User Guide

HP Remote Graphics Software 7.6

First Edition: January 2019

Document Part Number: L53029-001

Third-party software notice

Third-party source code and licenses are re-distributed, if required, with HP Remote Graphics Software.

User input syntax key

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

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

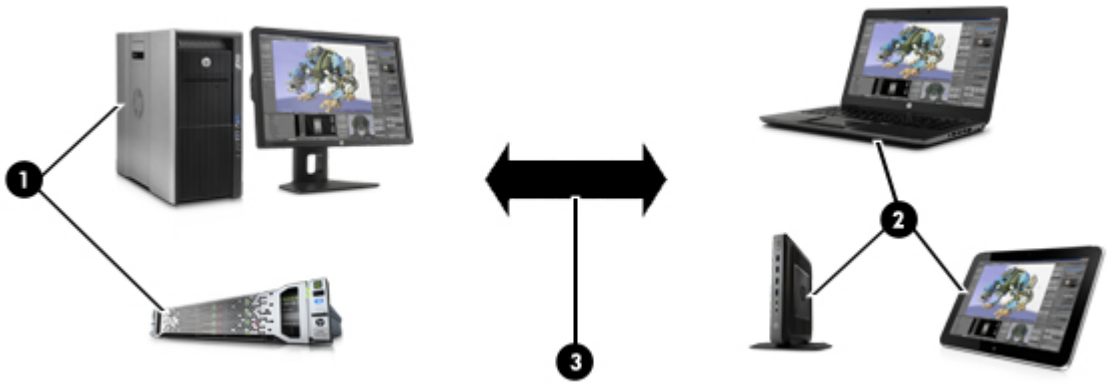
Table of contents

1 RGS overview

HP Remote Graphics Software (RGS) brings added security, performance, mobility, and collaboration to your workstation deployment. With RGS, you can use a lower-powered desktop, notebook, or thin client to remotely connect to a powerful workstation and use your graphics-intensive workstation programs wherever you go.

Your programs run natively on the remote workstation and take full advantage of its graphics resources. The desktop of the remote workstation is transmitted over a standard network to your local computer using advanced image compression technology specifically designed for digital imagery, text, and high frame rate video applications.

The following image and table demonstrate a typical RGS deployment.



Item	Description
1	The **sender** is typically a high-performance workstation, virtual workstation, blade, or server that hosts your software. **RGS Sender** is installed on the sender and transmits graphics, audio, and USB data to the receiver. The sender receives input and USB data from the receiver. **NOTE:** A monitor does not necessarily have to be connected to the sender.
2	The **receiver** is typically a desktop, notebook, tablet, or thin client with **RGS Receiver** installed. You establish the RGS connection from the receiver side. The desktop of the sender is displayed inside the **RGS Receiver window** on the receiver, and RGS Receiver transmits input to the sender, allowing you to interact with your programs remotely.
3	A TCP/IP network serves as the communication link between the sender and the receiver. **IMPORTANT:** The sender and receiver must be on the same network for an RGS connection to be established between them.

NOTE: RGS software and documentation might also refer to the sender and the receiver as the remote computer and the local computer respectively.

RGS system requirements, such as hardware and operating system support, are not discussed in this document. Some RGS features might have additional system requirements. System requirements are described in the *QuickSpecs* (see Finding more information on page 4).

Features

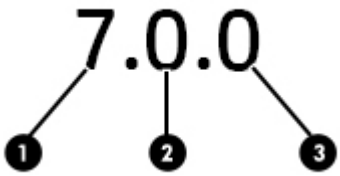
RGS includes a variety of features, including the ones described in the table below.

NOTICE: Some features are not supported by certain operating systems.

Feature	Description
3D graphics API support	Provides workstation-class performance for software based on OpenGL or Direct X **NOTICE:** See Software compatibility with RGS on page 3 for information about the types of programs and configurations that HP does and does not recommend for use with RGS.
Advanced Video Compression (Windows®/ Linux® only)	Reduces the network bandwidth needed for high-quality video streams See Advanced Video Compression (Windows/Linux only) on page 32 for more information.
Authentication methods	Support varied deployment scenarios and preferences, including smart card redirection See Authentication on page 33 for more information.
Collaboration	Lets multiple receivers connect to the same sender simultaneously, allowing multiple users to view and interact with the same desktop session and programs See Collaboration on page 35 for more information.
Directory Mode	Lets a single receiver connect to multiple senders simultaneously See Directory Mode on page 52 for more information.
Display resolution and layout matching	Adjusts the display resolution and display layout of the sender to match those of the receiver, even when using multiple monitors See Display resolution and layout matching on page 38 for more information.
HP Velocity (Windows/Linux only)	Improves performance within a wide area network (WAN) See HP Velocity (Windows/Linux only) on page 33 for more information.
Remote Audio	Transmits smooth, continuous, low-latency, high-quality audio from the sender to the receiver See Remote Audio on page 46 for more information.
Remote Clipboard	Lets you cut, copy, and paste data between the sender and the receiver or between two different senders See Remote Clipboard on page 48 for more information.
Remote USB (Windows/ThinPro only)	Lets receiver-side USB devices be mounted to and accessed by the sender through the RGS connection See Remote USB (Windows/ThinPro only) on page 49 for more information.
Sender screen blanking	Blanks the screen of the sender monitor (if one is connected) so that the desktop session is not visible at the sender See Sender screen blanking on page 44 for more information.
Touch features (Windows only)	Lets you control your remote desktop with touch input and configure custom gestures See Using touch features (Windows touch-capable devices only) on page 44 for more information.

Interoperability between different versions of RGS

Interoperability is supported between different versions of RGS Sender and RGS Receiver only if they have the same primary version number.



Item	Description
1	**Primary version number**—A primary release typically contains upgrades and changes significant enough that interoperability with previous primary releases is not guaranteed by HP. For example, a connection between different primary releases of RGS Sender and RGS Receiver might not function at an acceptable quality, or at all.
2	**Minor version number**—This number being non-zero represents a minor release, which typically introduces new features or enhances existing functionality, as well as rolling up changes from any previous patch releases. A connection between different minor releases (but the same primary release) of RGS Sender and RGS Receiver should function at an acceptable quality.
3	**Patch version number**—This number being non-zero represents a patch release, which is typically only for fixing major security issues or defects. A connection between different patch releases (but the same primary release) of RGS Sender and RGS Receiver should function at an acceptable quality.

NOTE: Each release of RGS is a complete release of the entire product, regardless of which components have changed.

Software compatibility with RGS

RGS works with most software that runs in windowed mode, including those based on OpenGL and Direct X. See below for some exceptions:

- The installation of RGS Sender disables video overlay surfaces on the sender. Most OpenGL-based software will adjust to this and still work correctly, but in some cases, the following could happen as a result:
  - Some OpenGL-based software might display incorrectly.
  - Media players that use video overlay surfaces might display incorrectly.

  If these types of issues occur, it is likely because the software is still trying to use video overlay surfaces even though they are disabled. This can sometimes be resolved if the software has an option to disable the use of video overlay surfaces.

NOTICE: RGS Sender does not support programs in full-screen exclusive mode. This means that RGS is not suitable for most full-screen games.

RGS Sender licensing

RGS Sender is included with HP Z workstations and HP ZBook mobile workstations. A separate license purchase is not required for RGS Sender on these products.

RGS Sender requires a license if installed on any other computer. Further information can be found in the *Licensing Guide* (see Finding more information on page 4).

NOTE: An RGS connection can be established without a license; however, a warning message about the missing license will overlay the RGS Receiver window, blocking a significant portion of the Sender desktop.

NOTE: RGS Receiver is a free download for all devices.

Finding more information

The table below can be used to find more information about RGS.

Resource	Contents
RGS website http://www.hp.com/go/rgs	• More RGS documentation, including the following: – *Licensing Guide*—Describes how to obtain and install licensing for RGS Sender. – *QuickSpecs*—Describes RGS system requirements.
RGS at HP Support Center http://www.hp.com/support/rgs	• User guides for some previous versions of RGS. Select **HP Remote Graphics Software (RGS)**. • Worldwide support – Online chat with an HP technician – Support telephone numbers **NOTE:** If your phone call is answered by a voice recognition system and you are asked to say the name of the product, say "Remote Graphics Software".

2 Getting started

The following procedure is a high-level description of how to get started using RGS:

1. Install RGS Sender and RGS Receiver.
2. Open RGS Receiver.
3. Start an RGS session with the sender.

   a. On the **Home** panel of RGS Receiver, enter the hostname or IP address of the sender, and then press the Enter key or select the **Connect** button.

   b. In the RGS authentication window that appears, enter the credentials of a user account that resides on the sender, and then select **OK**.

   If authentication is successful, the RGS session starts, and the sender desktop appears inside the RGS Receiver window that opens on the receiver.

NOTE: If the sender desktop was in a locked state when you started the RGS session, you must unlock the desktop by entering the credentials again, this time into the logon screen on the sender.

On a Windows®-based sender, if the logon screen instructs you to press Ctrl+Alt+Del to start the logon process, you must instead press Ctrl+Alt+End to trigger the desired action on the sender.

3 Installation

Installing RGS Receiver (Windows)

The installer wizard for the RGS Receiver allows for both Typical and Custom installations. The Typical installation installs Remote USB and Remote Clipboard. The Typical installation should be suitable for most deployments.

The Custom installation type lets you choose whether you want to install certain features, as well as specify proxy settings. A custom installation can be performed on the command line as well.

IMPORTANT: Windows administrator privileges are required to perform the installation.

NOTE: If the software is already installed, installing a newer version will perform an update. Attempting to install the same version or an older version will cause the installer to exit without making changes to the system.

NOTE: During the installation process, the installer creates a log file named `rgreceiverInstaller.log` in the location specified by the Windows `TEMP` environment variable.

Performing a custom RGS Receiver installation using the installer wizard

To perform a custom installation of RGS Receiver on Windows using the installer wizard:

1. Run `ReceiverSetup64.exe`, follow the on-screen instructions until you are prompted to choose a setup type, select **Custom**, and then select **Next**.
2. On the **Remote USB Configuration** page, select the desired installation setting for the Remote USB feature (options described below), and then select **Next**.
   - **USB devices are Local**—Remote USB is not installed on the receiver, and all receiver-side USB devices always mount to the receiver only, even during an RGS session.
   - **USB devices are Remote**—Remote USB is installed, and all receiver-side USB devices always mount to the sender only, which means the USB devices are accessible only during an RGS session. The USB devices cannot mount to the receiver at any time, regardless of the RGS connection state.
   - **USB devices are Local/Remote**—Remote USB is installed, and each USB device has its access set individually to either the receiver or the sender, depending on when the USB device is plugged in to the receiver.
     - If a USB device is plugged in to a USB port on the receiver while RGS Receiver is disconnected, the USB device becomes accessible by the receiver only.
     - If a USB device is plugged in to a USB port on the receiver while RGS Receiver is connected, the USB device becomes accessible by the sender only.

     Access to a particular device can be switched by removing it and then re-inserting it while RGS Receiver is in the opposite connection state.

NOTE: This setting controls whether Remote USB components are *installed*. To change this setting after installation, you must uninstall and reinstall RGS Receiver. If installed, Remote USB can be *disabled* (and re-enabled) later using RGS Receiver or the RGS Receiver Configuration tool.

Alternatively, the Remote USB installation setting can be overridden for individual devices (without a reinstallation) by an advanced option that is not offered by the installer (see Configuring the remoting behavior of individual USB devices (Windows only) on page 49).

3. On the **Remote Clipboard Configuration** page, select whether you want the Remote Clipboard feature installed, and then select **Next**.

NOTE: This setting controls whether Remote Clipboard components are *installed*. To change this setting after installation, you must uninstall and reinstall RGS Receiver. If installed, Remote Clipboard can be *disabled* (and re-enabled) later using RGS Receiver or the RGS Receiver Configuration tool.

4. If the next page of the wizard is titled **Proxy Configuration**, select the appropriate setting as described below, and then select **Next**. If the next page prompts you to start the installation next, then RGS automatically detected and leveraged the proxy settings from Internet Explorer, and you can skip this step.
   - If the receiver accesses the Internet through a proxy server, select **Use this proxy** and enter the proxy address and port.
   - If the receiver does not access the Internet through a proxy server, leave **Do not use a proxy** selected.

IMPORTANT: Proxy server settings must be configured correctly to activate RGS Advanced Features. See RGS Advanced Features (Windows/Linux only) on page 32 for more information.

5. Select **Install** to start the installation process.
6. When prompted, restart the computer to complete the installation.

Performing a custom RGS Receiver installation on the command line

RGS command-line options must be preceded by a `/z` flag and be enclosed in double quotes, with no space before or after the opening double quote and no space before the closing double quote. If using multiple commands, separate them with a single space. See the example below:

```
ReceiverSetup64.exe /z"/autoinstall /agreetolicense"
```

If you need to include a double quote as part of a parameter (such as for a folder path), then you should precede each of those double quotes with a backwards slash like in the following example:

```
ReceiverSetup64.exe /z"/autoinstall /agreetolicense /folder=\"C:\RGS Receiver\""
```

NOTE: This command must be issued from the location of the ReceiverSetup64.exe installation file.

Unless a folder path is specified, RGS will be installed in the folder: `C:\Program Files\HP\Remote Graphics Receiver`.

The following table describes the installation-related command-line options.

IMPORTANT: The options `/autoinstall` and `/agreetolicense` are always required when performing the installation on the command line.

Option	Description
`/autoinstall`	Initiates the installation
`/agreetolicense`	Accepts the license agreement
`/folder=\"<folder path>\"`	Specifies the folder path to install to, which is the following by default if not specified: `C:\Program Files\HP\Remote Graphics Receiver` **NOTE:** The folder path `C:\Program Files\HP\Remote Graphics Receiver` applies to 64-bit versions of Windows. On 32-bit versions of Windows, the folder path is `C:\Program Files\Hewlett-Packard\Remote Graphics Receiver`.
`/usb={local|remote|localRemote}`	Sets the desired Remote USB installation option, which is `localRemote` by default if not specified For a description of each option, see Performing a custom RGS Receiver installation using the installer wizard on page 6.
`/clipboard`	Installs the Remote Clipboard feature
`/noreboot`	Prevents the computer from restarting at the end of the installation process
`/proxy=<IP address>:<port>`	Configures proxy settings to allow for activation of RGS Advanced Features. **IMPORTANT:** Activation of RGS Advanced Features does not work through a proxy server if the proxy settings are not configured correctly. See RGS Advanced Features (Windows/Linux only) on page 32 for more information.

The following table describes additional command-line options for the installer.

NOTE: If either `/help` or `/viewlicense` is used, all other options are ignored.

Option	Description
`/help`	Displays the valid command line options
`/viewlicense`	Displays the EULA (End User License Agreement)
`/autoremove`	Initiates an uninstallation **NOTE:** The option `/noreboot` can be used in conjunction with this option.

Installing RGS Sender (Windows)

The installer wizard for the RGS Sender allows for both Typical and Custom installations. The Typical installation installs Remote USB and Remote Clipboard but not smart card redirection. The Typical installation should be suitable for most deployments.

The Custom installation lets you choose whether or not to install certain features. A custom installation can be performed on the command line as well.

IMPORTANT: Windows administrator privileges are required to perform the installation.

NOTE: If an older version of the software is already installed, installing a newer version will perform an update. Attempting to install the same version or an older version will cause the installer to exit without making changes to the system.

NOTE: During the installation process, the installer creates a log file named `rgsenderInstaller.log` in the location specified by the Windows `TEMP` environment variable.

Installer wizard installation

To perform a custom installation of RGS Sender on Windows using the installer wizard:

NOTE: The installer wizard might contain additional options not discussed below regarding installation of beta features. Do not install these features unless instructed to by HP.

1. Run `SenderSetup64.exe`, follow the on-screen instructions until you are prompted to choose a setup type, select **Custom**, and then select **Next**.
2. On the **Remote Graphics Sender Configuration** page, select whether you want the Remote USB, smart card redirection, and Remote Clipboard features installed, and then select **Next**.

   NOTE: These settings control whether the features are *installed*. To change these settings after installation, you must uninstall and reinstall RGS Sender. If installed, Remote Clipboard can be *disabled* (and re-enabled) later using the RGS Sender Configuration tool.
3. On the **Single Sign-On / Easy Login Configuration** page, select the desired authentication method, and then select **Next**.

   TIP: You can change the authentication method after installation. See Authentication on page 33 for more information and for a description of each of the authentication methods.

