Remote Control

Table of Contents:

◊ Desktop Control
◊ Configure
◊ Notification Policy
◊ Files/Processes
◊ Message with Users
◊ vPro
Release Notes

Kaseya 6.2.0.0

- Remote Control SSH - Remote Control > SSH page runs an SSH session to connect to Linux and Mac machines. This feature is similar to Remote Control > FTP. Some of the screenshots in this module may not include this feature.
Introduction

System administrators frequently need to directly work on the computers they manage to perform a variety of services such as troubleshooting, installing software systems, downloading files, and so on. This needs direct work on computers that are otherwise utilized by their users. However, direct access to computers must be performed without negatively impacting the productivity of users. In addition not all such computers are located in the same location making it even more difficult for the IT personnel to reach to each computer promptly. Clearly, as the number of computers increases, this extremely inefficient process of on-site maintenance becomes prohibitively expensive, both in terms of required man power and loss of productivity as the users usually remain idle while the maintenance work is being performed. What is needed is a way to facilitate a remote access to computer that is quick, secure and non-intrusive.

Kaseya’s Remote Control module provides this needed facility by allowing you to view and operate managed machines as if they were right in front of you simply by clicking its machine ID. The Remote Control module enables you to:

- Automatically connect the user to the remote computer independent of any gateway or firewall configurations, even for computers behind NAT.
- Remote control even without an agent using video streaming.
- Work independently or with the user to solve problems interactively where both parties can see what is happening in real time (i.e., remote screen sharing).
- Set policies that allow users to block remote control or require users to ask permission before accessing a machine.
- FTP to any managed machine and access files even behind NAT gateways and firewalls.
- Direct chat with any managed machine, which is suitable for supporting dial-up users with only a single phone line. Remote control and chat can be performed at the same time.
- Power up, power down, bootup or reboot vPro-enabled machines.
- Use Live Connect to perform tasks and functions solely for one managed machine. Live Connect is an integral part of the Kaseya IT Automation Framework that allows a short cut method to perform many of the core IT maintenance activities including: deployment, configuration, execution, update, logging, reporting, monitoring and remediation. These functions are part of the core tasks that an IT professional performs on a daily basis. The details of Live Connect is described in section 4.5.3.

Kaseya’s Remote Control module is lightweight and forms its own, completely secure TCP connection with the server, without the need for address management, implementation of port mapping schemes at each site or the establishment of cumbersome VPNs.

4.1 Desktop Control

4.1.1 Control Machine

The Control Machine page establishes a remote control session between the user’s local machine and a selected machine ID. The remote control session can be established by one of the following third party remote control packages:
WinVNC, K-VNC and RAdmin, are all based on VNC technology. Virtual Network Computing (VNC), also called remote control or remote desktop, is a graphical desktop sharing system which uses the Remote Frame buffer (RFB) protocol to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction, over a network. It is included with the KServer primarily to provide immediate technical support. VNC is platform-independent. A VNC viewer on any operating system can usually connect to a VNC server on any other operating system. The VNC server is the program on the remote machine that shares its screen. The VNC client (or viewer) is the program on the local machine that watches and interacts with the remote machine. The VNC client machine requires user access rights to the VNC server machine. Since Kaseya VNC sessions are relayed through the KServer, all VNC sessions are protected by the Kaseya 256 bit rolling encryption protocol. The new K2 (Kaseya 2) supports peer-to-peer VNC sessions, removing the relay to KServer, which results in much faster remote sessions and eliminating the unnecessary load on the KServer and your network connection to internet, in case both VNC client and server machines are behind the same firewall.

VNC client and server components are normally installed automatically when a remote control session is initiated. If WinVNC, K-VNC or RAdmin are not installed on a machine and a remote control session is initiated using Remote Control > Control Machine then these packages are automatically installed without requiring a reboot. While this automatic installation is quick (usually under one minute). This delay can be eliminated during first time use by pre-installing WinVNC, K-VNC, or RAdmin on any managed machine using Remote Control > Preinstall RC.

ActiveX Control
An ActiveX control automatically configures and runs the remote control or FTP package for you. The first time you use any remote control or FTP package on a new machine, your browser may ask if it is OK to download and install this ActiveX control. Click Yes when asked. If the ActiveX control is blocked by the browser from running, the user is presented with a link to manually download and run the remote control package manually.

