Kaseya 2

Remote Control

User Guide

Version 7.0

English

December 22, 2014

Agreement

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

©2014 Kaseya. All rights reserved. | www.kaseya.com

Contents

Remote Control Overview

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 behind NAT.
- Work independently or with the user to solve problems interactively where both parties can see what is happening in real time.
- 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. Perfect for supporting dial up users with only a single phone line. Remote control and chat at the same time.
- Power up, power down, bootup or reboot vPro-enabled machines.

Functions	Description
Control Machine *(page 1)*	Allows users to view and/or take control of a managed machine's desktop remotely for troubleshooting and/or instructional purposes.
Reset Password *(page 15)*	Reset the password for a local account on a managed machine.
Preinstall RC *(page 20)*	Install the remote control service
Uninstall RC *(page 24)*	Uninstall the remote control service
User Role Policy *(page 29)*	Determines how machine users are notified that a remote control session to their machine is about to begin. Set by VSA user role.
Machine Policy *(page 31)*	Determines how machine users are notified that a remote control session to their machine is about to begin. Set by machine ID.
FTP *(page 34)*	Initiate an FTP session with any remote managed machine.
SSH *(page 45)*	Runs an SSH command line session on a selected, active Linux or Apple machine.
Task Manager *(page 47)*	Remotely executes the NT task manager and displays data in the browser.
Chat *(page 47)*	Start a chat session between a user and any remote machine.
Send Message *(page 53)*	Allows users to send network messages to selected managed machines.

Control Machine

Remote Control > Desktop Control > Control Machine

The **Control Machine** page establishes a remote control session between the user's local machine and a selected machine ID. Remote control sessions can only be initiated from a Windows-based machine.

Automatic Installation

If K-VNC is not already installed on a machine and a remote control session is initiated using **Control Machine** *(page 1)*, then the package is automatically installed. Installation does not require a reboot. Automatic installation takes up to an extra minute. To eliminate this delay during first time use, you can pre-install K-VNC on any managed machine using **Preinstall RC** *(page 20)*.

> **Note:** Uninstalling an agent does not remove K-VNC or the KBU client, KES client, or KDPM client. Before you delete the agent, use Remote Control > **Uninstall RC** *(page 24)* to uninstall K-VNC on the managed machine. Uninstall all add-on module clients as well.

Initiating Remote Control

Initiate remote control by clicking the name of the target machine. Icons next to the managed machine ID indicate the current connection status for that machine. Only machine IDs with an

or

or

icon can be connected to target machines and have live links; all others will be inactive.

Online but waiting for first audit to complete

Agent online

Agent online and user currently logged on. Icon displays a tool tip showing the logon name.

Agent online and user currently logged on, but user not active for 10 minutes

Agent is currently offline

Agent has never checked in

Agent is online but remote control has been disabled

The agent has been suspended

Note: Users can disable remote control and FTP sessions by right-clicking the icon on their managed machine and selecting **Disable Remote Control**. You can deny users this ability by removing **Disable Remote Control** using Agent > Agent Menu.

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.

Remote Controlling the KServer

Clicking the **KServer** link starts a remote control session to the Kaseya Server itself. Use this feature to remotely manage your own Kaseya Server. Only master role users can remote control the Kaseya Server.

Remote Control for Machine Users

Machine users can have remote access to their agent machines using Agent > Portal Access.

Remote Control Malfunctions

Some reasons for remote control failure—for target machines with and without an agent—are:

- The remote machine is blocking outbound traffic on the agent check-in port (default 5721). The firewall may need to be reconfigured.
- The remote machine is on a slow connection. Let the applications run longer than the timeout period and see if that works.
- Anti-virus software on the remote machine may block the connection. This problem is eliminated if Endpoint Security protection is installed on the remote machine.
- Wrong primary Kaseya Server address - Remote control can only connect through the primary Kaseya Server address. Machines with an agent can connect through either the primary or secondary address. Verify the remote machine can see the primary Kaseya Server address using Agent > Check-in Control.

Record remote control to a file in the machine working directory

Applies to K-VNC only. If checked, creates a video recording of a remote control session.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent Quick View window.

Online but waiting for first audit to complete

Agent online

Agent online and user currently logged on.

Agent online and user currently logged on, but user not active for 10 minutes

Agent is currently offline

Agent has never checked in

Agent is online but remote control has been disabled

The agent has been suspended

Machine.Group ID

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

or

or

icon can be connected to target machines and have live links; all others will be inactive.

Current User

The user currently logged on to the managed machine.

Active Admin

The VSA user currently conducting a remote control session to this machine ID.

K-VNC Toolbar Options

A **K-VNC** remote control session can be started using the Remote Control > **Control Machine** *(page 1)* page. Administrators should use K-VNC for situations not supported by **Kaseya Remote Control** *(page 58)*, and when a web-based remote control solution is required. Only K-VNC remote control sessions support **Session recording** or **Notify user when session terminates** settings, located on the **User Role Policy** *(page 29)* and **Machine Policy** *(page 31)* pages of the **Remote Control** module.

A K-VNC session provides a set of toolbar buttons to manage the remote desktop viewer. Hover the

mouse over each button to display a tooltip.