   NOTE: If you select **Do not enable either**, then the standard authentication method will be used.
4. If the next page of the wizard is titled **Remote Graphics Sender Licensing**, complete this step. If the next page prompts you to start the installation next, then an RGS Sender license is either already installed or is not required, and you can skip this step.

   On the Remote Graphics Sender Licensing page, select the appropriate option depending on if you have an RGS Sender license file ready to install, select **Next**.

   If you chose to install a license file, follow the on-screen instructions to complete that procedure before proceeding to the next step.

   NOTE: For a brief overview of RGS Sender licensing requirements, see RGS Sender licensing on page 4. For detailed information and instructions about RGS Sender licensing, see Finding more information on page 4 to locate the *Licensing Guide*.
5. You will be prompted to restart your computer after the RGS Sender installation is complete. Select **Yes** when asked to restart the system.
6. Select **Install** to start the installation process.
7. When prompted, restart the computer to complete the installation.

Command-line installation

RGS command-line options must be preceded by a `/z` flag and be enclosed in double quotes, with no space before or after the opening double quote and no space before the closing double quote. If using multiple commands, separate them with a single space. See the example below:

```
SenderSetup64.exe /z"/autoinstall /agreetolicense"
```

If you need to include a double quote as part of a parameter (such as for a folder path), then you should precede each of those double quotes with a backwards slash like in the following example:

```
SenderSetup64.exe /z"/autoinstall /agreetolicense /folder="C:RGS Sender""
```

The following table describes the installation-related command-line options.

NOTE: This command must be issued from the location of the SenderSetup64.exe installation file.

NOTE: Unless a folder path is specified, RGS will be installed in the folder `C:\Program Files\HP\Remote Graphics Sender`.

IMPORTANT: The options `/autoinstall` and `/agreetolicense` are always required when performing the installation on the command line.

Option	Description
`/autoinstall`	Initiates the installation
`/agreetolicense`	Accepts the license agreement
`/folder=\"<folder path>\"`	Specifies the folder path to install to, which is the following by default: `C: Program Files HP Remote Graphics Sender` **NOTE:** The folder path `C:\Program Files\HP\Remote Graphics Sender` is applicable only to 64-bit versions of Windows. On 32-bit versions of Windows, the folder path is `C:\Program Files\Hewlett-Packard\Remote Graphics Sender`.
`/usb`	Installs the Remote USB feature
`/clipboard`	Installs the Remote Clipboard feature

`/el`
—or—
`/sso`
	Enables Easy Login or Single Sign-on
	NOTE: If neither option is specified, the standard authentication method will be used.

`/rgslicenseserver=[<port>@]<host>`
—or—
`/rgslicensefile=\"<file path>\"`
	IMPORTANT: You can use either `/rgslicenseserver` or `/rgslicensefile` but not both. If neither is used, RGS Sender is installed without a license.
	`/rgslicenseserver`—Specifies the license server that RGS Sender should acquire a license from during installation
	NOTE: If a port is not specified, the default port of the host is used.
	`/rgslicensefile`—Specifies the location of a license file on the local system

`/noreboot`	Prevents the computer from restarting at the end of the installation process.
`/smartcard`	Installs the smart card redirection feature.

The following table describes additional command-line options for the installer.

NOTE: If either `/help` or `/viewlicense` is used, all other options are ignored.

Option	Description
`/help`	Displays the valid command line options
`/viewlicense`	Displays the EULA (End User License Agreement)
`/autoremove`	Initiates an uninstallation

Option	Description
	NOTE: The option `/noreboot` can be used in conjunction with this option.

Installing RGS Receiver (Linux)

To install RGS Receiver on Linux®:

1. Log in as root.
2. Go to the download directory for the RGS Receiver and unpack the RGS package. RGS for Linux includes installers specific to Linux distributions. Change to the directory that matches your distribution.
3. Execute the following command:

   ```
   ./install.sh
   ```

TIP: Optionally, add the directory `/opt/hpremote/rgreceiver` to your `PATH` environment variable.

Installing RGS Sender (Linux)

To install RGS Sender on Linux:

IMPORTANT: Before proceeding, make sure you already have the appropriate NVIDIA® graphics driver installed on the sender. The NVIDIA driver installation creates the file `/etc/X11/xorg.conf`, which might be used during the installation process (depending on your Linux distribution), so the NVIDIA driver must be installed first. System requirements can be found in the *QuickSpecs* (see Finding more information on page 4).

1. Log in as root.
2. Go to the download directory for the RGS Sender and unpack the RGS package. RGS for Linux includes installers specific to Linux distributions. Change to the directory that matches your distribution.
3. Execute the following command:

   ```
   ./install.sh
   ```

4. The installer gives you the option to allow some configuration files to be modified automatically. You must accept this option to complete the installation.
5. If the sender has the pcsc-lite package installed, the installer gives you the option to install smart card redirection. By default, this feature does not install.

Installing RGS Receiver (Mac OS)

On Mac OS, you can install RGS Receiver using the installer wizard or on the command line.

NOTE: If the software is already installed, the installation process overwrites it.

Installer wizard installation

1. Log in as an administrator (or be able to provide administrator credentials).
2. Run **HP RGS Receiver.pkg**, and then follow the on-screen instructions.

Command-line installation

Execute the following command:

```
sudo installer -pkg "HP\RGS\Receiver.pkg" -target /
```

NOTE: To install RGS Receiver in a location other than the root of the boot volume, enter `/Volumes/OtherDrive` instead of `/` at the end of the command.

4 RGS Receiver overview

Opening RGS Receiver

To open RGS Receiver on Windows:

▲ Perform the action below that corresponds to the operating system of the receiver.

Operating system	Procedure
Windows 7	Select **Start**, select **All Programs**, select **HP**, select **HP Remote Graphics Software**, and then select **HP RGS Receiver**.
Windows 8.1	Select the **HP RGS Receiver** tile on the Start screen.
Windows 10	Select **Start** , type `RGS`, and then select **HP RGS Receiver** from the search results.

To open RGS Receiver on Linux:

▲ Run the executable `/opt/hpremote/rgreceiver/rgreceiver.sh`.

– or –

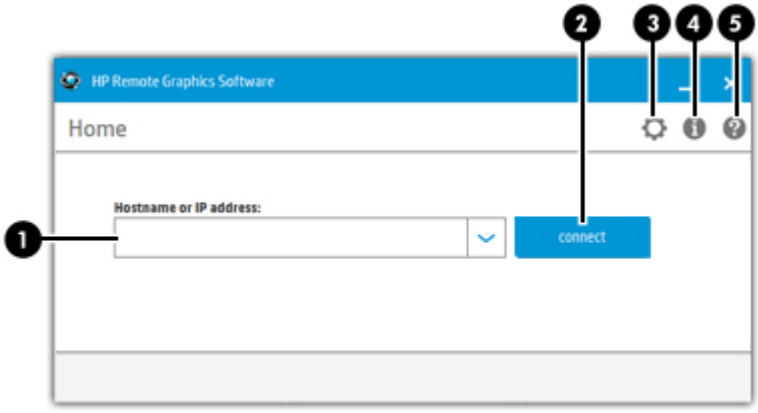
Select **Applications**, select **Internet**, and then select HP RGS Receiver.

To open RGS Receiver on Mac OS:

▲ Select the RGS Receiver icon in Launchpad.

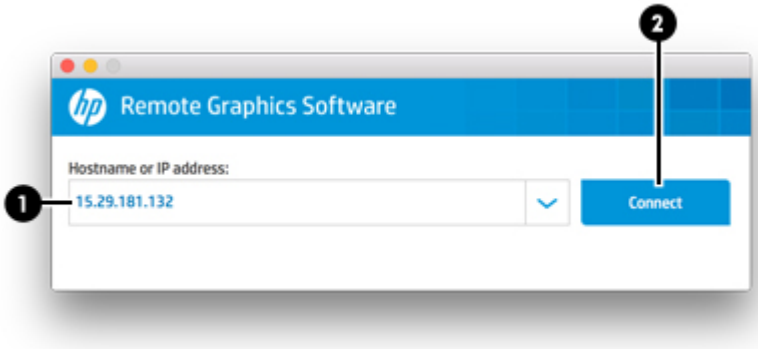
TIP: RGS Receiver can alternatively be started on the command line (see RGS Receiver command-line options on page 23).

RGS Receiver GUI (Windows/Linux)



Item	Description
1	Enter the hostname or IP address of the sender in this field. **TIP:** The drop-down list contains recent entries.
2	Initiates the connection.
3	Opens the **Settings** panel (see RGS Receiver settings on page 19 for more information).
4	Opens the **Info** panel, which contains version information and the *End User License Agreement* (EULA) for RGS, as well as third-party acknowledgments.
5	Opens the *User Guide* (this document).

RGS Receiver GUI (Mac OS)



Item	Description
1	Enter the hostname or IP address of the sender in this field. **TIP:** The drop-down list contains recent entries.
2	Initiates the connection.

Starting an RGS session

To start an RGS session:

1. On the **Home** panel of RGS Receiver, enter the hostname or IP address of the sender, and then press the Enter key or select the **Connect** button.
2. This step depends on the authentication method you are using (see Authentication on page 33).

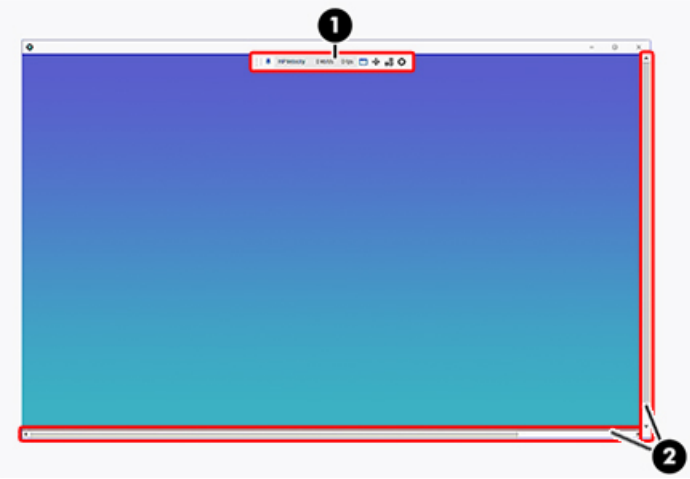
   Enter the credentials as required by the authentication method.

If authentication is successful, the RGS session starts, and the sender desktop appears inside the RGS Receiver window that opens on the receiver.

Note the following additional information about creating an RGS connection:

- If this is your first time establishing an RGS connection, you might receive a confirmation message or error message, depending on the activation status of RGS Advanced Features.
- You cannot connect to more than one sender at a time using the GUI of RGS Receiver. If an attempt is made to connect to a second sender, the connection to the first sender is terminated. For information about how to connect to more than one sender at a time, see Directory Mode on page 52.

RGS Receiver window GUI (Windows/Linux)

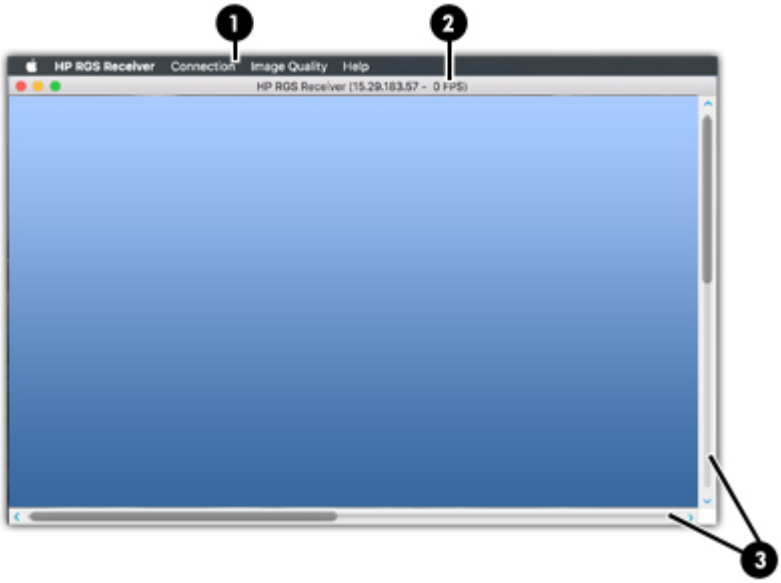


Item	Description
1	The **RGS Receiver toolbar** provides easy access to the most frequently used options (see RGS Receiver toolbar GUI (Windows/Linux) on page 16 for more information).
2	Scroll bars appear if the resolution of the sender is larger than the size of the RGS Receiver window.

RGS Receiver toolbar GUI (Windows/Linux)

Icon	Description
	By clicking and holding the left mouse button while moving the mouse, the toolbar may be moved horizontally.
	Allows the toolbar to be pinned or unpinned to the Receiver window. If it is unpinned, it will hide when not in use. To unhide the toolbar, hover the mouse near the top of the Receiver window.
	Displays the current status of HP Velocity (see HP Velocity (Windows/Linux only) on page 33 for more information).
	Displays the current network bandwidth consumed by the connection.
	Displays the number of image updates in frames-per-second.
	Opens the virtual keyboard (see Using touch features (Windows touch-capable devices only) on page 44 for more information).
	Enables the virtual mouse (see Using touch features (Windows touch-capable devices only) on page 44 for more information). **TIP:** The virtual mouse also can be enabled and disabled using the 4-finger tap gesture.
	Adds or removes window borders on the RGS Receiver window. When borders are removed, this icon is grayed out, and a minimize icon and an X (close) icon are displayed.
	Toggles Setup Mode (see Setup Mode on page 18).
	Sends a virtual Ctrl+Alt+Del command to the sender.
	Opens the **Settings** panel (see RGS Receiver settings on page 19 for more information).

RGS Receiver window GUI (Mac OS)



Item	Description
1	The **RGS Receiver toolbar** provides easy access to the most frequently used options via the following menus: • **HP RGS Receiver**—Lets you view version information, change settings (see RGS Receiver settings on page 19), and quit RGS Receiver. **NOTE:** RGS settings are also known as preferences on Mac OS. • **Connection**—Lets you enable Setup Mode (see Setup Mode on page 18), send a virtual Ctrl+Alt+Del command to the sender, and disconnect from the sender. • **Image Quality**—Lets you set the image quality (see Performance on page 20 for more information). • **Help**—Lets you open the *User Guide* (this document).
2	Displays the number of image updates in frames-per-second.
3	Scroll bars appear if the resolution of the sender is larger than the size of the RGS Receiver window, or when the Receiver window is adjusted below the size of the sender resolution.

Setup Mode

In Setup Mode, transmission of keyboard and mouse input to the sender is suspended. Instead, the keyboard and mouse can be used to interact with the RGS Receiver window on the receiver. In this mode, you can do the following:

- Move an RGS Receiver window that has its title bar and borders hidden
- Select (bring to the front) a specific RGS Receiver window that might be obscured by another RGS Receiver window in Directory Mode
- The following Setup Mode HotKeys can be used to control the HP RGS Receiver application:

  M: Display the RGS Receiver Settings window.

  N: Minimize the Receiver window.

  C: Close the Receiver window.

  G: Toggle Game Mode.

  H: Hide the toolbar.

  F: Fit the Receiver window size to the Sender desktop size.

Setup Mode can be activated in two ways:

- Select the Setup Mode button (Windows/Linux) or menu item (Mac OS) on the RGS Receiver toolbar to toggle the state of Setup Mode.
- Type the default hotkey sequence as follows:

  Press and hold down Left Shift. While pressing Left Shift, press and release Space. Setup Mode will remain active as long as Left Shift is held down.

NOTE: The default hotkey sequence can be changed (see Changing the Setup Mode hotkey sequence on page 18).

Changing the Setup Mode hotkey sequence

RGS allows you to change the Setup Mode hotkey sequence from its default value of Left Shift press, Space press, and Space release.

When defining a new Setup Mode hotkey sequence, the following keys can be used:

- Left Ctrl, Right Ctrl, Ctrl—Specifies a left, right, or side-insensitive Ctrl key, respectively.
- Left Alt, Right Alt, Alt—Specifies a left, right or side-insensitive Alt key, respectively.
- Shift
- Space

Every sequence must begin with Ctrl, Alt, or Shift. Two actions are associated with each key:

- Down: Specifies a key press.
- Up: Specifies a key release.

To change the Setup Mode hotkey sequence:

1. In the **Hotkeys** panel of the RGS Receiver settings, click **Set**.
2. Press and hold the first key that you want to use in the sequence.

3. Press and release the other keys that you want to use in the sequence.
4. Release the initial key.

Click **Reset** restores the Setup Mode hotkey sequence to its default values.

