboot, after the patch install completes, if the user is logged in. Use this setting to not interrupt your users and rely on then rebooting later or shutting down their computer at the end of the day.

If user logged in ask to reboot every N minutes until the reboot occurs.

This setting displays the message below to ask the user if it is OK to reboot now. If no one is at the computer or they answer no, the same message appears in N minutes (you may pick any number of minutes you like) until the system has been rebooted. If no one is currently logged in, the system reboots immediately.

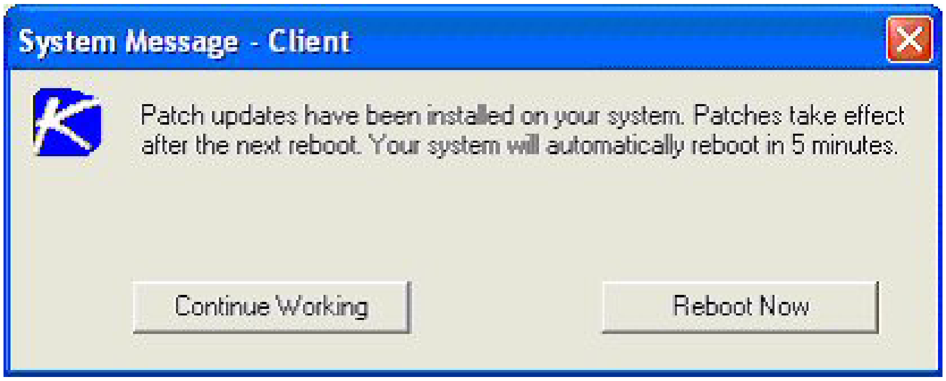


System Message - Client

New patches have been installed. Reboot your computer now?

If user logged in ask permission. Reboot if no response in N minutes. Reboot if user not logged in.

This setting displays the message below to ask the user if it is OK to reboot now. If no one is at the computer, it reboots automatically after N minutes (you may pick any number of minutes you like) **without saving** any open documents. If no one is logged in, reboot immediately.

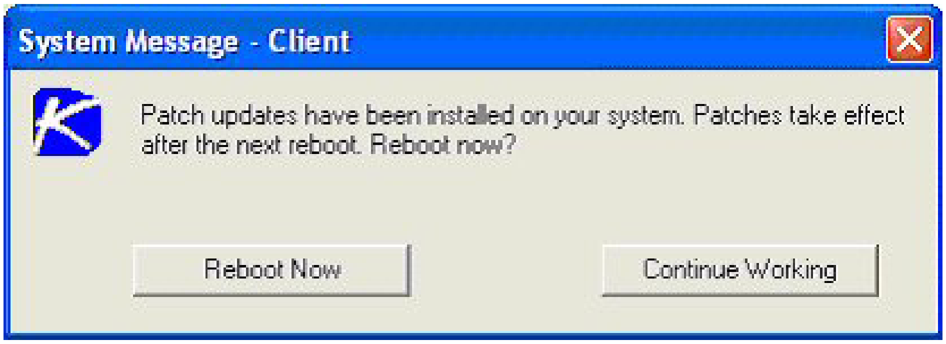


System Message - Client

Patch updates have been installed on your system. Patches take effect after the next reboot. Your system will automatically reboot in 5 minutes.

If user logged in ask permission. Do nothing if no response in N minutes. Reboot if user not logged in.

This setting displays the message below to ask the user if it is OK to reboot now. If no one is at the computer, the reboot is skipped. If no one is logged in, reboot immediately.



System Message - Client

Patch updates have been installed on your system. Patches take effect after the next reboot. Reboot now?

Do not reboot after update

Does not reboot. Use this if you users typically shut down their computer every night. You can rely on this behavior to reboot the machine for you. If the machine is a **server that you do not want to reboot** you can be notified via email when a new patch has been installed by checking **Email when reboot required** and filling in an email address.

Patch Mgmt > File Source

This function defines where each machine gets patch executable files from prior to installation and where these patch executables are copied on the local machine

Note: Patches are downloaded (or copied from a file share) to the local machine's hard disk. Several patches, especially service packs, also may require significant additional local disk space to completely install. Verify the machine in question has plenty of available disk space on the drive specified in the "Copy packages to temp directory on local drive with most free space" option.

Copy packages to temp directory on local drive with most free space

Before the scheduled patches are installed, they are all copied to the local computer. The default location is the temporary directory specified in Temp Directory on the local hard drive having the most free disk space. Uncheck this box to always use the temporary directory on the drive where the Agent is installed.

Delete package after install

After each patch install the patch install package is typically deleted to free up disk space. Uncheck this box to leave the package behind for debugging purposes. If the install fails and you need to verify the Command Line switches, do not delete the package so you have something to test with. The package is stored in the temporary directory specified in Temp Directory on the drive specified in the previous option.

Download from Internet

Each machine downloads the patch executable file directly from the internet at the URL specified in Patch Location.

Pushed from system server

First the server checks to see if it already has a copy of the server file. If not, the new patch executable is downloaded automatically by the system server, stored on the system server, and used for all subsequent distributions to managed machines. When a patch needs to be installed on a managed machine, this patch file is pushed to that machine from the system server.

Note: Default location for patch files stored on the server itself is C:\Kaseya\KaWeb\ManagedFiles\VSAPatchFiles\

Pulled from file server using UNC path

This method can be best if you support many machines on the same LAN. The patch executable file is copied from a file share accessible to this computer.

Note: The specified path to the file must be in UNC format such as \\computername\dir\.

First the server tasks the agent on the server providing the file share to see if the patch file is already in the file share. If not, the agent downloads the patch file either directly from the internet, or gets it from the system server. This procedure **automatically loads all patch install files to the file share for you.**

- Download from **the internet** - Use this setting when the server running the file share has full internet access.
- Download from **the system server** - Use this setting when the server running the file share is blocked from getting internet access.

Note: Your server MUST have access to the internet in either case, in order to download new patch files.

After the patch file has been downloaded to the file share the agent on the remote machine copies the patch install package from the file share to the \temp directory on a local disk drive with the most free space available. Connecting to a network drive requires a user credential with access rights to that file share. Two connection methods are available:

1. **Set Credential** - If a credential has been specified for this machine ID, the patch install script will use that credential to access the file share and to install the patch files.

2. **User Logged In** - If a credential has **not** been set for this machine ID, then a user *must be logged in* during the install process in order for the agent to connect to the remote file share. The patch file is then installed using the system privileges of the agent service.

Note: The file share computer must also have an agent on it. That agent automatically downloads each patch executable from the internet for later distribution to other managed machines on the network.

Monitor > Alerts

Show me an explanation of the items on this page.

How do I filter event log alerts (using event sets)?

You can activate alerts independently for event log entries in the **Application**, **Security**, and **System** event logs. Within each log type, you can also filter on event type. Checking the box on any of the following generates alerts for all log entries matching the selected type:

- Error
- Warning
- Information
- Success Audit
- Failure Audit

If you check any of these boxes then all events, matching the selected type, generate an email alert. You can further filter and restrict which events generate alerts by defining **Event Sets**. Event sets let you specify specific events to alert on or to ignore. Use event sets to group together related events into a single item. For example, if you are monitoring an domain control, you can group together all the events your do not want to receive alerts for into a single event set. Then just assign the event set to the machine you are monitoring. **You may assign more than one event set to the same machine**. This lets you better organize event sets into functional areas.

The **ignore flag** is there to let you alert on all errors (or any other event type) except for a list of events you may not care about.

1. First set up a machine to alert on Errors (check the box) and select < **All Events** > from the event set list. This tells the system to generate an alert for every error event type.
2. Second, assign another event set to the same machine that lists all the events you wish to ignore.

The secret is assigning multiple event sets to the same machine (one to get all the alerts, and others to ignore the alerts you don't want).

Ignore events ALWAYS take precedence over other event sets. It an event matches an ignore event set, nothing will be alerts.

What is the time delay between when events occur and when the system sends the email alert?

Some alerts are processed immediately and some are processed at the next audit. **Event log alerts** are processed immediately as follows:

If you have alerting turned on then the agent reports up new event log entries at the next check-in period. If alerting is turned off (for that log) then the events are not reported up until the next time the agent has something else to do. Once reported up to the server, a background task on the server processes them in a batch mode. The server background task runs every two minutes. So if you have alerts activated, the longest delay you incur is 2 minutes plus the quick check-in period, plus what ever processing lag your external email system may have.

Application changes, HW Changes, and **Low Disk** alerts are processed with each audit. The alerts get issued when the latest audit data shows a change from the last audit run.

Get Files, LAN Watch, and **Script Fail** alerts are all generated when the script executes on the machine. Alerts are processed as a batch by the system background task that runs every two minutes.

How do I cancel an alert?

To cancel an alert:

1. Select the client machine account checkbox.
2. Press Clear.

The alert information listed next to the client machine ID is removed.

Where is this email coming from?

Email is sent directly from the VSA to the admin email address specified in the alert. The SMTP service in IIS 4 or 5 sends the email directly to the address specified. The From Address in the email can be anything but should be a valid email address. Set the From Address on the Configure page under the System tab.

How do I pass alert information to the script that runs when the alert happens?

You can configure every alert to run a script when the alert email notification is sent. The script can run on the machine that generated the alert or on any machine you like.

To configure an alert to run a script perform the following steps:

1. Check the **after alert run** box
2. Click the **select script** link and select a script from the list.
3. To run the script on a different machine, click the **this machine ID** link and select a machine ID from the list. To run the script on the same machine that generated the alert, leave this link set to *this machine ID*.

You can pass alert specific data to your script. Prior to running the specified script, the system automatically generates several variables (like those created by the Get Variable command) you can use in your script.

The system passes your script variables for the email subject body, and all the **Data Keys** related to the particular alert. To see the data keys for each alert, click the Format Email button. This screen lists the data keys at the bottom. Variable names match these data keys without the <> tags. Typical variables passed to the script include:

	Alert email subject line
	Alert email body
	Machine ID that generated the alert
	Timestamp when the alert occurred

Why would I change the format of the email alert?

You may need to greatly restrict the size of an email alert message if the destination email address is a pager or some hand-held device.

How do I program an alert?

To program an alert:

1. Select the type of alert you want to program
2. Select the client machines you would like to apply the alert to.
3. In the Send Email To field, enter the email address where you want the alert sent to. To enter a separate email address for each client machine, select each client machine and enter an email address, then press Apply. Perform this for each client machine that requires a separate email address. Be sure to press Apply after entering each email address. To send an alert to multiple email addresses, enter the each email address separated with a comma in the Send Email To field.

- **Summary Quick** view summary showing what alerts are active on each machine. The email recipients list for each alert time appears if the alter is active on that machine ID. The alert type label becomes a link for active alerts. Clicking the link automatically selects the specific alert type and populates the form with the settings active in that alert.
- **Agent status** Generate an alert when the agent is offline, first goes online, or someone has disabled remote control on the selected machine. Check the box and enter the amount of time

the agent can be offline before the alert is sent. Checking the box to alert when an agent goes online sends an email every time the agent first goes online. Checking the box to disable remote control sends an email notification at the next quick check-in from the agent on the machine where remote control was disabled.

Note: When ever the KServer service stops, the system suspends all agent online/offline alerts. If the KServer stops for more than 30 seconds, then agent online/offline alerts are suspended for one hour after the KServer starts up again. Rather than continuously try to connect to the KServer when the KServer is down, agents go to sleep for one hour after first trying to connect a couple times. The one hour alert suspension prevents false agent offline alerts when the KServer starts back up.

- **Application Changes** Sends a notification email when a new application is installed on selected machines.
- **Get File Changes** Sends a notification email when a script's **Get File** or **Get File in Directory Path** command executes, uploads the file, and the file is now different from the copy previously stored on the server. If there was not a previous copy on the server, the alert is sent. The VSA issues the alert only if **send alert if file changed** option has been selected in the script.
- **Hardware Changes** Sends a notification email when a hardware configuration changes on the selected machines. Detected hardware changes are the addition or removal of: **RAM , PCI devices, disk drives**.
- **Low disk space** Sends a notification email when available disk space falls below the entered percentage of free disk space. When Low disk space is selected, the percentage of free disk space field appears.
- **New Agent installed** Sends a notification email when a new Agent is installed on a client machine in the selected groups.
- **Event Log** Sends a notification email when the selected machines write an event to the NT event log. When **Event Log** is selected, the three types of event log entries are shown: **System** , **Security** , and **Application** are the three event log entries that, when made, send out a notification email.
- **LAN Watch** Sends a notification email when the LAN Watch scan detects a new device connected to the machine's LAN.
- **Protection Violations** Sends a notification email when selected security breaches occur on a client machine: **File integrity violation, File access violation, and Network access violation.**
- **Script Exec Failure** Sends a notification email when a script fails to execute on a client machine.
- **System Alerts** Sends a notification email when selected events occur on the System Server: Admin account disabled and KServer stopped.
- Patch Alert is set in the Patch Alert function under the Patch Mgmt tab. The system sends the selected administrator an email alert whenever Scan Machine discovers one of the three different patch alert cases.

  1. A new patch is available for the selected Machine ID.
  2. A patch installation failed on the selected Machine ID.
  3. The patch location for a new patch available for any machine is missing. See Patch Location for details.
  4. Newly discovered patches have been added to all Patch Approval policies. See Patch Approval for details.

Depending on the alert selected, the information provided will change. Some alerts require you to enter a number or select a checkbox. After selecting an alert, make sure you enter the necessary criteria in the field, if necessary.

The email address is shown in the Email Address column next to each client machine.

Note: The System Alerts notification does not provide a client machine list. The events listed only apply to the System Server.

Explanation of items on this page

The following selections are accessible from the Alerts function:

Apply

Applies the information entered. Confirm the information in the client machine list.

Clear

Clears all entered information. Selecting a client machine then pressing Clear deletes any entered alert information.

Copy

Only active when **Summary** is selected. Copy takes all the alerts settings for the selected Machine ID (select by clicking the select machine ID link) and applies the same settings to all other checked machine IDs.

Select Alert to Activate

- **Agent status**. Generate an alert when the agent is offline, first goes online, or someone has disabled remote control on the selected machine. Check the box and enter the amount of time the agent can be offline before the alert is sent. Checking the box to alert when agent goes online sends an email every time the agent first goes online. Checking the box for disable remote control sends an email notification at the next quick check-in from the agent on the machine where remote control was disabled.
- **Application Changes** Sends a notification email when a new application is installed on selected machines.
- **Get File Changes** Sends a notification email when files retrieved from remote machines via a script Get File command changes from the last time the Get File command ran. The Get File command must have either the Overwrite existing file and send alert if file changed setting or the Save existing version, get file, and send alert if file changed setting selected.
- **Hardware Changes** Sends a notification email when a hardware configuration changes on the selected machines. Detected hardware changes are the addition or removal of: **RAM , PCI devices, disk drives**.
- **Low disk space** Sends a notification email when available disk space falls below the entered percentage of free disk space. When **Low disk space** is selected, the percentage of free disk space field appears.
- **New Agent installed** Sends a notification email when a new Agent is installed on a client machine in the selected groups.
- **Event Log** Sends a notification email when the selected machines write an event to the NT event log. When **Event Log** is selected, the three types of event log entries are shown: **Error**, **Security** , and **Application** are the three event log entries that, when made, send out a notification email.
- **LAN Watch** Sends a notification email when the LAN Watch scan detects a new device connected to the machine's LAN.
- **Protection Violations** Sends a notification email when selected security breaches occur on a client machine: **File integrity violation, File access violation, and Network access violation.**
- **Script Exec Failure** Sends a notification email when a script fails to execute on a client machine.
- **System Alerts** Sends a notification email when selected events occur on the System Server: **Admin account disabled** and **KServer stopped**.
- **Patch Alert**. Set in the Patch Alert function under the Patch Mgmt tab. The system sends the selected administrator an email alert when ever Scan Machine discovers one of the three different patch alert cases.
    1. A new patch is available for the selected Machine ID.
    2. A patch installation failed on the selected Machine ID.
    3. The patch location for a new patch available for any machine is missing. See Patch Location for details.

Email Recipients

Email address where the event notification is sent. You can specify a different email address for each client machine, even if it is for the same event. The "From:" email address is specified in the Server Info function of the System feature tab. The event notification may be sent to more than one email address by putting a comma before each additional address.

Add to current list

Select this radio button to add the email address to the current list of recipients for that alert. If the name is already on the list for a selected machine ID, then any changes to alert settings are applied but the address list remains the same.

Replace list

Set the recipient email list for this alert to the list entered. This over-writes any existing email list.

Remove

Remove an email address from the recipient list for all selected machines **without modifying any alert parameters**. Use this button to quickly remove an email address for alerts without having to worry about setting up alert parameters.

Format Email

Change the default message sent with each email alert by clicking this button.

After alert run...

When an alert is generated you can set up the system to automatically run a script at the same time the email notification is sent out. You can run the script on the machine that generated the alert or any other machine you wish.

Edit icon

Clicking the edit icon between the check box and the machine ID, for any machine, automatically loads the form with the settings matching the selected machine IDs alert.

Machine.Group ID

Lists the client machines according to the Specify Accounts criteria.

Email Address

Comma separated list of email address where the event notification will be sent.

Note: The System Alerts notification does not provide a client machine list. The events listed apply only to the System Server.

Patch > Windows Auto Update

Windows Automatic Update is a Microsoft tool that automatically delivers the latest high priority updates to a computer from both Microsoft Update and Windows Update. Automatic Update is supported in the following operating systems: Windows 2003, Windows XP, and Windows 2000 (SP3 or later). While Windows Millennium Edition (Me) has an Automatic Update capability, it cannot be managed as the above operating systems can.

Windows Auto Update is one feature that cannot be preconfigured in a template account. This is because Windows Automatic Update is only supported by Microsoft on Windows 2000 SP3/SP4, Windows XP, and Windows Server 2003. Since a template account cannot have a specified operating system, a setting for this feature cannot be accomplished in the template account. Also, we need to know the machine's current settings before we can override those settings. The current settings are obtained during the initial patch scan for the machine in question.

This function defines the configuration options for Windows Automatic Update:

Disable

Disable Windows Automatic Update to let patch management control system patching.

User Control

Let machine users control Windows Automatic Update.

Configure

Force Windows Automatic Update configuration to the following settings:

Automatic Update Options:

- Notify user for download and installation
- Automatically download and notify user for installation
- Automatically download and schedule installation

For option "Automatically download and schedule installation", select "Schedule on" to select the day of the week and select "at" to select the hour of the day to install the downloaded patches.

If the Windows Automatic Update Configuration column displays "**Automatic Update not initialized on machine**", the user must select the Automatic Update icon in the System tray to run the Automatic Update Setup Wizard to setup Automatic Updates.

The Disable and the Configure options **override the existing user settings** and disable the controls in Automatic Updates so the user *cannot* change any of the settings.

The checkbox will not be displayed for any machine that either has an operating system **that does not support Windows Automatic Update** or for which the initial patch scan has not been completed.

NOTE for Windows XP SP2 machines: Whenever an administrator disables or forces a specific configuration for Windows Auto Update, a registry setting is updated to prevent the bubble warning from the Security Center icon in the System Tray to be displayed for Automatic Updates. This is done to avoid end-user confusion since the end-user will not be able to make any changes to the Automatic Updates configuration. It is possible that some anti-malware tools will see this registry setting change as an attempt by malware to eliminate the user warning and therefore will reset the warning to "on".

Patch Mgmt > Pre/Post Script

Use Pre/Post Script to automate new machine preparation and setup by running scripts to perform common preparation tasks for each machine. You can specify a script to run prior to and/or after the scheduled Initial Update task.

Just select the machine, select the script to run before or after Initial Update and click Set.

NOTE: The Agent for the KServer will not be displayed on the Pre/Post Script screen. Initial Update cannot be used on the KServer; therefore, pre/post scripts are not used.

Patch Mgmt > Office Source

Office Source displays the current Office installation source location. This data is only available following the initial patch scan. Only machines with Office or an Office component application installed are displayed on this screen. Multiple entries for a given machine may be seen because the machine contains one or more Office component applications, such as FrontPage or Project, that were installed separately from their own installation source and were not part of the Office installation.

The displayed source location may be changed from the default CD-ROM (the typical installation source) to a network share or a directory on a local hard drive. This optional source may be configured to be read-only. It must contain an exact copy of the installation media contents including all hidden files and/or directories. By changing the installation source to a network share or a local directory, those patches that require the Office installation source for installation can get access without prompting the user for the installation media.

Usage:

To use this feature, the machine must have a credential set. 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.

Add the network share as a UNC path (i.e., \\machinename\sharename) or a local directory as a fully qualified path (i.e., C:\OfficeCD\Office2003Pro) in the installation source text box. Select the machine whose Office source location you want to change, and click on the **Apply** button. The specified location will be validated to be sure that the location is accessible from the machine and that the installation source in the specified location contains the correct edition and version of Office or the Office component application. Only after the validation succeeds, will the machine's registry be modified to use the specified location.

The original installation source (typically the CD-ROM) can be restored at any time. Select the machine whose Office source location you want to reset back to its original state, and click on the **Reset** button.

Processing:

The installed Office Source information (location, product code, etc.) is required to permit validation of the installation source modified by an admin. The standard patch scan process collects this information and includes it with the patch scan results. This data is placed in the database along with the rest of the patch data when the patch scan results are processed following the patch scan. Office Source information will not appear in the Office Source page for existing systems until a patch scan has been completed. For all machines added after verssion 4.7 has been installed, the initial patch scan will collect this data making it available available for initial patching.

When changing the Office Source to a new location (network share, etc.), the change is not immediate. It will take several minutes to perform the validation before the machine's registry is updated with the new validated Office Source location. When a new location is entered for a machine in the Office Source page and the "Apply" button is selected, a script is scheduled for the selected machine to perform the validation process. In this process, the new source location is searched for the appropriate Office MSI file, and it is copied back to the machine's temp directory to validate accessibility to the new location. Then the MSI file is checked to be sure that its internal product code matches the product code of the Office installation on the machine. A small XML file is created with the appropriate validation data and the MSI file is deleted from the machine. This small XML file is then returned to the KServer and is processed (very similar to the patch scan processing). The contents of this small XML file are evaluated and the database is updated with the validation results. If the validation is successful, a new script is executed on the machine to update the machine's registry with the new Office Source location and the Office Source page will show the status of "Office Source Updated".

Note: To take advantage of this feature, set the Office patches' command line switch to "/Q" to prevent the presentation of the Office patch installation dialog from being presented. Go to the Patch Mgmt > Command Line screen to accomplish this.

Note: Even though the process of deploying Office patches can be greatly simplified by eliminating the need for the user to provide the installation source media when requested by the patch, other issues may still be present.

Some patches, and particularly Office service packs, will still display progress dialogs even though the silent installation switch ("/Q") is used. These will not require any user

intervention.

Some patches and service packs will display a modal dialog indicating the update has completed, again even though the silent installation switch ("/Q") is used. This will require the user to click on the OK button to dismiss the dialog. Until this happens, the patch installation script will appear to be hung and will not complete until this dialog is dismissed!

Some Office service packs will fail for apparently no reason. Checking the machine's application event log reveals that another Office component service pack failed. This has been observed with Office 2003 service pack 2 requiring the availablility of FrontPage 2003 service pack 2. When the Office source loaction for the FrontPage 2003 was configured, the Office 2003 service pack 2 finally successfully installed.

Patch Mgmt > Command Line

This function defines the command line switches used to silently install the specified patch. Occasionally a patch is released that does not utilize the normal switch settings or the patch database has not been updated with the new switches. If you find a patch can not successfully install with the current **patch settings**, you can change them with this function.

Locate patch switches by clicking on the Q Number link and reading through the knowledge base article.

Patches and service packs for all machines (both missing and installed) that match the Machine ID/Group ID filter are listed here. To keep the amount of displayed data to a reasonable amount, the patches that are displayed are dependent on the filter drop down list.

WARNING: Changes to the switches effect all administrators.

Note: Because changes to the command line switch settings effect all administrators that deploy this patch, only a Master Administrator can access this function.

Usually you want to load a patch without requiring any user interaction at all. The system support batch installs of multiple patches at the same time and reboots once at the end of all patch installations. Therefore, try to suppress automatic reboot wherever possible.

Typical patch file switch settings for silent, unattended installs without reboot:

/u /q /z - Typical switch settings to silently install most new Microsoft Operating System patches. This is the default used by the system for any new patch.

/quite /norestart - 2003 and very recent patches have begun using this command line.

/m /q /z - Typical switch settings used by older patches released for Windows NT4.

/q:a /r:n - Internet Explorer and other application switch settings to install in quiet administrator mode (q:a) and not automatically reset (r:n) when the install completes.

Other switch settings found with Microsoft patch installations include:

/?: Display the list of installation switches.

/u: Use Unattended mode.

/m: Unattended mode in older patches.

/f: Force other programs to quit when the computer shuts down.

/n: Do not back up files for removal.

/o: Overwrite OEM files without prompting.

/z: Do not restart when the installation is complete.

/q: Use Quiet mode (no user interaction).

/l: List the installed hotfixes.

/x: Extract the files without running Setup.

Microsoft Office command line switches

The only switch permitted for use with Microsoft Office related patches (Patch ID starts with "ODT-") is "/Q". If "/Q" is not specified, Microsoft Office 2000 switches will be automatically reset to blank (no switch), and Microsoft Office XP and 2003 switches will be automatically reset to " /INSTALL-AS-USER". Microsoft Office 2003 patches may also include the " /MSOCACHE" switch used to attempt a silent install if the MSOCache exists on the machine. These settings are enforced by the application.

NOTE: The " /MSOCACHE" switch only applies to Office 2003. When the patch database is updated, this switch is automatically added to all Office 2003 patches where an administrator has never modified a particular patch's command line switches. It is not automatically added to Office 2003 service packs. When this switch is used, the system determines if the MSOCache exists on the target machine. If the MSOCache does exist and this switch is used, the system will automatically use the run silently switch ("/Q") thereby relying on the MSOCache rather than requiring the actual installation media. If the MSOCache does not exist on the target machine, the existing switch will be used. If a patch installation fails that uses the "/MSOCACHE" switch, it typically means that the MSOCache could not be used by the patch. In this case, you must clear out all command line switches for this patch. This will result in the "/INSTALL-AS-USER" switch to be automatically

added. Re-running the patch installation should now succeed. Unfortunately, this will require user intervention and also probably require the Office 2003 installation media.

Special server side command line switches

Special server side switches exist that may be used to direct the system to deploy a patch in a particular way.

/INSTALL-AS-USER - Tells the system to only install this patch as a user. Some (rare) patches do not install successfully unless someone is logged onto the machine. Add this switch if you find a patch is failing to install if no one is logged in. **WARNING:** This setting conflicts with the **Skip update if user logged in** setting found in Reboot Action. /INSTALL-AS-USER requires that a user be logged in to install.

/DELAY-AFTER=xxx - After the install wait xxx seconds before performing the reboot step. The reboot step starts after the install package completes. Some (rare) installers spawn additional programs that must also complete before rebooting. Add this switch to give other processes time to complete after the main installer is done.

Patch Mgmt > Patch Location

This function defines the URL from which each patch can be downloaded.

Note: Only Master Administrators get access to this function.

Patches and service packs for all machines (both missing and installed) that match the Machine ID/Group ID filter are listed here. To keep the amount of displayed data to a reasonable amount, the patches that are displayed are dependent on the filter drop down list.

The patches that show up as **Path missing** are typically patches where each language requires a separate download. For these, you can enter the patch yourself for the language you need. You can manually enter the location of the patch on this same page.

To find the URL to a missing path perform the following steps:

1. Click the Q number listed for the missing path.
2. Read through the Knowledge Base article and locate the download for product referenced **to the left of the Q number**.

Note: There may be several products referenced for the same Patch ID. For instance, each Windows operating system is a different product. Also, patches can be different for specific service packs of the operating system.

3. Click on the download link for your product. If a **different patch is available for each language**, you will be brought to a page to select a language.
4. Select the language you need.
5. Click Download link or button and download the patch file.
6. On your web browser, click the History icon to **view your URL history**.
7. Locate the file you just downloaded for your history list. Typically, the file will be in the **download.microsoft.com folder**.
8. **Right-click** the filename you just downloaded and select **Copy** from the menu. This copies the entire URL into your clipboard.
9. Return to the **Patch Location** function and:
   i. Paste the URL into the **New Location** edit box.
   ii. Select the radio button to the left of the Patch ID for which you are inputting a patch location.
   iii. Click the Apply button.

Remote Cntl Tab

View and operate managed machines as if they were right in front of you simply by clicking its machine ID.

- Automatically connects the administrator to the remote computer independent of any gateway or firewall configurations, even behind NAT
- Work independently or with the user to solve problems interactively where both parties can see what is happening in real time
- Policy settings allow users to block remote control or require administrators to ask permission before accessing a machine
- Integrates four best of breed remote control packages: WinVNC, pcAnywhere™ (Symantec), RAdmin (Famatech), or Terminal Server (Microsoft)
- FTP to any managed machine and access files even behind NAT gateways and firewalls
- Direct chat with any managed machine. Perfect for supporting dial up users with only a single phone line. Remote control and chat at the same time.
- Manual Control allows you to help remote machine even without a agent.

To access the Assistant, click Assistant from any function page.

The following functions are available in the Remote Cntl feature tab:

Functions	Description
Control Machine	Allows administrators to view and/or take control of a client machine's desktop remotely for troubleshooting and/or instructional purposes.
Video Streaming	Remote control machines that do not have an agent installed.
Reset Password	Reset the password for an local account on a managed machine.
Select RC Type	Specify the type of remote control software the VSA uses on a per machine basis. WinVNC, Remote Administrator, pcAnywhere, and Terminal Server are all supported.
Set Parameters	Specify the remote control settings to use with each remote control package.
Preinstall RC	Install the remote control service
Uninstall RC	Uninstall the remote control service
FTP	Initiate an FTP session with any remote managed machine.
Chat	Start a chat session between an administrator and any remote machine.
Send Message	Allows administrators to send network messages to selected client machines.
Task Manager	Remotely executes the NT task manager and displays data in the browser.

Control Machine

Remote Cntl > Control Machine

Assistant

In setting up a remote control session, the Agent eliminates gateway and port blocking problems by always initiating outbound connections from both the target machine and the administrator machine. Helper applications, unique to each supported remote control application, automatically determine the optimal routing path between the administrator machine and the target machine. If a direct connection is not possible then the helper applications route the remote control traffic through the VSA server on the same port used by the agents to check-in (default 5721).

Select user notification - Decide how you want to tell the user a remote control session of their machine is about to begin.

- **Silent** - do not tell the user anything. Take control immediately and silently.
- **Notify** - A dialog box notifies the remote user that the Administrator starting remote control.
- **Ask** - ask user if it is alright to begin a remote control session. Remote control can not proceed until the user clicks the **Yes** button. If nothing is clicked after 1 minute, No is assumed and the VSA removes the dialog box from the target machine.

Initiate remote control simply by clicking the name of the target machine. Only client machines with the Available to remote control icon (see icon list below) can be remote controlled and will have live links; all others will be inactivated. Icons next to the client machine ID indicate current connection status for that machine.

Available to remote control

Remote control has been disabled by the user

The Agent is currently offline

The Agent has never checked in

Note: Users can disable remote control from the agent menu. You can deny users this ability by removing Disable Remote Control from the Agent menu.

Remote Control VSA Server - Click this link to remote control the VSA server itself. Since you can not install an agent on the same machine as a VSA Server is loaded, use this link to remotely administer your VSA server.

Enable verbose relay checkbox.

Remote control to machines behind firewalls and NAT gateways may be relayed through the VSA server. A helper application relays this traffic. Checking this box displays status information for the normally invisible relay application.

Some reasons for remote control failure are:

- The administrator machine is blocking outbound traffic on the agent check-in port (default 5721). The firewall may need to be reconfigured.
- The target machine is on a slow connection. Let the applications run longer than the timeout period and see if that works.
- Wrong primary KServer address - Remote control can only connect through the primary KServer address. The agent can connect through either the primary or secondary address. Verify the remote machine can see the primary KServer address set in Check-in Ctl under the agent tab.

Related Info

Remote Cntl > Video Streaming

In setting up a Video Streaming session, the Agent eliminates gateway and port blocking problems by always initiating outbound connections from both the remote machine and the administrator machine. Helper applications, unique to each supported remote control application, automatically determine the optimal routing path between the administrator machine and the target machine. If a direct connection is not possible then the helper applications route the remote control traffic through the VSA server on the same port used by the agents to check-in (default 5721).

The Video Streaming function is only available in the Enterprise Edition of the system.

Click this button to start waiting for remote control requests from users.

The administrator must click the Wait for remote control request button to start a video streaming session.

Ask the user to click the administrator name.

Users got to /getHelp.asp and click the administrator name to invite in the administrator to remote control their machine.

Use alternate remote control

The default remote control service uses **WinVNC**. Check this box to use **RAdmin** as the remote control service.

Some reasons for remote control failure are:

- You accessed the VSA from a different address. The helper application gets connection information from a cookie on the local machine. To access this information, the helper passes the URL of the VSA to Windows. Say you downloaded the helper from www.yourVSA.net. Then you open a new browser and access the VSA by typing in its IP address 192.168.1.34. The VSA drops a cookie for 192.168.13.34 while the helper tries to get a cookie corresponding to www.yourVSA.net. The helper won't find the cookie. If this happens to you, just download a new helper application and try again.
- The administrator machine is blocking outbound traffic on the agent check-in port (default 5721). The firewall may need to be reconfigured.
- The target machine is on a slow connection. Let the applications run longer than the timeout period and see if that works.

Remote Cntl > Reset Password

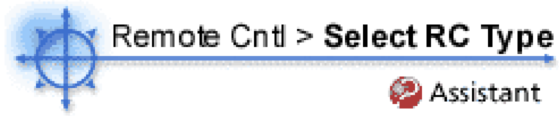
Use this function to set the password for any user account on a managed machine. Use this tool to reset the Administrator password on all your managed machines when:

- Your Administrator password is compromised.
- Someone leaves your organization who knew the Administrator password.
- It is time to change the Administrator password as part of a good security policy.

The **username** must already exist on the target machine. If the username does not already exist, checking the **Create new account** checkbox creates a new account with the specified password.

Reset Password returns an error if you attempt to reset the password for a username that is not already created on the managed machine or if you create a password for an account that already exists.

Select RC Type



Select Type specifies which remote control package the VSA uses to remotely manage a machine under the Control Machine function. You can assign different packages to different machines.

The VSA supports the following third party remote control packages.

1. **WinVNC** - This open source, freely available,remote control package comes bundled with the VSA. WinVNC is the default package used on all managed machines.
2. **Remote Administrator** - RAdmin is a commercially available remote control package offering both high speed and file transfer capability. Use RAdmin where bandwidth limitations exist or you need remote file transfer to the machine. The full version of RAdmin bundled with the VSA expires 30 days after first use.
3. **pcAnywhere** - The VSA supports this widely used remote control package from Symantec. The VSA allows you to use several existing installations of pcAnywhere across firewalls and through gateways without having to port map the gateway or modify the registry of the managed machines.
4. **Terminal Server** - Microsoft's Terminal Server runs on Windows 2000 and some Windows NT servers. You are required to obtain Client Access Licenses from Microsoft for every administrator location.

Assign any of the above remote control packages to a machine by:

1. Select the type of package to use from the drop down list.
2. Check the box to the left of all the machine IDs you want to use that remote control with.
3. Click the Assign button.

Remote Cntl > Set Parameters

This page sets the default parameters for your remote control session. These settings are remembered on a per administrator basis. Each time you start remote control, the VSA uses the last settings values.

WinVNC:

With WinVNC the administrator can specify viewer settings used on the administrator machine. Specify your selection prior to starting the WinVNC helper application, **KaWinVNC.exe**.

- **Full Screen mode** - The entire display of the administrator machine is used to display the screen contents of the target machine. Exit full screen mode by typing Ctrl-Esc Esc, then right-click on the vncviewer icon.
- **View Only Mode** - The administrator can view the remote machine. No mouse or keyboard events are sent to the target machine.
- **Restrict to 8-bit color** - The display on the listening machine is set to 8 bits. This is useful for slower connections.
- **Hide WinVNC system tray icon on the remote machine -** Check this box to hide the WinVNC icon on the remote machine.

Click the machine ID of the PC you wish to remote control. The VSA then tasks the agent to start WinVNC on the target machine at the next check-in. **If WinVNC is not already running on the target machine, the agent starts it automatically.** The displayed countdown tells the administrator the maximum amount of time to wait before remote control starts.

Note: If WinVNC is not already installed on the target machine, the VSA automatically installs it and starts the service (without a reboot!).

Remote Administrator:

With RAdmin the administrator can initiate any of RAdmin's modes or settings. Specify your selection prior to starting the RAdmin helper application, **KaRAdmin.exe**.

- **Full Control Session** - The administrator can view and remotely operate the remote machine.
- **View Only Session** - The administrator can view the remote machine. No mouse or keyboard events are sent to the target machine.
- **File Transfer Session** - Start a file transfer (FTP) session with the remote machine. This mode presents you with two standard file browsers, one for the target machine and one for the administrator machine. Drag and drop files between the two machines in this mode.
- **Full Screen View Mode** - The entire display of the administrator machine is used to display the screen contents of the target machine. This option is only available in a Full Control or View Only session.
- **Encrypt Data Stream** - Checking this boxes encrypts all traffic between the administrator and target machines.
- **Update/sec** - Sets the maximum number of update per second RAdmin generates. Higher update rates consume more CPU cycles on the remote machine.
- **Color Format** - Specify the color depth to use for remote control. You can select 16, 8, or 4 bit color. More color depth uses more bandwidth.

Click the machine ID of the PC you wish to remote control. **If RAdmin is not already running on the target machine, the agent starts it automatically.** The displayed countdown tells the administrator the maximum amount of time to wait before remote control starts.

Note: If RAdmin is not already installed on the target machine, the VSA automatically installs it and starts the service (*without a reboot*!).

pcAnywhere:

The VSA supports existing installations of pcAnywhere. Now you can use pcAnywhere through firewalls and across gateways without having to modify your network infrastructure.

Click the machine ID of the PC you wish to remote control. **If pcAnywhere is not already running on the target machine, the agent starts it automatically.** The displayed countdown tells the administrator the maximum amount of time to wait before remote control starts.

Note: The VSA does not bundle or automatically install pcAnywhere.

Terminal Server:

The VSA supports existing installations of Terminal Server on managed machines (with an Agent). Now you can use Terminal Server through firewalls and across gateways without having to modify your network infrastructure.

Note: The VSA does not bundle or automatically install Terminal Server on the remote machine.

Remote Cntl > Uninstall RC

The remote control system automatically detects if either **WinVNC** or **RAdmin** is already installed on the target machine. If not, then the VSA automatically installs and starts the selected service for you.

If an existing installation of WinVNC or RAdmin has problems then the VSA may not be able to establish a remote control session. If remote control fails then running the Remove RC function on that machine will clean out any existing problem installs and load a fresh copy with the next remote control attempt.

Note: Uninstalling the Agent will not remove the installed remote control package. Use Remove RC to uninstall remote control prior to deleting the agent.

Uninstall

Clicking uninstall schedules a script to remove either WinVNC or RAdmin from all selected machine IDs. WinVNC is removed from machines that are currently assigned WinVNC as their remote control package. RAdmin is removed from machines that are currently assigned RAdmin as their remote control package.

When an uninstall is pending on any machine ID this page automatically refreshes every 5 seconds until the script completes.

Note: Remove RC will not uninstall pcAnywhere or Terminal Server.

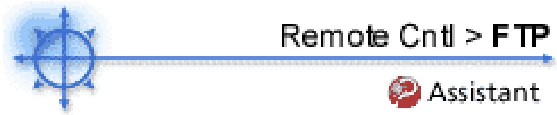
Cancel

Cancel pending uninstall scripts for any selected machine IDs.

Last Status

Pending indicates the uninstall will run the next time that machine checks into the VSA. Otherwise, this column displays the status and time of the last time uninstall ran on that machine.

FTP



Remote Cntl > FTP

Assistant

Just like the Control Machine function, the Agent eliminates gateway and port blocking problems by always initiating outbound connections from both the target machine and the administrator machine. Helper applications, unique to FTP, automatically determine the optimal routing path between the administrator machine and the target machine. If a direct connection is not possible then the helper applications route the remote control traffic through the VSA server on the same port used by the agents to check-in (default 5721).

The VSA uses the FTP client built into **Internet Explore** so you can operate with the same Windows look and feel. Once the FTP session has been initiated, a new browser pops up displaying the contents of a fixed disk on the remote machine. Just drag and drop files as normal.

Select a remote machine to FTP with simply by clicking the name of the target machine. Only client machines with the *Available to remote control* icon (see icon list below) can be remote controlled and will have live links; all others will be inactivated. Icons next to the client machine ID indicate current connection status for that machine.

OK **Available to remote control**

Remote control has been disabled by the user

The Agent is currently offline

The Agent has never checked in

> **Note: Users can disable remote control from the agent menu. You can deny users this ability by removing Disable Remote Control from the Agent menu.**

FTP to VSA Server - Click this link to start an FTP session with the VSA server itself. Since you can not install an agent on the same machine as a VSA Server is loaded, use this link to remotely administer your VSA server.

Select Remote Drive To FTP To. The browser window that opens displays the contents of a single fixed disk drive. Choose which drive on the remote machine to access from the list in step 2.

> **Note: The VSA can only determine how many fixed disks a remote machine has via its Latest Audit function. If you have not run Latest Audit on the selected machine, your only choice will be C:**

Some reasons for remote control failure are:

- The administrator machine is blocking outbound traffic on the agent check-in port (default 5721). The firewall may need to be reconfigured.
- The target machine is on a slow connection. Let the applications run longer than the timeout period and see if that works.

Related Info

Remote Cntl > Chat

Use Chat to initiate or continue chat sessions with user machines. Simply click the Machine ID of the machine you wish to start chatting with. A chat session window opens on the Administrator's machine and a chat window opens in a browser on the remote machine the next time it checks in.

Multiple chat sessions may be active at the same time. Each window title displays the Machine ID name for that session.

Multiple administrators may join the same chat session by clicking the **Join Session** link

The system automatically removes all messages *older than one hour*.

Machine ID link

Click the name of the remote machine to start a chat session with that machine.

Join Session link

Multiple administrators may participate in the same chat session with a user. If a chat session is in progress, the **Join Session** link appears next to that machine ID. Click this link to join the session. If the session was abnormally shut down, click this link to restart the chat session and recover all messages for the session.

Play tone with each new message

Check this box to cause a tone to sound every time a new message is sent or received by a chat window.

Customize the web page users see here

Click the **here** link to view and edit the web layout of the user access page. User Access is a frame set consisting of three pages: header frame, left frame, and right frame. You can select any page you like for the Header frame and the Left frame. You can also adjust the boundary location between the frames. System control pages run in the Right frame and can not be altered.

<table>
<tr><td colspan="2"><b>Header frame</b>
Add customer header files here</td></tr>
<tr><td><b>Left frame</b>
Add custom links here</td><td><b>Right frame</b>
System control pages run in this frame.</td></tr>
</table>

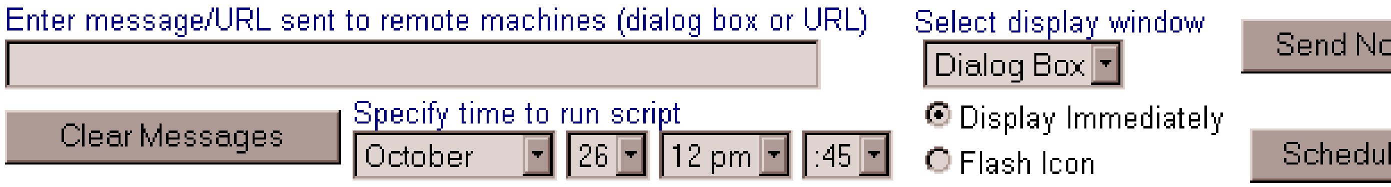
NOTE: Only master administrators may customize the web page.

Send Message

Remote Cntl > **Send Message**

Assistant

The Send Message feature is used to send network messages to a select group of users. Messages can be sent immediately at the next client machine check-in, or can be scheduled to be sent at a future date and time. Users can also be notified by a conventional Windows dialog box or through a browser window, which can automatically display an administrator-selected URL. This feature can be handy, for example, to automatically take users to a Web page displaying an updated contact sheet or other relevant information.



The following elements are displayed in the Send Message function:

Enter message/URL sent to remote machines (dialog box or URL)
Enter the message that is to be sent to client machines.

Select Display Window
This selects the manner in which the user is notified on the client machine. The default is dialog box, which displays a standard Windows dialog box with the network message. The browser selection displays the message in a Web browser window.

Send Now
Pressing send now sends the message when the recipient's machine conducts its next check-in. If a future date and time is set in the Specify Time to Run Script field and Send Now is pressed, the future date and time settings are ignored and the message is sent immediately at the next client machine check-in.

Clear Messages
Pressing Clear messages clears the queue from any messages that have not been delivered to client machines. The queued message can be viewed in the Messages Not Yet Sent column of the display. Select the checkbox next to the client machine whose message queue is to be cleared, then press clear messages.

Specify time to run script
Sends the message at a future date and time. Enter the text message and schedule a future date and time, then press Schedule. The message is queued and appears in the Messages Not Yet Sent column until the recipient client machine(s) conduct their next scheduled check-in.

Schedule
Pressing Schedule queues the message so that it is sent at a future date and time specified in the Specify Time to Run Script field.

Display Immediately/Flash Icon
This setting determines how client machine users are notified once their message has been retrieved from the Server. Display Immediately notifies the user immediately; Flash Icon flashes the Agent icon in the system tray until the user clicks the icon. The message is then displayed according to the settings in Select Display Window.

Machine.Group ID
Lists the client machines according to the Specify Accounts criteria.

Messages Not Yet Sent
This columns shows the message queue. Once message are sent, the queue is cleared. If messages are still displayed, they can be cleared by selecting the appropriate client machines checkbox and pressing Clear Messages.

Select All / Unselect All

Select All will select all user accounts on all account pages. Unselect All will unselect selected user accounts on all account pages. For individual accounts, select the checkbox next to the machine.group ID.

Check-in status

The check-in status of the machines shown in the client machine list is indicated by the icon shown to the left of the client machine ID. The icons and their status are as follows:

- OK **Agent has checked in**
- 🟨 **Agent has not recently checked in**
- 🟥 **Agent has never checked in**

Remote Cntl > Task Manager

Show me an explanation of the items on this page.

What is Task Manager used for?

Task Manager displays all active tasks on a remote managed system. It replicates the task manager included in Windows with the addition of running it remotely through a browser. Task Manager supports all Windows operating systems, Win9x and up.

Why do I need to wait for task manager results?

Task Manager collects data on the remote machine at the time when you click the name of the machine. Data collection itself runs for 10 seconds and that cannot start until the next agent check-in occurs.