- **Set Options** - Sets connection options for the current viewer session. See details below.
- **Show Connection Info** - Displays connection info about the current desktop viewer session.
- **Refresh Screen** - Refreshes the display of the desktop viewer.
- **Zoom Out**
- **Zoom In**
- **Zoom 100%**
- **Zoom to Fit Window**
- **Full Screen**
- **Send 'Ctrl-Alt-Del'** - Selects CTRL+ALT+DEL on the remote machine.
- **Send 'Win' key as 'Ctrl-Esc'** - Selects CTRL+ESC on the remote machine.
- **Ctrl-Lock** - If on, holds down the CTRL key.on the remote machine.
- **Alt-Lock** - If on, holds down the ALT key on the remote machine.
- **Disconnect** - Disconnects the current viewer session.

Set Options

Format and Encodings

Changes to these settings apply only to the current viewer session.

- **Preferred Encoding**
  - `Tight (default)` - Usually the best choice for low-bandwidth network connections.
  - `Hextile` - Usually the best choice for high-speed network connections.
  - `ZRLE` - Included in applet for compatibility with different VNC servers, but not required in Live Connect.
  - `Raw` - Fastest when the server and viewer are on the same machine.
- **Color format** - Reduce colors for better performance over slower network connections.
- **Custom compression level** - Level 1-9. Default is 6.
  - Level 1 uses minimum CPU time and achieves weak compression ratios.
  - Lower levels are recommended for high bandwidth network environments.
  - Level 9 offers best compression but is slow in terms of CPU time consumption on the remote machine.

  - Higher levels recommended for low bandwidth network environments.
- **Allow JPEG, set quality level** - Level 1-9. Defaults is 6.
  - Refers to JPEG compression level.
  - Level 1 gives bad image quality but high compression ratios, while level 9 offers very good image quality at lower compression ratios.
  - Lower levels recommended for low bandwidth network environments.
  - Higher levels recommended for high bandwidth network environments.
  - Disabling recommended only if perfect image quality is needed.
- **Allow CopyRect encoding** - Enabled by default. Saves bandwidth and drawing time when parts of the remote screen are moving around.

Restrictions

- **View Only** - Disables transfer of mouse and keyboard events from the viewer to remote machine.
- **Disable clipboard transfer** - Disables copy/paste between viewer and remote machine.

Mouse Cursor

- **Track Remote cursor locally** - Remote cursor location is shown in viewer.
- **Let remote server deal with mouse cursor** OR **Don't show remote cursor** - Remote cursor location is not shown in viewer. Conserves bandwidth.

Local cursor shape

- Selects the shape of the local cursor when the mouse is over the viewer window.

(Other)

- **Request shared session** - Always checked.

Reset Password

Remote Control > Desktop Control > Reset Password

The **Reset Password** page creates a new password and, if necessary, 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.

Note: To delete a user account, you can create a procedure to delete the user account or use remote control to manually delete the user account.

Resetting the User Password

Use **Reset Password** to reset the user password on all your managed machines when:

- 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.

Note: On non-domain controllers, only the local user account on the remote machine is changed. On domain controllers, **Reset Password** changes the domain user accounts.

Apply

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

Cancel

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

Username

Enter the username on the managed machine.

Create new account

Check this box to create a new user account on the managed machine.

as Administrator

Check this box to create the new user account with administrator privileges.

Password / Confirm

Enter a new password.

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent Quick View window.

Online but waiting for first audit to complete

Agent online

Agent online and user currently logged on.

Agent online and user currently logged on, but user not active for 10 minutes

Agent is currently offline

Agent has never checked in

Agent is online but remote control has been disabled

The agent has been suspended

Machine.Group ID

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

Status

The status of pending password changes and user account creations.

Preinstall RC

Remote Control > Configure > Preinstall RC

The **Preinstall RC** page installs **K-VNC** *(page 13)* on selected machine IDs without initiating a remote control session. When an install is pending on any machine ID this page automatically refreshes every 5 seconds until the procedure completes.

Automatic Installation

If K-VNC is not already installed on a machine and a remote control session is initiated using **Control Machine** *(page 1)*, then the package is automatically installed. Installation does not require a reboot. Automatic installation takes up to an extra minute. To eliminate this delay during first time use, you can pre-install K-VNC on any managed machine using **Preinstall RC** *(page 20)*.

Note: Uninstalling an agent does not remove K-VNC or the KBU client, KES client, or KDPM client. Before you delete the agent, use Remote Control > **Uninstall RC** *(page 24)* to uninstall K-VNC on the managed machine. Uninstall all add-on module clients as well.

Install

Click **Install** to install K-VNC on selected machine IDs. Linux and Apple OS X agents only use K-VNC.

Cancel

Click **Cancel** to clear pending install procedures for selected machine IDs.

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the

page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent Quick View window.

Online but waiting for first audit to complete

Agent online

Agent online and user currently logged on.

Agent online and user currently logged on, but user not active for 10 minutes

Agent is currently offline

Agent has never checked in

Agent is online but remote control has been disabled

The agent has been suspended

Machine.Group ID

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

Last Status

`Pending` indicates the install will run the next time that machine checks into the Kaseya Server. Otherwise, this column displays when the remote control package was installed on the machine ID.