RGS Receiver settings

This section describes the settings available in RGS Receiver, which are divided into the following categories:

- Connection
- Performance
- Gestures (Windows touch-capable devices only)
- Audio
- Network
- Hotkeys
- Logging
- Statistics (Windows/Linux only)

Connection

The following table describes the settings available in the **Connection** panel.

Setting	Description
Prompt for username and password	Forces the authentication prompt to display when starting an RGS connection. In certain scenarios, RGS will not prompt you to enter a domain, username, and password when starting an RGS connection. If you need to enter a domain, username, and password, then check this box. **TIP:** This is advantageous when using RGS in Directory Mode where there are different connection needs for each session.
Match Receiver display resolution	Attempts to set the sender's resolution to match the receiver's resolution. **NOTE:** This option is not supported on Linux by default. You must configure the X Server with the proper modelines and/or metamodes for this option to work. See Matching display resolution and layout (Linux-based sender) on page 41 for more information.
Match Receiver display layout	Attempts to set the sender's display layout to match the receiver's display layout. For example, if the receiver has two physical displays side-by-side and an overall display resolution of 2560x1024, RGS will attempt to set the sender to the same layout and resolution. If that fails, RGS will attempt to set a resolution of 2560x1024 on a single sender display. **NOTE:** This option is not supported if the sender is Linux-based.
Enable remote USB **NOTE:** Windows/HP ThinPro only	Enables Remote USB.
Select Sender	Becomes active when Directory Mode is enabled. Allows the user to remote USB devices to a sender selected from the drop-down list.
Enable remote clipboard	Enables Remote Clipboard.

Performance

The performance settings allow you to improve the interactive experience. Typically, these adjustments will be made when working with highly interactive applications (such as a CAD application) in a low-bandwidth or high-latency network environment.

The following table describes the settings available in the **Performance** panel.

Setting	Description
Enable HP Velocity **NOTE:** Windows/Linux only	Enables HP Velocity.
Advanced Video Compression on Sender **NOTE:** Windows/Linux only	Enables Advanced Video Compression.
Image Quality	Sets the maximum image quality. When not using **Adaptive image quality**, RGS will maintain the image quality specified by this option. When selecting **Adaptive image quality**, RGS will use this option's setting as the target image quality when the updates-per-second value allows.
Enable adaptive image quality Increase text rendering quality Minimum image quality Target update rate	When **Enable adaptive image quality** is selected, RGS will begin to degrade the image quality down to the **Minimum image quality** setting (from 0–100) anytime the updates-per-second value falls below the **Target update rate** (from 0–30 updates per second). When **Increase text rendering quality** is selected, RGS uses different encoding for areas of the sender's display with few colors (areas with mostly text) to increase the quality when those areas are displayed on the receiver. In video-centric or bandwidth-constrained environments, disabling this option might improve RGS performance. **NOTE:** These options are disabled when Advanced Video Compression is enabled.
TIP: See Performance optimization on page 74 for more information about ways to optimize RGS performance.	

Gestures (Windows touch-capable devices only)

NOTE: These features are not supported on Windows 7.

You can use the gesture settings to map hotkey sequences to the gestures that are not used by RGS by default. For a list of the gestures that can be customized, see Using touch features (Windows touch-capable devices only) on page 44.

To map a hotkey sequence to a gesture:

1. Select the pencil icon in the row of the desired gesture.
2. Enter the key sequence.
3. Optionally select **Enable sticky gesture** if you want the gesture to mimic the continual press of the hotkey sequence until the same gesture is used to disable the sequence.
4. Select **Save**.

To un-map a hotkey sequence from a gesture:

- Select the **X** icon in the row of the desired gesture.

Audio

The following table describes the settings available in the **Audio** panel.

Setting	Description
Stream audio from Sender	Enables the sending of the audio stream to the receiver
Stereo	Enables stereo audio for the audio stream sent from the sender to the receiver. **NOTE:** Stereo audio requires more network bandwidth.
Quality	Sets the quality for the audio stream being transmitted by the sender. **NOTE:** Higher-quality audio requires more network bandwidth.
Volume	Controls the volume level on the receiver. **NOTE:** This option is for Windows and Linux only. On Mac OS, use the system volume control instead.

Network

The following table describes the settings available in the **Network** panel.

Setting	Description
Error	Sets the time in seconds that RGS Receiver will wait before ending the connection after failing to detect RGS Sender.
Warning	Sets the time in seconds that RGS Receiver will wait before displaying a warning dialog to the local user after failing to detect RGS Sender.
Dialog	Sets the time in seconds that RGS Receiver will wait for a response to a dialog being displayed on the sender (such as an authentication dialog). The request will be canceled if there is no response.
NOTE: Windows and Linux only Use a proxy server for your LAN Address Port	Enables the use of a proxy server with RGS. If you use a proxy server, configuring these settings is required to activate RGS Advanced Features such as Advanced Video Compression and HP Velocity. See RGS Advanced Features (Windows/Linux only) on page 32 for more information.

Hotkeys

The following table describes the settings available in the **Hotkeys** panel.

Setting	Description
Send First Key	Forces the first key of a local hotkey sequence to be transmitted to the sender. By default, if a key press matches the first key of a local Setup Mode sequence, all key events are held until RGS determines whether the next keys pressed are completing the sequence. If it is not a Setup Mode sequence, all key press events are then transmitted to the sender. However, commands for some remote applications might require that the first key press event arrive separately for them to function correctly. Enabling this option will ensure the immediate transmission of the first key press.

Setting	Description
	NOTE: In addition to transmitting the first key press to the sender, the key is also still processed by the receiver.
Send CTRL-ALT-END key sequence as CTRL-ALT-DEL	Enables the use of a Ctrl+Alt+End key sequence as a Ctrl+Alt+Delete sequence for the sender. This is useful when logging into the sender because, on some computers, the local operating system will interrupt the standard Ctrl+Alt+Delete key sequence and bring up local Windows security options instead. **TIP:** The Ctrl+Alt+Del sequence can also be sent using the RGS Receiver toolbar.
Key Repeat	Enables the processing of key repeats for when the Shift key is held down. By default, key repeat processing is disabled by RGS, but some remote applications might require this functionality. **NOTE:** If this option is enabled, the default Setup Mode hotkey sequence will not trigger unless it is typed fast enough.
Setup Mode Sequence	Sets the hotkey sequence for switching to Setup Mode. For more information, see Changing the Setup Mode hotkey sequence on page 18.

Logging

The following table describes the settings available in the **Logging** panel.

Setting	Description
Enable message logging	Enables logging.
Log file path	Specifies the path of the log file.
Log level	Determines the level of information that is logged. For example, if **WARN** is selected, the log file will contain information of the type **WARN** and also anything more serious than that type (**ERROR** and **FATAL**). To log all information generated by RGS Receiver, select **DEBUG**.
Max logfile size (KB)	Limits the size of the log file.
Clear Log	Clears the contents of the log file.
View Log	Displays the contents of the log file.
Restore Defaults	Resets all logging settings to the default values.

Statistics (Windows/Linux only)

The following table describes the information displayed in the **Statistics** panel.

Item	Description
Total network usage (Mbits/sec)	Displays the combined network traffic received from all connections.
Image updates per second	Displays the combined number of image updates per second received from all connections.
Image compression	Displays the compression ratio of the update stream.

Item	Description
	In a multi-connection environment, the value is from the RGS Receiver window that currently has the keyboard focus. If none of the RGS Receiver windows have focus, the value will be zero. In a single-connection environment, the value will be always available even if the RGS Receiver window does not have focus.
Current network loss with HP Velocity Current network loss without HP Velocity Peak network loss without HP Velocity	These items display statistics about HP Velocity when it is activated and in use.

RGS Receiver command-line options

The following table describes the valid command-line options for the Windows executable **rgreceiver.exe**, the Linux shell script **rgreceiver.sh**, and the Mac OS executable **HP RGS Receiver**.

NOTE: These commands must be issued from the RGS receiver installation directory.

Option	Description
`-config <file name>`	Specifies the configuration file to use for the instance of RGS Receiver being opened **NOTE:** See Setting property values in a configuration file on page 69 for more information.
`-directory <file name>`	Opens RGS Receiver in Directory Mode using the configuration from the specified directory file **NOTE:** See Directory Mode on page 52 for more information.
`-nosplash`	Disables the splash screen that displays by default when RGS Receiver is opened
`-{version|ver|v}`	Displays version information for RGS Receiver
`-{help|h|?}`	Displays the valid command line options
`-<property name>=<value>`	Sets the specified RGS Receiver property to the specified value **NOTE:** See Setting property values on the command line on page 69 for more information.

5 RGS Sender overview

RGS Sender overview (Windows)

RGS Sender for Windows is comprised of three processes:

- `rgsendersvc.exe`—Runs as a Windows service named `rgsender` that starts automatically (by default) when Windows starts and also starts the other two processes
- `rgsender.exe`—The main process for RGS Sender
- `rgsender_gui.exe`—The notification icon, which can be found in the Windows notification area

If Windows is already started, there is no additional action required to start RGS Sender (unless you have manually disabled automatic startup for the rgsender service).

The rgsender service must be active for the other two processes to be running, so if you want to completely disable RGS Sender, stop the rgsender service.

To stop, start, or restart the rgsender service:

▲ On the **Services** panel of Windows Task Manager, right-click **rgsender**, and then select the desired option.

RGS Sender overview (Linux)

RGS Sender for Linux is started by the `rge` X server extension when Linux starts. RGS Sender cannot be manually started, stopped, or restarted on Linux.

TIP: You can verify that the extension loaded and that RGS Sender started by viewing the X server log file `Xorg.0.log`.

The sender is automatically restarted in the event of a failure. On Linux, the X server will restart the sender if it is stopped.

RGS Sender command-line options (Windows)

Command-line options for RGS Sender can be applied to the rgsender service by modifying a registry key.

To apply command-line options to the rgsender service:

1. Open the **Registry Editor** tool in Windows.
2. Navigate to and select the following registry key:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\rgsender`
3. Add the desired command-line options to the **ImagePath** value.

   For example, to disallow collaboration, change the value data to the following:

   `C:\Program Files\HP\Remote Graphics Sender\rgsendersvc.exe -nocollab`

IMPORTANT: The folder path `C:\Program Files\HP\Remote Graphics Sender\rgsendersvc.exe -nocollab` applies to 64-bit versions of Windows. On 32-bit versions of Windows, the folder path is `C:\Program Files\Hewlett Packard\Remote Graphics Sender\rgsendersvc.exe -nocollab`.

4. Restart the rgsender service.

The following table describes the valid command-line options.

Command	Description
`-nocollab`	Disables collaboration
`-timeout <value>`	Specifies the timeout value, in milliseconds, after which RGS Sender disconnects an inactive connection
`-authtimeout <value>`	Specifies the timeout value, in milliseconds, that the collaboration authentication dialog is shown before the request is denied automatically
`-{version|ver|v}`	Displays version information for RGS Sender
`-{help|h|?}`	Displays the valid command line options
`-<property name>=<value>`	Sets the specified RGS Sender property to the specified value **NOTE:** See Setting property values on the command line on page 69 for more information.

RGS Sender command-line options (Linux)

Command-line options for RGS Sender can be applied to the shell script `rgsender.sh`. The following table describes the valid command-line options.

Command	Description
`-{version|ver|v}`	Displays version information for RGS Sender
`-{help|h|?}`	Displays the valid command line options

RGS Sender notification icon (Windows only)

The notification icon for RGS Sender is located in the Windows notification area and animates if there is an active RGS session. You can use the notification icon to do the following:

- Left-click the notification icon to open the HP RGS Collaborators window (see Collaboration on page 35 for more information).
- Right-click the notification icon for quick access to the **About** and **Disconnect** options.

RGS Sender event logging (Windows only)

In addition to standard logging, RGS Sender logs events. This information is output to a log named `HPRemote`, which is viewable in the Event Viewer tool in Windows, and can be useful in several different ways:

- Troubleshooting—Event log information can help diagnose RGS connection issues.
- Remote application termination—See Creating an agent for remote application termination (Windows only) on page 84 for more information.
- Other automated actions—The basic principle behind using the event log for remote application termination can be used to create an agent that performs other automated actions.

Filtering access to RGS Senders

RGS connections may be restricted by configuring the Sender ipfilter.txt file to specify the IP addresses, subnet masks, and the fully qualified computer and/or domain names of the receiver systems that are allowed to make a connection. If a receiver does not match one of the filters, the connection will be denied.

The file ipfilter.txt is located in the installation folder on Windows and in `/etc/opt/hpremote/rgsender` on Linux.

Connection filtering based on hostname and domain name requires DNS to be configured to allow reverse DNS lookup. For example, if the receiver IP address is 10.13.19.1, the command `nslookup 10.13.19.1` will return a hostname and domain name. RGS will similarly use reverse look up for hostname and domain name filtering.

As an example, adding the following lines to the ipfilter.txt file on a sender system will only allow connections from receiver systems computername1 and computername2:

```
HOSTNAME:computername1.networkdomain.name

HOSTNAME:computername2.networkdomain.name
```

Filtering on the domain name compares the text after the first period in the domain name. For example, if DNS reverse lookup returns "`james.auth.corp.net`, the filter will compare `auth.corp.net` against domain name entries in the ipfilter.txt file to determine whether or not to allow connections from the receiver.

Filter types may be combined in one ipfilter.txt file. Once a match is made with a filter specified in the ipfilter.txt file, RGS will stop processing the file and allow the connection to be made. By default, the ipfilter.txt file does not filter out any connections. If the receiver connects to the sender over VPN or through another process that causes the IP address to be translated, RGS may prevent connections that users expect to work. For additional information, review the ipfilter.txt file on a system where the RGS Sender has been installed.

6 Configuring certificates

By default, HP RGS Receiver attempts to verify the identity of the sender by verifying the sender public-key infrastructure (PKI) certificate before a connection is made. By default, HP RGS Sender creates a self-signed certificate, but can be configured to use a certificate signed by a Certificate Authority (CA).

Sender verification

When the receiver attempts to connect to the sender, a warning is displayed if the certificate verification fails. The certificate verification can fail for the following reasons:

- The sender presented a self-signed certificate. This user can compare the certificate fingerprint to the fingerprint available in the Certificate panel of the RGS Sender Configuration tool. See End-user verification of a sender certificate on page 27.

NOTE: This is the most common failure, because RGS Sender generates a self-signed certificate by default.

- The sender address typed into the receiver window does not match the hostname on the sender certificate. This failure occurs if the user connects with an IP address instead of using the sender hostname. The user must be sure that the IP address resolves to the hostname on the sender certificate before connecting to that sender. Alternatively, the user can reconnect using the hostname on the sender certificate.
- The certificate is expired. If self-signed certificates are used, this error does not occur because a new self-signed certificate is generated when the current certificate approaches expiration.

Certificate Verification Error Policy

The Certificate Verification Error Policy determines how the receiver behaves if the identity of the sender cannot be verified. This setting can be configured in the RGS Receiver Configuration tool (see Using the RGS Receiver Configuration tool on page 55).

If the verification fails, the RGS Receiver can be configured to do one of the following:

- **Accept**: Certificate errors are ignored, and the receiver connects to the sender.
- **Prompt to accept** (default): A warning prompt is displayed, and the user can choose to connect despite the failure. An SHA-256 fingerprint of the sender certificate is displayed with the error message. To verify the identity of the sender, compare the fingerprint displayed with the error message to the fingerprint presented in the Certificate panel of the RGS Sender Configuration tool. An administrator can provide the fingerprint to the user if they do not have access to the RGS Sender Configuration tool.
- **Deny**: The receiver does not connect to the sender.

End-user verification of a sender certificate

If the receiver cannot verify the sender certificate and the Certificate Verification Error Policy is configured to prompt to accept, the user can verify that the fingerprint of the certificate displayed in the verification error message matches the fingerprint displayed in the RGS Sender Configuration tool on the sender. An administrator can provide the fingerprint from the RGS Sender Configuration tool, if necessary.

Using a certificate signed by a CA

For ease in deployment, HP RGS creates a self-signed certificate for the sender. For greater security, HP RGS can be configured to use a certificate signed by a CA.

To use a certificate signed by a CA, the CA certificate and key files must be present on the sender and receiver system.

Configuring the sender to use a certificate signed by a CA

For more information about setting RGS properties manually, see Setting RGS properties manually on page 68.

Modifying the sender Ice configuration file

1. Open the `config` file. On Windows, the file is located in the RGS Sender installation directory. On Linux, the file is located in `/etc/opt/hpremote/rgsender`.

NOTE: If HP Velocity is enabled, the following settings must be duplicated with `<IceSSL>` replaced by `<IceLive>`.