Helper Applications
In setting up a remote control or FTP session, gateway and port blocking problems are eliminated by always initiating outbound connections from both the target machine and the user machine. Helper applications, unique to each supported remote control or FTP package, automatically determine the optimal routing path between the VSA user machine and the remote machine. If a direct connection is not possible then the helper applications route the remote control traffic through the KServer on the same port used by agents to check-in (default 5721).

**Remote Control Malfunctions**

Reasons for remote control failure for target machines with and without an agent are:

1. The remote machine is blocking outbound traffic on the agent check-in port (default 5721). The firewall may need to be reconfigured.
2. The remote machine is on a slow connection. Let the applications run longer than the timeout period and see if that works.
3. Anti-virus software on the remote machine may block the connection. This problem is eliminated if Kaseya Endpoint Security protection is installed on the remote machine.
4. Wrong primary KServer address - Remote control can only connect through the primary KServer address. Machines with an agent can connect through either the primary or secondary address. Verify the remote machine can see the primary KServer address using Agent > Check-in Control.
5. XP supports only one RDP/Terminal Service session on the target machine and logs off other users. Starting a remote logon session from a second machine logs off the first remote logon session. The VSA uses the port relay to get through firewalls and gateways. To Windows XP, it appears as if the RDP session is connecting from the localhost.
6. The pcAnywhere viewer is connecting to your local machine, not the remote machine. The KServer 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.
7. pcAnywhere presents an error dialog saying cannot find callhost file: C:\Document and Settings\All Users\Application Data\Symantec\pcAnywhere\Network.CHF. There is no Network remote control item configured in pcAnywhere.

The figure below shows the generic view of the Control Machine page (Fig. 4.1). The functions available are listed below.
1. **Machine.Group ID:** The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view. Only machine IDs with a green or red icon can be connected to target machines and have live links; all others will be inactive. Clicking the KServ-er link starts a remote control session to the KServer itself. Use this feature to remotely manage your own KServer. Only master role users can remotely control the KServer.

2. **Current User:** The user currently logged on to the managed machine.

3. **Active Admin:** The VSA user currently working on this machine ID via a remote control session.

4. **Enable verbose relay:** Remote control or FTP of machines behind firewalls and NAT gateways may be relayed through the VSA server using a helper application. Checking this box displays a popup window with status information about the normally hidden helper application.

### 4.1.2 Video Streaming

The **Video Streaming** (Fig. 4.2) page allows you to establish a remote control session between the VSA user’s local machine and a machine without an agent. It can be used to help someone quickly on an infrequent basis.

For Video Streaming, the following conditions apply:

- The remote user must log into a URL after the user has started the video streaming session.
- The remote user must have administrator privileges on the local machine.
- Each VSA user can only initiate a single video streaming session at a time.

**Note:** Use Remote Control > Control Machine to remote control a target machine that has an agent.

If WinVNC, K-VNC or RAdmin are not installed on a machine and a remote control session is initiated using Video Streaming, then these packages are automatically installed. Installation does not require a reboot. When either side terminates the Video Streaming session, the remote server on the target machine uninstalls automatically, removing all remote control files and registry additions.

The generic view of the Video streaming page is shown in Fig. 4.2 below. The operations that are supported in this page are listed and explained below.

---

**Fig. 4.2:** Video Streaming
1. **Start**: The Start button allows you to initiate a video streaming session with the remote user. Provide the remote user the following link: “http://<yourKServerURL>/gethelp.asp” (e.g., http://kaseya2.cs.fiu.edu/gethelp.asp) and request them to click your user name to begin the video streaming session. Once the remote user chooses your name, the video streaming session can begin in a vnc or RAdmin window that is automatically popped on your screen.

2. **Enable verbose relay**: Remote control or FTP of machines that are behind firewalls and NAT gateways may be relayed through the VSA server using a helper application. Checking this box displays a popup window with status information about the normally hidden helper application.