Uninstall RC

Remote Control > Configure > Uninstall RC

The **Uninstall RC** page uninstalls **K-VNC** *(page 13)* from selected machine IDs. When an uninstall is pending on any machine ID this page automatically refreshes every 5 seconds until the procedure

completes.

If an existing K-VNC installation has problems then the VSA may not be able to establish a K-VNC session. If remote control using K-VNC fails then running **Uninstall RC** on that machine ID cleans out any existing problem installs. A fresh copy of K-VNC is installed the next time a remote control session is started or using **Preinstall RC** *(page 20)*.

Note: Uninstalling an agent does not remove K-VNC or the KBU client, KES client, or KDPM client. Before you delete the agent, use Remote Control > **Uninstall RC** *(page 24)* to uninstall K-VNC on the managed machine. Uninstall all add-on module clients as well.

Uninstall

Click **Uninstall** to uninstall the remote control package from selected machine IDs.

Cancel

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

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent Quick View window.

Online but waiting for first audit to complete

Agent online

Agent online and user currently logged on.

Agent online and user currently logged on, but user not active for 10 minutes

Agent is currently offline

Agent has never checked in

Agent is online but remote control has been disabled

The agent has been suspended

Last Status

`Pending` indicates the uninstall will run the next time that machine checks into the VSA. Otherwise, this column displays when the remote control package was uninstalled on the machine ID.

User Role Policy

Remote Control > Notification Policy > User Role Policy

The **User Role Policy** page determines how you want to notify users that a remote control session to their machine is about to begin. Policies are applied by user roles.

> **Note:** See **Machine Policy** *(page 31)* to apply remote control notification policies by machine ID. Machine policy takes precedence over user role policy.

Exceptions

K-VNC *(page 13)* supports all options on this page. **Kaseya Remote Control** *(page 58)* supports all options on this page except:

- Notify user when session terminates
- Record remote control to a file in the machine working directory

Apply

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

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 can not 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 can not 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 canceled.

Notify user when session terminates

Supported by K-VNC only. Check this box to notify the user when the session terminates.

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.

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.

Remove

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

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.

Record remote control to a file in the machine working directory

Supported by K-VNC only. If checked, remote control sessions are automatically recorded for machines assigned this policy.

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Delete

Click the delete icon next to a user role 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.

Role Name

The list of user roles.

Policy

The remote control policy applied to a user role.

Message

The text messages applied to a user role.

Machine Policy

Remote Control > Notification Policy > Machine Policy

The **Machine Policy** page determines how you want to notify users a remote control session to their machine is about to begin. This policy is applied to **machine IDs**.

Note: See **User Role Policy** *(page 29)* to apply remote control notification policies by machine ID. Machine policy takes precedence over user role policy.

Exceptions

K-VNC *(page 13)* supports all options on this page. **Kaseya Remote Control** *(page 58)* supports all options on this page except:

- Notify user when session terminates
- Record remote control to a file in the machine working directory

Apply

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

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 can not 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 can not 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 canceled.

Notify user when session terminates.

Supported by WinVNC only. Check this box to notify the user when the session terminates.

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.

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.

Remove

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

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.

Record remote control to a file in the machine working directory

Supported by WinVNC only. If checked, remote control sessions are automatically recorded for machines assigned this policy.

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Delete

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.

Machine.Group ID

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

Policy

The remote control policy applied to a machine ID.

Message

The text messages applied to a machine ID.

FTP

Remote Control > Files/Processes > FTP

The **FTP** page establishes an FTP session between the user's local machine and a selected machine ID. FTP sessions can only be initiated from a Windows-based machine. 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.

Note: You can also use **Live Connect** *(page 60)* to initiate a **File Manager** session with managed machines, depending on the OS type supported.

File Transfer Protocol (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 Kaseya Server 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 Kaseya Server, all FTP sessions are protected by the Kaseya 256 bit rolling encryption protocol.

Initiating FTP

Initiate an FTP session by clicking the name of the remote machine. Icons next to the managed machine ID indicate the current connection status for that machine. Only machine IDs with an

or

or

icon can be connected to target machines and have live links; all others will be inactive.

Online but waiting for first audit to complete

Agent online

Agent online and user currently logged on. Icon displays a tool tip showing the logon name.

