About Kaseya

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Control</td>
<td>3</td>
</tr>
<tr>
<td>Remote Cntl Tab</td>
<td>4</td>
</tr>
<tr>
<td>Control Machine</td>
<td>5</td>
</tr>
<tr>
<td>Video Streaming</td>
<td>7</td>
</tr>
<tr>
<td>Reset Password</td>
<td>9</td>
</tr>
<tr>
<td>Power Mgmt</td>
<td>10</td>
</tr>
<tr>
<td>Select Type</td>
<td>11</td>
</tr>
<tr>
<td>Set Parameters</td>
<td>13</td>
</tr>
<tr>
<td>Preinstall RC</td>
<td>14</td>
</tr>
<tr>
<td>Uninstall RC</td>
<td>15</td>
</tr>
<tr>
<td>Admin Role Policy</td>
<td>16</td>
</tr>
<tr>
<td>Machine Policy</td>
<td>18</td>
</tr>
<tr>
<td>FTP</td>
<td>19</td>
</tr>
<tr>
<td>Chat</td>
<td>22</td>
</tr>
<tr>
<td>Send Message</td>
<td>23</td>
</tr>
<tr>
<td>Task Manager</td>
<td>25</td>
</tr>
</tbody>
</table>
Chapter 1

Remote Control

In This Chapter

Remote Cntl Tab 4
Control Machine 5
Video Streaming 7
Reset Password 9
Power Mgmt 10
Select Type 11
Set Parameters 13
Preinstall RC 14
Uninstall RC 15
Admin Role Policy 16
Machine Policy 18
FTP 19
Chat 22
Send Message 23
Task Manager 25
Remote Cntl Tab

View and operate managed machines as if they were right in front of you simply by clicking its machine ID.

- Automatically connects the administrator to the remote computer independent of any gateway or firewall configurations, even behind NAT.
- Remote control even without a 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.
- Policy settings allow users to block remote control or require administrators to ask permission before accessing a machine.
- Integrates four best of breed remote control packages: WinVNC, pcAnywhere™ (Symantec), RAdmin (Famatech), or Terminal Server (Microsoft).
- FTP to any managed machine and access files even behind NAT gateways and firewalls.
- Direct chat with any managed machine. Perfect for supporting dial up users with only a single phone line. Remote control and chat at the same time.


<table>
<thead>
<tr>
<th>Functions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Machine</td>
<td>Allows administrators to view and/or take control of a managed machine's desktop remotely for troubleshooting and/or instructional purposes.</td>
</tr>
<tr>
<td>Video Streaming</td>
<td>Remote control machines that do not have an agent installed.</td>
</tr>
<tr>
<td>Reset Password</td>
<td>Reset the password for a local account on a managed machine.</td>
</tr>
<tr>
<td>Power Mgmt</td>
<td>Powers on, powers off or reboots vPro-enabled machines.</td>
</tr>
<tr>
<td>Select Type</td>
<td>Specify the type of remote control software the VSA uses on a per machine basis. WinVNC, Remote Administrator, pcAnywhere, and Terminal Server are all supported.</td>
</tr>
<tr>
<td>Set Parameters</td>
<td>Specify the remote control settings to use with each remote control package.</td>
</tr>
<tr>
<td>Preinstall RC</td>
<td>Install the remote control service</td>
</tr>
<tr>
<td>Uninstall RC</td>
<td>Uninstall the remote control service</td>
</tr>
<tr>
<td>FTP</td>
<td>Initiate an FTP session with any remote managed machine.</td>
</tr>
<tr>
<td>Chat</td>
<td>Start a chat session between an administrator and any remote machine.</td>
</tr>
<tr>
<td>Send Message</td>
<td>Allows administrators to send network messages to selected managed machines.</td>
</tr>
<tr>
<td>Task Manager</td>
<td>Remotely executes the NT task manager and displays data in the browser.</td>
</tr>
</tbody>
</table>
Control Machine

Remote Ctrl > Control Machine

The Control Machine page establishes a remote control session between the administrator's local machine and a selected machine ID. Select the type of package to remote control a managed machine using Select Type (page 11). Set parameters for remote control sessions using Set Parameters (page 13).

