



---

# Remote Control

---

**User Guide**

Version R94

English

February 9, 2017

## **Copyright 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."

# Contents

Remote Control Overview .....	1
RDP.....	1
K-VNC.....	2
Control Machine.....	2
Reset Password.....	4
Select Type.....	5
Set Parameters.....	6
Preinstall RC .....	7
Uninstall RC .....	8
User Role Policy.....	8
Machine Policy.....	10
FTP .....	11
SSH.....	12
Task Manager.....	13
Chat .....	14
Send Message.....	15
Index.....	19



---

# 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
<b>Control Machine</b> (page 2)	Allows users to view and/or take control of a managed machine's desktop remotely for troubleshooting and/or instructional purposes.
<b>Reset Password</b> (page 4)	Reset the password for a local account on a managed machine.
<b>Preinstall RC</b> (page 7)	Install the remote control service
<b>Uninstall RC</b> (page 8)	Uninstall the remote control service
<b>User Role Policy</b> (page 8)	Determines how machine users are notified that a remote control session to their machine is about to begin. Set by VSA user role.
<b>Machine Policy</b> (page 10)	Determines how machine users are notified that a remote control session to their machine is about to begin. Set by machine ID.
<b>FTP</b> (page 11)	Initiate an FTP session with any remote managed machine.
<b>SSH</b> (page 12)	Runs an SSH command line session on a selected, active Linux or Apple machine.
<b>Task Manager</b> (page 13)	Remotely executes the NT task manager and displays data in the browser.
<b>Chat</b> (page 14)	Start a chat session between a user and any remote machine.
<b>Send Message</b> (page 15)	Allows users to send network messages to selected managed machines.

---

## RDP

You can launch RDP sessions using the following methods:

- Navigate to Remote Control > Desktop Control > Control Machine and click on the hyperlinked machine.group name

## K-VNC

- Use the 'RDP Machine' button on the Quick Launch ribbon of Quick View. To display the 'RDP Machine' button set the Select Type for the machine to RDP, then click the 'Gear' icon in Quick View to add the button in the configuration window.

These additional pages support RDP sessions:

- Remote Control > Configure > **Select Type** (page 5) - You can now select the type of remote control session launched by each machine on the Control Machine page: K-VNC or RDP.
- Remote Control > Configure > **Set Parameters** (page 6) - Sets options for RDP sessions.
- RDP sessions can be managed using **User Role Policy** (page 8) and **Machine Policy** (page 10).

## Microsoft RDP

Microsoft RDP is licensed under terms set forth by the makers of Microsoft RDP (Microsoft) and is licensed separately. The VSA fully supports use of Microsoft RDP by you but does not automatically install it. You may use the VSA with your installations of Microsoft RDP to allow you to remote control Windows NT, 2000, XP, Vista, Windows 7, 8, 8.1, 2003, 2008, 2012, or 10 machines behind gateways without mapping ports or opening firewalls.

---

# K-VNC

A K-VNC remote control session can be started using the Remote Control > **Control Machine** (page 2) page. Administrators should use the **K-VNC** (page 5) for situations not supported by **Kaseya Remote Control** and **RDP** (page 1).

These additional pages support K-VNC sessions:

- Remote Control > Configure > **Select Type** (page 5) - You can now select the type of remote control session launched by each machine on the Control Machine page: K-VNC or RDP.
- K-VNC sessions can be managed using **User Role Policy** (page 8) and **Machine Policy** (page 10).

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. For an introduction to the toolbar see **RealVNC** (<https://www.realvnc.com/products/vnc/documentation/5.0/guides/user/af1014926.html>). Setting configuration options begins with **this topic**

(<https://www.realvnc.com/products/vnc/documentation/5.0/guides/user/af1015933.html>).



## Virtual Network Computing (VNC)

**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 Kaseya Server primarily to provide immediate technical support. VNC is platform-independent. A VNC viewer on any operating system can usually connect to a VNC server on any other operating system. The **VNC server** is the program on the remote machine that shares its screen. The **VNC client (or viewer)** is the program on the local machine that watches and interacts with the remote machine. The VNC client machine requires user access rights to the VNC server machine. Since Kaseya VNC sessions are relayed through the Kaseya Server, all VNC sessions are protected by 256 bit rolling encryption protocol.

---







# 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. The type of remote control session launched by a machine is specified using the **Select Type** (page 5) page.


### Actions

- **(Initiate Remote Control)** - Click the hyperlinked 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.
  -  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
- **Record all remote control session** - If checked, **Kaseya Remote Control** (page 2) sessions on Windows and Mac machines are recorded. Recordings are viewed using the Agent > Screen Recordings page. See Recording KRC Sessions.
- **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.

### Columns

- **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 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** - The user currently logged on to the managed machine.
- **Active Admin** - The VSA user currently conducting a remote control session to this machine ID.

### Additional Guidelines

- **Users Can Disable Remote Control Access** - 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.
- **Automatic Installation of K-VNC** - If K-VNC is not already installed on a machine and a remote control session is initiated using Control Machine, 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 7).
- **Uninstalling K-VNC** - 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 to uninstall K-VNC on the managed machine. Uninstall all add-on module clients as well.
- **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.

## Reset Password

- **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.

---

# 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
-  An agent icon adorned with a red clock badge is a temporary agent.

**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.

# Select Type

[Remote Control](#) > [Configure](#) > [Select Type](#)

The [Select Type](#) page specifies the remote control package used by [Control Machine](#) (page 2) to remote control a managed machine. Each machine ID displays the icon of the remote control package it is currently assigned to use.

