vPro

User Guide

Version R9

English

March 5, 2015

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

vPro Overview

Remote activation of vPro machines is provided by **vPro**. This includes: power up, Windows shut down, force power down, view/change vPro password, remote control using KVM for unresponsive machines, boot to BIOS, and boot from ISO.

A feature called vPro Proxy enables access to machines behind a firewall and the ability to bypass entering a consent code that only displays locally on the vPro machine to initiate a remote vPro session. **vPro** can optionally send power commands to vPro-enabled agentless machines detected by the **Discovery** module. It can also power on an agentless machine specified by IP address.

vPro Module Requirements

Kaseya Server

- The vPro R9 module requires VSA R9.
- Installation is required. Usage is enabled by customer support request.

Requirements for a vPro Proxy

- The vPro Proxy requires 200 MB free space
- Microsoft .NET Framework 3.5

> **Note:** See general **System Requirements** *(http://help.kaseya.com/WebHelp/EN/VSA/9000000/reqs/index.asp#home.htm).*

Automated

vPro > Setup > Automated

The **Automated** page detects and activates vPro machines. The automated setup can be started, then resumed. For example, you might start setup then close the browser before setup is complete. Click the **Resume** button to return to where you were in the setup for a machine.

Automated setup includes configuring **vPro proxies** as needed for the discovered networks. vPro proxy machines are agent machines that relay vPro commands between the VSA and any vPro machines that share the same network as the proxy machine. A **vPro Proxy** *(page 2)* is required on each network you wish to send vPro power commands to, or to remote control machines.

Actions

- **Start New Wizard** - Click to start the **Automatic vPro Detection and Activation** wizard.
  - **Wizard Page 1** - Select the machines you wish to test for vPro capable chipsets that have not yet been detected. Optionally check the **Show Already Detected Machines** checkbox.
  - **Wizard Page 2** - For each detected vPro machine, accept or change the selection of an agent machine on the same network as the detected machine to act as a vPro Proxy machine. A vPro Proxy machine does not have to be a vPro capable machine. It only has to relay vPro commands to vPro enabled machines on the same network.
    - ✓ **Reassign** - Reassigns all machines assigned to a proxy.
    - ✓ **Change Proxy** - Reassigns a single machine to a new proxy.

- **Wizard Page 3** - Configure the agent machines selected to act as vPro Proxy machines. Specify the port the vPro Proxy will use to listen for **KVMView** *(page 9)* sessions initiated from the VSA by an administrator. Ensure any firewall and router the vPro Proxy is behind has opened this same port number.
  - ✓ **Change** - Edits the port number.
  - ✓ **Verify Pending** - Tests the connection between the VSA and the vPro proxy.
- **Wizard Page 4** - Check the the status of the ongoing detection and activation processes. This page updates automatically.

Incomplete Wizards Columns

The **Incomplete Wizards** table shows you the state **Automated Setup** is in for vPro machines that have not completed their setup.

- **Current Page** - The current page of the wizard.
- **Machine ID FilterMachine Group** - The machine id/group ID of an agent machine.
- **View** - The view used by the administrator when **Automated Setup** was interrupted.
- **Scope** - The scope used by administrator when **Automated Setup** was interrupted.
- **Admin** - The administrator running **Automated Setup** when it was interrupted.
- **Date** - The date/time **Automated Setup** was interrupted.
- **Resume** - Click to continue running **Automated Setup** for the selected machine.

vPro Proxy

vPro > Setup > vPro Proxy

The **vPro Proxy** page enables you to:

- Create a vPro Proxy on an agent machine. vPro machines on the same LAN as the vPro Proxy machine are automatically assigned to that vPro Proxy. After the vPro Proxy is created it is configured using the **Configure vPro Proxy** option.
- Manually assign selected machines to use a different vPro Proxy machine then the vPro Proxy they were automatically assigned.
- Remove the vPro Proxy.