Why does kperfmon show up in the list of tasks?

kperfmon.exe is a small program run by the agent to collect task data on the target machine. It only runs while collecting task data. On some OS configurations kperfmon may take about 4% of the CPU during the 10 seconds that kperfmon collects data.

Explanation of items on this page

Task Manager preforms the same function as Microsoft's Windows NT/2000 task manager. Namely, it lists all currently active processes on a remote machine. Clicking a listed machine name tasks the agent on the managed machine to collect 10 seconds of process data at the next check-in. A count down timer above the list of machine names appears after clicking a machine name telling you how long you may need to wait for the entire process to complete. Task Manager displays the results in tabular form as described below.

Name

Name of the process actively running on the managed machine.

CPU

Percent of CPU time consumed by that process over the 10 second data collection interval.

Mem Usage

Amount of main memory used by each active process.

Threads

Number of active threads associated with each active process.

End Process

You can kill any active process on the managed machine by selecting the radio button to the left of the process name and then clicking the **End Process button**. In addition to killing the active process, it re-collects the task data again.

Assistant

Assist Control Machine

Show me an explanation of the items on this page.

How do I initiate a remote control session to a client machine?

Initiate remote control simply by clicking the name of the target machine. Only client machines with the "Available to remote" control icon (see icon list below) can be remote controlled and will have live links; all others will be inactive. Icons next to the client machine ID indicate current connection status for that machine.

🟩 **Available to remote control**

⛔ **Remote control has been disabled by the user**

🟨 **The Agent is currently offline**

🟥 **The Agent has never checked in**

> **Note: Users can disable remote control from the agent menu. You can deny users this ability by removing Disable Remote Control from the Agent menu.**

What is the ActiveX control for?

This control automatically configures and runs the remote control viewer package for you. The first time you use any remote control function on a new machine, your browser may ask if it is OK to download and install this ActiveX control. **Click yes when asked**.

Can I remote control the VSA server itself?

Yes. Clicking the Remote Control VSA Server link starts a remote control session to the VSA server itself. Use this feature to remotely manage your own VSA server.

> **Only Master Administrators can remotely access the VSA Server.**

How do I use WinVNC?

With WinVNC the administrator can specify viewer settings used on the administrator machine.

- **Full Screen mode** - The entire display of the administrator machine is used to display the screen contents of the target machine. Exit full screen mode by typing Ctrl-Esc Esc, then right-click on the vncviewer icon.
- **View Only Mode** - The administrator can view the remote machine. No mouse or keyboard events are sent to the target machine.
- **Restrict to 8-bit color** - The display on the listening machine is set to 8 bits. This is useful for slower connections.
- **Hide WinVNC system tray icon on the remote machine -** Check this box to hide the WinVNC icon on the remote machine.

Click the machine ID of the PC you wish to remote control. The VSA then tasks the agent to start WinVNC on the target machine at the next check-in. **If WinVNC is not already running on the target machine, the agent starts it automatically.** The displayed countdown tells the administrator the maximum amount of time to wait before remote control starts.

> **Note: If WinVNC is not already installed on the target machine, the VSA automatically installs it and starts the service (without a reboot!).**

How do I use Remote Administrator?

With RAdmin the administrator can initiate any of RAdmin's modes or settings. Specify your selection prior to starting the RAdmin helper application, **KaRAdmin.exe**.

- **Full Control Session** - The administrator can view and or control the screen keyboard and mouse of the target machine.
- **View Only Session** - The administrator can view the remote machine. No mouse or keyboard events are sent to the target machine.
- **File Transfer Session** - Start a file transfer (FTP) session with the remote machine. This mode presents you with two standard file browsers, one for the target machine and one for the administrator machine. Drag and drop files between the two machines in this mode.
- **Full Screen View Mode** - The entire display of the administrator machine is used to display the screen contents of the target machine. This option is only available in a Full Control or View Only session.
- **Encrypt Data Stream** - Checking these boxes encrypts all traffic between the administrator and target machines.
- **Update/sec** - Sets the maximum number of update per second RAdmin generates. Higher update rates consume more CPU cycles on the remote machine.
- **Color Format** - Specify the color depth to use for remote control. You can select 16, 8, or 4 bit color. More color depth uses more bandwidth.

Click the machine ID of the PC you wish to remote control. **If RAdmin is not already running on the target machine, the agent starts it automatically.** The displayed countdown tells the administrator the maximum amount of time to wait before remote control starts.

Note: If RAdmin is not already installed on the target machine, the VSA automatically installs it and starts the service (*without a reboot*!).

How do I use pcAnywhere?

The VSA supports existing installations of pcAnywhere. Now you can use pcAnywhere through firewalls and across gateways without having to modify your network infrastructure.

Click the machine ID of the PC you wish to remote control. **If pcAnywhere is not already running on the target machine, the agent starts it automatically.** The displayed countdown tells the administrator the maximum amount of time to wait before remote control starts.

pcAnywhere connection problems:

- **My viewer is connecting to my machine, not the remote machine.** The VSA relay is telling the viewer to connect to localhost. If you have a pcAnywhere host running on the machine you are viewing from, then the viewer connects to it and not the VSA relay. Right click the pcAnywhere icon in the system tray and select **Cancel Host**.
- **pcAnywhere presents an error dialog saying "Cannot find callhost file: C:\Document and Settings\All Users\Application Data\Symantec\pcAnywhere\Network.CHF".** There is not a "Network" remote control item configured in pcAnywhere. Open the pcAnywhere application and click on the Remote Control function.
  1. Click "Add Remote Control Item".
  2. Create an item named **Network**.
  3. Select TCP/IP as the connection device.
  4. Leave the host name blank.
  5. Close pcAnywhere.

Note: The VSA does not bundle or automatically install pcAnywhere.

How do I use Terminal Server?

The VSA supports existing installations of Terminal Server. Now you can use Terminal Server through firewalls and across gateways without having to modify your network infrastructure.

Note: The VSA does not bundle or automatically install Terminal Server.

With Terminal Server, why can't I logon as a user that is already logged in on a Windows XP

machine?

Windows XP prohibits more than one active connection at a time. While multiple users can be logged onto a Windows XP box at the same time, only one user is considered active and allowed to interact with the machine. Initiating a Terminal Server session across the network proceeds as follows:

1. XP notifies the remote user that another user is active. Proceeding switches out the active user.
2. Ask the active user if it is OK to allow the remote connection. If the user does not answer, OK is returned after a timeout.
3. Present remote user with a logon. The logon causes a switch user event and disconnects the active user.

However - The VSA uses the *port relay* to get through firewalls and gateways. To Windows XP, it appears as if the Terminal Server session is connecting from *localhost*. Using the credential of a currently logged on user this way confuses XP. It can not determine if the user is reactivating the existing session locally or remotely initiating a new connection. **As a result Window XP may hang, requiring a reboot to recover. The VSA can not protect you from this. Do not log on using the user name of an already logged on account.**

How do I install a remote control package?

The VSA automatically installs WinVNC or Remote Administrator on first use. You must install pcAnywhere on both the target machine and administrator machine yourself if you select pcAnywhere. You must install Terminal Server on the target machine.

What does the "Enable verbose relay" checkbox do?

Remote control to machines behind firewalls and NAT gateways may be relayed through the VSA server. A helper application relays this traffic. Checking this box displays status information for the normally invisible relay application.

What are some of the causes for remote control malfunction?

Some reasons for remote control failure are:

- The administrator machine is blocking outbound traffic on the agent check-in port (default 5721). The firewall may need to be reconfigured.
- The target machine is on a slow connection. Let the applications run longer than the timeout period and see if that works.
- Wrong primary KServer address - Remote control can only connect through the primary KServer address. The agent can connect through either the primary or secondary address. Verify the remote machine can see the primary KServer address set in Check-in Ctl under the agent tab.

Assist Remove RC

Show me an explanation of the items on this page.

The VSA remote control system automatically detects if either **WinVNC** or **RAdmin** is already installed on the target machine. If not, then the VSA automatically installs and starts the selected service for you.

If an existing installation of WinVNC or RAdmin has problems then the VSA may not be able to establish a remote control session. If remote control fails then running the Remove RC function on that machine will clean out any existing problem installs and load a fresh copy with the next remote control attempt.

Note: Uninstalling the Agent will not remove the VSA installed remote control package. Use Remove RC to uninstall remote control prior to deleting the agent.

Uninstall

Clicking uninstall schedules a script to remove either WinVNC or RAdmin from all selected machine IDs. WinVNC is removed for machines that are currently assigned WinVNC as their remote control package. RAdmin is removed for machines that are currently assigned RAdmin as their remote control package.

When an uninstall is pending on any machine ID this page automatically refreshes every 5 seconds until the script completes.

Remove RC will not uninstall pcAnywhere or Terminal Server.

Cancel

Cancel pending uninstall scripts for any selected machine IDs.

Last Status

Pending indicates the uninstall will run the next time that machine check into the VSA. Otherwise, this column displays the status and time of the last time uninstall ran on that machine.

Assist Video Streaming

Assistant

HELP HOME

Show me an explanation of the items on this page.

When would I use Video Streaming?

Use Video Streaming to support people on machines that do not have agents installed. It is perfect to help someone quickly on an infrequent basis. If you plan to provide continuous support we recommend you install an agent.

The Video Streaming function is only available in the Enterprise Edition of the system.

Do I need to uninstall Video Streaming after the session is over?

No. When either side terminates the Video Streaming session, the remote client removes all remote control files and registry additions automatically.

Why does the remote user not see any Administrator sessions listed?

All Video Streaming control sessions must be initiated by the Administrator. When the administrator clicks the *Wait for remote control request* button the VSA creates a remote control session naming it with the Administrator's logon name.

Can I run more than one Video Streaming session at a time?

No. Each administrator can only initiate a single Video Streaming session at a time.

Assist FTP

Show me an explanation of the items on this page.

Why can't I see all the fixed disks on the remote machine?

The VSA can only determine how many fixed disks a remote machine has via its **Latest Audit** function. If you have not run Latest Audit on the selected machine, your only choice will be C:

What is the ActiveX control for?

This control automatically configures and runs the remote control viewer package for you. The first time you use any remote control function on a new machine, your browser may ask if it is OK to download and install this ActiveX control. **Click yes when asked**.

Can I FTP to the VSA server itself?

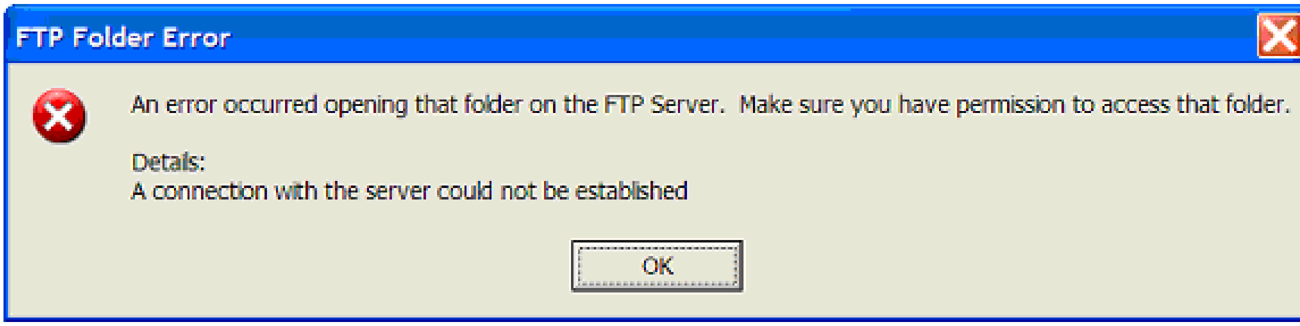
Yes. Clicking the FTP to VSA Server link starts an FTP session to the VSA server itself. Use this feature to remotely manage your own VSA server.

Only Master Administrators can remotely access the VSA Server.

What are some of the causes for FTP malfunction?

Some reasons for remote control failure are:

- You accessed the VSA from a different address. The helper application gets connection information from a cookie on the local machine. To access this information, the helper passes the URL of the VSA to Windows. Say you downloaded the helper from www.yourVSA.net. Then you open a new browser and access the VSA by typing in its IP address 192.168.1.34. The VSA drops a cookie for 192.168.13.34 while the helper tries to get a cookie corresponding to www.yourVSA.net. The helper won't find the cookie. If this happens to you, just download a new helper application and try again.
- The administrator machine is blocking outbound traffic on the agent check-in port (default 5721). The firewall may need to be reconfigured.
- The target machine is on a slow connection. Let the applications run longer than the timeout period and see if that works.
- FTP require **Passive FTP** be turned **off**. If you get the following error after attempting an FTP session:



FTP Folder Error

An error occurred opening that folder on the FTP Server. Make sure you have permission to access that folder.

Details:
A connection with the server could not be established

Then disable Passive FTP on your browser as follows:

1. Open "Internet Options..." from IE's "Tools" menu.
2. Click on the "Advanced" tab.
3. In the "Browsing" section, look for "Use Passive FTP" and **Uncheck** this setting.
4. Click OK and try FTP again.

Assist Chat

Assistant

HELP HOME

Show me an explanation of the items on this page.

Why did my chat window close by itself?

The chat window on the user side has been closed down or redirected. After the chat session on the user side closes down, the administrator side window closes automatically. To restart the same chat session, click the **Join Session** next to the machine ID.

What is the Join Session link for?

Multiple administrators may participate in the same chat session with a user. If a chat session is in progress, the **Join Session** link appears next to that machine ID. Click this link to join the session. If the session was abnormally shut down, click this link to restart the chat session and recover all messages for the session.

Why do the user's browser windows redirect to the chat session?

The default setting for Internet Explorer will reuse open browser windows when any task opens a new URL. This same behavior occurs when you click a link in an email or Word document (the already open browser window is redirected to the new URL). To set Internet Explorer's default behavior to open new URLs in a new window perform the following steps:

1. Select **Internet Option...** from the **Tools menu** of any Internet Explorer window.
2. Click on the **Advanced** tab.
3. Uncheck the box labeled **Reuse windows for launching shortcuts** (in the Browsing section).
4. Click **OK**

Why does my machine make a "clicking" noise every time the chat window refreshes?

Many Windows themes configure the system to play a sound every time Internet Explorer navigates to a new URL. One of these, start.wav, sounds like a click. To turn off the sound perform the following steps:

1. Open the **Control Panel** and select **Sounds and Multimedia**.
2. Click on the **Sounds** tab.
3. Scroll down and select **Start Navigation** (in the **Windows Explorer** section).
4. Select **(None)** from the drop down control labeled **Name:**
5. Click **OK**

Assist Select RC Type

Assistant

HELP HOME

Show me an explanation of the items on this page.

What if the remote control package is not installed on the target machine?

The VSA automatically installs WinVNC or Remote Administrator on first use. You must install pcAnywhere on both the target machine and administrator machine yourself if you select pcAnywhere. You must install Terminal Server on the target machine.

What does the "VSA Server" entry refer to?

Specify the type of remote control package used to remote control the VSA server itself with this row.

Only Master Administrators can remotely access the VSA Server.

Assist Send Message

Show me an explanation of the items on this page.

How do I send a message to client machine?
To send a network message to one or more client machines:

1. Select the checkbox next to the client machine you wish to send a message to. You can select more than one client machine.
2. Enter the message you wish to send by typing it in the **Enter message/URL sent to remote machines** field.
3. In the **Select display window** dropdown menu, select *Dialog Box* or *Browser*.
   - **Dialog Box** Displays the message in a standard Windows dialog box.
   - **Browser** Displays the message in a Web browser window.
4. Select either the *Display Immediately* or *Flash Icon* radio button.
   - **Display Immediately** The message, when sent, is displayed immediately without user intervention.
   - **Flash Icon** The Kaseya Agent icon in the client machine's system tray flashes. The user must click on the icon before the message is displayed.
5. To send the message, press send now. Or, if you wish to schedule the message to be sent at a future date and time, select the date and time using the dropdown menus under **Schedule time to send message**, then press schedule.
6. The message is queued and is shown in the **Messages Not Yet Sent** column. The message is sent at the recipient client machines' next quick check-in.

To cancel a message before it has been sent:

1. Select the recipient client machines' checkbox.
2. Press clear messages.
3. The messages shown under the **Messages Not Yet Sent** column are removed from the queue.

To send a network message to one or more client machines:

1. Select the checkbox next to the client machine you wish to send a message to. You can select more than one client machine.
2. Enter the message you wish to send by typing it in the **Enter message/URL sent to remote machines** field.
3. In the **Select display window** dropdown menu, select *Dialog Box* or *Browser*.
   - **Dialog Box** Displays the message in a standard Windows dialog box.
   - **Browser** Displays the message in a Web browser window.
4. Select either the *Display Immediately* or *Flash Icon* radio button.
   - **Display Immediately** The message, when sent, is displayed immediately without user intervention.
   - **Flash Icon** The Agent icon in the client machine's system tray flashes. The user must click on the icon before the message is displayed.
5. To send the message, press send now. Or, if you wish to schedule the message to be sent at a future date and time, select the date and time using the dropdown menus under **Schedule time to send message**, then press schedule.
6. The message is queued and is shown in the **Messages Not Yet Sent** column. The message is sent at the recipient client machines' next quick check-in.

To cancel a message before it has been sent:

1. Select the recipient client machines' checkbox.
2. Press clear messages.
3. The messages shown under the **Messages Not Yet Sent** column are removed from the queue.

Feature Tab > Backup

Use the functions in the Backup tab to install, configure, and schedule recurring backups for any managed machines.

The following functions are available in the Backup feature tab:

Functions	Description
Schedule Volumes	Schedules backup for selected hard disk volumes on any managed machine.
Schedule Folders	Can independently schedule backup for individual folders.
Backup Status	Review the status of scheduled backups for any machine.
Backup Logs	Review the logs generated by every backup action.
Explore Volumes	Mounts a backup as a new drive letter on the managed machine.
Explore Folders	Copies the .zip archive back to the managed machine.
Verify Images	Verify any volume or folder backup image
Auto Recovery	Select a volume backup image to automatically restore to a selected machine. Requires the machine can still boot and the agent can communicate with the server.
CD Recovery	Boot the remote machine from a CD and then automatically restore a selected volume backup image.
Manual Recovery	Instructions to produce a boot CD to restore a backup image manually by walking through a wizard
Offsite Servers	Specify a machine to act as an offsite server (receives files from a local server)
Local Servers	Specify a machine to act as a local server (sends files to an offsite server)
Offsite Alert	Generate alerts when a local server fails to connect to an offsite server.
Schedule Transfer	Set up a day by day schedule for each local server to push files to an offsite server.
Install/Remove	Install and uninstall the backup driver and software on any managed machine.
Image Location	Path to storage location (usually LAN based file server) to save backups to.
Image Password	Look up the password used to protect backup images.
Folder Backup	Specify a list of folders to backup during Schedule Folders
Backup Alert	Activate/deactivate alerts associated with backup events.
Pre/Post Script	Specify a script to run before and/or after Volume Backup
Compression	Set compression level used by both volume and folder backups
Max File Size	Set a maximum file size used for backup images. Images larger than this

	maximum are broken into multiple files.
Max Log Age	Set the maximum number of days to save backup log data.
Secure Zone	Install a secure zone to support Auto Recovery

Backup > Schedule Volumes

Specify a recurring schedule to backup volumes for the selected machine IDs. You may backup individual drive letters (partitions) or entire disk drives. To **insure recovery from complete disk failure**, you should backup entire disk drives. Only by backing up entire disks **will you capture hidden recover partitions** that may have been installed by your PC system vendor.

Full backups take significant time to complete compared with incremental or differential backups. To save time and disk space, schedule full backups to run less frequently than incremental backups. Typically full backups are scheduled once per week or once per month, while incremental backups run daily. All files associated with the full backup and all incremental backups are saved together in a **full backup set**. You may save any number of full backup sets you wish.

The system saves each full backup set in its own folder. The backup system saves backup images in the path specified in Image Location. Inside the volume path specified in Image Location, backup data gets saved in the following **directory structure**:

- Image Location Path
  - testbox.workstations
    - FldrBackup
    - VolBackup
      - 20060621 18.13.01
        - testbox.workstations2.tib
        - testbox.workstations3.tib
        - testbox.workstations4.tib
        - testbox.workstations.tib
      - 20060628 18.12.55
        - testbox.workstations2.tib
        - testbox.workstations3.tib
        - testbox.workstations4.tib
        - testbox.workstations.tib

Schedule

Click Schedule to set all volume backup parameters assigned to selected machine IDs. The full backup always runs first after clicking Schedule. **To run a new full backup, click Schedule.** Clicking Schedule **creates a new full backup set**.

NOTE: Backups may consume significant network bandwidth when pushing file to the network file store. To prevent congesting the network during normal business hours, schedule backups to run at off hours.

Backup Now

Task a new incremental or differential backup to run immediately. If a full backup does not already exist, the system creates a full backup image.

NOTE: The backup logs always list an incremental or differential backup after clicking Backup Now, even if a full backup image is created.

Incremental

Incremental backups capture all the changes to the target system **since the last incremental** backup. Restoring from an incremental backup requires all previous incremental image file plus the original full backup. Do not remove files from the full backup set directory.

WARNING: Incremental backups detect changes at the sector level. If you defragment your hard disk, a large number of disk sectors will move and appear to change. This results in a large incremental backup file. This is perfectly normal for a sector level backup system.

Differential

Differential backups capture all the changes to the target system **since the last full** backup. To save disk space, only the latest differential backup image is saved with each full backup set. **Select differential backups to minimize backup image storage requirements.**

Full backup every

Select a recurring interval to run the full backup. For example, once per month or once every 3 months.

Save the last N full backup set

Specify the number of full backup sets to keep here. Starting a new full backup, creates a new full backup set. So, entering 3 here will maintain the current full backup, plus that last two full backup sets (full backup plus all incrementals or the differential).

Verify Backup

You may optionally verify each backup image immediately after each full, incremental, or differential backup completes. **Verify takes the same amount of time as the original backup to complete.** Only verify in situations where you question the integrity of the network connection to the image location. You do not generally need to use this option. Use the Verify Images function to spot check backup images any time.

Disks

Disk number to backup. Backup an entire disk to insure any hidden partitions that may have been installed by your PC vendor are also backed up. These hidden partitions may be required to boot your system in the event of a restore.

Partitions

The system lists each available local hard disk for each machine. To include any or all of these drives in the volume backup, check the desired drive letter.

Backup > Schedule Folders

Specify a recurring schedule to backup folders for the selected machine IDs. You may backup any number of folders specified in the Folder Backup function. Folder Backup also lets you exclude specific file times. For example, you may wish to exclude *.avi, *.mp3, and *.bmp files when backing up someone's My Documents folder.

Folder backups perform sector level backups of selected folders. Sector level copying allows the system to backup locked and in-use files so you can safely backup at any time of the day.

Like, volume backups, the system saves folder backups in full backup sets. In addition to full backups, folder backups my capture **incremental or differential** backups also. Each set gets its own folder. Separate Image Location paths may be set for volume and folder backups. Inside the folder path specified in Image Location, backup data gets saved in the following **directory structure**:

- Image Location Path
  - testbox.workstations
    - FldrBackup
      - 20060621 18.13.01
        - testbox.workstations2.tib
        - testbox.workstations3.tib
        - testbox.workstations4.tib
        - testbox.workstations.tib
      - 20060628 18.12.55
        - testbox.workstations2.tib
        - testbox.workstations3.tib
        - testbox.workstations4.tib
        - testbox.workstations.tib
    - VolBackup

Schedule

Click Schedule to set all folder backup parameters assigned to selected machine IDs. The full backup always runs first after clicking Schedule. **To run a new full backup, click Schedule.** Clicking Schedule **creates a new full backup set**.

NOTE: Backups may consume significant network bandwidth when pushing file to the network file store. To prevent congesting the network during normal business hours, schedule backups to run at off hours.

Backup Now

Task a new incremental or differential backup to run immediately. If a full backup does not already exist, the system creates a full backup image.

NOTE: The backup logs always list an incremental or differential backup after clicking Backup Now, even if a full backup image is created.

Incremental

Incremental backups capture all the changes to the target system **since the last incremental** backup. Restoring from an incremental backup requires all previous incremental image file plus the original full backup. Do not remove files from the full backup set directory.

Differential

Differential backups capture all the changes to the target system **since the last full** backup. To save disk space, only the latest differential backup image is saved with each full backup set. **Select differential backups to minimize backup image storage requirements.**

Full backup every

Select a recurring interval to run the full backup. For example, once per month or once every 3 months.

Save the last N full backup set

Specify the number of full backup sets to keep here. Starting a new full backup, creates a new full backup set. So, entering 3 here will maintain the current full backup, plus that last two full backup sets (full backup plus all incrementals or the differential).

Verify Backup

You may optionally verify each backup image immediately after each full, incremental, or differential backup completes. **Verify takes the same amount of time as the original backup to complete.** Only verify in situations where you question the integrity of the network connection to the image location. You do not generally need to use this option. Use the Verify Images function to spot check backup images any time.

Backup > Backup Status

Backup Status displays status for any selected machine by clicking the desired machine ID. Only status for currently available backups are displayed here.

Volume backup status

Displays time volume backup completed, lists volumes backed up, success/failure, and the duration of the volume backup for the most recent full backup and each incremental backup after that.

Folder backup status

Displays time folder backup completed, lists folders backed up, success/failure, and the duration of the folder backup for all the backups saved, as specified in Schedule Folders.

View last backup log

Link to the raw log file returned by the backup subsystem running on each managed machine. Backup Status processes this log when each volume or folder backup completes. You should never need to look at this log file unless backup reports strange or unexplained failures. In those cases, the log may provide more insight into the cause of the backup failure such as identifying corrupt files or disk sectors.

NOTE: Bad disks may cause backup failures. Running Check Disk (CHKDSK.EXE C:) on the drive in question may resolve failures.

Backup > Backup Logs

A log is created for each machine every time a backup operation runs. The log contains the Date, Type, Duration, Result and Description of the backup operation performed.

Click the machine ID of interest to display the backup logs for that machine.

Backup > Explore Volumes

Volume backups may be mounted **as a new drive letter** on the *same machine* or on a *different machine*. The backup volume may then be browsed, just like any other drive, with Windows Explorer. Individual files or folders my be retrieved simply by dragging and dropping files.

NOTE: A user with access rights to the Image Location must be logged in at the time the backup is mounted.

Mount to machine ID

Select to mount the backup image to the same machine ID that the backup image was made on.

Mount to select machine ID

Select to mount the backup image to the different machine ID than the backup image was made on.

Mount

To explore the full or any incremental/differential backup, click the radio button next to the date listed. The complete image, **as of that date**, gets mounted on the remote machine as a new drive letter. Click the **Mount** button to generate a script to mount the backup image. The screen automatically refreshes every 5 seconds and reports status of the mount until the mount script completes execution.

Unplug All

Click the Unplug All button to remove any mounted volume backups.

Backup > Explore Folders

The **Explore Folders** function restores the folder backups to the specified directory on the target machine (either the machine that did the backup or a different machine). Unlike Explore Volumes, this function can not mount the data as a new drive letter. Folder backups are placed on the target machine as folders, maintaining the same structure they had in the backup.

Restore Path
Enter the path on the target machine to re-create the backed up folder into.

Mount to machine ID
Select to mount the backup image to the same machine ID that the backup image was made on.

Mount to select machine ID
Select to mount the backup image to the different machine ID than the backup image was made on.

NOTE: Folder Backup does not support Unplug. Manually delete the restored folders to remove them.

Backup > Verify Images

Verify Images performs a one time verification of any selected volume or folder backup. User this function to spot check that backups are completing successfully. Successful backups may fail to verify if the backup image file was not copies successfully to the Image Location path. This problem typically only occurs in slow or unreliable networks. On slow networks, consider selecting the Verify Backup option in Schedule Volumes and Schedule Folders to verify the backup every time.

Verify from machine ID

Select to verify the backup image stored at the Image Location path from the same machine that performed the backup.

Verify from select machine ID

Select to verify the backup image stored at the Image Location path from a different machine on the same network as Image Location.

Verify Volumes

Select the time stamp of the volume backup image to verify.

Verify Folders

Select the time stamp of the folder backup image to verify.

Backup > Auto Recovery

Automatically restores any volume backup image to the same machine the backup was created on. Use Auto Recovery to restore images **if the agent is still communicating with the server**. Auto Recovery lets you select any backup image (full, incremental, or differential) for the selected machine ID to restore **without any user interaction at all**.

NOTE: Requires Secure Zone installed.

The server and agent configure the hidden secure zone partition to automatically restore the selected backup image from the Image Location path. Once configuration completes, the agent reboots the machine (*without warning*). The machine boots into the secure zone partition and automatically restores the selected backup image.

The restore may be scheduled to run at any time of day or on a recurring schedule. Set a **recurring schedule to auto restore** a machine in a public area subject to abuse by random users.

Schedule

Specify a time of day to restore the image. Remember, the restore will reboot the machine and restore the image without warning the user first.

Restore Now

Restore the backup image to the selected machine ID immediately.

Run recurring

Schedule selected machines to restore the backup image on a repeating scheduled basis.

Select backup to restore

Select a backup image to restore from a drop down control listing all available backups for the selected machine ID.

Restore may fail for any of the following reasons:

- If the Image Location points to a **local driver letter** - When Windows boots, drive letters are automatically assigned to hard drives starting with C: With the disk manager, you can reassign these to any other unused drive letter. For example, you may decide to turn your D: drive into G: and set the Image Location path to G:\backups. The recovery boot process **will not know about the driver letter mapping** and will assign D: to the hard disk. The restore will then **fail trying to access G:\backups**. You can resolve this problem by setting your image location to D:\backups prior to selecting the restore options. Restore will then successfully access D:\backups.
- **Image stored on a USB drive** - Similar to the issue above, when the recovery boot process assigns drive letters, it **may assign the USB drive a different drive letter** than Windows assigned it. You can resolve this problem by setting your image location to the new drive letter prior to selecting the restore options. Restore will then successfully access the USB drive.
- **Image stored on a network drive** - If the remote drive (or the machine hosting the drive) is **not turned on**, or if the username and password have changed, then the recovery boot process will not be able to access the network drive.

Backup > CD Recovery

Restores any volume backup image to the same machine the backup was created on. Use CD Recovery to restore images **if the agent can not communicating with the server**. CD Recovery requires someone to boot the effected machine from a CD. The CD boot communications with the server and automatically restores the image you specify. User do **not need to interact with a wizard or answer any questions**. They only need to boot the machine from a CD.

The boot CD may be created **without specifying which image to restore**. The boot CD communicates with your server and receives instructions at that time, identifying the image to restore. This lets you create the CD in advance and distribute the boot CD to all the locations you manage.

You may create any number of CD images for use by your server. Each administrator may set up their own CD image; you may create a CD image for each group ID; or any other combination you wish.

Create New ISO

Creates a new ISO image to use. You may independently assign a machine image to restore to each CD image. Machine image assignments may be changed at any time **so you do not need to recreate the boot CD when you wish to restore a different machine**.

Share

By default, ISO images are private to the administrator that created it. You may also share an ISO image with other administrators or administrator roles.

Machine ID

Select the machine ID you wish to restore with a boot CD.

Backup Date

Select the backup image (by date) to restore with a boot CD.

Restore may fail for any of the following reasons:

- If the Image Location points to a **local driver letter** - When Windows boots, drive letters are automatically assigned to hard drives starting with C: With the disk manager, you can reassign these to any other unused drive letter. For example, you may decide to turn your D: drive into G: and set the Image Location path to G:\backups. The recovery boot process **will not know about the driver letter mapping** and will assign D: to the hard disk. The restore will then **fail trying to access G:\backups**. You can resolve this problem by setting your image location to D:\backups prior to selecting the restore options. Restore will then successfully access D:\backups.
- **Image stored on a USB drive** - Similar to the issue above, when the recovery boot process assigns drive letters, it **may assign the USB drive a different drive letter** than Windows assigned it. You can resolve this problem by setting your image location to the new drive letter prior to selecting the restore options. Restore will then successfully access the USB drive.
- **Image stored on a network drive** - If the remote drive (or the machine hosting the drive) is **not turned on**, or if the username and password have changed, then the recovery boot process will not be able to access the network drive.

Backup > Manual Recovery

Manual Recovery requires someone at the machine to boot from the CD and navigate through the recovery wizard to restore the backup image. Manual recovery requires a user with knowledge of the Image Location path and the Image Password to restore a backup image.

A damaged boot volume may prevent a system from even booting. To restore images to the system partition, requires that the system boot from a separate partition. This recovery CD provides that image. Follow the on screen instructions to create the Recovery CD and restore a volume.

Backup > Offsite Servers

Use **Offsite Replication** to **safely and securely** transfer backup images from the LAN to a remote location. Typically all machines on a LAN have their Image Location set to store backup images on a LAN based file server. Designating that file server to be the **Local Server** tells the agent on that file server to push all new backup image data to an **Offsite Server** on a transfer schedule you define.

The offsite server listens on any TCP port you specify. The offsite server is always running and listening for connections from local servers. The TCP port may not already be in use on that machine.

Any machine ID may act as an offsite server. You may also have as many offsite servers as you like. Example Offsite Replication configurations include:

1. **One global offsite server** - a local server at each managed LAN pushes data to the global offsite server.
2. **Multiple offsite servers** - several local servers are assigned to each offsite server. Multiple offsite servers used for load balancing reasons.
3. **Cross offsite server** - Support offsite replication for companies with multiple locations. The backup data from one company site is offsited to a second company site. Backup data from the second company site is offsited back to the first site.

The offsite server stores data received from the local servers in the directory specified. Data from each individual local server is stored in a sub-directory **named after the machine ID** of the local server. **The offsite server directory may be a UNC path pointing to a directory on a network file share.** The offsite server *must* have a credential set in order to access the network. The following diagram illustrates a typical offsite server directory structure.

- Offsite Server Path
    - localserver.company1
        - machine1.company1
        - machine2.company1
        - machine3.company1
    - localserver.company2
        - machine1.company2
        - machine2.company2
        - machine3.company2
    - localserver.company3
        - machine1.company3
        - machine2.company3
        - machine3.company3

NOTE: The Offsite Server requires a credential be set to operate correctly.

Only file changes are pushed to the offsite server. Interrupted file transfers are picked up where they left off the next time the local server component runs. Offsite replication uses the same communications technology used in the agent/server communications. All traffic is 256-bit encrypted. Broken file transfers are automatically restarted at the point the left off. Restarting the file transfer from the beginning is **not required**.

WARNING: You may assign the offsite server to be the same machine as the local server. This is NOT recommended but is allowed to support copying image data to secondary disk drives.

Backup > Local Servers

Use **Offsite Replication** to **safely and securely** transfer backup images from the LAN to a remote location. Typically all machines on a LAN have their Image Location set to store backup images on a LAN based file server. Designating that file server to be the **Local Server** tells the agent on that file server to push all new backup image data to an **Offsite Server** on a transfer schedule you define.

Typically the file server used to host the Image Location is designated as the local server. For each local server specify:

1. The offsite server to push files to
2. The local directory path to push to the offsite server
3. Optional bandwidth limit

NOTE: Specify when files are pushed using Schedule Transfer

The local server directory may be a UNC path pointing to a directory on a network file share. The local server *must* have a credential set in order to access the network.

NOTE: The Local Server requires a credential be set to operate correctly.

Individual local server data is stored in a sub-directory on the offsite server, named after the machine ID of the local server.

Only file changes are pushed to the offsite server. Interrupted file transfers are picked up where they left off the next time the local server component runs. Offsite replication uses the same communications technology used in the agent/server communications. All traffic is 256-bit encrypted. Broken file transfers are automatically restarted at the point the left off. Restarting the file transfer from the beginning is **not required**.

WARNING: You may assign the offsite server to be the same machine as the local server. This is NOT recommended but is allowed to support copying image data to secondary disk drives.

Create

Assign the selected machine ID to act as a **Local Server**, sending all its data to the **selected Offsite Server**.

Bandwidth Limit

The local server will try to send data to the offsite server *as fast as possible* unless you place a bandwidth limit on the local server.

Full path to local directory

The local server sends the total contents of the directory specified here, to the offsite server.

Status

For better bandwidth management, the Schedule Transfer function lets you specify the times, on a daily basis, files get sent to the offsite server.

- **Active -** indicates files are actively being sent to the offsite server.
- **Suspended** - the local server is suspended per the schedule set out in Schedule Transfer.

At the **end of each active cycle**, the system checks the local server and reports back the amount of data **left to be written**.

NOTE: You can check the amount of data left to be written at any time by pushing the Check Status button.

Backup > Offsite Alert

Configure an alarm when the specified local server can not connect to the offsite server. Alarms are only generated during the times allowed by Schedule Transfer for each local server.

Backup > Schedule Transfer

Designate the time of day each local server pushes files to the offsite server. You may set different start and end times for each day of the week. For example, you may push files from 6pm to 6am on weekdays and all day long during the weekends.

Backup > Install/Remove

Backup must be installed separately on each machine. Backup can backup all volumes, including the boot volume, while in use. Backup accomplishes this through the use of a low level driver. As such, backup **require a reboot** to complete its installation. After installation completes, if a user is logged in, the systems asks them to **Reboot Now** or **Continue Working**. If the dialog is not answered within 5 minutes, Continue Working is assumed. If no one is logged in, the system reboots immediately. *Reboot is required for installation to complete.*

NOTE: Installing backup on a server when no one is logged in, will reboot the server when backup installation completes.

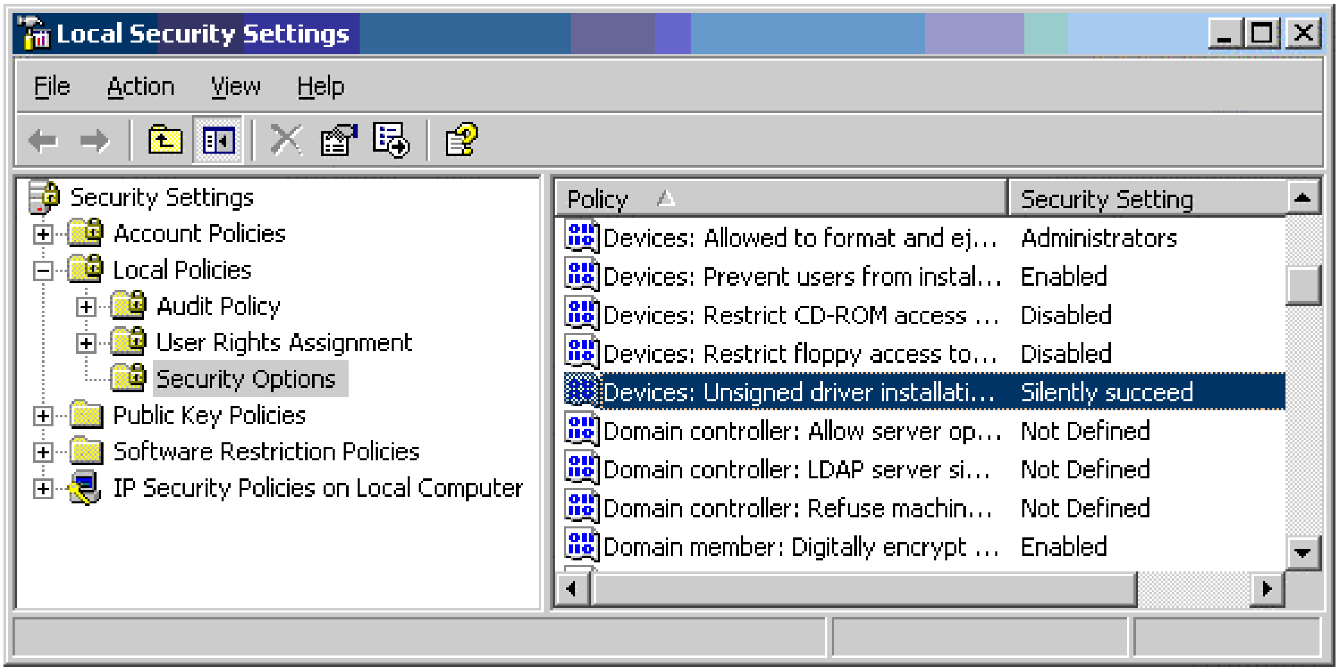
Backup requires additional agent capability so you may be prompted to update the agent prior to installing backup.

WARNING: Backup installation requires Windows Installer v3 and up. Your system checks the results from the last audit for v3. Your system will not recognize you have installed the latest Windows Installer until after the next audit runs on that machine.

Failed to install on Windows 2003 Server. Why?

By default, Windows 2003 Server **warns before installing any low level drivers**. To date, Microsoft will only sign their own low level drivers. Acronis can only deliver an unsigned driver as part of their backup system. To successfully install on a 2003 server, you must do one of the following:

- Click yes when asked if it is OK to install the unsigned driver. If this dialog box gets no response in two minutes, then Windows assumes no and blocks the installation.
- Prior to installation, set the Local Group Policy to **Silently Succeed** for **Devices: Unsigned driver installation** (see below).



Policy	Security Setting
Devices: Allowed to format and ej...	Administrators
Devices: Prevent users from instal...	Enabled
Devices: Restrict CD-ROM access ...	Disabled
Devices: Restrict floppy access to...	Disabled
Devices: Unsigned driver installati...	Silently succeed
Domain controller: Allow server op...	Not Defined
Domain controller: LDAP server si...	Not Defined
Domain controller: Refuse machin...	Not Defined
Domain member: Digitally encrypt ...	Enabled

Install/Reinstall

Select the desired machines, specify the install schedule and click Install. When scheduling the installation, you can also elect to *copy backup settings* from an existing machine. This copies the backup configuration and schedules from the existing machine to all the selected machines.

After the install completes, the system displays **Awaiting Reboot** if the user skipped the reboot at the end of the install (or the dialog timed out). To force a reboot in this case, click the reboot button displayed next to that machine's status.

Note: The backup install file is over 100MB. Avoid the file transfer from the Server to each machine in a LAN by setting the File Source function in the Patch Management module. Select and complete the "Pulled from file server using" option. Once set, the system writes a single copy to the LAN file share for use by all machines on the same LAN. The backup installation runs from that location for all agents on that LAN.

Remove

Remove backup from machines by selecting the machines and clicking the Remove button. A reboot on the machine is required to remove the low level driver and complete the removal of the backup feature.

Verify Install

Successful installation may be verified later if required. Verify install if you suspect someone removed the backup installation at the client machine.

Backup > Image Location

The backup system stores all volume backups and folder backups on the local network or local drive. Typically this is a path to a LAN based file server such as \\LAN_Server\Backups\. But it can also be as simple as another physical drive on the machine, such as a USB drive, or a shared network drive.

Separate paths may be specified for volume and folder backup paths.

NOTE: Mapped drive letters are not supported. The path must be a full UNC path or a local physical drive.

If a UNC path is specified, user credentials for the machine must be setup under the Agent tab. This login must be a user on the machine with access to the UNC path. Without the credentials, the machine will *not* have access to the image location and the backup will fail.

WARNING: You can not save the backup image to the same drive you are backing up.

NOTE: Windows 98 and Windows ME do not support user credentials. You may only use local drive paths for 98 and ME.

Check free space

You can check the amount of free space available on any machine's image location directory by checking the desired machine IDs and clicking the **Check** button. Also use this check to **verify the credential** is set correctly for the client to access the image location.

NOTE: Available free space changes all the time. To prevent showing stale data, reported free space only remains available for 10 minutes after the free space check completes.

The system saves each full backup set in its own folder. The backup data gets saved in the following **directory structure**:

```
Image Location Path
    testbox.workstations
        FldrBackup
        VolBackup
            20060621 18.13.01
              testbox.workstations2.tib
              testbox.workstations3.tib
              testbox.workstations4.tib
              testbox.workstations.tib
            20060628 18.12.55
              testbox.workstations2.tib
              testbox.workstations3.tib
              testbox.workstations4.tib
              testbox.workstations.tib
```

Backup > Image Password

Folder backup and volume backup .tib are all **password protected** using a unique password for each machine ID. This password remains constant for each client. If you decide to keep backups images outside of this system, print out the password for each machine ID or you will not be able to recover the backup later.

NOTE: For security reasons, only your system has this password. Kaseya can not recover a backup image for you if you loose this password.

You may set the password to anything you like. The same password my be set on multiple machines.

Backup > Folder Backup

You may backup any number of folders specified in the Folder Backup function. Folder Backup also lets you exclude specific file times. For example, you may wish to exclude *.avi, *.mp3, and *.bmp files when backing up someone's My Documents folder.

Folder backups perform sector level backups of selected folders. Sector level copying allows the system to backup locked and in-use files so you can safely backup at any time of the day.

Include Directories

Specify the full path to the folder you wish to backup on the selected machine. Paths must point to local drives, **not mapped drives or network paths**.

Exclude Files

Exclude a files or class of files from the included directories. Paths are not allowed. Only file names, with or without wild cards, are allowed. For example: *.jpg, outlook.pst

Remove...

Removes any included directory or excluded file from the selected machines.

Backup > Backup Alert

Backup alerts notify you when the system detects a problem with backup. As with all other alerts within the system, the content of the alert and the recipient can be set per alert. At the time the alert is generated, a script can also be run.

To set the alert for a particular machine or selected machines, check the alert, customize the alert message if necessary, identify a script to run if necessary and click apply.

Alerts can be cancelled and parameters reset at any time.

Backup Complete

Alerts when a backup process completes successfully.

NOTE: You may specify different alert email addresses for each backup alert type. This lets you send backup complete alerts to the user and only send failures to the administrator.

Backup fails

Alerts when a backup process stops prior to completion for any reason. Typically, backup fails because the machine is turned off mid-backup or because the network connection to the file server referenced by Image Location is lost.

Recurring backup skipped - machine offline

This alert gets issued when *Skip if machine offline* is set in Schedule Volumes and the backup is rescheduled because the machine is offline. Use this alert to notify you that backups are not even starting because the machine is turned off at the schedule volume backup time.

Backup > Pre / Post Script

Use Pre/Post Script to prepare a system for backup. For example, you may wish to force a system service, such as Exchange or a database, to write all its data to disk prior to system backup. Typically this can be done *without* requiring the service in question to be down during backup. So all critical services may be left fully operational at all time. You can specify a script to run prior to and/or after the schedule backup task.

For example, to backup an Exchange Server, a snap shot of the database is needed prior to the backup start. A script will quickly start and stop Exchange to take the snapshot of the database prior to the start of the backup.

Just select the machine, select the script to run before or after backup and click Set.

Backup > Compression

Specify the compression level used by backup. Higher compression takes longer to complete backup. Lower compression produces larger backup file sizes. The compression setting **effects both folder and volume** backup.

- None
- Normal - the default
- High
- Maximum

Backup > Max File Size

Max File Size applies to Volume backups only. When a Volume backup runs, image files of the volume get created. These file size specified in this option is the maximum size of each image file. For example, a volume containing 10 GB of data has been set to run. The image that gets created for a full backup may be 5 GB. If the max file size is set to 600 MB, the system will create 9 files, 8 that are 600 MB and 1 file with the balance of the data.