2. Add the following settings to this file:

   - `IceSSL.DefaultDir=<certificate and key files directory>`
   - `IceSSL.CertFile=<program certificate file>`

     This file might contain the private key, encoded using the PEM format, in addition to the program certificate. This certificate must be signed by the CA certificate identified by the IceSSL.CertAuthFile setting.
   - `IceSSL.KeyFile=<file containing the private key associated with the certificate identified by the IceSSL.CertFile setting>`

     The private key must be encoded using the PEM format.
   - `IceSSL.Password=<password necessary to decrypt the private key>`

     NOTE: Using a plain-text password in a configuration file is a security risk.

3. You can also configure the sender to verify a certificate that identifies the receiver. Add the following setting to enable the sender to verify the receiver certificate:

NOTE: By default, HP RGS does not create or use a receiver certificate.

```
IceSSL.VerifyPeer={0 | 1 | 2}
```

   - 0: Do not verify the receiver certificate.
   - 1: Verify the receiver certificate if it is provided, but do not require a receiver certificate.
   - 2: Require a receiver certificate and verify it.

4. If you configure the sender to require a receiver certificate, you must make sure that the sender can access the same CA root certificate that is used to sign the receiver certificate. Add the following setting:

   `IceSSL.CertAuthFile=<file containing the certificate of a trusted CA>`

   The file must be encoded using the PEM format.

Modifying the sender configuration file

1. Open the `rgsenderconfig` file. On Windows, the file is located in the RGS Receiver installation directory. On Linux, the file is located in `/etc/opt/hpremote/rgreceiver`.
2. Remove the comment from the following line and change the value to 0:

   ```
   Rgsender.Network.GenerateCertificate=0
   ```

After this procedure is complete, HP RGS does not generate new certificates or use a self-signed certificate for sender verification.

You must delete any existing RGS certificates from the file system. See Removing a certificate on page 30.

Configuring the receiver to use a certificate signed by a CA

For more information about setting RGS properties manually, see Setting RGS properties manually on page 68.

Modifying the receiver Ice configuration file

1. Open the `config` file. On Windows, the file is located in the RGS Receiver or RGS Sender installation directory. On Linux, the file is located in `/etc/opt/hpremote/rgreceiver` or `/etc/opt/hpremote/rgsender`. On Mac OS, this file is named `iceconfig` and is located in `/Library/Application Support/HP/rgreceiver`.

   NOTE: If HP Velocity is enabled, the following settings must be duplicated with `<IceSSL>` replaced by `<IceLive>`.

2. Add the following settings to this file:

   - `IceSSL.DefaultDir=<certificate and key files directory>`
   - `IceSSL.CertFile=<program certificate file>`

     This file might contain the private key, encoded using the PEM format, in addition to the program certificate. This certificate must be signed by the CA certificate identified by the IceSSL.CertAuthFile setting.

   - `IceSSL.KeyFile=<file containing the private key associated with the certificate identified by the IceSSL.CertFile setting>`

     The private key must be encoded using the PEM format.

   - `IceSSL.Password=<password necessary to decrypt the private key>`

     NOTE: Using a plain-text password in a configuration file is a security risk.

3. If you provide a certificate signed by a CA to verify the sender, the receiver must verify that certificate when a connection is attempted. Add the following setting to enable the receiver to verify the sender certificate:

   ```
   IceSSL.VerifyPeer={0 | 1}
   ```

- 0: Do not verify the sender certificate.
- 1: Require a sender certificate and verify it.

4. If you configure a certificate signed by a CA for the sender, you must make sure that the receiver can access the same CA root certificate that is used to sign the sender certificate. Add the following setting:

   `IceSSL.CertAuthFile=<file containing the certificate of a trusted CA>`

   The file must be encoded using the PEM format.

Modifying the receiver configuration file

1. Open the `rgreceiverconfig` file. On Windows, the file is located in the RGS Receiver or RGS Receiver installation directory. On Linux, the file is located in `/etc/opt/hpremote/rgreceiver` or `/etc/opt/hpremote/rgreceiver`. On Mac OS, this file is named `iceconfig` and is located in `/Library/Application Support/HP/rgreceiver`.
2. Remove the comment from the following line and change the value to 0:

   `Rgreceiver.Network.VerifyCertificate=0`

After this procedure is complete, HP RGS does not use the default self-signed certificate.

Removing a certificate

If certificate verification fails, the user can accept the certificate and connect when prompted.

If the **Don't ask about this certificate again** check box is selected, RGS Receiver stores the end-user verification of the hostname and certificate. If a user tries to reconnect to the same hostname and the same certificate is presented by the sender, RGS Receiver automatically accepts or rejects the certificate based on the previous choice. This information is stored locally on the receiver. To stop automatically accepting or rejecting the certificate, you must remove the certificate from where it is stored.

Windows

1. Open the Registry Editor and find the folder **HKEY_CURRENT_USER/Software/HP/KnownSenders**.
2. To clear all certificates, delete the **KnownSenders** folder. To remove a specific certificate, in the **KnownSenders** folder, delete the subfolder that matches the hostname of the certificate.

Linux

1. Go to the file named **$HOME/.config/HP/KnownSenders.conf**.
2. To clear all certificates, delete the **KnownSenders.conf** file. To remove a specific certificate, open the **KnownSenders.conf** file, and then delete the entry that starts with the hostname of the certificate.

macOS

1. Go to the file named **$HOME/Library/Preferences/com.hp.KnownSenders.plist**.
2. To clear all certificates, delete the **KnownSenders.plist** file.
3. Restart the computer.

Troubleshooting the certificate configuration

To diagnose network or certificate configuration issues, set the Log level to `DEBUG` and set Ice properties in the sender or receiver Ice configuration files.

1. Open the `config` file. On Windows, the file is located in the RGS Receiver or RGS Sender installation directory. On Linux, the file is located in `/etc/opt/hpremote/rgreceiver` or `/etc/opt/hpremote/rgsender`. On Mac OS, this file is named `iceconfig` and is located in `/Library/Application Support/HP/rgreceiver`.
2. Add the following settings:
   - `IceSSL.Trace.Security={0 | 1}`
     - 0: Security tracing is disabled.
     - 1: Security tracing is enabled.
   - `Ice.Trace.Network={0 | 1 | 2 | 3}`
     - 0: Network tracing is disabled.
     - 1: Network tracing is enabled during connection establishment and closure.
     - 2: Network tracing is enabled during connection establishment and closure, with more detail logged.
     - 3: Network tracing is enabled during connection establishment and closure, with more detail and data transfer logged.
   - `Ice.Trace.Protocol={0 | 1}`
     - 0: Protocol message tracing is disabled.
     - 1: Protocol message tracing is enabled.

7 Using RGS features

This chapter discusses the following RGS features and topics:

RGS Advanced Features (Windows/Linux only)

This section discusses RGS Advanced Features:

IMPORTANT: On Windows-based receivers, RGS Advanced Features require a one-time activation that occurs when the first RGS connection is established, and this activation requires Internet access. If using a proxy server for your LAN, make sure your proxy settings are configured correctly (see Network on page 21). Activation does not work with a proxy auto-configuration (PAC) file or with the Web Proxy Auto-Discovery (WPAD) protocol.

The activation process uses anonymous access, so you must configure your proxy server to allow anonymous access for the IP address activation.rgs.ext.hp.com (15.0.92.201).

For thin clients with a write filter, HP recommends disabling the write filter prior to the first RGS connection so that the files created during activation are permanently written to the hard drive. The write filter should be re-enabled afterwards.

NOTE: The old activation IP address, 192.151.30.9, has been decommissioned.

Advanced Video Compression (Windows/Linux only)

Advanced Video Compression is an RGS Advanced Feature that enables the use of a modern video codec to greatly reduce the network bandwidth needed for high-quality video streams.

Advanced Video Compression is ideal for video or 3D applications in textured mode. It is not recommended for use with wireframes or fine lines, as screen artifacts might appear when in motion. Advanced Video Compression can be enabled in the **Performance** panel of the RGS Receiver settings.

IMPORTANT: System requirements for Advanced Video Compression might be higher than the base RGS system requirements, all of which are described in the *QuickSpecs* (see Finding more information on page 4).

NOTICE: The performance of Advanced Video Compression for resolutions larger than full HD (1920x1080) varies depending on the content.

Advanced Video Compression does not currently support 4K (Ultra HD) resolutions.

HP Velocity (Windows/Linux only)

HP Velocity is an RGS Advanced Feature that improves performance within a wide area network (WAN).

HP Velocity status is displayed on the RGS Receiver toolbar:

- Blue—HP Velocity is monitoring network loss and is ready to be used.
- Green—HP Velocity is actively working to improve network conditions.
- Grey—HP Velocity has not been activated.

NOTE: HP Velocity might increase network bandwidth usage.

Authentication

Authentication methods

There are three different authentication methods available for an RGS connection:

- **Standard authentication**—supported for RGS Sender on Windows and Linux.
- **Easy Login**—supported for RGS Sender on Windows and Linux.
- **Single Sign-on**—supported for RGS Sender on Windows only.

On Windows, the authentication method is selected during installation of RGS Sender and can be changed later using the RGS Sender Configuration tool (see Using the RGS Sender Configuration tool on page 62). Smart card redirection is supported for standard authentication and Easy Login (see Using smart card redirection on page 34).

On Linux, Easy Login can be enabled during installation and disabled using an RGS Sender property (see Other global properties on page 69).

Standard authentication

Standard authentication is the process by which a local user attempts to connect to a sender that has neither Single Sign-on nor Easy Login enabled.

In normal operation, users are required to authenticate twice when establishing an RGS connection from a receiver to a sender. The two steps are as follows:

1. The first authentication step is from RGS Receiver to RGS Sender. The dialog for this authentication step is generated and displayed by RGS Receiver on the receiver.
2. The second authentication step is when logging in to or unlocking the sender desktop session. The login or unlock dialog is generated by the sender and is displayed in the RGS Receiver window on the receiver.

NOTE: If another user is already logged in to the sender, the second authentication step does not take place. Instead, the currently logged-in user receives an authorization prompt to allow or deny the new user access to join the existing desktop session (see Collaboration on page 35 for more information).

When a Windows Receiver and Windows Sender are in the same workgroup and the same username and password are used on both systems, the first authentication step will be accomplished using a secure token.

The user will not be required to enter a password. To connect as a different user, enable the prompt for username and password setting (for more information, see RGS Receiver settings on page 19.)

Using Kerberos Authentication

When a Windows or Linux Sender is connected to a Windows domain, the first authentication step can be accomplished using Kerberos when using a Windows Receiver connected to the same domain. The user will not be required to enter a password. Kerberos authentication to a Linux Sender requires a hostname to be entered as the Sender identifier. Kerberos authentication to a Linux Sender will not work with an IP address. To connect as a different user, enable the Prompt for username and password setting (see RGS Receiver settings).

Easy Login

If you use Easy Login, the first authentication step (RGS authentication) is skipped.

NOTE: At the login screen, you might see an additional user account named HP RGS ELO. Do not use this account to log in. Use your normal user account.

NOTE: There are several issues that can prevent an Easy Login authentication. The Diagnostics panel of the RGS Sender Configuration tool can help troubleshoot these issues. See Using the RGS Sender Configuration tool on page 62 for more details.

Single Sign-on

With Single Sign-on, the second (System) authentication is skipped. When connecting, the user will be prompted for user name a password. Upon verification, the user will be connected directly to the sender's desktop.

NOTE: Single Sign-on does not support smart card or ActivKey authentication.

NOTE: If you lock the desktop, you might see an additional user account named HP RGS SSO. Do not use this account to log in. Use your normal user account.

Using smart card redirection

NOTE: Smart card redirection is supported on Windows-based receivers and Windows-based and Linux-based senders only.

On Windows-based and ThinPro-based receivers, smart cards can be remoted using Remote USB. See Remote USB (Windows/ThinPro only) on page 49.

When smart card redirection is enabled, both the receiver and sender can access the same smart card that physically exists on the receiver-side only. This means that you can unlock the receiver desktop using the smart card, connect to the sender, and then use the same smart card with the sender desktop.

NOTE: Smart card redirection can be used with standard authentication or Easy Login only. It cannot be used with Single Sign-on.

To use smart card redirection:

1. Enable smart card redirection during the installation of both RGS Receiver and RGS Sender (see Installation on page 6).
2. Install the vendor driver for the smart card reader on the receiver.
3. Install the vendor driver for the smart card on both the receiver and sender.
4. If Remote USB is enabled, see Configuring Remote USB for smart card redirection on page 35.

NOTE: If the smart card removal policy has been set on the receiver, the receiver desktop is locked if the smart card is removed. If the smart card removal policy has been set on the sender, the sender desktop is locked when the RGS connection is ended or when the smart card is removed.

Configuring Remote USB for smart card redirection

Smart card readers typically connect to the system via USB, so you must prevent the smart card reader from being remoted by the Remote USB feature to use the smart card redirection feature.

To prevent the smart card reader from being remoted:

- If you used the default Remote USB installation option **USB devices are Local/Remote** when installing RGS Receiver, connect the smart card reader to the receiver before starting an RGS session, and do not disconnect the smart card reader during the session.

  – or –

  Set the remoting behavior of the smart card reader to `local` (see Configuring the remoting behavior of individual USB devices (Windows only) on page 49).

Limitations

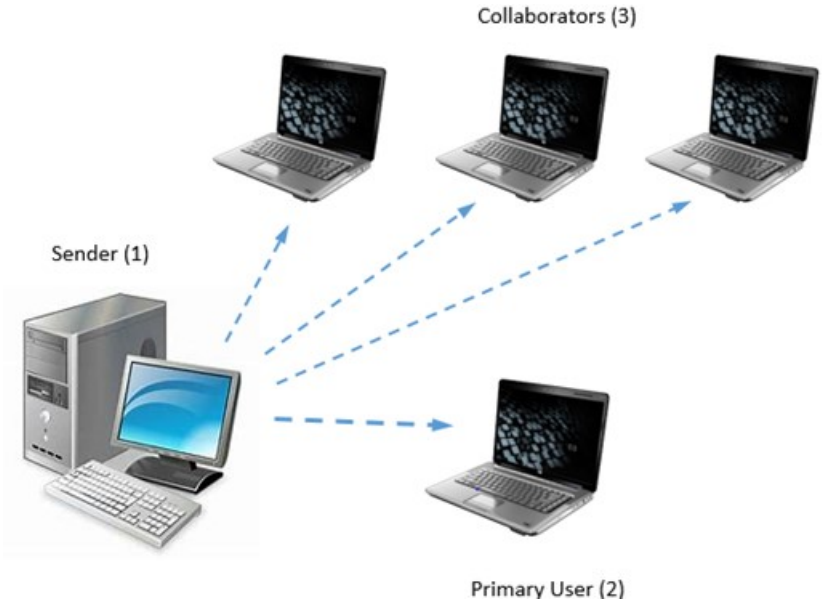
Consider the following limitations when using smart card redirection:

- Smart card redirection is limited to the primary user.
- Smart card redirection is limited to the first smart card detected by the receiver. If there are two or more smart cards, including virtual smart cards, enabled on the receiver, smart card redirection might not be predictable.
- Disconnecting and reconnecting a smart card reader during an RGS session causes the smart card reader to be remoted via Remote USB. In this situation, the receiver no longer sees the smart card reader or smart card. If the smart card removal policy is enabled, the receiver desktop locks.

Collaboration

RGS enables the primary user to share their desktop session with several users simultaneously. This feature can be used in a variety of collaborative scenarios including classroom instruction, design reviews, and technical support.

A collaboration session is created when one or more users are authorized by the primary user to connect to the primary user's desktop session. This allows all users to view and interact with the primary user's desktop.



Item	Description
1	**Sender**—Hosts RGS Sender, which transmits the sender desktop session to RGS Receiver on each receiver.
2	**Primary user**—The primary user is logged into the sender and has control over the session. The primary user authorizes who can join and actively participate in the session.
3	**Collaborators**—Collaborators, once authorized, can view the sender's desktop and make changes as permitted by the primary user.
NOTE: The image above is just an example of one possible configuration. Any combination of hardware supported by RGS Receiver can be used by the primary user and collaborators.	

The user currently controlling the mouse and keyboard is called the floor owner. Only one user, the floor owner, can interact with the desktop at a time. To transition the floor owner, the current floor owner must cease using the keyboard or mouse for 0.5 seconds. If another user uses the mouse or keyboard while the current floor owner is inactive after this period, floor ownership transfers to the new user.

TIP: The delay's value of 0.5 seconds can be changed using the RGS Sender Configuration tool on Windows (see Using the RGS Sender Configuration tool on page 62 for more information).