A vPro Proxy is an agent machine that relays a connection to vPro machines. A vPro Proxy is required in the following cases:

- The target vPro machines are behind a firewall and you want to remote power up/force power down. The vPro Proxy is on the same LAN and requires no addition configuration.
- The target vPro machines are behind a firewall and you want to connect to them via **KVM** *(page 9)*. The vPro Proxy is on the same LAN and has a public IP address and port configured. You provide the VSA with the public IP address and port used by the vPro Proxy using the **Configure vPro Proxy** dialog.
- You want to enable (activate) target vPro machines via KVM without entering a consent code each time a KVM session is started. The vPro Proxy shares the same DNS server as the target machines and the vPro Proxy has a certificate appropriately configured. The certificate is only used when the vPro machine is enabled (activated). After that, KVM sessions start without entering a consent code.

Only one **KVMView** *(page 9)* session can run at a time, per vPro Proxy. The vPro Proxy requires Windows XP or later and does not have to be a vPro machine.

Configuring a vPro Proxy

1. Select a machine and click **Create a vPro Proxy**.
2. Click the **Configure** button for that machine.

3. Configure any of the three sections of the **Configure vPro Proxy** dialog independently from each other.
   - **Certificate Server** - Check this checkbox if you have **configured a security certificate on the the vPro Proxy machine** *(https://helpdesk.kaseya.com/entries/33171573)*.
   - **KVM Proxy** - Enter the public IP address and port of the vPro Proxy. This information is required if you want to use **KVMView** *(page 9)* to connect to vPro machines located behind a firewall.
   - **Remote ISO** - Select the **ISO files that you would like to boot vPro machines from** *(page 3)* that are assigned this vPro Proxy.

Actions

- **Create vPro Proxy** - Adds a **Configure** button to the **Configure** column of selected machines. Click a **Configure** button to configure vPro proxy settings for that machine.
- **Remove vPro Proxy** - Removes vPro proxy settings for selected machines.
- **Test vPro Proxy** - Tests connectivity to selected vPro proxy machines.

Table Columns

- **Machine ID** - The machine ID of an agent machine.
- **Is vPro Proxy** - `Yes`, if this machine is already a vPro Proxy. Otherwise this column displays messages like the following.
  - `Set Credential Account required for vPro Proxy` - See **Set Credential** *(http://help.kaseya.com/webhelp/EN/VSA/9000000/index.asp#352.htm)*.
  - `vPro Proxy is only supported on Windows operating systems`
  - `Windows XP or alter is required for vPro Proxy`
- **Has Certificate** - `Yes`, if the system has a vPro certificate.
- **KVM Proxy IP** - The IP address used to connect to the vPro Proxy.
- **KVM Proxy Port** - The port used to connect to the vPro Proxy.
- **Configure** - Click the **Configure** button for a row to change vPro Proxy settings on that machine.
- **Last Verified On** - The date/time the vPro Proxy connection was last verified.
- **Last Verify Status** - The result of the last verification.

Manage Boot ISOs

vPro > Setup > Manage Boot ISOs

The **Manage Boot ISOs** page uploads ISOs to your Kaseya Server. vPro machines are booted from ISOs using the **Remote Control** *(page 9)* page.

Note: A **vPro Proxy** *(page 2)* is required if the target vPro machine is behind a firewall.

Configuration

1. Upload ISOs to your Kaseya Server using vPro > Setup > **Manage Boot ISOs**.
2. Click the **Add ISO** button. Browse for the ISO you want to upload.

   Note: If a vPro machine is assigned a vPro Proxy then the ISO must then be uploaded to the vPro Proxy machine, using the **vPro Proxy** *(page 2)* page.

3. Use the vPro > **Remote Control** *(page 9)* page to **Boot from ISO**.

> **Note:** For more information about uploading large ISO files, see the Kaseya **knowledge base** *(https://helpdesk.kaseya.com/entries/35998997)*.

Actions

- **Add ISO** - Uploads an ISO to your Kaseya Server
- **Remove** - Removes an IOS from your Kaseya Server.

Table Columns

- **Name** - The name of a previously uploaded ISO file.
- **Description** - A description of the ISO.
- **Size** - The size in megabytes of the ISO.
- **Date** - The date/time the ISO was uploaded.