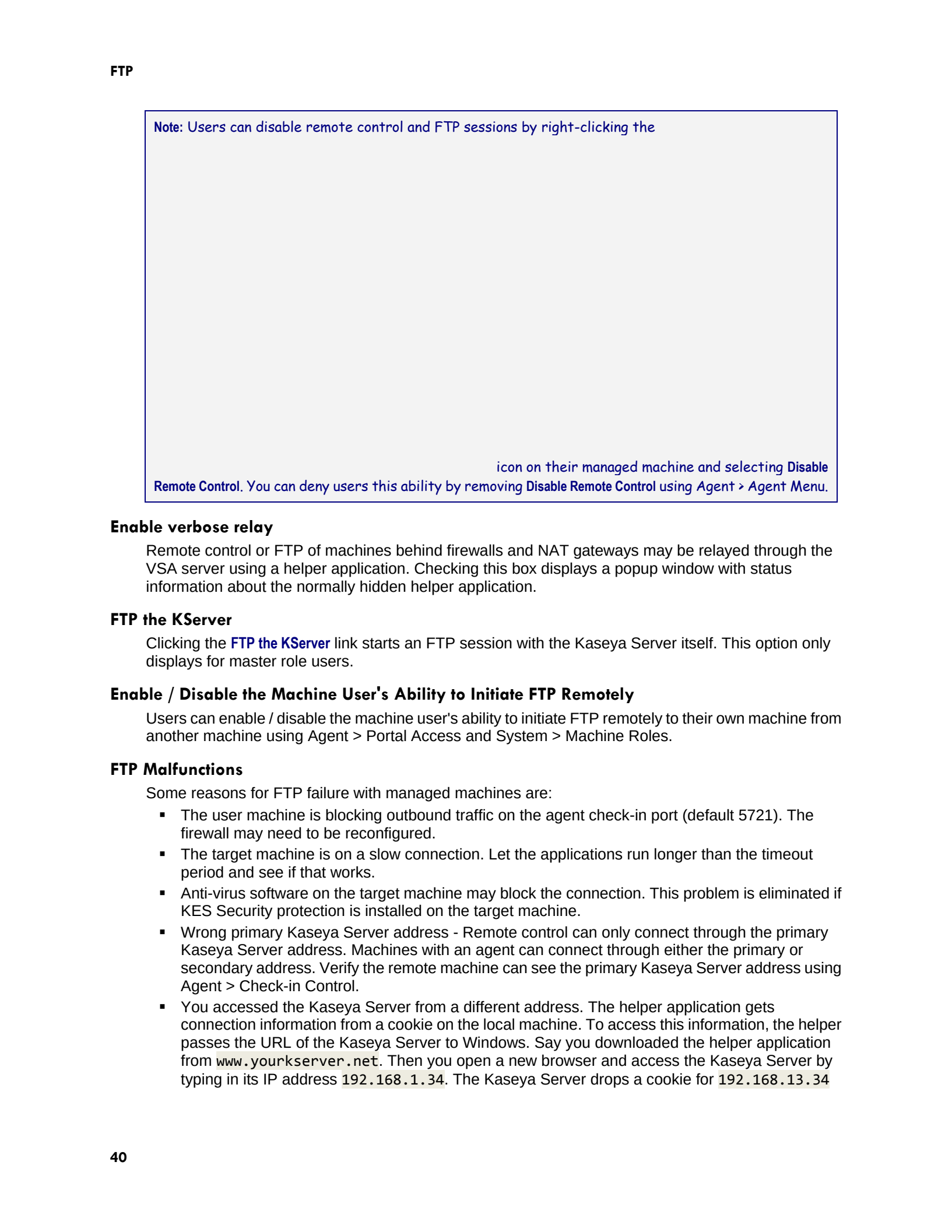
Agent online and user currently logged on, but user not active for 10 minutes

Agent is currently offline

Agent has never checked in

Agent is online but remote control has been disabled

The agent has been suspended

> **Note:** Users can disable remote control and FTP sessions by right-clicking the
>
> 
>
> icon on their managed machine and selecting **Disable Remote Control**. You can deny users this ability by removing **Disable Remote Control** using *Agent > Agent Menu*.

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.

FTP the KServer

Clicking the **FTP the KServer** link starts an FTP session with the Kaseya Server itself. This option only displays for master role users.

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 > Portal Access and System > Machine Roles.

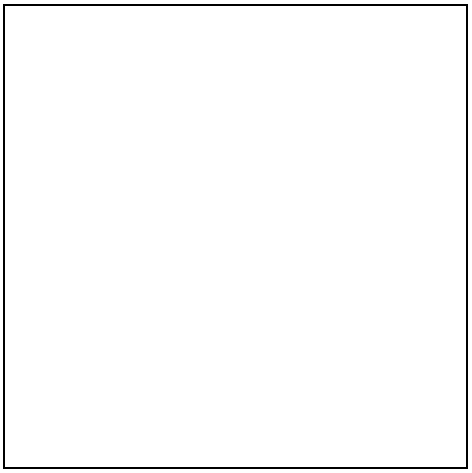
FTP Malfunctions

Some reasons for FTP failure with managed machines are:

- The user 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.
- 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.
- Wrong primary Kaseya Server address - Remote control can only connect through the primary Kaseya Server address. Machines with an agent can connect through either the primary or secondary address. Verify the remote machine can see the primary Kaseya Server address using Agent > Check-in Control.
- You accessed the Kaseya Server 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 Kaseya Server to Windows. Say you downloaded the helper application from `www.yourkserver.net`. Then you open a new browser and access the Kaseya Server by typing in its IP address `192.168.1.34`. The Kaseya Server drops a cookie for `192.168.13.34`

while the helper tries to get a cookie corresponding to `www.yourkserver.net`. The helper won't find the cookie. If this happens to you, just download a new helper application and try again.

- FTP requires **Passive FTP** be turned **off**. If you get the following error after attempting an FTP session:



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.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent Quick View window.

Online but waiting for first audit to complete

Agent online

Agent online and user currently logged on.

Agent online and user currently logged on, but user not active for 10 minutes

Agent is currently offline

Agent has never checked in

Agent is online but remote control has been disabled

The agent has been suspended

Machine.Group ID

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

Enter a drive letter to FTP to

Enter the drive letter to FTP to, instead of selecting a remote fixed drive option.

