HP Remote System Controller User Guide

SUMMARY

The HP Remote System Controller provides a secure and easy to use, out-of-band remote management solution for supported HP platforms, with the remote KVM capabilities providing universal remote keyboard, video, and mouse support for almost any computer device.

Legal information

© Copyright 2023-2025 HP Development Company, L.P.

Chrome is a trademark of Google LLC. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Edge, Microsoft, and Windows are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. NVIDIA is trademark and/or registered trademark of NVIDIA Corporation in the U.S. and other countries. DisplayPort and the DisplayPort logo are trademarks owned by the Video Electronics Standards Association (VESA) in the United States and other countries.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Sixth Edition: August 2025

First Edition: May 2023

Document Part Number: N55811-006

Third-party software notice

Third-party source code and licenses are redistributed, if required, with HP Remote System Controller Software.

User input syntax key

Text that you must enter into a user interface is indicated by `fixed-width font`.

User input syntax key

Item	Description
`Text without brackets or braces`	Items you must type exactly as shown
`<Text inside angle brackets>`	A placeholder for a value you must provide; omit the brackets
`[Text inside square brackets]`	Optional items; omit the brackets
`{Text inside braces}`	A set of items from which you must choose only one; omit the braces
`|`	A separator for items from which you must choose only one; omit the vertical bar
`...`	Items that can or must repeat; omit the ellipsis

Table of contents

1 Getting started 1

Requirements 1

Supported features 2

Front panel components (external) 2

Left and right panel components (external) 3

Front components (internal) 4

Connecting the computer (external) 4

Connecting to AC power (select products only) 5

Disconnecting the HP Remote System Controller 6

2 Configuring the HP Remote System Controller 7

Initial setup for the HP Remote System Controller 7

Accessing the software interface for the HP Remote System Controller 8

Configure the Proxy settings 9

Configure the IPv4 Assignment 9

Configure the IPv4 DNS Server Assignment 10

Configure the IPv6 Configuration Method 10

Configure the IPv6 Gateway 11

Configure the IPv6 DNS Server Assignment 11

Configure the 802.1x Security 11

Configure KVM 12

Configuring the access security 13

Configure the password 13

Certificate Management 13

Configure Firmware Updates settings 14

Configure Date and Time settings 16

Configure local users 16

Add a local user 17

Edit local user permissions 17

Delete local user 18

Configure directory-based authentication 18

Configuring the domain controller address 18

Configuring the base search entry 18

Configuring the groups allowed to authenticate 19

Log in with domain credentials 19

Managing current user sessions 19

Managing all user sessions 19
Enrolling into HP Remote System Management 19
Network requirements for Remote System Management 20
Bulk enrollment of devices to Remote System Management 21
3 Accessing and controlling the remote host 23
Control the remote host power 23
Turn on the remote host 23
Turn off the remote host 23
Restart the remote host 24
Stopping the boot process in the BIOS menu 24
Accessing the remote host using KVM 24
KVM hardware compatibility 24
Using the KVM menu 25
Start a KVM session 26
Using KVM 27
Using the keyboard 27
Viewing the video 27
Using the mouse 27
Navigating and accessing host information 28
Accessing host information 28
Navigate the host information interface 28
Mounting a virtual drive using virtual media 29
Using virtual media 29
Choosing a virtual media mode 29
Mounting the file 30
Unmounting the file 30
Removing a file 30
Installing a microSD card 30
Navigating and configuring BIOS settings 30
Accessing BIOS settings 31
Navigating the BIOS interface 31
Adjusting BIOS settings 31
Booting to the virtual media drive 31
4 Administering the Remote System Controller 33
Perform a factory reset 33
Restart the Remote System Controller 33
Appendix A Specifications 34
Input power 34
Operating environment 34
Appendix B Troubleshooting 36
LED display status 36
Remote host LED display status 36

Remote System Controller LED status 36
Network LED display status 36
Issue resolution 37
Generating log file information 40
Appendix C Accessibility 41
HP and accessibility 41
Finding the technology tools you need 41
The HP commitment 41
International Association of Accessibility Professionals (IAAP) 42
Finding the best assistive technology 42
Assessing your needs 42
Accessibility for HP products 42
Standards and legislation 43
Standards 43
Mandate 376 – EN 301 549 43
Web Content Accessibility Guidelines (WCAG) 43
Legislation and regulations 44
Useful accessibility resources and links 44
Organizations 44
Educational institutions 44
Other disability resources 45
HP links 45
Contacting support 45
Index 46

1 Getting started

HP Remote System Controller (RSC) enables you to monitor, troubleshoot, and control power and hardware alerts on a remote host, and offers other out-of-band management capabilities.

Features include:

- Access the host and hardware information at any time
- Initiate a keyboard, video, and mouse (KVM) session to control the remote host
- Control power to the remote host
- Access BIOS; change host BIOS settings on the remote host without KVM
- Edit the Remote System Controller settings
- Check event logs
- Mount virtual media to the host, for imaging or updates
- Control multiple systems from the HP Remote System Management (RSM) fleet manager (https://rsm.hp.com).

Requirements

Before you use HP Remote System Controller, make sure that your environment meets the following requirements.

- Locate the laser-etched label on the bottom next to the QR code for the HP Remote System Controller, or on a sticker on the HP Integrated Remote System Controller. A copy of this sticker for the HP Integrated Remote System Controller is on the outside of the host chassis when configured from the factory. You can also scan the QR code with a smartphone camera to see the following information as a comma-separated list:
  - Serial number
  - Default password
  - MAC address

  NOTE: You can change only the password. You cannot change the MAC address or serial number.
- When the Remote System Controller is connected to a network, an IP address is assigned to it. The Remote System Controller displays the IP address it was assigned. If an IP address was not assigned to the Remote System Controller, an IP address from the network—a Link Local address—is assigned, starting with *169.254.xxx.xxx*.

NOTE:

- The HP Integrated Remote System Controller does not have an LCD display to view information.

- A dedicated network port, which does not support network traffic passthrough to the host, is required for the HP Integrated Remote System Controller.
- An AC outlet is required for the HP Remote System Controller for Universal KVM (7K7N2AA) version of the product.

- Use a Google Chrome™ or Edge® browser to view the Remote System Controller GUI.
- HP systems shipped to certain regions have the **Maximum Power Savings** BIOS setting enabled, which prevents the HP Remote System Controller from getting power from the host main board. HP recommends that you disable this setting so that the Remote System Controller has power when the host system is turned off.

Supported features

The features are supported by the following platforms.

NOTE: For Z4, Z6, Z8 G4 and ZCentral G4, the latest BIOS update is required to enable the host to provide power to the HP Integrated Remote System Controller in all host power states.

NOTE: For Z4, Z6, Z8/Fury G5, the latest BIOS update is required to enable the host telemetry feature.

Table 1-1 Supported features by platform

Feature	Z4, Z6, Z8/Fury G5	Z2 G9, Z2 G1i/a, and Engage Flex Pro/Pro-C G2	Z4, Z6, Z8 G4, ZCentral 4R	Other Computers (with Universal KVM SKU 7K7N2AA)
Power button control	Yes	Yes	Yes	Not available
Direct BIOS communication	Yes	Yes	Not available	Not available
Remote Virtual Media	Yes	Yes	Yes	Yes
IP KVM	Yes	Yes	Yes	Yes
Hardware system inventory	Yes	Yes	Not available	Not available
Hardware alerts	Yes	Yes	Partial	Not available
Remote System Controller firmware updates	Yes	Yes	Yes	Yes
Host Telemetry	Yes	Coming soon	Not available	Not available

Front panel components (external)

Use the illustration and table to identify the front panel components for the HP Remote System Controller.

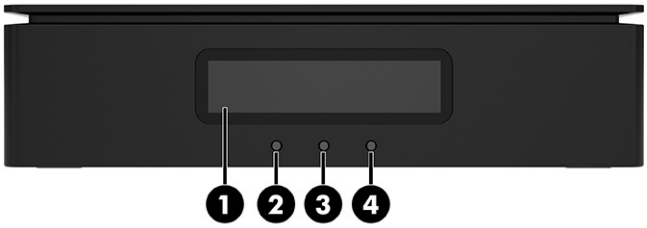
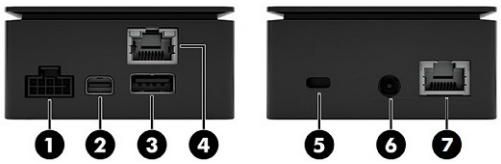


Table 1-2 Identifying the front panel components

	Front panel components
(1)	LCD screen
(2)	Host status LED
(3)	Remote System Controller status LED
(4)	Remote connection status LED

Left and right panel components (external)

Use the illustration and table to identify the left and right panel components for the HP Remote System Controller.



NOTE: If you install the HP Z4/Z6/Z8G4 / ZCentral 4R Remote System Controller Cable Adapter (7K6E5AA), the HP Remote System Controller or HP Integrated Remote System Controller redirects power from the front USB ports on the host to power the Remote System Controller in all host states. In this situation, bus-powered devices such as keyboards, mice, USB thumb drives, and other peripherals cannot be powered when they are installed in the front USB ports. Powering the HP Remote System Controller or HP Integrated Remote System Controller in all host states requires an update to the latest available BIOS for the ZCentral 4R, Z4G4, Z6G4, and Z8G4 platforms.

Table 1-3 Identifying the left and right panel components

	Left panel components		Right panel components
(1)	10-pin cable connector	(5)	Security cable slot
(2)	Mini DisplayPort™ for graphics input	(6)	Power cable connector

Table 1-3 Identifying the left and right panel components (continued)

	Left panel components		Right panel components
(3)	USB3 for Mouse/Keyboard/Virtual Media Emulation	(7)	RJ-45 network jack (network-facing)
(4)	RJ-45 network jack (host-facing)		

Front components (internal)

Use the illustration and table to identify the front panel components for the HP Integrated Remote System Controller.