Note: Use Video Streaming (page 7) to remote control a target machine that does not have an agent.

Automatic Installation

If WinVNC, K-VNC or RAdmin are not installed on a machine and a remote control session is initiated using Control Machine (page 5) or Video Streaming (page 7), then these packages are 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 WinVNC, K-VNC or RAdmin on any managed machine using Preinstall RC (page 14).

Note: Uninstalling an agent does not remove the installed remote control package. Before you delete the agent, use Remote Control > Uninstall RC (page 15) to uninstall remote control on the managed machine.

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

- Agent has checked in
- Agent has checked in and user is logged on. Tool tip lists the logon name.
- Agent has not recently checked in
- Agent has never checked in
- Online but waiting for first audit to complete
- The agent is online but remote control is 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.

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 administrator or 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 administrator machine. Helper applications, unique to each supported remote control or FTP package, automatically determine the optimal routing path between the administrator machine and the target machine. If a
Remote Control

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).

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 KServer itself. Use this feature to remotely manage your own KServer. Only master administrators can remote control the KServer.

Remote Control and FTP for Users
Administrators can provide users with the same remote control and FTP access that administrators have using Agent > User Access.

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

- The administrator machine is blocking outbound traffic on the agent check-in port (default 5721). The firewall may need to be reconfigured.
- The target machine is on a slow connection. Let the applications run longer than the timeout period and see if that works.
- 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 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.
- 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 Terminal Server session is connecting from the localhost.

Warning: Using the credential of a currently logged on user confuses XP. It can not determine if the user is reactivating the existing session locally or remotely initiating a new connection. As a result, Window XP may hang, requiring a reboot to recover. The VSA can not protect you from this. Do not log on using the user name of an already logged on account.

- Your pcAnywhere viewer is connecting to your administrator machine, not the target 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.
- 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.
  1. Open the pcAnywhere application and click on the Remote Control function.
  2. Click Add Remote Control Item.
  3. Create an item named Network.
  4. Select TCP/IP as the connection device.
  5. Leave the host name blank.
Check-in status

These icons indicate the agent check-in status of each managed machine:

- 🟢 Agent has checked in
- 🔴 Agent has checked in and user is logged on. Tool tip lists the logon name.
- 💡 Agent has not recently checked in
- ⬤ Agent has never checked in
- 🟠 Online but waiting for first audit to complete
- 🟠 The agent is online but remote control is disabled
- 🔴 The agent has been suspended

Remote Control Package

The remote control package assigned to this machine ID. Select the type of package to remote control a managed machine using Select Type (page 11).

- 🔴 WinVNC
- 🟠 K-VNC
- 🔴 Remote Administrator
- 🟠 pcAnywhere
- 🟠 RDP/Terminal Server

Machine.Group ID

The list of Machine ID.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the administrator is authorized to see using System > Group Access. Only machine IDs with an 🟢 icon can be remote controlled and have live links; all others will be inactive.

Current User

The user currently logged into the managed machine.

Active Admin

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

---

Video Streaming

Remote Cnt! > Video Streaming

The Video Streaming page establishes a remote control session between the administrator's local machine and a machine without an agent. Use it to help someone quickly on an infrequent basis. If you plan to provide continuous support we recommend you install an agent.

The following conditions apply:

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

Set parameters for remote control sessions using Set Parameters (page 13). See Select Type (page 11) for a description of the different types of remote control packages.
Remote Control

Note: Use Control Machine (page 5) to remote control a target machine that has an agent.

Automatic Installation
If WinVNC, K-VNC or RAdmin are not installed on a machine and a remote control session is initiated using Control Machine (page 5) or Video Streaming (page 7), then these packages are automatically installed. Installation does not require a reboot. Automatic installation takes up to an extra minute.