3. **Select remote control package to use**: The default remote control service uses WinVNC. See Remote Control > Select Type for a description of the different types of remote control packages.
   - WinVNC
   - K-VNC
   - RAdmin

4. **Specify the default HTML message seen by users when no administrator is waiting to help**: This is the message displayed to the remote users when there are no administrators available for assistance. This is displayed when the remote user clicks the http://<yourKServerURL>/gethelp.asp web page. After making changes to this message, click the Apply button to save it. Click Default to reset the message back to its default setting.

### 4.1.3 Reset Password

The **Reset Password** page (Fig. 4.3) changes the password for a user and, if necessary, creates a new user account on a managed machine. It can also change domain user accounts on domain name controllers. 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 that is already being used by a user account. Blank passwords are not permitted.

**Resetting the User Password**

Reset Password can be used to reset the user password for a local account on one of the managed computers or a domain account as needed. A user password can only be changed by going to the machine where the account resides, in other words, a local account can be changed only on its respective local machine and a domain account can be changed only on its respective domain controller.

Among other reasons, the change might be needed because:

- Your user password is compromised.
- Someone leaves your organization who knew the user password.
- It is time to change the user password as part of a good security policy.

Fig. 4.3 below shows the Reset password page. The functions supported by this module are listed on the next page.
Chapter 4 - Remote Control

1. **Apply**: Click *Apply* to apply password and user account parameters to selected machine IDs.

2. **Cancel**: Click *Cancel* to clear pending password changes and user account creations on selected machine IDs.

3. **Username**: Enter the username on the managed machine.

4. **Create new account**: Check this box to create a new user account on the managed machine.

5. **As Administrator**: Check this box to create the new user account with administrator privileges.

6. **Password / Confirm**: Enter a new password.

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

8. **Status**: The status of pending password changes and user account creations.

4.2 Configure

4.2.1 Select Type

The **Select Type** page specifies which remote control package is used by **Remote Control > Control Machine** to remote control a managed machine. You can assign different packages to different machines. Each machine ID displays the icon of the remote control package it is currently assigned to use.

Assign Remote Control Packages to Machine IDs

1. Select the type of package to use from the drop-down list. (See Fig. 4.4)

2. Check the box to the left of machine IDs you want to use this remote control package.

3. Click the *Select* button.
Ensure the list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

4.2.2 Set Parameters

The Set Parameters page sets the default parameters for your remote control session. These settings are remembered on a per VSA user basis. Changes take effect immediately and are reused every time you start remote control.

Fig. 4.5 below shows the generic view of the Set Parameters page. The options supported on this page are listed and explained below.
1. WinVNC and K-VNC Options

- **View Only Mode** - You can view the remote machine. No mouse or keyboard events are sent to the remote machine.

- **Hide WinVNC system tray icon on the remote machine** - Check this box to hide the WinVNC icon on the remote machine.

- **Restrict to 64 colors** - The display is set to 64 colors. This is useful for slower connections.

- **Full Screen mode** - The entire display of your local machine is used to display the screen contents of the remote machine. Exit by displaying the remote control menu (default F8) and unselect *Full screen*.

2. RAdmin Options

- **Full Control** - You can view and/or control the screen keyboard and mouse of the remote machine.

- **View Only** - You can view the remote machine. No mouse or keyboard events are sent to the remote machine.

- **File Transfer** - Start a file transfer (FTP) session with the remote machine. This mode presents you with two standard file browsers, one for the remote machine and one for your local machine. Drag and drop files between the two machines in this mode.

- **Full Screen View Mode** - The entire display of your local machine is used to display the screen contents of the remote machine. This option is only available for Full Control or View Only sessions.

- **Encrypt Data Stream** - Checking this box encrypts all traffic between your local machine and the remote machine.

- **Updates/sec** - Sets the maximum number of updates per second RAdmin generates. Higher update rates consume more CPU cycles on the remote machine.

- **Color Format** - Specifies the number of colors used for remote control. Large color formats use more bandwidth.

3. RDP Options

- **Console mode** - Remote control the console session of the remote machine.

- **Full Screen mode** - Use your full screen to remote control the remote machine.

- **Fixed Screen size** - Set a fixed width and height for your remote control session.

- **Share Disk Drives** - Connect your disk drives to the remote machine.

- **Only share the following disks** - Enter the specific drive letters to share, or leave blank to share all disks.