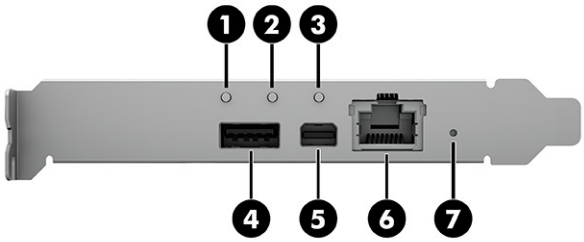


Table 1-4 Identifying the front components

	Front components
(1)	Host status LED
(2)	Remote System Controller status LED
(3)	Remote connection status LED
(4)	USB3 for Mouse/Keyboard/Virtual Media Emulation*
(5)	Mini DisplayPort for graphics input
(6)	RJ-45 network cable connector and jack
(7)	Soft reset/factory reset button

* The front USB port is not needed if the internal USB 3.0 connector is used.

Connecting the computer (external)

Use the illustration and table to connect the computer to the HP Remote System Controller.

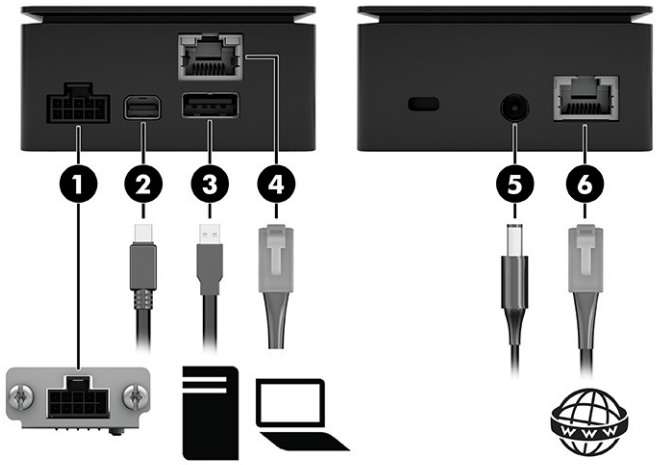


Table 1-5 **Connecting the computer**

	Cables
(1)	10-pin power and signal cable connector
(2)	Mini DisplayPort cable
(3)	USB3 cable
(4)	RJ-45 (network) jack cable
(5)	Power input (optional when a 10-pin cable is connected)
(6)	Network jack uplink cable

Connecting to AC power (select products only)

An AC outlet is required for the HP Remote System Controller for Universal KVM (7K7N2AA) version of the product. You must connect the AC adapter to an AC power source. When connected to power, the AC power source provides up to 40 W of power through the power connector. The HP Remote System Controller uses up to 18 W when all computer resources are in use, but typically idles at less than 5 W of power.

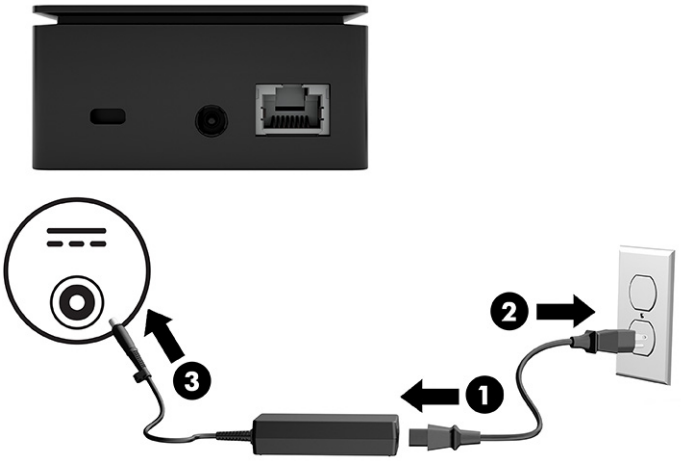
⚠ **WARNING!** To reduce the risk of electric shock or damage to the equipment:

- Plug the power cord into an AC outlet that is easily accessible at all times.
- Disconnect power from the equipment by unplugging the power cord from the AC outlet.
- If provided with a 3-pin attachment plug on the power cord, plug the cord into a grounded (earthed) 3-pin outlet. Do not disable the power cord grounding pin, for example, by attaching a 2-pin adapter. The grounding pin is an important safety feature.

To ensure the correct performance of all features, connect the HP Remote System Controller to an AC power source using the AC adapter.

1. Connect one end of the power cord to the AC adapter (1), and connect the other end of the power cord to an AC outlet (2).

2. Connect the AC adapter to the power connector (3) on the HP Remote System Controller.



Disconnecting the HP Remote System Controller

To disconnect the HP Remote System Controller, do the following:

- Disconnect the cables from the computer
- Disconnect the power cable from the HP Remote System Controller

NOTE: Do not disconnect the HP Remote System Controller while you are updating the software. Doing so might cause the HP Remote System Controller to become unusable.

2 Configuring the HP Remote System Controller

You can adjust settings for the HP Remote System Controller either programmatically using the Redfish API or through the embedded graphical user interface.

For more information about the Redfish API, go to the following webpage:
https://developers.hp.com/hp-remote-system-controller/api/hp-remote-system-controller-api-2412

TIP: Replace the last four digits of the URL with the major and minor version numbers. For example, enter 2404 to find API documentation for version `24.04`.

Initial setup for the HP Remote System Controller

The first time you use the HP Remote System Controller, you must perform the following setup tasks.

1. Open a web browser (either Chrome or Microsoft Edge) and type the Remote System Controller URL in the address field.

   To determine the URL, access the user interface by typing `https://<hostname>.<domain>`, where the default hostname is `rsc-<serial_number>`.

   NOTE: The Remote System Controller uses multicast DNS (mDNS) to provide a default hostname. To resolve mDNS addresses, your computer needs access to UDP port 5353. The mDNS protocol is not routable—both the machine and the Remote System Controller must be in the same LAN/VLAN. Some switches might use additional configuration to allow mDNS messages to traverse across VLANs. If you want to disable mDNS so that the Remote System Controller is not discoverable through mDNS, you can disable it after you log in by configuring the settings in the **RSC Settings** section under **Network Configuration**.

   If there is no enterprise DHCP and DNS, a local address is assigned to the Remote System Controller and you can access it by typing `https://rsc-<serial_number>.local`, where:

   - **rsc** is a fixed keyword
   - **<serial_number>** is a variable you replace with the serial number for your Remote System Controller
   - **local** is the network domain

   NOTE: When no DHCP is in the network, the Remote System Controller starts and falls back to the link-local IPv4 configuration automatically, enabling a unique IP that can be reached in the local network for Remote System Controller configuration/provisioning. Make sure your operating system has a link-local address added to the network interface in the same LAN/VLAN as the Remote System Controller, and then type the URL `https://rsc<serial>.local` to start the configuration. IPv4 link-local addresses are assigned from address block 169.254.0.0/16 (169.254.0.0 through 169.254.255.255).

2. Enter `admin` as the user name and enter the default password that is printed on the Remote System Controller label.

3. Accept the license agreement.

NOTE: You must accept the license agreement to be able to use the Remote System Controller.

4. Change the password from the default password to a new one that includes the recommended security criteria. See Configure the password on page 13.

5. Set the firmware update policy. HP recommends updating the Remote System Controller firmware after the initial login because new features and bug fixes are available in new firmware versions on a regular basis. If the Remote System Controller firmware is not updating automatically, go to https://rsm.hp.com/console/download/firmware to download the latest firmware packages.

6. Choose whether you want to enroll the device to an organization in the HP Remote System Management fleet management software at the following link: https://rsm.hp.com. You can enroll a device anytime. You can also enroll multiple devices on the same network by using the bulk enrollment function in the **RSM Settings** tab from a single Remote System Controller device. The bulk enrollment function allows you to discover Remote System Controller devices, change passwords, and enroll multiple Remote System Controller devices to Remote System Management in a single workflow.

NOTE: You must be connected to the same network as the Remote System Controller for initial access.

NOTE: For optimum security, configure certificates in the Remote System Controller.

Accessing the software interface for the HP Remote System Controller

You can access the internal functions of the HP Remote System Controller using the following methods:

- Use an application program interface (API) to build programmatic access from an external program. The API follows the industry-standard Redfish specification. For more information about the Redfish API, go to the following webpage: https://developers.hp.com/hp-remote-system-controller/api/hp-remote-system-controller-api-2412.

TIP: Replace the last four digits of the URL with the major and minor version numbers. For example, enter `2404` to find API documentation for version 24.04.

- Access the web interface using an internet browser and the Remote System Controller IP address shown in the interface. The web interface is designed to handle different desktop screen sizes.

During a typical session you might perform the following functions:

- Open a browser and enter the Remote System Controller URL.

NOTE: If you perform a directory login, you can also use your directory user name and password. See Configure directory-based authentication on page 18 for setup instructions.

- Enter `admin` as the user name and the password to log in.
- Perform any host management tasks required.
- If you open a KVM session, a new browser window opens. To close a KVM session, close the window or use the toolbar icon to exit.

- To close the Remote System Controller session, select the user icon in the upper-right corner and select **Log out this session**.

NOTE: If your session is inactive for one hour, the session closes automatically and the login screen is displayed. All sessions expire after eight hours, even if the session is active.

Configure the Proxy settings

Use this procedure to configure the Proxy settings.

1. On the left side of the dashboard, select **RSC Settings**.
2. In the **Network Configuration** section, under **Proxy**, select **Edit**.
3. Select the **Disabled** toggle to enable the proxy server.

   NOTE: By default, the proxy server is disabled.

4. Type the address that the proxy server needs to access, for example, `https://yourproxyserver.domain:8088`.
5. If you there are any addresses that need to be accessed without proxy, enter the addresses, separating each address by a semicolon (;). For example, `10.10.10.254;192.34.154.13`.
6. Select **Confirm** to implement the updates.
7. After changing the settings, select **Close** to close the confirmation message.