Detect and Activate

vPro > Setup > Detect and Activate

The **Detect and Activate** page detects and displays machines with vPro capable chipsets. Once detected, **vPro** can issue a command to enable or disable vPro on that machine. With a vPro enabled machine you can also use this page to manually assign a **vPro proxy** *(page 2)*. You can also enter a known password for a vPro machine activated outside of Kaseya or change the password of a vPro machine activated by Kaseya.

Actions

- **Detect** - Determines if selected machines have the vPro chipset and are vPro capable.

  > **Note:** See http://communities.intel.com/docs/DOC-2033 for help identifying versions of vPro capable machines.

- **Enable vPro** - Enables (activates) vPro capability on selected machines. A vPro machine must be enabled to perform any of the other functions on this page. The ability to enable a vPro machine remotely from the VSA depends on the version of AMT on the vPro machine.
  - **AMT 6.0 and below** - vPro must be enabled manually.
  - **AMT 6.1** - Host Based Configuration is *disabled* by default. Once enabled, vPro can be enabled by clicking the **Enable vPro** button.
  - **AMT 6.2** - Host Based Configuration *may be enabled*. Once enabled, vPro can be enabled by clicking the **Enable vPro** button.
  - **AMT 7.0 and above** - Host Based Configuration is *enabled* by default. vPro can be enabled by clicking the **Enable vPro** button.
- **Disable vPro** - Disables (deactivates) vPro capability on selected machines.
- **vPro Password**
  - **Assign New Password** - Reset a known, existing vPro password in both the vPro machine and the VSA. If a vPro machine is enabled for the first time using **vPro** then matching passwords are automatically set.
  - **Enter Existing Password** - If a vPro machine has already been enabled (activated) prior to being detected by the VSA the vPro password already exists. Use this option to enter the matching vPro password.

  > **Note:** The **AMT Password** column on this page shows the assigned vPro password for a machine.

- **Manually Assign vPro Proxy** - Manually assigns selected machines to a different **vPro Proxy** *(page 2)*.

Table Columns

- **Machine ID** - The machine ID / group ID of the agent machine.
- **AMT Version** - The version of Intel Active Management Technology used by the vPro machine.
- **Enabled** - If checked, vPro is enabled on this machine.
- **AMT Password** - The AMT password used to access to the vPro machine.
- **KVM Password** - The KVM password assigned this vPro machine.
- **KVM Mode**
  - **Client Control Mode** - When a **KVMView** *(page 9)* session is started, a randomly generated consent code is displayed on the remote machine's monitor. *You will need a local user to read the consent code to you.* Or,
  - **Admin Control Mode -** The machine was previously activated while associated with a vPro Proxy configured with a security certificate. **Instructions are provided for configuring a security certificate for a vPro Proxy** *(https://helpdesk.kaseya.com/entries/33171573)*. This advanced feature enables a VSA user to start a KVM session without requiring a consent code provided by a local user.
- **AMT SKU** - The type of Active Management Technology device. Different AMT SKUs support different sets of vPro features.
- **Associated vPro Proxy** - The vPro Proxy that relays a vPro connection to this machine.
- **Detection Date** - The date/time the vPro machine was detected.

Wireless

vPro > Setup > Wireless

The **Wireless** page creates WiFI profiles and associates them with managed vPro machines. This enables connection to vPro machines using wireless networks. A vPro machine must already have an agent installed on it and be activated to display on this page.

Creating Wifi Profiles

Select the **Create New Profile** drop-down option. Enter the following details for an existing WiFi network that can be used to connect to one or more of the managed vPro machines.

- **Profile Name** - The name of the WiFi profile.
- **SSID** - The WiFi network name.
- **Security Method** - `None`, `WEP`, `TKIP`, `CCMP`
- **Authentication Method**
  - For `None` or `WEP` security methods - `Open System` or `Shared Key`
  - For `TKIP` or `CCMP` security methods - `WPA PSK`, `WPA IEEE 802.1x`, `WPA2 PSK`, `WPA2 IEEE 802.1x`
- **Password** - Required for any authenticatication method other than `Open System`.
- **Limit to Kaseya Group** - Limits assignment of this WiFi profile to vPro machines in the specified organization/machine group.
- **Default for Kaseya Group** - Specifies this WiFi profile as the default profile for the specified organization/machine group.