If you are going to write the image files to a CD or DVD, select the file size that is appropriate for the media.

Backup > Max Log Age

A log is created for each machine every time a backup operation runs. The log contains the Date, Type, Duration, Result and Description of the backup operation performed.

You can specify how long you would like to retain the data within the log. Entries older than the specified maximum are automatically deleted.

Backup > Secure Zone

Creates a secure zone on the selected machine. The secure zone is a 56 MByte hidden boot partition used by Auto Recovery to restore backup volume images without any user interaction.

Install

Load the secure zone on the selected machines. Installing the secure zone **reboots the selected machine**.

Remove

Uninstall the secure zone from the selected machines. Removing the secure zone **reboots the selected machine**.

Verify

Successful installation may be verified later if required. Verify install if you suspect someone removed the backup installation at the client machine.

Show Partitions

Verify scans the machine identifying disks and partitions. Checking Show Partitions lists these results from the verify.

Reports Tab

Reports allows administrators to generate detailed use information about client machines. An administrator may want to use the remote control feature to provide instructional training, or make changes to a user account machines which can not be accomplished by scripting. Use the Help Desk Feature tab to locate your customized help desk scripts.

To access the Assistant, click Assistant from any function page.

The following functions are available in the Reports feature tab:

Functions	Description
Set Logo	Allows custom logos to be placed on generated reports.
Schedule Reports	Automatically run reports at a scheduled time. Reports may be posted or delivered via email.
Executive Summary	Create a concise summary report reflecting the system health of a selected group of machines.
Aggregate Table	Create a single table with one row per machine and using any data as columns.
Machine Summary	Generate reports on deployed Agents and the machines they reside on.
Machine Changes	Run a difference report between each machine's latest audit and either the baseline or latest audit from a selected machine.
Patch Management	Displays composite and individual patch status reports
Inventory	Inventory summary for the selected audit category.
Software	Get detailed information regarding the software installed and used by client machines.
Disk Utilization	Generate graphical report on capacity and usage of all fixed disks.
Network Statistics	View detailed network usage information, from the entire network down to a client machine.
Uptime History	Chart the powered up, online, and abnormal shutdown history of each machine vs. time.
Logs	Generate reports on all logged information collected by the VSA.
Ticketing	Report status of all trouble tickets.
Backup	Report on the backup log and status

Reports > Set Logo

How do I add my company information to a report?

The top of every report is fully customizable. The system places any HTML you enter here at the top of every report. Make the header as simple or as complex as you want. You have full control over the HTML entered. Each header is **saved uniquely for each administrator**. When an administrator runs the report, that report has the header for that administrator.

The master administrator can **customize the default report header** seen by all administrators. Click the Customize function under the System tab and enter the custom header in the filed labeled **Header HTML shown on all reports**. If you do not want other administrators to change the custom header, **block them** from seeing the Set Logo using Function Access under the System tab.

Apply

Clicking this button updates the system with the new HTML used on all reports run by that administrator.

Default

Click to restore the header to the product default setting.

Related Info

Reports > Schedule Reports

Use **Schedule Reports** to automatically export reports to a URL on the VSA web site that **does not require a login** to access. Schedule Reports gives you a method to post reports accessible to non-administrators. Schedule recurring reports to post up to date data your users can access.

Set unique **"Specify Accounts"** settings for each scheduled instance of a report. This lets you define a single report and schedule it to run for each individual machine or group of machines. For instance, you could create a single Software report and then schedule it to output a unique report for each group ID.

You can optionally **email** a copy of the report or a short message with the URL to the report. Customize the message content by clicking the Format Email button.

Note: Only master administrators can change the format of the scheduled reports email.

Reports are posted to the *dataReports* directory, on the VSA's website, in a sub directory named after the administrator login that scheduled the report and a sub directory for the specify accounts filter. This convention groups all reports for a specific machine or group of machines into a common directory. For example:

http://www.your_vsa.com/dataReports/joe_admin/mach.group/report_name.htm

Since the system runs these reports without the administrator logging in, **only saved reports that specify all saved parameters may be scheduled**.

NOTE: Standard administrators can not schedule reports that use < All Groups >. Only master administrators can schedule < All Groups > reports.

Show reports from all administrators

Checking this box displays reports (shared and private) for all administrators on the VSA server. Check this box to view/delete/modify scheduled reports for any administrator.

Note: Only master administrators can show reports for all administrators.

Select report to schedule

This drop down control lists all saved reports visible to the currently logged in administrator. Select the report to be scheduled from this list. The output report web page has the same filename as the report. Selecting a new report from this control resets the specify account settings to those saved with the report. The VSA displays the report type below this control.

Schedule

Click Schedule to run the report at the specified time and save the file in the dataReports directory.

Recurring

Check Recurring to repeatedly run the report at the specified interval. The report runs the first time at the time specified with the Run At control.

Enter email address to notify when report is ready

List of email addresses to send the report to. Depending on how the notification is formatted, either the entire report is sent or a short message with a link to the report is sent. Leave this list bank to disable email notification. Comma separate each email address to send multiple notifications/reports.

Format Email

Click this button to change the subject and body of the email sent when a report runs. Enter any text you like for either the subject line or body of the email. Special tags are available to insert unique report data.

<at> Time stamp of when the report was created

<er> Embed full report - **NOTE: Report completely replaces entire message body**

<id> Specify accounts filter used to run the report

<rt> Report title

<ru> URL to the report stored on your VSA web site.

Filename

List of reports that have run and are scheduled to run. If the report has already run, the filename appears as a link to the report.

Last Run

Time when the report was last produced.

Next Run

Time the report is schedule to run next. If this field is blank, the report is not scheduled to run again.

Recurring

Recurring interval at which the report runs.

Report Type

Type of report that has been scheduled. For example, Disk Utilization.

Account Filter

Values of the specify account filter used to run each scheduled report.

Email Address

Comma separated list of addresses to email the report or notification to. Leave blank to disable email notification.

Reports > Executive Summary

This report summarizes the status and health of all selected machines in one quick view. The report computes an overall score projecting the over all health of the managed group of machines.

The Executive Summary report shows the following sections:

- **Client Information** - Displays number of machines (servers and workstations) and the names of the primary points of contact for this group.
- **System Activity** - Quick view enumerating number of times machines were audited and scanned for missing patches. This section also shows the total number of patches installed during the specified number of days. Click **Change Rows...** to fully customize this section.
- **Ticket Status**- Summary of tickets status over the specified number of days.
- **Disk Space Used** - Graph presents the percent of free disk space on all selected machines. Restrict this chart to servers only by checking the "Only list servers in Disk Space Used" box.
- **Network Health Score** - Displays individual component scores and overall health score for all the selected machines as a group. (*see Network Health Score section below for details*) Click **Change Score...** to fully customize this section.
- **Operating Systems** - Pie chart showing the break down of operating systems in the selected group.
- **Patch Status** - Pie chart summarizing the state of missing patches for all selected machines.
- **Alert Notifications** - Summarizes alerts issued in the specified number of days. This section breaks the alert count down by category of alert.
- **License Summary** - Summarizes the OS and MS Office licenses found by audit.

Network Health Score

The overall network health score gives you an at a glance view of the health and usability of the selected machines. The score is broken into 5 components and scored from 0 to 4 (4 is the highest) as follows:

- **Patch** - The average score for each machine gives the patch score. Each machine is scored based on the number of missing patches as follows:

Fully patched	
missing 1-2 patches	
missing 3-5 patches	
missing > 5 patches	
unscanned machines	

OS - Modern operating systems score higher than older operating systems. The overall OS score is an average of each machine's score calculated as follows:

2003 and XP	
2000	
NT4	
98 and ME	

95	

Disk - Full disk drives can have a severe negative impact on your system. As such disk space used contributes to the overall system score. Disk score is computed as follows:

0% to 65% full	
65% to 75% full	
75% to 85% full	
85% to 95% full	
100% full	

Ticket - Past due tickets assigned to machines are scored as follows:

0 past due	
1 or 2 past due	
3 to 5 past due	
more than 5 past due	

NOTE: The system does not delete tickets when deleting machine IDs. The ticket summary chart includes tickets matching the Machine ID and Group ID filters. Because no machine data exists for deleted Machine IDs, Views are not applied to this table.

- **Event Log Score** - Monitored event log alerts represent potential system problems. The number of event log alerts generated by each machine over the specified period of time is scored as follows:

0 alerts	
1 to 4 alerts	
5 to 10 alerts	
more than 10	

Backup Score - Counts days since the backup last ran. The older the backup is, the lower the score.

Alarm Score - The fewer alarms generated, the lower the score.

Script Score - Scripts provide a recurring beneficial service to a machine. The more often the script runs, the better shape that machine is likely to be in. The longer it has been since the script ran, the lower the score. The weighted thresholds for the script score count the number of days since the script last ran on the machines. The default values provide the following score:

	0 to 2 days since script ran	
	2 to 3 days since script ran	
	3 to 4 days since script ran	
	4 or more days since script ran	

You can adjust how heavily each category effects the final score by adjusting the **weight** value for each category. Weights range from 0 to 100. Set the weight to **0 to turn off that category**.

The final network health score computes the weighted average of the above scores and normalizes them providing the final percentage score, 100% representing perfect.

Contact Person

The contact person displayed in the **Client Information** section represents the point of contact inside the organization receiving IT service.

IT Manager

The person listed as the **IT Manager** represents the person responsible for delivering IT services to the client organization.

Summarize data collected in the last N days

Patch, ticket, alert, and status information is time dependent. Only data collected in the specified number of days contributes to this report.

Only list servers in Disk Space Used section

Check this box to only display used disk space for servers. This box is valuable to highlight file server space as a function of network health.

Report Permission

Select **Shared** or **Private** to assign a permission to the report. By default, the **Private** setting will be selected. **Private** reports can only be viewed and run by the administrator that created the report. **Shared** reports can be viewed and run by all administrators.

Save As...

The settings of the report can be saved for later use. Pressing Save As... brings up a dialog box where the report can be named. The report will be listed in the left-hand navigation bar along with the corresponding permission icon, depending on whether it is labeled as private or shared .

Choosing a Report

Selecting a saved report from the left-hand navigation bar displays the settings of the report, and also gives the administrator the ability to edit, rename, or delete the report. Some of the functions below appear only when a saved report is selected from the left-hand navigation bar.

Report Name

Lists the name of the report as entered by the administrator.

Save

After making changes to the report, press Save to save the current settings.

Save As...

To make a copy of the current report, press save as... and give the report a new name. Before saving as, give the new report a permission by selecting either the **Private** or **Shared** radio button.

Rename...

To rename the report, press Rename... A dialog box will appear and a new name can be entered.

Pressing **OK** confirms the new name and saves the report. The new name will shortly be listed in the left-hand navigation bar.

Delete...

To delete the report, press delete...

Update

Pressing Update synchronizes the information shown in the Group ID/Machine ID field with the information specified in the Specify Accounts filter.

Step 1

Select the columns of data to display

Select any number of columns to display. Each selection creates an additional column of data in the table. There is always one row for each machine that matches the Specify Accounts filter.

Step 2

Run the Report

Enter Title Displayed On Report Header

Enter a title to display in the resulting report page header. This title is saved with the report.

Step 3

Run the Report

Pressing run displays the result of the report in a new browser window.

Advanced Filter

Some reports support the Advanced Filter. The advanced filter lets you design complex searches to isolate data to just those values you want. Enter the filter string into the same line you normally enter the simple text filter into. Advanced filter supports the following operations:

White Space

To search for white space in a string, enclose the string in double quotes.

For example: **"Microsoft Office*" OR "*Adobe *"** Note that the * is included inside the double quotes.

Nested operators

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

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

NOT

Search for the a string not containing the match data.

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

AND

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

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

OR

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

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

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

Returns all data whose value is numerically less than, if a number. If this is alphabetic data then it returns all strings appearing earlier in the alphabet.

For example: **< G*** returns all applications starting with a letter less than "G" (any string starting with an "F" or lower).

Note: Dates may also be tested for but must be in the following format: YYYYMMDD HH:MM:SS where YYYY is a four digit year, MM is a two digit month (01 to 12), DD is a two digit day (01 - 31), HH is a two digit hour (00 - 23), MM is a two digit minute (00 - 59), and SS is a two digit second (00 - 59). HH:MM:SS is optional. Date and time are separated with a space. Remember that all white space must be enclosed in double quotes.

For example: < "20040607 07:00:00" will return all dates earlier than 7:00 on 7 June 2004.

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

Returns all data whose value is numerically greater than, if a number. If this is alphabetic data then it returns all strings appearing after it in the alphabet.

For example: **> G*** returns all applications starting with a greater than "G" (any string starting with an "G" or higher).

Reports > Aggregate Table

Create a table mixing any data collected by the VSA with an Aggregate Table report. Each report generates a single table with a row for each machine and a column for each piece of data specified.

Advanced Filter

Click Advanced Filter to restrict the amount of data displayed. You can specify a different advanced filter for each column of data displayed.

Report Permission

Select **Shared** or **Private** to assign a permission to the report. By default, the **Private** setting will be selected. **Private** reports can only be viewed and run by the administrator that created the report. **Shared** reports can be viewed and run by all administrators.

Save As...

The settings of the report can be saved for later use. Pressing Save As... brings up a dialog box where the report can be named. The report will be listed in the left-hand navigation bar along with the corresponding permission icon, depending on whether it is labeled as private or shared .

Choosing a Report

Selecting a saved report from the left-hand navigation bar displays the settings of the report, and also gives the administrator the ability to edit, rename, or delete the report. Some of the functions below appear only when a saved report is selected from the left-hand navigation bar.

Report Name

Lists the name of the report as entered by the administrator.

Save

After making changes to the report, press Save to save the current settings.

Save As...

To make a copy of the current report, press save as... and give the report a new name. Before saving as, give the new report a permission by selecting either the **Private** or **Shared** radio button.

Rename...

To rename the report, press Rename... A dialog box will appear and a new name can be entered. Pressing **OK** confirms the new name and saves the report. The new name will shortly be listed in the left-hand navigation bar.

Delete...

To delete the report, press delete...

Update

Pressing Update synchronizes the information shown in the Group ID/Machine ID field with the information specified in the Specify Accounts filter.

Step 1

Select the columns of data to display

Select any number of columns to display. Each selection creates an additional column of data in the table. There is always one row for each machine that matches the Specify Accounts filter. Data columns are the same columns you can specify in Agent Status.

Step 2

Run the Report

Enter Title Displayed On Report Header

Enter a title to display in the resulting report page header. This title is saved with the report.

Step 3

Run the Report

Pressing run displays the result of the report in a new browser window.

Related Info

Reports > Machine Summary

Machine Summary produces a detailed report for **each** machine ID matching the filter. Use the **Machine Summary** report to generate comprehensive reports for individual machines.

To generate an Agent report:

1. In the Specify Accounts filter, select the machines you want an Agent report on.
2. Select the information you want displayed in the Agent report. To have an item display in the report, select it from the **Not Displayed** list and press Add>>. It is moved to the **Displayed** list. You can change the order of items displayed in the report by selecting the item in the **Displayed** list and pressing the Up or Down arrows:
   - **Computer/Network** Displays the client machine Windows network name, operating system, CPU, RAM, IP address, gateway, DNS/DHCP server, and WINS server information.
   - **Printers** Lists the printers found by the audit for this machine.
   - **Logical Disk** Lists the logical volumes on the client machines, including removable, fixed, and CD-ROM drives.
   - **Physical Disk** Lists physical disk information for the client machine, such as hard disks, DVD, and CD-ROM drives.
   - **PCI Devices** Lists installed PCI devices on the client machine.
   - **System Info** All items collected by the System Info function under the Audit Tab.
   - **Registered Apps** All registered applications for the selected machine.
   - **Unregistered Apps** All unregistered applications (.exe files) for the selected machine.

Note: Registered applications place an App Paths key in the registry identifying the location of their main executable. Sorting on this value is a good way to separate main applications from all the helper and secondary applications.

   - **Baseline - Added Apps** All new applications detected by Latest Audit that have appeared on the machine since the Baseline Audit was run.
   - **Baseline - Removed Apps** All applications that were present when the Baseline Audit was ran but are missing when Latest Audit last ran.
   - **User Profile** Lists out user contact information associated with this machine ID
   - **Agent Control/Check-In** Displays information on baseline and latest audits, last check-in times, quick check-in periods, primary and secondary server and port information.
   - **Pending Scripts** Lists scheduled scripts on the client machine.
   - **Recurring Scripts** Lists scripts that are executed on a scheduled basis on the client machine.
   - **File Integrity** Lists files that are integrity-protected.
   - **File Access** Lists protected files.
   - **Network Access** Lists applications that have restricted network access.
   - **Miscellaneous** Lists miscellaneous Agent settings, such as WinVNC and user logs status.
3. Enter a title you want displayed in the report header.
4. Press run. The report is generated and shown in a new browser window.

Report Permission

Select **Shared** or **Private** to assign a permission to the report. By default, the **Private** setting will be selected. **Private** reports can only be viewed and run by the administrator that created the report. **Shared** reports can be viewed and run by all administrators.

Save As...

The settings of the report can be saved for later use. Pressing Save As... brings up a dialog box where the report can be named. The report will be listed in the left-hand navigation bar along with the corresponding permission icon, depending on whether it is labeled as private or shared .

Choosing a Report

Selecting a saved report from the left-hand navigation bar displays the settings of the report, and also gives the administrator the ability to edit, rename, or delete the report. Some of the functions below appear only when a saved report is selected from the left-hand navigation bar.

Report Name

Lists the name of the report as entered by the administrator.

Save

After making changes to the report, press Save to save the current settings.

Save As...

To make a copy of the current report, press save as... and give the report a new name. Before saving as, give the new report a permission by selecting either the **Private** or **Shared** radio button.

Rename...

To rename the report, press Rename... A dialog box will appear and a new name can be entered. Pressing **OK** confirms the new name and saves the report. The new name will shortly be listed in the left-hand navigation bar.

Delete...

To delete the report, press delete...

Update

Pressing Update synchronizes the information shown in the Group ID/Machine ID field with the information specified in the Specify Accounts filter.

Step 1

Select Display Settings

Move the items you want displayed in the report from the **Not Displayed** to the **Displayed** box by selecting the item and pressing **Add>>**. You can remove items by selecting the item in the **Displayed** box and pressing **<<Remove**. It is then displayed in the **Not Displayed** box.
You can change the order of the items displayed in the report by selecting the item you want to move in the **Displayed** box and clicking the up or down buttons.

Step 2

Enter Title Displayed On Report Header

Enter a title to display in the resulting report page header. This title is saved with the report.

Machine ID/Group ID/Update

These fields and the button are active only when a saved report is selected from the left-hand navigation bar. The Machine ID and Group ID fields populate with the settings of the saved report. The settings can be changed by entering new filter criteria in the Specify Accounts field, pressing Update, and re-saving the report.

Step 3

Run the Report

Pressing run displays the result of the report in a new browser window.

Related Info

Reports > Machine Changes

Run a difference report between each machine's latest audit and its own baseline **or** either the baseline or latest audit from a selected machine.

Compare with machine's own baseline audit

Displays all changes, both hardware and software, found on each machine by comparing the information from the latest audit against the information from the baseline audit.

Compare to select machine ID

Displays all changes, both hardware and software, found on each machine by comparing the information from the latest audit against the audit from a **specific machine ID**. Use this function to identify differences in a group of machines when compared against the standard for the group. Check **use baseline** to compare with the baseline audit information from the specific machine ID.

Reports > Patch Management

This report lists the patch state for all selected machines. There are both group composite reports and individual machines reports available.

Show machine patch summary pie chart
Display a pie chart showing the number of machines that are:

- Fully patched systems
- Missing 1 or 2 patches
- Missing 3, 4, or 5 patches
- Missing more than 5 patches
- Have never been scanned

Show missing patch occurrence bar chart
Display a bar chart illustrating which patches have the most machines that are missing that patch.

Show table of missing patches
This is a composite report that shows all patches that are missing from any and all machines in the selected group. This table lists a section for each missing patch showing: patch ID, knowledge base article number, and patch title. If **Show list all machines missing each patch** is also checked, then the report lists each machine ID missing the patch.

Show table of installed patches
This is a composite report that shows all patches that are installed on any and all machines in the selected group. This table is basically the opposite of the **missing patches** section. This table lists a section for each installed patch showing: patch ID, knowledge base article number, and patch title. If **Show list all machines containing each patch** is also checked, then the report lists each machine ID with the patch installed.

Show patch status for each machine
For each machine ID a list of both installed and missing patches are shown. Patches are grouped by application. If **Show summaries for each patch** is checked that the summary describing the patch is also displayed.

Show missing patches for each machine
For each machine ID a list only of missing patches are shown. Patches are grouped by application. If **Show summaries for each patch** is checked that the summary describing the patch is also displayed.

Show patches installed in the last xx days
For each machine ID, a list of patches are displayed that were installed during the last number of days specified in the text box.

Report Filtering

- **Bulletin ID Filter** – Enter a bulletin filter by using the asterisk (*) as a wild card for multiple characters and/or the underscore (_) as a wild card for a single character.
- **Ignore machines without data** – Check the checkbox to exclude all machines without patch scan data (default).
- **Show patches denied by Patch Approval Policy** – By default, only missing patches that have been approved for installation in the Patch Approval Policy are included in the report. Check the checkbox to ignore the Patch Approval Policy and include all patches whether approved or denied by the Patch Approval Policy.

Report Permission
Select **Shared** or **Private** to assign a permission to the report. By default, the **Private** setting will be selected. **Private** reports can only be viewed and run by the administrator that created the report. **Shared** reports can be viewed and run by all administrators.

Save As...
The settings of the report can be saved for later use. Pressing Save As... brings up a dialog box where the report can be named. The report will be listed in the left-hand navigation bar along with the corresponding permission icon, depending on whether it is labeled as private or shared .

Choosing a Report

Selecting a saved report from the left-hand navigation bar displays the settings of the report, and also gives the administrator the ability to edit, rename, or delete the report. Some of the functions below appear only when a saved report is selected from the left-hand navigation bar.

Report Name

Lists the name of the report as entered by the administrator.

Save

After making changes to the report, press Save to save the current settings.

Save As...

To make a copy of the current report, press save as... and give the report a new name. Before saving as, give the new report a permission by selecting either the **Private** or **Shared** radio button.

Rename...

To rename the report, press Rename... A dialog box will appear and a new name can be entered. Pressing **OK** confirms the new name and saves the report. The new name will shortly be listed in the left-hand navigation bar.

Delete...

To delete the report, press delete...

Update

Pressing Update synchronizes the information shown in the Group ID/Machine ID field with the information specified in the Specify Accounts filter.

Step 1

Select the columns of data to display

Select any number of columns to display. Each selection creates an additional column of data in the table. There is always one row for each machine that matches the Specify Accounts filter.

Step 2

Run the Report

Enter Title Displayed On Report Header

Enter a title to display in the resulting report page header. This title is saved with the report.

Step 3

Run the Report

Pressing run displays the result of the report in a new browser window.

Pressing **Export** will create the report and then allow you to save the report as either an HTML file, a MS Excel file, or as a MS Word file.

Reports > Inventory

What does the Inventory report show me?

Inventory lists all unique items collected during an audit and identifies the machines containing that item. Any item in **System Info** or **PCI & Disk HW** may be selected to run an inventory report on.

What does a filter do?

The filter restricts the items listed in the inventory to only those items matching the filter. For example, If you run an Inventory report on the **Motherboard Manufacturer** field and set the filter to "*Intel*" you will only see items manufactured by Intel (or Intel Corp or any other variation) in the report.

Report Permission

Select **Shared** or **Private** to assign a permission to the report. By default, the **Private** setting will be selected. **Private** reports can only be viewed and run by the administrator that created the report. **Shared** reports can be viewed and run by all administrators.

Save As...

The settings of the report can be saved for later use. Pressing Save As... brings up a dialog box where the report can be named. The report will be listed in the left-hand navigation bar along with the corresponding permission icon, depending on whether it is labeled as private or shared .

Choosing a Report

Selecting a saved report from the left-hand navigation bar displays the settings of the report, and also gives the administrator the ability to edit, rename, or delete the report. Some of the functions below appear only when a saved report is selected from the left-hand navigation bar.

Report Name

Lists the name of the report as entered by the administrator.

Save

After making changes to the report, press Save to save the current settings.

Save As...

To make a copy of the current report, press save as... and give the report a new name. Before saving as, give the new report a permission by selecting either the **Private** or **Shared** radio button.

Rename...

To rename the report, press Rename... A dialog box will appear and a new name can be entered. Pressing **OK** confirms the new name and saves the report. The new name will shortly be listed in the left-hand navigation bar.

Delete...

To delete the report, press delete...

Update

Pressing Update synchronizes the information shown in the Group ID/Machine ID field with the information specified in the Specify Accounts filter.

Step 1

Enter Title Displayed On Report Header

Enter a title to display in the resulting report page header. This title is saved with the report.

Machine ID/Group ID/Update

These fields and the button are active only when a saved report is selected from the left-hand navigation bar. The Machine ID and Group ID fields populate with the settings of the saved report. The settings can be changed by entering new filter criteria in the Specify Accounts field, pressing Update, and re-saving the report.

Chart Type

- **Bar** Displays a stacked bar chart with a bar for each fixed disk on each selected machine. Blue region displays the amount of used disk space. Gray displays the amount of free disk space. Total length of the bar represents total disk size.

- **Table** All the same data as the Bar display in numeric form.

Step 2

Run the Report

Pressing run displays the result of the report in a new browser window.

Related Info

Reports > Software

The **Software Report** displays summaries of applications present on all selected machines. Each reports uses data collected from audit to display the state of each group's software installed base. There are four primary report types: All Applications, Software Licenses, Summary Licenses, and Operating Systems.

All Applications

Generates a table showing each unique application found on all machines by audit. The total number of unique copies of the application are also listed. You can optionally show or hide each column of data. Hiding a column may reduce the number of rows reported if the uniqueness of the data drops. For instance, your report may show 50 copies of an application with v2.0.1 and 127 copies of the same application with v2.8. If you hide the version, by unchecking the box, then the report lists 177 copies of that application. The All Application report lists:

- **Applications** - The application name (theApp.exe)
- **Product Name** - Product name string as provided by the software vendor.
- **Description** - Software description string as provided by the software vendor.
- **Manufacturer** - The software vendor name
- **Version** - Software version number.

Checking **Show unregistered applications** lists all the unregistered applications in addition to registered applications. Registered applications place an App Paths key in the registry identifying the location of their main executable. Sorting on this value is a good way to separate main applications from all the helper and secondary applications.

If **List machine IDs that contain each application** is checked then the machine ID of each machine containing the application is listed.

Note: To locate specific applications use the Advanced Filter option by clicking the Advanced... link.

Software Licenses

Generates a table listing the number of software licenses found in a group of machines discovered by audit. This report lists the total number of licenses and the number of unique licenses found across all machines. In addition, Software Licenses lists:

- Publisher - The software vendor name
- Title - The software title for each license found.

If **List machine IDs that contain each application** is checked then the machine ID of each machine containing the application is listed.

Note: To locate specific applications use the Advanced Filter option by clicking the Advanced... link.

License Summary

Generates a table summarizing the licenses on all machines in a group or view. This report presents four tables of information summarizing the following:

- **Servers** - lists all server types found and the number of machines running that server OS.
- **Workstations** - lists all workstation types found and the number of machines running that workstation OS.
- **Microsoft Office Licenses** - lists the number of machines with each version of Microsoft Office loaded.
- **Other Applications** - summarizes the number of machines with each application license found that is not contained in the first 3 tables.

Operating Systems

Charts a composite view of all operating systems found on all machine IDs.

Note: Each machine reports its operating system type and version with each check-in. Audit does not have to complete to obtain operating system information. Therefore, the number of operating systems reported by this report may be higher than the number of licenses

reported for that operating system if all machines have not completed an audit.

Three Operating System report styles are available:

- Pie chart
- Bar chart
- Table

Advanced Filter

Click Advanced Filter to restrict the amount of data displayed. You can specify a different advanced filter for each column of data displayed.

Report Permission

Select **Shared** or **Private** to assign a permission to the report. By default, the **Private** setting will be selected. **Private** reports can only be viewed and run by the administrator that created the report. **Shared** reports can be viewed and run by all administrators.

Save As...

The settings of the report can be saved for later use. Pressing Save As... brings up a dialog box where the report can be named. The named report will be listed in the left-hand navigation bar along with a corresponding icon, depending on whether it is labeled as a private or shared report.

Choosing a Report

Selecting a saved report from the left-hand navigation bar displays the settings of the report, and also gives the administrator the ability to edit, rename, or delete the report. Some of the functions below appear only when a saved report is selected from the left-hand navigation bar.

Report Name

Lists the name of the report as entered by the administrator.

Save

After making changes to the report, press Save to save the current settings.

Save As...

To make a copy of the current report, press save as... and give the report a new name. Before saving as, give the new report a permission by selecting either the **Private** or **Shared** radio button.

Rename...

To rename the report, press Rename... A dialog box will appear and a new name can be entered. Pressing **OK** confirms the new name and saves the report. The new name is listed in the left-hand navigation bar.

Delete...

To delete the report, press delete...

Update

Pressing Update synchronizes the information shown in the Group ID/Machine ID field with the information specified in the Specify Accounts filter.

Step 1

Choose a Report Type

- **All Applications** Displays a list of applications installed on the client machine(s) selected in the Specify Accounts filter. The list of applications can be filtered by pressing **filter**, which brings up the application filter control.
- **Software Licenses** Lists all licenses found for all applications
- **License Summary** Summarizes all the licenses found.
- **Operating Systems** Displays a list of the operating systems installed on the client machine(s) selected in the Specify Accounts filter.

Step 2

Enter Title Displayed On Report Header

Enter a title to display in the resulting report page header. This title is saved with the report.

Choose the Sort Order

- **group.machine** The report results are displayed alphabetically by group ID.
- **machine.group** The report results are displayed alphabetically by machine ID.

Chart Type

- **Pie** Results are displayed in a standard pie chart. Clicking on a pie slice displays a table with a more detailed view of the information that comprises the slice.
- **Bar** Results are displayed in a standard bar chart. Clicking on a bar segment displays a table with a more detailed view of the information that comprises the bar.
- **Table** The table view provides an alphabetical (either by group or machine ID, as selected in the sort order) list of all the results of the selected report. The Table view provides the entire set of information gathered in the report; using the Pie and Bar chart types provides the administrator with a subset of the information when a pie slice or bar segment is selected. The Table view is useful for printing purposes.

Note: After running the Operating Systems report, you can select from Pie, Bar, or Table in the dropdown list provided in the report window.

Machine ID/Group ID/Update

These fields and the button are active only when a saved report is selected from the left-hand navigation bar. The Machine ID and Group ID fields populate with the settings of the saved report. The settings can be changed by entering new filter criteria in the Specify Accounts field, pressing Update, and resaving the report.

Filter

Pressing filter brings up the application filter control, which provides a way to control the list of applications shown in the applications list.

Step 3

Run the Report

Pressing run displays the result of the report in a new browser window.

Related Info

Reports > Disk Utilization

Disk Utilization presents a graphical representation of the

- size of each disk drive
- amount of used space on each disk drive
- amount of free space on each disk drive

Hovering the mouse over any segment on the chart presents a tool tip that reads out the exact number of MBytes in that segment.

To generate a disk utilization report:

1. Enter a title you want displayed in the report header.
2. Choose the order of the displayed results:
    - **machine.group** Listed alphabetically by machine name.
    - **group.machine** Listed alphabetically by group name.
3. Select the chart type. These options may be disabled depending on the type of report selected.
4. Verify that the Machine ID and Group ID parameter match the parameters specified in the Specify Accounts filter. This only applies if you running a previously saved report.
5. Press run. The report is generated and shown in a new browser window.

Report Permission

Select **Shared** or **Private** to assign a permission to the report. By default, the **Private** setting will be selected. **Private** reports can only be viewed and run by the administrator that created the report. **Shared** reports can be viewed and run by all administrators.

Save As...

The settings of the report can be saved for later use. Pressing Save As... brings up a dialog box where the report can be named. The report will be listed in the left-hand navigation bar along with the corresponding permission icon, depending on whether it is labeled as private or shared .

Choosing a Report

Selecting a saved report from the left-hand navigation bar displays the settings of the report, and also gives the administrator the ability to edit, rename, or delete the report. Some of the functions below appear only when a saved report is selected from the left-hand navigation bar.

Report Name

Lists the name of the report as entered by the administrator.

Save

After making changes to the report, press Save to save the current settings.

Save As...

To make a copy of the current report, press save as... and give the report a new name. Before saving as, give the new report a permission by selecting either the **Private** or **Shared** radio button.

Rename...

To rename the report, press Rename... A dialog box will appear and a new name can be entered. Pressing **OK** confirms the new name and saves the report. The new name will shortly be listed in the left-hand navigation bar.

Delete...

To delete the report, press delete...

Update

Pressing Update synchronizes the information shown in the Group ID/Machine ID field with the information specified in the Specify Accounts filter.

Step 1

Enter Title Displayed On Report Header

Enter a title to display in the resulting report page header. This title is saved with the report.

Machine ID/Group ID/Update

These fields and the button are active only when a saved report is selected from the left-hand navigation bar. The Machine ID and Group ID fields populate with the settings of the saved report. The settings can be changed by entering new filter criteria in the Specify Accounts field, pressing Update, and re-saving the report.

Chart Type

- **Bar** Displays a stacked bar chart with a bar for each fixed disk on each selected machine. Blue region displays the amount of used disk space. Gray displays the amount of free disk space. Total length of the bar represents total disk size.
- **Table** All the same data as the Bar display in numeric form.

Step 2

Run the Report

Pressing run displays the result of the report in a new browser window.

Related Info

Reports > Network Statistics

To generate a network statistics report:

1. Select the type of report you want to generate:

- **Applications** Displays a graph outlining each application and corresponding network bandwidth consumption over the time period entered in the **Specify Period of Time** setting. The number of applications displayed can be selected in the dropdown list, up to a maximum of 20.
- **Machines** Displays a graph outlining the machine(s) selected in the Specify Accounts filter and corresponding network bandwidth consumption over the time period entered in the **Specify Period of Time** setting. The number of machines displayed can be selected in the dropdown list, up to a maximum of 20.

2. Enter a title you want displayed in the report header.

3. Specify the number of days you want the report to cover.

4. Verify that the Machine ID and Group ID parameter match the parameters specified in the Specify Accounts filter. This only applies if you running a previously saved report.

5. Press run. The report is generated and shown in a new browser window.

NOTE: This report requires the Network Access driver be enabled. This driver hooks the TCP/IP stack to measure network traffic by application. The driver is disabled by default.

Report Permission

Select **Shared** or **Private** to assign a permission to the report. By default, the **Private** setting will be selected. **Private** reports can only be viewed and run by the administrator that created the report. **Shared** reports can be viewed and run by all administrators.

Save As...

The settings of the report can be saved for later use. Pressing Save As... brings up a dialog box where the report can be named. The report will be listed in the left-hand navigation bar along with the corresponding permission icon, depending on whether it is labeled as private or shared .

Choosing a Report

Selecting a saved report from the left-hand navigation bar displays the settings of the report, and also gives the administrator the ability to edit, rename, or delete the report. Some of the functions below appear only when a saved report is selected from the left-hand navigation bar.

Report Name

Lists the name of the report as entered by the administrator.

Save

After making changes to the report, press Save to save the current settings.

Save As...

To make a copy of the current report, press save as... and give the report a new name. Before saving as, give the new report a permission by selecting either the **Private** or **Shared** radio button.

Rename...

To rename the report, press Rename... A dialog box will appear and a new name can be entered. Pressing **OK** confirms the new name and saves the report. The new name will shortly be listed in the left-hand navigation bar.

Delete...

To delete the report, press delete...

Update

Pressing Update synchronizes the information shown in the Group ID/Machine ID field with the information specified in the Specify Accounts filter.

Step 1

Choose a Report Type

- **Applications** Displays a graph outlining each application and corresponding network bandwidth consumption over the time period entered in the **Specify Period of Time** setting. The number of applications displayed can be selected in the dropdown list, up to a maximum of 20.
- **Machines** Displays a graph outlining the machine(s) selected in the Specify Accounts filter and their corresponding network bandwidth consumption over the time period entered in the **Specify Period of Time** setting. The number of machines displayed can be selected in the dropdown list, up to a maximum of 20.

Step 2

Enter Title Displayed On Report Header

Enter a title to display in the resulting report page header. This title is saved with the report.

Specify Period of Time

Sets how far back, in days or hours, the report retrieves information.

Machine ID / Group ID / Update

These fields and the button are active only when a saved report is selected from the left-hand navigation bar. The Machine ID and Group ID fields populate with the settings of the saved report. The settings can be changed by entering new filter criteria in the Specify Accounts field, pressing Update, and re-saving the report.

Step 3

Run the Report

Pressing run displays the result of the report in a new browser window.

Related Info

Reports > Uptime History

What does this report show me?

Uptime History presents a graphical representation of

- when each managed machine was turned on
- when each managed machine was connected to the network
- any abnormal shut downs

Hovering the mouse over any segment on the chart presents a tool tip that reads out the exact start and end time of that segment.

How do I generate an Uptime History report?

To generate a Uptime History report:

1. Enter a title you want displayed in the report header.
2. Choose the number of days worth of data to display
3. Verify that the Machine ID and Group ID parameter match the parameters specified in the Specify Accounts filter. This only applies if you running a previously saved report.
4. Press run. The report is generated and shown in a new browser window.

To generate a Uptime History report:

1. Enter a title you want displayed in the report header.
2. Choose the number of days worth of data to display
3. Verify that the Machine ID and Group ID parameter match the parameters specified in the Specify Accounts filter. This only applies if you running a previously saved report.
4. Press run. The report is generated and shown in a new browser window.

Report Permission

Select **Shared** or **Private** to assign a permission to the report. By default, the **Private** setting will be selected. **Private** reports can only be viewed and run by the administrator that created the report. **Shared** reports can be viewed and run by all administrators.

Save As...

The settings of the report can be saved for later use. Pressing Save As... brings up a dialog box where the report can be named. The report will be listed in the left-hand navigation bar along with the corresponding permission icon, depending on whether it is labeled as private or shared .

Choosing a Report

Selecting a saved report from the left-hand navigation bar displays the settings of the report, and also gives the administrator the ability to edit, rename, or delete the report. Some of the functions below appear only when a saved report is selected from the left-hand navigation bar.

Report Name

Lists the name of the report as entered by the administrator.

Save

After making changes to the report, press Save to save the current settings.

Save As...

To make a copy of the current report, press save as... and give the report a new name. Before saving as, give the new report a permission by selecting either the **Private** or **Shared** radio button.

Rename...

To rename the report, press Rename... A dialog box will appear and a new name can be entered. Pressing **OK** confirms the new name and saves the report. The new name will shortly be listed in the left-hand navigation bar.

Delete...

To delete the report, press delete...

Update

Pressing Update synchronizes the information shown in the Group ID/Machine ID field with the information specified in the Specify Accounts filter.

Step 1

Enter Title Displayed On Report Header

Enter a title to display in the resulting report page header. This title is saved with the report.

Select number of days worth of data to display

The last N days (from the time the report was generated) are displayed.

Specify Accounts

Verify that the correct set of machines you want in the report are addressed in the Specify Accounts filter.

Step 2

Run the Report

Pressing run displays the result of the report in a new browser window.

Reports > Logs

How do I generate a Logs report?

Select Log to Display

Select the type of log you want in the report. Then specify the number of days worth of log data to display. For instance, selecting 30 days will report the last 30 days of log data every time you run the report.

Enter Title Displayed On Report Header

Enter a title to display in the resulting report page header. This title is saved with the report.

Machine ID/Group ID/Update

These fields and the button are active only when a saved report is selected from the left-hand navigation bar. The Machine ID and Group ID fields populate with the settings of the saved report. The settings can be changed by entering new filter criteria in the Specify Accounts field, pressing Update, and re-saving the report.

Run the Report

Pressing run displays the result of the report in a new browser window.

Report Permission

Select **Shared** or **Private** to assign a permission to the report. By default, the **Private** setting will be selected. **Private** reports can only be viewed and run by the administrator that created the report. **Shared** reports can be viewed and run by all administrators.

Save As...

The settings of the report can be saved for later use. Pressing Save As... brings up a dialog box where the report can be named. The report will be listed in the left-hand navigation bar along with the corresponding permission icon, depending on whether it is labeled as private or shared .

Choosing a Report

Selecting a saved report from the left-hand navigation bar displays the settings of the report, and also gives the administrator the ability to edit, rename, or delete the report. Some of the functions below appear only when a saved report is selected from the left-hand navigation bar.

Report Name

Lists the name of the report as entered by the administrator.

Save

After making changes to the report, press Save to save the current settings.

Save As...

To make a copy of the current report, press save as... and give the report a new name. Before saving as, give the new report a permission by selecting either the **Private** or **Shared** radio button.

Rename...

To rename the report, press Rename... A dialog box will appear and a new name can be entered. Pressing **OK** confirms the new name and saves the report. The new name will shortly be listed in the left-hand navigation bar.

Delete...

To delete the report, press delete...

Update

Pressing Update synchronizes the information shown in the Group ID/Machine ID field with the information specified in the Specify Accounts filter.

Step 1

Select Log to Display

Select the type of log you want in the report. Then specify the number of days worth of log data to display. For instance, selecting 30 days will report the last 30 days of log data every time you run the report.

Step 2

Enter Title Displayed On Report Header

Enter a title to display in the resulting report page header. This title is saved with the report.

Machine ID / Group ID / Update

These fields and the button are active only when a saved report is selected from the left-hand navigation bar. The Machine ID and Group ID fields populate with the settings of the saved report. The settings can be changed by entering new filter criteria in the Specify Accounts field, pressing Update, and re-saving the report.

Ignore machines without data

Check this box and you will only display machine IDs that have data matching the specified filter parameters. Use this to create reports that only list machines with that log entry of interest.

Step 3

Run the Report

Pressing run displays the result of the report in a new browser window.

Related Info

Reports > Ticketing

A ticket report creates a table listing all trouble tickets assigned to the selected machine IDs. In Step 1 specify the subset of tickets you wish to display. Check the **Display notes with each ticket** checkbox to include all the detail notes with each ticket.

Create a table listing all trouble tickets assigned to the selected machine IDs. In Step 1 specify the subset of tickets you wish to display. Check the Display notes with each ticket checkbox to include all the detail notes with each ticket.

NOTE: The system does not delete tickets when deleting machine IDs. The ticket summary chart includes tickets matching the Machine ID and Group ID filters. Because no machine data exists for deleted Machine IDs, Views are not applied to this report.

Step 1

Select column to sort on

The report engine uses this column to sort the ticket data displayed. Combine with **ascending / descending** radio buttons to specify the direction of the sort.

Display notes with each ticket

Check this box to include all the detail notes with each ticket.

Category, Status, Priority

Filter displayed notes based on these selections. For instance, to only report on **Open** tickets, select Open from the Status drop down control.

Select Fields...

Specify which ticket fields to display in the report.

Step 2

Run the Report

Enter Title Displayed On Report Header

Enter a title to display in the resulting report page header. This title is saved with the report.

Step 3

Run the Report

Pressing run displays the result of the report in a new browser window.

Save the report as HTML, Word, or Excel

Pressing Export generates the report and then allows you to select on export format.

Report Permission

Select **Shared** or **Private** to assign a permission to the report. By default, the **Private** setting will be selected. **Private** reports can only be viewed and run by the administrator that created the report. **Shared** reports can be viewed and run by all administrators.

Save As...

The settings of the report can be saved for later use. Pressing Save As... brings up a dialog box where the report can be named. The report will be listed in the left-hand navigation bar along with the corresponding permission icon, depending on whether it is labeled as private or shared .

Choosing a Report

Selecting a saved report from the left-hand navigation bar displays the settings of the report, and also gives the administrator the ability to edit, rename, or delete the report. Some of the functions below appear only when a saved report is selected from the left-hand navigation bar.

Report Name

Lists the name of the report as entered by the administrator.

Save

After making changes to the report, press Save to save the current settings.

Save As...

To make a copy of the current report, press save as... and give the report a new name. Before saving as, give the new report a permission by selecting either the **Private** or **Shared** radio button.

Rename...

To rename the report, press Rename... A dialog box will appear and a new name can be entered. Pressing **OK** confirms the new name and saves the report. The new name will shortly be listed in the left-hand navigation bar.

Delete...

To delete the report, press delete...

Update

Pressing Update synchronizes the information shown in the Group ID/Machine ID field with the information specified in the Specify Accounts filter.

Step 1

Select column to sort on

The report engine uses this column to sort the ticket data displayed. Combine with **ascending / descending** radio buttons to specify the direction of the sort.

Display notes with each ticket

Check this box to include all the detail notes with each ticket.

Category, Status, Priority

Filter displayed notes based on these selections. For instance, to only report on **Open** tickets, select Open from the Status drop down control.

Select Fields...

Specify which ticket fields to display in the report.

Step 2

Run the Report

Enter Title Displayed On Report Header

Enter a title to display in the resulting report page header. This title is saved with the report.

Step 3

Run the Report

Pressing run displays the result of the report in a new browser window.

Save the report as HTML, Word, or Excel

Pressing Export generates the report and then allows you to select on export format.

Reports > Backup

Generate a report summarizing data retrieved from the backup logs.

Show backup logs from the last N days

Specify how many days of backup log entries to include in the report.

Show backup log summary data

Include a summary table totaling backup event found in the last N days.

- Machines with Backup - counts number of backup licenses used.
- Successful backups last N days - Total number of successful backups for all machines in the last N days.
- Failed backups last N days - Total number of failed backups for all machines in the last N days.
- Total backup attempts last N days - Total number of backup processes run for all machines in the last N days.

Show backup log status by machine and event

List the backup log information collected in the last N days for each machine.

- Type - Full backup or Incremental Backup.
- Backup Completed - Date/Time when the backup completed.
- Duration - Amount of time the backup took to complete.
- Result - Success or Failed.

Assistant

assist export

When should I export a report?

When you run a report and want to archive it, send it to someone else, or further manipulate the data outside of the VSA.

When I click the MS Excel or MS Word Format links the HTML document opens. Why?

Since the VSA is a web based tool, clicking the link sends the data to your browser. If you do not have Excel or Word loaded on your local machine, the page displays as plain HTML.

Feature Tab > Agent

Functions in the Agent tab allow administrators to create, edit, and delete machine IDs, customize the appearance of the machine's Agent icon in the system tray, control Agent check-in frequency, and to update Agent versions that reside on Agent machines. Customized Agent-related scripts can also be stored and accessed from the left-hand navigation bar in the Agent feature tab.

To access the Assistant, click Assistant from any function page.