NOTE: If the proxy server requires authentication, you can configure it by using the following pattern in the Proxy Settings Address field for the URL: `scheme://username:password@server.domain:PORT`. For example, `https://yourusername:yourpassword@yourproxysever.domain:8088`.

Configure the IPv4 Assignment

Use this procedure to configure the IPv4 Assignment.

1. On the left side of the dashboard, select **RSC Settings**.
2. In the **Network Configuration** section, under **IPv4 Addresses Assignment**, select **Edit**.
3. Do one of the following:
   - Select **Manual** from the drop-down menu to manually type the following values:
     - IPv4 Address
     - Subnet Mask
     - Gateway
   - Select **Automatic (DHCP)** to have the settings automatically issued by a DHCP server on the network.
4. Select **Confirm** to confirm the changes to the settings.

5. After changing the settings, select **Close** to close the confirmation message.

NOTE: The current IP settings are shown under IPv4 Address in the **Network Configuration** section.

NOTE: If the IPv4 Addresses Assignment is set to Automatic (DHCP), and there is no DHCP server on the network, then a Link Local address (169.254.xxx.xxx) is assigned for a local connection to be established. When a Link Local address is set, the Remote System Controller resets the network interface every 10 minutes to look for a DHCP server.

Configure the IPv4 DNS Server Assignment

Use this procedure to configure the IPv4 DNS Server Assignment.

1. On the left side of the dashboard, select **RSC Settings**.
2. In the **Network Configuration** section, under **IPv4 DNS Server Assignment**, select **Edit**.
3. Do one of the following:
   - Select **Manual** from the drop-down menu to manually type the following values:
     - Preferred DNS
     - Alternate DNS
   - Select Automatic (DHCP) to have the settings automatically detected.
4. Select **Confirm** to confirm the changes to the settings.
5. After changing the settings, select **Close** to close the confirmation message.

NOTE: A list of DNS servers is displayed under **Edit**.

Configure the IPv6 Configuration Method

Use this procedure to configure the IPv6 Configuration Method.

1. On the left side of the dashboard, select **RSC Settings**.
2. In the **Network Configuration** section, under **Enable IPv6 Network**, toggle the setting to **Enabled**.

   By default, IPv6 is enabled with the Automatic method selected, which assigns a Link Local address and DHCP addresses (if a DCHP server is present on the network). To change methods, continue to the next step.
3. In the **Network Configuration** section under **IPv6 Configuration Method**, select the dropdown arrow to the far right.
4. Do one of the following:
   - Select **Automatic** to have the settings automatically issued by a DHCP server on the network in addition to the Link Local Address, and to any static addresses that are configured. You might see both /64 and /128 prefix length addresses.
   - Select **DHCPv6 Only** to use only DHCPv6-issued addresses, where you might receive only /128 prefix length addresses.

- Set a Static IPv6 Address
  a. In the **Network Configuration** section under **IPv6 Static Addresses**, select **Edit**.
  b. Type in an IPv6 address, then a prefix length, and select **Add**.
  c. When finished adding static addresses, select **Confirm**.
  d. Only once a Static IPv6 Address is set can the IPv6 Address Configuration Method be set to Manual Only.

NOTE: The current IPv6 settings are shown under the **IPv6 Address Configuration Method** section.

NOTE: If the IPv6 Addresses Configuration Method is set to **Automatic (DHCP)** and there is no DHCP server on the network, then a Link Local address (fe80::xxxx:xxxx:xxxx:xxxx/64) is assigned for a local connection to be established. When a Link Local address is set, the Remote System Controller resets the network interface every 10 minutes to look for a DHCP server.

Configure the IPv6 Gateway

Use this procedure to configure the IPv6 Gateway.

1. On the left side of the dashboard, select **RSC Settings**.
2. In the **Network Configuration** section, under **IPv6 Gateway**, select **Edit**.
3. Do one of the following:
   - Select **Manual** from the drop-down menu to manually type the IPv6 Gateway address value (no prefix length required).
   - Select **Automatic (DHCP)** to have the settings automatically detected.
4. Select **Confirm** to confirm the change to the settings.

Configure the IPv6 DNS Server Assignment

Use this procedure to configure the IPv6 Gateway.

1. On the left side of the dashboard, select **RSC Settings**.
2. In the **Network Configuration** section, under **IPv6 DNS Server Assignment**, select **Edit**.
3. Do one of the following:
   - Select **Manual** from the drop-down menu to manually type the IPv6 DNS Server address value.

     NOTE: To add additional IPv6 DNS Server addresses, select **Add** and repeat.
   - Select **Automatic (DHCP)** to have the settings automatically detected.
4. Select **Confirm** to confirm the change to the settings.

Configure the 802.1x Security

Use this procedure to configure the 802.1x Security.

1. On the left side of the dashboard, select **RSC Settings**.
2. In the **Network Configuration** section, under **802.1x Security**, select **Edit**.
3. Either enable or disable 802.1x security.
4. When enabling 802.1x security, you are required to select an authentication method.
5. Each authentication method has its own fields that can be configured.
6. Configure all the mandatory fields.
7. Select **Confirm** to confirm the changes to the settings.

NOTE: Do not turn this setting on unless the network the Remote System Controller is connected to requires 802.1x authentication. If this setting is enabled and the network does not support 802.1x, you must factory reset the Remote System Controller so it can connect to a non 802.1x enabled network again.

NOTE: To enable 802.1x, an 802.1x CA certificate must be installed so the Remote System Controller can verify the authenticity of the authentication server. This certificate can be uploaded from the 802.1x configuration dialog or from the **Certificate Management** section.

Configure KVM

Follow this procedure to configure the KVM settings.

1. On the left side of the dashboard, select **RSC Settings**.
2. In the **KVM Configuration** section, the following settings are available:

   - **Enable HP vDisplay Only During KVM Session**

     When this feature is enabled, the Remote System Controller virtual monitor is available only to the connected host while there is an active KVM session. If this feature is disabled, the virtual monitor is always available to the connected host. If this feature is enabled, a KVM session might need to be started prior to opening the UEFI BIOS menus. In other operating system environments, connecting to monitors while the system is on might not be supported, which might require the KVM session to be started prior to entering certain operating systems.

   - **Enable Collaboration During KVM Session**

     Enabling this feature allows more than one user to access the KVM session at the same time. If this feature is disabled, only one user can access the KVM session. If a new user joins the KVM session, the previous user is removed from it.

   - **Collaboration Requires Authorization**

     This setting is available only if the Collaboration setting is enabled. When the setting is enabled, every time a collaborator joins a KVM session, an authorization request is displayed to the main user (the first user in the session). The main user can then allow or deny the collaboration request. If this setting is disabled, all collaboration requests are automatically accepted.

   - **Port Range**

This feature allows the user to select which port range the KVM agent running inside the Remote System Controller uses when a new KVM connection is attempted. The default port range values are 3478 to 3481, starting with the 24.04 firmware version and later. Prior versions had a much larger port range, which might have been difficult to manage when dealing with local firewalls. The number of ports in the configured port range corresponds to the number of KVM sessions that can be created during KVM Collaboration. For instance, by default four ports are used in the port range, which allows up to four KVM sessions to be active during KVM Collaboration.

- **Maximum Bandwidth**

  This setting allows the user to control the maximum network bandwidth that a KVM session can use. Typically, a KVM session uses less bandwidth than the maximum value that is set. The default value is 4 Mbps. Increasing the maximum bandwidth can improve the image quality of the remote desktop, especially on higher resolutions.

Configuring the access security

Use this information to configure the Remote System Controller for the optimum web server and API access security.

- Use a strong password. See Configure the password on page 13.
- Install a trusted certificate (not required, but recommended)
- Enable directory authentication to control access by designated security groups

Configure the password

Use this information to configure the password.

1. On the left side of the dashboard, select **RSC Settings**.
2. In the **Passwords** section, click **Change**. Type the new information in the **Old password**, **New password**, and **Confirm new password** fields.

NOTE: You cannot use a password that has already been used as one of the last 24 passwords you created.

- Use a minimum of 12 characters
- Make sure that the password contains at least three of the following:
  - Lowercase character
  - Uppercase character
  - Number
  - Special character

Certificate Management

The Certificate Management section allows you to configure all the different kinds of certificates used in the Remote System Controller. It is divided into four different sections:

- Trusted certificates authenticate external servers such as the fleet manager or servers that store data such as virtual media images. These certificates also update packages or subscribers to hardware alerts. In the Trusted Certification Authorities section you can add or remove trusted certificates through the UI or an API.
- The Remote System Controller web service and KVM use the HTTPS server certificate to provide TLS connections. The HTTPS Certificate section can be used to change the server certificate the Remote System Controller uses.
- 802.1x Certification Authorities are used to verify the authenticity of the authentication server when 802.1x Security is enabled. You can upload and manage multiple certificates in this section.
- An 802.1x Client Certificate is needed when using EAP-TLS authentication in 802.1x. This certificate identifies the Remote System Controller to the authentication server. A single certificate can be uploaded in this section. The certificate must be in .PEM format and the certificate file must also include the certificate's private key. The following format is what the Remote System Controller expects in the .PEM file:

  -----BEGIN CERTIFICATE-----

  [Certificate content]

  -----END CERTIFICATE-----

  -----BEGIN RSA PRIVATE KEY-----

  [RSA Private Key Content]

  -----END RSA PRIVATE KEY-----

NOTE: Not installing your own server certificate causes the Remote System Controller to use self-signed certificates, which is not recommended.

NOTE: All certificates can also be managed through the API.

Configure Firmware Updates settings

Follow this procedure to configure the RSC Firmware Updates settings.