- **Share Printers** - Connect your printers to the remote machine.

- **Disable Desktop Wallpaper** - Turn off wallpaper on the remote machine for faster processing.
4.2.3 Preinstall RC

The Preinstall RC page (Fig. 4.6) installs WinVNC, K-VNC or RAdmin on selected machine IDs without initiating a remote control session. Select the type of package to remote control a managed machine using Remote Control > Select Type. When an install is pending on any machine ID, this page automatically refreshes every 5 seconds until the installation process completes.

Note: Preinstall RC does not install pcAnywhere or RDP.

1. **Install:** Click *Install* to install WinVNC, K-VNC or RAdmin on selected machine IDs.
2. **Cancel:** Click *Cancel* to clear pending install procedures for selected machine IDs.
3. **Last Status:** Pending indicates the install will run the next time that machine checks into the KServer. Otherwise, this column displays when the remote control package was installed on the machine ID.

Steps to install a remote control package PreInstall RC

1. Select the type of package to remote control a managed machine using Remote Control > Select Type and click *Select*.
2. Select the machine ID of your choice on PreInstall RC page.
3. Click *Install*.

4.2.4 Uninstall RC

The Uninstall RC page (Fig. 4.7) uninstalls WinVNC, K-VNC or RAdmin on selected machine IDs. Multiple types of remote control packages may be installed on a single machine ID. Select the type of package to uninstall from a managed machine using Remote Control > Select Type. When an uninstall is pending on any machine ID, this page automatically refreshes every 5 seconds until the procedure completes.

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 Uninstall RC on that machine ID cleans out any existing installation problem. A fresh copy of the remote control package is installed the next time a remote control session is started or using Remote Control > Preinstall RC.
**Note:** Uninstalling an agent does not remove the installed Remote Control package. Before you delete the agent, use Remote Control > Uninstall RC to uninstall remote control on the managed machine. Uninstall all add-on module clients as well.

**Automatic Uninstallation**

Uninstall RC is not required for Video Streaming. When either side terminates the Video Streaming session, the remote server on the target machine uninstalls automatically, removing all remote control files and registry additions.

The generic view of the Uninstall RC page is shown in Fig. 4.7 below. The functions supported on this page are listed and explained below.

1. **Uninstall:** Click Uninstall to uninstall WinVNC, K-VNC or RAdmin on selected machine IDs.

2. **Cancel:** Click Cancel to clear pending uninstall procedures for selected machine IDs.

3. **Last Status:** Pending indicates the uninstall will run the next time that machine checks in to the VSA. Otherwise, this column displays when the remote control package was uninstalled on the machine ID.

### 4.3 Notification Policy

#### 4.3.1 User Role Policy

The User Role Policy page (Fig. 4.8) allows you to specify how remote users should be notified that a remote control session to their machine is about to begin. Policies are applied by System > User Security > User Roles.
1. **Select User Notification Type**

   - **Silently take control** - This option allows you to take control of the machine without informing the user. Control can be taken immediately and silently.

   - **If user logged in display alert** – This option allows you to display an alert before taking control of the machine. The alert text can be edited in the text box below this option.

   - **If user logged in ask permission** – This option allows you to ask the user if it is alright to begin a remote control session. The *Ask Permission text* can be edited in the text box below this option. Remote control cannot proceed until the user clicks the *Yes* button. If nothing is clicked after one minute, *No* is assumed and the VSA removes the dialog box from the target machine. If no user is logged in, proceed with the remote control session.

   - **Require Permission. Denied if no one logged in** – This option allows you to ask the user if it is alright to begin a remote control session. The *Ask Permission text* can be edited in the text box below this option. Remote control cannot proceed until the user clicks the *Yes* button. If nothing is clicked after one minute, *No* is assumed and the VSA removes the dialog box from the target machine. The remote control session is cancelled. This option is the same as above, but if the user is not logged in, the permission for the remote control session is denied.

2. **Apply**: Click *Apply* to apply policy parameters to selected machine IDs.

3. **Notify user when session terminates**: Check this box to notify the user when the session terminates.

4. **Session Termination Message**: Displays only if the *Notify user when session terminates* box is checked. Modify the default message if necessary. The `<admin>` variable is the only variable that can be used in this message.