Actions

- **Assign Wifi Profile** - Assigns a selected WiFi profile to selected vPro machines.
- **Create New Profile/<select>/Remove Existing Profile** - Creates, selects or removes WiFi profiles from this page.
- **Edit Profile** - Edits an existing WiFi profile.

- **Set Default Connection** - Sets the default connection used by Kaseya to connect to vPro machines assigned a WiFi profile.
  - `Connect via WiFi`
  - `Connect via Ethernet`
  - `Auto-Detect Connection` - Connects via the Ethernet connection if an IP address was detected on the Ethernet connection the last time vPro detection ran. Connects via the WiFi connection if an IP address was not detected on the Ethernet connection.

Alerts

`vPro > Setup > Alerts`

The **Alerts** page creates alerts in response to the success or failure of vPro events. The list of machine IDs you can select depends on the machine ID / group ID filter and the scope you are using.

To Create an Alert

1. Check any of these checkboxes to perform their corresponding actions when an alert condition is encountered:
   - Create **A**larm
   - Create **T**icket
   - Run **S**cript
   - **E**mail Recipients
2. Set additional email parameters.
3. Select one of the following:
   - `on vPro Power On Success`
   - `on vPro Power On Failed`
   - `on vPro Force Power Down Success`
   - `on vPro Force Power Down Failed`
4. Check the machine IDs to apply the alert settings to.
5. Click **Set** to assign the alert settings to selected machine IDs.

To Copy Alert Settings

1. Select `copy all settings from`.
2. Click **(click to select)** to select the **Desktop Policy** managed machine to copy alert settings from.
3. Check the machine IDs to apply the alert settings to.
4. Click **Set** to assign the alert settings to selected machine IDs.

Create Alarm

If checked and an alert condition is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List, Monitor > Alarm Summary and Info Center > Reporting > Reports > Logs > Alarm Log.

Create Ticket

If checked and an alert condition is encountered, a ticket is created.

Run Script

If checked and an alert condition is encountered, an agent procedure is run. You must click the **click to select** link to choose an agent procedure to run. You can optionally change the machine ID the agent procedure is run on by clicking **the machine with the alert** link.

Send email to

If checked and an alert condition is encountered, emails are sent to the specified email addresses.

- If the **Add to current list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.
- If the **Replace list** radio option is selected, when **Apply** is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.
- If **Remove** is clicked, all email addresses are removed **without modifying any alert parameters**.
- Email is sent directly from the Kaseya Server to the email address specified in the alert. Set the **From Address** using System > Outbound Email.

Check-in status

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

- Online but waiting for first audit to complete
- Agent online
- Agent online and user currently logged on.
- Agent online and user currently logged on, but user not active for 10 minutes
- Agent is currently offline
- Agent has never checked in
- Agent is online but remote control has been disabled
- The agent has been suspended

Machine.Group ID

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

Alert Name

Lists the alerts possible for each machine ID.

Responses

The ATSE response code assigned to each alert for each machine IDs:

- A = Create **A**larm
- T = Create **T**icket
- S = Run **S**cript
- E = **E**mail Recipients

Script to Run

The script to run, if this alert condition occurs.

Run Script On

The machine ID the script is run on, if this alert condition occurs.

Email To

A comma separated list of email addresses where notifications are sent.

Power

vPro > Setup > Power

The **Power** page performs the following tasks on selected vPro machines.

- Power up
- Shutdown
- Force power down
- Power up agentless machines

These tasks can be performed immediately or by schedule.

> **Note:** If the target vPro machines are behind a firewall and you want to power up a **vPro Proxy** *(page 2)* is required.