The following functions are available in the Agent feature tab:

Functions	Description
Agent Status	Displays active user accounts, IP addresses and last check-in times.
Agentt Logs	There are a variety of logs compiled by the System Agent:
Script Log	Displays a log of successful/failed scripts executed.
Agent Log	Displays a log of Agent system and error messages.
Configuration Changes	Displays a log of configuration changes made by an administrator.
Network Statistics Log	Displays a log of send/receive data for applications that access the network.
NT Log	Displays Application, System, and Security NT Event Log data collected from managed machine.
Log Settings	Allows administrators to activate/deactivate Agent Logs on Agent machines.
Create/Delete Collection	Create, delete, or rename machine collections
Collection Membership	Defines which machines are members of which collections
Deploy Agents	Create Agent install packages
Create	Allows administrators to create new machine accounts.
Delete	Allows administrators to delete machine accounts.
Rename	Rename existing machine account.
Change Group	Reassign any number of machines to a new group ID at once
Copy Settin	Mass copy settings from one machine to many.

gs	
Edit Profile	Allows administrators to edit machine account information.
User Access	Set up accounts to allow users remote control access to their own machines
Check-In Ctl	Allows administrators to control Agent check-in frequency on Agent machines.
Set Credential	Set a login credential for the Agent to use in Patch Management and the Use Credential script command.
Agent Menu	Allows administrators to customize the appearance of the Agent system tray icon settings.
Update Agent	Allows administrators to remotely update Agents on Agent machines.

Agent > Agent Status

Agent Status gives a quick view of a wide variety of data pertaining to each Agent. You may choose all the data columns yourself to fully customize the view. You have the same options available in this display as provided by the Aggregate Table report.

Select Columns...

Specify which columns of data to display and the order to display them in.

> **Note: Click Advanced Filter to search for specific strings in any field. For example, to search for the machine ID that "jsmith" is logged into, click Advanced Filter and enter jsmith in the edit box next to Current User.**

Column Definitions

Machine ID - Machine ID label used throughout the system

Group ID - just the group ID porting of the machine ID

First Checkin Time - time when a machine first checked into the system

Last Checkin Time - most recent time when a machine checked into the server

Last Reboot Time - time of the last known reboot of the machine

Current User - login name of the user currently logged into the machine (if any)

Last Logged In User - login name of the last person to log into the machine.

User Access Logon - login name given to a user for log into the Kaseya server

Computer Name - computer name assigned to the machine

Operating System - Operation system type the machine is running

OS Version - Operation system version string

IP Address - IP address assigned to the machine

Subnet Mask - networking subnet assigned to the machine

Default Gateway - default gateway assigned to the machine

Connection Gateway - IP address seen by the Kaseya server when this machine checks in. If the machine is behind a DHCP server, this will be the public IP address of the subnet.

MAC Address - MAC address of the LAN card used to communicate with the Kaseya server

DNS Server 1,2 - IP address of the DNS servers assigned to the machine

Primary/Secondary WINS - WINS settings

CPU Type - processor make and model

CPU Speed - clock speed of the processor

RAM Size - MBytes of RAM on the machine

Agent Version - Version number of the Kaseya Agent loaded on the machine

User Access Remote Cntl - Enabled if this user can log in and get remote control access to their machine. Disabled if access is denied.

User Access Ticketing - Enabled if this user can log in and enter trouble tickets. Disabled if access is denied.

User Access Chat - Enabled if this user can start chat sessions with an administrator. Disabled if access is denied.

Primary/Secondary KServer Address - IP address / name the machine uses to communicate with the Kaseya server.

Quick Checkin Period - Quick check in time setting (in seconds)

Contact Name - User name entered in Edit Profile

Contact Email - Email address entered in Edit Profile

Contact Phone - Phone number entered in Edit Profile

Contact Notes - Notes entered in Edit Profile

Manufacturer - system manufacturer

Product Name - system product name

System Version - product version number

System Serial Number - system serial number

Chassis Serial Number - serial number on the enclosure

Chassis Asset Tag - asset tag number on the enclosure

External Bus Speed - motherboard bus speed

Max Memory Size - max memory size the motherboard can hold

Max Memory Slots - total number of memory module slots available

Chassis Manufacturer - manufacturer of the enclosure

Chassis Type - enclosure type

Chassis Version - enclosure version number

Motherboard Manufacturer - motherboard manufacturer

Motherboard Product - motherboard product ID

Motherboard Version - motherboard version number

Motherboard Serial Num - motherboard serial number

Processor Family - processor type installed

Processor Manufacturer - processor manufacturer

Processor Version - processor version ID

CPU Max Speed - max processor speed supported

CPU Current Speed - speed processor is currently running at

Check-in status

The check-in status of the machines shown in the Agent machine list is indicated by the icon shown to the left of the Agent machine ID. The icons and their status are as follows:

OK **Agent has checked in**

⚑ **Agent has not recently checked in**

⚑ **Agent has never checked in**

Related Info

Agent > Agent Logs

Logs collect event information on or relating to machines. The different types of logs that can be generated are:

Select Log

Select the audit log which you would like to view for a specific user. Then select the hyperlink text for a specific user account you would like to view.

Script Log

Selecting a user account hyperlink displays a log of successful/failed scripts.

Agent Log

Selecting a user account hyperlink displays a log of Agent system and error messages.

Configuration Changes

Selecting a user account hyperlink displays a log of configuration changes made by each Administrator.

Network Statistics Log

Selecting a user account hyperlink displays a log of send/receive data for network applications.

Alert Log

List out all the email alerts issued against the selected machine.

Application Event Log, Security Event Log, System Event Log

Shows the Event Log data collected by Windows. (Not available for Win9x)

Events Per Page

Select the amount of events to display on each page. Navigate from page to page by selecting the hypertext number at the bottom of the events page.

Related Info

Agent > Log Settings

The server logs numerous items in several logs on both the Agent side and server side of the system. You have full control over how much of that data to save in the database on a per log basis. The more data you save, the larger your database grows.

The following selections are accessible from the Logging Control function:

Machine.Group ID
Lists the Agent machines according to the Specify Accounts criteria.

Alert Log
Captures all the email alerts issued against the selected machine.

Network Statistics Logging
Network Statistics Logging collects incoming and outgoing packet count information and the application or process transmitting and/or receiving such packets. This information can be viewed in detail in the Network Statistics User Log.

Configuration Changes Logging
The system logs all changes made by administrators to each machine ID

Agent Message Logging
Logs Agent activity and/or errors for each machine ID

Script Log
Logs each script run on every machine ID.

Application Events, Security Events, System Events
Captures all Windows event log data. The system saves the most recent 500 events from each type (application, security, and system). No age setting applies to event logs.

Select All/Unselect All
Select All will select all user accounts on all account pages. Unselect All will unselect selected user accounts on all account pages. For individual accounts, select the checkbox next to the machine.group ID.

Update
Pressing update will update all selected user accounts. Unselected accounts will not be updated.

Check-in status
The check-in status of the machines shown in the Agent machine list is indicated by the icon shown to the left of the Agent machine ID. The icons and their status are as follows:

OK **Agent has checked in**

🏳 **Agent has not recently checked in**

🚩 **Agent has never checked in**

Related Info

Agent > Create / Delete Collection

Machine collections let you group any number of arbitrary machines together. Any machine can be made a member of any collection. Machines can also be members of more than one collection at the same time. Collections work together with group ID and machine ID filters to sort and list various machines. For example, you create a collection named *servers* and assign all your servers to be members of this collection. Then if you want to see all the servers in the *accounting* machine group, define a view that shows the *servers* collection and the *accounting* machine group.

Create

To define a new collection, enter a name for the collection and click the **Create** button.

Delete

To define a new collection, check the box to the left of the collection name and click the **Delete** button.

Edit Icon

You can rename any collection by clicking the edit icon to the left of each collection name.

Collection Name

This column lists all the collections that have been defined for the entire system.

Member Count

Shows the number of machines that are members of the corresponding collection.

Show Machines

Click this button, to the right of each collection name, to see a detailed list of all members of a collection.

Agent > Collection Membership

Use this function to assign any machine ID to become a member of one or more collection. Collections are arbitrary groups of machines. Any machine can be made a member of any collection. Machines can also be members of more than one collection at the same time. Collections work together with group ID and machine ID filters to sort and list various machines. For example, you create a collection named *servers* and assign all your servers to be members of this collection. Then if you want to see all the servers in the *accounting* machine group, define a view that shows the *servers* collection and the *accounting* machine group.

Add

Add machines to one or more collections by first checking the box to the left of the machine ID. Then select the collection names from the collection list. Finally click the **Add** button.

Remove

Remove machines from collections by first checking the box to the left of the machine ID. Then select the collection names to remove from the collection list. Finally click the **Remove** button.

Machine.Group ID

This column lists all the collections that have been defined for the entire system.

Member of Collection

This column shows a comma separated list of collections that the corresponding machine ID is a member of.

Agent > Deploy Agents

Any administrator can create an install package. Agent installation packages are preset with all configuration settings so users are not required to do anything to install an Agent.

Create an install package unique to each group Id you manage.

Create Package

Clicking Create Package opens a wizard where you can specify all configuration parameters for the Agent.

Set Default

Each administrator can specify their own default Agent by selecting the radio button to the left of the package name. (**Set Default** column.)

Click ✗ to remove a package from the list

Remove a package from your list. If you created the package, then this also deletes the package from the system and removes it for all administrator's lists.

Click 📝 to edit package parameters

Edits the parameters associated with this package using the package creation wizard. The wizard is a 6 step process used to uniquely configure each Agent install package to suit the needs of any deployment.

1. Define rules for naming the machine ID
2. Define rules for naming the group ID
3. Specify installer command line options including the ability to install silently, without any task bars or dialog boxes.
4. Specify a machine account to use as a template configuration for the new install. All settings and pending scripts applied to the template account are copied to the new account created with this install package.
5. Optionally bind in an administrator logon credential to the install package. When the Agent package installs it first tries to install using the rights of the currently logged in user. If that user does not have sufficient rights, the administrator credential is used. The Agents install easily without any user interaction at all, even for users with restricted rights.
6. Name the install package for easy reference later.

Share a package with other administrators

After creating an install package, you can share that package with other administrators by clicking the Share function. Master Administrators can make a package public and available to all administrators.

Download the package

Click the package name link to download the install package directly from this page.

Agent > Create

The following selections are accessible from the Create function:

Copy settings from selected

Clicking a radio button next to any listed existing user account will copy all Agent setting from that account to use in the new account you are creating.

Machine ID

The unique name assigned to the Agent machine or user.

Group ID

Designates which group the Agent machine user (designated by the Machine ID) will belong to. Clicking the dropdown menu shows a list of groups currently administered by the System Server. These groups can only be created by the master administrator, and are created/edited in the Admin Account function of the System feature tab.

Create Account

Press this button after inputting all of the user information in the fields listed above.

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

Clicking the Set link assigns the account selected with the radio button in the **Select Copy** column, to be the default account to copy settings from for the current Group ID. When ever a new account is created for the for this Group ID the default account will be automatically selected. Click Clear to remove this assignment.

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

This link is only visible when logged on as a Master Administrator. Clicking the Set link assigns the account selected with the radio button in the **Select Copy** column, to be the default account to copy settings from when ever a Group ID with no default assigned is active. Click Clear to remove this assignment.

Admin Email

Enter the e-mail address of the individual responsible for administering support to the Agent machine. This may be the administrator, but is often someone who is part of the IT staff of the Agent company.

Auto

Check Auto Assign to automatically enter a user email address when creating a new machine account. The email address is set to **machineid@groupid.com**

Contact Name

Enter the name of the individual using the Agent machine.

Contact Email

Enter the e-mail address of the individual using the Agent machine.

Contact Phone

Enter the phone number of the individual using the Agent machine.

Download/Email Agent Installation

Selecting the unique Agent machine link displays the Web page Agent machine users will see before installing the Agent. Instructions on installing the Agent are displayed on the setup download screen. To send the link to the Agent machine user via e-mail, click the Email Link To link.

First Checkin

Lists the time that each Agent checked into the server for the first time.

Check-in status

The check-in status of the machines shown in the Agent machine list is indicated by the icon shown to the left of the Agent machine ID. The icons and their status are as follows:

- 🟩 **Agent has checked in**
- 🟨 **Agent has not recently checked in**
- 🟥 **Agent has never checked in**

Agent > Delete

The following selections are accessible from the Delete function:

Delete Accounts

Pressing delete accounts removes the selected Agent machine accounts from the Server. A dialog box confirms deletion, or cancels the action. Select the accounts to be deleted by checking the checkbox next to the Agent machine ID, then pressing delete accounts. To automatically remove the agent from a machine first, select **Uninstall agent first at next check-in**.

Uninstall agent first at next check-in.

Select this option first to remove the agent from the machine in addition to deleting the account from the VSA server. The next time the agent on all selected machines check-in, the VSA tasks the agent to uninstall itself. Once successfully uninstalled, the VSA deletes the account from the server. *The account is not deleted until the next time the agent successfully checks in.*

Delete account now without uninstalling the agent.

Removes the machine account from the VSA server. Already installed agents with this account name are *not* removed from the Agent machine.

Uninstall the agent and keep the account.

Uninstall the agent on the managed machine without deleting the account on the VSA. Select this option if you want to remove the agent from a remote machine but keep all the data collected about that machine in the VSA.

Machine.Group ID

Lists the Agent machines according to the Specify Accounts criteria.

Last Check-In

Displays the time the Agent machine's Agent last checked in to the Server.

Check-in status

The check-in status of the machines shown in the Agent machine list is indicated by the icon shown to the left of the Agent machine ID. The icons and their status are as follows:

OK **Agent has checked in**

⚑ **Agent has not recently checked in**

⚑ **Agent has never checked in**

Agent > Rename

Use this function to rename any existing machine account. You can change either the machine ID or group ID to any account name you wish.

Rename

Pressing Rename changes the account name of the selected Agent machine. If **Rename Agent at next check-in then rename account on the VSA server** is selected then the Agent is renamed first. Once the Agent is successfully renamed, the account name on the VSA is changed.

Rename Agent at next check-in then rename account on the VSA server

Select this option to dynamically change an account name for an actively checking in Agent. This option guarantees that the Agent and server remain in sync.

Rename account on VSA immediately

Select this option for accounts you wish to rename prior to deploying the Agent. Renaming an account immediately on the VSA for an account with an actively checking in Agent prevents that Agent from successfully checking in again until the new account name is entered at the Agent. (Right click the Agent menu and enter the new account name.)

Merge offline account <Offline Machine ID> into <Select Machine ID>

Use merge to combine log data in two different accounts that pertain to the same machine. This could be necessary if an Agent was uninstalled and then reinstalled with a different account name. Also, loading a new Agent onto a machine that has had an Agent before may create a duplicate account for the same machine.

New Name

Enter a name you wish to change the machine ID to be.

Group ID

Select the group ID you wish to assign to this account. The default leaves the group ID unchanged.

Machine.Group ID

Lists the Agent machines according to the Specify Accounts criteria. Click the radio button to the left of the machine account you wish to rename.

New Name at Next Check-in

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

Agent > Change Group

Use this command to move several machines into a new machine group. Like the Rename function , Change Group renames all selected machines to the new group. Machines that are currently offline rename themselves the next time they check in. If you rename a machine immediately, instead of waiting for the next checkin, the account gets renamed on the server but *not* on the Agent. If that Agent checks into the server again, it will try to recreate an account using the original name.

Move

Automatically move all selected machine IDs into the new group ID.

Cancel

Cancels any pending moving for all selected machine IDs. You will only be able to cancel moves for machines schedule to **Move Agent at next check-in** that have not already executed the move.

Move Agent at next check-in then rename account on the VSA server.

Select this radio button to schedule selected machines to be renamed the next time they check in. **This is the preferred rename method.**

Move account on VSA immediately. Deployed Agent may re-create old account.

Select this radio button to rename all account data on the server immediately.

Warning: If you rename a machine immediately, instead of waiting for the next checkin, the account gets renamed on the server but *not* on the Agent. If that Agent checks into the server again, it will try to recreate an account using the original name.

Select new group ID

Specify the **new group ID** to rename each selected machine ID into.

Client > LAN Watch

Show me an explanation of the items on this page.

LAN Watch periodically scans the local area network **of the designated Client** for any and all new devices connected to that the LAN since the last time LAN Watch ran. Optionally, the VSA sends an **alert** when LAN Watch discovers any new device. LAN Watch effectively uses the Client as a proxy to scan a LAN behind a firewall that would not normally be accessible from a remote server.

NOTE: You must have an Client already installed on at least one machine on the LAN you wish to scan.

Since LAN Watch monitors the entire LAN there is no need to schedule LAN Watch to run on more than one machine per LAN. Attempts to run LAN Watch on multiple machines on the same LAN are allowed but display a warning that you are introducing unnecessary network traffic by doing so.

What does LAN Watch do?

LAN Watch periodically checks the local area network looking for any and all new devices connected to the LAN since the last time LAN Watch ran. Optionally, the VSA sends an **alert** when LAN Watch discovers any new device.

Why is it unnecessary to run LAN Watch on more than one machine on the same LAN?

Since LAN Watch monitors the entire LAN there is no need to schedule LAN Watch to run on more than one machine per LAN. Attempts to run LAN Watch on multiple machines on the same LAN are allowed but display a warning that you are introducing unnecessary network traffic by doing so.

NOTE: LAN Watch will not scan more than 65,536 IP addresses. If the specified IP address range is larger than 65,536 then LAN Watch will truncate it to 65,536 addresses.

How long does a LAN Watch scan take?

The scanner pings every IP address in the specified range. If a device exists at that address, the response comes back right away. The scanner times out after 200ms if no device exists at that address. If you scan the **maximum range of 65,536** addresses, the scan may take up to **3.6 hours** to complete if very few of the addresses reply to the ping.

NOTE: The system automatically adjusts the recurring interval to be longer than the maximum scan time as defined by number of IP addresses at 200ms per address.

What triggers a LAN Watch alert?

An email alert is sent to all email addresses listed in Email Recipients when a new device is discovered by LAN Watch.

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

Explanation of items on this page

Scan Button

Click Scan to schedule a recurring LAN Watch scan on each machine selected (with the check box) from the list of displayed machine IDs. The scan runs every interval that you set (default is 1 day).

NOTE: LAN Watch will not scan more than 65,536 IP addresses. If the subnet mask of the machine running LAN Watch specifies a larger IP range, LAN Watch will truncate it to 65.536 addresses.

Cancel Button

Click Cancel to stop the scheduled scan from running any more. Cancel also deletes all records of the devices identified on a LAN from the VSA. If you re-schedule LAN Watch, after clicking Cancel, each device on the LAN will generate a new alert.

Scan 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**.

Alert when new device appears on LAN

Checking this box sends an alert to all email addresses listed in Email Recipients when a new device is discovered by LAN Watch.

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

Email Recipients

Email address where the event notification is sent. You can specify a different email address for each client machine, even if it is for the same event. The "From:" email address is specified in the Server Info function of the System feature tab.

Machine.Group ID

Lists the client machines according to the Specify Accounts criteria.

IP Range

The IP addresses that will be scanned by the selected Client when LAN Watch runs.

Last Scan

Timestamp showing when the last LAN Watch scan ran on a machine. When this date changes, new LAN Watch data has been processed and is available for viewing

Recurring Interval

The time interval used to determine how often LAN Watch runs.

Alert Active

A check mark appears if LAN Watch alerts are enabled for this scan. If checked, then an email alert is sent every time LAN Watch discovers a new device on the LAN. Email notification addresses may be viewed and/or edited in the Alerts function.

Client > View LAN

Show me an explanation of the items on this page.

View LAN is a sub-function of **LAN Watch**. Go to View LAN to see the results of the latest LAN Watch scan. A list of machines with scan results are displayed when you first enter this function. Clicking on any machine ID displays the table of data collected from the scan on that machine.

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

What does View LAN do?

View LAN is a sub-function of **LAN Watch**. Go to View LAN to see the results of the latest LAN Watch scan. A list of machines with scan results are displayed when you first enter this function. Clicking on any machine ID displays the table of data collected from the scan on that machine.

How do I view the results from a LAN Watch scan?

Click on any machine ID to see the results for the latest scan.

Why don't I see all the machine IDs listed?

Only machine IDs with returned scan data are available.

Why don't all the devices have host names?

Host Name is only available from computers. Hubs, switches, routers, or other network appliances will not return a Host Name.

Explanation of items on this page

Host Name

Host Name of each devices discovered by the scan. Host Name is only available from computers. Hubs, switches, routers, or other network appliances will not return a Host Name.

IP Address

Private IP address of each devices discovered by the scan.

MAC Address

MAC address of each devices discovered by the scan.

Last Seen

Time each device was last detected by the scan.

Client > Install Clients

Show me an explanation of the items on this page.

Install Clients lets you **remotely install the Client** on any PC detected by LAN Watch. Remote install is only available for Window NT, 2000, and XP based computers. A list of machines with scan results are displayed when you first enter this function. Clicking on any machine ID displays a table listing all machines **with a host name**.

NOTE: Clients may only be installed on PC computers. Remote install is only supported by Windows NT, 2000, and XP.

How do I install Clients on a machine without going to each machine?

Install Clients lets you **remotely install the Client** on any PC detected by LAN Watch. Remote install is only available for Window NT, 2000, and XP based computers. A list of machines with scan results are displayed when you first enter this function. Clicking on any machine ID displays a table listing all machines **with a host name**.

How does this work?

The machine that ran the scan is tasked to run psexec.exe and remotely install the Client on all selected machines. A valid login with administrator rights is required to successfully install an Client remotely.

Typical reasons for failure

- **Blocked by network security policy** - PSEXEC 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 PSEXEC to operate across the network.

NOTE: Classic is the default setting for machines that are members of a domain. Guest is the default setting for machines that are *not* in a domain. Microsoft does not allow Windows XP Home Edition to become a domain member.

- **Blocked by Anti-Virus program** - PSEXEC is a powerful program capable of remotely running processes on a machine (assuming the it has a valid administrator login). Some anti-virus programs classify PSEXEC as a security threat and may block its execution.
- **Username/password does not have administrator** - The credential must have administrator rights on the local machine. The Client installs as a system service requiring full administrator privileges to install successfully. The username may be a domain administrator of the form *domain\user.*

Agents will not install. What can I do?

LAN Watch will try to connect to \\<computer>\admin$ using the credentials that you supplied.

First we need to test that the computer is available. Start a Command Prompt and type the following:

```
ping <IP address>
```

If you dont get a reply see troubleshooting below. If you do get a reply, we know that the machine is turned on and a firewall is not blocking connections. Next, verify that the share is available. Start a command prompt and type the following:

```
start \\<computername>\admin$
```

If you have a problem see troubleshooting below. If all is ok a window appears containing the remote computers c:\windows directory. Now, we now know that the machine is turned on and the share exists. Next verify the psexec command works correctly. Remote control the machine *you ran LAN Watch on.* Start a command prompt and type

```
c:\temp\psexec.exe \\<computername> -u <username> -p <password> ipconfig
```

You should see the results of ipconfig for the target computer displayed on the machine you are running remote control on. If not, the RPC service on the target machine is probably disabled and blocking remote procedure calls.

Troubleshooting

PSEXEC's ability to run processes remotely requires:

- Both local and remote computers have file and print sharing enabled
- The default Admin$ share (a hidden share that maps to the \Windows directory) is defined on the remote system

Pings fails - either the machine is not on, or there is a firewall on the machine stopping pings. Either of these will stop the process and need to be corrected before continuing.

Start fails - If windows does not accept the username/password combination, you will see a box pop up asking you to try again. Correct the mistake and try again.

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.

PSEXEC failed 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 workgroup** - RPC **disabled** by default ("Use simple file sharing" is checked).
- **XP Home** - RPC **disabled** always ("Use simple file sharing" is not available).

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 PSEXEC to retrieve a list for you.

Type PSEXEC \\<computername> "net share". check that admin$ is shared exists and points to c:\windows (or c:\winnt on older OS's)

What is *domain\user* format?

Typically, you need administrator rights to install software on the remote machine. Multiple accounts may have administrator rights on the same machine. Your domain administrator account may be different than the local administrator account. To insure you are using the domain account enter the login name in the domain\user format. If the domain is left off, the local account will be used.

How do I hide devices that already have Clients installed.

Check the "Hide devices that match the MAC address of existing accounts" box to remove all machines that may already have an Client installed. Any device on the LAN with a MAC address matching the MAC address of an existing Client account is hidden.

What happens if I try to install an Client on a machine that already has an Client?

Nothing happens. The Client installer detects an Client is already there and exits immediately.

Where can I get PSEXEC.EXE?

http://download.sysinternals.com/Files/PsExec.zip

Where do the error messages come from?

If the installation failed for any reason, the VSA passes back the results reported by PSEXEC. Typically, PSEXEC is simply reporting OS errors that it received trying to execute a call.

What command line is PSEXEC.EXE being run with?

The Client tasks PSEXEC with the following command line:

c:\temp\psexec \\hostname -u "adminname" -p "password" -c -f -d "c:\temp\kcssetup.exe" > c:\temp\LANInsA*ipAddr*.txt

where *hostname* and *ipAddr* refer to the remote machine. If the Client is on a drive other than C: then the temp files are referenced to the same drive the Client is installed on.

Explanation of items on this page

Install Button

Click Install to schedule a remote Client installation to all selected machines. Remote install runs from the same machine that ran the scan and attempts to remotely connect to the selected machine across the LAN to perform the Client install using the supplied administrator credential for that machine.

Admin Logon Name

Administrator name to use on the selected machine. This account 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 insure you are using the domain account enter the login name in the domain\user format. If the domain is left off, the local account will be used.

Password

Password associated with the Admin Logon Name.

Hide devices that match the MAC address of existing accounts

Check this box to remove all machines that may already have an Client installed. Any device on the LAN with a MAC address matching the MAC address of an existing Client account is hidden.

Host Name

Host Name of each devices discovered by the scan. Host Name is only available from computers. Hubs, switches, routers, or other network appliances will not return a Host Name.

IP Address

Private IP address of each devices discovered by the scan.

MAC Address

MAC address of each devices discovered by the scan.

Last Seen

Time each device was last detected by the scan.

Agent > Copy Settings

Copy Agent settings from a single machine ID to any number of selected machine IDs. Use this function to quickly re-configure a group of machines to match the settings from a machine you know to be set up correctly. The following settings are copied:

- Check-in Control
- User Access rights (Remote Control, Ticketing, Chat)
- Agent Menu setup
- Agent Log Settings
- Script schedules (including Audit and patch scan)
- Alerts
- Patch Management configuration *(except for Initial Update and Windows Auto Update)*
- Remote Control configuration

Select Machine Id

Click this link to specify which Machine ID to copy settings from.

Copy button

Click to transfer the settings from the selected machine ID to all checked machine IDs.

Status

Shows **Update Pending** for any machine ID whose settings have changed by not taken effect yet. Settings take effect at the next Agent quick check-in.

Agent > Edit Profile

Select the Agent to edit by selecting the checkbox next to the corresponding machine ID. Multiple machine IDs can be edited simultaneously by selecting multiple checkboxes. To apply global changes, click Select All. Accounts can also be filtered by using the Specify Accounts area.

The following selections are accessible from the Edit Profile function:

Notes

Enter any notes about the Agent machines. Helpful information may include location, Agent machine type, company, or any other identifying information about the Agent machine. The notes for a particular machine are displayed in the Agent machine ID list.

Admin Email

Enter the e-mail address of the individual responsible for administering support to the Agent machine. This can be the administrator, but is often someone who is part of the IT staff of the Agent company. This setting is displayed in the **Admin Email** column.

Contact Name

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

Contact Email

Enter the e-mail address of the individual using the Agent machine. This setting is displayed in the **Contact Email** column.

Contact Phone

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

Machine.Group ID

Lists the Agent machines according to the Specify Accounts criteria.

Update

Pressing update applies all the changes to the selected user account(s).

Check-in status

The check-in status of the machines shown in the Agent machine list is indicated by the icon shown to the left of the Agent machine ID. The icons and their status are as follows:

OK **Agent has checked in**

🟨 **Agent has not recently checked in**

🟥 **Agent has never checked in**

Agent > User Access

User access lets administrators create a username and password their users can login with and remote control and FTP their machine. Users get the same remote control access administrators do. Users login at **http://your_VSA_address/access/**. Master Administrators can customize the web page seen by users to add their company's logo, look, and feel to the web experience for their users.

The user login page has a line to email the user a new password if they **forgot the user password**. A new random password is sent to the user email address of record the managed machine. You can set the user email address with the Edit Profile function under the Agent tab.

Set Password

Click Set Password to create a login for the selected machine ID. Select the machine ID by clicking the radio button to the left of the machine name in the Machine.Group ID column.

To enable user logon, the administrator must set a password for the user. The user may change that password after successful login.

Clear

Permanently removes the login credential from the selected machine ID. To temporarily disable user access, uncheck the box in the **Enable Login** column next to the machine ID (see below).

Login Name

Users may log into the VSA to enter trouble tickets and/or get remote access to their machine. The Contact Name, entered here, acts as the login credential for that users.

All login names must be unique in the system. ***Since users may also login using their machine ID, User Names, machine IDs, and Administrator names must all be unique.***

Create Password, Confirm Password

Define a password for the user login. Passwords must be at least 6 characters long.

Machine.Group ID

Lists the Agent machines according to the Specify Accounts criteria. Click the radio button to the left of the machine account you wish to rename.

Login Name

Users that have been granted remote access to their machine may login using *either* their machine ID or Login Name.

User Web Logon

Displays **Enabled** if remote user logon is allowed. User remote logon lets users log into the user page from a web browser on any machine. They can always get to that same page by double clicking the Agent icon or selecting Contact Administrator... from the Agent menu.

Enable Remote Cntl

Check this box to allow users remote control access to their machine when they log on to the VSA through any web browser. This is the same remote control capability administrators have, except it restricts them to their machine only.

Enable Ticketing

Check this box to allow users to create and modify trouble tickets for their own machines. Users can only see trouble tickets assigned to their machine.

Enable Chat

Check this box to allow users to initiate a chat session with a logged in administrator. They will only be able to chat with administrators that have access rights to the group ID that user's machine belongs to.

Agent > Check-In Ctl

The following selections are accessible from the Check-In Control function:

Select All/Unselect All

Clicking **Select All** will select all user accounts on all account pages. Clicking **Unselect All** will unselect selected user accounts on all account pages. For individual accounts, select the checkbox next to the user account's machine/group ID.

Update

Pressing update will update all selected user accounts. Unselected accounts will not be updated.

Machine.Group ID

Lists the Agent machines according to the Specify Accounts criteria.

Check-In Period

Enter the interval time value for an Agent to perform a check-in with the System Server. A check-in consists of a check for a recent update to the user's account, which is determined by an administrator. If a recent update has been set by a Kaseya Server administrator, the Agent starts working on the task at the next check-in. This setting is displayed in the **Check-In Period** column.

Primary KServer

Enter the IP address or fully qualified hostname of the Agent machine's primary server. This setting is displayed in the **Primary KServer** column.

Primary Port

Enter the port number of either the primary Virtual System Server. This setting is displayed in the **Primary KServer** column.

Note: Do NOT use computer name for your server. The Agent utilizes standard WinSock calls to resolve a fully qualified hostname 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, using NETBIOS over TCP/IP or the LMHOSTS file or other method. NETBIOS is an optional last choice that the Windows will attempt to use to resolve a name. Therefore, only fully qualified names or IP addresses are supported.

Secondary KServer

Enter the IP address or fully qualified hostname of the Agent machine's primary System Server. This setting is displayed in the **Secondary KServer** column.

Secondary Port

Enter the port number of either the secondary Kaseya Server. This setting is displayed in the **Secondary KServer** column.

Bandwidth Throttle

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

Warn if multiple Agents use same account

The VSA can detect more than one Agent connecting to the VSA using the same machine ID/group 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 VSA as an administrator.

Warn if Agent on same LAN as server connects through gateway

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

NOTE: Agents on the same LAN as the VSA server should be configured to connect directly to the VSA using the Check-In Control function.

Check-in status

The check-in status of the machines shown in the Agent machine list is indicated by the icon shown to the left of the Agent machine ID. The icons and their status are as follows:

- OK **Agent has checked in**
- 🟨 **Agent has not recently checked in**
- 🟥 **Agent has never checked in**

Related Info

Agent > Temp Directory

Depending on the task at hand, the Agent uses several additional files. The server transfers these files to the Agent at the directory referenced here. You can set the directory the Agent uses for working files on a per machine ID basis. Change the temporary directory from the system default, C:\temp, to any other location.

Change the directory in order to isolate files used by the system from other operations used by other applications on the machine. You can also approve this directory in security programs, such as virus checkers, to allow operations such as remote control from being blocked.

Agent > Set Credential

Set a login credential for the Agent to use in Patch Management and the Use Credential script command. **The credential should almost always have administrator rights on the machine**. The Use Credential script command behaves the same as Impersonate User except the credential can be uniquely assigned to each machine as opposed to using a fixed credential in a script. If a credential is present, then **patch management installs all new patches using this credential**. Therefore, Set Credential should **always be an administrator credential**.

Username

Enter the username for the credential. (Typically and administrator account).

Password

Password associated with the username above.

Domain

Domain name to log into. Leave this field blank to log into a local machine account.

Apply

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

Clear

Remove the credential from all checked machine IDs.

Agent > Agent Menu

The following selections are accessible from the Agent Menu function:

Making items available in the Agent icon menu

Select the checkboxes next to the items that are to be shown in the machine user's Agent system tray icon when it is right-clicked. Remove the icon all together by unchecking **Enable Agent Icon**.

Menu ACObSRx

This column summarizes the checkboxes selected, thus denoting which menu options will appear in the machine's Agent icon when it is right-clicked by the user. **ACObSRx** applies to the Windows-style keyboard shortcuts that are used to access each item in the Agent icon's menu, which is accessed by right-clicking the icon in the system tray. The letter corresponding to the menu item indicates that the function will appear in the user's Agent when the icon is right-clicked. A "-" indicates that menu item is disabled. Select a Agent machine, choose which options to display in the Agent icon, then press update. Unchecking the **Enable Agent Menu** checkbox prevents right-click access to the Agent icon's features, even if the various functions are selected.

A = **A**bout **Agent**
C = **C**ontact Administrator, Enter Trouble Tickets, ...
O = Launches the URL specified in the URL field. The Agent displays the text listed in the field to the left of the URL field.
b = Disa**b**le Remote Control
S = **S**et Account
R = **R**efresh
x = E**x**it

Machine.Group ID

Lists the Agent machines according to the Specify Accounts criteria.

Contact URL

Displays the URL associated with the Contact Administrator... item in the Agent menu. The default shows **User Login page**. Double clicking the Agent icon selects the default item from the Agent menu, Contact Administrator.... By default, this logs into the user access page with the access rights for that machine ID. You can now change that URL to anything you like. Optionally, you can also pass in the machine ID and/or group ID used by that Agent in your custom URL.

URL Title

Displays the text that is shown in the Agent's icon when it is right-clicked. This text, when selected, automatically launches the URL as specified in the URL section below.

Custom URL

Specifies the URL that is accessible from the Agent system tray icon. For example, entering http://www.yourdomain.com in the URL field will direct Agents to the specified URL when the Agent icon in the system tray icon is double-clicked, or when Your Company Name is selected in the system tray icon. The default URL is www.kaseya.com.

Entering a title and enabling the checkbox will change the menu title in the Agent's menu. The menu can be displayed by right-clicking the Agent icon in the Windows system tray (status area).

The remaining checkbox items can be activated or deactivated, depending on whether the administrator wants to allow Agent access to these features.

Select All/Unselect All

Select All will select all user accounts on all account pages. Unselect All will unselect selected user accounts on all account pages. To select individual accounts, select the checkbox next to the user account's machine.group ID.

Update

Pressing update will update all selected user accounts with the chosen settings.

Enable Agent Menu

Unchecking this checkbox disables the menu that is accessible by right-clicking the Agent icon. All of the feature checkboxes are automatically dimmed when this checkbox is unchecked.

Check-in status

The check-in status of the machines shown in the Agent machine list is indicated by the icon shown to the left of the Agent machine ID. The icons and their status are as follows:

- OK **Agent has checked in**
- ⚑ **Agent has not recently checked in**
- ⚑ **Agent has never checked in**

Related Info

Agent > Update Agent

The Update Agent page allows administrators to quickly deploy the latest Agent version to selected Agent machines. With the press of a button, the system can be tasked to automatically send Agent machines the latest Agent version during the Agent machine's regularly scheduled check-in period.

The following elements are displayed in the Update Agent function:

Machine.Group ID

Lists the Agent machines according to the Specify Accounts criteria.

Update Agent

Pressing Update Agent sends the latest Agent version to selected Agent machines.

Remind me at logon when Agents need an update

Selecting this checkbox will remind the administrator at login that Agents under their control need to be updated. Administrators can disable this feature at login time and can re-activate it by selecting this checkbox.

Force update even if Agent is at version x.x.x.x

Checking this box when updating an Agent forces new files to replace the current Agent files on the Agent machine. This performs a "clean" installation of the Agent files.

Cancel Update

Pressing **Cancel Update** after selecting a Agent machine cancels a pending update to the Agent.

Last Update

The date in which the Agent was last updated on the Agent machine.

Agent Version

Version of the Agent running on the Agent machine. Version numbers listed in red indicate that the version on the Agent machine is not the same as the latest version available.

Select All/Unselect All

Select All will select all user accounts on all account pages. Unselect All will unselect selected user accounts on all account pages. For individual accounts, select the checkbox next to the machine.group ID.

Check-in status

The check-in status of the machines shown in the Agent machine list is indicated by the icon shown to the left of the Agent machine ID. The icons and their status are as follows:

OK **Agent has checked in**

🟨 **Agent has not recently checked in**

🟥 **Agent has never checked in**

Related Info

Assistant

Assist Deploy Agents

Show me an explanation of the items on this page.

Any administrator can create an install package. Agent installation packages are preset with all configuration settings so users are not required to do anything to install an Agent.

Clicking Create Package opens a wizard where you can specify all configuration parameters for the Agent.

After creating an install package, you can share that package with other administrators by clicking the Share function. Master Administrators can make a package public and available to all administrators.

What is an Installation Package?

Install new Agents with either **Automatic** or **Individual** install packages.

Load an Automatic Agent install package on any machine. The first time that Agent checks in, it registers itself with the VSA and creates a new account. Configure automatic installs to run via login scripts, email, or manually.

Individual install packages contain all settings for an existing machine account. Click the Create button under the Agent tab to get Individual install packages.

What is the default Agent?

Clicking the link "Click to download and install the default Agent" downloads an Agent with all the default settings specified by the currently logged on administrator. Each administrator can specify their own default Agent by selecting the radio button to the left of the package name. (**Set Default** column.)

Can users download the default Agent directly without an administrator account on the VSA?

Yes. Anyone can download the Agent from **http://your.vsa.addr/dl.asp**. This page displays complete instructions for downloading and installing the **default Agent**. The page is accessible with any web browser and does not require a login.

Assist Agent Menu

Show me an explanation of the items on this page.

How do I hide the Agent icon on a Agent machine?

Normally, Agent machine users can access different functions on their Agent by right-clicking the system tray Agent icon.

To hide the Agent icon all together:

1. Select the Agent machine checkbox in the Agent machine list. Multiple machines can be selected, or you can click **Select All** to apply the change to all Agent machines in group.

2. Uncheck the **Enable Agent Icon** checkbox.

3. Press Update.

All of the checkbox settings will become dimmed, indicating that all of the Agent menu features have been disabled.

How do I prevent a Agent machine user from terminating the Agent service?

If the Exit feature is enabled on a Agent machine user's Agent icon, the user can terminate the Agent service on the Agent machine by selecting **Exit** from the Agent icon menu. With the Kaseya Agent service inoperative, the Agent machine is invisible to the user and can no longer receive any commands from the System Server.

To remove the Exit function from a Agent machine's Agent icon:

1. Select the Agent machine checkbox in the Agent machine list. Multiple machines can be selected, or you can click **Select All** to apply the change to all Agent machines in group.

2. Uncheck the **Exit** checkbox.

3. Press Update.

The Menu column indicator will reflect the change. **ACObSR-** will be shown in the affected Agent machine's **Menu** column. To get more information on the **Menu ACObSRx** column, click here.\

What does ACObSRx mean?

The items listed in the interface (with the following letters underlined) correspond to the items listed by right-clicking on the Agent icon in the system tray:

A = **A**bout **Agent**
C = **C**ontact Administrator...
O = Launches the URL specified in the URL field. The Agent displays the text listed in the field to the left of the URL field.
b = Disa**b**le Remote Control
S = **S**et Account
R = **R**efresh
x = E**x**it

The **Menu ACObSRx** column summarizes the checkboxes selected, thus denoting which menu options will appear in the Agent machine's Agent icon when it is right-clicked by the user. **ACObSRx** applies to the Windows-style keyboard shortcuts that are used to access each item in the Agent icon's menu, which is accessed by right-clicking the icon in the system tray. The letter, corresponding to the menu item, indicates that the function will appear in the user's Agent when the icon is right-clicked. Select a Agent machine, choose which options to display in the Agent icon, then press update. Unchecking the **Enable Agent Menu** checkbox prevents right-click access to the Agent icon's features, even if the various functions are selected.

Assist Automatic Install

Assistant
HELP HOME

Automatic Installation Packages

Automatic installation packages are the easiest way to deploy Agents. The resulting Agents automatically create new accounts on the system saving you the trouble of individually creating a new account in advance for each new machine.

Pre-configure automatic installation packages with any Agent setting by copying Agent settings from any existing account. The **Automatic Install Wizard** produces a custom install package, KcsSetup.exe, with all the custom features you ask for.

How do I deploy Agents to all machines on my network?

You can use the same install package to load Agents and create new accounts for all the machines on your network.

Install Agents using one of the following methods:

1. 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 this machine.
2. Email KcsSetup.exe to all users on the network. The automatic install package can carry an Administrator credential for your network so users do not need to be logged on as an Administrator to successfully install the Agent.
3. Manually install KcsSetup.exe on each machine.

How do I deploy Agents with NT logon scripts?

Running an automatic installation package from an NT logon script allows you to simply deploy Agents to all machines on your network with a single command line. If an Agent has already been installed on the machine, KcsSetup.exe exits immediately. When you create KcsSetup, the **Automatic Install Wizard** includes all required parameters based on answers to questions the wizard presents.

Just include the following line in the NT logon script:

```
KcsSetup.exe
```

Can the Agent be installed by a non-administrator?

Ordinary users, without rights to install software, can install the Agent if you enter an **Administrator Credential** at the time you download the Agent install package. When ordinary users run the install package (either directly or via an NT logon script), the installer uses the credential to complete the installation. The administrator credential is **encrypted** and bound to the install package, KcsSetup.exe, at download time when you fill in the administrator credential form.

The administrator credential is encrypted at all times and never available in clear text form.

How do I specify parameters for the *Default Agent Install* package?

Clicking the "Click to download and install the default Agent" link on either the **start page** or **Machine Accounts** downloads the Default Agent Install package. You can specify all this package's parameters using the same Automatic Install Wizard used to create any other Agent Install package. At the last screen in the wizard, the download screen, a link titled "Set this package as the default Agent Install package" appears at the top of the screen. Clicking this link rebuilds the Default Agent Install package with on the parameters you just set.

The "Set this package as the default Agent install package" is only displayed to Master Administrators..

How is the new Machine ID determined for an automatic installation?

Automatic installation packages create new accounts in the system. The **Automatic Install Wizard** lets you select a name via one of four options:

- prompt the user to enter 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

Can I manually create a new account at the Agent machine?

1. Right-click on the blue K in the system tray.
2. Select **Specify Account...**
3. Enter the machine ID you wish to create in the **Username** field
4. Enter **NewKaseyaAgent-*copyMach.group*** in the **Password** field. *copyMach.group* is the machine ID this new account copies settings from.
5. **NOTE: Leaving *copyMach.group* off creates a new default account. For a new default account enter NewKaseyaAgent- (including the "-") in the password field.**

How do I specify the group ID during an automatic install?

Automatic installation packages create new accounts in the system. You can direct what **Group ID** the new account gets by adding command line switches when running KcsSetup.exe.

- **KcsSetup.exe** - prompt the user to enter Group ID
- **KcsSetup.exe /d** - use the domain name of the currently logged on user as the Group ID
- **KcsSetup.exe /g=xxx** - use **xxx** as the Group ID

How do I pre-configure Agent settings for an automatic installation package?

Automatic installation packages are always created by copying settings from an existing machine account. All settings from the account you specify to copy settings from, except Machine ID and Group ID, apply to every new account created with this package.

How can I push Agents out using LAN Watch?

LAN Watch scans the entire sub-net of any LAN looking for all computers on that LAN. The Install Agents sub-function (under the Monitor tab) can push Agents out to any of those discovered machines as long as you have an **administrator login credential** for that machine.

Can I distribute the install package via email?

You can email the installation package as an attachment to as many email addresses as you like.

Warning: Command line switches are **not** carried in the installation package.

How do I manually install an Agent?

Execute KcsSetup.exe, the installation package by:

1. **Double clicking** KcsSetup.exe within Windows to launch it.
2. Open a **DOS command prompt** and type KcsSetup.exe followed by any desired command line switches.
3. Select **Run...** from the Windows Start menu and type KcsSetup.exe followed by any desired command line switches.

Agent Command line switch definitions:

Add command line parameters after **KcsSetup.exe** at a DOS prompt or from Run... in the Windows Start menu. Switches are case insensitive and order independent. Separate switches with an empty space.

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

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

/d - Use the current domain name as the Group ID for the new account. If the domain name cannot be determined programmatically, the user will be prompted to enter the Group ID (except in silent mode, /s, in which case the installation stops and an error is logged to the installation log).

/e - Exit immediately if the installer detects that an Agent is already installed. Use /e at the end of logon scripts. (/k or /r override /e).

/g=xxx - Specifies the Group ID to use for the new account. **xxx** must be an alpha-numeric string and can not contain spaces or punctuation marks.

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

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

/k - Displays a dialog box asking the user if it is ok to re-install when the Agent is already detected on the machine. Without this switch, in installer exists if an Agent is already present.

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

/p "install_path" - Overrides the default installation path by specifying the full directory path, including drive letter, in which to install the Agent. By default, the Agent installation creates a directory named "**Program Files\Kaseya\Agent"** off the root of the drive on which Windows is installed.

/r - Reinstall - Executes the installation program even if an Agent is already on the machine.

/s - Run in silent mode. Suppress all dialog boxes.

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

/u - Use the current user name as the Machine ID for the new account. If the user name cannot be determined programmatically, the user will be prompted to enter a Machine ID (except in silent mode, /s, in which case the installation stops and an error is logged to the installation log).

/w - Overwrite the existing configuration file with the on included in the Agent installation. Intended to be used with the /r switch to re-install with new server settings for an existing Agent that is attempting to connect to a server that no longer exists.

/x - Disable remote control after successfully installing the Agent. This option is ignored when updateing or re-installing. Remote control of this machine can only occur after the user selects the "Enable Remote Control" menu item from the system tray icon.

/z "Message" - Specify the message shown to the user when installation completes (except in silent mode, /s, in which case the installation completes and the status message is written to the installation log). The default message is: "*The Agent has been installed successfully on your computer.*".