1. On the left side of the dashboard, select **RSC Settings**.
2. In the **Operations** section, select the **Firmware Updates** button.
3. On the **Automatic Updates** tab, you can change the automatic update mode and frequency using these options:
   - **Automatically check and install updates**: When this mode is selected, the Remote System Controller automatically downloads and installs the latest updates.
   - **Notify me of updates, and I will install it manually**: When this mode is selected, the Remote System Controller checks for the latest updates automatically but does not download or install them. You must follow step 5 to update the firmware manually.

- **Do not check for updates**: When this mode is selected, the Remote System Controller does not check for the updates automatically. You must follow step 4 or 5 to update the firmware manually.

NOTE: The checks for these two modes happens according to the selected Schedule frequency (Daily, Weekly, or Monthly).

4. When enabling the **Automatically check and install updates** or **Notify me of updates, and I will install it manually** update modes, you can configure a schedule for when the firmware update checks are performed. The following scheduling options are available:

   - Daily: Specify the time of day (hh:mm) for the firmware check.
   - Weekly: Specify the day of the week (e.g., Monday) and the time of day for the firmware check.
   - Monthly: Specify the day of the month (1–31) and the time of day for the firmware check.

   NOTE: If a scheduled date does not exist in the current month, the firmware check automatically occurs on the last day of that month.

   NOTE: If an automated check for a firmware update occurs during an active session and there is a firmware update ready to be applied, the firmware update is applied after there are no active sessions in order not to disrupt any manual Remote System Controller operations performed by a user.

5. On the **Manual Updates** tab, you can perform a firmware update manually by following this procedure:

   a. Download the latest firmware update package from https://rsm.hp.com/console/download/firmware.

   b. Select the blank field to open a file explorer window.

   c. Find and select the firmware file with the extension `tar.gz` on the local computer.

      NOTE: Be sure to match the firmware update file to the version of Remote System Controller that you are using, depending on whether the file name contains *external* or *internal*, which correlates to the Remote System Controller and Integrated Remote System Controller, respectively.

      The file transfers, and the update starts automatically. The update might take several minutes. When the update is complete, a message is displayed, notifying you of the result of the operation.

   If the update is successful, you can see the new firmware version in **RSC Settings**. When security updates are included, the login page is displayed and you must restart the session. When updating from versions prior to 23.12, you might see an error message indicating that the update failed. It is recommended to wait another 30 minutes before attempting to reset the Remote System Controller in case the error is invalid and the update is still in progress. Check the Remote System Controller status LED to confirm whether a firmware update is still in progress. For more information, see Remote host LED display status on page 36.

6. The information about available updates is displayed at the top of the page. If you select **Check for Updates** to get the latest updated information, you can see your current installed version, and the last time it was checked.

   a. When a new update is available, select the **Release Notes** button to check the release notes.

b. Install the new update by selecting the **Update Now** button.

c. Accept all the prompts that come next.

If the update is successful, you can see the new firmware version in **RSC Settings**. When security updates are included, the login page is displayed and you must restart the session. When updating from versions prior to 23.12, you might see an error message indicating that the update failed. It is recommended to wait another 30 minutes before attempting to reset the Remote System Controller in case the error is invalid and the update is still in progress. Check the Remote System Controller status LED to confirm whether a firmware update is still in progress. For more information, see Remote host LED display status on page 36.

Configure Date and Time settings

Follow this procedure to configure the date and time settings.

1. On the left side of the dashboard, select **RSC Settings**.
2. In the **Operations** section, select **Date and Time**.

   By default, NTP will be enabled. When NTP is enabled, it will try to use the NTP servers advertised by the DHCP server, if DHCP is enabled.

   If the DHCP server is not configured to provide NTP server configuration, or if DHCP is disabled, the `time.nist.gov` NTP server will be used by default.
3. To override the automatic NTP server configuration, you can add NTP servers to the manual NTP server list.

If you do not want to manually configure date and time using an NTP server, you can disable NTP and manually configure the date and time settings.

You can also manually adjust the time zone.

Configure local users

The Local User Administration feature allows IT Admins to create local users, and grant or limit access to capabilities within the Remote System Controller. This feature includes user-defined role creation and works in conjunction with LDAP. Local users are users who are able to log in to only the Remote System Controller.

The following is a list of current permissions and the responsibility of each permission.

- **RSC Settings**
  - Edit RSC-Hostname
  - Edit Network Configuration
  - KVM Configuration
  - Controls (Firmware Update, Date and Time, Language Settings, Reset, Factory Reset)
  - Certificate Management
  - Directory Authentication Settings
- **Configure Users**

  - Create, Edit, Delete Local Users
  - Change Passwords of Users
  - Manage Users Active Session
- **Configure Host**
  - Boot to BIOS
- **BIOS Settings**
  - BIOS Settings
- **Power Operations**
  - Perform Power Operations
- **Start KVM Session**
  - Start KVM Session (including connecting to signaling server)
- **Delete Security Logs**
  - Delete Security Logs
- **RSM Settings**
  - RSM Settings
- **Virtual Media**
  - Configure Virtual Media
  - Mount/Unmount Virtual Media

Add a local user

Use this procedure to add a local user and assign permissions.

1. To view the Local User Administration feature, select **User Configuration** on the left side of the dashboard.
2. Select **Add** inside the Local User Administration area.
3. Fill in the User Information form with **User Name**, **New Password** and **Confirm New Password** fields. On the **User Permissions** section, choose between three predefined ones (**Administrator**, **Operator** and **Read Only**), or select the individual permissions to create a new custom role.
4. Select **Confirm**.
5. Enter the current logged user password in the **Confirm your login password** field, and then select **Confirm**.

Edit local user permissions

Use this procedure to edit local user permissions.

1. To view the Local User Administration feature, select **User Configuration** on the left side of the dashboard.

2. Select any user in the table inside the Local User Administration area. After selecting one, and only one, select the **Edit** button.
3. If you want to change the password of the selected local user, fill in the **New Password** and **Confirm New Password** in the User Information area. If not, you can just change the user permissions to any predetermined or a custom one.
4. Select **Confirm**.
5. Enter the current logged user password in the **Confirm your login password** field, and then select **Confirm**.

Delete local user

Use this procedure to delete a local user.

1. To view the Local User Administration feature, select **User Configuration** on the left side of the dashboard.
2. Select any user in the table inside the **Local User Administration** area. After selecting at least one user, select **Delete**.
3. Select **Confirm** on the confirmation dialog.

Configure directory-based authentication

You can configure the Remote System Controller to allow users to log in with their domain user names and passwords. You need to specify which users of the intended groups must be members of your directory to be allowed to authenticate into the Remote System Controller. Being a member of any of the groups specified enables authentication. Every authenticated user in the Remote System Controller has the same permission levels as the admin user.

Follow the steps in the next sections to configure directory-based authentication.

The Remote System Controller uses LDAPS (secure LDAP) to access the domain controllers. A root certificate that can verify the LDAP server certificate needs to be added to the Remote System Controller. Refer to the Certificate Management on page 13 section on how to add trusted certificates.

Configuring the domain controller address

Use this procedure to configure the domain controller address.

- In the **Server Host Name** form field, enter the domain controller's IP address or hostname. For example, you might enter `18.2.3.4` or `domaincontroller.mydomain.com`. If DNS is set up properly, entering only the domain name might be sufficient, for example, `mydomain.com`.

  The default port for LDAPS is used. If a different port is needed, follow the IP address or hostname with a colon and the port number, for example, `myserver.mydomain.com:8123`.

Configuring the base search entry

Use this procedure to configure the base search entry.

- Enter a distinguished name (DN) of the base search entry in the **Base DN** form field.

  This entry is the search root for users and groups in the domain. For example, `CN=Users,DC=mydomain,DC=com`

Configuring the groups allowed to authenticate

Use this procedure to configure the groups allowed to authenticate to the Remote System Controller.

- To add groups allowed to authenticate into the Remote System Controller, select the **Add Group** button, then enter the DN of the group.

  Optionally, if you are targeting a Microsoft Active Directory domain, you can additionally enter the group's security identifier (SID) string. In this case, groups fetched through their DNs must also match the SID.

NOTE: When using Microsoft Active Directory domains, the LDAP group search is recursive. If group A is allowed, group B is a child of group A, and user U belongs to group B, user U is allowed to log in.

Log in with domain credentials

After the directory-based authentication is enabled and configured, users can log in to the Remote System Controller using one of the following formats of user name.

- Distinguished name (DN) (for example, `CN=John Smith,CN=Users,DC=mydomain,DC=com`)
- Domain email address (for example, `john.smith@mydomain.com`)
- Domain\username (for example, `mydomain\johnsmith`)

Managing current user sessions

Follow this procedure to manage current user sessions for HP Remote System Controller. This shows only the active session for the current logged user.

To see the active sessions for all users, refer to Managing all user sessions on page 19.

1. To view the current number of active sessions, select the user icon in the upper-right corner of the user interface and expand **Other active sessions** for this user.
2. To log out from all other sessions, select **Log out from all other active sessions**.

Managing all user sessions

Follow this procedure to manage all user sessions for HP Remote System Controller. This shows all the active sessions for all users.

1. On the left side of the dashboard, select **User Configuration** and scroll down to find **Local User Active Sessions**.
2. To log out from any session, select the session you want and select **Terminate Selected Sessions**.

Enrolling into HP Remote System Management

HP Remote System Management is a cloud-based tool that uses HP Remote System Controllers to manage fleets of computers. Each Remote System Controller must enroll into Remote System Management to enable being managed from the cloud. Remote System Management users can create organizations which are collection devices managed by Remote System Controllers. Users can have multiple organizations, allowing them to group devices from multiple company divisions or geographies.