> **Note:** The Kaseya Server determines how many fixed disks a managed machine has via its Latest Audit.

SSH

Remote Control > Files/Processes > SSH

The **SSH** page runs an SSH command line session on a selected, *active* Linux or Apple machine. SSH sessions can only be initiated from a Windows-based machine. Only Linux or Apple machines with an

or

or

icon are active.

ActiveX Control

Remote control, FTP and SSH can only be initiated from Windows OS machines. An ActiveX control automatically configures and runs the package for you. The first time you use any of these packages 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 package manually.

Running an SSH Session

1. Click any Linux or Mac machine that displays a hyperlink beneath the machine ID name.
   - A second page states the encrypted SSH session is starting.
   - It attempts to automatically load the ActiveX control. If the ActiveX control fails to load, click the **here** hyperlink to download the ActiveX control manually and run it.
   - Once the ActiveX control is downloaded and run, the SSH command line window displays on this same page.
2. The SSH command line session prompts you to enter an administrator username and password.

3. Click the **Back** hyperlink to end the SSH command line session.

Task Manager

Remote Control > Files/Processes > Task Manager

The **Task Manager** page performs the same function as Microsoft's Windows NT/2000 task manager. It lists all currently active processes on a managed machine. 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. Task Manager 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.

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

VSA users can enable / disable the machine user's access to Task Manager on their own machine remotely from another machine using the System > Machine Roles > Access Rights tab

Name

The name of the process actively running on the managed machine.

CPU

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

Mem Usage

The amount of main memory used by each active process.

Threads

The 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.

Chat

Remote Control > Message with Users > Chat

The **Chat** page initiates or continues chat sessions with logged on users

on managed machines. Multiple chat sessions may be active 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. Press the **Shift-Enter** key combination to insert a carriage return into a message.

> **Note:** You can also use **Live Connect** *(page 60)* to chat and video chat with a managed machine. Video chat allows you to video chat with anyone, not just a managed machine user.

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 to send the message.

To Respond to a Chat Session

If a chat popup window displays while you are logged on to the Kaseya Server, 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 with scope rights 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 the System > Machine Roles > Access Rights tab.

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:

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.**

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:

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.**

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent Quick View window.

Online but waiting for first audit to complete

Agent online

Agent online and user currently logged on.

Agent online and user currently logged on, but user not active for 10 minutes

Agent is currently offline

Agent has never checked in

Agent is online but remote control has been disabled

The agent has been suspended

Machine.Group ID

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

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.

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.

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.

Remove your name from chat list seen by users

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

Send Message

Remote Control > Message with Users > Send Message

The **Send Message** page 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.

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.

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.

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.

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.

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.

Display Immediately/Flash Icon

This setting determines how managed machine users are notified once their message has been retrieved from the Kaseya 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**.

Select All/Unselect All

Click the **Select All** link to check all rows on the page. Click the **Unselect All** link to uncheck all rows on the page.

Check-in status

These icons indicate the agent check-in status of each managed machine. Hovering the cursor over a check-in icon displays the agent Quick View window.

Online but waiting for first audit to complete

Agent online

Agent online and user currently logged on.

Agent online and user currently logged on, but user not active for 10 minutes

Agent is currently offline

Agent has never checked in

Agent is online but remote control has been disabled

The agent has been suspended

Machine.Group ID

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

Current User

Displays the currently logged on user.

Messages Not Yet Sent

This column displays messages not yet sent.

Kaseya Remote Control

Kaseya Remote Control is the primary remote control capability used throughout **Virtual System**

Administrator™. **Kaseya Remote Control** connects in seconds to remote machines that already have **Kaseya Remote Control** installed. **Kaseya Remote Control** maintains a reliable, secure and encrypted connection.

Starting Kaseya Remote Control

Click any agent icon that supports **Kaseya Remote Control** to automatically start or re-start it. You can also hover over the agent icon to display Quick View. Click the **Remote Control** button to launch **Kaseya Remote Control**.

Note: You can launch **Live Connect** *(page 60)* by *Ctrl+clicking* the agent icon. You can also click the **Live Connect** button in **Quick View**.

Installing and Updating Kaseya Remote Control

Kaseya Remote Control is installed as a viewer/server pair of applications: the viewer on the administrator's local machine and the server on the remote agent machine. The **Kaseya Remote Control** server is installed as a component of the agent when a new agent is installed, or when the agent is updated using Agent > Update Agent.

If the **Kaseya Remote Control** application is not already installed on your local administrator machine, when you start your first session a dialog prompts you to download and install it. If already installed and a Kaseya patch release has made a later version available, a dialog prompts you to download and install the updated version. There is no independent launching of the **Kaseya Remote Control** application outside of the VSA.

Main Features

- Supports remote control with or without a machine user being logged in.
- Connects to the console session. If a user is logged on, the administrator shares the console session with the user.
- Allows the administrator to select any additional *monitors* that may be running on the remote system.
- Multiple view sessions can connect to the same agent machine, viewing the same monitor or different monitors.
- Copies and pastes (CTRL+C and CTRL+V) *plain text* between local and remote systems.
- Supports the use of numerous native **Windows and Apple shortcut keys** *(https://helpdesk.kaseya.com/entries/58322696)* on the remote machine.
- Uses the keyboard layout configured on the remote machine. Characters on the administrator's local keyboard might not match the characters shown on the remote user interface.