Click the RGS Sender notification icon in the Windows notification area to open the HP RGS Collaborators window, which allows you to do the following:

- View who the primary user and collaborators are
- Enable or disable collaborator input for individual collaborators or all collaborators at once by clicking the appropriate mouse pointer icon

  TIP: Individual collaborator input can also be enabled when authorizing the collaborator to connect by selecting **Enable Input for this user** in the authorization dialog.

- Disconnect individual collaborators or all collaborators at once by clicking the appropriate **X** icon

Note the following additional information about collaboration:

- Collaboration requires unique login credentials on the sender for each participant.
- If guest accounts are enabled in Windows, a collaborator can join by using "Guest" as the username and leaving the password blank. However, only one guest collaborator can join at a time. If another guest collaborator joins, the first one will be kicked out of the session.
- On Windows, if the primary user disconnects, the desktop is locked, but all collaborators will remain connected. On Linux, if the primary user disconnects, the desktop is locked, and all collaborators are disconnected.
- The update rate of all collaborators is limited by the lowest update rate of any one collaborator. Collaborators with low update rates can use the **Performance** panel in the RGS Receiver settings to improve their update rate, which will improve the experience for all collaborators.
- To collaborate in a session that has Advanced Video Compression or HP Velocity enabled, each collaborator must have the same Advanced Video Compression and HP Velocity settings on their RGS Receiver, or the connection will be refused.

Display

Display resolution and layout matching

Many RGS scenarios require that the resolution and display layout transmitted by the sender match the display configuration on the receiver. The following sections describe how to configure the sender if RGS is unable to match the resolution and display layout by default.

Multi-monitor overview

During an RGS connection, RGS transmits the sender's entire desktop area to the receiver. If the sender has more monitors or higher-resolution monitors than the receiver, scroll bars appear in the RGS Receiver window so you can view the sender's entire desktop area. If the sender has multiple monitors, it might be beneficial to use the options described in Matching display resolution and layout (Windows-based sender) on page 38 or Matching display resolution and layout (Linux-based sender) on page 41.

Multiple monitors on the receiver are also useful for a many-to-one connection. If the receiver is connected to two senders, each sender frame buffer can be displayed on its own monitor if the receiver has two monitors (see the following image).

NOTE: On Mac OS, if the OS setting **Displays have separate Spaces** is not selected, an RGS Receiver window can span multiple sender monitors. If the RGS Receiver has multiple monitors, one monitor displays full-screen mode and the other monitors display nothing.

Matching display resolution and layout (Windows-based sender)

If the **Match Receiver display resolution** and **Match Receiver display layout** options are enabled (see Connection on page 19), RGS will automatically try to set the resolution and display layout of the sender to match that of the receiver. However, there are some scenarios where some manual configurations might be required to achieve the desired result, such as when the sender has no monitor attached.

When attempting to match the resolution and display layout, the most important thing to remember is that the sender must support the same resolution and layout as the receiver.

To avoid possible resolution-matching problems, test the resolution in advance using the following procedure:

1. Establish an RGS connection with the **Match Receiver display resolution** setting disabled.
2. When the connection is established, manually attempt to set the sender's resolution to match the receiver's resolution.

   If you can match the resolution, then RGS can also do it for you automatically.

   If you cannot match the resolution, see the additional information in this section.

Depending on the NVIDIA GPU and driver you are using, you might need to perform additional configurations on the sender. The required configurations can vary depending on the hardware, as described below:

- **Blade workstation**—If the sender is a blade workstation, then its NVIDIA driver exposes all display outputs to the operating system as if they have monitors attached. The resolutions provided by the NVIDIA driver cover a broad range of settings and should meet most user needs. If the desired resolution is not available, see Adding custom resolutions on page 41.
- **Virtual workstation**—If the sender is a virtual workstation with a hypervisor, the NVIDIA driver presents a single display to the operating system. The resolutions provided by the NVIDIA driver cover a broad range of settings and should meet most user needs. If you are using a single display at the receiver, no further action is required. If you need to configure additional resolutions and/or make additional displays available, see NVIDIA resolution-matching (Windows-based senders with NVIDIA graphics only) on page 39.
- **Traditional workstation**—If the sender is a traditional workstation, then its NVIDIA driver expects to find a display attached to one or more outputs. When it does, it queries the EDID (Extended Display Information Data) information from the display for its supported resolutions and makes the display and resolutions available to the operating system. On Windows 7, if there is not a display attached, the NVIDIA driver reverts to a single VGA output with basic display resolutions. On Windows 10, resolution matching is enabled by default and appropriate EDID files are created automatically and used for the duration of the RGS connection. The property `AllowNvidiaResolutionMatching` is enabled by default on Windows 8.1 and Windows 10 but must be enabled on Windows 7. For servers, rack-mounted workstations, and non-NVIDIA graphics, use an EDID emulator device or create an EDID file to allow resolution matching. See Creating and applying an EDID file on page 40 and Matching display resolution and layout (Windows-based sender) on page 38 for more information. Alternatively, RGS will load EDID files automatically. See NVIDIA resolution-matching (Windows-based senders with NVIDIA graphics only) on page 39.
- **Headless workstation**—When connecting to a workstation that has no physical displays connected, RGS requires that an EDID be loaded first. RGS can be configured to automatically load a custom EDID which supports most resolutions up to 4k. To enable automatic EDID loading on headless workstations with Nvidia GPU:

1. In `rgsenderconfig`, set `Rgsender.Compatibility.Displays.ForceEdidOnHeadless` to `1`.
2. Restart the RGS Sender service.

   – or –

   Restart the sender.

NOTE: This property will only apply an EDID to a system if it is headless when the RGS Sender service starts. If the workstation is not headless when the RGS Sender service starts, then no EDID will be loaded.

NVIDIA resolution-matching (Windows-based senders with NVIDIA graphics only)

NVIDIA resolution-matching provides the following additional features over the default resolution-matching method:

- Automatic loading and unloading of EDID files to allow a sender with fewer monitors than the receiver to "fake" displays

NOTE: This is especially useful for virtual workstations where the hypervisor typically provides only one display.

- Rotated monitors on virtualized systems (specifically, Citrix and VMware virtual machines)
- Automatic application of custom resolutions on virtualized systems

NOTE: If NVIDIA resolution-matching fails to match the requested resolution/resolutions, RGS attempts the default resolution-matching method.

To enable NVIDIA resolution-matching:

1. In `rgsenderconfig`, set `Rgsender.Compatibility.Displays.AllowNvidiaResolutionMatching` to `1`.
2. Restart the RGS Sender service.

   – or –

   Restart the sender.

NOTE: For more information about setting the property, see Setting property values in a configuration file on page 69.

EDID files

Extended Display Identification Data (EDID) data is a standardized means for a display to communicate its capabilities, such as resolution and video characteristics, to a source device. This allows the source device (PC, graphics card) to generate the necessary graphics that match the needs of the system. EDIDs provide a powerful and convenient method for RGS to manage complex customer requirements.

Creating and applying an EDID file

There are software tools available to create and edit an EDID file, but the easiest method is to use an existing monitor from the receiver, temporarily attaching it to the sender and using the NVIDIA Control Panel to export the EDID file. If you have several different displays that you use on the receiver, HP recommends that you capture the EDID information of the monitor that has the highest display resolution. This will address all other resolution needs.

Creating the EDID file:

1. Attach a monitor to the sender or the receiver.

   NOTE: This is not possible with blade workstations that use MXM graphics.

2. Open the NVIDIA Control Panel and click **View system topology**.
3. Find and select **EDID** for the connected monitor.
4. The **Manage EDID** dialog box opens. Select the link labeled **Monitor**.
5. Select **Export EDID** and save the output to a file. This file can be imported on the sender system.

Importing the EDID file:

1. On the sender system, under **View system topology** select **EDID** on the connector port you want to use.
2. In the **Manage EDID** dialogue box , select the **Load** tab and then **Browse** and select the EDID file you created.

3. Under **Connector** select the port (DVI, DisplayPort) that you want to use for the EDID monitor.
4. Select **Load**. The EDID information is applied.
5. Select **OK** and then select cancel to close the **Manage EDID** dialogue box.

NOTE: If you apply the file to multiple DisplayPort connectors, RGS will be able to support multi-display configurations.

Under the View System Topology screen of the NVIDIA Control Panel, you should now be able to see that an EDID file has been applied to the DisplayPort connectors that you selected. RGS should now be able to match the desired display resolution and display layout.

Adding custom resolutions

The following steps describe how to add a resolution that is not already supported by the NVIDIA driver:

1. Open the NVIDIA Control Panel and click **Change Resolution**.
2. Click **Customize**.

NOTE: The first time you do this you might see a warning—accept it.

3. Enable the **Enable resolutions not exposed by the display** checkbox, and then click **Create Custom Resolution**.
4. Add the desired custom resolutions.

Matching display resolution and layout (Linux-based sender)

If the **Match Receiver display resolution** option is enabled (see Connection on page 19), RGS automatically tries to set the resolution and display layout of the sender to match that of the receiver. Because RGS supports a single remote X screen only, it tries to set the resolution of the sender to the combined resolution of all displays attached to the receiver.

For example, if the receiver has dual-monitors set at a 1280x1024 resolution, RGS asks the sender to set its resolution to 2560x1024. If the resolution is not supported, RGS instead uses the preferred resolution of the sender from the file `xorg.conf`.

The easiest way to check if the sender can match the receiver resolution is to attempt to set the resolution on the sender manually. If you can set the resolution manually, then RGS can do it for you automatically. If you cannot set the resolution manually, you must modify the file `xorg.conf` to support the additional required resolutions.

To test if you can match the resolution manually, establish an RGS connection with the following connection settings **disabled**:

- **Match Receiver display resolution**
- **Match Receiver display layout**

NOTE: This setting should always be disabled when connecting to RGS Sender on Linux.

Once you establish an RGS session, open an X terminal window and use the `xrandr` tool to list all the currently supported resolutions for the X server. The tool can also be used to configure the X server display settings, including size and orientation.

Previous releases of the X Window System used the file `/etc/X11/xorg.conf` to store initial setup information. When a change occurred with the monitor or video card, you were required to edit the file manually. Although current releases of Red Hat® Enterprise Linux® (RHEL) have largely automated the process, you still need to edit the file to support configurations where no monitor is attached or where you

want the X server to simulate that it has a different monitor attached to it with different resolution capabilities. Similarly, this is also the case when you want to match the receiver's resolution in an RGS session where the X server cannot determine the capabilities of the receiver's monitors.

NOTE: Some window managers (such as GNOME) allow you to modify display preferences, which can sometimes result in the creation of the following file:

```
$HOME/.config/monitors.xml
```

When you log in to the system and a window manager starts a session, it uses information from this file to set the current desktop resolution. This can reverse the resolution matching performed by RGS and cause the desktop to be set to an undesired resolution.

For example, if you set the desktop resolution of the sender to 1024x768 using a window manager, that resolution is stored in `monitors.xml`. If an RGS connection is then established with display resolution matching enabled on a receiver with a resolution of 1920x1200, the sender display resolution changes to 1920x1200 and then to 1024x768. There is no notification that the resolution match request failed (because it did not).

To avoid this behavior, avoid setting the resolution using window manager controls. It is safe to delete `monitors.xml` to restore display resolution matching functionality. See the documentation for your operating system or window manager for more information about where and how it manages display settings.

Configuring the X server

The X server can be configured in several different ways. This section describes the suggested methods for two different scenarios.

Scenario 1: All receivers have the same configuration

If all receivers have the same configuration, then using the **Virtual** entry under the **Screen** section of the file `xorg.conf` is the easiest method.

For example, if all receivers have four monitors configured at 1280x1024 each, configure the X server to run at a resolution of 5120x1024 by making the following additions to the file `xorg.conf`.

Add the following under the **Device** section:

```
Option "UseDisplayDevice" "none"

Option "UseEDID" "false"
```

Add the following under the **Screen** section:

```
SubSection "Display"

Virtual 5120 1024

Depth 24

EndSubSection
```

Now the X server is configured to have a single screen running at a resolution of 5120x1024, which covers all four of the receiver's monitors. You can use this method to support a very large virtual display limited only by frame buffer memory.

Scenario 2: Some receivers have different configurations

In the more likely scenario where you need to support many different display resolution and monitor configurations, you can use the NVIDIA TwinView® mode to match the resolutions. TwinView mode is where two display devices (digital flat panels, CRTs) can display the contents of a single X screen in different

configurations. This method for using multiple monitors has the following distinct advantages over other techniques such as Xinerama (which is not supported by RGS):

- It uses only a single X screen. The NVIDIA driver conceals all information about multiple display devices from the X server. As far as the X server is concerned, there is only one screen.
- Both display devices share one frame buffer. Thus, all the capabilities present on a single display (for example, accelerated OpenGL) are available with TwinView.
- There is no additional overhead when emulating a single desktop.

For example, if all receivers have either single or dual monitors, you should configure the X server to think it has the monitor with the highest resolution used on any of the receivers. This allows the X server to support as many display resolutions as possible. You do this by capturing the EDID information from the monitor (see Creating an EDID file on page 43) and making the following additions to the file `xorg.conf`.

The below example uses dual HP LP2465 displays. The following text is added under the **Device** section of `xorg.conf`:

```
Option "ConnectedMonitor" "DFP-0,DFP-1"

Option "CustomEDID" "DFP-0:/etc/X11/lp2465edid.bin;DFP-1:/etc/X11/
lp2465edid.bin"
```

Now that the X server thinks it has dual HP LP2465 displays attached to it, enable TwinView support and configure the supported single and dual display layouts under the **Screen** section:

```
Option "TwinView" "True"

Option "MetaModes" "DFP-0: 1920x1200 +0+0, DFP-1: 1920x1200 +1920+0;
DFP-0: 1920x1200 +0+0, DFP-1:NULL"

SubSection "Display"

Depth 24

EndSubSection
```

NOTE: In the above example, `NULL` represents a single display configuration. This line will cover both dual and single display configurations.

To support additional resolutions, define additional combinations on the same line:

```
Option "MetaModes" "DFP-0: 1920x1200 +0+0, DFP-1: 1920x1200 +1920+0;
DFP-0: 1920x1200 +0+0, DFP-1:NULL; DFP-0: 1680x1050 +0+0, DFP-1:
1680x1050 +1680+0; DFP-0: 1680x1050 +0+0, DFP-1:NULL; DFP-0: 1600x1200
+0+0, DFP-1: 1600x1200 +1200+0; DFP-0: 1600x1200 +0+0, DFP-1:NULL; DFP-0:
1400x1050 +0+0, DFP-1: 1400x1050 +1400+0; DFP-0: 1400x1050 +0+0,
DFP-1:NULL; DFP-0: 1280x1024 +0+0, DFP-1: 1280x1024 +1280+0; DFP-0:
1280x1024 +0+0, DFP-1:NULL"
```

NOTE: The EDID file provided to the X server must still support the listed resolutions.

Creating an EDID file

To create an EDID file:

▲ Use the NVIDIA tool `nvidia-settings` to create an EDID file in either .bin or .txt format.

IMPORTANT: A physical display must be attached before you can use the NVIDIA tool.

TIP: You can also use the method for Windows described in Creating and applying an EDID file on page 40 and copy the EDID file to the Linux system.

Sender screen blanking

RGS Sender, by default, blanks the screen of the sender monitor (if one is connected) so that the desktop session is not visible at the sender side.

IMPORTANT: Screen blanking is not supported if the sender is a virtual machine.

The default behavior is that the sender screen, with the exception of the cursor, blanks to black when you start an RGS session. The sender screen un-blanks when the RGS session is ended.

See the following additional information about RGS Sender screen blanking:

- There might be a delay of up to two seconds after an RGS session is started before the sender screen is blanked.
- If, for any reason, RGS Sender is unable to blank the sender screen, a warning dialog is displayed on the receiver.
- If the sender is an HP workstation, then most input from any physically-connected keyboards or mice at the sender side is blocked while screen blanking is occurring. When RGS Sender receives keyboard or mouse input from RGS Receiver, the sender monitor enters a power-saving mode, which blanks the cursor as a result.
- The Ctrl+Alt+Del key sequence is not blocked by RGS Sender for any physically connected keyboards at the sender side. When this sequence is input into the sender using a physically-connected keyboard, the Windows logon screen of the remote desktop is displayed at the receiver side in the RGS Receiver window. The sender monitor remains blank while this occurs, but the monitor will exit its power-saving mode, and sender keyboard input is not blocked until the logon screen is closed.
- Screen blanking is supported for a Linux-based sender using multiple monitors only if NVIDIA TwinView is in use.
- Screen blanking can be disabled using the RGS Sender Configuration tool (see Using the RGS Sender Configuration tool on page 62).