Actions

- **Run Now**
  - **Power Up** - Powers up the vPro machine immediately. A **vPro Proxy** *(page 2)* is required if the target vPro machine is behind a firewall.
  - **Windows Shutdown** - Shuts down the vPro machine immediately.
  - **Force Power Down** - Forces a power down immediately. Equivalent to pulling the plug on the machine. A **vPro Proxy** *(page 2)* is required if the target vPro machine is behind a firewall.
  - **Power Up Agentless Machine** - Power up a known agentless vPro-enabled machine by specifying an IP address. You must also select another machine to serve as the vPro Proxy that issues the power up command. See **Agentless Power Control** *(page 8)*.
- **Schedule -** Schedule a task once or periodically. Each type of recurrence—Once, Minutes, Hourly, Daily, Weekly, Monthly—displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence.
  - **Schedule Power Up** - Schedules a power up. A **vPro Proxy** *(page 2)* is required if the target vPro machine is behind a firewall.
  - **Schedule Windows Shutdown** - **Schedules** *(page 7)* a Windows shutdown.
  - **Cancel Scheduled Power Up** - Cancels a scheduled power up.
  - **Cancel Scheduled Windows Shutdown** - Cancels a scheduled Windows shutdown.
- **Show Discovered Assets** - If checked, display agentless vPro machines designated assets and discovered using **Discovery**. **Agentless Power Control** *(page 8)* can be powered up or force powered down.

Table Columns

- **Current User** - The user currently logged on to the operating system of the machine.
- **Next Power Up** - The date/time of the next power up.
- **Power Up Recurrence** - The recurring schedule for power ups on this machine.
- **Next Windows Shutdown** - The date/time of the next Windows shut down.
- **Windows Shutdown Recurrence** - The recurring schedule for Windows shutdowns on this machine.
- **AMT Password** - The AMT password used to access to the vPro machine.
- **Associated vPro Proxy** - The vPro Proxy that relays a vPro connection to this machine.

Agentless Power Control

Agentless Power Control Using Discovery Integration

vPro can issue power commands to any vPro-enabled, agentless machines discovered using the **Discovery** module.

- After a **Discovery** scan has detected the vPro-enabled machines on a network, these agentless vPro machines display on the vPro Management page if the vPro > vPro Actions > **Power** *(page 7)* > **Show Discovered Assets** checkbox is checked.

- vPro-enabled machines detected by **Discovery** can be powered on—on demand or by schedule—and powered off on demand.
- A vPro machine does not have to be "promoted to an asset" in **Discovery** to display on the vPro page in **vPro**.
- The **Discovery** probe machine used to discovered these vPro-enabled machines serves as the **vPro Proxy** *(page 2)* used to issue power commands to these same machines.

Agentless Power Control by IP Address

Independent of detection by **Discovery**, a power on command can be sent to a known vPro-enabled machine without an installed agent by specifying an IP address. The command is issued using the vPro > vPro Actions > **Power** *(page 7)* > **Power Up Agentless Machine** option. Enter the following options:

- **Send Power Up via vPro Proxy** - Since **Discovery** was not used to detect the vPro-enabled machine, the user must specify an agent machine on the same network as the target vPro-enabled machine to serve as the vPro Proxy machine. The vPro Proxy issues the power on command to the vPro-enabled machine.
- **IP address of Machine to Power On** - The IP address of the target vPro machine you want to power on.
- **AMT User Name** - The AMT username used to access the vPro machine.
- **AMT Password** - The AMT password used to access to the vPro machine.

Remote Control

vPro > Setup > Remote Control

The **Remote Control** page enables you to troubleshoot or boot unresponsive vPro machines. A **vPro Proxy** *(page 2)* is required if the target vPro machine is behind a firewall.

> **Note:** For standard Windows logon sessions, **Kaseya Remote Control** *(http://help.kaseya.com/webhelp/EN/VSA/9000000/index.asp#17978.htm)* provides a faster connection.

Actions

- **Remote Control** - Runs a **KVMView** *(page 9)* session.
- **Boot to BIOS** - Boots the vPro machine to **access the BIOS** *(page 10)* in a KVMView session.
- **Boot from ISO** - Boots the vPro machine from **list of ISOs** *(page 11)*.

KVMView

KVM stands for "keyboard, video and mouse" remote control of a vPro machine, even if the machine's operating system is not yet installed or malfunctioning. A KVM session is started when performing the following commands from **vPro**.