Assist Check-In Ctl

Show me an explanation of the items on this page.

How do I change the check-in period of a Agent machine?

Changing the check-in period can be accomplished as follows:

1. Select the individual or group of Agent machines by checking the appropriate checkbox in the Agent machine list.
2. Enter the full check-in and/or check-in period in the respective fields.
3. Press Update.

The changes are reflected in the **Check-In Period** column.

Why doesn't the value I enter show up in the table for the machine I'm updating?

Minimum and maximum ranges for all the values set on the **Check-In Control** page are subject to the limits specified for each group ID's **Group Policy**. Master Administrators set the Group Policy for each group ID. To set the group policy click the System tab and then click the Group Policy button.

When does the setting change take effect on the Agent? (What is that red text?)

The VSA transfers new settings to Agents at the next check-in. The VSA displays new settings in **red** until they have been sent to the Agent.

How do I limit the bandwidth consumed by an agent?

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

How do I migrate Agents from one VSA to another?

You may decide for performance or logistical reasons to support a collection of desktop machines from a new VSA. Migrating Agent to a new VSA Server can be done at any time, whether or not the Agents are currently checking in.

1. At the original VSA, set the primary KServer setting to point to the **new** VSA address.
2. At the original VSA, point the secondary KServer setting to the **original** VSA.
3. At the new VSA, set both the primary and secondary KServer to point to the new VSA.
4. Wait for all the Agents to successfully check into the new VSA. At that time, the original VSA can be taken off-line.
5. 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

How do I change the port used by the Agent to check into the KServer with?

You can specify the TCP port used by the Agent to communicate with the KServer on.

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. Go to the Server Info function under the System tab. Enter the new port number by "Specify port Agents check into server with: " and click the **Change Port** button.

2. **Note**: If any Agents have not migrated to the new port before you switch the KServer, you will have to manually change the port at the Agent. Right click the Agent's menu and select **Set Account** and enter the server address and port. eg) 192.168.1.7:1234

Why do I need a warning if Agents on the same LAN as the VSA connect through a gateway?

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

Assist Create

Assistant

HELP HOME

Show me an explanation of the items on this page.

How do I create a new Agent machine account?

To create a new Agent machine account:

1. Click the **Create blank account** radio button. Or, to copy the settings from an existing Agent machine, select the radio button next to the Agent machine on the Agent machine list then select the **Copy settings from selected** radio button.
2. Type in a machine ID in the **Machine ID** field.
3. Select the group ID in the **Group ID** dropdown menu that the Agent machine will belong to.
4. In the **Notes** field, type in any information to help identify the Agent machine (e.g., company name, building number, city and state, etc.).
5. Type in the e-mail address of the individual responsible for administering the Agent machine in the **Admin Email** field. This e-mail address will be accessible from the Agent machine's Agent icon menu.
6. Type in the name of the Agent machine user in the **Contact Name** field, if applicable.
7. Type in the e-mail address of the Agent machine user in the **Contact Email** field, if applicable.
8. Type in the phone number of the Agent machine user in the **Contact Phone** field, if applicable.
9. Press Create Account. The new account is created and shows up in the Agent machine list.

What is the Auto check box for?

Check **Auto** to automatically enter a user email address when creating a new machine account. The email address is set to

machineid@groupid.com

What does the Set/Clear links do?

New accounts created in group ID <Group ID> copy settings from <machine ID>

Clicking the Set link assigns the account selected with the radio button in the **Copy Settings** column. All new accounts created in this group ID will copy their settings from this default account. When ever a new account is created for the for this Group ID the default account radio button is automatically selected. Click Clear to remove this assignment.

Accounts created in unassigned group IDs copy settings from <machine ID>

This link is only visible when logged on as a Master Administrator. Clicking the Set link assigns the account selected with the radio button in the **Copy Settings** column, to be the default account for this group ID. All new accounts created in any group ID without a default settings account specified, will copy their settings from this default account. Click Clear to remove this assignment.

What are the Setup Download links used for?

The **Setup Download** links are used to view the page Agent machine user's see when the Agent is installed on their system.

To send the link to the Agent machine user, either for new installations or to re-install:

1. Click on the appropriate **Email Link To** link in the Agent machine list. This will initiate the MAPI-compliant mail program on your system and automatically embed the link in the mail message body.
2. Type in any support information in the e-mail body to assist the Agent machine user in installing the Agent on their machine. Otherwise, the user, by simply clicking the link in the e-mail message, will be shown a Web browser window with step-by-step instructions in installing the Agent on their machine.
3. Send the message to the Agent machine user by sending according to your e-mail application.

Assist Delete

How do I delete a Agent machine account?

1. Select the checkbox next to the Agent machine you wish to delete.
2. Select **Uninstall Agent first at next check-in** if you want to uninstall the Agent on the machine first. Select **Delete account now without uninstalling the Agent** to delete the account from the server immediately.
3. Press Delete Accounts.

What happens if an Agent is left on a machine with a deleted account name?

The Agent continues to try to check into the VSA. The server automatically creates a new account for that Agent if one does not already exist on the machine. If the VSA server address is no longer valid you can remove the Agent just as you would uninstall any other software program using the Add/Remove Programs control panel item.

Why would I uninstall the Agent without deleting the account?

Select this option if you want to remove the Agent from a remote machine but keep all the data collected about that machine in the VSA.

Show me an explanation of the items on this page.

Assist Rename

How do I rename a machine account that already exists?

1. Select the radio button next the Agent machine you wish to rename.
2. Select **Rename Agent at next check-in then rename account on the system server** if you want to rename the account name on both the Agent and the server (*best for actively checking in machines*). Select **Rename account on system immediately** to rename the account on the server immediately.
3. Press **Rename**.

What happens if an account is renamed on the system without renaming the Agent first?

The Agent continues to try to check into the system with the old name. The server will automatically create a new account for that machine using the name it is trying to check in with. Update the account name at the Agent by right clicking the Agent menu and entering the new account name.

Why would I use the merge function?

Use merge to combine log data in two different accounts that pertain to the same machine. This could be necessary if an Agent was uninstalled and then reinstalled with a different account name. Also, loading a new Agent onto a machine that has had an Agent before may create a duplicate account for the same machine. 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 setting from the selected account are kept.
- Pending scripts from the selected account are kept. Pending scripts from the old offline account are discarded.
- **The old account is deleted after the merge.**

NOTE: Since the machine can only be active on a single account, only offline accounts are given as options to merge with.

Show me an explanation of the items on this page.

Assist Edit Profile

Show me an explanation of the items on this page.

How do I change the settings of an existing Agent machine account?

After creating a user account, you may need to change its settings. For example, the Agent machine is now used by a different user; or, the phone number where the Agent machine resides has changed.

To change user accounts settings:

1. In the Agent machine list, select the checkbox next to the Agent machine whose settings you wish to edit.
2. In the provide fields (Notes, Admin Email, Contact Name, Contact Email, Contact Phone), enter the new information.
3. Press Update.
4. The newly entered settings are shown in the respective Agent machine account's fields.

Assist Settings

Show me an explanation of the items on this page.

What is the Logging Control function used for?

The Logging Control function is used to control how much data, logged for each machine, is saved by the system.

- **Alert Log** - Records each alert generated by the monitoring system associated with a machine.
- **Agent Log** - Error conditions and machine activity recorded by the Agent
- **Configuration Changes** - All actions made to a machine by an administrator
- **Network Statistics** - Records bandwidth utilization by every application vs. time.
- **Script Log** - Status for each script executed

The maximum age for these logs can also be set to prevent the logs from recording too much information, thus creating large log files.

The information recorded in the logs are viewed by accessing the Agent Logs function.

Windows Event Log Capture

You can collect windows event log data for any machine ID. The **last 500 event log entries are saved** for each log type.

- **Application Event Log** - Windows Application event log
- **System Event Log** - Windows System event log
- **Security Event Log** - Windows Security event log

Enable or disable collection of any event type, **independently for each log**, to maximize the length of time events of interest are saved for each log. Event types are:

- Error
- Warning
- Information
- Success Audit
- Failure Audit

Assist User Access

Show me an explanation of the items on this page.

Why must the Login Name be unique?

Users may log into the VSA to enter trouble tickets and/or get remote access to their machine. The Login Name, entered here, acts as the login credential for that users. All login names must be unique in the system.

Users may also login using their machine ID. Login Names, machine IDs, and Administrator names must be unique system wide.

Can I customize the User Access pages?

Yes. Master Administrators can specify the look seen by their users to display a custom logo or links. Click the **here** link to view and edit the web layout of the user access page. User Access is a frame set consisting of three pages: header frame, left frame, and right frame. You can select any page you like for the Header frame and the Left frame. You can also adjust the boundary location between the frames. User Access control pages run in the Right frame and can not be altered.

How many logins can I assign to a machine?

One. Each machine can have only one remote user login credential assigned to it. Users may login using either the Machine ID or the Login Name. Login names and passwords are case sensitive. Passwords must be at least six characters long.

What happens if a user forgets their password?

The user login page has a line to email the user a new password if they **forgot their password**. A new random password is emailed to the user listed for that managed machine. You can set the user email address with the Edit Profile function under the Agent tab.

Can I stop a user from chatting with an administrator

Uncheck the box next to a machine name under the **Enable Chat** column to prevent that machine from starting chat session.

Why did the user logon no longer show Enabled

User logons follow the same Login Policy as administrator 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.

Assist Update Agent

Assistant

HELP HOME

Show me an explanation of the items on this page.

What is Update Agent function used for?

Use the **Update Agent** function to update the Agent on selected Agent machines. By viewing the information provided in the Machine Accounts function of the Agent feature tab, administrators can quickly see which Agent machines need their Agent updated.

Administrators can enable the **Remind me at logon when Agents need an update** checkbox to remind them of Agents that need to be updated. Only Agents that belong to the administrator will activate this feature.

How do I update the Agent on a Agent machine?

To update the Agent on a Agent machine:

1. In the Agent machine list, select the checkbox next to the Agent machine whose Agent you wish to update.

Note: More than one Agent machine can be selected if you wish to update more than one machine.

2. Press Update Agent.
3. In the **Last Update** column, update progress information will be shown. If the update is successful, the time and date of the update will be shown.

Since the server must wait for the Agent machine to check-in, according to the check-in schedule as specified in the Check-In Control function of the Agent feature tab, **Pending** will be shown in the **Last Update** column if the Agent machine hasn't checked in yet. When the Agent machine checks in and the update is successful, the time and date of the update will then be shown.

System Tab

The System feature tab allows a master administrator to create, delete, and set login policies for standard administrators. A master administrator can also set the start page for standard administrators to view at login.

Note: Standard administrators only have access to the Admin Profile and Alerts function of the System tab.

To access the Assistant, click Assistant from any function page.

The following functions are available in the System feature tab:

Functions	Description
Preferences	Set email where alerts are sent to and to change administrator passwords.
Machine Group Create / Delete	Create, edit, and delete Machine Group IDs.
Naming Policy	Automatically enforce naming policy based on each machines IP address, network, and computer name
Check-in Policy	Set limits on a variety of agent check-in parameters.
Admin Roles Create / Delete	Create and delete administrator roles. Assign administrators to roles to inherit administrator rights.
Membership	Define which administrators belong to which administrator roles
Group Access	Define which Machine groups each Administrator role gets access to.
Function Access	Defines the functions available to an administrator role
Admin Account Create / Delete	Create and delete standard or master administrators.
Enable/Disable	Enable or disable standard or master administrator accounts.
Set Password	Change administrator account passwords.
Admin History	Display the functions visited in the last 30 days for each administrator.
Request Support	Access Kaseya support and/or give Kaseya support access to your server.
Configure	View server information, license code and subscription information, obtain latest server updates, and server IP information.
System Log	Logs events that can not be tracked by machine ID for 60 days.
Statistics	Display VSA server performance statistics
Login Policy	Set login policies.
Customize	Customize the login page and graphical user interface for the system.

Migrate VSA	Distribute the server load across multiple servers. Groups can be located across several servers but still be administered from the same console.
Database Views	Configures database view access

System > Preferences

Show me an explanation of the items on this page.

How do I set the To: address for alerts sent to me?

To set the To: address for alerts sent to you:

1. Enter the email address where you want to receive alerts.
2. Press APPLY.

How do I change my login name and/or password?

To change your login name and password:

1. Enter your new name in the **Change** field.
2. Enter the new password in the **New Password** field.
3. **Note: If you would like the system to generate a strong password for you, press SUGGEST PASSWORD. A dialog box will appear showing the new password; the new password is automatically entered in the New Password and Confirm Password fields. Be sure to write it down before pressing OK to clear the dialog box.**
4. Confirm the password by re-typing it in the **Confirm Password** field.
5. Enter the email address where you want to receive alerts.
6. Press **CHANGE**.

Select display format for long names

The web pages are designed to display well for typical string sizes. Occasionally data fields contain long names that will not display properly on the web pages. You can specify how long names display as follows:

- **Limit names for better page layout** - This settings limits the string size to fit well on the web page. Strings exceeding a maximum length are limited with a ... To view the entire name, hover the mouse of the string and a tool tip pops up showing the entire name.
- **Allow long name wrapping** - Long strings are allowed to wrap within the web page. This may disturb the normal web page layout and names may wrap at any character position.

Explanation of items on this page

The following elements are displayed in the Admin Profile function:

Set email address to deliver messages for this administrator to

Specifies the email address that alerts will be sent to. After entering the email address, press **APPLY** to make it active. Previously set alerts retain the original email address specified when the alerts were set.

Apply

Sets the email address entered in the Set Email Address field.

Change Login Name

Enter the administrator name that you wish to use to login.

New Password

When changing the administrator password, enter the new password in the New Password field.

Confirm Password

Confirm the new password by re-typing it in the **CONFIRM PASSWORD** field.

Change

After entering a new password and confirming it, press **CHANGE** to make the change.

Suggest

Creates a new, strong password and automatically enters it in the **NEW PASSWORD** and **CONFIRM PASSWORD** fields. The new password is displayed in a dialog box. Be sure to write the new password down.

System > Machine Group Create / Delete

Show me an explanation of the items on this page.

How do I create a new group ID?

To create a new machine group:

1. Enter a new group name in the text box.
2. Press **Create** to create to create the new machine group ID. The new machine group is displayed in the list.

You can now assign administrators to administer the new group.

How do I delete a group ID?

To delete a machine group:

1. Select the checkbox next to the machine group ID you wish to delete. More than one checkbox can be selected if you wish to delete multiple machine groups at the same time.
2. Press **Delete**.
3. A dialog box confirms the deletion. Press OK to delete, or Cancel. The groups are removed from the list.

Only **empty** machine groups may be deleted. If any machine is assigned to a machine group, then the checkbox beside the group name will be disabled and shown in gray.

Note: Deleting a group also deletes any associated subgroups.

Explanation of items on this page

The following elements are displayed in the Membership function:

Enter name for new machine group

Enter the name of a new machine group ID that you wish to create.

Allow standard administrators to create root groups

By default, standard administrators may not create or delete root level machine groups. If you wish to allow standard administrators to create or delete root level machine group check this box.

When a standard administrator creates a new root machine group, **permission to access** that machine group is automatically granted to **all administrator roles that administrator belongs to**.

Note: Only master administrators by enable this permission

Create as subgroup of

Create **subgroups** within machine groups. To create a subgroup select the parent group from this dropdown control prior to clicking Create. To create a new top level root group leave the dropdown control set to **< New Root Group >**

Create

Press **Create** to create a new machine group with the specified name.

Delete

Press **Delete** to delete an empty machine group. An empty machine group is one with no machines assigned to that group.

Total Machines

This value allows the administrator to see the number of machines managed.

Total Groups

This value allows the administrator to see the number of groups defined.

Machine Group

Each machine group defined is displayed under **Machine Group**. The checkbox beside the machine group is enabled only if no machines are assigned to that group ID. The checkbox may be selected to delete empty machine groups.

Total Group

Shows the administrator the number of machines in each machine group **including any associated subgroups**. This can be used to evenly distribute machines per group, or to plan migration of some groups to a new server.

Sub Group

Shows the administrator the number of machines in an individual machine group. If the group has subgroups, none of the machines in those subgroups are counted.

System > Naming Policy

Show me an explanation of the items on this page.

What is the naming policy used for?
The **Naming Policy** allows an administrator to define the IP address criteria used to automatically assign machines to group IDs. The connection gateway and/or IP address of each machine will be used to determine if it matches the specification for a group ID. If a match is found and the machine is in a different machine group, then the machine is automatically renamed.

Each machine group may have multiple name policies. Use this capability to automatically assign machines with different IP address ranges into the same machine group.

An administrator may optionally choose to enforce the naming convention that all machines in a group must use its computer name as its machine ID. If any machine is found with a machine ID other than its computer name and the computer name policy is enabled for the machine's group ID, then the machine is automatically renamed.

Note: Machines are renamed to the new group ID at their next FULL CHECKIN. The quick checkin cycle will not trigger a rename. To rename a group of machines quickly using Naming Policy, schedule the Force Checkin sample script located in the Agent Control folder (under the Install tab).

How do I assign a naming policy to a machine group?
To assign a naming policy to a group ID:

1. Optionally select the checkbox beside the **Connection Gateway** to enable the criteria based on the IP address of the machine as viewed from the server. The connection gateway is typically the WAN address of the managed machine. Enter the connection gateway IP address. This rule may be applied independently to a group ID.
2. Optionally select the checkbox beside the **IP Range** to enable the criteria based on the IP address assigned to the machine. Enter the IP addresses, such as 192.168.1.2 – 192.168.1.254, to define a range that the machine must fall in order to be assigned to a group ID. This rule may be applied independently to a group ID.
3. Optionally select the checkbox beside **Force machine ID to always be computer name** to enable the system to enforce the rule that a machine uses its computer name as its machine ID. This rule may be applied independently to a group ID.
4. Select the radio button beside a **Machine Group**.
5. Press **Update/Add** to apply the naming policy to the selected machine group. The system will immediately begin enforcing the group ID's new rule to machines checking in to the server.

How do I remove a naming policy assigned to a machine group?
To remove a naming policy from a group ID:

1. Select the radio button beside a **Machine Group**.
2. Press **Clear** to remove the naming policy assigned to the selected machine group. The system will immediately stop applying the rule for the machine group.

Explanation of items on this page
The following elements are displayed in the Membership function:

Connection Gateway
Check the box to enable use of the **Connection Gateway** as naming policy criteria for a group ID. Enter the IP address of the machine as viewed from the system server. This gateway is typically the WAN address of the managed machine. The managed machine must have this IP address as its connection gateway in order to be automatically placed into a group ID.

IP Range
Check the box to enable use of the **IP Range** as naming policy criteria for a group ID. Enter the IP addresses to specify a range in which a managed machine must have in order to be automatically placed into a group ID.

Force machine ID to always be computer name
Check the box to enable enforcement of computer name as the machine ID of all machines assigned to a machine group.

Update

Press **Update** to set the naming policy for a machine group.

Add

Press **Add** to insert an addition naming policy for a machine group.

Each machine group may have multiple name policies. Use this capability to automatically assign machines with different IP address ranges into the same machine group.

Clear

Press **Clear** to remove the naming policy from a machine group.

Machine Group

This column contains the machine groups defined for this system.

Group Naming Policy

This column shows the naming policy assigned to the **Machine Group**. If there is no policy set for a **Machine Group**, then *No Policy set* is displayed.

Force Machine ID

When an administrator enables the computer name enforcement rule for a **Machine Group**, an indicator, such as a check mark, is shown in this column.

System > Check-in Policy

Show me an explanation of the items on this page.

What is the function of Group Policy?

The Group Policy allows master administrators to set parameters on the different functions set by standard administrators. These parameters prevent administrators from making changes to the system that may cause performance degradation and place unnecessary load on the server.

The Group Policy allows master administrators to set the parameters of the following functions:

- **Maximum Age for Log Entries** Sets the minimum/maximum settings that can be entered in the *Set Max Age for Log Entries* setting of the Logging Control function of the Agent feature tab.
- **Quick Check-In Period** Sets the minimum/maximum settings that can be entered in the *Quick Check-In* setting of the Check-In Control function of the Agent feature tab.
- **KServer Address Fixed/Admin Defined** Selecting the Primary and/or Secondary radio buttons relegates the setting of the KServer addresses to the settings specified in the *Primary KServer* and/or *Secondary KServer* settings of the Check-In Control function of the Agent feature tab. Specifying a setting in the *Admin Defined* fields prevents standard administrators from changing the settings in the Check-In Control function. In this case, the Agents will check in to the KServer specified in these fields.

How do I set Group Policy parameters?

To set policy parameters for a group or set of groups:

1. The **Group IDs** column will list all the groups administered by the server. Select the group you would like to apply policies to by selecting the checkbox next to the group ID. More than one group can be selected if you wish to apply the same settings to multiple groups.
2. In the following fields, enter the minimum and/or maximum parameters:

- **Maximum Age for Log Entries** Sets the minimum/maximum settings that can be entered in the *Set Max Age for Log Entries* setting of the Logging Control function of the Agent feature tab.
- **Quick Check-In Period** Sets the minimum/maximum settings that can be entered in the *Quick Check-In* setting of the Check-In Control function of the Agent feature tab.
- **Admin Defined/KServer Address Fixed** Selecting the Primary and/or Secondary radio buttons relegates the setting of the KServer addresses to the settings specified in the *Primary KServer* and/or *Secondary KServer* settings of the Check-In Control function of the Agent feature tab. Specifying a setting in the *KServer Address Fixed* fields prevents administrators from changing the settings in the **Check-In Control** function. In this case, the Agents will check in to the KServer specified in these fields.

3. Press **update**.
4. The minimum and maximum settings are displayed in the **KServer**, **Stats**, **Log Age**, **Full**, and **Quick** columns.

Note: The KServer column will display Editable if the Primary/Secondary radio buttons are selected in the *Admin Defined* field. This designates that the KServer settings have been relegated to the settings specified by an administrator in the *Primary KServer* and *Secondary KServer* settings in the Check-In Control function of the Agent feature tab. Otherwise, the IP address/host name entered in the *KServer Address Fixed* field will be displayed, and thus cannot be changed by an administrator in the Check-Control function.

How do I remove a setting from a field?

To remove a setting from only one field:

1. In the field that you want removed, enter **0** (zero).
2. Leave all other fields blank.
3. Press update.

The setting is update in the client list view. All other settings remain untouched.

How do I prevent agents from automatically creating new accounts when they first check in?

Uncheck **Allow automatic account creation for groups without a policy** to block agents checking in for the first time from automatically creating new accounts in a group without any policy set. Typically you will leave this box checked to allow anyone to quickly load up an agent and get that agent checking into your server. Allowing automatic account creation is **not** a security problem because the person is effectively giving you full control over there system without gaining any access to your server.

Note: Automatic account creation is enabled by default.

How do I make a change to only one field at a time?

If you need to make a change to only setting in a group:

1. In the field you want changed, enter the new value.
2. Leave all other fields empty. This indicates that these fields will remain unchanged.
3. Press update.

Only the field whose value was changed is updated. All other fields retain their original setting.

Explanation of items on this page

The Group Policy function allows master administrators to set parameters for a variety of functions. These settings can prevent standard administrators from configuring settings that place undue stress on servers running the kserver service. Defining a minimum Quick Check-In period, for example, prevents standard administrators from entering a value that would overload the server with multiple simultaneous check-in requests.

The Group Policy also allows master administrators to place limits on the quick check-in times of deployed Agents, as defined in the Check-In Control function. This prevents other administrators from entering values that may overload the server with constant check-in requests.

The following elements are displayed in the Group Policy function:

Set Max Age for Log Entries

Sets the minimum and maximum value allowed for the Max Age in the Check-In Control function.

Quick Check-In Period

Sets the minimum and maximum value allowed for the Quick Check-In in the Check-In Control function.

Admin Defined

Selecting either the Primary and/or Secondary radio buttons sets the primary and/or secondary server IP/host name addresses to the value specified in the **Primary KServer** and **Secondary KServer** fields in the Check-In Control function (Agent tab). Selecting these radio buttons allows standard administrators to control these settings independently.

KServer Address Fixed

Selecting the radio buttons and entering an IP/hostname address in the **KServer Address Fixed** fields prevents standards administrators from changing the settings specified in the **Primary KServer** and **Secondary KServer** fields in the Check-In Control function (Agent tab).

Allow automatic account creation

You can enable/disable automatic account creation on a per Group ID basis. Accounts are automatically created when the Automatic Installation Package is run.

Allow automatic account creation for groups without a policy

Uncheck this box to block agents checking in for the first time from automatically creating new accounts in a group without any policy set.

Note: Automatic account creation is enabled by default.

Update

Pressing Update enters all of the changes for the selected group(s). To change only the minimum or maximum setting in each field, ensure that the field that is to remain unchanged is empty before pressing update. Entering a '0' in any field and pressing update clears the field.

Select All/Unselect All

Select All will select all groups on all account pages. Unselect All will unselect selected groups on all account pages. To select an individual group, select the checkbox next to the group ID.

Groups IDs

Shows all groups administered by the administrator currently logged in to the system, as shown in the upper left-hand corner of the console window.

KServer (1st/2nd)

Shows the IP addresses/host names of the primary(1st) and secondary(2nd) servers used by the specified group(s). These settings are edited using the **Admin Defined** and **KServer Address Fixed** fields, shown above. If *Editable* is shown, the primary and secondary server addresses are configurable by the group's administrator in the Check-In Control function (Agent tab).

Log Age (Min/Max)

Shows the settings entered in the **Set Max Age For Log Entries** fields, as shown above.

Quick (Min/Max)

Shows the settings entered in the **Quick Check-In Period** fields, as shown above.

Select All/Unselect All

Select All will select all admin accounts on all account pages. Unselect All will unselect selected admin accounts on all account pages. To select an individual admin account, select the checkbox next to the username.

System > Admin Roles Create / Delete

Show me an explanation of the items on this page.

Administrators belong to none, one, or more administrator roles. Administrators in the same role may share scripts and Agent installation packages. Administrators in the same role have access to the same machine groups assigned to the admin role.

How do I create a new administrator role?

To create a new administrator role:

1. Type in a name for the new administrator role.
2. Press CREATE. The new role is created and appears in the role list.

Member Administrators information is displayed to show the administrators belonging to each role. An administrator may belong to more than one admin role.

How do I rename an existing administrator role?

To rename an administrator role:

1. Click the edit icon beside an administrator role you wish to rename.
2. Type in the new name for the administrator role.
3. Press **OK** to rename, or Cancel.

How do I delete an administrator role?

To delete an administrator role:

1. Select the checkbox next to the administrator role you want to delete. More than one checkbox can be selected if you wish to delete more than one role at the same time.
2. Press **DELETE**. A dialog box confirms the deletion. Press OK to delete, or Cancel.
3. The administrator role(s) are deleted.

The Master role cannot be deleted. Being a member of the Master role grants an administrator privileges to configure settings for the server as well as administer both administrator and user accounts. Administrators who are not a member of the Master role may only administer user accounts.

Explanation of items on this page

The following elements are displayed in the Create / Delete function:

Enter name for new administrator role

Enter the name for the administrator role to create.

Create

Press **CREATE** to create the new administrator role.

Delete

Press **DELETE** to delete the administrator role(s) that are selected. Select the roles by checking the checkbox next to each role you wish to delete.

Role Name

The existing administrator roles are displayed under the column labeled role Name.

Member Administrators

The administrators belonging to each role are displayed under the column labeled **Member Administrators**.

Edit icon

Click on the edit icon beside each administrator role name you wish to rename.

System > Admin Role Membership

Show me an explanation of the items on this page.

Administrators belong to none, one, or more administrator roles. Administrators in the same role may share scripts and Agent installation packages. Administrators in the same role have access to the same machine groups assigned to the admin role.

How do I assign an administrator to an admin role?

To assign an administrator membership to an admin role:

1. Select the checkbox next to the administrators you wish to assign to one or more admin roles. More than one checkbox can be selected if you wish to assign more than one administrator at the same time.
2. Select the administrator roles by clicking the left mouse button over the admin role name. More than one admin role can be selected by holding down the <CTRL> key while selecting additional admin role names.
3. Press **Add** to assign the selected administrators to the selected admin roles.

How do I remove an administrator from an admin role?

To remove an administrator's membership from an admin role:

1. Select the checkbox next to the administrators you wish to remove from one or more admin roles. More than one checkbox can be selected if you wish to remove multiple administrators from the selected admin roles at the same time.
2. Select the administrator roles by clicking the left mouse button over the admin role name. More than one admin role can be selected by holding down the <CTRL> key while selecting additional admin role names.
3. Press Remove to remove the selected administrators from the selected admin roles.

Explanation of items on this page

The following elements are displayed in the Membership function:

Assign administrators to roles

A list of all existing administrator roles is displayed. You may choose one or more admin roles from this list to add or remove administrator membership.

Add

Press **ADD** to add administrator(s) to the selected administrator role(s).

Remove

Press **REMOVE** to remove administrator(s) from the selected administrator role(s).

Standard Admin/Master Admin

Administrators are listed under this column. A background of two alternating shades of beige designates master administrators. A background of two alternating shades of grey designates standard administrators. Master administrators are members of the Master admin role. A master administrator can create and manage both user and admin accounts, as well as configure the server settings. A standard admin can create and manage user accounts.

Admin role

roles that each administrator is a member of are displayed under **Admin role**.

System > Group Access

Show me an explanation of the items on this page.

Administrators belong to none, one, or more administrator roles. Administrators in the same role may share scripts and Agent installation packages. Administrators in the same administrator role have access to the same machine groups.

How do I assign machine groups to an administrator role?

To assign machine groups to an administrator role:

1. Select the checkbox next to the administrator role you wish to assign one or more machine groups. More than one checkbox can be selected if you wish to assign machine groups to more than one admin role at the same time.
2. Select the machine groups by clicking the left mouse button over the machine group name. More than one admin role can be selected by holding down the <CTRL> key while selecting additional machine group names.
3. Press Add to assign the selected machine groups to the selected admin roles.

> **Note: Adding a machine group automatically adds access to any associated subgroups.**

How do I remove machine groups from an administrator role?

To remove machine groups from an administrator role:

1. Select the checkbox next to the administrator role from which you wish to remove one or more machine groups. More than one checkbox can be selected if you wish to remove machine groups from multiple administrator roles at the same time.
2. Select the machine groups by clicking the left mouse button over the machine group name. More than one machine group can be selected by holding down the <CTRL> key while selecting additional machine group names.
3. Press Remove to remove the selected machine groups from the selected admin roles.

> **Note: Removing a machine group automatically removes access to any associated subgroups.**

How do I rename an existing administrator role?

To rename an administrator role:

1. Click the edit icon beside an administrator role you wish to rename.
2. Type in the new name for the administrator role.
3. Press OK to rename, or Cancel.

Explanation of items on this page

The following elements are displayed in the Membership function:

Give administrator roles access to machine groups

A list of all existing machine groups is displayed. You may assign machine groups to one or more administrator roles.

Add

Press ADD to add machine group(s) to the selected administrator role(s).

Remove

Press REMOVE to remove machine group(s) from the selected administrator role(s).

Admin role

Each administrator role defined is displayed under Admin role. The Master role is designated with a beige background. All other roles are designated by two alternating shades of grey. Members of the Master admin role can create and manage both user and admin accounts, as well as configure the VSA server settings. Members of all other admin roles can create and manage user accounts.

Machine Group

Lists the groups that the administrator role has permission to administer. If the administrator role has permission to administer all groups, All Group IDs is listed in the Machine Group column. Administrators with membership to the admin role have permission to manage all machines in the machine groups assigned to the admin role.

Edit icon

Click on the edit icon beside each administrator role name you wish to rename.

System > Function Access

Limit the functions accessible to an administrator role. Function Access lets you provide limited functionality to an administrator role. Say you have someone you wish to let remote control a group of machines but do not want to let them run scripts, access audit, change monitoring configuration, or control patch management. The following steps let you create an administrator role with that limited access.

1. Create a new Administrator Role
2. Give this administrator role access to the desired machine groups with the Group Access function.
3. Click the **Function Access** function.
4. Select the new administrator role from the **Select administrator role** drop down control.
5. *Uncheck* all the tabs and functions you do not want to let this administrator role use.

Each administrator role can be assigned a different set of functions. System functions related to creating administrators, administrator roles, or server management can never be accessed by standard administrators.

Note: Master administrators ALWAYS get access to all functions

System > Login Hours

You can restrict system access to certain hours of operation on a per administrator role basis. Use this function to limit administrator login to certain **times of day**. Each **day of the week** may have different hours of operation set.

- Set unique policies for each administrator role.
- Set approved hours of access independently for each day of the week.
- Approve all day access independently for each day of the week.

System > Admin Create / Delete

Show me an explanation of the items on this page.

How do I create a new administrator?

To create a new administrator:

1. Type in a name for the administrator in the **Admin Name** field.
2. Select the group to which the new administrator belongs. After creating the account, the administrator's group membership may be changed, added, or deleted by using the **Membership** function under the **Admin Groups** category.

   If the new administrator will be a master administrator, select the Master group membership. If an administrator is not a member of the Master group, then the administrator is a standard administrator.
3. Enter an email address for the new administrator.
4. Type in a password in the **Create Password** field. Confirm the password by re-typing it in the **Confirm Password** field.

> **Note: If you would like the system to generate a strong password for you, press SUGGEST PASSWORD. A dialog box will appear showing the new password; the new password is automatically entered in the New Password and Confirm Password fields. Press OK to clear the new password dialog box.**

5. Press **CREATE ADMIN**. The new account is created and appears in the administrator list with the corresponding administrator color and groups they are permitted to administer.

How do I delete an administrator account?

To delete an administrator account:

1. Select the checkbox next to the administrator whose account you want to delete. More than one checkbox can be selected if you wish to delete more than one account at the same time.
2. Press **DELETE**. A dialog box confirms the deletion. Press OK to delete, or Cancel.
3. The administrator account(s) are deleted.

Explanation of items on this page

Master administrators can also **delete** and **enable/disable** accounts.

The following elements are displayed in the Create / Delete function:

Standard Admin/Master Admin

Membership in the **Master role** determines whether the administrator is a master administrator. A master administrator can create and manage both user and admin accounts, as well as configure the server settings. A standard admin can create and manage user accounts. A background of two alternating shades of beige designates master administrators. A background of two alternating shades of grey designates standard administrators.

Admin Name

Enter the name for the administrator being created.

Set Admin Group Membership

The drop down menu shows the available administrator groups to which an administrator may belong. Select an admin group to initially place the new administrator. The administrator group membership may be changed any time after creation.

Admin Email

Enter the administrator's email address. Needed to automatically set alerts for machine IDs created by this administrator.

Create/Confirm Password

Enter the administrator's password and password confirmation in the appropriate fields.

Suggest

Pressing **SUGGEST PASSWORD** will generate a strong random password for better security. A dialog box will display the random password (make sure to write it down). The password and confirm password fields will automatically populate with the generated password.

Create

Press **Create** to create the new administrator account.

Delete

Press **Delete** to delete the administrator account(s) that are selected. Select the accounts by checking the checkbox next to each administrator name you wish to delete.

System > Enable / Disable

Show me an explanation of the items on this page.

How do I disable/enable an administrator account?

The system automatically locks out an administrator account if they exceed the number of failed login attempts, as specified in the Login Policy function of the System feature tab. Normally, the administrator has to wait the time specified in the Login Policy. Only another master administrator can enable their account.

To *enable* an administrator account:

1. Select the administrator whose account has been disabled by selecting the radio button next to the administrator name. **Disabled by Admin** is displayed in the **Last Login** column of the disabled account.
2. Press enable account.
3. **Disabled by Admin** is removed from the **Last Login** column and the administrator account is now enabled.

To *disable* an administrator account:

1. Select the administrator whose account you want to disable by selecting the radio button next to the administrator name.
2. Press disable account.
3. The account is disable. **Disabled by Admin** is displayed in the **Last Login** column of the disabled account.

The system automatically locks out an administrator account if they exceed the number of failed login attempts, as specified in the Login Policy function of the System feature tab. Normally, the administrator has to wait the time specified in the Login Policy. Only another master administrator can enable their account.

To *enable* an administrator account:

1. Select the administrator whose account has been disabled by selecting the radio button next to the administrator name. **Disabled by Admin** is displayed in the **Last Login** column of the disabled account.
2. Press enable account.
3. **Disabled by Admin** is removed from the **Last Login** column and the administrator account is now enabled.

To *disable* an administrator account:

1. Select the administrator whose account you want to disable by selecting the radio button next to the administrator name.
2. Press disable account.
3. The account is disable. **Disabled by Admin** is displayed in the **Last Login** column of the disabled account.

Explanation of items on this page

This function allows master administrators to enable and disable administrator accounts. Select the user(s) to enable or disable by selecting the appropriate radio button, then pressing either Enable Account or Disable Account.

Master administrators can also create and delete accounts.

The following elements are displayed in the Enable/Disable function:

Enable Account

Select the administrator by checking the checkbox next to the administrator, then press enable account to enable a previously disabled master or standard administrator account.

Disable Account

Select the administrator by checking the checkbox next to the administrator, then press disable account to disable a master or standard administrator account. When the account is disabled, *Disabled by Admin* is listed in the **Last Login** column.

Standard Admin/Master Admin

Lists all the administrators on the server. The color alternates to assist in viewing: Master administrators are designated by two alternating shades of beige; the standard administrators by two alternating shades of gray.

Last Login

(Normal text) Date/time that this administrator last logged into the VSA

OR

(Red text) This administrator account has been disabled until the date/time displayed.

Account Created

Date/time that this administrator account was created.

System > Set Password

Show me an explanation of the items on this page.

How do I change an administrator password?
To change an administrator password:

1. Select the radio button next to the administrator's account whose password you would like to change
2. Enter the new password in the **New Password** field.

> **Note: If you would like the system to generate a strong password for you, press Suggest Password. A dialog box will appear showing the new password; the new password is automatically entered in the New Password and Confirm Password fields. Be sure to write it down before pressing OK to clear the dialog box.**

3. Confirm the password by re-entering it in the **Confirm Password** field.
4. Press change password.

The password is changed. Don't forget to notify the administrator of the password change.

To change an administrator password:

1. Select the radio button next to the administrator's account whose password you would like to change
2. Enter the new password in the **New Password** field.

> **Note: If you would like the system to generate a strong password for you, press Suggest Password. A dialog box will appear showing the new password; the new password is automatically entered in the New Password and Confirm Password fields. Be sure to write it down before pressing OK to clear the dialog box.**

3. Confirm the password by re-entering it in the **Confirm Password** field.
4. Press change password.

The password is changed. Don't forget to notify the administrator of the password change.

How do I clear the Total Login Failures counter for an administrator?
To clear the Total Login Failures counter for an administrator:

1. Select the checkbox next to the administrators whose Total Login Failures counter you would like to clear. You can click **Select All** to automatically select all listed administrators.
2. Press clear total. The Total Failed Logins counter for the selected administrator accounts are reset to zero.

To clear the Total Login Failures counter for an administrator:

1. Select the checkbox next to the administrators whose Total Login Failures counter you would like to clear. You can click **Select All** to automatically select all listed administrators.
2. Press clear total. The Total Failed Logins counter for the selected administrator accounts are reset to zero.

Explanation of items on this page
The following elements are displayed in the Set Password function:

New Password
Select an account in the administrator list and enter a new password in this field.

Confirm Password
Confirm the password entered in the **New Password** field by re-entering it here.

Change Password
Press change password after entering the new password and confirmation. A dialog box will indicate a successful password change.

Suggest Password
Pressing Suggest Password will generate a strong random password for better security. A dialog box will display the random password (make sure to write it down). The password and confirm password fields will automatically populate with the generated password.

Clear Total

Clears all of the values shown in the **Total Failed Logins** column for selected machines.

Select Account
Ensure a radio button is selected before pressing CHANGE PASSWORD.

Standard Admin / Master Admin
Lists all the administrators on the System Server. The color alternates to assist in viewing: Master administrators are designated by two alternating shades of beige; the standard administrators by two alternating shades of gray.

Failed Logins in a Row
Lists the number of failed logins in a row. This information is helpful in monitoring possible system security attacks. If the number of failed logins in a row exceeds the number specified in the Login Policy function, the administrator's account is disabled for a set amount of time and can only be enabled by waiting the specified amount of time or by having another master administrator manually enable the account.

Total Failed Logins
Lists the total number of failed logins attempted by an administrator.

System > Admin History

Every time an administrator logs in and selects a function, the system records that action in this log. The system saves history data for each administrator for 30 days.

View administrator history by clicking the desired **administrator name** from the list. The system then displays a time ordered list of functions visited by that administrator.

In addition to a history of functions visited, this log also displays any actions captured by the System Log that performed by the selected administrator.

Note: This function may only be viewed by a Master Administrator.

Note: This log data does not appear in any reports. Reports are only available for data associated with a machine ID.

System > Request Support

Use this function to contact Kaseya support. Answers to common questions are posted to the Support Forum at http://www.kaseya.com/kforum. The Support Forum hosts an interactive community of Kaseya users that discuss a wide variety of issues and solutions on a daily basis. **Subscribe to the forum** to get new posts of interest directly emailed to you as new information appears.

Kaseya support engineers can solve problems with your system quickly and efficiently when they can directly access your KServer. We realize the security implications of providing access to your server. To protect this login, your system creates a secure login. **No one has access to the password**, *not even the Kaseya support engineer*.

Create button

Create a **kaseyasupport** master administrator account on your system. The password gets changed every time you click this button. Your system securely transmits this information to a Kaseya Support system. The Kaseya Support engineer can use our system to log into your system and help solve any problems. For security reasons, our support engineers never have access to this password.

Your Information

Typically Kaseya support needs some basic information about your system to begin providing support. Your **email address** and **Customer ID** at a minimum.

Submit Trouble Tickets

There are three ways to submit support requests to Kaseya.

1. You can **directly create and track tickets in our support system** by clicking the **Login** button.
2. Email requests to support@kaseya.com
3. Call our support engineers from 6am to 6pm Eastern Time, Monday through Friday at 1-415-694-5700.

Note: You can track any and all tickets you submit through the Login system. Tickets submitted via support@kaseya.com or the phone can not be tracked by you through the online system.

System > Configure

Show me an explanation of the items on this page.

How do I change the IP address/host name of the server?

The client machines must be able to resolve the IP address/host name of the system in order for the Agents to properly check-in with the system server.

The exposed IP address/host name can be changed by:

1. Enter an IP address or host name in the text box titled "Change external name / IP address of Server".
2. Press Change name/IP.

The IP address/host name is changed.

Note: Do NOT use computer name for your server. The Agent utilizes standard WinSock calls to resolve a fully qualified hostname 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, using NETBIOS over TCP/IP or the LMHOSTS file or other method. 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.

How long are database backups kept?

Database backups older than three times the backup and maintenance period are discarded automatically to prevent your disk drive from filling up. For example, if the backup occurs every 7 days, any backup older than 21 days is deleted. Backup database files are stored in the BACKUP directory with the database (typically **C:\Kaseya\UserProfiles\@dbBackup**).

How do I update the system software?

To see if a newer version of system software is available for download, press **CHECK FOR UPDATE**. If a newer version is available, the update is automatically downloaded. You are then shown a list of the update's changed and modifications, and are asked whether the update should be applied immediately or at a later time.

The current version of the software is shown in the **Version Number** field.

How do I apply the last downloaded version of the system software?

The most recent version of system software can be re-installed by pressing RE-APPLY DATABASE. This is convenient, especially if you are having problems with the software and you want to perform a re-install.

How do I send a test email from the system?

To confirm that the system can send an email, click the **Test** button to specify a recipient's email address. Click the OK button to send the email to the specified email address. Click Cancel to abort. The system uses the Default SMTP Virtual Server to send email. This service must be installed and running in order to send email. The service must also be able to resolve DNS addresses to route email to other SMTP servers. If you suspect that you are not receiving emails from the VSA server, send test emails to various recipient addresses to confirm whether the Default SMTP Virtual Server can send email or is unable to resolve to a specific domain.

Explanation of items on this page

The Server Info function displays important information about the system server and Service. General maintenance information is displayed and configuration settings can easily be set on the Server Info screen. Updates to the system software can be applied automatically.

The following elements are displayed in the Server Info function:

Version Number

Shows the version number of the sytem software and the hotfix level of your system. To check to see if a new update exists for the Kaseya Server Service, press **CHECK FOR UPDATE**. The server will check the Master Server to see if a new update exists; if an update exists, a message will alert the administrator that an update is currently available and will be applied at the next master administrator login. An update is only downloaded if the version currently running is older than the version available. Otherwise, no action is performed.

Pressing **RE-APPLY DATABASE** reinstalls the last database schema that was downloaded using the **CHECK FOR UPDATE** feature.

Warn if the VSA cannot get updates from update.kaseya.net on port 5721

Your VSA connects back to update.kaseya.net to fetch the latest Hotfix Checker list, the latest PCI ID list used by audit, and VSA software update notifications. Your VSA attempts to automatically fetch this information from update.kaseya.net on port 5721. Please verify that **port 5721 outbound** is not blocked by your firewall.

Manually apply hotfixes here

Kaseya frequently posts hotfixes to correct small problems in the latest release. Each KServer connects back to http://vsaupdate.kaseya.net **once every day** to check for new hotfixes. The KServer automatically downloads and applies hotfixes without any user interaction.

If your system is not connecting to the internet or can not reach http://vsaupdate.kaseya.net, then click this list.

- **Check Now** - Forces the system to check for new hotfixes now. If any new hotfixes are available, they are downloaded and automatically applied. Only new hotfixes get loaded.
- **Reload** - Re-downloads and applies all hotfixes for this system version.

The hotfix mechanism addresses minor issues only. Typically either cosmetic typos, or ASP page errors. The KServer, Agents, or database schema are never updated via hotfix. Any changes effecting system operation go into full product updates that you can approve or not. Hotfixs just correct minor issues without having to wait for the release cycle.

Warn when the VSA license reaches the maximum number of seats

Check this box to display a warning when the number of machine accounts reaches the maximum for your VSA.

NOTE: Each installed agent counts against your license for 30 days. If you uninstall an agent, it will count against your license for 30 more days.

Specify VSA Alert Email Address

Specifies the "From:" email address used in the Alerts function of the System feature tab. The email address entered must contain a resolvable domain name that supports SMTP. Press **SET EMAIL** to apply the email address entered. Verify the VSA can send email from this address by pressing the **TEST** button and enter an address to send an email to.

Perform database backup and maintenance every X Days @ 2:00 AM

The VSA automatically backups and maintains the MS-SQL database and transaction log for you. Set the frequency of the maintenance here. Backups are scheduled to run at 2:00AM because it may take a while to complete. If your VSA server is shut down at the scheduled backup time, the backup will occur the next time the VSA goes online.

Backup folder on DB server

Set a path to a directory to store database backups in. Backup database files are typically stored in C:\Kaseya\UserProfiles\@dbBackup.