5. **Notification Alert Text / Ask Permission Text**: This text box is displayed only if the *Select User Notification Type* is not *Silently take control*. Modify the default message if necessary. The `<admin>` vari-
able is the only variable that can be used in this message.

6. **Remove**: Click Remove to clear policy parameters from selected machine IDs.

7. **Require admin note to start remote control**: Click this box to require VSA users to enter a note before starting the remote control session. The note is included in the remote control log and is not displayed to the machine user.

8. **Role Name**: This column displays the list of user roles that are available.

9. **Policy**: This column displays the remote control policy applied to a user role.

10. **Message**: The text messages applied to a user role is displayed in this column.

Clicking the delete icon next to a user role will clear the policy and clicking a row’s edit icon to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

### 4.3.2 Machine Policy

The **Machine Policy** page (Fig. 4.9) allows you to specify remote users should be notified that a remote control session to their machine is about to begin. This policy is applied to **machine IDs**.

Fig 4.9 shows the Machine Policy page and all the functions that this module provides.

1. **Select User Notification Type**
   - **Silently take control** - Do not tell the user anything. Take control immediately and silently.
   - **If user logged in display alert** - Display notification alert text. The alert text can be edited in the text box below this option.
   - **If user logged in ask permission** - Ask the user if it is alright to begin a remote control session. The ask permission text can be edited in the text box below this option. Remote control cannot proceed until the user clicks the **Yes** button. If nothing is clicked after one minute, **No** is assumed and the VSA removes the dialog box from the target machine. If no user is logged in, proceed with the remote control session.
   - **Require Permission. Denied if no one logged in** - Ask the user if it is alright to begin a remote control session. The ask permission text can be edited in the text box below this option. Remote control cannot proceed until the user clicks the **Yes** button. If nothing is clicked after one minute, **No** is assumed.
and the VSA removes the dialog box from the target machine. The remote control session is cancelled.

2. **Apply:** Click **Apply** to apply policy parameters to selected machine IDs.

3. **Notify user when session terminates:** Check this box to notify the user when the session terminates.

4. **Session Termination Message:** Displays only if the **Notify user when session terminates** box is checked. Modify the default message if necessary. The `<admin>` variable is the only variable that can be used in this message.

5. **Notification Alert Text / Ask Permission Text:** Displays only if the **Select User Notification Type** is not Silently take control. Modify the default message if necessary. The `<admin>` variable is the only variable that can be used in this message.

6. **Remove:** Click **Remove** to clear policy parameters from selected machine IDs.

7. **Require admin note to start remote control:** Click this box to require VSA users to enter a note before starting the remote control session. The note is included in the remote control log and is not displayed to the machine user.

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

9. **Policy:** The remote control policy applied to a machine ID.

10. **Message:** The text messages applied to a machine ID.

**Delete Icon:** Click the delete icon next to a machine ID to clear the policy.

**Edit Icon:** Click a row’s edit icon to populate header parameters with values from that row. You can edit these values in the header and re-apply them.

## 4.4 Files / Processes

### 4.4.1 FTP

File Transfer Protocol (FTP) is a commonly used protocol for exchanging files over any network that supports the TCP/IP protocol. The FTP server is the program on the target machine that listens on the network for connection requests from other computers. The FTP client is the program on the VSA user’s local machine that initiates a connection to the server. The FTP client machine requires user access rights to the FTP server machine. It is included with the KServer primarily to provide immediate technical support. Once connected, the client can upload files to the server, download files from the server, rename or delete files on the server and so on. Any software company or individual programmer is able to create FTP server or client software because the protocol is an open standard. Virtually every computer platform supports the FTP protocol. Since Kaseya FTP sessions are relayed through the KServer, all FTP sessions are protected by the Kaseya 256 bit rolling encryption protocol.

The **FTP** page establishes an FTP session between the user’s local machine and a selected machine ID. Once the FTP session is initiated, a new browser window pops up displaying the contents of a fixed disk on the managed machine. Just drag and drop files as you normally would.

**FTP Malfunctions**
Some reasons for FTP failure with managed machines are:

1. The user machine is blocking outbound traffic on the agent check-in port (default 5721). The firewall may need to be reconfigured.