Input

Using touch features (Windows touch-capable devices only)

NOTE: RGS does not support touch features for Windows 7.

RGS supports the following touch features:

- **Gestures**—See the table below for more information.
- **Virtual keyboard and virtual mouse**—The virtual keyboard and virtual mouse can be accessed using the RGS Receiver toolbar. The virtual mouse provides a visual indication of the remote cursor position, which is normally not present in the tablet GUI. The virtual mouse is useful when precise cursor positioning or hovering is required.

  TIP: The virtual mouse can also be enabled and disabled using the 4-finger tap gesture.

- **Hotkey sequence mapping**—See Gestures (Windows touch-capable devices only) on page 20 for more information.

The following table describes the gestures supported by RGS.

IMPORTANT: A **press** is 0.5 seconds or more, while a **tap** is less than 0.5 seconds.

Gesture	Description
1-finger tap	Left-click
1-finger double tap	Double-click
1-finger press and drag	Left-click and drag
2-finger tap	Right-click
2-finger press and drag	Right-click and drag
2-finger pinch/spread	Zoom out/in **NOTE:** The zoom will snap to 100% if close after you lift your fingers.
2-finger drag	Pan (when zoomed in)
3-finger swipe or drag	Scroll wheel
4-finger tap	Enable or disable the virtual mouse
4-finger press and drag	Center-click and drag
1-finger press 1-finger swipe left 1-finger swipe right 1-finger swipe up 1-finger swipe down 3-finger tap 3-finger press 4-finger press	These gestures can be customized. See Gestures (Windows touch-capable devices only) on page 20 for more information.

TIP: For a graphical demonstration of these gestures, select the **Gestures** panel in the RGS Receiver settings, and then select **See gestures tutorial**.

NOTE: Some gestures are disabled when the virtual mouse is enabled.

Using a Wacom pen (Linux)

To use a Wacom pen for input on Linux, the correct Wacom drivers must be installed on both the sender and the receiver. For HP ThinPro, Wacom drivers are either included in the RGS installation package or are preinstalled on the operating system image. For all other Linux operating systems, kernel modules and X drivers need to be compiled and installed on the both the sender and the receiver. Source code and instructions can be found at https://sourceforge.net/projects/linuxwacom/ (in English only).

Wacom pen capability should first be tested on both the sender and the receiver independently. For Linux operating systems other than HP ThinPro, this is most easily tested with pressure sensitive applications, which help verify that pen events are being created instead of mouse events. For HP ThinPro, you need to ensure only that the cursor moves with the Wacom pen.

After a Wacom pen is connected, it is usable only within the RGS Receiver window. A mouse is necessary to interact with the RGS interface and the local desktop.

NOTE: A Wacom pen does not respect floor control in a collaboration session. Multiple users attempting to simultaneously provide any kind of input might result in undesirable behavior.

The usage of Remote USB and the usage of a Wacom pen are mutually exclusive. To enable the usage of a Wacom pen when Remote USB is enabled, open USB Manager in HP ThinPro and set the USB protocol to **Local**.

Game Mode (Windows only)

Game Mode lets you lock the cursor inside the RGS Receiver window to perform functions that rely on relative cursor movements, such as 3D environment interaction. If Game Mode is not enabled, such interactions might cause erratic cursor behavior.

The default state of Game Mode (enabled or disabled) can be set using the RGS Receiver Configuration tool, and Game Mode can be toggled on and off while RGS Receiver is in Setup Mode by pressing the G key.

Supported keyboard layouts

All keyboard layouts and languages are supported.

Remote Audio

Remote Audio allows audio generated by the sender to play back on the speakers of the receiver.

The following sequence describes the path taken by audio during an RGS connection:

1. Software on the sender generates audio output.
2. The audio output is routed to RGS Sender using a physical or virtual audio device.
3. RGS Sender encodes and transmits the audio output to RGS Receiver on each receiver.
4. RGS Receiver decodes and sends the audio output to the audio mixer of the operating system.
5. The audio mixer of the operating system sends the audio to the default audio playback device.
6. The audio device plays the audio output on a connected audio peripheral, such as a speaker.

NOTE: Sounds that play through an internal speaker, such as the ToggleKeys sound on Windows, are not captured by RGS.

For information on the audio settings in RGS Receiver, see Audio on page 21.

For Remote Audio troubleshooting tips, see Remote Audio issues on page 80.

Using Remote Audio (Windows-based sender)

On Windows, Remote Audio should work by default. If the sender has an audio device, the RGS Sender installation process detects it. If the sender does not have an audio device (or if you disable all audio devices prior to installation of RGS Sender), then the `HP Remote Audio` virtual audio device is also installed during the RGS Sender installation process and will be used by RGS instead.

Using Remote Audio (Linux-based sender)

On Linux, some manual configuration might be required for Remote Audio depending on the audio capture method you intend to use.

If the sender has an audio device, RGS supports two different methods of audio capture:

- PulseAudio—See PulseAudio on page 47.
- Advanced Linux Sound Architecture (ALSA)—See ALSA on page 47.

The following property specifies which audio capture method will be used (see Other global properties on page 69 for more information):

```
Rgsender.Audio.Linux.RecorderApi
```

NOTE: Some audio device drivers might not have the capability to capture application-generated audio.

PulseAudio

Any audio device that is configured for PulseAudio can be used. PulseAudio provides a software interface similar to the Stereo Mix capability for ALSA. PulseAudio also provides a dummy device that allows the audio system to function when no hardware audio devices are available.

When using PulseAudio to capture audio, RGS Sender attempts to detect and connect to the monitor of the default playback device of the sender automatically. Explicit control of the PulseAudio capture device is available through the following property (see Other global properties on page 69 for more information):

```
Rgsender.Audio.Linux.DeviceName
```

If this property is set, RGS Sender attempts to connect to the device specified by this property. The command `pactl list` is useful for determining the PulseAudio device names. To capture from a specific device, specify the corresponding PulseAudio monitor source string (such as `alsa_output.pci-0000_00_1b.0.analog-stereo.monitor`).

PulseAudio allows the user to configure and control the audio devices in the system. Changing the output device during an RGS session results in a loss of audio. To restore audio, either reselect the original device or stop and start the audio stream using the audio settings in RGS Receiver.

ALSA

When using the ALSA audio system to capture audio, an audio device is required to be installed on the sender for application-generated audio to be sent to the receiver. Furthermore, the audio device installed in the sender must have the ability to record from a control that is the mix of all audio signals. On a Windows computer, by way of comparison, this control is often called **Stereo Mix**. Linux, however, does not follow a standard naming convention for this control, hence the need to evaluate individual audio devices to determine their suitability for use on Linux.

The audio devices on Linux are not consistent in the naming conventions of the audio controls. The RGS Sender installer will attempt to adjust volume levels for known audio devices to allow audio to be captured. This section describes how to adjust volume levels for the supported audio devices. This information may be helpful for configuring audio devices that are not currently supported by the RGS Sender installer.

Volume levels can typically be adjusted through the Volume Control application. This is usually found in the gnome panel or the system preferences menu. The Volume Control application may not show all available volume controls. The preferences for the Volume Control application may need to be adjusted to allow access to hidden volume controls.

The alsamixer is a command-line tool for adjusting volume. This application will not hide audio controls like its GUI counterpart; however, it is not as intuitive. Press the h key after running alsamixer to get additional information on how to control capture volumes.

Unsupported PCI audio devices are known to allow capture of application generated audio. The names of the controls that need to be adjusted are not consistent. Names of controls that might need to be adjusted include **PCM**, **Capture**, and **Mix**.

The device the audio is recorded from must be specified using the following property:

```
Rgsender.Audio.Linux.DeviceName
```

Run the command:

```
cat /proc/asound/devices
```

From this, you will see a list of the audio devices and it will look something like this:

```
0: [ 0] : control
1: : sequencer
8: [ 0- 0]: raw midi
16: [ 0- 0]: digital audio playback
17: [ 0- 1]: digital audio playback
24: [ 0- 0]: digital audio capture
32: [ 1] : control
33: : timer
48: [ 1- 0]: digital audio playback
56: [ 1- 0]: digital audio capture
```

Use an audio device only if it contains the word `capture` (device number 24 or 56 in the example above). Between each pair of square brackets, the first number is the sound card and the second number is the mixer device.

Use the following syntax to set the audio capture device, where `<c>` is the sound card number and `<d>` is the mixer device number:

```
Rgsender.Audio.Linux.DeviceName=plughw:<c>,<d>
```

Using the example above, you could specify audio device number 24 like below:

```
Rgsender.Audio.Linux.DeviceName=plughw:0,0
```

You could alternatively specify audio device number 56 like below:

```
Rgsender.Audio.Linux.DeviceName=plughw:1,0
```

Remote Clipboard

Remote Clipboard allows you to cut, copy, and paste data between the receiver and the sender or between two different senders.

Cutting and pasting text is supported on Windows, Linux, and Mac OS. Cutting and pasting an image is only supported between a Windows-based sender and Windows-based receiver.

On Windows, Remote Clipboard must be enabled during both the RGS Sender and RGS Receiver installations (see Installation on page 6).

On Linux, Remote Clipboard is installed by default.

On Windows, Linux, and Mac OS, Remote Clipboard must also be enabled in RGS Receiver (see Connection on page 19).

TIP: Setting the logging level of RGS Receiver or RGS Sender to `DEBUG` enables Remote Clipboard log information.

Remote USB (Windows/ThinPro only)

Remote USB allows a receiver's physically-attached USB devices to be virtually attached (mounted) to the sender. This gives the sender direct access to the USB devices, as if the devices were physically attached to it.

See the following list for information about Remote USB support:

- The sender must be Windows-based.
- The receiver can be either Windows-based or ThinPro-based.
- A receiver's physically-attached USB devices can be collectively attached to a single sender. The devices cannot be split between multiple senders, nor can they be collectively attached to multiple senders.
- RGS supports all four USB data transfer types (bulk, isochronous, interrupt, and control).
- USB devices that adhere to the USB 1.x or 2.x standard should work. However, webcams and devices that are sensitive to timing might experience decreased performance, or they might not function at all. HP recommends thoroughly testing any USB device intended for use with RGS.
- USB 1.x and USB 2.x devices are supported on USB 3.x ports, but USB 3.x devices are not supported.
- File copies might take longer due to the additional overhead of the network protocol on top of the USB protocol.

Configuring the remoting behavior of individual USB devices (Windows only)

The remoting behavior for individual USB devices can be altered from what was set globally during installation.

IMPORTANT: This configuration requires modifications to the Windows registry. Registry modifications should be made with extreme caution, and you should always make a backup of the registry prior to making any changes.

To configure the remoting behavior of a USB device:

1. Find the vendor ID and device ID for the USB device (see Determining USB device information (Windows) on page 51).
2. Open the Registry Editor and create the following registry key:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\hprpusbh
   \Parameters\Device
   ```

3. Create the following registry key:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\hprpusbh
   \Parameters\Device VID_VendorID&PID_ProductID
   ```

4. For the key you just created, create a string value named `Mode`.
5. Set the value of `Mode` to `auto`, `local`, or `remote`.

NOTE: If set to `auto`, the USB device switches its mounted location between the sender and the receiver at the start and end of an RGS connection respectively. If set to `remote`, you must physically disconnect the USB device from the receiver after the RGS session ends and then reconnect the USB device for it to be usable on the receiver.

USB microphones

The Remote USB driver (on the receiver) supports the USB isochronous data type, which is commonly used for streaming data such as that generated by audio and video devices. This enables certain isochronous USB microphones to be accessed directly by the sender in the same manner as other USB devices.

To remotely attach USB microphones to the sender, either of these Remote USB Configuration settings can be selected:

- **USB devices are Remote**—If selected, a USB microphone can be accessed anytime by the sender.
- **USB devices are Local/Remote**—If selected, how the USB microphone can be accessed by the sender depends on when the microphone is connected to the receiver relative to establishment of the RGS connection:
  - If the microphone is connected to the receiver after establishment of an RGS connection, the microphone will be a remote device only and can be accessed directly by the sender.

TIP: The Windows **Recording devices** dialog in the sender allows the user to set the default sound recording device (microphone).

Remote USB Access Control List

RGS Sender supports an Access Control List (ACL) file that contains rules that specify whether to allow a Remote USB connection from a USB device on the receiver side.

Each rule in the ACL file has a type of `allow` or `deny`. The rules are evaluated for each Remote USB connection request as described below:

- If any rule indicates the USB connection should be denied, the connection is denied, regardless of any other rule.
- If any rule indicates the USB connection should be allowed, and if there are no rules that deny the connection, the connection is allowed.
- If no rules match at all, the connection is denied.

The ACL file is implemented in XML format and is accompanied by an XSD (XML Schema Definition) file that defines the XML elements. The default ACL file `hprDefaultUsbAcl.xml` and the XSD file `hprUsbAcl.xsd` are both in the RGS Sender installation directory.

TIP: You can specify different files using the RGS Sender Configuration tool (see Using the RGS Sender Configuration tool on page 62).

The default ACL file contains the following contents, which allows all USB connections to be made:

```
<hprUsbAcl> <ruleset> <rule type="allow"> <name>Allow all USB devices (HP default)</name> </rule> </ruleset></hprUsbAcl>
```

Rules can contain the filters described in the following table.

TIP: See `hprUsbAcl.xsd` for examples of using filters.

Filter	Description
`bDeviceClass`	The device class
`bDeviceSubclass`	The device subclass
`bDeviceProtocol`	The device protocol

Filter	Description
idVendor	The vendor ID
idProduct	The product ID
bcdDevice	The device version number
manufacturer	The manufacturer name
product	The product name
serialNumber	The product serial number
peerAddress	The IP address of the receiver
group	The domain group of the user logged on to the receiver

IMPORTANT: Filtering by `manufacturer`, `product`, or `serialNumber` is not reliable because the manufacturer is not required to fill in those values.

Determining USB device information (Windows)

To determine USB device information:

1. Open Device Manager and find the USB device under **Universal Serial Bus controllers**.
2. Double-click the USB device, and then select the **Details** tab in the window that appears.
3. Determine the vendor ID, product ID, class, subclass, and protocol.
   a. Select **Hardware Ids** from the drop-down menu. The vendor ID and product ID are displayed in the following format:

      ```
      USB\VID_<vendor ID>&PID_<product ID>
      ```

      In the below example, the vendor ID is `1234` and the device ID is `5678`:

      ```
      USB VID_1234&PID_5678
      ```

   b. Select **Compatible Ids** from the drop-down menu. The class, subclass, and protocol are represented by numerical codes and are displayed in the following format:

      ```
      USB\Class_<class code>&SubClass_<subclass code>&Prot_<protocol code>
      ```

      In the below example, the class code is `08`, the subclass code is `06`, and the protocol code is `50`:

      ```
      USB Class_08&SubClass_06&Prot_50
      ```

Determining USB device information (Linux)

To determine USB device information, use an open source program named USBView, which is available at http://sourceforge.net/projects/usbview.

Enabling Remote USB on HP ThinPro

Remote USB can be enabled for RGS Receiver on HP ThinPro if the sender is Windows-based.

To enable Remote USB on HP ThinPro:

1. In HP ThinPro, open the USB Manager and set the USB protocol to **RGS**.
2. Restart the thin client.
3. Ensure that **Enable remote USB** is enabled in RGS Receiver.

Directory Mode

Directory Mode lets you connect to multiple senders simultaneously from a single receiver. When you start RGS Receiver in Directory Mode, it looks for a directory file containing user names and computer names. RGS Receiver reads this file and attempts to connect to each specified sender automatically.

The default directory file is `directory.txt` in the RGS Receiver installation directory.

NOTE: This file contains examples that are commented out using the `#` character.

Directory file format

The directory file is often a common file for a group, department, organization, or an entire company. The directory file can manage and administer the senders for any number of users. HP recommends that you save the directory file on a readily-accessible network file share or mapped drive so it can be shared by multiple receivers.

The directory file is a text file with the following format for each user:

```
<domain name> <user name> <computer name> [<computer name> ...]
```

The domain name of a Windows-based sender depends on the environment. For a domain account, using the example `worldwide\user1`, the domain name used for Directory Mode would be `worldwide`.

The following example directory file specifies the senders for user1 and user2 in a domain account environment:

```
worldwide user1 RC_1 RC_2 RC_3
worldwide user2 RC_4 RC_5 RC_6
```

For a local account, using the example `user1_computer\user1`, the domain name used for Directory Mode would be `user1_computer`.