Automatic Uninstallation
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.

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 administrator or 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 administrator machine. Helper applications, unique to each supported remote control or FTP package, automatically determine the optimal routing path between the administrator machine and the target machine. If a direct connection is not possible then the helper applications route the remote control traffic through the KServer on the same port used by agents to check-in (default 5721).

Remote Control Malfunctions
Some reasons for remote control failure—for both target machines with and without an agent—are:
- The administrator machine is blocking outbound traffic on the agent check-in port (default 5721). The firewall may need to be reconfigured.
- The target machine is on a slow connection. Let the applications run longer than the timeout period and see if that works.
- 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 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.

Start
Click the Start button. Ask the remote user to display the http://<yourKServerURL>/gethelp.asp web page and click your administrator name to begin the video streaming session.

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.

Select remote control package to use
The default remote control service uses WinVNC. See Select Type (page 11) for a description of the different types of remote control packages.
Specify the default HTML message seen by users when no administrator is waiting to help.

This is the message displayed if the user displays the http://<yourKServerURL>/gethelp.asp web page and no administrator is logged into the KServer.

Reset Password

The Reset Password page creates a new password and, if necessary, a new user account on a managed machine. If the username does not already exist, checking the Create new account checkbox creates a new account with the specified password. Reset Password returns an error if you attempt to reset the password for a username that is not already created on the managed machine or if you create a password that is already being used by a user account. Blank passwords are not permitted.

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

Resetting the Administrator Password

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

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

Note: On non-domain controllers, only the local user account on the target 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 as an administrator.

Password / Confirm

Enter a new password.
Remote Control

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:

- ![Agent has checked in](image)
- ![Agent has checked in and user is logged on. Tool tip lists the logon name.](image)
- ![Agent has not recently checked in](image)
- ![Agent has never checked in](image)
- ![Online but waiting for first audit to complete](image)
- ![The agent is online but remote control is disabled](image)
- ![The agent has been suspended](image)

Machine.Group ID

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

Status

The status of pending password changes and user account creations.

Power Mgmt

Remote Cntl > Power Mgmt

The Power Mgmt 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.

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

This page provides you with the following actions:

- **Schedule** - Display a popup window of the following schedule options:
  - **Schedule / Cancel** - Schedule or cancel these schedule options.
  - **Schedule Date/Time** - Select the date and time to schedule this task.
  - **Recurrence** - Select whether to run this task once, hourly, daily monthly. If more than once, enter the number of times to run this task for the period selected.
  - **Skip if offline** - Check to perform this task only at the scheduled time. If the machine is offline, skip and run the next scheduled period and time. Uncheck to perform this task as soon as the machine connects after the scheduled time.
  - **Stagger by N minutes** - You can distribute the load on your network by staggering this task. If you set this parameter to 5 minutes, then the scan on each machine ID is staggered by 5 minutes. For example, machine 1 runs at 10:00, machine 2 runs at 10:05, machine 3 runs at 10:10, ...
- **Run Now** - Run the power management options now on selected machine IDs.
Remote Control

- **Cancel** - Cancel schedule options for selected machined IDs.
- **Power Up / Power Down / Reboot** - Select the power management option to execute.

**Host Name**

The unique local name and domain name of a vPro enabled-machine on a network, using the format `<domainname>.<computername>`.

**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.

**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.

**Type**

The power management option scheduled to be executed.

**Last Power Mgmt**

The last time a power management option was executed.

**New Power Mgmt**

The next time a power management option is scheduled to be executed.

**Credentials**

If not-checked, a vPro credential is not registered in the VSA for this vPro-enabled machine and you cannot execute power management option. If checked, a vPro credential is registered in the VSA. In either case, you can click any cell in the **Credentials** column to display a popup window that lets you register a credential.

**Recur Interval**

The interval for the scheduled task to recur.

**Skip if Machine Offline**

If a checkmark ☑ displays and the machine is offline, skip and run the next scheduled period and time. If no checkmark displays, perform this task as soon as the machine connects after the scheduled time.