2. The target machine is on a slow connection. Let the applications run longer than the timeout period and see if that works.

3. Anti-virus software on the target machine may block the connection. This problem is eliminated if KES Security protection is installed on the target machine.

4. Wrong primary KServer address - Remote control can only connect through the primary KServer address. Machines with an agent can connect through either the primary or secondary address. Verify the remote machine can see the primary KServer address using Agent > Check-in Control.

5. You accessed the KServer 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 KServer to Windows. Say you downloaded the helper application from www.yourKServer.net. Then you open a new browser and access the KServer by typing in its IP address 192.168.1.34. The KServer drops a cookie for 192.168.13.34 while the helper tries to get a cookie corresponding to www.youKServer.net. The helper won’t find the cookie. If this happens to you, just download a new helper application and try again.

Initiating FTP

FTP session can be initiated by clicking the name of the remote machine. Fig. 4.10 shows the screenshot of the FTP page. Select the machine ID that you want to establish an FTP session with. Icons next to the managed machine ID indicate the current connection status for that machine. Only machine IDs with an or icon can be connected to target machines and have live links; all others will be inactive.

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

2. FTP the KServer: Clicking the FTP the KServer link starts an FTP session with the KServer itself. This option is displayed only for master role users.

3. Enable verbose relay: Remote control or FTP of machines behind firewalls and NAT gateways may be relayed through the VSA server using a helper application. Checking this box displays a popup window with status information about the normally hidden helper application.

Enable / Disable the Machine User’s Ability to Initiate FTP Remotely: Users can enable / disable the machine user’s ability to initiate FTP remotely to their own machine from another machine using Agent >

After selecting the machine ID, we need to specify the drive letter for which the FTP session will be established. Fig. 4.11 shows the screenshot of the page that appears after selecting the machine ID. You can either select the remote fixed drive option (drive C) or specify another drive letter for the FTP session.

![Fig. 4.11: Select the drive letter to establish an FTP session](image)

Note: Remote Control > SSH page runs an SSH session to connect to Linux and Mac machines. This is a new feature on Kaseya and some of the screenshots may not include the new feature.

### 4.4.2 Task Manager

The Task Manager page (Fig. 4.12) performs the same function as Microsoft’s Windows NT/2000 task manager, except that it lists all currently active processes on all managed machines. Clicking the link of a machine ID tasks the agent on the managed machine to collect 10 seconds of process data at the next check-in. Task Manager displays the results in tabular form and it supports all Windows operating systems, Windows 95 and up.

**Kperfmon.exe**

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.exe may take about 4% of the CPU during the 10 seconds required to collect data.

**zmc**

Enable / Disable the Machine User’s Ability to Access Task Manager Remotely

Users can enable / disable the machine user’s access to Task Manager on their own machine remotely from another machine using Agent > Portal Access and System > Machine Roles.

To view the tasks running on a particular machine ID, select the machine ID. The tasks running on that machine ID will appear on the screen as shown in the Fig. 4.12. To end a process, select the process name by clicking on the checkbox next to it and click on *End Process.*
1. **Name**: The name of the process actively running on the managed machine.

2. **CPU**: The percent of CPU time consumed by that process over the 10 second data collection interval.

3. **Mem Usage**: The amount of main memory used by each active process.

4. **Threads**: The number of active threads associated with each active process.

5. **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.

### 4.5 Message with Users

#### 4.5.1 Chat

The **Chat** page initiates or continues chat sessions with logged on users on managed machines. Multiple chat sessions can be initiated at the same time. Each window title displays the machine ID name for that session. The system automatically removes all messages older than one hour.

To initiate a chat session click the machine ID of the machine you wish to start chatting with. A chat session window opens on your machine and a chat window opens in a browser on the remote machine. Enter text in the text pane. Click the **Send** button as show in the Fig. 4.13 to send the message.
To Respond to a Chat Session
If a chat popup window displays while you are logged on to the KServer, respond by entering text in the text pane. Click the Send button to send the message.

Join Session link
Multiple VSA users may participate in the same chat session with a machine user. If a chat session is in progress, the Join Session link displays 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.