To enroll the Remote System Controller into Remote System Management, the following preconditions must be met:

1. A Remote System Management account must already be created in https://rsm.hp.com.
2. The Remote System Controller needs to have internet access. Make sure that the Remote System Controller network settings allow the Remote System Controller to reach the Remote System Management service. See Network requirements for Remote System Management on page 20 for firewall configuration details for Remote System Controllers to access Remote System Management.
3. The Remote System Controller date and time settings must be correct. Because the communication to Remote System Management uses TLS, incorrect time settings might cause certificates to be rejected. If necessary, a local NTP server might need to be configured under **RSC Settings** > **Date and Time Settings**.

To perform enrollment, follow these steps:

1. On the left side of the dashboard, select **RSM Settings**.
2. Select **Enroll**. The Remote System Controller performs a series of reachability checks to the Remote System Management servers, and then contacts the Remote System Management services to initiate enrollment.
3. A window is displayed, instructing you to confirm the enrollment at the Remote System Management webpage. Select **Confirm**.
4. The Remote System Management page is displayed. Log in to Remote System Management, accepting the terms and conditions.
5. Select an organization for the Remote System Controller device. You can move Remote System Controller devices between your organizations afterwards.

The Remote System Controller device is listed in the selected organization within a few minutes.

Network requirements for Remote System Management

To connect a Remote System Controller to the Amazon Web Services (AWS) hosting of Remote System Management, the Remote System Controller must be able to access the internet. It is recommended to constrain access to the internet by configuring firewalls. This section describes the required web addresses and ports that must be opened for the Remote System Controller to be able to adequately connect to Remote System Management.

Depending on the region where you are connecting to the Remote System Controllers, the following KVM TURN servers may be used with the wildcard (*) to allow for changes to Remote System Management specific TURN servers. When configuring a global fleet, you may decide to only configure the TURN server closest to each individual Remote System Controller:

Table 2-1 KVM TURN servers country location

Country	Domain	Port	Protocol
Singapore	*.kinesisvideo.ap-southeast-1.amazonaws.com	443	TCP/UDP
USA	*.kinesisvideo.us-west-2.amazonaws.com	443	TCP/UDP

Table 2-1 KVM TURN servers country location (continued)

Country	Domain	Port	Protocol
Germany	*.kinesisvideo.eu-central-1.amazonaws.com	443	TCP/UDP
China	*.kinesisvideo.cn-north-1.amazonaws.com.cn	443	TCP/UDP

For general IoT traffic, the following AWS gateways should be added to the firewall policies with the wildcard (*) to allow for changes to the Remote System Management specific gateway.

Table 2-2 AWS gateways for IoT traffic

Domain	Port
*.iot.us-east-1.amazonaws.com	443 and 8883
*.credentials.iot.us-east-1.amazonaws.com	443
*.s3.us-east-1.amazonaws.com	443 and 8883

For the various HP services to be accessible, the following should be added (no wildcard required):

Table 2-3 Gateways for HP services

Domain	Port
discovery.hpdaas.com	443
iot.api.hp.com	443
help-doc-icicle.oc.hp.com	443
signal-icicle.oc.hp.com	443
rsm.hp.com	443
rsmapi.hp.com	443

Bulk enrollment of devices to Remote System Management

To perform a bulk enrollment of multiple devices into HP Remote System Management (RSM), the process is slightly different from enrolling a single device. Use the following procedure to proceed with bulk enrollment.

Be sure that each Remote System Controller device has internet access. Be sure that the network settings of each Remote System Controller device allow communication with the RSM service. Users can have multiple organizations.

1. Access RSM settings: From the side menu on the dashboard, open the **RSM Settings** page.
2. Initiate bulk enrollment: In the **Enroll other devices to RSM** section, select the **Start** button to begin the bulk enrollment process.

3. Add devices: On the next page, choose one of the following methods to add devices:

   - **Upload a CSV File**: Upload a CSV file that contains the information for each device that you want to enroll. Ensure that the CSV file is correctly formatted according to the required specifications.
   - **Discover Devices on the Network**: Select the **Discover** button to find devices on the network automatically. You must provide the admin password to perform this operation.
   - **Add Manually**: Select the **Add manually** button to enter the IP address or host name and the admin password for each device individually.

4. Validate devices: After adding the devices, select the **Next** button to move to the validation section. In the validation section, select the **Validate all devices** button. This action checks the status of each device and updates them in the status column of the table.
5. Enroll devices: If some devices are marked as *ready to enroll* after validation, select the **Next** button to continue to the enroll section. In the enroll section, choose the **Enroll all devices** option for all devices that are ready.
6. Confirm enrollment: A modal window is displayed, asking for confirmation to redirect to the HP RSM portal. Select **Confirm** to be redirected to the HP Remote System Management portal, where you complete the bulk enrollment process.
7. Complete enrollment in RSM portal: Log in to the HP Remote System Management portal using your credentials. Accept the terms and conditions. Assign the enrolled devices to an organization. You can move devices between organizations later, if necessary.
8. Ensure enrollment: The enrolled devices are displayed in the selected organization within a few minutes. Check the organization to be sure that all devices have been successfully enrolled. This process allows you to enroll multiple devices at once.

3 Accessing and controlling the remote host

Learn how to use the HP Remote System Controller software interface to monitor and control a remote host.

Control the remote host power

The HP Remote System Controller can directly manipulate the power button signal on the remote host to control power.

The power options that are displayed are based on the remote host power status, which is determined by looking at the remote host power button LED signals. For the power controls to function properly, you should ensure that the 10-pin power and signal cable is connected to the remote host.

NOTE: Only certain Z by HP Desktop Workstation models currently support this feature. For a complete list of supported features, see Supported features on page 2.

Turn on the remote host

Follow this procedure to turn on the remote host.

1. On the left side of the dashboard, select **Host**.
2. In the Controls section, select **Power On**.

The remote host turns on.

NOTE: You can start a KVM session at any time to view the remote host display. See Accessing the remote host using KVM on page 24.

Turn off the remote host

Follow this procedure to turn off the remote host.

1. On the left side of the dashboard, select **Host**.
2. Do one of the following to turn off the remote host:
   - Select **Shutdown**, which is similar to turning off the remote host with a short press of the power button.
   - Select **Force Power Off**, which is similar to turning off the remote host with a long press of the power button.

NOTE: During the **Shutdown** operation, you can start a KVM session to monitor the progress of the shutdown. See Accessing the remote host using KVM on page 24.

After the remote host has been turned off, a message is displayed to alert you that no video output has been detected. Select **OK** to close the dialog, or select **Restart** to restart the remote host.

Restart the remote host

Use this procedure to restart the remote host.

1. On the left side of the dashboard, select **Host**.
2. Do one of the following:
   - Select **Restart**. This action is equivalent to a short press of the remote host power button, which triggers the operating system shutdown and power off according to the power button configuration in the operating system. After the remote host is turned off, the Remote System Controller automatically turns on the remote host.
   - Select **Force Restart**. This action is equivalent to a long press of the remote host power button to turn power off immediately, and then a short press of the power button to start the remote host.

NOTE: During the shutdown, you can start a KVM session to monitor progress.

While the remote host is turned off, a message displays to alert you that no video output has been detected. The video stream displays automatically when the remote host restarts.

Stopping the boot process in the BIOS menu

To stop the boot process and enter the workstation BIOS menus, without having to manually connect KVM and press the esc key to stop the boot, follow this procedure.

1. Access the embedded web interface of the Remote System Controller device.
2. In the **Host** screen, search for `Stop the boot process` in the BIOS menu switch.
3. Toggle the switch to the **On** state to enable this feature.
4. Restart the remote host using the **Restart** button.

Accessing the remote host using KVM

You can use the keyboard, video, and mouse (KVM) functionality to access the remote host and control functions remotely.

KVM hardware compatibility

Refer to the information below to determine the KVM hardware compatibility for your environment.

Table 3-1 KVM hardware compatibility

Function	Non-HP remote host	ZCentral 4R, Z4, Z6, or Z8 G4	Engage Flex Pro/Pro-C G2, Z2 G9, Z2 G1i/a, Z4, Z4 Rack, Z6, or Z8 G5
Video resolution in pixels and frames per second	Up to 4096 × 2160 at 25 fps or 2560 × 1440 at 60 fps	Up to 4096 × 2160 at 25 fps or 2560 × 1440 at 60 fps	Up to 4096 × 2160 at 25 fps or 2560 × 1440 at 60 fps
Mouse cursor	Yes	Yes	Yes
USB in preboot	Yes	Yes	Yes
USB in operating system	Yes	Yes	Yes

Table 3-1 KVM hardware compatibility (continued)

Function	Non-HP remote host	ZCentral 4R, Z4, Z6, or Z8 G4	Engage Flex Pro/Pro-C G2, Z2 G9, Z2 G1i/a, Z4, Z4 Rack, Z6, or Z8 G5
Function	Non-HP remote host	ZCentral 4R, Z4, Z6, or Z8 G4	Engage Flex Pro/Pro-C G2, Z2 G9, Z2 G1i/a, Z4, Z4 Rack, Z6, or Z8 G5
Support	Noncertified, supported in best effort approach	Certified, minimum BIOS firmware 2.90, full KVM support	Certified, full KVM support

Using the KVM menu

Use the KVM floating menu to perform the following tasks on the remote system.

Table 3-2 KVM floating menu tasks

Icon	Definition
	Select and hold the **Drag** icon to move the KVM floating menu.
	Click the **Pin** icon to make the KVM menu visible at all times.
136 Kbps | 22 fps | 0 ms	Displays the connection speed and the frames per second for the current session.
	Click the **Fullscreen** icon to view the remote session in fullscreen mode. Click it again to exit fullscreen mode. NOTE: While the current sessions is in fullscreen mode, you can execute common key press combinations on the remote system, for example, alt + tab.
	Click the **Ctrl + Alt + Del** icon to execute the ctrl + alt + del key press combination on the managed host. NOTE: To use other key press combinations on the managed host, use your keyboard in fullscreen mode.
	Click the **Pointer Lock** icon to control the cursor directly only on the managed host. Press esc to return to your local cursor. If you are in fullscreen mode, press esc for two seconds to recover your cursor. NOTE: Due to some application limitations, Pointer Lock mode activates the relative mouse mode as an alternative method to send mouse coordinates to the managed host. For example, mouse pointer positioning with some BIOS interfaces and some Linux® login screens only works properly using relative mouse coordinates.
	Displays the current KVM session users and who owns the input control. This is especially useful in collaboration mode.
	Opens the KVM session settings dialog.