**Stagger By**

The number of minutes to stagger this task on multiple machines.

---

**Select Type**

*Remote Ctrl > Select Type*

The **Select Type** page specifies which remote control package is used by **Control Machine** (page 5) 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.
Virtual Network Computing

Virtual Network Computing (VNC), also called remote control or remote desktop, is a graphical desktop sharing system which uses the Remote Framebuffer (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 target machine that shares its screen. The VNC client (or viewer) is the program on the administrator's machine that watches and interacts with the target 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 VSA supports the following third party remote control packages.

- WinVNC - This open source, freely available, remote control package comes bundled with the VSA. WinVNC is the default package used on all managed machines. The VSA automatically installs WinVNC servers on selected machines the first time you remote control that machine.

- K-VNC - The enterprise version of VNC. This is the only remote control option available for Vista. It can also be used on Windows 2000, XP and 2003. The VSA automatically installs the K-VNC server on selected machines the first time you remote control that machine.

- Remote Administrator - RAdmin is a commercially available remote control package offering both high speed and file transfer capability. Use RAdmin where bandwidth limitations exist or you need remote file transfer to the machine. The VSA automatically installs the RAdmin server on selected machines the first time you remote control that machine. The RAdmin package bundled with the VSA expires after 30 days. Obtain licenses from www.radmin.com.

- pcAnywhere - pcAnywhere is a widely used remote control package available from Symantec. The VSA fully supports pcAnywhere but does not automatically install it. You must purchase pcAnywhere separately and install it on the workstation before you can use this option. Combining the VSA with existing installations of pcAnywhere allows you to remote control machines behind gateways without mapping ports or opening firewalls.

- Terminal Server - Microsoft Terminal Server is only available with Windows NT, 2000, XP, or 2003. The VSA does not automatically install Terminal Server but does allow you to remote control machines behind gateways without mapping ports or opening firewalls. XP comes pre-installed with Terminal Service access for a single user. For other operating systems see Terminal Service Client Access License requirements on the Microsoft website.

To Assign Remote Control Packages to Machine IDs

1. Select the type of package to use from the drop down list.
2. Check the box to the left of machine IDs you want to use this remote control package.
3. Click the Select button.

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:

- Agent has checked in
- Agent has checked in and user is logged on. Tool tip lists the logon name.
- Agent has not recently checked in
Remote Control

- Agent has never checked in
- Online but waiting for first audit to complete
- The agent is online but remote control is disabled
- The agent has been suspended

**Machine Group ID**

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

**Remote Control Package**

The remote control package assigned to this machine ID.

- WinVNC
- K-VNC
- Remote Administrator
- pcAnywhere
- RDP/Terminal Server

---

**Set Parameters**

*Remote Cntl > Set Parameters*

The *Set Parameters* page sets the default parameters for your remote control session. These settings are remembered on a per administrator basis. Changes take effect immediately and are reused every time you start remote control. See *Select Type* (page 11) for a description of the different types of remote control packages.

**WinVNC and K-VNC Options**

- **View Only Mode** - The administrator can view the remote machine. No mouse or keyboard events are sent to the target 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 on the listening machine is set to 64 colors. This is useful for slower connections.
- **Full Screen mode** - The entire display of the administrator machine is used to display the screen contents of the target machine. Exit by displaying the remote control menu (default F8) and unselect Full screen.

**RAdmin Options**

- **Full Control** - The administrator can view and/or control the screen keyboard and mouse of the target machine.
- **View Only** - The administrator can view the remote machine. No mouse or keyboard events are sent to the target 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 target machine and one for the administrator machine. Drag and drop files between the two machines in this mode.
- **Full Screen View Mode** - The entire display of the administrator machine is used to display the screen contents of the target machine. This option is only available in a Full Control or View Only session.
Remote Control

- **Encrypt Data Stream** - Checking this box encrypts all traffic between the administrator and target machines.
- **Update/sec** - Sets the maximum number of update per second RAdmin generates. Higher update rates consume more CPU cycles on the remote machine.
- **Color Format** - Specifies the number of colors used for remote control. Large color formats use more bandwidth.