Change DB

Connect your server to a database on a different machine by following these steps:

1. Backup your existing database by clicking Backup Now.
2. Copy the database backup file to the server running the database you wish to connect to.
3. Verify you new database is set to **mixed mode authentication**.
    1. Open the SQL Enterprise Manager
    2. Right click the database and select properties
    3. Click the Security tab
    4. Under authentication, select **SQL Server and Windows**
    5. Click OK
4. Verify your server is on the same LAN as your new database server and port 1433 is open on the database server.
5. Click the **Change DB** button.
6. Enter the database location using one of the following formats:
    1. computer name
    2. computer name\instance name
    3. IP address
7. Enter a database login name. (Default login name is "sa")

8. Enter the password associated with this login name.
9. Click the Apply button. The system then connects to the remote database and configures it.
10. Click the restore button to load the data from the back up file you made in step one into your new database.

Note: This login is only used to configure the database. The system creates its own database login to use going forward.

Backup Now

Initiate a full database backup now. Use this function when you plan to shut down or move your VSA server in order to always have the latest VSA data saved to a backup. The backup will be scheduled to run within the next 2 minutes.

Restore

Restores the VSA's database from a backup file. Clicking restore displays a list of VSA database backup files the VSA can see (a browse button is also available to locate files stored elsewhere).

Service Status

Shows the current status of the System Server Service (**Running** or **Stopped**). The Service can be stopped by pressing **STOP SERVICE**.

View Log

Displays the last 200 kbytes of the KServer's log file. The entire log file is up to 5 Mbytes in size and is located in at xx\KServer\KServer.log where xx is the parent directory of the VSA web directory.

Select time format

Click the appropriate radio button to select am/pm time display (the default) or 24-hour time display.

am/pm format looks like this -> 9:55:50 pm 9-Apr-05

24-hour format looks like this -> 21:55:50 9-Apr-05

Note: both these display formats are compatible with Microsoft Excel

Change external name/IP address of System Server

Shows the current external name or IP address of the System Server. This is the address client machines access for check-in purposes. The address can be changed by inputting a new address or host name in the field and pressing **CHANGE NAME/IP**.

Change System Server Port

Specify a port used by the Agents to check into the KServer on. Clicking the **CHANGE PORT** button switches the port the KServer listens for agent check-ins on immediately. Before you change the server port be sure that all the agents are listening for this port as their primary or secondary KServer. Configure the Agents with the Check-in Control under the **Agent** tab.

License Code

Shows the current license code of the System and its current expiration date. If a new code is obtained, enter the new code and press **UPDATE CODE**. The terms of the license agreement can be read by pressing **SHOW LICENSE**.

Update Code

Press this button to enter a new product license code.

Subscription Expiration Date

Shows the current expiration date of the system running with the current license code.

Release Notes

Pressing **RELEASE NOTES** opens up a new browser window that lists the changes and enhancements made in the last version of software released. Changes and enhancements made in previous versions of VSA are also listed.

Number of Machines Under Management

Shows the number of machines that the server is currently managing.

Max Number of Machines Supported

Shows the number of machines that the server is capable of administering with the current license code.

System > System Log

Logs events occurring throughout the system, that can not be tracked by machine ID, for a period of 60 days. This log captures events not contained in any of the agent logs. Examples include:

- Deleting machine IDs
- Failed and successful login attemps
- Video streaming sessions
- Starting/stopping of the KServer
- Deleting trouble tickets assigned to a group (not a machine)
- Scheduling reports

Select Page

The system displays all log entries in a time ordered list. The Rows control determines the number of rows displayed on each page. Click << or >> to move to the previous or next page of data. Select the timestamp of the first row of a page from the drop down control to quickly get to a point in time you may be interested in.

Search

The search function acts as a filter on the **Description** field. Enter a set of words to search for and click the Search button. Only rows matching the search criteria are listed.

Note: This function may only be viewed by a Master Administrator.

Note: This log data does not appear in any reports. Reports are only available for data associated with a machine ID.

System > Statistics

The Statistics function displays various statistics to provide an indication that the server running the Service is running optimally.

The following elements are displayed in the Statistics function:

Agents currently online

Number of agents currently checking into the system

Total Machine IDs

Number of machine IDs on the system, whether they have ever checked in or not.

KServer CPU usage

over the last 5 minutes: x%

long term average: x%

Total System CPU usage

over the last 5 minutes: x%

long term average: x%

Remote Control Sessions

The number of remote control sessions relayed through the KServer that are currently active.

Pending Alerts

Alerts are processed by the background task every two minutes. This number shows how many alerts are backed up waiting to be processed by your system. If more than 0 alerts are pending, a button appears labeled Clear Alerts appears. Click this button to clear out all pending alerts.

Database Size

Total size of your database. Typical systems consume about 1 to 2 MB of database size per machine ID.

Database File Location

Full path to the database on the database server machine.

Kaseya File Location

Full path on the Kaseya server to the location of it system files.

Statistics Collected

- **Full checkins completed per min**

  This number indicates the number of managed machines that have completed a full checkin in the last minute from the time specified.
- **Quick checkins completed per min**

  This number indicates the number of managed machines that have completed a quick checkin in the last minute from the time specified.
- **Current active connections**

  This number indicates the number of managed machines that have active connections to the KServer at the time specified.
- **Seconds paused**

  This number indicates the number of seconds that the KServer has paused in the last minute from the time specified. The KServer pauses whenever it detects that the CPU usage been excessively high over a period of time. The KServer attempts to minimize its contributions to the CPU load while the total system CPU usage is high.
- **Database CPU utilization**

  This number indicates the percentage of CPU utilization by the database server at the time specified. Excessively high values for prolonged periods may be an indication that this server is underpowered or could benefit from additional RAM.
- **Total connections processed since KServer start**

  This number indicates the total Agent connections processed by the KServer since the service last started.
- **Total thread failures since KServer start**

  This number indicates the total Agent connections that were discarded by the KServer since the service last started. If Agent connections cannot be handled, then this may be an indication that this server is underpowered or could benefit from additional RAM.

Top scripts run in the last hour

This table lists the scripts that have run and completed execution in the last hour. This table provides the administrator an indication of what tasks the machines have executed recently.

Top scripts pending (online machines only)

List the scripts waiting to execute on any online machines. Displayed with the script past due to execute on the most machines first.

System > Login Policy

What is the login policy used for?

The main purpose of the Login Policy function is to prevent a brute force break-in to the system. By limiting the successive number of bad login attempts and disabling rogue accounts for a set amount of time, you can prevent unauthorized users from gaining entry into the system by repeatedly entering random passwords.

How do I set a login policy?

To set the login policy:

1. Specify the number of consecutive bad logins an administrator is allowed before their account is disabled in the **Number of consecutive failed login attempts allowed before disabling** account field. The count is reset to zero after a successful login.
2. Specify the amount of time, in hours or days, that the account is disabled in the **Length of time to disable account after max login failures exceeded** field.
3. Specify the time period of administrator inactivity before the administrator is automatically logged out. Set the number of minutes of inactivity in the **Minutes of inactivity before an administrator session expires** field.
4. Press **Update** to apply the settings.

Note: To activate the account manually before the lockout time elapses, another master administrator must enable the account in the Enable/Disable function of the System feature tab.

System > Customize

How do I customize the home page first seen by administrators?

How do I customize the home page first seen by users?

Customize the entire system interface

How do I create new agent icons?

How do I upload my custom Agent icons into the Kaseya server to deploy to my managed machines?

I created custom agent icons and deployed a new Agent installation, but my icons are not showing up in the system tray of the managed machine. How do I proceed?

When will my custom icons be deployed?

How do I update existing Agents with my new custom agent icons?

How do I customize the home page first seen by administrators?

To customize the Function List on the home page first seen by administrators:

1. Click on the link **Customize** the function list first seen by **administrators** after logon. A customization web page will open in a new browser window.
2. Click the **Category** button at the bottom of the page to create a new category label in the Function List. This change is applied immediately.
3. Click the **Link** button at the bottom of the page to create a new link in the Function List. This change is applied immediately.
4. Click the delete icon to remove a category label or link from the Function List. This change is applied immediately.
5. Click the up and down arrow icons to move a category label or link up or down in the Function List. This change is applied immediately.
6. In the left text box of each row, enter the name of the category label or link to be shown in the Function List.
7. In the right text box of each row, enter the URL to direct the browser when the link is selected from the Function List.
8. Click the **Update** button at the top of the page to apply the text settings.
9. Click the **Default** button at the top of the page restore the default settings for the home page seen by administrators. This change is applied immediately.
10. Click the **Close** link at the top of the page to exit the customization web page.

How do I customize the home page first seen by users?

To customize the Function List on the home page first seen by users:

1. Click on the link **Customize** the function list first seen by **users** after logon. A customization web page will open in a new browser window.
2. Enter the URL to place in the top most frame of the web page in the **URL of top frame** field.
3. Click the **Category** button at the bottom of the page to create a new category label in the Function List. This change is applied immediately.
4. Click the **Link** button at the bottom of the page to create a new link in the Function List. This change is applied immediately.
5. Click the delete icon to remove a category label or link from the Function List. This change is applied immediately.
6. Click the up and down arrow icons to move a category label or link up or down in the Function List. This change is applied immediately.
7. In the left text box of each row, enter the name of the category label or link to be shown in the Function List.
8. In the right text box of each row, enter the URL to direct the browser when the link is selected from the Function List.
9. Enter the height in pixels of the top most frame of the web page in the **Top frame height** field.
10. Enter the text first shown to users on the web page in the **Default text displayed on the user welcome page** text box.
11. Click the **Update** button to apply the text settings.
12. Click the **Default** button to restore the default settings home page first seen by users. The default setting will remove all additional categories and links.
13. Click the **Close** link at the top of the page to exit the customization web page.

Note: The header on this page is used for both the administrator and user logon page.

Customize the entire system interface

Click Customize the Kaseya graphical user interface to change the entire look of all the web pages. In addition to changing the color scheme, you have full ability to customize the top frame of the interface. You can also swap out the Kaseya agent icon displayed in the system tray of each managed machine with your own icon.

Note: Full customization is only available in the Enterprise Edition.

How do I create new agent icons?

You must create four icons in the Windows icon format to incorporate your brand into the Agent icon shown in the system tray of each managed client machine. These four icons must be named:

- · online.ico – The blue K icon displayed when Agent is connected to the Server
- · offline.ico – The gray K icon displayed when Agent is not connected to the Server
- · blink.ico – The white K icon displayed when Agent requires the user to click the icon to display a message that has been received through the Send Message command found under the Remote Control tab.
- · noremote.ico – The red K icon displayed when the user has selected the “Disable remote control” menu item from the Agent popup menu

To create an icon in the Windows format, use an editor such as one in the Microsoft Visual Studio development environment. Use the following steps create your own Agent icons:

1. Select New… from the File menu in Microsoft Visual Studio
2. Select the File tab
3. Click the Icon File type in the pane under the File tab
4. Uncheck the Add to Project check box since this new file will be standalone
5. Enter a filename, such as online.ico, and location for the file
6. Click the OK button
7. Edit the standard 32x32 icon device and save it.

Note: Full customization is only available in the Enterprise Edition.

How do I upload my custom Agent icons into the Kaseya server to deploy to my managed machines?

Use the following steps to upload your own Agent icons into the Kaseya server:

1. Click on the System tab
2. Select Login Policy function
3. Click the link labeled “Customize the Kaseya graphical user interface.”
4. In the configuration window that pops up, scroll to the bottom of the page to use the “Browse…” and “Change Image” buttons to select and update the Agent icon images for each of the following items labeled:

a. Agent system tray icon when agent is online (must be .ico format)

b. Agent system tray icon when agent is offline (must be .ico format)

c. Agent system tray icon when agent is blinking (must be .ico format)

d. Agent system tray icon when remote control is disabled (must be .ico format)

The Agent will display the default Kaseya icons if any of the custom icons are omitted.

I created custom agent icons and deployed a new Agent installation, but my icons are not showing up in the system tray of the managed machine. How do I proceed?

The custom icon will fail to load if it is not properly formatted for such reasons as:

- The color depth exceeds 256 colors
- The format is not the Windows icon format (e.g. a simple bitmap file was renamed to .ico extension).
- The size is larger than 32x32 pixels.

When will my custom icons be deployed?

The custom icons are automatically deployed with all new Agent installation packages. If you have an Agent installation package deployed using a domain login script, then you must download and replace the KcsSetup.exe file residing on the domain server.

How do I update existing Agents with my new custom agent icons?

Schedule an Agent update using the Update Agent function under the Agent tab. You will need to check the "Force update" check box to update Agents that are already at the current version.

Explanation of items on this page

The Login Policy function is used to specify the number of bad logins allowed before an account is disabled. Enter the number of failed logins allowed before and administrator account is disabled. Also enter a selected length of time an administrator account is disabled after a preset number of failed logins are exceeded.

The following elements are displayed in the Login Policy function:

Specify the bad login attempt policy

- In the *Number of failed login attempts allowed before disabling account* field, specify the number of failed logins the administrator is allowed before the system disables the account.
- In the *Length of time to disable account after max login failures exceeded* field, specifies how long the administrator account is disabled after the number of bad logins (specified above) have been exceeded.

Minutes of inactivity before an administrator session expires

When you log in the system keeps track of activity from this administrator. After a programmable amount of inactivity, the session expires.

Define navigation links on the home page

- Using the function, *Customize the function list first seen by* ***administrators*** *after logon*, you may edit the home page that is shown when an admin first logs in. You can edit the function list found on the left side of the home page by adding in new category labels and function links. Both labels and URL in each function link may be customized.
- Using the function, *Customize the function list first seen by* ***users*** *after logon*, you may edit the home page that is shown when a user first logs in. You can edit the function list found on the left side of the home page by adding in new category labels and function links. Both labels and URL in each function link may be customized. In addition, the top frame of the home page displayed to users may also be customized.

System > Migrate VSA

Show me an explanation of the items on this page.

How do I copy/move accounts from one server to another?

The Migrate VSA function allows administrators to copy client machine accounts from one server to another. The function is initiated on the target machine (new server) and copies client machine accounts from the old server to the new one. To original account is left on the old server.

Note: The VSA connects directly to the MS-SQL server on the remote VSA. The MS-SQL port on the remote VSA must be open. Microsoft uses **port 1433** as the default for MS-SQL.

To copy client machine accounts, follow these steps from the new server:

1. Enter the IP address or hostname of the source (old) machine in the **Remote Server** field.
2. Enter Master Administrator login name in the **Master Admin** field.
3. Enter the administrator password in the **Password** field.
4. Select the number of client machine accounts and administrators you would like to view after the accounts are obtained from the source server by using the **Rows/Page** dropdown menu. The choices are **10**, **30**, and **100**.
5. Press connect. The **Group ID** list box, **Machine.Group ID** and **Assigned Admin** columns populate with the groups, client machines, and administrators, respectively, from the source server.
6. In the **Group ID** list box, select the group whose client machine accounts you would like to view. The client machine accounts of the group are displayed in the **Settings** column. If *<All Groups>* is displayed, all client machine accounts are displayed in the **Settings** column.
7. In the **Machine.Group ID** column, select the checkboxes next to the client machine accounts you would like to copy to the target server. To select all available client machine accounts, click *Select All*.
8. In the **Assigned Admin** column, select the administrator accounts you would like to copy to the target server. All administrators, master and standard, with an account on the source server are displayed. To select all available administrator accounts, click *Select All*.
9. Select **Overwrite Duplicate Data** if you would like to overwrite the accounts on the target Server with the same client machine accounts and administrators.
10. Select **Copy Public Scripts and Reports** if you would like to import all public scripts and reports from the remote VSA.
11. Press Copy.

After the accounts have been copied from the source Server to the new target Server, they must be edited on the new Server to update the KServer's hostname / IP address.

12. On the new target Server, select the Agent tab.
13. Click on the **Check-In Ctl** function.
14. Enter the hostname or IP address of the new server in the Primary KServer text edit field.
15. Enter the hostname or IP address of the new server in the Secondary KServer text edit field.
16. Select All Groups in the Group ID filter in the Specify Accounts area below the function tabs.
17. Click Select All to check the boxes beside every managed machine.
18. Click the Update button.

Finally, configure the Agents to check in to the new target Server.

19. On the old source Server, select the **Agent tab**.
20. Click on the **Check-In Ctl** function.
21. Enter the hostname or IP address of the new server in the Primary KServer text edit field.
22. Select All Groups in the Group ID filter in the Specify Accounts area below the function tabs.
23. Click Select All to check the boxes beside every managed machine.
24. Click the Update button. Upon the next check in to the old source server, the Agents will receive the new server's address as the primary KServer. Subsequently, the Agent will check in to the new server.

How do I re-install a Kaseya VSA server on another Windows server and maintain all of the existing managed machine data?

The following procedure should be followed when you have installed a Kaseya VSA server on a new Windows server and you wish to copy all of the machine data to the new server. This procedure assumes that the new server will be a replacement for the old server and that it will take the external hostname / IP address of the old server. If your new server will have a different external hostname or IP address, refer to the section below. This procedure may also be used if you are upgrading the operating system or the SQL server on your current server.

1. Log in to your current VSA server as a master administrator.
2. Select the **System tab**.
3. Click on the **Server Info** function.
4. Click the **Backup Now** button. An SQL database backup will run within the next two minutes.
5. To confirm the completion of the database backup, locate the SQL database backup file named *<Kaseya_Installation_Directory>\UserProfiles\@dbBackup\ksubscribers_db_yyyymmddhhmm.BAK*. By default, the *<Kaseya_Installation_Directory>* is **c:\Kaseya\**. The *yyyymmddhhmm* portion of the filename contains the current year, month, day, hour, and minute of the database backup.
6. Copy the entire directory *<Kaseya_Installation_Directory>*\UserProfiles\ to your new server. This directory contains the files associated with your managed machines.
7. With the exception of the subdirectory **VSAHiddenFiles**, copy the entire directory *<Kaseya_Installation_Directory>*\WebPage\ManagedFiles\ to your new server. This directory contains the scripts and managed files belonging to each administrator.

WARNING: Do not copy VSAHiddenFiles from an old system to a new system. This directory contains many system helper files. Your new system installation contains the latest versions of these files.

8. If you are re-installing the operating system or SQL server on this same Windows server, then save the directories in Steps 6 and 7. After re-installing the server and VSA, copy back the two directories.
9. Log in to your new VSA server as a master administrator.
10. Select the **System tab**.
11. Click on the **Server Info** function.
12. Click the **Restore** button.
13. Select the link containing the date of the SQL database backup from the list that matches the backup created in Step 5. Click the **Restore** button to confirm the database restore operation.
14. After the database restore completes, you will have to log back in to the VSA server using one of the original administrator accounts.
15. If necessary, set the external name or IP address of the new server to match the server that you have replaced by selecting the **System tab** and clicking on the **Server Info** function.

What if I am putting the new server at a different IP address or external hostname?

Prior to shutting down the existing VSA server, you will need to configure the Agents to check into the new VSA server's IP address or external hostname if it will be different.

1. Log in to your current VSA server as a master administrator.
2. Select the **Agent tab**.
3. Click on the **Check-In Ctl** function.
4. Enter the hostname or IP address of the new server in the **Primary KServer** text edit field.
5. Enter the hostname or IP address of the current server in the **Secondary KServer** text edit field.
6. Select **All Groups** in the **Group ID** filter in the **Specify Accounts** area below the function tabs.
7. Click **Select All** to check the boxes beside every managed machine.
8. Click the **Update** button.
9. The new settings will appear in red at first. Once an Agent has checked in and received the new setting, it will be displayed in black again. Wait for all machines to check in and receive the updated check in configuration before taking the current server offline.

Explanation of items on this page

Migrate allows administrators to switch servers without the need for downtime. Administrators setup the system on the new server. Then, using the Migrate function from the new server, they connect to the old server and copy over existing client machine accounts and administrator accounts. Since accounts are copied, and not moved, the administrator must manually delete the accounts from the old server. Otherwise, the accounts are left intact. To ensure that the deployed Agents can find the new server, be sure that the host name/IP address settings are correct, as specified in Server Info.

Note: The VSA connects directly to the MS-SQL server on the remote VSA. The MS-SQL port on the remote VSA must be open. Microsoft uses port 1433 as the default for MS-SQL.

The following elements are displayed in the Migrate VSA function:

Remote Server

The fully qualified host name or IP address of the **source** server. This is the server that user accounts will be migrated from.

Master Admin

A Master Administrator login name valid on the remote server.

Password

The Master Administrator password that corresponds with the **Master Admin** field.

Group ID

Shows a list of the group IDs on the remote server. All groups can be selected or multiple groups can be selected by holding down the <CTRL> key while clicking on the group names.

Select/Unselect All

Select All will select all user accounts on all account pages. Unselect All will unselect selected user accounts on all account pages. For individual accounts, select the checkbox next to the machine.group ID.

Connect

Initiates the connection to the server specified in the **Remoter Server** field.

Copy

Starts copying the selected machine accounts from the source server. Hence that it is a copy command; the original accounts are not deleted or moved from the source server.

Overwrite duplicate data

Selecting this checkbox prompts the server to automatically overwrite any duplicate machine accounts on the new server.

Copy Public Scripts and Reports

Selecting this checkbox copies any public scripts and reports from the source server. Otherwise, only private scripts are copied from the remote Server, assuming that the corresponding administrator accounts are also copied.

Settings

Shows the client machines according to the group(s) selected in the **Group ID** list. Check the checkboxes next to the client machine accounts that are to be copied to the new server from the source Server.

Settings and private data

Shows all of the master and standard administrators on the source machine. Private scripts are copied along with the administrator accounts if their corresponding checkbox is selected. Check the checkboxes next to the administrators that are to be copied to the new server from the source Server.

System > Database Views

View Definitions defined here.

The system exposes set of **database views** allowing clients to directly access data within the Kaseya repository. These views can be used by to bring data into a spreadsheet for analysis or to prepare reports. This document describes the views and gives two example applications, Crystal Reporting and Microsoft Excel. Kaseya does not present itself as an expert in how to use Excel or Crystal. These examples are to assist in the basics of getting started. For third party product training or other questions please contact the third party tool vendor. Finally, an appendix is provided with a field-by-field description of the contents of the views.

The views provided can be broken into **three groups**. The first group provides information on all the machines being monitored. The second group provides information about the activity and current status of key parts of the system. The third group provides information on the ticketing system. The views provided are:

Machines Group	
vBaseApplicationInfo	The baseline list of applications on a client desktop machine.
vBaseCpuInfo	The baseline list of the CPUs in a client desktop machine.
vBaseDiskInfo	The baseline list of the disks in a client desktop machine.
vBaseDriveManufacturer	The baseline list of the manufacturers of the disks in a client desktop machine.
vBasePciInfo	The baseline list of the PCI cards in a client desktop machine.
vBasePrinterInfo	The baseline list of printers in a client desktop machine.
vCollectionMember	List the collections each machine ID belongs to (if any)
vCurrApplicationInfo	The current list of applications on a client desktop machine.
vCurrCpuInfo	The current list of the CPUs in a client desktop machine.
vCurrDiskInfo	The current list of the disks in a client desktop machine.
vCurrDriveManufacturer	The current list of the manufacturers of the disks in a client desktop machine.
vCurrPciInfo	The current list of the PCI cards in a client desktop machine.
vCurrPrinterInfo	The current list of printers in a client desktop machine.
vSystemInfo	All items collected by the System Info function under the Audit tab.
VLicenseInfo	The licenses of applications on this machine.
vMachine	The information known about each client desktop machine.
vOnBoardDeviceInfo	The current list of on board devices in a client desktop machine.
vPortInfo	The current list of ports in a client desktop machine.

Activity / Status Group	
vAgentConfiguration	Lists agent specific configuration data
vAdminNotesLog	Notes each admin enters manually for a machine or group of machines. Entries in this log never expire.
vAlertLog	Logs each alert sent out via email. Multiple rows per machine.
vBackupLog	Logs all backup related events
vConfigLog	Log of all configuration changes. One entry per change.
vNetStatsLog	Network statistics log from the Agent.
vNtEventLog	NT Event log data collected from each managed machine.
vPatchStatus	Information on the state of all patches on a per machine basis. There is one row per patch for each machine.
vScriptLog	Log of script executions as viewed by the KServer.
vScriptStatus	Script status for each client.

Ticketing Group	
vTicketSummary	Trouble ticket summary. One row per ticket. Column names are used as the names displayed in the view summary table.
VTicketNote	The notes associated with a ticket. Potentially multiple rows per ticket.
VticketField	The fields associated with a ticket. The standard fields, category, status and

	priority are always attached to a ticket. User fields added will also be included in this view.

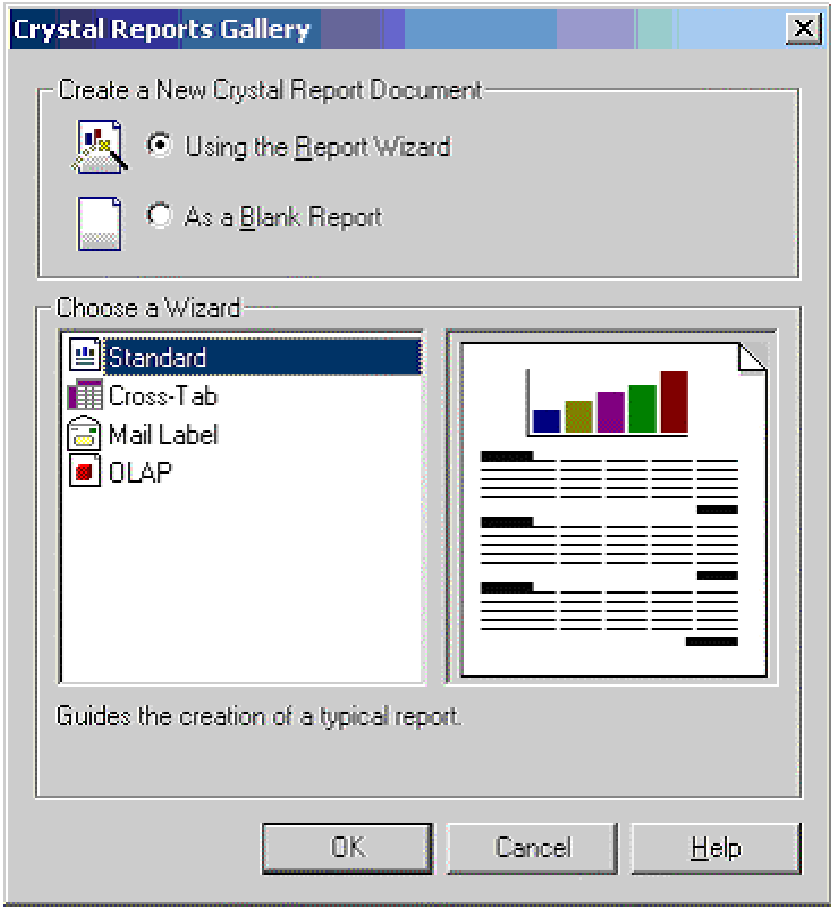
Monitor Alarm Group	
vMonitorAlarmCounter	The current list of alarms for all monitor counters.
vMonitorAlarmService	The current list of alarms for all monitor services.
vMonitorAlarmProcess	The current list of alarms for all monitor processes.
vMonitorAlarmSNMP	The current list of alarms for all monitor SNMP Get objects.
vMonitorAlarmAlert	The current list of alarms for all alerts.
vMonitorAlarmSystemCheck	The current list of alarms for all system checks.

Access to Views

The views are installed whenever the Reapply Schema action is taken. Once this is accomplished the views are ready to be used. A single data user id, **KaseyaViews** will be provided. To give access to these views an administrator needs to go to the system menu. Under the title View Access there is a function to change the password of KaseyaViews. By selecting this option the administrator will be presented with a screen to enter a password. Once this is accomplished, the new views can be accessed using the KaseyaViews user id and the password entered.

Crystal Reporting Usage

Crystal Reporting can be used to create client specified reports. Crystal 9 and 10 can be used to produce various output formats include PDF, Word and Excel. To set up a report the Crystal Report Wizard can be used. This process begins with the following dialog.



Crystal Reports Gallery

Create a New Crystal Report Document

● Using the Report Wizard

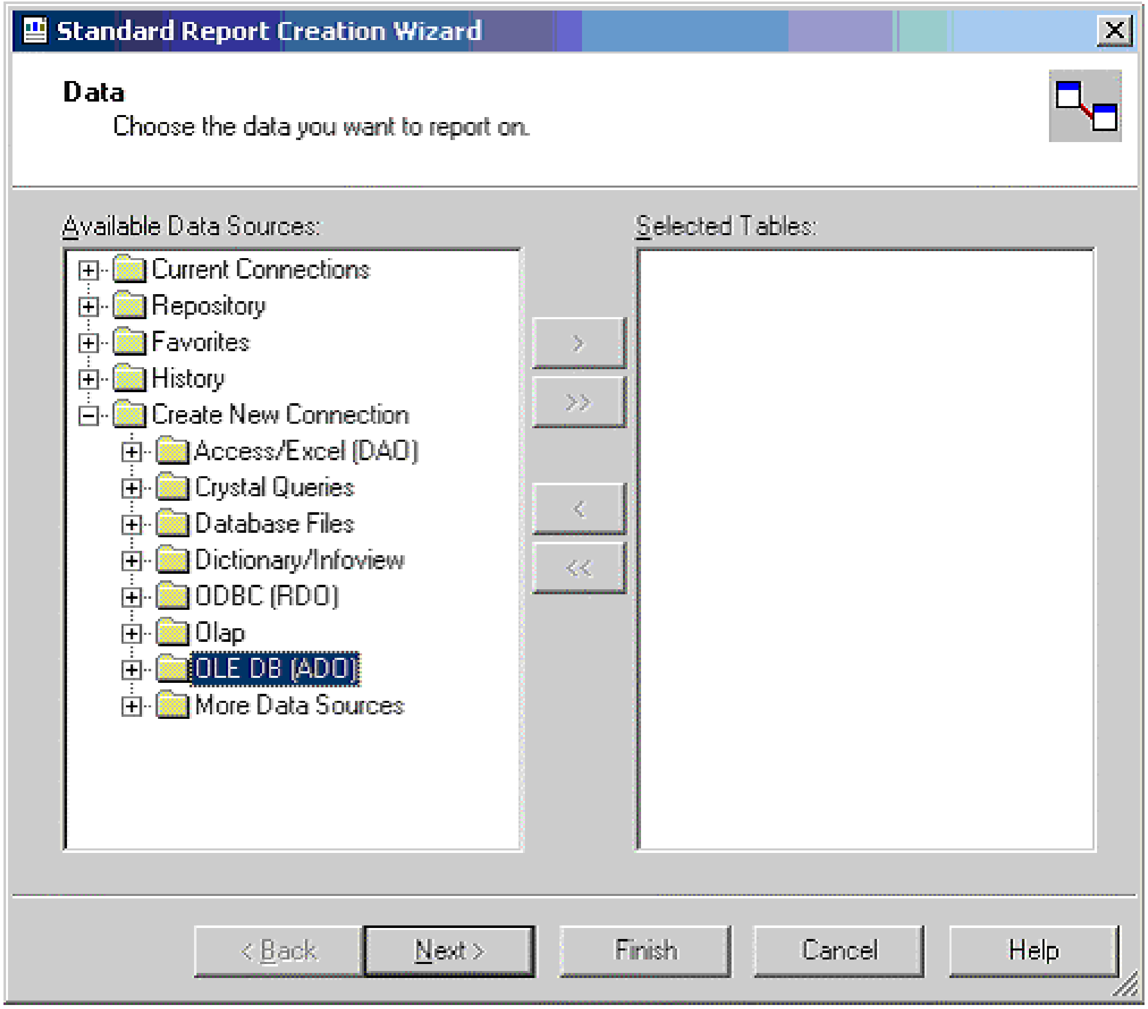
○ As a Blank Report

Choose a Wizard

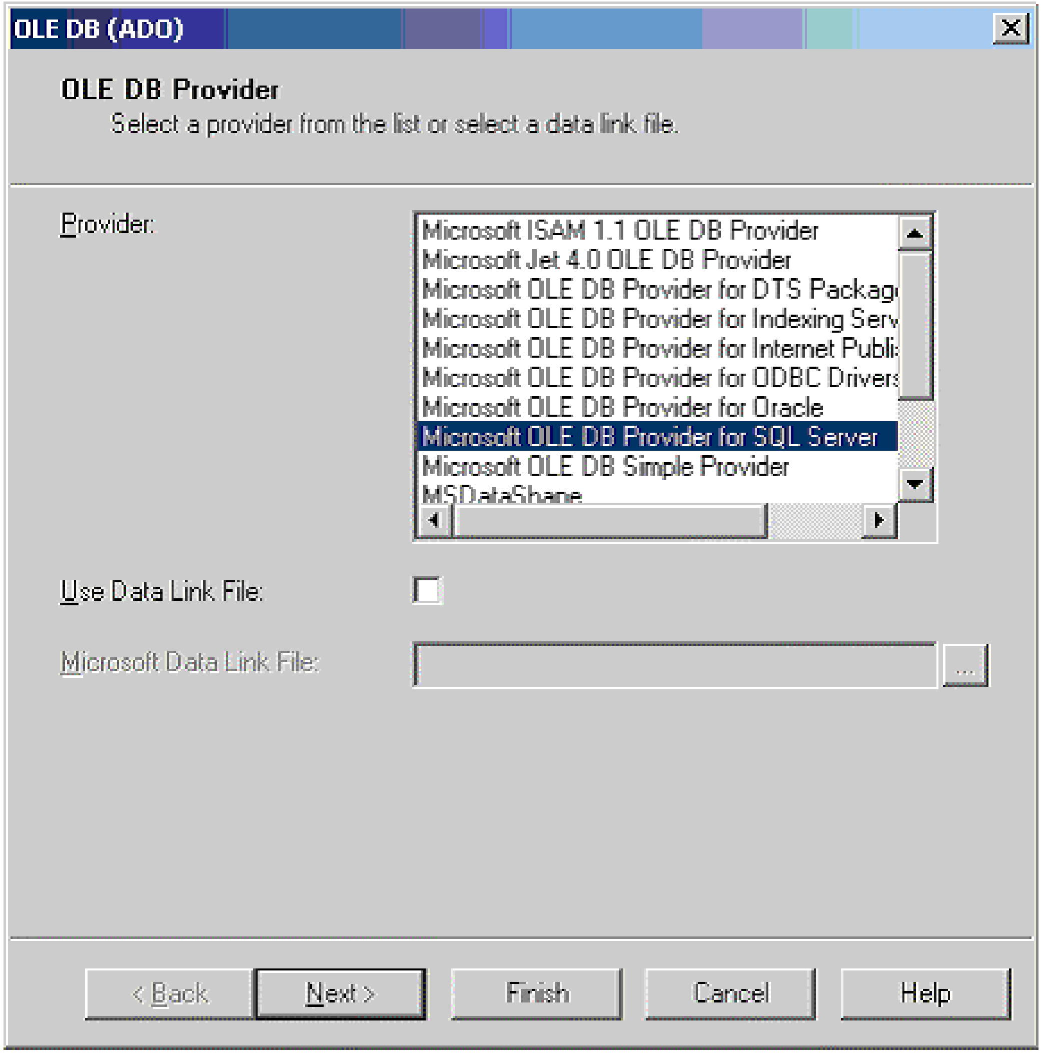
Standard

Guides the creation of a typical report.

The client picks a report format. For this example standard will be used.



Next the data source is selected. This begins by picking an access method. ADO should be selected.



OLE DB (ADO)

OLE DB Provider

Select a provider from the list or select a data link file.

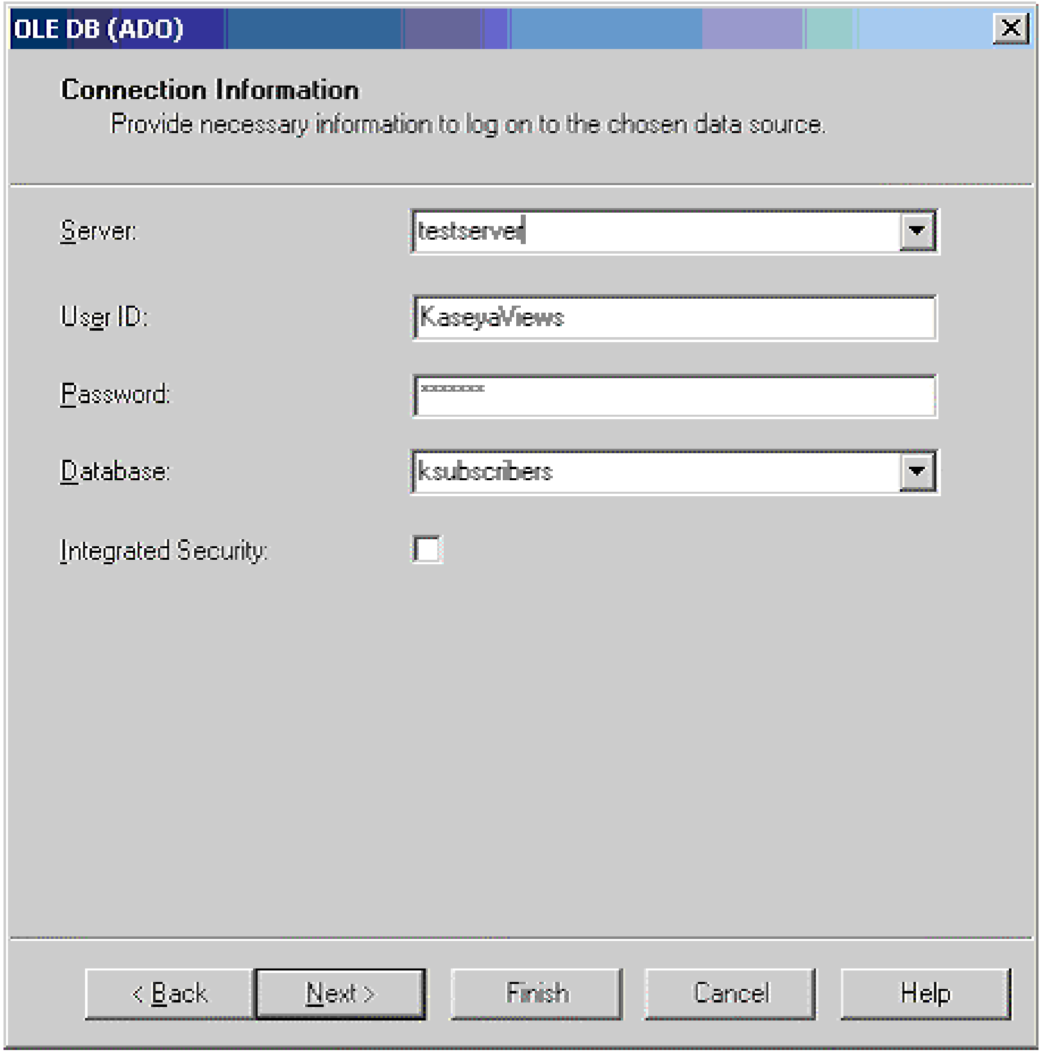
Provider:

- Microsoft ISAM 1.1 OLE DB Provider
- Microsoft Jet 4.0 OLE DB Provider
- Microsoft OLE DB Provider for DTS Packag
- Microsoft OLE DB Provider for Indexing Serv
- Microsoft OLE DB Provider for Internet Publi
- Microsoft OLE DB Provider for ODBC Drivers
- Microsoft OLE DB Provider for Oracle
- Microsoft OLE DB Provider for SQL Server
- Microsoft OLE DB Simple Provider
- MSDataShape

Use Data Link File: □

Microsoft Data Link File:

Once ADO is selected the SQL Server driver can be selected. This is the correct selection to access the Kaseya database.



OLE DB (ADO)

Connection Information

Provide necessary information to log on to the chosen data source.

Server: testserver

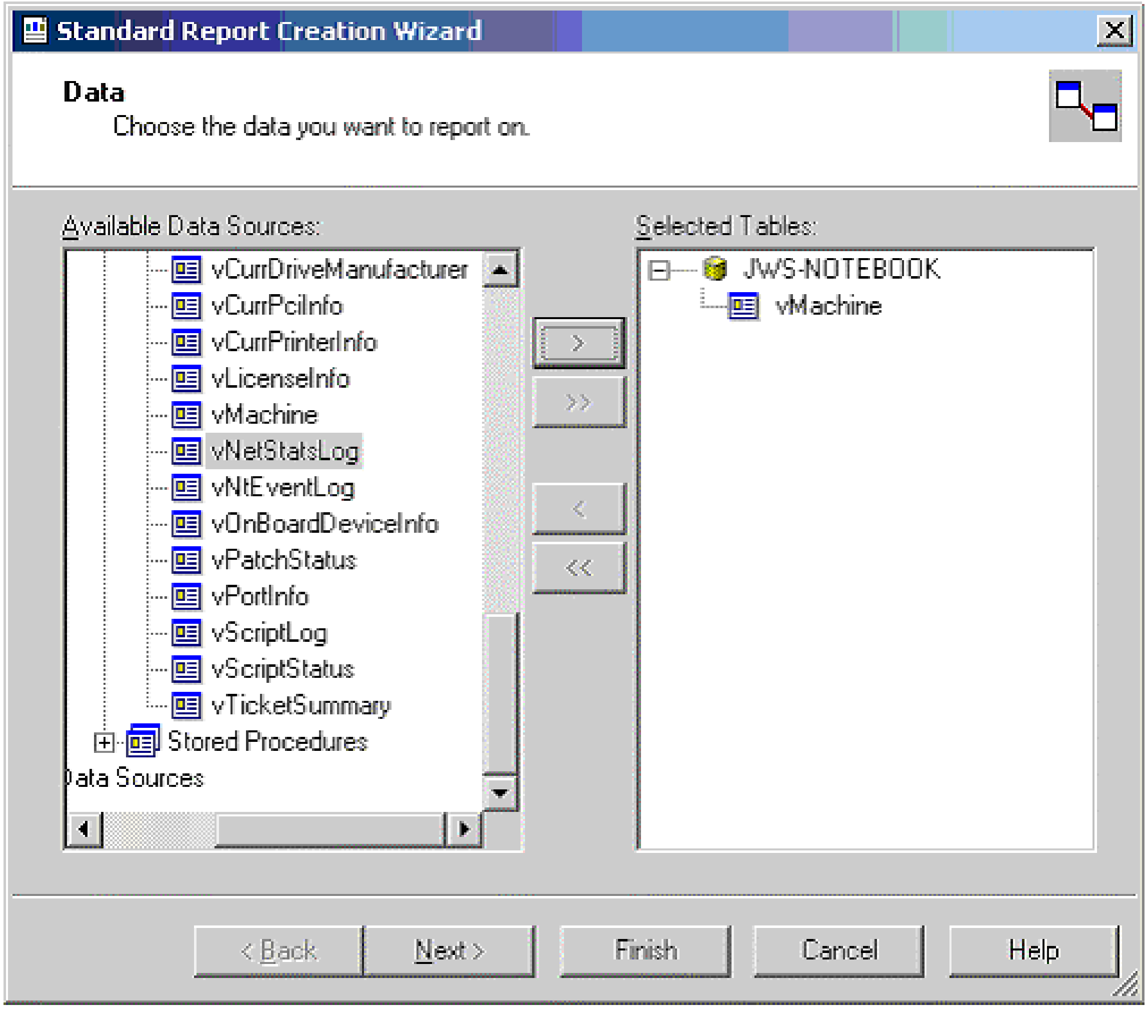
User ID: KaseyaViews

Password: ********

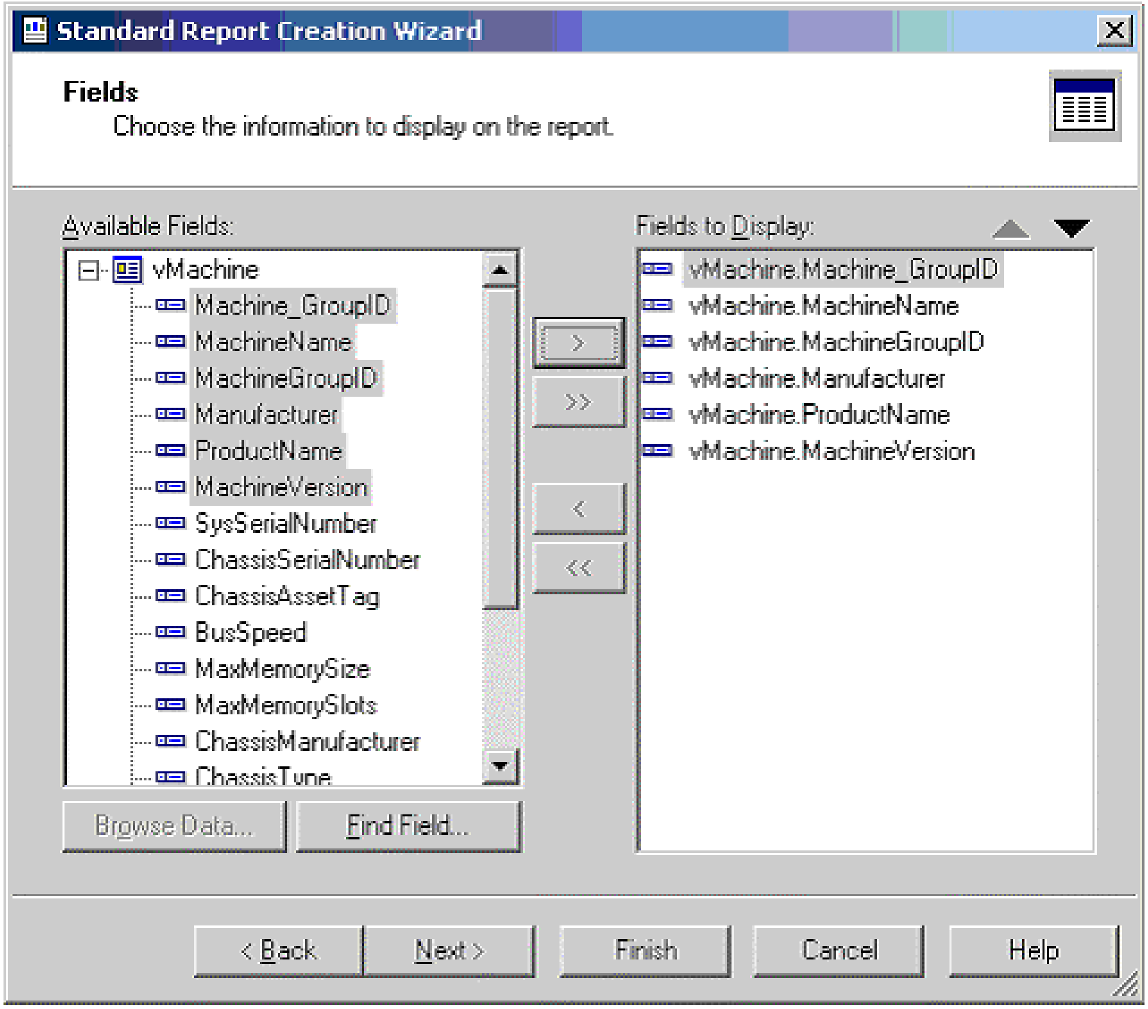
Database: ksubscribers

Integrated Security: □

The next step is providing the credential to make connection to the database. As shown in this dialog, the Server, User Id, Password, and Database must be provided.