Table 3-2 KVM floating menu tasks (continued)

Icon	Definition
	Click the **Exit** icon to close the remote session.

The KVM session settings are described in the table below.

Table 3-3 KVM Session Settings

Setting Name	Definition
Display collaboration border	If enabled, a border is displayed around the remote host desktop during a collaboration session.
Override display resolution	The Remote System Controller attempts to match the resolution of the host monitor. However, in some cases, a resolution change might not be correctly detected by the Remote System Controller. When this happens, a mouse offset can be introduced. You can use this setting to manually override the resolution detected by the Remote System Controller and correct the mouse offset issue.
Automatic resolution change detection	On Windows® systems, some resolution changes might not be detected by the Remote System Controller (see the notes below). If this setting is enabled, the Remote System Controller attempts to automatically detect these changes and fix any mouse offset issues.

NOTE: To avoid resolution detection issues, when available, HP recommends using an NVIDIA® Control panel to change the resolution of the Remote System Controller virtual display on Windows.

NOTE: If an NVIDIA Control Panel is not available, use the following procedure to change the resolution and avoid detection issues on Windows systems:

1. Open the *Display Settings* Panel.
2. Select **RSC virtual display**.
3. Select **Advanced display settings**.
4. Select **Display adapter properties**.
5. Select the **List all modes** button.
6. Select the desired resolution.
7. Select the **OK** button.
8. Select the **Apply** button.

Start a KVM session

Follow this procedure to start a KVM session.

1. On the left side of the dashboard, select **Host**.
2. In the Controls section, select **Start Session (KVM)**.

The KVM session appears in a new window and remains active as long as the remote host is turned on. See Using the KVM menu on page 25 for a complete list of the KVM menu options.

Using KVM

Follow these recommendations when you are working in a KVM session.

Using the keyboard

See the following recommendations for using the keyboard during a KVM session.

- Use the same keyboard layout on your local and remote host. If there are keyboard layout mismatches, some key presses might be incorrectly sent to the remote host.
- To ensure that key press combinations are correctly sent to the remote host, HP recommends that you use a Chrome or Microsoft Edge browser in fullscreen mode. If you are not in fullscreen mode, some key press combinations might not be sent correctly.

Viewing the video

See the following recommendations for viewing the video during a KVM session.

- The video on the remote host behaves like a physical monitor. The DisplayPort video stream is sent to the KVM browser window. The maximum resolution is 4096 × 2180.
- Because BIOS and preboot are displayed only in the primary physical monitor, you must ensure that the controller cable is connected to the primary display port on the remote host for the best quality video.
- If both the local monitor and the Remote System Controller require video streams, HP recommends that you use a DisplayPort splitter adapter that duplicates the DisplayPort stream from the primary display port to both the local monitor and the Remote System Controller mDP input.
- For optimum operating system desktop visualization with one or more physical monitors attached, HP recommends that you set duplicate monitors at the operating system level.

NOTE: The cursor might not behave as expected on the lock screen for this configuration due to operating system limitations.

- If you need to enter the BIOS of the host machine via KVM and *Enable vDisplay only during KVM Sessions* is turned on, be sure to initiate your KVM session before the host machine enters the BIOS. If the host machine has entered the BIOS before a KVM session as been initiated, start a KVM window and restart the host machine with the *Boot to BIOS* option enabled.

Using the mouse

See the following recommendations for using the mouse during a KVM session.

- Mouse movements and button presses are sent to the remote host. In the default mode, both the local and remote mouse cursors are visible. You can turn on the pointer lock mode by clicking the **Pointer Lock** icon  in the toolbar. This mode hides your local cursor and moves the remote cursor using relative coordinates, which might be required by some applications, for example, some BIOS interfaces.

- If the remote cursor does not move, HP recommends that you use the pointer lock mode feature in the toolbar. To exit pointer lock mode, press the esc key. When you are in fullscreen mode, press and hold the esc key for two seconds to exit pointer lock mode.

Navigating and accessing host information

Learn how to navigate and access host information.

Accessing host information

Use this procedure to access host information.

1. On the left side of the dashboard, select **Host**.
2. In the **Host** details area find the advanced host information.

Navigate the host information interface

Use this topic to navigate the host information interface.

There are three sections on the host information interface.

Table 3-4 Host information interface sections

Tab	Description
General	The **General** tab offers general details about the host, including the following information: • Manufacturer • Model • Serial number • BIOS version • Asset tracking number • Total system memory
CPU	The **CPU** tab provides information about the processors that the host contains, including the following information: • Model • Manufacturer • Cores • Threads • Clock speed • Turbo speed • Serial number • Part number

Table 3-4 Host information interface sections (continued)

Tab	Description
Memory	The **Memory** tab provides information about memory devices, such as a DIMM, and their configuration, including the following information: • Slot • Size (MiB) • Operating speed (MHz) • Memory type • Manufacturer • Serial number • Part number
Sensors	The **Sensors** tab provides telemetry information, such as system temperature and percentage of maximum fan speed. It also includes the following information: • Temperature: degrees/celsius or degrees/ Fahrenheit • Fan: percentage of maximum speed

NOTE: Only certain Z by HP Desktop Workstation models currently support this feature. For a complete list of supported features, see Supported features on page 2.

Mounting a virtual drive using virtual media

You can use the virtual media functionality to mount a drive image, such as ISO files, and present it to the host as if it were physically attached. This drive can be used as a boot target by the BIOS, making it useful for reimaging the host.

Using virtual media

Follow the steps in the following sections to use an image file as a virtual media in the host.

Choosing a virtual media mode

You choose between these modes for accessing the contents of an image file.

- Upload an image file to the Remote System Controller internal storage.
- Instruct the Remote System Controller to download a file from a network location.
- Streaming a file from a network location.

NOTE: The Remote System Controller supports the following protocols as the location for either mode: HTTP, HTTPS, FTP, and FTPS.

The Remote System Controller has limited internal storage. Without a microSD card installed, the maximum available space is 4.7 GB. To increase storage capacity, you can install an ATP Securstor microSD card (contact HP Sales for more details). Files that cannot fit in the Remote System Controller storage should use the streaming option.

Mounting the file

Follow this procedure to mount an image from the file menu.

- After the file is in the Remote System Controller internal storage, or the streaming target has been defined, mount the image from the file table by toggling the **Mount** key.

The Remote System Controller supports multiple virtual media instances, but only one image can be mounted at a time. The host detects that a new drive is being attached if an operating system is running. You can also target the virtual device as a boot target, if the image is capable of being booted.

Unmounting the file

Use this procedure to unmount the file.

- Toggle the **Mount** key to unmount a file.

  The file is still available for mounting again.

Removing a file

Use this procedure to remove a file from the Remote System Controller storage.

- Select the trash bin icon in the file table to either delete the file from the Remote System Controller storage, or remove the streaming target setup. In either case, the file is unmounted first.

Installing a microSD card

You can increase the storage capacity of the Remote System Controller by installing an ATP Securstor microSD card. Contact HP Sales for more details. Only supported microSD cards can be used.

If you are installing a microSD card, note the following:

- Installation instructions should be included with the card.
- You should not insert the microSD card into any other device before installing it in the Remote System Controller.
- You do not need to configure anything before installing the microSD card.
- After the microSD card is installed, the card will be used on the next boot.
- The Remote System Controller will securely configure the card such that the card can only be used with that particular Remote System Controller.

NOTE: Any virtual media files that are stored on the Remote System Controller when the microSD card is installed will be removed.

Navigating and configuring BIOS settings

This section describes how to navigate and configure BIOS settings.

Accessing BIOS settings

Follow the instructions outlined here to enter the Host BIOS settings section.

1. On the left side of the dashboard, select **Host**.
2. Scroll down to locate the Host BIOS settings.

NOTE: The Host BIOS settings that are displayed depend on what the host BIOS supports. HP recommends that you update the host BIOS to the latest version to gain access to the maximum number of BIOS settings.

Navigating the BIOS interface

The BIOS settings page offers an overview and several navigational tabs.

Table 3-5 **BIOS settings tabs**

Tab	Description
Main	General information about your system and basic settings
Advanced	Detailed settings for your hardware components
Security	Security features such as passwords and boot integrity settings
Boot Settings	Configuration for boot order and other options
Other	Additional settings not covered in the other tabs.

Adjusting BIOS settings

Follow this procedure to adjust BIOS settings.

1. Select a tab to view and adjust settings.
2. Navigate through the available options and adjust settings as needed.
3. Select **Apply Changes**. A dialog box opens with the following options:
   - **Apply Now and Reboot**: Immediately applies the changes and restarts your system.
   - **Apply on Next Reboot**: Changes are applied the next time you restart your system.
   - **Cancel**: No changes are applied, and you are returned to the previous screen.

IMPORTANT:

- Changes in BIOS settings are not applied until you choose to apply them. Be sure to select the correct option in configuration modal.
- Incorrect BIOS configurations can affect system stability. If you are uncertain, use the default settings or consult support documentation.

Booting to the virtual media drive

Use this procedure to boot to the virtual media drive in HP Remote System Controller.

The virtual media drive is attached through USB to the host.

- To enable booting from the virtual media drive, perform either of the following procedures:
  - In the BIOS boot menu, select the **USB boot** option.
  - Change the boot order BIOS configuration so that the USB option is located at the top.