Administrators can temporarily change the keyboard layout on the remote machine to map to their local keyboard. This might apply when entering passwords.

- Connects when a Windows machine is booted into *Safe Mode with Network*.
- A log entry is created in the VSA > System > System Log each time **Kaseya Remote Control** successfully connects to a remote control session.

> **Note:** See **Kaseya Remote Control Requirements** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/Reqs/index.asp#18007.htm).*

User Interface

The basic layout of the **Kaseya Remote Control** user interface includes the following:

- The machine name displays at the top of the remote control session window.
- A narrow menu bar displays at the top.
- When connecting to Windows machines only, a 'Send CTRL+ALT+DEL' option displays in the menu bar for remote logins.
- When multiple monitors are available on the remote machine, a drop-down list of monitors displays and can be selected to display a specific monitor.
- Closing the window disconnects the session.
- The default screen size for a session window is 1280 X 800. The default position is centered on the screen. New session windows use the size and position last used by the administrator.

Legacy Remote Control Features Removed

With the release of 7.0 all features having to do with RADMIN, PC Anywhere, WINVNC, x11vnc Server and UltraVNC viewer have been removed from the Remote Control module. The Remote Control > **Select Type** and **Set Parameters** pages have also been removed.

Using K-VNC

A **K-VNC** remote control session can be started using the Remote Control > **Control Machine** *(page 1)* page. Administrators should use the K-VNC for situations not supported by **Kaseya Remote Control**, and when a web-based remote control solution is required. Only K-VNC remote control sessions support **Session recording** or **Notify user when session terminates** settings, located on the **User Role Policy** *(page 29)* and **Machine Policy** *(page 31)* pages of the **Remote Control** module.

Live Connect

Live Connect is a web-based, single-machine user interface. You can access **Live Connect** by

Ctrl+clicking the agent icon , or by clicking **Live Connect** button in Quick View. **Live Connect** enables you to perform tasks and functions solely for one managed machine. A menu of tabbed property sheets provide access to various categories of information about the managed machine.

Additional menu items display, depending on the add-on modules installed and the operating system of the target machine.

> **Note:** Both the **Live Connect** and **Portal Access** plug-in installers can be pre-installed using the Agent > Update Agent page.

Windows

Live Connect for Windows machines supports the following menu items: **Home**, **Agent Data**, **Audit Information**, **File Manager**, **Command Shell**, **Registry Editor**, **Task Manager**, **Event Viewer**, **Ticketing**, **Chat**, **Desktop Access** and **Video Chat**.

> **Windows Cross-Platform OS Support:** On Windows XP and later systems, using any of our supported browsers, you can use the **File Manager**, **Command Shell**, **Registry Editor**, **Task Manager**, **Event Viewer**, **Desktop Access** enhanced features with Windows XP and later and **File Manager**, **Command Shell**, **Desktop Access** enhanced features with Mac OS X 10.5 Leopard (Intel) and later systems.

Apple

Live Connect for Macintosh machines supports the following menu items: **Home**, **Agent Data**, **Audit Information**, **File Manager**, **Command Shell**, **Ticketing**, **Chat**, **Desktop Access** and **Video Chat**.

> **Apple Cross-Platform OS Support:** On Mac OS X 10.5 Leopard (Intel) and later systems, using any of our supported browsers, you can use the **File Manager**, **Command Shell**, **Desktop Access** enhanced features with Windows XP and later and Mac OS X 10.5 Leopard (Intel) and later systems.

Linux

Live Connect for Linux machines supports the following menu items: **Home**, **Agent Data**, **Audit Information**,

Ticketing, **Chat**, and **Video Chat**. Does not include a thumbnail preview image of the desktop in **Live Connect**. Use the **Control Machine** *(page 1)*, **FTP** *(page 34)* and **SSH** *(page 45)* pages to remote control Linux agents.

Window Header

Basic information about the managed machine displays at the top of the **Live Connect** window.

- **Thumbnail View** - The desktop of the currently logged on user displays in a thumbnail view, if a user is logged onto the machine.
- **Machine Info** - Lists basic information about the managed machine.
- **Performance Graphs** - Shows CPU % and Memory % performance graphs for the managed machine.
- **Log Off** - Only displays if a machine user using **Portal Access** is logged in remotely from the machine.
- **Help** - Displays online help for **Live Connect**.

Menu Options

A menu of tabbed property sheet provides access to various categories of information about the managed machine.