**Select remote control package to use with selected machines**

- [K-VNC](#)  - The enterprise version of VNC. Administrators should use K-VNC for situations not supported by [Kaseya Remote Control](#) and RDP.
- [RDP](#)  - Microsoft RDP is only available with Windows NT, 2000, XP, Vista, Windows 7, 2003 or 2008.
- [KRC](#) - Kaseya Remote Control.

**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.










## Set Parameters

### 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
-  An agent icon adorned with a red clock badge is a temporary agent.

### 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.

### Remote Control Package

The remote control package assigned to this machine ID.

-  K-VNC
-  RDP

---

# Set Parameters

## Remote Control > Configure > Set Parameters

The [Set Parameters](#) page sets the default parameters for **RDP** (*page 1*) sessions. *These settings are remembered on a per VSA user basis. Changes take effect immediately and are reused every time you start remote control.*

### RDP Options

- **Console mode** - Remote control the console session of the remote machine.
- **Full Screen mode** - Use your full screen to remote control the remote machine.
- **Fixed Screen size** - Set a fixed width and height for your remote control session.
- **Share Disk Drives** - Connect your disk drives to the remote machine.
  - **Only share the following disks** - Enter the specific drive letters to share, or leave blank to share all disks.
- **Share Printers** - Connect your printers to the remote machine.
- **Disable Desktop Wallpaper** - Turn off wallpaper on the remote machine for faster processing.

# Preinstall RC

[Remote Control](#) > [Configure](#) > [Preinstall RC](#)

The [Preinstall RC](#) page installs K-VNC 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 of K-VNC

If K-VNC is not already installed on a machine and a remote control session is initiated using [Control Machine](#) (page 2), 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 7).

**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 8) 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.

## 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
-  An agent icon adorned with a red clock badge is a temporary agent.

## 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 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 7).

**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 8) 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
-  An agent icon adorned with a red clock badge is a temporary agent.

## 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 10) to apply remote control notification policies by machine ID. Machine policy takes precedence over user role policy.

## Exceptions

K-VNC supports all options on this page. Kaseya Remote Control supports all options on this page except **Notify user when session terminates**.

## Actions

- **Apply** - Applies policy parameters to selected roles.
- **Remove** - Clears policy parameters from selected roles.
- **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.

## Parameters

- **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.
- **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.
- **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.
- **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 all remote control session** - If checked, **Kaseya Remote Control** (page 2) sessions on Windows and Mac machines are recorded. Recordings are viewed using the Agent > Screen Recordings page. See Recording KRC Sessions.

## Columns

- **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 8) to apply remote control notification policies by machine ID. Machine policy takes precedence over user role policy.

## Exceptions

K-VNC supports all options on this page. Kaseya Remote Control supports all options on this page except **Notify user when session terminates**.

## Actions

- **Apply** - Applies policy parameters to selected machine IDs.
- **Remove** - Clears policy parameters from 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.
- **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.

## Parameters

- **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.
- **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.
- **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.
- **Require admin note to start remote control** - Check 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 all remote control session** - If checked, **Kaseya Remote Control** (page 2) sessions on Windows and Mac machines are recorded. Recordings are viewed using the Agent > Screen Recordings page. See Recording KRC Sessions.

### Columns

- **Machine.Group ID** - The list of Machine 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.


### Actions

- **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.
  -  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
- **Enter a drive letter to FTP to** - After clicking a machine ID you can optionally 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.

- **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 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.

### Additional Guidelines

- **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.
- **Users Can Disable Remote Control Access** - 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.
- **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

## SSH

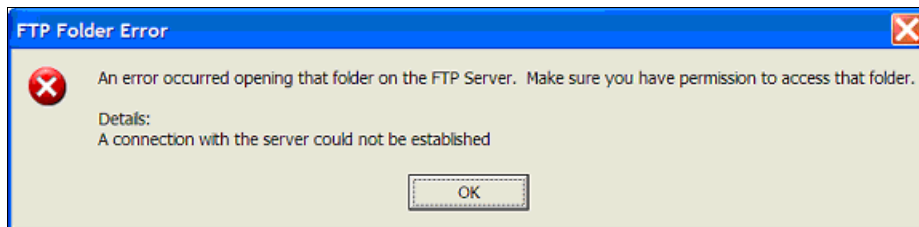
primarily to provide immediate technical support. Once connected, the client can upload files to the server, download files from the server, rename or delete files on the server and so on. Any software company or individual programmer is able to create FTP server or client software because the protocol 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 256 bit rolling encryption protocol.

- **Uploading Files** - You can also use Live Connect to upload and download files using the **Files** menu.

### 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.

---

## 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](#) to chat with machine users.

### 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
-  An agent icon adorned with a red clock badge is a temporary agent.

### 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.

## Send Message

### 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
-  An agent icon adorned with a red clock badge is a temporary agent.

**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.



---

# Index

## C

Chat • 14  
Control Machine • 2

## F

FTP • 11

## K

K-VNC • 2

## M

Machine Policy • 10

## P

Preinstall RC • 7

## R

RDP • 1  
Remote Control Overview • 1  
Reset Password • 4

## S

Select Type • 5  
Send Message • 15  
Set Parameters • 6  
SSH • 12

## T

Task Manager • 13

## U

Uninstall RC • 8  
User Role Policy • 8