4 Administering the Remote System Controller

Learn about the HP Remote System Controller administration features.

Perform a factory reset

When you perform a factory reset, the HP Remote System Controller resets to its initial configuration state. Complete one of the following tasks to perform a factory reset.

NOTE: The HP Remote System Controller does not retain any user data after a factory reset.

- In the **Operations** section in the **RSC Settings** tab, select **Factory Reset**.
- While the Remote System Controller is turned on, use a paper clip to carefully push the button (long press) in the RESET hole on the bottom of the controller (external), or on the PCIe bracket (internal) for 10 seconds.
- Use a Redfish API call

NOTE: When you perform a factory reset, the connection is closed and all configuration data pertaining to that particular Remote System Controller is not retained. Any data stored on an installed ATP Securstor microSD card is securely erased.

NOTE: A factory reset does not remove any firmware updates.

Restart the Remote System Controller

Complete one of the following tasks to restart the Remote System Controller:

NOTE: When you restart the Remote System Controller, it interrupts any activity that is currently occurring.

- Using a paper clip, carefully push the reset button (short press) in the RESET hole on the bottom of the controller (external), or on the PCIe plate (internal).
- Disconnect, and then reconnect the power cord from the Remote System Controller.
- Using API or through the web interface, restart the controller.

A Specifications

This section contains technical specifications for the physical aspects of your product, such as the weight and dimensions, as well as required environmental operating conditions and power source ranges.

Input power

The power information in this section can be helpful if you plan to travel internationally with the HP Remote System Controller.

NOTE: The AC power source must be rated at 100 V to 240 V, 50 Hz to 60 Hz. Although the Remote System Controller can be powered from a standalone AC power source, it should be powered only with the AC adapter that is supplied and approved by HP for use with the HP Remote System Controller, or by DC power from the remote host.

The HP Remote System Controller operates with the AC power adapter within the following specifications.

Table A-1 Input power ratings

Input Power	Rating
Operating voltage and current	40 W; input 100 V to 240 V, 1.2 A, 50 to 60 Hz. Output is 12 V at 3.33 A.

NOTE: This product is designed for IT power systems in Norway with phase-to-phase voltage not to exceed 240 V rms.

NOTE: You can find the HP Remote System Controller operating voltage and current on the regulatory label on the device.

Operating environment

This section provides information about the recommended operating environment for the HP Remote System Controller.

Table A-2 Operating environment specifications

Factor	Metric	U.S.
Temperature		
Operating	0°C to 40°C with AC adapter, 0°C to 50°C without AC adapter	32°F to 104°F with AC adapter, 32°F to 122°F without AC adapter
Nonoperating	-40°C to 60°C	-40°F to 140°F
Relative humidity (noncondensing)		
Operating	10% to 90%	10% to 90%

Table A-2 Operating environment specifications (continued)

Factor	Metric	U.S.
Nonoperating	5% to 95%	5% to 95%
Maximum altitude (unpressurized)		
Operating	-15 m to 5000 m	-50 ft to 16,404 ft
Nonoperating	-15 m to 12,192 m	-50 ft to 40,000 ft

B Troubleshooting

Use this information to troubleshoot issues with the HP Remote System Controller.

LED display status

The HP Remote System Controller LEDs indicate the following status information.

Remote host LED display status

The remote host LED indicates the following status information.

Table B-1 Remote host LED status

LED status	Definition
Off	Remote host is off.
Slow green blinking	Remote host is powered on.
Solid red	Remote host detects an error.

Remote System Controller LED status

The Remote System Controller LED indicates the following status information.

Table B-2 Remote System Controller LED status

LED status	Definition
Off	Remote System Controller is off.
Slow green blinking	Remote System Controller is starting up.
Fast green blinking	Remote System Controller is updating.
Solid green	Remote System Controller has completed startup.
Solid red	Remote System Controller error.

Network LED display status

The network LED indicates the following status information.

Table B-3 Network LED status

LED status	Definition
Off	Network is not connected.
Slow green blinking	Network is connected.
Solid green	Indicates an active KVM connection.

Table B-3 Network LED status (continued)

LED status	Definition
Solid red	Network error.

Issue resolution

Use this information to resolve HP Remote System Controller issues.

Table B-4 Issue resolution

Category	Issue	Cause	Solution
Login	Wrong user name or password.	• Make sure that you use *admin* (all lowercase) as the user name, and that you are typing the correct password, including capitalized letters. NOTE: If you forget the password, you can reset the Remote System Controller to the factory default settings and go through initial setup again.	Wrong user name or password.
	Server could not be contacted.	The certificate has changed.	Refresh the login page.
Power state	Unknown or inconsistent power state.	• 10-pin cable is not connected. • State is on while the remote host is in suspended mode.	• Reconnect the 10-pin cable. • Wake up the remote host by moving the mouse or pressing a key on the keyboard.
Health status	Status is critical.	Hardware component failure detected by remote host hardware.	Check the Logs menu for detailed information.
Host information	Host information is unknown.	• Remote host is not supported. • Remote host firmware is not supported.	• See Supported features on page 2 for more information. • Update the firmware for the remote host. NOTE: The Remote System Controller must be up and running when the remote host starts to see the remote host information.

Table B-4 Issue resolution (continued)

Category	Issue	Cause	Solution
KVM	No video detected and remote host power status is On.	• Video cable is disconnected or damaged. • Remote host is sleeping or suspended.	• Reconnect or replace the video cable. • Wake up the remote host by moving the mouse or pressing a key on the keyboard.
	Remote cursor is not showing up or is not aligned to the local cursor.	Remote host cursor might be positioned by another monitor.	• Activate Pointer Lock mode in the KVM toolbar. See. Using the KVM menu on page 25. • Unplug the monitor attached to the remote host.
	Screen is visible but the keyboard and mouse do not respond.	• Interrupted remote session. • USB cable disconnected or damaged.	Do one of the following: • Exit the session from the KVM toolbar, and then start a new session. • Use the Remote System Controller restart function to reset the controller.
	Image in the KVM video stream shows only a blank screen.	This might happen in the preboot state when a monitor is attached to the remote host and the main screen is not on the Remote System Controller.	Unplug the monitor or make sure that the Remote System Controller is the primary display.
	KVM session cannot be initiated while host machine is in BIOS.	This can happen if the KVM session is being initiated after the host machine has booted to BIOS and the feature “Enable vDisplay only during KVM sessions” is enabled.	If the setting for **Enable vDisplay only during KVM Sessions** is turned on, then restart the system with the KVM window active. While this setting is enabled, be sure to start the KVM session before entering the BIOS.
Firmware update	"Update Failed" message is displayed.	• Possible mismatch in the firmware image by selecting **Internal** to update an external controller or vice versa. • A previous version of the firmware was selected for updating rather than the current version. • If updating from versions older than 23.12, the update failure message might be a false positive.	Make sure that you are selecting the current firmware version.
Date and time	Wrong date and time are displayed.	NTP configuration with invalid data.	Make sure that the NTP server is valid, for example, Time.google.com.

Table B-4 Issue resolution (continued)

Category	Issue	Cause	Solution
Factory reset	After a factory reset, the current Remote System Controller firmware version is still shown.	The factory reset does not downgrade Remote System Controller firmware to the factory state. Only configuration and data revert to the factory state.	Expected behavior, no action required.
Restart	The browser reload does not return to the login page when you restart.	The Remote System Controller is still starting up.	Wait a few minutes, and then reload the page manually.
	Browser does not reload automatically.	The Remote System Controller is still starting up.	Wait a few minutes, and then reload the page manually.
Passwords	You are unable to change the password.	• You cannot use the last 24 passwords as your new password. • Password does not meet the minimum requirements.	Create a new password following the guidelines in Configure the password on page 13.
Network Connectivity	Cannot access the link loop address to start configuring the Remote System Controller for the first time.	The network does not have a DHCP, and the client computer running the browser does not have a route to the link loop network.	Manually add a route in your client computer operating system. IPv4 link-local addresses are assigned from address block 169.254. 0.0/16 (169.254. 0.0 through 169.254. 255.255). You need to add a route or a subnet to be able to access Remote System Controller addr with the URL https://rsc-%3cserial%3e.local. It is an operating system task in the machine where you have started the browser.
RSC Power	Remote System Controller is not powered in all host states.	The BIOS settings are configured to remove power in certain states.	Maximum Power Savings: This setting removes power to the Remote System Controller when the host is powered off. Therefore, HP recommends that you disable the setting when a Remote System Controller is installed. Energy/Performance BIOS Control = BIOS Controls EPB: On the ZCentral 4R, Z4 G4, Z6 G4, and Z8 G4 workstation platforms, power for the Remote System Controller is directed from the front USB ports. This setting can affect the power that is normally delivered to the front USB ports. To ensure that the BIOS maintains power to the Remote System Controller, HP recommends that you use the **BIOS Controls EPB** setting.

If you cannot resolve an issue, contact HP Support for further assistance. Be sure that you have the Remote System Controller log files available. See Generating log file information on page 40.

Generating log file information

If you are not able to resolve an issue, you can generate log files to use when you contact support for more assistance.

1. On the left side of the dashboard, select **RSC Settings**.
2. To create a `.zip` file containing the internal log files, select **Download Diagnostics Data**. You can use these log files to help resolve issues in the following areas:
   - Firmware
   - Network
   - Security
   - Services
   - Remote access
   - API

C Accessibility

HP's goal is to design, produce, and market products, services, and information that everyone everywhere can use, either on a standalone basis or with appropriate third-party assistive technology (AT) devices or applications.

HP and accessibility

Because HP works to weave diversity, inclusion, and work/life into the fabric of the company, it is reflected in everything HP does. HP strives to create an inclusive environment focused on connecting people to the power of technology throughout the world.