The following example directory file specifies the senders for user1 and user2 in a local account environment:

```
user1_computer user1 RC_1 RC_2 RC_3
user2_computer user2 RC_4 RC_5 RC_6
```

For Linux-based senders, use `UNIX` as the domain name.

The domain name does not apply when using the directory file for Linux users. Instead, use the keyword `UNIX` in place of the domain name. For example:

```
UNIX user1 RC_1 RC_2 RC_3
```

If the user name contains white-space characters, the name can be enclosed in double-quotes as shown below:

```
domain1 "user1 user" RC_1 RC_2 RC_3
domain1 "user2 user" RC_4 RC_5 RC_6
```

Starting RGS Receiver in Directory Mode (Windows)

NOTE: Before attempting a connection in Directory Mode for the first time, HP recommends that you first verify that RGS can connect to each computer individually.

- Windows 7: Select **Start**, select **All Programs**, select **HP**, select **HP Remote Graphics Software**, and then select **HP RGS Receiver Directory Mode**.

  Windows 8.1: Select the **HP RGS Receiver Directory Mode** tile on the Start screen.

  Windows 10: Select **Start** , type `RGS`, and then select **HP RGS Receiver Directory Mode** from the search results.

Alternately, RGS Receiver can be started in Directory Mode on the command line, using either of the following:

```
rgreceiver.exe -directory <file name>
```

```
rgreceiver.exe -directory
```

If a file name is specified after `-directory`, RGS Receiver uses that file as the directory file. If no file name is specified, you are prompted to specify the path and name of the directory file.

In Directory Mode, RGS Receiver displays the name of the directory file. The **Change** button enables you to specify a different directory file. The **Connect All** button is used to establish a connection to the senders listed in the directory file.

After clicking **Connect All**, you'll need to independently authenticate and log into each sender.

To bring a specific RGS Receiver window to the front:

1. Enable Setup Mode using the hotkey sequence (see Setup Mode on page 18).
2. Press Tab to open the RGS Receiver window selector, and then select the desired RGS Receiver window.

Starting RGS Receiver in Directory Mode (Mac OS)

- Run either of the following commands on the command line:

  ```
  open -a "HP RGS Receiver" --args -directory Filename
  ```

  ```
  open -a "HP RGS Receiver" --args -directory
  ```

  If a file name is specified after `-directory`, RGS Receiver uses that file as the directory file. If no file name is specified, you are prompted to specify the path and name of the directory file.

8 Configuration tools and properties

On Windows and Linux, RGS Receiver and RGS Sender each include a configuration tool that allows you to modify some of the more advanced RGS settings. Most of the options in the configuration tools correspond to one of the properties in the `rgreceiverconfig` and `rgsenderconfig` files respectively.

On Mac OS, properties must be set manually by editing the file `/Library/Application Support/HP/rgreceiverconfig`.

This chapter discusses the following topics:

NOTE: When settings are changed using the configuration tools, the process described in Setting property values in a configuration file on page 69 is automated. Manual editing of the configuration files is not necessary unless you want to add or modify properties that do not have a corresponding option in one of the configuration tools, such as the per-session properties of RGS Receiver.

See Setting RGS properties manually on page 68 and Other properties on page 69 for more information.

RGS Receiver setting override hierarchy

When an option's setting is changed using the RGS Receiver Configuration tool (or by manually editing the properties in the `rgreceiverconfig` file), the new setting overrides any setting for that option that was previously persisted when RGS Receiver was last closed. However, the setting can be further overridden on the command line or using the RGS Receiver settings (if the same option is available).

In the following hierarchy, settings configured using methods higher on the list override settings configured using methods lower on the list (with 1 being the highest and 5 being the lowest).

1. Settings configured in RGS Receiver
2. Settings configured on the command line
3. Settings configured using the RGS Receiver Configuration tool (or by manually editing the properties in the `rgreceiverconfig` file)
4. Settings that were persisted the last time RGS Receiver was closed
5. Default settings

Using the RGS Receiver Configuration tool

To use the RGS Receiver Configuration tool:

1. Navigate to the RGS Receiver installation directory, and start the tool:
   - On Windows, run the following executable:

     `receiverConfigApp.exe`
   - On Linux, execute the following command:

     `./receiverconfigapp.sh`
2. Configure options as desired.

NOTE: See the tables in the following sections for descriptions of each of the options.

3. Select **Save** to save your changes.

TIP: To restore all default RGS Receiver Configuration settings, make sure RGS Receiver is not running, and then select **Restore to default** in the lower-left corner of the RGS Receiver Configuration tool. Alternatively, uninstalling and then reinstalling RGS Receiver restores all default settings.

General

The following table describes the options available in the **General** panel of the RGS Receiver Configuration tool. The corresponding property in the `rgreceiverconfig` file is noted for reference.

Option	Description
Enable borders on the Receiver window	Enables borders on the RGS Receiver window. Configuration file property (Windows/Linux only): `Rgreceiver.IsBordersEnabled`
Snap the Receiver window when close to the edge of the screen	When enabled, the RGS Receiver window will snap when close to the top or left edge of the screen. Configuration file property (Windows/Linux only): `Rgreceiver.IsSnapEnabled`
Enable the Receiver window Toolbar	Enables the RGS Receiver toolbar. Configuration file property (Windows/Linux only): `Rgreceiver.IsMenubarEnabled`
Display a warning that disconnecting from RGS while logged in will not log the user out of the remote system	When enabled, RGS Receiver will display a warning that disconnecting an RGS connection will not automatically log them out of the sender. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.IsDisconnectWarningEnabled`
Network disruption warning color	Use the **Color** and **Transparency** controls to set the color that overlays the RGS Receiver window when RGS Receiver detects a network disruption. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.ConnectionWarningColor`
Enable RGS to communicate mouse cursor snaps	When enabled, mouse cursor snaps (such as to the default button of a dialog box) will be communicated by RGS.

Option	Description
	Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.IsMouseSyncEnabled`
Number of recent remote connections listed	Sets the number of recent remote connections to list in RGS Receiver. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.MaxSenderListSize`
File used for Directory Mode	Specifies the file to use for Directory Mode. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Directory`
Always prompt for the domain, username, and password when establishing a connection	When enabled, RGS Receiver will always prompt for the domain, username, and password when establishing a connection. Configuration file property (Windows/Linux only): `Rgreceiver.IsAlwaysPromptCredentialsEnabled`
Certificate Verification Failure Policy	Specifies what RGS Receiver does if the verification of the sender certificate fails. Select **Accept**, **Prompt to accept**, or **Deny**. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Network.Certificate.VerificationPolicy={Accept | Prompt to accept | Deny}`
Allow user to modify Certificate Verification Failure Policy	Enables the user to change the **Certificate Verification Failure Policy** setting. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Network.Certificate.VerificationPolicy.IsMutable={0 | 1}`
Allow user to set whether the Remote Clipboard is enabled	When enabled, a user can modify the **Enable remote clipboard** setting in RGS Receiver . Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Clipboard.IsMutable`
Enable Remote Clipboard by default	Enables Remote Clipboard by default. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Clipboard.IsEnabled`
Remote Clipboard filters	**IMPORTANT:** This property is for advanced users only. It should only be changed from its default value if Remote Clipboard does not support the clipboard format required by your application. The **Selected filters** window specifies the clipboard formats that are allowed to be transferred using Remote Clipboard. By default, all filters are selected, but filters can be removed by moving them to the **Available filters** window. **NOTE:** For more information about clipboard formats, go to http://msdn2.microsoft.com/en-us/library/ms649013.aspx. Configuration file property (Windows only): `Rgreceiver.Clipboard.FilterString`

Image and Display

The following table describes the options available in the **Image and Display** panel of the RGS Receiver Configuration tool. The corresponding property in the `rgreceiverconfig` file is noted for reference.

Option	Description
Enable Advanced Video Compression on Sender	Enables Advanced Video Compression by default. Configuration file property (Windows/Linux only): `Rgreceiver.ImageCodec.IsH264Enabled`
Advanced Video Compression encoding	Sets whether Advanced Video Compression encoding should be handled by the sender's GPU or CPU. Configuration file property (Windows/Linux only): `Rgreceiver.ImageCodec.UseGPU`
Maximum number of cores	Sets the maximum number of CPU cores on the receiver that can be used for decoding. **NOTE:** This option is not available if Advanced Video Compression is enabled. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Decoder.ThreadPoolSize`
Increase text rendering quality	Improves image quality for images containing significant amounts of text or lines. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.ImageCodec.IsBoostEnabled`
Enable image quality slider	When enabled, the image quality slider can be adjusted by a user, either in RGS Receiver or on the RGS Receiver toolbar. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.ImageCodec.IsMutable`
Image Quality by default	Sets the default image quality (from 0 to 100). Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.ImageCodec.Quality`
Enable adaptive image quality by default	When enabled, RGS will use the **Adaptive image quality** settings by default. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Experience.Mode`
Minimum image quality	Sets the default value for the **Minimum image quality** setting. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Experience.MinImageQuality`
Target update rate	Sets the default value for the **Target update rate** setting. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Experience.MinUpdateRate`
Max number of image update requests	This property provides performance optimization in high-latency network environments by setting the maximum number of image updates RGS Sender can send across the network without hearing back from RGS Receiver. Increasing

Option	Description
	this value might help increase the frame rate at the expense of increased network bandwidth consumption. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.MaxImageUpdateRequests`
Force full screen image updates	Enables the **Force full screen image updates** option in RGS Receiver by default. Configuration file property (Windows/Linux only): `Rgreceiver.IsGlobalImageUpdateEnabled`
Enable Match Receiver display resolution by default	Enables the **Match Receiver display resolution** option in RGS Receiver by default. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.IsMatchReceiverResolutionEnabled`
Enable Match Receiver display layout by default	Enables the **Match Receiver display layout** option in RGS Receiver by default. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.IsMatchReceiverPhysicalDisplaysEnabled`

Audio

The following table describes the options available in the **Audio** panel of the RGS Receiver Configuration tool. The corresponding property in the `rgreceiverconfig` file is noted for reference.

Option	Description
Allow user to modify audio settings	When enabled, a user can modify the audio settings in RGS Receiver . Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Audio.IsMutable`
Enable Remote Audio by default	Enables Remote Audio by default. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Audio.IsEnabled`
Enable stereo audio by default	Enables stereo audio by default. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Audio.IsInStereo`
Audio quality	Sets the default audio quality. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Audio.Quality`
Only play audio from current Receiver window	When enabled, audio will play only from the RGS Receiver window that has focus. When disabled, audio from all RGS Receiver windows will be combined. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Audio.IsFollowsFocusEnabled`

Network

The following table describes the options available in the **Network** panel of the RGS Receiver Configuration tool. The corresponding property in the `rgreceiverconfig` file is noted for reference.

Option	Description
Allow user to modify network timeout settings	When enabled, a user can modify the network settings in RGS Receiver . Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Network.Timeout.IsMutable`
Enable the warning dialog for when the RGS connection is about to time out	Enables the warning dialog for when the RGS connection is about to time out due to the inability to contact RGS Sender. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Network.Timeout.IsGuiEnabled`
Error timeout (seconds)	Sets the time in seconds that RGS Receiver will wait before ending the connection after failing to detect RGS Sender. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Network.Timeout.Error`
Warning timeout (seconds)	Sets the time in seconds that RGS Receiver will wait before displaying a warning dialog to the local user after failing to detect RGS Sender. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Network.Timeout.Warning`
Dialog timeout (seconds)	Sets the time in seconds that RGS Receiver will wait for a response to a dialog being displayed on the sender (such as an authentication dialog). **NOTE:** The request will be canceled if there is no response. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Network.Timeout.Dialog`
RGS Sender network port	Specifies the port to use for communication between RGS Receiver and RGS Sender. **IMPORTANT:** This setting must match the port setting on RGS Sender. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Network.Port`

HP Velocity (Windows/Linux only)

The following table describes the options available in the **HP Velocity** panel of the RGS Receiver Configuration tool. The corresponding property in the `rgreceiverconfig` file is noted for reference.

NOTE: See HP Velocity documentation for more information about HP Velocity settings.

Option	Description
Enable HP Velocity	Enables HP Velocity. Configuration file property (Windows/Linux only): `Rgreceiver.Network.HPVelocity.Enabled`

Option	Description
Operational Mode	Sets whether HP Velocity should correct network loss (**Active Mode**) or just monitor it (**Monitor Mode**). Configuration file property (Windows/Linux only): `Rgreceiver.Network.HPVelocity.LiveUdpMode`
Target loss rate (10k packet sample)	Sets the amount of network loss that HP Velocity will tolerate before adding packet-protection redundancy to the data flow. Configuration file property (Windows/Linux only): `Rgreceiver.Network.HPVelocity.LiveUdpTargetLossRate`
Level of congestion control	Sets the level of congestion control, where **Standard** handles the effects of a high-latency network and **Friendly** uses the standard TCP-like congestion-control algorithm. Configuration file property (Windows/Linux only): `Rgreceiver.Network.HPVelocity.LiveUdpCongestionControlAlgorithm`

USB (Windows/Linux only)

The following table describes the options available in the **USB** panel of the RGS Receiver Configuration tool. The corresponding property in the `rgreceiverconfig` file is noted for reference.

Option	Description
Allow user to modify Remote USB settings	When enabled, a user can modify the Remote USB settings in RGS Receiver . Configuration file property (Windows/Linux only): `Rgreceiver.Usb.IsMutable`
Enable Remote USB by default	Enables Remote USB by default. Configuration file property (Windows/Linux only): `Rgreceiver.Usb.IsEnabled`
USB active session	Specifies which sender to attach USB devices to for Directory Mode. Configuration file property (Windows/Linux only): `Rgreceiver.Usb.ActiveSession`

Hotkeys

The following table describes the options available in the **Hotkeys** panel of the RGS Receiver Configuration tool. The corresponding property in the `rgreceiverconfig` file is noted for reference.

Option	Description
Allow user to modify hotkey settings	When enabled, a user can modify the hotkey settings in RGS Receiver . Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Hotkeys.IsMutable`
Enable the Send Ctrl+Alt+End key sequence as Ctrl+Alt+Del option by default	Enables the **Send CTRL-ALT-END key sequence as CTRL-ALT-DEL** option in RGS Receiver by default.

Option	Description
	Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Hotkeys.IsSendCtrlAltEndAsCtrlAltDeleteEnabled`
Process a Ctrl+Alt+Delete sequence on both the local and remote computers	When enabled, both the receiver and the sender will process a Ctrl+Alt+Delete sequence. When disabled, only the receiver will process a Ctrl+Alt+Delete sequence. Configuration file property (Windows only): `Rgreceiver.Hotkeys.IsCtrlAltDeletePassThroughEnabled`
Enable the Setup Mode hotkey sequence	Enables the Setup Mode hotkey sequence. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Hotkeys.IsSetupModeEnabled`
Setup Mode sequence	Specifies the Setup Mode hotkey sequence. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Hotkeys.SetupModeSequence`
Enable the Send First Key option by default	Enables the **Send First Key** option in RGS Receiver by default. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Hotkeys.IsSendFirstKeyInSequenceEnabled`
Enable the Key Repeat option by default	Enables the **Key Repeat** option in RGS Receiver by default. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Hotkeys.IsKeyRepeatEnabled`
Enable Game Mode	Enables Game Mode. Configuration file property (Windows/Linux only): `Rgreceiver.Hotkeys.IsGameModeEnabled`

Logging

The following table describes the options available in the **Logging** panel of the RGS Receiver Configuration tool. The corresponding property in the `rgreceiverconfig` file is noted for reference.

Option	Description
Allow user to modify logging settings	When enabled, a user can modify the logging settings in RGS Receiver. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Log.IsMutable`
Enable RGS Receiver logging by default	Enables logging for RGS Receiver by default. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Log.IsFileLoggerEnabled`
Log Level	Sets the lowest level of output to log. The specified level and anything more serious will be logged in the RGS Receiver log file. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Log.Level`

Option	Description
Log file path	Specifies the path to the RGS Receiver log file. Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Log.Filename`
Max logfile size (KB)	Sets the maximum size the RGS Receiver log file can be in kilobytes (KB). Configuration file property (Windows/Linux/Mac OS): `Rgreceiver.Log.MaxFileSize`

Activation (Windows/Linux only)

The following table describes the options available in the **Activation** panel of the RGS Receiver Configuration tool. The corresponding property in the `rgreceiverconfig` file is noted for reference.