Once the credentials are provide all the available views are displayed. Pick one or more for the report desired.



Standard Report Creation Wizard

Fields

Choose the information to display on the report.

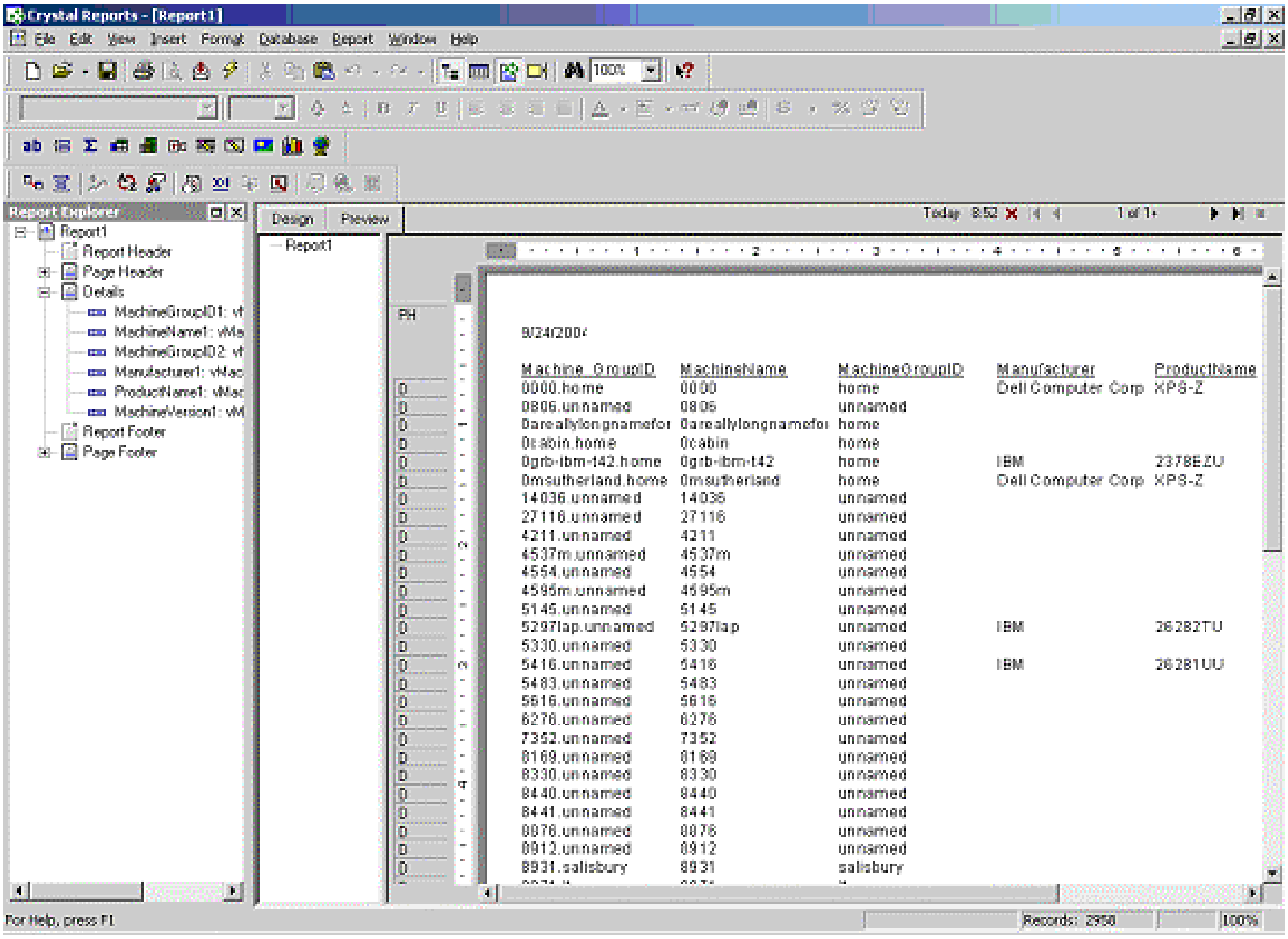
Available Fields:

- vMachine
  - Machine_GroupID
  - MachineName
  - MachineGroupID
  - Manufacturer
  - ProductName
  - MachineVersion
  - SysSerialNumber
  - ChassisSerialNumber
  - ChassisAssetTag
  - BusSpeed
  - MaxMemorySize
  - MaxMemorySlots
  - ChassisManufacturer
  - ChassisType

Fields to Display:

- vMachine.Machine_GroupID
- vMachine.MachineName
- vMachine.MachineGroupID
- vMachine.Manufacturer
- vMachine.ProductName
- vMachine.MachineVersion

After a view is selected the columns to be included can then be selected. Crystal provides a variety of ways to format this data. This document does not attempt to describe these options. The Crystal documentation should be reviewed for this information.



9/24/2004

Machine_GroupID	MachineName	MachineGroupID	Manufacturer	ProductName
0000.home	0000	home	Dell Computer Corp	XPS-Z
0806.unnamed	0806	unnamed		
0areallylongnamefor	0areallylongnamefor	home		
0cabin.home	0cabin	home		
0grb-ibm-t42.home	0grb-ibm-t42	home	IBM	2378EZU
0msutherland.home	0msutherland	home	Dell Computer Corp	XPS-Z
14036.unnamed	14036	unnamed		
27116.unnamed	27116	unnamed		
4211.unnamed	4211	unnamed		
4537m.unnamed	4537m	unnamed		
4554.unnamed	4554	unnamed		
4595m.unnamed	4595m	unnamed		
5145.unnamed	5145	unnamed		
5297lap.unnamed	5297lap	unnamed	IBM	26282TU
5330.unnamed	5330	unnamed		
5416.unnamed	5416	unnamed	IBM	26281UU
5483.unnamed	5483	unnamed		
5616.unnamed	5616	unnamed		
6276.unnamed	6276	unnamed		
7352.unnamed	7352	unnamed		
8169.unnamed	8169	unnamed		
8330.unnamed	8330	unnamed		
8440.unnamed	8440	unnamed		
8441.unnamed	8441	unnamed		
8876.unnamed	8876	unnamed		
8912.unnamed	8912	unnamed		
8931.salisbury	8931	salisbury		

The resulting report can be printed or emailed to the appropriate consumers of the report. The format of the report can be designated. This facility can be used to produce a PDF or a variety of other formats.

Excel Usage

Microsoft Excel can access the views by setting up a data source. Selecting the Settings option from the Start button allows the creation a data source. From the Settings option select the Control Panel. From the Control Panel next select Administrative Tools. From this menu a data source can be created.

The data source should be set up as a System DSN. From this dialog, create a source using the SQL Server driver. The set-up will require the name of the database server (usually the ComputerName), the user id (KaseyaViews) and password, and the database schema name (ksubscribers).

Once a data source is created it can be referenced by Excel. Selecting Get External Data from the Data menu does this. A new database query can be started from this selection. The user is prompted for the credentials to the database. Once this completes a view can be selected. A SQL query can be constructed to bring information directly into Excel at this point.

A data source is a core definition within Microsoft. Most Microsoft products have facilities to access data through a data source definition.

MSDE/SQL Server Variations

If you are using MSDE/SQL Server rather than the full SQL Server, there are a few minor variations to the steps listed above.

1. The SQL server name will always be [ComputerName]\KVSAMSDE.
2. Always set the authentication using a login ID and password. This will be KaseyaViews with the password you have defined.

View Definitions

vAdminNotesLog	Notes each admin enters manually for a machine or group of machines. Entries in this log never expire.	
Column Name	**Type**	**Purpose**
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
AdminAdmin	varchar	Admin logon name. (note: no not name this col adminName)
EventTime	datetime	Time stamp string representing the time the action took place. Default is CURRENT_TIMESTAMP so nothing needs to be entered here.
NoteDesc	varchar	description of the action

vAgentConfiguration	Logs each alert sent out via email. Multiple rows per machine	
Column Name	**Type**	**Purpose**
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
firstCheckin	datetime	timestamp recording the first time this agent checked into the system
lastCheckin	datetime	timestamp recording the most recent time this agent checked into the system
currentUser	varchar	login name of the currently logged in user. Blank if no one logged in at this time
lastLoginName	varchar	login name of the last user to log into this system
lastReboot	datetime	timestamp when this system was last rebooted
agentVersion	int	version number of agent installed on this system
contactName	varchar	User contact name assigned to this agent
contactEmail	varchar	User email address assigned to this agent
contactPhone	varchar	Contact phone number assigned to this agent
contactNotes	varchar	Notes associated with the contact information for this agent
enableTickets	int	0 if this user does not have access to ticketing through the user interface
enableRemoteControl	int	0 if this user does not have access to remote control through the user interface
enableChat	int	0 if this user does not have access to chat through the user interface
loginName	varchar	Login Name assigned to this user (if any) to access the system user portal interface.
credentialName	varchar	The username of the credential set for this agent (if any)
primaryKServer	varchar	address:port agent connects to for its primary kserver connection
secondaryKServer	varchar	address:port agent connects to for its secondary kserver connection
agentTempDir	varchar	The temp directory used by the agent on this system

vAlertLog	Logs each alert sent out via email. Multiple rows per machine	
Column Name	**Type**	**Purpose**
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
EventTime	datetime	time stamp when the event was recorded
AlertEmail	varchar	email address to send the alert to
AlertType	int	1 -> Admin account disabled 2 -> Get File change alert 3 -> New Agent checked in for the first time 4 -> Application has been installed or deleted 5 -> Script failure detected 6 -> NT Event Log error detected 7 -> KServer stopped

		8 -> Protection violation detected. 9 -> PCI configuration has been changed 10 -> Disk drive configuration change 11 -> RAM size changed. 12 -> Test email sent by serverInfo.asp 13 -> Scheduled report completed 14 -> LAN Watch alert type 15 -> agent offline 16 -> low on disk space 17 -> disabled remote control 18 -> agent online 19 -> new patch found 20 -> patch path missing 21 -> patch install failed 23 -> Backup Alert
EmailSubject	varchar	Email subject line
EmailBody	varchar	Email body

vBackupLog	Logs each alert sent out via email. Multiple rows per machine	
Column Name	**Type**	**Purpose**
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
EventTime	datetime	time stamp when the event was recorded
description	varchar	description of the reported task
durationSec	int	number of seconds the reported task took to complete
statusType	int	0: full backup 1: offsite replication 2: incremental backup 3: offsite replication suspended 4: offsite replication skipped because backup failed 5: folder backup 6: offsite folder suspended
result	int	0: failure 1: success 2: archive incomplete

vBaseApplicationInfo **vCurrApplicationInfo**	audit results for installed applications. One entry per installed application found in the registry key HKEY_LOCAL_MACHINE\Software\Microsoft\ Windows\CurrentVersion\App Paths.	
Column Name	**Type**	**Purpose**
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
ProductName	varchar	Product name (e.g. Microsoft Office 2000)
ProductVersion	varchar	Version (e.g. 9.0.3822)
ApplicationName	varchar	Application name (e.g. Winword.exe)
Manufacturer	varchar	Manufacturers name (e.g. Microsoft Corporation)
ApplicationDesc	varchar	Description (e.g. Microsoft Word for Windows)
LastModifiedDate	varchar	File date (e.g. 02/24/2000 17:23:44)
ApplicationSize	varchar	File size in bytes (e.g. 8810548)
DirectoryPath	varchar	Directory path on client desktop (e.g. C:\PROGRA~1\MICROS~4\OFFICE)

vBaseCPUInfo **vCurrCPUInfo**	audit results for the CPU in a client desktop machine. One entry per audit of a client desktop.	
Column Name	**Type**	**Purpose**
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
CpuDesc	varchar	CPU description (e.g. Pentium III Model 8)
CpuSpeed	varchar	CPU speed in MHz (e.g. 601)
CpuCount	varchar	Number of processors (e.g. 1)
TotalRam	varchar	Amount of RAM in MBytes (e.g. 250)

vBaseDiskInfo **vCurrDiskInfo**	audit results for the logical disks found in a client desktop machine. One entry per logical disk from an audit of a client desktop.	
Column Name	**Type**	**Purpose**
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
DriveLetter	varchar	Logical disk drive letter (e.g. C)
TotalSpace	varchar	Total MBytes on the disk (e.g. 28609 for 28.609 GB) May be null if unavailable.
UsedSpace	varchar	Number of MBytes used (e.g. 21406 for 21.406 GB). May be null if unavailable.
FreeSpace	varchar	Number of MBytes free (e.g. 21406 for 21.406 GB). May be null if unavailable.
DriveType	varchar	Fixed = hard diskRemovable = floppy or other removable mediaCDROMNetwork = mapped network drive
VolumeName	varchar	Name assigned to the volume
FormatType	varchar	NTFS, FAT32, CDFS, etc.

vBaseDriveManufacturer **vCurrDriveManufacturer**	Hardware audit results for the IDE & SCSI drives manufacturer and product info found in a client desktop machine. One entry per drive from an audit of a client desktop.	
Column Name	**Type**	**Purpose**
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
DriveManufacturer	varchar	Manufacturer name (data currently has 8 characters max)
DriveProductName	varchar	Product identification (data currently has 16 characters max)
DriveProductRevision	varchar	Product revision (data currently has 4 characters max)
DriveType	varchar	Type of disk drive found

vBasePciInfo **vCurrPciInfo**	Hardware audit results for the PCI cards manufacturer and product info found in a client desktop machine. One entry per PCI card from an audit of a client desktop.	
Column Name	**Type**	**Purpose**
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
VendorName	int	PCI Vendor Name

ProductName	int	PCI Product Name
ProductRevision	int	Product revision
PciBaseClass	int	PCI base class number
PciSubclass	int	PCI subclass number
PciBusNumber	int	PCI bus number
PciSlotNumber	int	PCI slot number

vBasePrinterInfo **vCurrPrinterInfo**	Printer audit results for the printers found for the current user logged on to a client desktop machine. One entry per printer from an audit of a client desktop. If no user is logged in, then Agent audits the printers for the system account, typically administrator.	
Column Name	**Type**	**Purpose**
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
PrinterName	varchar	Name given to the printer. Same as shown in the Control Panels printer configuration window.
PortName	varchar	Name of the port to which the printer is attached. Same as shown in the Control Panels printer configuration window.
PrinterModel	varchar	Model name is the driver name retrieved from the printer information.

vCollectionMember	Lists all collections each machine ID is a member of (if any).	
Column Name	**Type**	**Purpose**
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
collectionName	varchar	Collection Name

vConfigLog	Log of all configuration changes. One entry per change.	
Column Name	**Type**	**Purpose**
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
EventTime	datetime	Time stamp string representing the time the change was entered. (note: timestamp type was picked to force times into the database as year-month-day-hr-min-sec all in numeric format independent of the format sent in the SQL command. This allows records to be easily sorted by time during retrieval.)
ConfigDesc	varchar	Description of the change

vSystemInfo	Data collected by System Info function	
Column Name	**Type**	**Purpose**
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
Manufacturer	varchar	System manufacturer string
Product Name	varchar	Name or model number of the machine supplied by the manufacturer
System Version	varchar	Machine version string
System Serial Number	varchar	Machine serial number string entered by the manufacturer
Chassis Serial Number	varchar	Serial number string supplied by the manufacturer

Chassis Asset Tag	varchar	Asset tag string supplied by the manufacturer
External Bus Speed	varchar	Motherboard bus speed
Max Memory Size	varchar	Max memory this system may be configured with
Max Memory Slots	varchar	Max number of memory slots this system has
Chassis Manufacturer	varchar	Name of manufacturer of the chassis
Chassis Type	varchar	system chassis type
Chassis Version	varchar	version string of the chassis
Motherboard Manufacturer	varchar	Name of motherboard manufacturer
Motherboard Product	varchar	Motherboard model name
Processor Family	varchar	processor family name
Processor Manufacturer	varchar	processor manufacturer name
Processor Version	varchar	processor version string
CPU Max Speed	varchar	max speed of this processor
CPU Current Speed	varchar	configured speed of this processor
Custom Fields	varchar	Additional columns for each customer field created.

vLicenseInfo	License information collected during audit.	
Column Name	**Type**	**Purpose**
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
Publisher	varchar	software publisher (usually in the Publisher reg value)
ProductName	varchar	Software title (usually in DisplayName value but may be the reg key title)
LicenseCode	varchar	License code (usually in the ProductID value)
LicenseVersion	varchar	version string returned by the scanner (if any)
InstallDate	varchar	install date string returned by the scanner (if any)

vMachine	The information known about each client desktop machine.	
Column Name	**Type**	**Purpose**
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	full machine name. Everything to the left of the left most decimal point is the machine name.
groupName	varchar	full group name for this account. Everything to the right of the left most decimal point is the group name.
Manufacturer	varchar	Manufacturer string (type 1)
ProductName	varchar	Product Name string (type 1)
MachineVersion	varchar	Version string (type 1)
SysSerialNumber	varchar	Serial Number string (type 1)
ChassisSerialNum	varchar	Chassis Serial Number (type 3)
ChassisAssetTag	varchar	Chassis Asset Tag number (type 3)
BusSpeed	varchar	External Bus Speed (in MHz) (type 4)
MaxMemorySize	varchar	Maximum Memory Module Size (in MB) (type 16 - Maximum Capacity or if type 16 not available, Maximum Memory Module Size type 5)
MaxMemorySlots	varchar	Number of Associated Memory Slots (Number of Memory Devices in type 16 or if type 16 not available Number of Associated Memory Slots in type 5)
ChassisManufacturer	varchar	Chassis Manufacturer (type 3)
ChassisType	varchar	Chassis Type (type 3)
ChassisVersion	varchar	Chassis Ver (type 3)
MotherboardManfacture	varchar	Motherboard Manufacturer (type 2)

r		
MotherboardProductCode	varchar	Motherboard Product Code (type 2)
MotherboardVersion	varchar	Motherboard Version (type 2)
MotherboardSerialNumber	varchar	Motherboard Serial Number (type 2)
ComputerName	varchar	Name of the Computer
IpAddress	varchar	IP Address of the computer in a.b.c.d notation
SubnetMask	varchar	Subnet mask in a.b.c.d notation. String is empty if data is unavailable
DefaultGateway	varchar	Default gateway IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer1	varchar	DNS server #1s IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer2	varchar	DNS server #2s IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer3	varchar	DNS server #3s IP address in a.b.c.d notation. String is empty if data is unavailable.
DnsServer4	varchar	DNS server #4s IP address in a.b.c.d notation. String is empty if data is unavailable.
DhcpEnable	int	0 -> Data is unavailable 1 -> DHCP on client computer is enabled 2 -> Disabled
DhcpServer	varchar	DHCP servers IP address in a.b.c.d notation. String is empty if data is unavailable.
WinsServer	int	0 -> Data is unavailable 1 -> WINS resolution on client computer is enabled 2 -> Disabled
PrimaryWinsServer	varchar	Primary WINS servers IP address in a.b.c.d notation. String is empty if unavailable.
SecondaryWinsServer	varchar	Secondary WINS servers IP address in a.b.c.d notation. String is empty if unavailable.
ConnectionGatewayIp	varchar	IP Address in a.b.c.d notation obtained by the Kserver as the source address of the Agent. This IP is the Agents network gateway and will be different from the IpAddress if the computer is behind NAT for example. String is empty if unavailable.
OsType	varchar	String contains OS type, such as 95, 98, NT4, 2000, NT3.51, or WIN32s. Derived from portions of MajorVersion, MinorVersion, and PlatformId.
OsInfo	varchar	String contains additional OS info, such as Build 1381 Service Pack 3. Derived from portions of BuildNumber and CsdVersion.
MajorVersion	varchar	Major version number from GetVersionEx() Windows function call.
MinorVersion	varchar	Minor version number from GetVersionEx() Windows function call.If PlatformId is Win32 for Windows, then a 0 MinorVersion indicates Windows 95. If PlatformId is Win32 for Windows, then then a MinorVersion > 0 indicates Windows 98.
BuildNumber	int	Build number from GetVersionEx() Windows function call.For NT or 2000, this value is the build numberFor 95 or 98, the high order word contains the major / minor version and the low order word contains the build number.
PlatformId	int	Platform ID from GetVersionEx() Windows function call. 0 -> Win32s 1 -> Win32 on Windows 2 -> Win32 on NT
CsdVersion	varchar	String from GetVersionEx() Windows function call containing additional OS info, such as Service Pack number and other arbitrary data.
MacAddr	varchar	String containing the physical address, i.e. the Media Access Control address, of the connection. A MAC address has the form of: 00-03-47-12-65-77

LoginName	varchar	User name of the currently logged on user. This value is updated with every quick check in. The agent error log file is updated with each change.

vNetstatsLog	network statistics log from the Agent	
Column Name	**Type**	**Purpose**
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
EventTime	datetime	Time stamp string representing the time the change was entered. (note: timestamp type was picked to force times into the database as year-month-day-hr-min-sec all in numeric format independent of the format sent in the SQL command. This allows records to be easily sorted by time during retrieval.)
BytesRcvd	int	Number of bytes received during this statistics period
BytesSent	int	Number of bytes sent during this statistics period
ApplicationName	varchar	Application name using the network

vNtEventLog	Event log data collected from each managed machine	
Column Name	**Type**	**Purpose**
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
LogType	int	1 -> Application Log 2 -> Security Log 3 -> System Log
EventType	int	1 -> Error 2 -> Warning 4 -> Informational 8 -> Success Audit 16 -> Failure Audit
EventTime	datetime	Time the event occurred
ApplicationName	varchar	event log source
EventCategory	varchar	event log category
EventId	int	event log event ID
UserName	varchar	event log user
ComputerName	varchar	event log computer name
EventMessage	varchar	event log message

vOnBoardDeviceInfo	Data collected by KaSmBios.exe during an audit for on-board device information. There is one row per active slot. All information is retrieved from Type 10.	
Column Name	**Type**	**Purpose**
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
DeviceType	varchar	Device Type
DeviceDesc	varchar	Device Description

vPatchStatus	Shows the state of all patches on a per machine basis. There is one row per patch for each machine.	
Column Name	**Type**	**Purpose**

Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
BulletinID	varchar	bulletin ID string reported from the patch scanner
QNumber	int	Q Number for this patch. Refers to the Knowledge Base article on Microsofts site
FixedInServPackFlag	int	0 -> not part of a service pacelse the service pac ID that this patch has been incorporated into.
PatchAppliedFlag	int	0 -> patch has not been applied 1 -> patch has been applied
PatchIgnoreFlag	int	0 -> process this patch 1 -> ignore this patch
InstallDate	dateTime	timestamp when this patch was applied by the VSA
InstalledBy	varchar	Name of admin (if we installed the patch) or value from registry (if scanner retuned the value)

vPortInfo	Data collected by KaSmBios.exe during an audit on port connector information. There is one row per active slot. All information is retrieved from Type 8.	
Column Name	**Type**	**Purpose**
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
InternalDesc	varchar	Internal Description
ExternalDesc	varchar	External Description
ConnectionType	varchar	Connection Type
PortType	varchar	Port Type

vScriptLog	Log of script executions as viewed by the KServer	
Column Name	**Type**	**Purpose**
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
EventTime	datetime	Time stamp string representing the time the change was entered. (note: timestamp type was picked to force times into the database as year-month-day-hr-min-sec all in numeric format independent of the format sent in the SQL command. This allows records to be easily sorted by time during retrieval.)
ScriptName	varchar	Name of script
ScriptDesc	varchar	Event description
AdminName	varchar	Admin name that scheduled this script.

vScriptStatus	script status for each client	
Column Name	**Type**	**Purpose**
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
ScriptName	varchar	Name of script
lastExecTime	datetime	Time stamp string representing the last time that the script was executed
lastExecStatus	varchar	Status of the last execution. The string will be one of the following:Script Summary: Success <ELSE or THEN>Script Summary: Failed <ELSE or THEN> in # step<ELSE or THEN> is replaced with the respective word

		ELSE or THEN.# is replaced by the number of steps that failed in the script (not useful unless allowing the processing to continue after a failure)step is replaced by the work steps if the script failed more than 1 step.
AdminLogin	varchar	Admin name that last scheduled this script. (Dont name this column adminName because that is a primary key used by database migration. adminName and emailAddr should not appear in the same table.

vTicketSummary	Trouble ticket summary. One row per ticket. Column names are used as the names displayed in the view summary table.	
Column Name	**Type**	**Purpose**
TicketID	int	unique trouble ticket ID number
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
machName	varchar	Machine Name used for each agent
groupName	varchar	Group Name used for each agent
TicketSummary	varchar	summary string briefly describing the ticket
Assignee	varchar	Admin name this ticket is assigned to
CreatedBy	varchar	admin name (or machine ID if entered by user) of the person that created this ticket
CreationDate	datetime	timestamp when the ticket was created
DueDate	datetime	ticket due date
ResolutionDate	datetime	timestamp when the ticket was closed
UserName	varchar	The name of the submitter
UserEmail	varchar	The email address of the submitter
UserPhone		The phone number of the submitter
LastModifiedDate	varchar	Date of the most recent note entered for this ticket

vTicketNote	Trouble ticket notes are stored in the database. Each ticket summary can have multiple notes. There is a timestamp that identifies the order they were attached.	
Column Name	**Type**	**Purpose**
TicketID	int	unique trouble ticket ID number
TicketNoteTime	dateTime	Timestamp identifying when the note was added
Author	varchar	person who wrote this note in the ticket
TicketNote	varchar	Contents of the ticket note
HiddenNote	int	0 if the note is visible. 1 if the note is hidden.

vTicketField	Each ticket will have a set of fields associated with it. Three of these fields are standard fields, status, priority, and category. Also, a series of user fields can be added that will also be seen in this view. Each field has a datatype. All lists are stored as integer values. The view vTicketFieldValue has the associated text for each list value.	
Column Name	**Type**	**Purpose**
TicketID	int	unique trouble ticket ID number
FieldLabel	varchar	The label of the field
IntegerValue	int	The value of a integer field
NumberValue	NUMBER(22,4)	The value of a number field
StringValue	varchar	The value of a string field
ListValue	varchar	The value of a list field

vMonitorAlarmCounter	Listing of all alarms created by monitor counters.	
Column Name	**Type**	**Purpose**
MonitorAlarmID	int	unique monitor alarm number

Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with
MachineName	varchar	Machine Name used for each agent
MonitorType	int	0 -> Monitor Counter
MonitorName	varchar	Name of monitor counter object
AlarmType	int	0 -> Alarm 1 -> Trending
AlarmState	smallint	1 -> Open 2 -> Closed
Note	varchar	Notes administrator has entered on the alarm
Message	varchar	Message created from alarm, email message body
AlarmSubject	varchar	Subject of alarm and email subject
AlarmEmail	varchar	Email Address(es) alarm is sent to
EventTime	datetime	Date and Time of alarm
TicketID	int	Ticket ID created from alarm
LogValue	float	Value causing alarm
AdminName	varchar	Administrator who assigned monitor counter to machine

vMonitorAlarmService	Listing of all of the alarms created by monitor services.	
Column Name	**Type**	**Purpose**
MonitorAlarmID	int	unique monitor alarm number
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with.
MachineName	varchar	Machine Name used for each agent
MonitorType	int	0 -> Monitor Service
MonitorName	varchar	Name of monitor service object
AlarmType	int	0 -> Alarm 1 -> Trending
AlarmState	smallint	1 -> Open 2 -> Closed
Note	varchar	Notes administrator has entered on the alarm
Message	varchar	Message created from alarm, email message body
AlarmSubject	varchar	Subject of alarm and email subject
AlarmEmail	varchar	Email Address(es) alarm is sent to
EventTime	datetime	Date and Time of alarm
TicketID	int	Ticket ID created from alarm
LogValue	float	Value causing alarm, below are service values: -1 -> Does not exist 0 -> Reserved 1 -> Stopped 2 -> Start Pending 3 -> Stop Pending 4 -> Running 5 -> Continue Pending 6 -> Pause Pending 7 -> Paused
AdminName	varchar	Administrator who assigned monitor service to machine

vMonitorAlarmProcess	Listing of all alarms created by monitor processes.	
Column Name	**Type**	**Purpose**
MonitorAlarmID	int	unique monitor alarm number

Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with
MachineName	varchar	Machine Name used for each agent
MonitorType	int	2 -> Monitor Process
MonitorName	varchar	Name of monitor process object
AlarmType	int	0 -> Alarm 1 -> Trending
AlarmState	smallint	1 -> Open 2 -> Closed
Note	varchar	Notes administrator has entered on the alarm
Message	varchar	Message created from alarm, email message body
AlarmSubject	varchar	Subject of alarm and email subject
AlarmEmail	varchar	Email Address(es) alarm is sent to
EventTime	datetime	Date and Time of alarm
TicketID	int	Ticket ID created from alarm
LogValue	float	Value causing alarm, below are process values: 0 -> Stopped 1 -> Running
AdminName	varchar	Administrator who assigned monitor process to machine

vMonitorAlarmSNMP	Listing of all alarms created by monitor SNMP Get objects.	
Column Name	**Type**	**Purpose**
MonitorAlarmID	int	unique monitor alarm number
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with
MachineName	varchar	Machine Name used for each agent
MonitorType	int	3 -> Monitor SNMP Get
MonitorName	varchar	Name of monitor SNMP Get object
AlarmType	int	0 -> Alarm 1 -> Trending
AlarmState	smallint	1 -> Open 2 -> Closed
Note	varchar	Notes administrator has entered on the alarm
Message	varchar	Message created from alarm, email message body
AlarmSubject	varchar	Subject of alarm and email subject
AlarmEmail	varchar	Email Address(es) alarm is sent to
EventTime	datetime	Date and Time of alarm
TicketID	int	Ticket ID created from alarm
LogValue	float	Value causing alarm, if the return value of the SNMP Object Get command is a string the value will be the the Message
SNMPName	varchar	Name returned from SNMP Device on scan
SNMPCustomName	varchar	Custom name for SNMP Device
AdminName	varchar	Administrator who assigned monitor SNMP Get to machine

vMonitorAlarmAlert	Listing of all alarms created by monitor alerts.	
Column Name	**Type**	**Purpose**
MonitorAlarmID	int	unique monitor alarm number
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with
MachineName	varchar	Machine Name used for each agent
MonitorType	int	4 -> Monitor alert
EventLogType	smallint	Only applies to AlertType=6(NT Event Log) 0 -> Application Event Log

		1 -> System Event Log 2 -> Security Event Log
AlarmType	int	0 -> Alarm 1 -> Trending
AlarmState	smallint	1 -> Open 2 -> Closed
Note	varchar	Notes administrator has entered on the alarm
AlertType	int	2 -> Get File change alert 3 -> New Agent checked in for the first time 4 -> Application has been installed or deleted 5 -> Script failure detected 6 -> NT Event Log error detected 8 -> Protection violation detected 9 -> PCI configuration has been changed 10 -> Disk drive configuration change 11 -> RAM size changed 14 -> LAN Watch alert type 15 -> Agent offline 16 -> Low on disk space 17 -> Disabled remote control 18 -> Agent online 19 -> New patch found 20 -> Patch path missing 21 -> Patch install failed 23 -> Backup Alert
Message	varchar	Message created from alarm, email message body
AlarmSubject	varchar	Subject of alarm and email subject
AlarmEmail	varchar	Email Address(es) alarm is sent to
EventTime	datetime	Date and Time of alarm
TicketID	int	Ticket ID created from alarm
AdminName	varchar	Administrator who assigned monitor alert to machine

vMonitorAlarmSystemCheck	Listing of all alarms created by monitor system checks.	
Column Name	**Type**	**Purpose**
MonitorAlarmID	int	unique monitor alarm number
Machine_GroupID	varchar	A concatenated representation of the machine id and the group id it is associated with
MachineName	varchar	Machine Name used for each agent
MonitorType	int	5 -> Monitor system check
SystemCheckType	smallint	1 -> Web Server 2 -> DNS Server 4 -> Port Connection 5 -> Ping 6 -> Custom
AlarmType	int	0 -> Alarm 1 -> Trending
AlarmState	smallint	1 -> Open 2 -> Closed
Note	varchar	Notes administrator has entered on the alarm
Paremeter1	varchar	First parameter used in system check
Parameter2	varchar	(Optional) Second parameter used by system check
Message	varchar	Message created from alarm, email message body

AlarmSubject	varchar	Subject of alarm and email subject
AlarmEmail	varchar	Email Address(es) alarm is sent to
EventTime	datetime	Date and Time of alarm
TicketID	int	Ticket ID created from alarm
AdminName	varchar	Administrator who assigned of monitor counter to machine

Administrator Notes

Administrator Notes allow you to log what you did to a machine or group of machines into the system database. The next time you have a problem with any machine, check the notes and see what other administrators have done on that machine. The system time-stamps each administrator note and associates the note with an administrator name.

Open the notes editor by clicking the Notes button in the toolbox. In addition to viewing any machine's notes log, you can also view the log under the Agent Tab by clicking the User Logs function. Print the Administrator Notes Log by clicking the Reports Tab and setting up a Logs report.

Machine.Group ID

List of machines that match the Specify Accounts area selection on the main page. Check the box in front of all the machines you wish to apply the note to.

Time

This field displays the time-stamp when the note was first entered. The time-stamp can be edited by clicking the Edit icon next to the specific note whose time-stamp you wish to change.

Admin

Login name of the administrator that entered the note. If a different administrator edits the note, this field is updated with the new administrator's name.

✕**Delete the note**

Click the icon to delete the adjacent note. If more than one machine has the same note entered by the same administrator and has the same time-stamp, the system asks if you want to delete all occurrences of the note.

📝**Edit the note**

Modify any note by clicking the edit icon next to it. Click the **Apply** button to commit the changes. Click **Cancel** to restore the original text. If more than one machine has the same note entered by the same administrator and has the same time-stamp, the system asks if you want to modify all occurrences of the note.

Note

Displays the administrator entered note for the selected machine.

Notes per Page

Number of notes to display at a time. Choices are 10, 30, and 100.

Assistant

Assist Admin Notes

Show me an explanation of the items on this page.

What is the Administrator Notes Database?

Administrator Notes allow you to log what you did to a machine or group of machines into the system database. The next time you have a problem with any machine, check the notes and see what other administrators have done on that machine. The system time-stamps each administrator note and associates the note with an administrator name.

Do notes ever expire in the database?

No. Administrator notes never expire. Notes are only removed from the database by clicking the ☒ icon next to the note or deleting the machine account the note is associated with.

When I edit a note, does the time-stamp automatically update?

No, the time-stamp remains the same. You can specify any other time you wish though using the drop down control that appears when you edit the note.

Can I generate a report containing these Administrator notes?

Yes. Under the Reports tab, the Logs function permits you to select Admin Notes as the log type for a report.

Using Scripts

View **IF / THEN / ELSE** parameter definitions...

Script Locations

All scripts are accessed under the Install tab. There individual scripts may be organized into folders. Only scripts designated as shared scripts can be seen by other administrators. Clicking the script on the left-hand navigation bar displays a list of active accounts and machines. Schedule a script to execute on any or all machines under management by selecting the checkbox in front of the desired machine account then pressing the appropriate script execution button.

Script Toolbar

Open/expand all folders

Close/collapse all folders

Reorder all scripts and folders alphabetically

Search tool used to locate a script

Import a new script

Create a new script and open the script editor

Script Manager

Click on any script folder to open the script manager. **Rename**, **delete**, **re-order**, or **move** any script or folder contained in the selected script folder. Clicking the script name or folder name automatically moves the system focus to that item. To **move an item**, select the new destination folder from the dropdown control associated with the item you wish to move.

Executing Scripts

Scripts automate tasks on remote machines and can be performed on single or multiple machines simultaneously. You can schedule scripts to run immediately or at any specific time. Check the box in front of **Run recurring** to task a script to execute at a recurring interval of your choosing.

Click edit to view / modify the script.

Clicking the edit link opens the current script in the script editor. Here you can view and/or modify any script step.

Schedule

Press Schedule to schedule a script to run on the selected client machines. The scripts runs at the specified date and time. If **Run recurring** is checked, the script runs once every interval specified. If the remote machine is offline at the scheduled time, the remote machine will run the script the next time it goes online.

If the interval is at least one day, then the recurring script runs at the scheduled time every interval. If the interval is less than one day, the interval is added to the last execution time of the script. For example, schedule a machine to execute a script at 2am. with a recurring interval of 1 day. If the machine is turned off at 6pm and back on at 8am, the script runs at 8am. The VSA next schedules that script to run at 2am the next morning. If the interval were set to 3 hours, then the VSA next schedules that script to run at 11am the same morning.

Specify time to execute

Using the dropdown menus, enter the date and time to execute the script. After entering a date and time, press Schedule to schedule the script on the selected client machines.

Cancel

Press cancel to cancel the scheduled scripts from executing on the selected client machines.

Run recurring

To execute a script indefinitely at a regular interval, check the Run recurring checkbox and enter the interval time in day(s) or hour(s).

Note: If the interval is at least one day, then the recurring script runs at the scheduled time every interval. If the interval is less than one day, the interval is added to the last execution time of the script.

Stagger by

Scheduling a the same script to run at the same time on multiple machines my excessively load your server and/or internet connection. To automatically spread out the execution times, enter the number of minutes to stagger the script start time by. Clicking Schedule with multiple machine IDs selected, sets the execution time for the first machine at the scheduled time. It schedules the second machine at that time plus stagger minutes, and so on.

Skip if offline

Checking this box to only allow the script to run at the scheduled time of day (15 minute window). If the machine is offline at the scheduled time, then the script will not execute at all. If recurring is set, then the script is rescheduled to run at the next appointed time.

Last Execution Time/Last Execution Status

If a previous script was performed, the date of the last script and its status is displayed.

Next Scheduled Run/Recurring Interval

Shows the time of the next scheduled script and its execution frequency.

Auto Refresh Table

Selecting this checkbox will automatically update the client list table every five seconds. This checkbox is automatically selected and activated whenever Schedule is pressed.

Related Info

Script Editor

View **IF/THEN/ELSE** parameter definitions...

The following elements are displayed in the Script Editor:

Share...
You can share scripts with other individual administrators, entire administrator groups, or make the script public to all administrators. Only the **script owner** can set the share rights for a script.

Note: If the administrator that created a script leaves, the master administrator can take ownership of a script and change the share rights.

Save As...

Select *Save As...* to save a script to a different name/group. A dialog box will ask you to enter the name to save the script as. The script name must be less than 64 characters in length.

Save

Select *Save* to save changes to a configured script.

Rename...

A script can be renamed by selecting the script from the **Select Script** dropdown box, then selecting *Rename*. A dialog box will ask you to enter the new name for the script. When finished, press OK. The script name must be less than 64 characters in length.

Delete

You can delete a script by selecting a script from the **Select Script** dropdown menu, then selecting *Delete*.

Import Script.../Export Script...

Selecting the import/export script links will bring up a dialog box that will allow you to import and export a script file. Exporting a script will display the script's text, which can be copied to the clipboard. Importing a script will allow you to browse and select a text file to import into the scripting engine.

Note: Only scripts *exported* by the Script Editor can be *imported* into the Script Editor.

Manage Files...

Selecting the Manage Files hyperlink text will invoke a dialog box that enables files to be uploaded to the server. Press browse to locate files to upload. Press upload to upload the file to the server. The *Remove file from the server* function permanently removes a file from the server. Any type of binary or ASCII file can be uploaded to the Server. Uploaded files can then be used within scripting steps. If the file no longer exists on the Server, an error message will appear next to the dropdown list.

Note: An alternate method of uploading files is to copy them directly to the managed files directory on the IIS server. This directory is normally located in the directory [drive]:\Inetpub\wwwroot\ManagedFiles\. In that directory are several sub-directories. Put private files into the directory named for that administrator. Put shared files into the VSASharedFiles directory. Any files located in this directory will automatically update what is available in the scripting user interface at the next administrator logon.

Manage Variables...

Variable Manager allows administrators to create short, easy-to-remember names that contain long, difficult-to-remember directory paths and commands. These names (variables) are used in the Script Editor by using the syntax **<VariableName>**. The same variable can be assigned different values for each group ID.

Note: Built-in scripts that reference LAN server directories use the variable <FileServer>. Use the Variable Manager to assign the <FileServer> variable a directory that applies to your network environment.

Script Notes

Enter any notes about the script.

Operating System Detect

When writing a THEN/ELSE function, you can select on which operating system the function will execute. This function is useful when you want to write one script that can be executed on different operating systems. For example, directory paths in Windows 95 and Windows NT can differ and require different directory path syntax in order to work correctly. Creating two separate script steps within the same script and labeling them Windows 95 and Windows NT, respectively, avoids having to create an extra script for a separate operating system.

Related Info

IF / THEN / ELSE Definitions

IF/THEN/ELSE Definitions

HELP HOME

Click on a script parameter to view its definition:

IF Definitions	
Application is Running	Test to see if the specified application is running.
Check Registry Value	Evaluate the given Registry Value.
Check Variable	Evaluate the given Agent Variable.
Test File	Test for the existence of a file.
Test File in Directory Path	Test for the existence of a file in the current Directory Path.
Test Registry Key	Test for the existence of the given Registry Key.
True	Always returns True, executing THEN branch.
User Is Logged In	Tests whether a specific user (or any user) is logged in or not.
User Response is Yes	Presents a Yes/No dialog box to the user.
THEN / ELSE Definitions	
Close Application	Close a running application.
Delete File	Delete a file from the remote machine.
Delete File in Directory Path	Delete file in directory returned by Get Directory Path From Registry.
Delete Registry Key	Delete the key from the registry.
Delete Registry Value	Delete the value from the registry.
Execute File	Execute any file as if it was run from the Run item in the Windows Start menu.
Execute File in Directory Path	Same as execute file. File location is relative to the directory returned by Get Directory Path From Registry.
Execute Script	Start another VSA script.
Execute Shell Command	Run any command from a command shell.
Get Directory Path From Registry	Returns the directory path stored in the registry at the specified location.
Get File	Get a file from the remote machine and save it to the VSA server.
Get File in Directory Path	Get a file from the remote machine located relative to the directory returned by Get Directory Path From Registry and save it to the VSA server.
Get Variable	Get a value from the agent on the remote

	machine and assign it to a variable
Impersonate User	Use the specified credential to execute a file or shell when Execute as user specified.
Pause Script	Pause the script for N seconds.
Reboot	Reboot the remote machine.
Rename Locked File	Renames a file that is currently in use.
Rename Locked File in Directory Path	Renames a file in directory returned by Get Directory Path From Registry that is currently in use.
Send Message	Display a message in a dialog box on the remote machine.
Send a URL	Open a browser to the specified URL on the remote machine.
Set Registry Value	Set the registry value to a specific value.
Use Credential	Use the user login credentials set for the machine ID in Set Credential to execute a file or shell when Execute as user specified.
Write File	Write a file stored on the VSA to the remote machine.
Write File in Directory Path	Write a file stored on the VSA to the remote machine at into the directory returned by Get Directory Path From Registry.
Write Script Log Entry	Write a string to the Script Log.

IF Definitions

Application is Running

Checks to see if a specified application is currently running on the client machine. If the application is running, the THEN statement is executed; otherwise, the ELSE statement is executed. When this option is selected from the dropdown list, the "Enter the application name" field appears.

Check Registry Value

After entering the registry path, the value contained in the key is returned. A check can be made for existence, absence, equality, or size differences. For example, HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\AppPaths\AgentMon.exe\path contains the directory path identifying where the Agent is installed on the target machine. The test determines if the value stored at the key exists, thereby verifying the Agent is installed.

Note: a backslash character \ at the end of the key returns the default value that key. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\WORDPAD.EXE\ will return the default value something like %ProgramFiles%\Windows NT\Accessories\WORDPAD.EXE

The available tests are:

- Exists : true if the registry key exists in the hive
- Absent : true if the registry key does **not** exist in the hive
- = : true if value of the registry key equals the test value
- Not = : true if value of the registry key does **not** equal the test value
- > : true if value of the registry key is greater than the test value (value must be a number)
- >= : true if value of the registry key is greater than or equal to the test value (value must be a number)
- < : true if value of the registry key is less than the test value (value must be a number)
- <= : true if value of the registry key is less than or equal to the test value (value must be a number)
- Contains : true if the test value is a sub string of the registry key value (value must be a string)

- Not Contains : true if the test value is **not** a sub string of the registry key value (value must be a string)

Check Variable

Enter an Agent Variable name, in the form #var_name#, in the space provided. Check Variable evaluates the current values assigned the #var_name# and compares it with the supplied value. The supplied value may also be another Variable name in the form of #var_name#. If the check is true, THEN steps are executed. If the check is false, ELSE steps are executed.The available tests are:

- Exists : true if the variable exists
- Absent : true if the variable does **not** exist
- = : true if value of the variable equals the test value
- Not = : true if value of the variable does **not** equal the test value
- > : true if value of the variable is greater than the test value
- >= : true if value of the variable is greater than or equal to the test value
- < : true if value of the variable is less than the test value
- <= : true if value of the variable is less than or equal to the test value
- Contains : true if the test value is a sub string of the variable (variable must be a string)
- Not Contains : true if the test value is **not** a sub string of the variable (variable must be a string)

For the tests =, Not =, >, >=, <, and <= the variables compared may be a string, a number, a date in the format of yyyy/mm/dd or yyyy/mm/dd hh:mm or yyyy/mm/dd hh:mm:ss, or a version number containing dots or commas such as 1.2.3 or 4,5,6,7.

Test File

Determines if a file exists on a remote machine. Enter the full path and filename. For example, entering c:\windows\notepad.exe returns **True** if Notepad.exe exists, **False** if it does not.

Back to Top

Note: Environment variables such as %windir%\notepad.exe are acceptable.

Test File in Directory Path

Enter the name of a file to see if it exists on the remote machine. Because a THEN or ELSE step must be executed prior to this IF test, *Test File in Directory Path* is only useful for scripts that are executed by THEN or ELSE steps.

Test Registry Key

Tests for the existence of a registry key. *Test Registry Key* differs from *Check Registry Value* since it can check for a directory level registry entry that only contains more registry keys (no values). *Test Registry Key* detects if an entire registry branch exists.

True

Selecting ***True*** directs the THEN steps to execute. Use ***True*** to directly execute a series of steps that do not require any decision points, such as Does a file already exist?

User Is Logged In

Tests to see if a specific user or any user is logged in on the remote machine. Enter the user's login name or leave the field blank to check for any user logged in. The THEN steps are executed if a user is logged in. The ELSE steps are executed if the user is not logged in.

User Response is Yes

Displays a dialog box on the remote machine with a **Yes** and **No** button. Also carries out the ELSE command if an administrator-configured specified amount of time has elapsed (timeout). If **Yes** is selected, the THEN function is executed. If the selection times out or the user selects **No,** the ELSE function is executed. This function requests the user's permission to proceed with the script. This query is useful for scripts that require a reboot of the remote machine before completion.

