Remote Control

User Guide

Version R95

English

July 7, 2021

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

Contents

Remote Control Overview

View and operate managed machines as if they were right in front of you simply by clicking its machine ID. The **Remote Control** module enables you to:

- Automatically connect the user to the remote computer independent of any gateway or firewall configurations, even behind NAT.
- Work independently or with the user to solve problems interactively where both parties can see what is happening in real time.
- Set policies that allow users to block remote control or require users to ask permission before accessing a machine.
- FTP to any managed machine and access files even behind NAT gateways and firewalls.
- Direct chat with any managed machine. Perfect for supporting dial up users with only a single phone line. Remote control and chat at the same time.
- Power up, power down, bootup or reboot vPro-enabled machines.

Functions	Description
Reset Password *(page i)*	Reset the password for a local account on a managed machine.
User Role Policy *(page iii)*	Determines how machine users are notified that a remote control session to their machine is about to begin. Set by VSA user role.
Machine Policy *(page iv)*	Determines how machine users are notified that a remote control session to their machine is about to begin. Set by machine ID.

Live Connect & Remote Control - Video Overview

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.

- Agent is currently offline
- User Logged In and Agent is Active
- User Logged In and Agent is Inactive
- User Not Logged In and Agent is online
- User Not Logged In and Agent is Idle
- The agent has been suspended
- Agent has never checked in

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.

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

Exceptions

Applies only to "shared" (console) remote control sessions. Does not apply to **Terminal Server Sessions http://help.kaseya.com/WebHelp/EN/VSA/9050000/17978.htm**.

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.

> **Note:** Only the console user will receive notifications and have the ability to approve sessions. Notifications will not be displayed for terminal server *(RDP)* session users. If the "If user logged in ask permission" option is selected, the remote control session will proceed if there is no user logged onto the console (even if there are terminal session users logged in).

- **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** - 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.
- **Disable Remote Control File Transfer** - gives the ability to transfer files directly between the source machine and the remote control target, directly within the remote control application. In this case, users do not have to use the Live Connect application to transfer files while working in an active Remote Control session. This option is enabled by default per user role and per machine.

> **Note:** By VSA design, Machine Policy takes precedence over User Role Policy. For example, if a VSA agent has Remote Control File Transfer "disabled" in its Machine Policy, Remote Control File Transfer will be disabled for any user of VSA when Remote Controlling said device. If Remote Control File Transfer is not "disabled" in a Machine Policy but is "disabled" in a User Role Policy, Remote Control File Transfer will be disabled for any Remote Control session performed while such User Role is in use.

- **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 i)* sessions on Windows and Mac machines are recorded. Recordings are viewed using the Agent > Screen Recordings page. See Recording KRC Sessions.
- **1-Click Access -** - If checked, it enables 1-Click Access function to selected role.. See 1-Click Access Requirements.

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

Exceptions

Applies only to "shared" (console) remote control sessions. Does not apply to **Terminal Server Sessions http://help.kaseya.com/WebHelp/EN/VSA/9050000/17978.htm**.

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.

Note: Only the console user will receive notifications and have the ability to approve sessions. Notifications will not be displayed for terminal server *(RDP)* session users. If the "If user logged in ask permission" option is selected, the remote control session will proceed if there is no user logged onto the console (even if there are terminal session users logged in).

- **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** - 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.
- **Disable Remote Control File Transfer** - gives the ability to transfer files directly between the source machine and the remote control target, directly within the remote control application. In this case, users do not have to use the Live Connect application to transfer files while working in an active Remote Control session. This option is enabled by default per user role and per machine.

  Note: By VSA design, Machine Policy takes precedence over User Role Policy. For example, if a VSA agent has Remote Control File Transfer "disabled" in its Machine Policy, Remote Control File Transfer will be disabled for any user of VSA when Remote Controlling said device. If Remote Control File Transfer is not "disabled" in a Machine Policy but is "disabled" in a User Role Policy, Remote Control File Transfer will be disabled for any Remote Control session performed while such User Role is in use.

- **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 i)* sessions on Windows and Mac machines are recorded. Recordings are viewed using the Agent > Screen Recordings page. See Recording KRC Sessions.
- **1-Click Access -** If checked, it enables 1-Click Access function to selected role.. See 1-Click Access Requirements.

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.

Index