Finding the technology tools you need

Technology can unleash your human potential. Assistive technology removes barriers and helps you create independence at home, at work, and in the community. Assistive technology helps increase, maintain, and improve the functional capabilities of electronic and information technology.

For more information, see Finding the best assistive technology on page 42.

The HP commitment

HP is committed to providing products and services that are accessible for people with disabilities. This commitment supports the company's diversity objectives and helps ensure that the benefits of technology are available to all.

The HP accessibility goal is to design, produce, and market products and services that can be effectively used by everyone, including people with disabilities, either on a standalone basis or with appropriate assistive devices.

To achieve that goal, this Accessibility Policy establishes seven key objectives to guide HP actions. All HP managers and employees are expected to support these objectives and their implementation in accordance with their roles and responsibilities:

- Raise the level of awareness of accessibility issues within HP, and provide employees with the training they need to design, produce, market, and deliver accessible products and services.
- Develop accessibility guidelines for products and services, and hold product development groups accountable for implementing these guidelines where competitively, technically, and economically feasible.
- Involve people with disabilities in the development of accessibility guidelines and in the design and testing of products and services.
- Document accessibility features, and make information about HP products and services publicly available in an accessible form.
- Establish relationships with leading assistive technology and solution providers.
- Support internal and external research and development that improves assistive technology relevant to HP products and services.

- Support and contribute to industry standards and guidelines for accessibility.

International Association of Accessibility Professionals (IAAP)

IAAP is a not-for-profit association focused on advancing the accessibility profession through networking, education, and certification. The objective is to help accessibility professionals develop and advance their careers and to better enable organizations to integrate accessibility into their products and infrastructure.

As a founding member, HP joined to participate with other organizations to advance the field of accessibility. This commitment supports HP's accessibility goal of designing, producing, and marketing products and services that people with disabilities can effectively use.

IAAP will make the profession strong by globally connecting individuals, students, and organizations to learn from one another. If you are interested in learning more, go to http://www.accessibilityassociation.org to join the online community, sign up for newsletters, and learn about membership options.

Finding the best assistive technology

Everyone, including people with disabilities or age-related limitations, should be able to communicate, express themselves, and connect with the world using technology. HP is committed to increasing accessibility awareness within HP and with our customers and partners.

Whether it's large fonts that are easy on the eyes, voice recognition that lets you give your hands a rest, or any other assistive technology (AT) to help with your specific situation—a variety of assistive technologies make HP products easier to use. How do you choose?

Assessing your needs

Technology can unleash your potential. AT removes barriers and helps you create independence at home, at work, and in the community. AT helps increase, maintain, and improve the functional capabilities of electronic and information technology.

You can choose from many AT products. Your AT assessment should allow you to evaluate several products, answer your questions, and facilitate your selection of the best solution for your situation. You will find that professionals qualified to do AT assessments come from many fields, including those licensed or certified in physical therapy, occupational therapy, speech/language pathology, and other areas of expertise. Others, while not certified or licensed, can also provide evaluation information. You will want to ask about the individual's experience, expertise, and fees to determine if they are appropriate for your needs.

Accessibility for HP products

These links provide information about accessibility features and assistive technology, if applicable and available in your country or region, that are included in various HP products. These resources will help you select the specific assistive technology features and products most appropriate for your situation.

- HP Aging & Accessibility: Go to http://www.hp.com, type `Accessibility` in the search box. Select **Office of Aging and Accessibility**.
- HP computers: For Windows® products, go to http://www.hp.com/support, type `Windows Accessibility Options` in the **Search our knowledge** search box. Select the appropriate operating system in the results.
- HP Shopping, peripherals for HP products: Go to http://store.hp.com, select **Shop**, and then select **Monitors** or **Accessories**.

If you need additional support with the accessibility features on your HP product, see Contacting support on page 45.

Additional links to external partners and suppliers that may provide additional assistance:

- Microsoft Accessibility information (Windows and Microsoft Office)
- Google Products accessibility information (Android, Chrome, Google Apps)

Standards and legislation

Countries worldwide are enacting regulations to improve access to products and services for persons with disabilities. These regulations are historically applicable to telecommunications products and services, PCs and printers with certain communications and video playback features, their associated user documentation, and their customer support.

Standards

The US Access Board created Section 508 of the Federal Acquisition Regulation (FAR) standards to address access to information and communication technology (ICT) for people with physical, sensory, or cognitive disabilities.

The standards contain technical criteria specific to various types of technologies, as well as performance-based requirements which focus on functional capabilities of covered products. Specific criteria cover software applications and operating systems, web-based information and applications, computers, telecommunications products, video and multimedia, and self-contained closed products.

Mandate 376 – EN 301 549

The European Union created the EN 301 549 standard within Mandate 376 as an online toolkit for public procurement of ICT products. The standard specifies the accessibility requirements applicable to ICT products and services, with a description of the test procedures and evaluation methodology for each requirement.

Web Content Accessibility Guidelines (WCAG)

Web Content Accessibility Guidelines (WCAG) from the W3C's Web Accessibility Initiative (WAI) helps web designers and developers create sites that better meet the needs of people with disabilities or age-related limitations.

WCAG advances accessibility across the full range of web content (text, images, audio, and video) and web applications. WCAG can be precisely tested, is easy to understand and use, and allows web developers flexibility for innovation. WCAG 2.0 has also been approved as ISO/IEC 40500:2012.

WCAG specifically addresses barriers to accessing the web experienced by people with visual, auditory, physical, cognitive, and neurological disabilities, and by older web users with accessibility needs. WCAG 2.0 provides characteristics of accessible content:

- **Perceivable** (for instance, by addressing text alternatives for images, captions for audio, adaptability of presentation, and color contrast)
- **Operable** (by addressing keyboard access, color contrast, timing of input, seizure avoidance, and navigability)
- **Understandable** (by addressing readability, predictability, and input assistance)
- **Robust** (for instance, by addressing compatibility with assistive technologies)

Legislation and regulations

Accessibility of IT and information has become an area of increasing legislative importance.

The HP policy landscape website provides information about key legislation, regulations, and standards in the following locations:

- United States
- Canada
- Europe
- Australia

Useful accessibility resources and links

These organizations, institutions, and resources might be good sources of information about disabilities and age-related limitations.

NOTE: This is not an exhaustive list. These organizations are provided for informational purposes only. HP assumes no responsibility for information or contacts you encounter on the internet. Listing on this page does not imply endorsement by HP.

Organizations

These organizations are a few of the many that provide information about disabilities and age-related limitations.

- American Association of People with Disabilities (AAPD)
- The Association of Assistive Technology Act Programs (ATAP)
- Hearing Loss Association of America (HLAA)
- Information Technology Technical Assistance and Training Center (ITTATC)
- Lighthouse International
- National Association of the Deaf
- National Federation of the Blind
- Rehabilitation Engineering & Assistive Technology Society of North America (RESNA)
- Telecommunications for the Deaf and Hard of Hearing, Inc. (TDI)
- W3C Web Accessibility Initiative (WAI)

Educational institutions

Many educational institutions, including these examples, provide information about disabilities and age-related limitations.

- California State University, Northridge, Center on Disabilities (CSUN)
- University of Wisconsin - Madison, Trace Center

- University of Minnesota computer accommodations program

Other disability resources

Many resources, including these examples, provide information about disabilities and age-related limitations.

- ADA (Americans with Disabilities Act) Technical Assistance Program
- ILO Global Business and Disability network
- EnableMart
- European Disability Forum
- Job Accommodation Network
- Microsoft Enable

HP links

These HP-specific links provide information that relates to disabilities and age-related limitations.

HP comfort and safety guide

HP public sector sales

Contacting support

HP offers technical support and assistance with accessibility options for customers with disabilities.

NOTE: Support is in English only.

- Customers who are deaf or hard of hearing who have questions about technical support or accessibility of HP products:
  - Use TRS/VRS/WebCapTel to call (877) 656-7058 Monday through Friday, 6 a.m. to 9 p.m. Mountain Time.
- Customers with other disabilities or age-related limitations who have questions about technical support or accessibility of HP products:
  - Call (888) 259-5707 Monday through Friday, 6 a.m. to 9 p.m. Mountain Time.

Index

A

access host information 28
access security 13
accessibility 41, 42, 44, 45
accessibility needs
  assessment 42
add a local user 17
administration 33
assistive technology (AT)
  finding 42
  purpose 41
AT (assistive technology)
  finding 42
  purpose 41

C

Certificate Management 13
configure 802.1x Security 11
configure IPv4 assignment 9
configure IPv4 DNS server
  assignment 10
configure IPv4 DNS Server
  assignment 10
configure IPv4 Gateway 11
configure IPv6 DNS Server
  Assignment 11
configure local users 16
configure proxy settings 9
connecting the computer
  (external) 4
connecting to AC power 5
controller 7
customer support,
  accessibility 45

D

delete local user 18
disconnect the controller 6

E

edit local user permissions 17

F

factory reset 33
features 2
first use 7
front components (internal) 4
front panel components 2

G

getting started
  software features 1

H

HP Assistive Policy 41

I

input power 34
interface 23
International Association of
  Accessibility Professionals 42
issue resolution 37

K

KVM
  icons 25
  menu 25
  using 24
KVM compatibility 24
KVM session 27
  keyboard 27
  starting 26

L

LEDs 36
left panel components 3
logs 40

M

mouse 27

N

navigate and access host
  information 28
navigate the host information
  interface 28

O

operating environment 34

P

passwords 13
power off
  remote system 23
power on
  remote system 23

R

Redfish API 7
Remote System Controller LED
  status 36
requirements 1
resources, accessibility 44
restart 33
restart remote host 24
right panel components 3
RSM
  network requirements 20

S

Section 508 accessibility
  standards 43
specifications 34
standards and legislation,
  accessibility 43

T

troubleshooting 36
turn off
  remote system 23
turn on
  remote system 23

U

using the interface 8

V

video 27