- **Home** - *The* **Home** *tab is the first tab displayed when the* **Live Connect** *window opens*.
  - **Home** - Typically the **Home** tab displays a welcome message and the URL page of the agent service provider. The **Run Procedures** section of the **Home** tab enables the **Live Connect** user to run agent procedures on the managed machine immediately. A **Custom Links** section may display on the **Home** tab, if specified by the service provider, offering links to additional resources. Multiple customized **Home** tabs are possible, each with a unique name, if specified by the service provider.
  - **Change Logon** - Changes the *remote* logon user name and password for this managed machine. These logon options enable a user to access the **Live Connect** window to this managed machine from any other machine, including initiating a remote desktop session with the managed machine, if **Desktop Access** is enabled by the service provider. Enter the same URL used to logon to the VSA. Then enter the **Live Connect** user name and password specified in this tab. Accessing **Live Connect** remotely in this manner from another machine is called **Portal Access**. **Portal Access** logon options can also be maintained within the VSA using Agent > Portal Access.
  - **Change Profile** - Changes the contact information for this managed machine. This information populates a ticket with contact information when **Live Connect** is used to create a ticket. This information can also be maintained using Agent > Edit Profile.
- **Agent Data** - Displays the following tabs:
  - **Pending Procedures** - Displays and schedules pending agent procedures for a managed machine and the **Procedure History** for that machine. Includes the execution date/time, status and user who scheduled the procedure.
    - ✓ Click the **Schedule Another Procedure** button to schedule a procedure not yet pending. Once selected and scheduled, the procedure displays at the bottom of the **Pending Procedures** section.
    - ✓ Click the **Schedule** button to schedule a selected procedure to run in the future or on recurring basis.
    - ✓ Click the **Run Now** button to run a selected procedure once immediately.
    - ✓ Click the **Cancel** button to cancel any selected pending procedure.
  - **Logs** - Displays the logs available for a machine: Alarm Log, Monitor Action Log, Agent Log, Configuration Changes, Network Statistics, Event Log, Agent Procedure Log, Remote Control Log, Log Monitoring.
  - **Patch Status** - Displays `Missing` and `Pending` Microsoft patches and schedules missing patches. If a machine belongs to a patch policy, missing patches may be further identified as

`Denied (Pending Approval)`. The user can manually override the denied patch policy by scheduling the patch.

- ✓ Click the **Show History** link to display the history of patches installed on the managed machine.
- ✓ Click the **Schedule** button to schedule the deployment of missing patches.
- ✓ Click the **Scan Now** button to scan for missing patches immediately.
- ✓ Click the **Cancel** button to cancel a selected pending patch.
- ✓ Click the **Set Ignore** button to prevent installing a patch using any of the installation methods. To be installed, the **Set Ignore** checkbox must be cleared.
- ✓ Check the **Hide patches denied by Patch Approval** - If checked, patches denied by Patch Approval are not displayed.

➢ **Agent Settings** - Displays information about the agent on the managed machine:

- ✓ **Agent version**
- ✓ **Last check-in**
- ✓ **Last reboot**
- ✓ **First time check-in**
- ✓ **Patch Policy Membership** - Defined using Patch Management > Membership: Patch Policy
- ✓ **View Definition Collections** - Defined using the **Only show selected machine IDs** option in View Definitions.
- ✓ **Working Directory** - Can also be defined using Agent > Working Directory.
- ✓ **Check-In Control** - Can also be defined using Agent > Check-In Control.
- ✓ **Edit Profile** - Can also be defined using Agent > Edit Profile.

➢ **Documents** - Lists documents uploaded to the Kaseya Server for a managed machine. You can upload additional documents. Provides the same functionality as Audit > Documents.

➢ **Get File** - Accesses files previously uploaded from a managed machine. Click the link underneath a file to display the file or run it. Provides the same functionality as Agent Procedures > getFile().

- **Audit Information** - Information tabs include: **Machine Info**, **Installed Apps**, **System Info**, **Disk Volumes**, **PCI & Disk Hardware**, **Printers**, **Software Licenses**, and **Add/Remove Programs**. Provides audit information based on your Latest Audit. You can perform an an immediate audit using the **Machine Info** tab.
- **File Manager** - Displays two file managers, one for your local machine and one for the managed machine. Using the *upper panes* only you can:
  - ➢ Create directories and delete, refresh or rename files or directories using either file manager.
  - ➢ *Move* files within the *same* file manager using drag and drop.
  - ➢ *Copy* files *between* file managers using drag and drop.
- **Command Shell** - Opens a command shell on the managed machine. Defaults to the `c:\windows\system32` directory.
- **Registry Editor** - Displays the registry of the managed machine ID. You can create, rename, refresh or delete keys and values, and set the data for values.
- **Task Manager** - Lists Windows Task Manager data for the managed machine. You can stop or prioritize **Processes**, stop and start **Services**, check typical **Performance** benchmarks for each process, categorized by CPU, disk, network, and memory, review **Users** session data, **Reboot**, power off the managed machine, or log off sessions on the managed machine, and display **User and Groups** on the managed machine. Launching the **Task Manager** lets you create or modify monitor sets using a wizard, based on processes and services. Hovering the cursor over the monitor icon of a log entry displays a wizard.

- A monitor wizard icon displays next to each process and service listed on the **Processes** and **Services** tabs of the **Task Manager**. These two wizards enable you to create a new monitor set criteria based on a selected process or service. The new process or service criteria can be added to any new or existing monitor set. The new or changed monitor set is immediately applied to the machine that served as the source of the process or service criteria. Changing an existing monitor set affects all machines assigned to use that monitor set. See Monitor > Monitor Set > Process Status and Monitor > Monitor Set > Services Check a description of each field shown in these two wizards.

- **Event Viewer** - Displays event data stored on the managed machine by event log type.