Chatting with Other VSA Users
The names of logged on VSA users who belong to the organizations and group IDs currently displayed by the machine ID/group ID filter display on the Chat page as well. Click the link of another logged on VSA user to initiate a chat with that VSA user.

Enable / Disable the Machine User’s Ability to Initiate Chat with VSA Users
Users can enable / disable the machine user’s ability to initiate a chat session with VSA users using Agent > Portal Access and System > Machine Roles.

Ensuring Chat Opens a New Window
The default setting for Internet Explorer reuses 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:

- Select Internet Options from the Tools menu of any Internet Explorer window.
- Click on the Advanced tab.
- Uncheck the box labeled Reuse windows for launching shortcuts in the Browsing section.
- Click OK.

My Machine Makes 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:
• Open the **Control Panel** and select **Sounds and Multimedia**.
• Click on the **Sounds** tab.
• Scroll down and select **Start Navigation** in the **Windows Explorer** section.
• Select *(None)* from the drop-down control labeled **Name**.
• Click **OK**.

The other options that are provided by the Chat module are shown in Fig. 4.14 below:

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

2. **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.

3. **Automatically close chat window when either party ends chat**: Check this box to close the chat window when either party ends the chat. Leave blank, if you want each party to be able to view and copy text from the chat window, even if the other party ends the chat.

4. **Remove your name from chat list seen by other administrators**: Check this box to remove your name from the chat list seen by other VSA users.

5. **Remove your name from chat list seen by users**: Check this box to remove your name from the chat list seen by machine users.

### 4.5.2 Send Message

The **Send Message** page (Fig. 4.15) sends network messages to selected machine IDs. Messages can be sent immediately at the next managed machine check-in, or can be scheduled to be sent at a future date and time.

The message either displays immediately on the managed machine or the agent icon in the system tray of the managed machine flashes between a white background and its normal background when a message is waiting to be read. When the machine user click’s the flashing icon the message displays.

Machine users can also be notified by a conventional Windows dialog box or through a browser window. If a browser window is used, enter a URL instead of a text message. 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 general view of the Send Message page is shown in the Fig. 4.15 below. The options that are available for this module are listed below:

1. **Enter message/URL sent to remote machines (dialog box or URL):** The text you enter depends on the display window you select.
   - Enter a text message if the display window is a dialog box.
   - Enter a URL if the display window is a browser.

2. **Select display window:** Select the manner in which the user is notified on the managed machine. The default is Dialog Box, which displays a standard Windows dialog box with the network message. Browser displays a URL in a web browser window.

3. **Send Now:** Click **Send Now** to send the message immediately to selected machines. The message displays in the *Messages Not Yet Sent* column until the message is received by the machine. For example, the machine may be offline.

4. **Clear Messages:** Click **Clear Messages** to remove messages that have not been delivered to managed machines. Schedule time to send message. Enter the year, month, day, hour, and minute to send the message.

5. **Schedule:** Click **Schedule** to schedule delivery of the message to selected machine IDs using the schedule options previously selected. The message displays in the *Messages Not Yet Sent* column until the message is received by the selected machine.

6. **Display Immediately/Flash Icon:** This setting determines how managed machine users are notified once their message has been retrieved from the KServer.
   - **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**.

7. **Machine.Group ID:** The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.
8. **Current User:** Displays the currently logged on user.

9. **Messages Not Yet Sent:** This column displays messages not yet sent.

### 4.6 vPro

#### 4.6.1 Power Management

The **Power Management** page powers on, powers off or reboots vPro-enabled machines. Power management options are executed using the agent of the managed machine that originally identified the vPro-enabled machine using LAN Watch. A vPro credential is required to execute power management options on a vPro-enabled machine. You can specify a credential using this page.

**Note:** You can display the hardware assets of vPro-enabled machines with credentials using Agent > View vPro

The general view of the Power Management page is shown in the Fig 4.16 below. The options that are available for this module are listed below:

![Fig. 4.16: Power Management](image)

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

3. **Cancel**: Cancel schedule options for selected machined IDs.

4. **Power Up / Power Down / Reboot**: Select the power management option to execute.

5. **Machine ID. Group ID**: The machine ID.Group ID of this vPro-enabled machine, if an agent is installed. Blank, if no agent is installed.