- **Boot to BIOS** *(page 10)*
- **Boot from ISO** *(page 3)*
- **vPro Remote Control** *(page 9)*

KVMView

KVMView is an application used to manage the KVM connection between the VSA user's machine and the target vPro machine. Installing KLC plugins is a prerequisite. Your browser may display a prompt asking you to confirm starting **KVMView**. The browser typically includes an option to skip this prompt the next time a KVM session is started.

KVMView Access Using a vPro Proxy

KVMView sessions require a **vPro Proxy** *(page 2)* if the target vPro machines are behind a firewall. In addition, the vPro Proxy must have a public IP address and port. Use the vPro > Setup > **vPro Proxy** page to specify the vPro Proxy's public IP address and port.

vPro Security

Starting a KVM session requires either:

- Entering a randomly generated consent code that is displayed on the remote machine's monitor. *You will need a local user to read the consent code to you.* Or,
- The machine was previously activated while associated with a vPro Proxy configured with a security certificate. **Instructions are provided for configuring a security certificate for a vPro Proxy** *(https://helpdesk.kaseya.com/entries/33171573)*. This advanced feature enables a VSA user to start a KVM session without requiring a consent code provided by a local user.

KVMView Actions

- **File**
  - **Exit** - Closes the **KVMView** application.
- **Connecting**
  - **Start** - Starts a **KVMView** connection.
  - **Stop** - Stops the **KVMView** connection.
  - **Refresh** - Refreshes the display of the host computer's desktop.
  - **Color Quality** - Sets the quality of the rendered color within the **KVMView** window: `Maximum`, `Medium`, `Low`.
  - **Scale Video** - If selected, the entire vPro desktop is resized to fit inside your **KVMView** window. If not selected, a cropped portion of the vPro desktop displays at full size inside your **KVMView** window.
  - **Full Screen** - If selected, maximizes the **KVMView** window to full screen.
- **Tools**
  - **Send Ctrl-Alt-Del** - Sends the CTRL-ALT-DELETE command to the host computer. (Pressing this key combination would be interpreted by the client computer.)
  - **Send IDER Session** - Starts a boot from ISO session.
  - **Options** - Not enabled if already connected.

Boot to BIOS

After a vPro machine is enabled you can you boot the vPro machine and access the BIOS in a **KVMView** (page 9) session. A **vPro Proxy** *(page 2)* is required if the target vPro machine is behind a firewall.

1. Click the **Boot to BIOS** button for a machine on the vPro > vPro Actions > **Remote Control** *(page 9)* page.
2. **Unless the machine is assigned a vPro Proxy and the vPro Proxy is configured with a security certificate** *(https://helpdesk.kaseya.com/entries/33171573)*.
   - Enter a consent code. *You will need a local user to read the consent code to you.*
   - Click the **I've authenticated** button that displays in a popup window in the VSA to continue.
3. Access the BIOS of the target vPro machine displayed in the **KVMView** window.

Boot from ISO

After a vPro machine is enabled you can you boot the vPro machine from a selected ISO.

- You must have previously uploaded the ISO to the Kaseya Server using the **Manage Boot ISOs** *(page 3)* page.
- If the target vPro machine is behind a firewall a **vPro Proxy** *(page 2)* machine is required. In this case, you must also upload the ISO to the vPro Proxy machine.

Booting from an ISO

1. Click the **Boot from ISO** button for a selected vPro machine on the vPro > vPro Actions > **Remote Control** *(page 9)* page.
2. Select an ISO from the list of uploaded ISOs.
3. Click **Boot from ISO**.

Rebate Form

vPro > Setup > Rebate Form

Kaseya participates in a vPro rebate program offered by Intel. Select vPro-enabled machines on this page, then click this option. If the vPro machine qualifies for the rebate, you can quickly generate a CSV file containing the information you to need to document your rebate claim with Intel. An **Intel® vPro™ Technology Activation Rebate Rules** *(http://www.intel.com/cd/channel/reseller/asmo-na/eng/products/platforms/vpro_activate/index.htm)* link describes the rebate requirements.

Action

- **Generate Rebate Form** - Downloads a CSV file for selected machines that are eligible for a rebate.

Logs

vPro > Administration > Logs

The **Logs** page displays a log for a managed vPro machine.

- Event Time
- Event Type

Index