Terminal Service 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 remote computer for faster processing.

Preinstall RC

Remote CntI > Preinstall RC

The Preinstall RC page 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 **Select Type** (page 11). When an install is pending on any machine ID this page automatically refreshes every 5 seconds until the script completes.

**Note:** Preinstall RC does not install pcAnywhere or Terminal Server.

Automatic Installation

If WinVNC, K-VNC or RAdmin are not installed on a machine and a remote control session is initiated using **Control Machine** (page 5) or **Video Streaming** (page 7), then these packages are 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 WinVNC, K-VNC or RAdmin on any managed machine using **Preinstall RC** (page 14).

**Note:** Uninstalling an agent does not remove the installed remote control package. Before you delete the agent, use Remote Control > Uninstall RC (page 15) to uninstall remote control on the managed machine.

Install

Click **Install** to install WinVNC, K-VNC or RAdmin on selected machine IDs.

Cancel

Click **Cancel** to clear pending install scripts 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:
Remote Control

- Agent has checked in
- Agent has checked in and user is logged on. Tool tip lists the logon name.
- Agent has not recently checked in
- Agent has never checked in
- Online but waiting for first audit to complete
- The agent is online but remote control is disabled
- The agent has been suspended

**Machine.Group ID**

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

**Remote Control Package**

The remote control package assigned to this machine ID. Select the type of package to remote control a managed machine using Select Type (page 11).

- **WinVNC**
- **K-VNC**
- **Remote Administrator**
- **pcAnywhere**
- **RDP/Terminal Server**

**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.

---

**Uninstall RC**

**Remote Cntl > Uninstall RC**

The Uninstall RC page 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 Select Type (page 11). When an uninstall is pending on any machine ID this page automatically refreshes every 5 seconds until the script 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 problem installs. A fresh copy of the remote control package is installed the next time a remote control session is started or using Preinstall RC (page 14).

**Note:** Uninstall RC does not uninstall pcAnywhere or Terminal Server.

**Note:** Uninstalling an agent does not remove the installed remote control package. Before you delete the agent, use Remote Control > Uninstall RC (page 15) to uninstall remote control on the managed machine.

**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...
Remote Control

registry additions.

Uninstall

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

Cancel

Click **Cancel** to clear pending uninstall scripts 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:

- ![Agent has checked in](image)
- ![Agent has checked in and user is logged on. Tool tip lists the logon name.](image)
- ![Agent has not recently checked in](image)
- ![Agent has never checked in](image)
- ![Online but waiting for first audit to complete](image)
- ![The agent is online but remote control is disabled](image)
- ![The agent has been suspended](image)

Remote Control Package

The remote control package assigned to this machine ID. Select the type of package to remote control a managed machine using **Select Type** (page 11).

- ![WinVNC](image)
- ![K-VNC](image)
- ![Remote Administrator](image)
- ![pcAnywhere](image)
- ![RDP/Terminal Server](image)

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.

Admin Role Policy

**Remote Cntl > Admin Role Policy**

The **Admin 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 administrator roles.

Note: See Machine Policy (page 18) to apply remote control notification policies by machine ID. Machine policy takes precedence over administrator role policy.
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 cancelled.

Notify user when session terminates.

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 administrators 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 user.

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 an administrator 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 administrator roles.
Remote Control

Policy

The remote control policy applied to an administrator role.

Message

The Session Termination Message applied to an administrator role.

Machine Policy

Remote Cntl > 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 Admin Role Policy (page 16) to apply remote control notification policies by machine ID. Machine policy takes precedence over administrator role policy.

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 cancelled.

Notify user when session terminates.

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 administrators 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 user.

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 ID.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the administrator is authorized to see using System > Group Access.

Policy

The remote control policy applied to a machine ID.