Each script consists of a simple IF-THEN-ELSE clause. IF tests for something on a remote machine. If the test passes, (was true, the file exists, etc.) the statements in the THEN section are executed. If the test fails, the statements in the ELSE section are executed. Refer to the section below to create/edit a script with IF-THEN-ELSE clauses.

Note: Script variables (#varName#) may be used inside the User Response is Yes fields to dynamically generate messages based on script data.

Back to Top

Note: The /qn parameter passed with setup.exe commands Microsoft install files to install quietly without prompting the user for any information. If a product key is required, the program asks for it on first use. This option allows installation of programs to all machines in parallel without any per-machine interaction.

THEN/ELSE Definitions

Operating System Detect

When writing a THEN/ELSE function, you can select on which operating system the function will execute. This function is useful when you want to write one script that needs to be executed on different operating systems. For example, directory paths in Windows 95 and Windows NT can differ; create two separate script steps and label them Windows 95 and Windows NT, respectively.

Close Application

If the specified application is running on the remote machine, then that application is closed down.

Delete File

Deletes a file on a remote machine. Enter the full path and filename.

Note: Environment variables are acceptable if they are set on a user's machine. For example, using a path %windir%\notepad.exe would be similar to C:\windows\notepad.exe.

Back to Top

Delete File in Directory Path

Deletes the specified file located at the path returned from a *Get Directory Path From Registry* call.

Delete Registry Value

Delete the value stored at the specified registry key.

Delete Registry Key

Delete the specified registry key and all its sub-keys.

Execute File

Executes the specified file on the remote machine. This function replicates launching an application from the **Run...** command located in the Microsoft Windows **Start** menu. This function takes three parameters:

1. Full path filename to the .exe file.
2. Argument list to path to the .exe file
3. Flag indicating whether the script should wait until the .exe completes or not. (1 to wait, 0 to have the script continue without waiting).Note: Environment variables are acceptable, if they are set on a user's machine. For example, using a path %windir%\notepad.exe, would be similar to C:\windows\notepad.exe.

Execute File in Directory Path

Same as Execute File except the location of the .exe file is located at the path returned from a *Get Directory Path From Registry* call.

Note: Environment variables are acceptable if they are set on a user's machine. For example, using a path %windir%\notepad.exe would be similar to C:\windows\notepad.exe.

Back to Top

Execute Script

Causes another named script to execute. Use this capability to string multiple IF-THEN-ELSE clauses together. If the script no longer exists on the server, an error message will appear next to the script dropdown list.

Execute Shell Command

Allows the script to pass commands to the command interpreter on the client machine. When this command is selected, the field *Enter the command to execute in a command prompt* is displayed. Enter a command in the field. The command must be syntactically correct and executable with the OS version on the client machine. Commands and parameters containing spaces should be surrounded by quotes. Since the command is executed relative to the Agent directory, absolute paths should be used when entering commands.

Note: Execute Shell Command opens a Command Prompt window on the remote machine to execute in. If you do not want a window opening on the remote machine (it may confuse uses), put all the commands into a batch file. Send that file to the remote machine (using Write File). Then run the batch file with the Execute File command. Execute File does not open a window on the remote machine.

Get Directory Path From Registry
Returns a file path stored in the specified registry key. Use this command to fetch file location. For instance, use this command to find the directory where an application has been installed.

Back to Top

Get File
Upload the file at the specified path from the remote machine. Be sure to enter a full path filename (including the filename) that you want the file to upload. The file is stored on the VSA in a private directory for each remote machine. Access the uploaded file from the Get File function under the Configure Tab.

As an option, existing copies of uploaded files will be renamed with a .bak extension prior to the next upload of the file. This allows you to examine both the latest version of the file and the previous version.

Also as an option, an email alert can be sent when a change in the uploaded file has been detected (compared to the last time the same file was uploaded).

Get File in Directory Path
Just like **Get File** but it adds the path returned from a *Get Directory Path From Registry* call to the beginning of the remote file path. Access the uploaded file from the Get File function under the Configure Tab.

Back to Top

Get Variable
Defines a new Agent variable. When the script step executes, the system defines a new variable and assigns it a value based on data fetched from the remote machine's agent. You can refer to this value in an subsequent script line (or subsequent script) by adding # around the variable name. e.g. #var_name#

Impersonate User
Use the specified credential to execute a file or shell when Execute as user specified. Enter a username, password, and domain for the agent to log in with. Leave **domain blank to log into an account on the local machine**.

Pause Script
Pause the script for N seconds. Use this command to give Windows time to complete an asynchronous task, like starting or stopping a service.

Reboot
Unconditionally reboots the remote machine. To warn the user first, preface this command with a *User Response is Yes* message. A *User Response is Yes* message will prompt the user before rebooting their machine.

Rename Locked File
Renames a file that is currently in use. The file is renamed the next time the system is rebooted. The specified filename is a complete file path name. *Rename locked file* can also be used to delete a file that is currently in use if the destination is empty. The file is deleted when the system is rebooted.

Back to Top

Rename Locked File in Directory Path
Renames a file that is currently in use. The file is renamed the next time the system is rebooted. The specified file name is appended to the directory path. *Rename locked file in directory path* can also be used to delete a file that is currently in use if the destination is empty. The file is deleted when the system is rebooted.

Send Message

Sends the entered message to a remote machine. Selecting *Immediately* will display a message dialog box immediately. Selecting *After user clicks the flashing system tray icon* flashes the Agent system tray icon when a message is received. The message is displayed when the user clicks the icon.

Send a URL
Sends the entered URL to a remote machine. Selecting *Immediately* launches the default Web browser and the specified URL is displayed. Selecting *After user clicks the flashing system tray icon* flashes the Agent system tray icon when a message is received. The URL is displayed in the default Web browser when the user clicks the icon.

Back to Top

Set Registry Value
Writes data to the specified registry key. This function takes three parameters:

1. Registry key path
2. Data to write to the registry key
3. Data type of the registry key (String Value, DWORD Value, Binary Value).

Use Credential
Use the user login credentials set for the machine ID in Set Credential to execute a file or shell when Execute as user specified.

Write File
Writes a new file to the remote machine at the specified path and filename. Be sure to enter a full path filename (including the filename) that you want the file to be named. The source file is pulled from the server from the drop down control. To add more files to the server, click *Manage Files...*

Each time a script executes the "Write File" command, the agent checks to see if the file is already there or not (hashes the file to verify integrity). If not, the file is written. If the file is already there, the script moves to the next step. **You can repeatedly run a script with Write File that sends a large file to a remote machine and know that the VSA will only download that file once.**

Note: Environment variables are acceptable if they are set on a user's machine. For example, using the path %windir%\notepad.exe would be equivalent to C:\windows\notepad.exe.

Write File in Directory Path
Writes the specified filename to the path returned from a *Get Directory Path From Registry* call.

Write Script Log Entry
Writes the supplied string to the script log for the agent executing this script.

Back to Top

Related Info

Variable Manager

View **IF/THEN/ELSE** parameter definitions...

The following elements are displayed in the Variable Manager:

Select Variable
Dropdown list where variable names can be selected. To change a variable's name or value, select the variable from the list and enter the new name or value in the appropriate field and press apply. To create a new variable, select **<New Variable>** from the dropdown list and enter a new name and value in the appropriate fields.

Rename/Create Variable
Enter a name to rename a current variable, or a new name when creating a new variable.

Set Variable Value
Enter a new value when changing a current variable's value, or a new value when creating a new variable.

Shared
Selecting the *Shared* radio button allows the variable to be used by all administrators. However, only master administrators can create and edit shared variables.

Private
Selecting the *Private* radio button allows the variable to be used only by the administrator who created it.

Apply
After selecting the group IDs from the group ID list, press Apply to set the variable name and variable value.

Delete
After selecting the group IDs from the group ID list, press delete to remove the variables from the group ID it is assigned to.

Select All/Unselect All
Clicking **Select All** selects all groups IDs shown in the list. Clicking **Unselect All** deselects any group IDs selected in the list.

Group ID
All group IDs administered by the logged in administrator are shown.

Value
Lists the value of the variable applied to the group ID.

Related Info

Assistant

Assist Script Editor

Assistant

HELP HOME

IF/THEN/ELSE Definitions

How do I create a script?

Script commands are carried out in the Script Editor window, which can be accessed by clicking the Script Editor icon in the Toolbox. The Toolbox is located in the upper left-hand corner of the system console.

To create a script:

1. Click the *New...* link.
2. In the dialog box, enter a name for your new script.
3. Press OK.
4. In the **Select Feature Group** dropdown menu, select the feature tab where you would like your script to be located.
5. Select the Shared Script or Private Script radio button.
   - **Shared Script** This script will be accessible by any administrator who logs on to the system. A shared script is located in the left-hand navigation bar and is adorned by the shared script icon (shown above).
   - **Private Script** This script can only be viewed and accessed by the administrator who created it. A private script is separated from shared scripts by a horizontal rule and is adorned by the private script icon (shown above).
6. In the **Script Notes** field, enter any information to help you identify/describe the script, such as its function, length, or actions it performs.
7. Start creating your script using the IF/THEN/ELSE statements. For more information on creating and executing scripts, follow the links below:

   IF/THEN/ELSE Definitions Provides information on the multiple IF/THEN/ELSE statements available.

   Script Editor Provides information on the functionality of the Script Editor interface.

   Using Scripts Provides information on using scripts after they have been created. Includes information on executing and scheduling scripts on one or multiple client machines.
8. When you are finished creating your script, you can save it by clicking the *Save* link. To create a copy of your script with a different name, click *Save As...*, then enter a new name and press OK.

How do I edit an existing script?

To edit an existing script from the Script Editor:

1. In the **Select Script** dropdown menu, select the script that you would like to edit.
2. The script's configuration is displayed in the IF/THEN/ELSE fields as well as the script's Script Notes. The script's security status (shared/private) is also displayed.
3. Make the necessary edits.
4. Click *Save*.
5. The changes are made and the script is saved.

To edit an existing script from the system interface:

1. Click the script's private/shared icon. The script editor is launched and the script can be edited.

Or

1. Click on the script in the left-hand navigation bar.

Note: Only scripts that you have access to will be shown. Private scripts created by other administrators will not be shown, thus they cannot be edited.

2. In the client machine list, the script execution controls are shown (i.e., Run Now, Run At, Recurring, Edit).
3. Press Edit.
4. The Script Editor is displayed and the script's configuration is displayed in the IF/THEN/ELSE fields as well as the script's Script Notes. The script's security status (shared/private) is also displayed.
5. Make the necessary edits.
6. Click *Save*.
7. The changes are made and the script is saved.

How do I delete a script?

To delete a script:

1. Click the Script Editor icon located in the Toolbox.
2. In the **Select Script** dropdown list, select the script you would like to delete.
3. Click the *Delete* link.
4. In the confirmation dialog box, click OK.
5. The script is deleted.

Show me an explanation of the items on this page.

Assist Variable Manager

Assistant

HELP HOME

How do I create a variable?

To create a variable:

1. Select **<New Variable>** from the **Select Variable** dropdown list in step 1.
2. Enter a name for the variable in the **Rename/Create Variable** field.
3. Enter a value for the variable in the **Set Variable Value** field.
4. Assign a permission to the variable.
5. Select the group IDs that will use the new variable from the group ID list.
6. Press apply.

   The variable value is shown in the **Value** column. Click **Close** to close the Variable Manager.

How do I change a variable name or value?

To change a variable name or value:

1. Select the variable from the **Select Variable** dropdown list.
2. Edit the variable name in the **Rename/Create Variable** field.
3. Edit the variable value in the **Set Variable Value** field.
4. Press apply.

   The variable's value and/or name is changed in all the group IDs the variable is assigned to.

Show me an explanation of the items on this page.

Forgotten Administrator Password

If you have forgotten your Master Administrator account password, the system provides a way for you to create a new Master Administrator account, which enables you to log back in to the system and retrieve the forgotten account information.

Note: You must have Administrator (Windows NT/2000) privileges on the server running the system. Due to security reasons, you cannot perform the following procedure remotely.

To create a new Master Administrator account:

1. Log in to the machine running the server component of the system.
2. Access the following web page: http://localhost/LocalAuth/setAccount.asp
3. Enter a new account name in the **Master Administrator Name** field.
4. Enter a password in the **Enter Password** field and confirm it by re-typing it in the **Confirm Password** field.
5. Press Create.

   You will now be logged in to the system as a master administrator.

Changing the Administrator Password

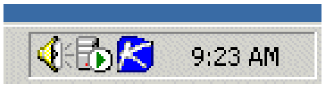
To change your administrator password, use the Preferences function of the System feature tab.

Agent Icon

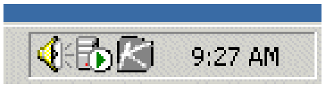
HELP HOME

Once installed on a machine, the agent displays it icon in the computer's system tray. This icon is the user's only interface to the agent. The icon may be disabled at the discretion of the Administrator in the Agent Menu function.

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

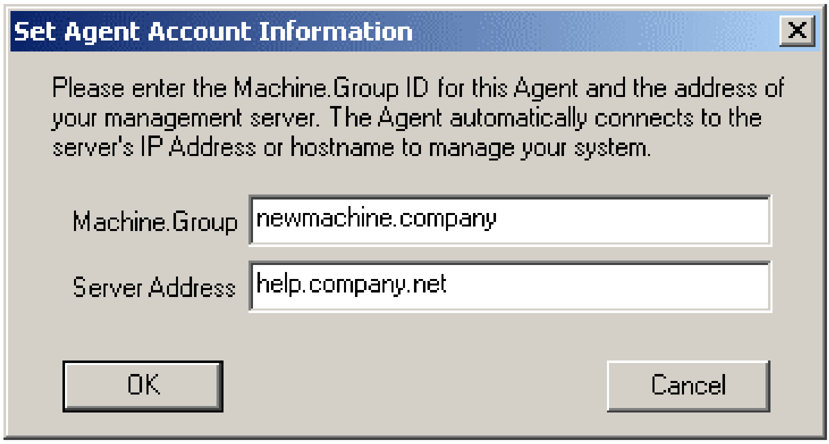


A running agent that can **not** check into the VSA displays a **gray icon**. This indicates that either the network connection is down or the agent is pointed at the wrong address for the VSA.



If the agent icon is gray check the following:

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



Set Agent Account Information

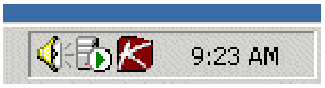
Please enter the Machine.Group ID for this Agent and the address of your management server. The Agent automatically connects to the server's IP Address or hostname to manage your system.

Machine.Group: newmachine.company

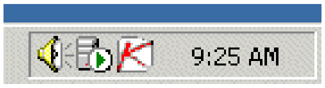
Server Address: help.company.net

1

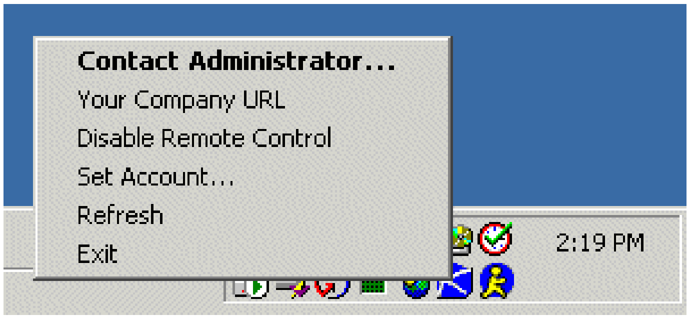
The agent icon turns **red** when a user manually disables remote control. Users prevent anyone from remote controlling their machine by selecting **Disable Remote Control** when they right click the agent menu.



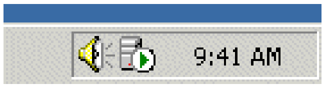
The agent icon **flashes** between a white background and its normal background when a message is waiting to be read. Clicking the icon displays the message.



Right clicking the agent menu pops up a menu of options available to the user. Each menu item may be turned on or off at the discretion of the administrator



Administrators may completely disable the agent menu and remove the icon for the machine's desktop.



Note: The Enterprise Edition lets you fully customize the agent icon. Click here for full instructions.

Edit Views

The system lets you manage 1,000 machines as easily as one machine. **Views** let you refine the list of machines you wish to work on at one time. In addition to sorting based on machine group, views let you sort by attributes found on the machine (such as operating system type).

Quickly change views by selecting a different view from the **Select View** dropdown control located on every page. You can create and name multiple views. To create/change any view click the **Edit...** button located to the right of the Select View dropdown control.

Creating a new view

1. Click the **Edit...** button to the right of the Select View dropdown control to open the View Definitions editor.
2. Enter a name for the view in the **Edit Title** area.
3. Enter the desired filter specifications.
4. Click the **Save As** button.

Edit an existing view

1. Click the **Edit...** button to the right of the Select View dropdown control to open the View Definitions editor.
2. Select the desired view from the **Select View** dropdown control.
3. Modify the desired filter specifications.
4. Click the **Save** button.

View by machine ID

- **Set machine ID** - Checking this box overrides the Machine ID filter on the main page Select Machine area with the value entered here. The machine ID field is disabled to prevent inadvertent changes while displaying a view with *Force machine ID* selected.
- **Set group ID** - Checking this box overrides the Group ID filter on the main page Select Machine area with the value entered here. The Group ID field is disabled to prevent inadvertent changes while displaying a view with *Force group ID* selected.
- **Show/Hide members of collection** - Checking this box works together with the machine ID and group ID filters to only list specific machines belonging (**Show**) or not belonging to (**Hide**) a specific collection. Define collections here.

View by network status and address

- **Show machines that have/have not been online in the last N Days** - Check this box to only list machines whose agents have checked into server (or not) within the specified period of time.
- **Connection gateway filter** - Check to only list machines that have a connection gateway matching the specified filter. Use * for a wildcard if necessary. For example 66.221.11.* matches all connection gateway addresses from 66.221.11.1 through 66.221.11.254
- **IP address filter** - Check to only list machines that have an IP address matching the specified filter. Use * for a wildcard if necessary. For 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 by the Name/OS Info function under the Audit tab.
- **OS Version** - Check to only list machines that match the OS version string as reported by the Name/OS Info function under the Audit tab. Use this filter to **identify machines by service pack**.

View machines based on script history/status

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

Note: Click the select script link to specify the script by name.

- **Last execution status success/failed**- Check to only list machines that have already executed the selected script Select the appropriate radio button to list machines that successfully executed the script or failed to execute the script.

- **Script has / has not executed in the last N days** - Check to only list machines that have or have not executed the script in the specified period of time.

Status Monitor

HELP HOME

The status monitor continuously monitors selected machines, notifying you when they go online or offline. If someone is currently logged onto the machine, Status Monitor displays their user name in bold along with the IP address of the machine. **Master Administrators** can also display the list of logged on administrators

Turn off sound

A unique audible tone sounds each time a machine goes online, machine goes offline, an administrator logs in, or an administrator logs out. Turn these sounds off by checking this box.

Refresh Rate

Refreshes the browser every 30 sec, 1, 2, or 5 minutes. Each browser refresh gets the latest status from the VSA. To get an immediate update, click the "**Refresh Now"** link.

List logged on administrators

Uncheck this box to hide the list of administrators. (*Available to Master Administrators only.)*

Sort By

List machines in any of the following order:

1. Connection Gateway - Best for grouping machines by how they are connected on the network.
2. Group ID - Alphabetically by group ID.
3. Machine ID - Alphabetically by machine ID.

Hide offline machines

Unchecking this box lists all machines. Offline machines have a grayed out icon.

Show me an explanation of the items on this page.

What are user logs used for?

Logs collect event information on Agent machines. The different types of logs that can be generated are:

- Agent Log
- Configuration Changes
- Network Statistics
- Alert Log
- Application Event Log
- Security Event Log
- System Event Log
- Script Log

The logs capture the following information:

Script Log Shows a list of scripts executed on the selected Agent machine. The date and time of each script execution is also noted, as well as whether it completed successfully or not.

Agent Log Shows a list of activity associated with the Agent machine Agent. Start and stop times, successful remote control sessions, .ini file changes, and other information is captured. The date and time of each activity is also noted.

Configuration Changes Shows a log of changes made by a master or standard administrator to a Agent machine's Agent configuration.

Network Statistics Shows a list of applications that have accessed the network and the packet size of the information exchanged during the network access session. The time of the exchange is also listed.

Alert Log List out all the email alerts issued against the selected machine.

Application Event Log, Security Log, System Log Shows the Event Log data collected by Windows. (Not available with Win9x)

Show me an explanation of the items on this page.

Agent Status gives a quick view of which Agent are online, who is currently logged onto that machine what IP address the machine is at, and the last time that machine was online (if it is currently offline). The following elements are displayed in the Agent Status function:

Machine.Group ID

Lists the Agent machines according to the Specify Accounts criteria.

Login Name

Username of the currently logged in user on this machine (if any).

Search... button

Clicking this button displays an alphabetized list of all currently logged on users for all machines. Use this function to quickly locate the machine a particular user is logged into at the moment. The table displays **Login Name**, **Machine ID**, **Contact Name**, and **Computer Name** for all machine accounts. Click any column header to resort the table alphabetically by that column's data.

IP Address

Lists the IP address in use by the Agent machine. The IP Info function in the Audit tab displays more in-depth IP information.

Last Check-in

Lists the date and time the Agent's Agent last performed a full or quick check-in to the System Server. If the last check-in time is twice as old or older than the quick check-in period, the date and time are displayed in red. This helps administrators troubleshoot potential Agent problems.

Also, if the password on the Agent machine doesn't match the password on the System Server, **Bad Password** is displayed. The administrator can correct this problem by reapplying the correct password on the Agent machine by accessing the **Set Account** function in the Agent icon menu.

Check-in status

The check-in status of the machines shown in the Agent machine list is indicated by the icon shown to the left of the Agent machine ID. The icons and their status are as follows:

OK **Agent has checked in**

🟨 **Agent has not recently checked in**

🟥 **Agent has never checked in**

Feature Tab > **Alerts**

The Alerts tab contains functions related to real time monitoring of all your managed machines.

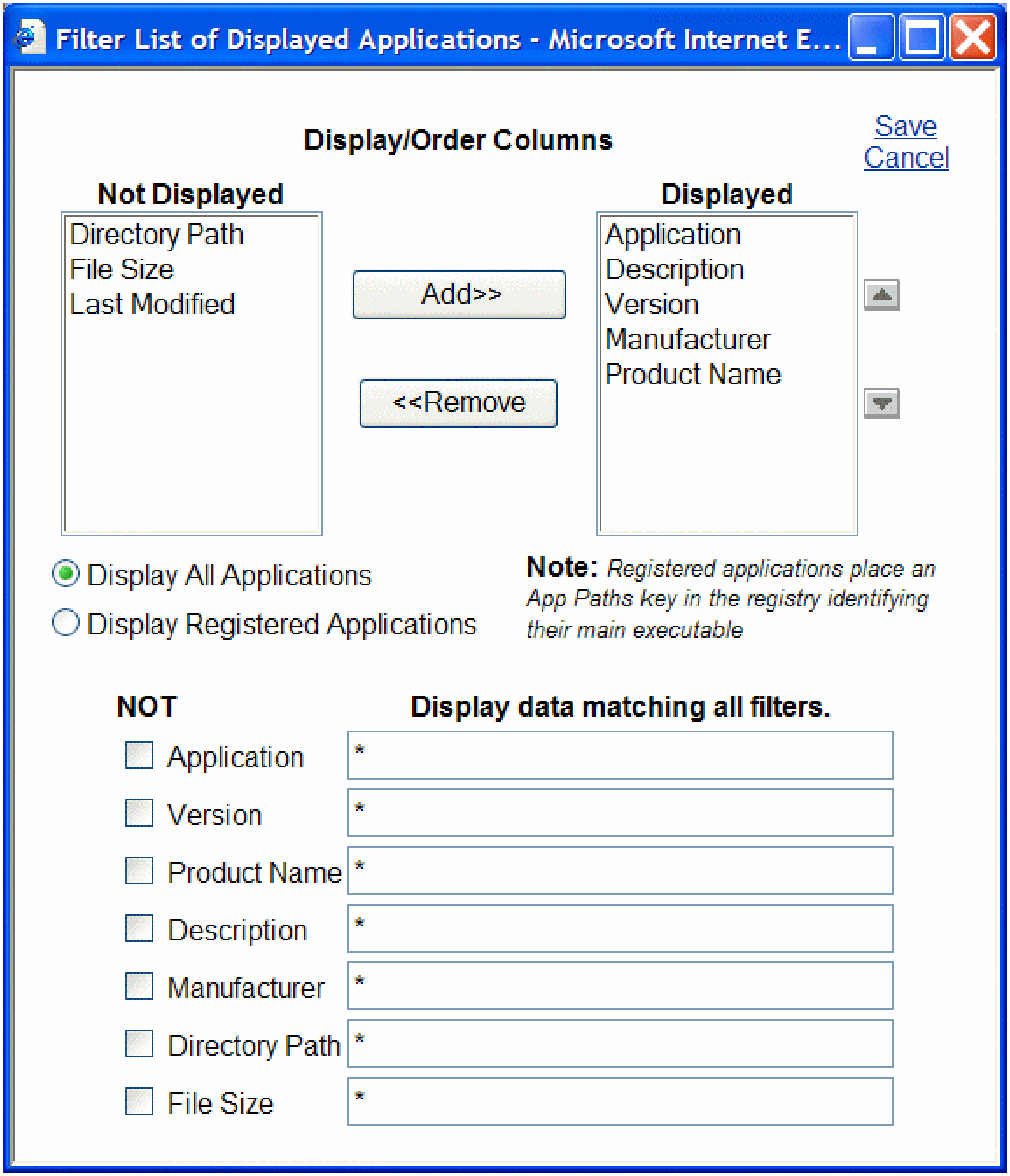
To access the Assistant, click Assistant from any function page.
The following functions are available in the Monitor feature tab:

Functions	Description
Alerts	Define email alerts on a per machine basis.
LAN Watch	Periodically poll a LAN and identify all new devices on that LAN
Install Agents	Remotely install agents on any machine discovered by LAN Watch that does not already have an agent.
View LAN	List devices discovered by LAN Watch
File Access	Allows administrators to set permissions on files and applications.
Network Access	Allows administrators to limit network access by selected applications on client machines.
Application Blocker	Prevents applications from running are target machines.

Application Filter

HELP HOME

The application filter provides a way to control the list of applications shown in the applications list. After entering the criteria you want displayed by adding it to the right pane, you can then narrow down your search by entering search parameters in the fields below.



Filter List of Displayed Applications - Microsoft Internet E...

Display/Order Columns

Not Displayed	Displayed
Directory Path	Application
File Size	Description
Last Modified	Version
	Manufacturer
	Product Name

● Display All Applications

○ Display Registered Applications

Note: *Registered applications place an App Paths key in the registry identifying their main executable*

NOT	Display data matching all filters.
□ Application	*
□ Version	*
□ Product Name	*
□ Description	*
□ Manufacturer	*
□ Directory Path	*
□ File Size	*

Remote Cntl > **Preinstall RC**

The remote control system automatically detects if either **WinVNC** or **RAdmin** is already installed on the target machine. If not, then the VSA automatically installs and starts the selected service for you. Automatic installation of remote control takes up to an extra minute the first time remote control is used. To **eliminate that first time delay**, you can pre-install remote control on any machine.

Note: Uninstalling the Agent will not remove the installed remote control package. Use Remove RC to uninstall remote control prior to deleting the agent.

Install

Clicking Install schedules a script to install either WinVNC or RAdmin to all selected machine IDs. WinVNC is installed on machines that are currently assigned WinVNC as their remote control package. RAdmin is installed on machines that are currently assigned RAdmin as their remote control package.

When an install is pending on any machine ID this page automatically refreshes every 5 seconds until the script completes.

Note: Preinstall RC will not install pcAnywhere or Terminal Server.

Cancel

Cancel pending install scripts for any selected machine IDs.

Last Status

Pending indicates the install will run the next time that machine checks into the VSA. Otherwise, this column displays the status and time of the last time install ran on that machine.

Assistant

HELP HOME

Show me an explanation of the items on this page.

How do I deploy the software vendor's install package?

Most vendors provide either a single file (when downloaded from the web) or set of files (when distributed on a CD). Executing the installer file (typically named **setup.exe or abc.msi**) installs the vendor's application on any operating system.

The Application Deploy wizard takes you though an interview process to determine the type of installer and automatically generates a script to deploy install vendor packages.

How do I find out what kind of installer my software vendor used?

The VSA provides a small utility to automatically identify all supported installer types. Download and run kInstId.exe to automatically identifies the installer type.

Information on creating custom scripts...

Information on creating silent install packages

Show me an explanation of the items on this page.

Patch Deploy is a wizard tool to automatically create a script to distribute and apply Microsoft patches.

What is the 6-digit article number?

Microsoft Publishes a vast assortment of information about its operating system in the **Microsoft Knowledge Base**. Each article in the Knowledge Base is identified with a 6-digit Q number (e.g. Q324096. All Microsoft patches have an associated knowledge base article number.

Entering the article number is optional. Leave it blank if you do not know it.

Should I send the patch from the VSA or execute it from a file share?

The patch needs to execute on the managed machine to install. The wizard generated script tells the remote machine where to get the patch file to execute. The Patch Deploy Wizard asks you in step 4 if you want to "Send the patch from the VSA server to the remote machine and execute it locally" or "Execute the patch from a file share on the same LAN as the remote machine."

Pushing the patch down to each machine from the VSA may be bandwidth intensive. If you are patching multiple machines on a LAN no internet bandwidth is used to push out the patch. Each machine on the LAN can execute the patch file directly from a common file share.

Information on creating custom scripts...

Monitor > **Define SNMP Set**

This operation allows the user create and modify all components of a SNMP Set. This is where the user will name the set as well as select all the MIB (SNMP Management Information Base) Objects that the user wants to monitor with this set. **A SNMP Set should be used as a logical collection of things to monitor. A logical grouping, for example, could be to monitor all the pertinent MIB Objects for the CISCO 1700.**

Note: Certain Command Line functions from Net-SNMP suite of applications are used to implement SNMP v1, SNMP v2c retrieval of information from SNMP capable devices in accordance with all pertinent copyright requirements.

Note: Sample SNMP Sets can be loaded from the System->Configure function .

SNMP Set Name

Name the SNMP Set in such as way that it is identifiable when presented in the SNMP Set list.

SNMP Set Description

Allows the user a more verbose method of describing the monitor set. **The rationale for the creation of the set is meaningful here; the reason for the creation of the set is sometimes lost over time.**

Group Alarm Column Name (Drop down list)

Select which column header in the Group Alarm Status view (View Console) that the Alarms generated by this SNMP Set will be associated with (red light indicator)

Automatic Deployment to (Drop down list)

The user can select to have this SNMP Set automatically deployed to this type of SNMP Device when discovered by the LAN Watch function.

Share (button)

If the current user is the owner of the SNMP Set, the Share button is available and opens a dialog that allows sharing this SNMP Set with others.

Take Ownership (link)

If the current user is NOT the owner, but is a master administrator, then the Take Ownership link allows the ownership to be transferred (and logged) to current user.

Save (button)

Allows the user to save any changes to the SNMP Set Name, Description, Automatic Deployment or Group Alarm Column.

Save As (button)

Allows the user to make a copy of the current SNMP Set under another name.

Delete (button)

Allows the user to delete, with confirmation, the entire SNMP Set (including all associated Counters, Processes and Services).

Export (link)

Opens a dialog that will allow the user to export, in an XML format, a representation of the SNMP Set to be imported at a later date and likely on a different system.

SNMP Sets (tab)

Select to view all the MIB Objects associated to this SNMP Set. Select the **VCR buttons ('<<> and ">>")** to page through the list of SNMP Objects. Select the **Delete Icon** to remove the selected MIN Object, with confirmation, from the SNMP set.

Select the **Edit Icon** to open the detail of the MIB Object in an **edit mode**.

In **Edit Mode,** a Wizard-like presentation leads the user through the six steps of adding or editing a MIB Object:

1. Add the MIB Object, SNMP Version, SNMP Instance combination required by the SNMPGet Command.
    - **MIB Object** - Select the MIB Object. **Add Object** (button) allows the user to immediately add a MIB Object that currently does not exist via the Monitor Lists feature.
    - **SNMP Version**- Select a SNMP Version that the SNMP Device supports for this MIB Object.
    - **SNMP Instance**- Enter the interfaces of the SNMP Table or '0' if just a single result value for the SNMP Device. If there are many interfaces to enter, the user can enter common range indicators, such as 1-5,6 or 111,113,115. **If the user is not sure what interface numbers are valid for a particular SNMP Device, go to the Script feature and select the KSNMPWALK script: enter the appropriate Community Name and IP address; then schedule it to execute on the machine that was set up for SNMP activyt (via SNMP Community and LAN Watch functions). The script will return the ifEntry table information of the MIB II. It will indicate all the interfaces that are responding on that SNMP Device.**
    - **Value Returned as** - If the value returned by this MIB Object is a number, the user has the option to return this value as a Total or a Rate Per Second.
2. Name and describe the Monitor Counter.
    - **Name** - A short name to recognize the SNMP Set in a list
    - **Description** - This is an opportunity to describe the detail of the monitor levels.
3. Collection Threshold. The user selects the collection threshold of the returned counter values. This is the opportunity to not collect unwanted log data. If the user only wants to see and report upon data values over or under a certain threshold, they would set those values here.
    - **Collection Operator** - Select the over, under, equal or not.
    - **Collection Threshold** - Set the level at which the agent will begin to return log data.
    - **Sample Interval** - This defines how frequently the data will be sent up from agent.
4. Alarm Threshold. The user can set the point at which the returned values will generate an Alarm.
    - **Alarm Operator** - Select the over, under, equal or not
    - **Alarm Threshold** - Set the level at which the agent will begin to return log data.
    - **Duration** - This setting tells the server to look back over this defined period and if all values exceed this Alarm Threshold, the Alarm will be generated. Many Alarm conditions are only alarming if the level is sustained over a long period of time.
    - **Ignore additional alarms for** - This tells the server to generate only one Alarm for this time period. **This successfully reduces the confusion of many alarms for the same issue.**
5. The user can set a percentage value that will allow the logs to indicate via a yellow flag (see Monitor Icons later in this help page) data that is within that percentage of the Alarm Threshold
6. Allows the user to turn on a Trending mode. Allowing a Trending Alarm to be generated if, based on historical data, the Alarm Threshold will be reached within the Trending Window
    - **Trending Active?** - Not all values make sense to trend, but if the user selects 'yes', a linear regression will periodically run on log values for this counter. If there is indication that the Alarm Threshold will be met within the Trending Window, a Trending Alarm will be generated
    - **Trending Window** - Set this time period to the amount of time that the user needs to prepare for a certain Alarm condition. For Example, the user may want 10 days notice that the hard drive will reach Alarm condition, to accommodate ordering, shipping and installing a larger hard drive.
    - **Ignore additional trending alarms for** - tells the server to generate only one Alarm for this time period.

Next (Button)

Will move the user to the next wizard page

Previous (Button)

Will move the user back to the previous wizard page

Cancel (Button)

Ignore any changes and return to the Counter Thresholds list.

Save (Button on the last page of the wizard)

Save changes.

Monitor Icons (tab)

This process allows the user to associate different monitor icons to the different presentation possibilities (Alarm, Warning, Trending,etc.). This allows certain monitor sets to be more visible (important) with bigger or flashing icons.

Select Image for 'OK' Status - The default icon is a green traffic light. The user can select from an existing list or import their own.

Select the Image for 'Alarm' Status - The default icon is a red traffic light. The user can select from an existing list or import their own.

Select Image for 'Warning' Status - The default icon is a yellow traffic light. The user can select from an existing list or import their own.

Select the Image for 'Trending' Status - The default icon is a orange traffic light. The user can select from an existing list or import their own.

Select the Image for 'Not Deployed Status - The default icon is a grey traffic light. The user can select from an existing list or import their own.

Save (button) - Save the changes that have been made to the Monitor Icons.

Upload new Monitor Icons (link) - Select and upload additional graphics to choose from. Once a new graphic has been uploaded it is available in all the status icon 'drop down' lists.

Restore Defaults (button) - Restores ALL the Monitor Icons associated to this SNMP Set back to their defaults.

HELP HOME

Monitor > **Define Monitor Set**

This operation allows the user create and modify all components of a Monitor Set. This is where the user will name the set as well as select all the Counters and/or Services and/or Processes that the user wants to monitor with this set. **A Monitor Set should be used as a logical collection of things to monitor. A logical grouping, for example, could be to monitor all the counters and services integral to running an Exchange Server.**

Note: Sample Monitor Sets can be loaded from the System->Configure function .

Monitor Set Name

Name the Monitor Set in such as way that it is identifiable when presented in the Monitor Set list.

Monitor Set Description

Allows the user a more verbose method of describing the monitor set. **The rationale for the creation of the set is meaningful here; the reason for the creation of the set is sometimes lost over time.**

Group Alarm Column Name (Drop down list)

Select which column header in the Group Alarm Status view (View Console) that the Alarms generated by this Monitor Set will be associated with (red light indicator)

Share (button)

If the current user is the owner of the Monitor Set, the Share button is available and opens a dialog that allows sharing this Monitor Set with others.

Take Ownership (link)

If the current user is NOT the owner, but is a master administrator, then the Take Ownership link allows the ownership to be transferred (and logged) to current user.

Save (button)

Allows the user to save any changes to the Monitor Set Name, Description or Group Alarm Column.

Save As (button)

Allows the user to make a copy of the current Monitor Set under another name.

Delete (button)

Allows the user to delete, with confirmation, the entire Monitor Set (including all associated Counters, Processes and Services).

Export (link)

Opens a dialog that will allow the user to export, in an XML format, a representation of the Monitor Set to be imported at a later date and likely on a different system.

Counter Thresholds (tab)

Select to view all the counters associated to this monitor set. Select the **VCR buttons ('<<> and ">>")** to page through the list of Counters. Select the **Delete Icon** to remove the selected counter, with confirmation, from the monitor set.

Select the **Edit Icon** to open the detail of the counter in an **edit mode**.

In **Edit Mode,** a Wizard-like presentation leads the user through the six steps of adding or editing a counter:

1. Add the Object/Counter and Instance combination required by the PerfMon interface. **The selection of the Object drop down list will re-populate the Counter and Instance drop down lists.**
    - **Object** - Select the Counter. **Add Object** (button) allows the user to immediately add a object that currently does not exist via the Monitor Lists feature.
    - **Counter** - Select a related Counter. **Add Counter** (button) allows the user to immediately add a counter that currently does not exist via the Monitor Lists feature.

- **Instance** - Not all Counter Objects have related Instances . **Add Instance** (button) allows the user to immediately add a instance that currently does not exist via the Monitor Lists feature.

2. Name and describe the Monitor Counter.
   - **Name** - A short name to recognize the Monitor Set in a list
   - **Description** - This is an opportunity to describe the detail of the monitor levels.
3. Collection Threshold. The user selects the collection threshold of the returned counter values. This is the opportunity to not collect unwanted log data. If the user only wants to see and report upon data values over or under a certain threshold, they would set those values here.
   - **Collection Operator** - Select the over, under, equal or not.
   - **Collection Threshold** - Set the level at which the agent will begin to return log data.
   - **Sample Interval** - This defines how frequently the data will be sent up from agent.
4. Alarm Threshold. The user can set the point at which the returned values will generate an Alarm.
   - **Alarm Operator** - Select the over, under, equal or not
   - **Alarm Threshold** - Set the level at which the agent will begin to return log data.
   - **Duration** - This setting tells the server to look back over this defined period and if all values exceed this Alarm Threshold, the Alarm will be generated. Many Alarm conditions are only alarming if the level is sustained over a long period of time. **For example, CPU utilization above 95% is only concerning it that level is maintained for a duration of 10 minutes.**
   - **Ignore additional alarms for** - This tells the server to generate only one Alarm for this time period. **This successfully reduces the confusion of many alarms for the same issue.**
5. The user can set a percentage value that will allow the logs to indicate via a yellow flag (see Monitor Icons later in this help page) data that is within that percentage of the Alarm Threshold
6. Allows the user to turn on a Trending mode. Allowing a Trending Alarm to be generated if, based on historical data, the Alarm Threshold will be reached within the Trending Window
   - **Trending Active?** - Not all values make sense to trend, but if the user selects 'yes', a linear regression will periodically run on log values for this counter. If there is indication that the Alarm Threshold will be met within the Trending Window, a Trending Alarm will be generated
   - **Trending Window** - Set this time period to the amount of time that the user needs to prepare for a certain Alarm condition. For Example, the user may want 10 days notice that the hard drive will reach Alarm condition, to accommodate ordering, shipping and installing a larger hard drive. more info ...
   - **Ignore additional trending alarms for** - tells the server to generate only one Alarm for this time period.

Next (Button)
Will move the user to the next wizard page

Previous (Button)
Will move the user back to the previous wizard page

Cancel (Button)
Ignore any changes and return to the Counter Thresholds list.

Save (Button on the last page of the wizard)
Save changes.

Services Check (tab)
Select to view all the Services associated to this monitor set. Select the **VCR buttons ('<<> and ">>")** to page through the list of Services. Select the **Delete Icon** to remove the selected counter with confirmation from the monitor set.

Select the **Edit Icon** to open the detail of the counter in an edit mode.

Service - The user will select the service from the drop down list that will be monitored for stopping.

Description - Describe the service and the reason for monitoring.

Restart Attempts - Tell the system how many times it should restart.

Restart Interval - Tell the system how long to wait between attempts. Certain services need more time to try to start.

Ignore additional alarms for - tells the server to generate only one Alarm for this time period.

Save (Button)
Save changes.

Cancel (Button)
Ignore any changes and return to the Services Check list.

Process Status (tab)

Select to view all the counters associated to this monitor set. Select the **VCR buttons ('<<> and ">>")** to page through the list of Counters. Select the **Delete Icon** to remove the selected counter with confirmation from the monitor set.

Select the **Edit Icon** to open the detail of the counter in an edit mode.

Process- The user will select the Process from the drop down list that will be monitored.

Description - Describe the service and the reason for monitoring.

Alarm on Transition - Tell the system to Alarm as the process (application) transitions 'up' or 'down'.

Ignore additional alarms for - tells the server to generate only one Alarm for this time period.

Save (Button)
Save changes.

Cancel (Button)
Ignore any changes and return to the Process Status list.

Monitor Icons (tab)

This process allows the user to associate different monitor icons to the different presentation possibilities (Alarm, Warning, Trending,etc.). This allows certain monitor sets to be more visible (important) with bigger or flashing icons.

Select Image for 'OK' Status - The default icon is a green traffic light. The user can select from an existing list or import their own.

Select the Image for 'Alarm' Status - The default icon is a red traffic light. The user can select from an existing list or import their own.

Select Image for 'Warning' Status - The default icon is a yellow traffic light. The user can select from an existing list or import their own.

Select the Image for 'Trending' Status - The default icon is a orange traffic light. The user can select from an existing list or import their own.

Select the Image for 'Not Deployed Status - The default icon is a grey traffic light. The user can select from an existing list or import their own.

Save (button) - Save the changes that have been made to the Monitor Icons.

Upload new Monitor Icons (link) - Select and upload additional graphics to choose from. Once a new graphic has been uploaded it is available in all the status icon 'drop down' lists.

Restore Defaults (button) - Restores ALL the Monitor Icons associated to this Monitor Set back to their defaults.

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Copyright (c) 2003-2005, Sparta, Inc

All rights reserved.

Copyright (c) 2004, Cisco, Inc and Information Network
Center of Beijing University of Posts and Telecommunications.
All rights reserved.

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003
oss@fabasoft.com
Author: Bernhard Penz

HELP HOME

Monitor > **SNMP Type**

The **SNMP Type** page allows you to edit the type of SNMP devices that have been discovered via the LAN Watch. The type of the device will determine how it is graphically represented in the SNMP Topology report. You can also give individual SNMP devices custom names and descriptions as well as remove the device from your database.

Assign

Applies the selected type to each selected (checked) SNMP device.

Delete

Removes the selected SNMP devices from your database. If the device still exists it will be re-added to the database the next time a LAN Scan is performed. This is useful if a device's IP or MAC Address changes.

Name

List of SNMP devices generated for the specific Mahcine ID by the LAN Watch function.

Type

The type the SNMP device is currently assigned to.

Custom Name

The custom name and custom description given to the SNMP device. If a device is given a custom name, this name will appear instead of the SNMP name or IP Address in alarms, and when selecting the device in the SNMP Log. To change the custom name click on the icon next to the custom name. A text box will appear. Enter the desired name and press [Enter]. You can change the custom description the same way. It is possible to modify multiple custom names or descriptions at once, however only the one that the cursor is in when [Enter] is pressed will be saved.

Device IP

IP Address of device.

MAC Address

MAC Address of device.

SNMP Name

SNMP Device information.

HELP HOME

Monitor > **Trending**

This operation allows the user to chose certain counters to perform a linear regression upon. Certain monitor sets are very predictable in nature due to the systematic nature of their usage; disk utilization would be a good example.

Trending Window -

The operative value set from the 'Define Monitor Set' page is the Trending Window. This window of time is used to predict whether the Alarm Threshold value will be met during this time frame. As an example; the System Administrator set this value to predict (using linear regression) whether the disk will hit the alarm level within this 'trending Window'.

Note: The trending algorithm will run every hour, so a trending window of less than one hour will not achieve desired results.

Patch Mgmt > **Exclude Machines**

Apply Updates list patches missing from all machines. This function removes patches reported a missing from the selected machines, from the Apply Update summary list.

Exclude

Check the box to the left of all machines you wish to exclude for the Apply Update summary list.

Note: Machines set for Automatic Update are already excluded from the Apply Update list.

Include

Check the box to the left of all machines you wish to include for the Apply Update summary list.

HELP HOME

Ticketing > **Delete / Archive**

You may reach the point where your system has so many old tickets that they are cluttering up searches with obsolete data. Use the Delete/Archive function to eliminate old tickets, tickets in a particular category, or of a particular status.

In addition to delete, you can also **archive** tickets. Archived tickets stay in the database but are moved to separate tables. Use archive to move obsolete or old tickets out of the active database *without* deleting them from the system.

NOTE: You can always move tickets back and forth between into the active database table and the archive database table.

Filter

Select the tickets to view using the same technique described in View Summary. The filter settings restrict the tickets displayed in the list.

Hide tickets last modified after

Use this date control to list only tickets last modified after the specified date. If you want to archive **Closed** tickets older than 6 months perform the following steps.

- Select **Closed** from the Status control
- Set the date control to 6 months ago
- Click the **Set** button
- Click the **Select All** link
- Click the **Archive...** button.

Display archived tickets instead of active tickets

Check this box to search and examine the archived tickets. You can move tickets back to the active table here using the **Restore...** button

Why can't I delete a ticket?

Master administrators may disable ticket delete and edit privileges for users and standard administrators. See Access Policy.

Index