6. **vPro Host Name**: The name for the vPro-enabled machine set by vPro configuration.

7. **Proxy Agent**: The machine ID.group ID of another managed machine used to execute power on, power off or reboot this vPro-enabled machine. The Proxy Agent must be on the same LAN as the vPro machine.

8. **OS Computer Name**: The name for the vPro-enabled machine set by the operating system.

9. **IP Address**: The IP address of the vPro-enabled machine.

10. **Credentials**: A vPro credential is typically collected during a LAN Watch scan. A credential is required by the vPro machine to respond to both Power Management and Remote ISO Boot requests. If no credential exists or the credential needs to be changed you can click this cell to enter a new credential.

The other options that are available in this page are:

- **Expand / Collapse**: Click the plus icon of a vPro machine ID to display a history table of power management actions performed on that machine. Click the minus icon to collapse the history table.

- **Type**: The power management option scheduled to be executed.

- **Last Power Management**: The last time a power management option was executed.

- **New Power Management**: The next time a power management option is scheduled to be executed.
4.6.2 Remote ISO Boot

The Remote ISO Boot page boots vPro machines from an ISO image. An agent machine on the same LAN as the target vPro machine is used to mount a virtual disk on the VPro machine. The virtual disk points to a UNC share on the LAN containing an ISO image. The agent machine then boots the VPro machine from the virtual disk. A Remote ISO Boot cannot be scheduled. The boot occurs immediately.

VPro Configuration Requirements

- The agent cannot be on the vPro machine. It has to be on a different machine in the same LAN.
- The VPro machine being booted must be VPro 3.0 or greater.
- SOL/IDE-R must be enabled in the Intel AMT BIOS extension. This cannot be done remotely.
- The agent machine used to boot the vPro machine, the VPro machines being booted and the UNC must all be on the same LAN.
- Only UNC shares can be specified. Mapped drives are not allowed.
- Credentials must be defined in advance, providing access to:
  - The agent machine - Use Agent > Set Credential if necessary.
  - The UNC share on the LAN - The network credentials and UNC are both specified when the ISO boot icon is clicked in the Remote ISO Boot grid.
  - The vPro machine - vPro credentials are configured either during LAN Watch scan or by clicking on the credentials icon in the Remote ISO Boot or Power Management grid.

Components

ISO boot is implemented via the following components:

- **VProProxy.dll** - This dll is used by the agent on the agent machine to communicate with the VPro machine.
- **Redirect.exe** - This process is run with the passed in network credentials and manages the virtual drive.

Switches

The following are switches sent to VProProxy.dll when doing an ISO boot.

- `-redirect` - We’re going to do a redirect operation. Possible values - command
- `-username` - The VPro user name (like admin)
- `-password` - The password for the VPro user
- `-ip` - The ip address of the target machine
- `-iso` - The UNC path to the ISO image
- `-redirectPath` - The path to redirect.exe
- `-o` - The full name and path of the out file for VProProxy.dll
- `-redirectOut` - The full name and path of the out file for redirect.exe
- `-netUsername` - The name of the network user with authority to access iso image. Name must be in the form of name@domain.
- `-newPassword` - The password for the network user

Fig 4.17 below shows the generic view of the Remote ISO boot page. The options shown on this page are listed and explained below.
1. **Host Name**: The name for the vPro-enabled machine set by vPro configuration.

2. **Proxy Agent**: The machine ID, group ID of another managed machine used to execute power on, power off or reboot this vPro-enabled machine. The Proxy Agent must be on the same LAN as the vPro machine.

3. **Machine, Group ID**: The machine ID, group ID of this vPro-enabled machine, if an agent is installed. Blank, if no agent is installed.

4. **Credentials**: The vPro credentials are typically collected during a LAN Watch scan. The credentials are required by the vPro machine to respond to both Power Management and Remote ISO Boot requests. If none are defined or they need to be changed you can click this cell to define a new credential.

5. **Remote ISO Boot**: Click the Remote ISO Boot icon to specify the UNC File Path, User Name and Password. Then click the Go button.
   - The UNC File Path must include the filename of the ISO image.
   - The User Name and Password is required to access to the ISO image file on the LAN.