  - A monitor wizard icon displays next to event log entries in the VSA and in **Live Connect**. Hovering the cursor over the monitor wizard icon of a log entry displays a wizard. The wizard enables you to create a new event set criteria based on that log entry. The new event set criteria can be added to any new or existing event set. The new or changed event set is immediately applied to the machine that served as the source of the log entry. Changing an existing event set affects all machines assigned to use that event set. The monitor wizard icon displays in:
    - ✓ Agent > Agent Logs
    - ✓ Live Connect > Event Viewer
    - ✓ Live Connect > Agent Data > Event Log

  See Monitor > Event Log Alerts for a description of each field shown in the wizard.

- **Ticketing** - Displays and creates tickets for the managed machine. Displays and creates tickets for **Ticketing** module tickets or tickets and knowledge base articles for the **Service Desk** module, depending on which module is activated.

> **Note:** A service desk must be a member of the Anonymous scope to display **Service Desk** tickets in a machine user **Portal Access** session of **Live Connect**.

- **Chat** - Initiates a chat session with the currently logged on user of the managed machine. You can invite other VSA users to join your chat session. See Remote Control > **Chat** *(page 47)* for more information.
- **Remote Control** - Initiates a **Kaseya Remote Control** *(page 58)* session with the managed machine.
- **Video Chat** - If a machine user is logged on to a managed machine, then a **Live Connect** user can initiate a audio/video chat session with that logged on machine user. The session can be audio only for one or both machines if video is not supported on one or both machines.
  - **Video Chat with the Machine User** - Click the Call button to initiate the video chat session. The machine user will see a browser window or browser tab display on their machine that lets them see your video image and their own video image if their machine has a webcam installed.
  - **Video Chat with Anyone** - Click the Connect URL button. This copies a URL to your clipboard. Copy the URL address into any email or instant message program and send it to anyone. When that URL is entered in a browser the individual will be able to video chat with you. *Video chat does not require the person receiving the chat invitation to be a managed machine.*
  - **Video Chat Confirmation** - The Adobe Flash Player used to transmit the audio/video stream requires each user click an "Allow" button to proceed with their side of the video chat.
  - **Audio/Video Controls** - Hover the mouse over either video image in the chat window to display audio/video controls.
  - **Text Chat** - You can text chat and video chat at the same time using the same window.
- **VPN** - Windows only. Clicking this option creates a VPN connection between your local machine and the **Live Connect** machine. Once connected, the administrator can connect to other machines sharing the same LAN as the **Live Connect** machine, even if those machines do not have an agent installed on them. This includes using applications such as SSH, or telnet or creating another browser instance that targets these other machines on the same LAN. The VPN session ends when the **Live Connect** window closes or the **Stop VPN** button is selected on the **VPN** menu.
- **AntiMalware** - Displays the **AntiMalware** status of the managed machine, if installed.
- **Antivirus** - Displays the **Antivirus** status of the managed machine, if installed.
- **Data Backup** - If **Data Backup** is enabled for the managed machine, you can use this menu to:
  - Run backups immediately.
  - Restore selected backups, directories and files, but only to the same machine.
  - Display the status and history of backups.
- **Discovery** - Displays the **Network Discovery** status of the machine, if installed.

Plugin Manager

Live Connect's enhanced functionality of the browser is managed by a *plug-in manager*.

- **Plug-in Manager Installation** - The user is prompted to install Plug-in Manager after the first logon. Installation of the Plug-in Manager can be deferred until **Live Connect** is started for the first time.
- **Plug-in Updates** - IE and Firefox browsers will detect plug-ins that are out of date and automatically download them in the background. Browser restart is not required for these two browsers. Chrome and Safari browsers also detect out of date plug-ins and automatically download them in the background, with little to no user interaction required.

Additional Notes

- Access to specific **Live Connect** functions depends on access rights in System > User Roles > Access Rights and Machine Roles > Access Rights.

- All of the **Live Connect** menu options are enabled when the machine is connected to **Live Connect**. Only **Home**, **Audit Information, Agent Data** and **Ticketing** are enabled when the machine disconnected from **Live Connect**.
- *You can customize the* **Live Connect Home** *page using System > Customize: Live Connect.*
- **Event Viewer** data does not depend on Agent > Event Log Settings.
- If a `externalLink.xml` exists in the `\Webpages\install` directory of the Kaseya Server a **New Ticket** link displays next to the **Help** link in **Live Connect**. Clicking the **New Ticket** link redirects users to the URL specified in `externalLink.xml`. See **Customized New Ticket Link** *(page 66)* for details.

Customized New Ticket Link

To customize **New Ticket** links on the **Live Connect** page, fill out the `externalLink.xml` file as described in the comments section of the XML below. To activate the new ticket link, place the `externalLink.xml` file in the `\WebPages\install\` directory of your Kaseya Server.

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<externalLinks>
  <!--
  URL STRING SUBSTITUTIONS: The URL string displayed is associated
  with a particular machine ID. The string is searched for the following
  case sensitive values and substituted for the values below.
  machineNameVal - the machine name for the active machine is substituted
                   in the URL string.
  groupNameVal - the group name for the active group.
  -->
  <ticketLink displayName="Ext Ticket"
url="http://192.168.212.52/?mname=machineNameVal&amp;gname=groupNameVal"/>
</externalLinks>
```

Index