Message

The Session Termination Message applied to a machine ID.

FTP

Remote Cntl - FTP

The FTP page establishes a FTP session between the administrator's local machine and a selected machine ID. The VSA uses the FTP client built into Internet Explorer so you can operate with the same Windows look and feel. 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.

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 administrator's 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.

Initiating FTP

Initiate a FTP session 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 icon can be connected to target machines and have live links; all others will be inactive.
Remote Control

- Agent has checked in
- Agent has checked in and user is logged on. Tool tip lists the logon name.
- Agent has not recently checked in
- Agent has never checked in
- Online but waiting for first audit to complete
- The agent is online but remote control is 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.

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 administrator or 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 administrator machine. Helper applications, unique to each supported remote control or FTP package, automatically determine the optimal routing path between the administrator machine and the target machine. If a direct connection is not possible then the helper applications route the remote control traffic through the KServer on the same port used by agents to check-in (default 5721).

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 KServer itself. Only master administrators can FTP the KServer.

Remote Control and FTP for Users

Administrators can provide users with the same remote control and FTP access that administrators have using Agent > User Access.

FTP Malfunctions

Some reasons for FTP failure with managed machines are:

- The administrator machine is blocking outbound traffic on the agent check-in port (default 5721). The firewall may need to be reconfigured.
- The target machine is on a slow connection. Let the applications run longer than the timeout period and see if that works.
- 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 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.

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.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:

- Agent has checked in
- Agent has checked in and user is logged on. Tool tip lists the logon name.
- Agent has not recently checked in
- Agent has never checked in
- Online but waiting for first audit to complete
- The agent is online but remote control is disabled
- The agent has been suspended

Machine.Group ID

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

Enter a drive letter to FTP to

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

Note: The KServer determines how many fixed disks a managed machine has via its Latest Audit.
Chat

The Chat page initiates or continues chat sessions with 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.

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 the next time it checks in. 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 into the KServer, respond by entering text in the text pane. Click the Send button to send the message.

Join Session link
Multiple administrators may participate in the same chat session with a user. If a chat session is in progress, the Join Session link 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 Administrators
The names of logged in administrators with Group Access rights to the group IDs currently displayed by the machine ID.group ID filter display on the Chat page as well. Click the link of another logged in administrator to initiate a chat with that administrator.

Enable / Disable the User's Ability to Initiate Chat with Administrators
Administrators can enable / disable the user's ability to initiate a chat session using Agent > User Access.

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.
4. Select (None) from the drop down control labeled Name.
5. Click OK.
**Remote Control**

**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 administrators.

**Remove your name from chat list seen by users**

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

**Check-in status**

These icons indicate the agent check-in status of each managed machine:

- ![Agent has checked in](image)
- ![Agent has checked in and user is logged on. Tool tip lists the logon name.](image)
- ![Agent has not recently checked in](image)
- ![Agent has never checked in](image)
- ![Online but waiting for first audit to complete](image)
- ![The agent is online but remote control is disabled](image)
- ![The agent has been suspended](image)

**Machine.Group ID**

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

---

**Send Message**

**Remote Cntl > Send Message**

The **Send Message** page sends network messages to a select group of users. 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 user click's the flashing icon the message displays.

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.

**Note:** Send and receive messages to and from other administrators using Home > View Dashboard.
Remote Control

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 when the recipient's machine conducts its next check-in. The message displays in the Messages Not Yet Sent column until the message is received by the recipient machine.

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 recipient machine.

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.

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:
- Agent has checked in
- Agent has checked in and user is logged on. Tool tip lists the logon name.
- Agent has not recently checked in
- Agent has never checked in
- Online but waiting for first audit to complete
- The agent is online but remote control is disabled
- The agent has been suspended
Remote Control

**Machine.Group ID**

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

**Current User**

Displays the currently logged on user.

**Messages Not Yet Sent**

This column displays messages not yet sent.

---

## Task Manager

Remote Cntl > 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.

**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.