Option	Description
Enable activation to the HP activation server	Enables activation of RGS Advanced Features. Configuration file property (Windows/Linux only): `Rgreceiver.Registration.IsEnabled`
Use a proxy server when activating RGS Advanced Features	Enables the use of a proxy server for activation of RGS Advanced Features. Configuration file property (Windows/Linux only): `Rgreceiver.Network.ProxyEnabled`
Proxy server address	Specifies the proxy server address to use for activation of RGS Advanced Features. Configuration file property (Windows/Linux only): `Rgreceiver.Network.ProxyAddress`
Proxy port	Specifies the proxy server port to use for activation of RGS Advanced Features. Configuration file property (Windows/Linux only): `Rgreceiver.Network.ProxyPort`

RGS Sender setting override hierarchy

To override default settings in RGS Sender:

▲ Use the RGS Sender Configuration tool or manually edit the properties in the rgsenderconfig file.

Using the RGS Sender Configuration tool

To use the RGS Sender Configuration tool:

1. Navigate to the RGS Sender installation directory, and start the tool:
   - On Windows, run the following executable:

`senderConfigApp.exe`

- On Linux, execute the following command:

  `./senderconfigapp.sh`

2. Configure options as desired.

NOTE: See the tables in the following sections for descriptions of each of the options.

3. Select **Save** to save your changes.

TIP: To restore all default RGS Sender Configuration settings, make sure the RGS Sender service is stopped, and then select **Restore to default** in the lower-left corner of the RGS Sender Configuration tool. Alternatively, uninstalling and then reinstalling RGS Sender restores all default settings.

NOTE: Sender authentication settings can also be changed via the command line. When the tool is used with command line arguments, the tool's GUI is not displayed. See Authentication (Windows only) on page 64 for details.

General

The following table describes the options available in the **General** panel of the RGS Sender Configuration tool. The corresponding property in the `rgsenderconfig` file is noted for reference.

Option	Description
End the RGS session and disconnect all collaborators when the primary user logs out	When enabled, RGS Sender will end the RGS connection and disconnect all collaborators when the primary user logs out. **NOTE:** On Linux, the RGS connection is always ended when the primary user logs out. Configuration file property (Windows only): `Rgsender.IsDisconnectOnLogoutEnabled`
Enable session reconnection after logout or fast user switching.	Enables session reconnection after logout or Fast User Switching Configuration file property (Windows only): `Rgsender.IsReconnectOnConsoleDisconnectEnabled`
Enable monitor blanking on Sender when a remote user connects	When enabled, the sender's screen will blank and its keyboard and mouse will disable when a remote user connects. Configuration file property (Windows/Linux): `Rgsender.IsBlankScreenAndBlockInputEnabled`
Enable Remote Audio	Enables Remote Audio. Configuration file property (Windows/Linux): `Rgsender.Audio.IsEnabled`
Enable Remote Clipboard	Enables Remote Clipboard. Configuration file property (Windows/Linux): `Rgsender.Clipboard.IsEnabled`

Authentication (Windows only)

The **Authentication** panel of the RGS Sender Configuration tool can be used to choose between standard authentication, Easy Login, or Single Sign-on.

NOTE: This panel replaces the RGS Admin tool previously included with RGS Sender on Windows.

TIP: Authentication settings can also be changed via the command line. The following commands are supported:

Enable Standard Authentication: `senderConfigApp.exe -enableStandardLogin`

Enable Single Sign-on: `senderConfigApp.exe -enableSSO`

Enable Easy Login: `senderConfigApp.exe -enableEasyLogin`

Display the current selected method: `senderConfigApp.exe -status`

Display usage message: `senderConfigApp.exe -h`

Image and Display

The following table describes the options available in the **Image and Display** panel of the RGS Sender Configuration tool. The corresponding property in the `rgsenderconfig` file is noted for reference.

Option	Description
Preferred display methods	Sets the order of methods to detect image changes. If a method is not currently supported with the system, the next method in the list will be tried. The available methods are as follows: • `GPU`—Uses the GPU hardware to quickly compare one full screen to a previous full screen • `ChangeList`—Uses the RGS mirror-driver on Windows and the RGS X server extension on Linux to detect display changes • `Comparitron`—Uses the system's CPU to compare one full screen to a previous full screen **NOTE:** This option has no effect if Advanced Video Compression is enabled. Configuration file property (Windows/Linux): `Rgsender.PreferredDisplayMethods`
Maximum number of cores	Sets the maximum number of CPU cores on the sender that can be used for encoding. Configuration file property (Windows/Linux): `Rgsender.Encoder.ThreadPoolSize`
Maximum image update rate	Sets the maximum number of image updates per second. If set to 0, the update rate will be unlimited. Configuration file property (Windows/Linux): `Rgsender.MaxImageUpdateRate`
Image codec	Sets the order of codecs to use for all transmitted image data. If a codec is not currently supported with the system, the next codec in the list will be tried. The available codecs are as follows: • `HP3`—This codec has been the default since RGS 5.0. • `HP2`—This codec was the default prior to RGS 5.0.

Option	Description
	• `JPEG-LS`—This codec is mathematically lossless. **NOTE:** This option has no effect if Advanced Video Compression is enabled. Configuration file property (Windows/Linux): `Rgsender.ImageCodec.Preferred`

Network

The following table describes the options available in the **Network** panel of the RGS Sender Configuration tool. The corresponding property in the `rgsenderconfig` file is noted for reference.

Option	Description
Error timeout (seconds)	Sets the time in seconds that RGS Sender will wait before ending the connection after failing to detect RGS Receiver. Configuration file property (Windows/Linux): `Rgsender.Network.Timeout.Error`
Listen for RGS connections on all network interfaces	When enabled, RGS Sender will listen for connections on all network interfaces. Configuration file property (Windows/Linux): `Rgsender.Network.IsListenOnAllInterfacesEnabled`
Listen to a specific network interface	Specifies which network interfaces RGS Sender will listen for connections on. See Sender network interface binding on page 77 for more information on how to determine the value that corresponds with each network interface. **NOTE:** This option is not available if the **Listen for RGS connections on all network interfaces** option is enabled. Configuration file property (Windows/Linux): `Rgsender.Network.Interface.<n>.IsEnabled` **NOTE:** If setting the property manually, replace `<n>` with the number of the network interface.
Listen to a specific range of IP addresses	Specifies the range of IP addresses that RGS Sender will listen for connections on. A network interface must be enabled using the **Listen to a specific network interface** option, and its IP address must be in the specified range. **NOTE:** This option is not available if the **Listen for RGS connections on all network interfaces** option is enabled. Configuration file property (Windows/Linux): `Rgsender.Network.AllowIpAddressSubnet`
RGS Sender network port	Specifies the port to use for communication between RGS Sender and RGS Receiver. **IMPORTANT:** This setting must match the port setting on RGS Receiver. Configuration file property (Windows/Linux):

Option	Description
	Rgsender.Network.Port

HP Velocity

The following table describes the options available in the **HP Velocity** panel of the RGS Sender Configuration tool. The corresponding property in the `rgsenderconfig` file is noted for reference.

NOTE: See HP Velocity documentation for more information about HP Velocity settings.

Option	Description
Enable HP Velocity	Enables HP Velocity. Configuration file property (Windows/Linux): `Rgsender.Network.HPVelocity.Enabled`
Operational Mode	Sets whether HP Velocity should correct network loss (**Active Mode**) or just monitor it (**Monitor Mode**). Configuration file property (Windows/Linux): `Rgsender.Network.HPVelocity.LiveUdpMode`
Target loss rate (10k packet sample)	Sets the amount of network loss that HP Velocity will tolerate before adding packet-protection redundancy to the data flow. Configuration file property (Windows/Linux): `Rgsender.Network.HPVelocity.LiveUdpTargetLossRate`
Level of congestion control	Sets the level of congestion control, where **Standard** handles the effects of a high-latency network and **Friendly** uses the standard TCP-like congestion-control algorithm. Configuration file property (Windows/Linux): `Rgsender.Network.HPVelocity.LiveUdpCongestionControlAlgorithm`

USB

The following table describes the options available in the **USB** panel of the RGS Sender Configuration tool. The corresponding property in the `rgsenderconfig` file is noted for reference.

Option	Description
ACL file name (XML)	Specifies the name of the XML file that implements the Remote USB Access Control List (ACL). Configuration file property (Windows/Linux): `Rgsender.Usb.Acl.RulesetPath`
ACL schema file (XSD)	Specifies the name of the schema file that accompanies the Remote USB XML file. Configuration file property (Windows/Linux): `Rgsender.Usb.Acl.SchemaPath`
Amount of time that the RGS Sender will wait before disconnecting all USB devices if the	Sets the amount of time in milliseconds that RGS Sender will wait before disconnecting all USB devices if the USB ACL file disappears or becomes inaccessible.

Option	Description
USB ACL file becomes inaccessible (milliseconds)	**NOTE:** If the file is restored prior to expiration of the timeout period, the USB devices remain connected. Configuration file property (Windows/Linux): `Rgsender.Usb.Acl.RulesetErrorTimeout`

Collaboration

The following table describes the options available in the **Collaboration** panel of the RGS Sender Configuration tool. The corresponding property in the `rgsenderconfig` file is noted for reference.

Option	Description
Display list of users connected to the remote computer	Enables the collaboration notification dialog. **IMPORTANT:** This option should normally remain enabled. When disabled, neither remote users nor local users are notified who is participating in a collaboration session. The warning dialog that is displayed when the sender is unable to blank its monitor is also prevented from being displayed. Configuration file property (Windows/Linux): `Rgsender.IsCollaborationNotificationEnabled`
Automatically give permission for authorized collaborators to join the session	When enabled, collaborators will always be accepted without having to be authorized by the primary user. Configuration file property (Windows/Linux): `Rgsender.Collaboration.AlwaysAcceptCollaborators`
Collaboration request timeout (milliseconds)	Sets the amount of time in milliseconds that the collaboration authentication dialog is shown before the request is denied automatically. **NOTE:** Set the value to be equal to or less than `Rgreceiver.Network.Timeout.Dialog` for all collaborating receivers. See Network on page 59 for more information. Configuration file property (Windows/Linux): `Rgsender.CollabUI.Dialog.Timeout`
Delay before another user can take floor control when active user stops giving input	Sets the delay in milliseconds after the active user stops making inputs before another user can take control of the floor in a collaboration session. The value can range from 500 milliseconds (0.5 seconds) to 15000 milliseconds (15 seconds). Configuration file property (Windows/Linux): `Rgsender.RequestFloorControlTime`

Logging

The following table describes the options available in the **Logging** panel of the RGS Sender Configuration tool. The corresponding property in the `rgsenderconfig` file is noted for reference.

Option	Description
Log Level	Sets the lowest level of output to log. The specified level and anything more serious will be logged in the RGS Sender log file.

Option	Description
	Configuration file property (Windows/Linux/Mac OS): `Rgsender.Log.Level`
Log file path	Specifies the path to the RGS Sender log file. Configuration file property (Windows/Linux/Mac OS): `Rgsender.Log.Filename`
Max logfile size (KB)	Sets the maximum size of the RGS Sender log file (in kilobytes). Configuration file property (Windows/Linux/Mac OS): `Rgsender.Log.MaxFileSize`

Diagnostics

The **Diagnostics** panel of the RGS Sender Configuration tool can be used to detect potential issues that might prevent a remote connection.

Certificates

The **Certificates** panel of the RGS Sender Configuration tool provides information about the self-signed certificate generated by the RGS Sender.

Section	Description
File Location	Identifies the file location of the certificate used by the RGS Sender.
Expiration	Identifies the expiration date of the certificate by the RGS Sender.
Fingerprint	Identifies the SHA256 fingerprint of the certificate being used by the RGS Sender.

Setting RGS properties manually

Property syntax

The following example shows the RGS property syntax:

```
Rgreceiver.Network.Timeout.Warning=10000
```

In this example, the name of the property is `Rgreceiver.Network.Timeout.Warning`, and the value of the property is `10000`. This setting specifies that RGS Receiver will wait 10,000 milliseconds (10 seconds) before displaying a warning dialog that indicates that it is no longer able to communicate with RGS Sender. This particular setting is duplicated in the Network panel of the RGS Receiver settings.

A property could also be set to an empty value like in the following example:

```
Rgreceiver.Browser.Name=
```

Properties with empty values initialize as follows:

- If the value of the property is of type **string**, the value will be set as an empty string.
- If the value of the property is of type **int**, **int vector**, or **bool**, the value will be set to `0`.

IMPORTANT: No user notification is provided if a property name is misspelled, and the property will not take effect. If you specify a property in a configuration file or on the command line and it does not take effect, verify that the property name is spelled correctly (including uppercase and lowercase usage).

Setting property values in a configuration file

RGS property values can be set in a configuration file. The Receiver configuration file is named `rgreceiverconfig` and the Sender configuration file is named `rgsenderconfig`. On Windows, the files are located in the RGS Receiver or the RGS Sender installation directory. On Linux, the files are located in `/etc/opt/hpremote/rgreceiver` or `/etc/opt/hpremote/rgsender`. On Mac OS, the rgreceiverconfig file is located in `/Library/Application Support/HP/rgreceiver`.

The configuration files contain one property per line. All properties in the configuration files are initially commented out with the `#` character. To set a property in a configuration file, first delete the `#` character preceding the property name, and then set the property to the desired value. For RGS Receiver, once a property is uncommented in the configuration file, the property's setting is persisted when RGS Receiver is closed.

IMPORTANT: After an RGS Receiver property is persisted, commenting out the property in the configuration file again will not reset its value to default. To reset a value to default, set the property back to its default value in the configuration file and leave the line uncommented.

NOTE: If a property is listed more than once, the value of the last entry is used.

NOTE: RGS properties set in a configuration file might not take effect until the computer is restarted.

Setting property values on the command line

Property values for RGS Receiver on Windows and Linux, and for RGS Sender on Windows, can be set on the command line. See RGS Receiver command-line options on page 23 and RGS Sender command-line options (Windows) on page 24 for examples.

NOTE: Per-session property values cannot be set on the command line.

Other properties

This section describes the RGS properties that do not have a corresponding option in the configuration tools and can only be set via the configuration file or on the command line.

Other global properties

Property	Description
`Rgreceiver.Smartcard.IsEnabled`	When enabled, the receiver uses smart card redirection with senders that have smart card redirection installed and enabled.
`Rgsender.Smartcard.IsEnabled`	When enabled and smart card redirection is installed, the receiver is allowed to use smart card redirection.
`Rgreceiver.IsSendCtrlLeftMouseClickAsRightMouseClickEnabled`	**NOTE:** Mac OS only When enabled, if you simultaneously press and hold Ctrl and click the left mouse button, the combination is translated to a right-click and sent to the sender. When disabled, if you simultaneously press and hold Ctrl and click the left mouse button, the combination is sent to the sender with no modification.

Property	Description
`Rgreceiver.Experience.IsMutable`	When enabled, a user can modify the settings under the Experience heading in RGS Receiver.
`Rgreceiver.Audio.Linux.DeviceName`	**NOTE:** Linux only This property specifies the name of the audio device that is to be used.
`Rgreceiver.Registration.ServerAddresses`	**IMPORTANT:** This setting should not be modified unless instructed by HP. Specifies the IP addresses of the HP servers used for activation of RGS Advanced Features.

Property	Description
`Rgsender.ConsoleLogonTimeout`	This property sets the time in seconds to wait for a system login event to complete. If the login does not occur within this limit, the sender will be shut down.
`Rgsender.IsClassicEasyLogonEnabled`	For Windows, this property enables multiple users to connect to a locked desktop before logon. For Linux, this property enables Easy Login.
`Rgsender.Audio.Linux.DeviceName`	**NOTE:** Linux only This property specifies the name of the audio device that is to be used.
`Rgsender.Audio.Linux.RecorderApi`	**NOTE:** Linux only If set to `pulse` (the default), audio is captured using PulseAudio. If set to `alsa`, audio is captured using the ALSA audio system.
`Rgsender.Audio.Linux.IsVolumeMonitorEnabled`	**NOTE:** Linux only When enabled, RGS Sender tracks volume changes on the sender side, and RGS Receiver adjusts its volume level automatically in response.
`Rgsender.PreferredLicenseOrder`	This property sets the preferred order in which RGS will look for each license type.
`Rgsender.Compatibility.Displays.ConfigureVmwareDisplaysForBestPerformance`	**NOTE:** For VMware® with a Windows guest operating system only When enabled, this property disables the VMware SVGA 3D display at the start of an RGS connection, enables any available NVIDIA displays, and forces the GPU display method to be used. **NOTE:** If this property is enabled, you cannot access any VMware virtual machines via the VMware vSphere® console, because that function requires the VMware SVGA 3D display. To re-enable the VMware SVGA 3D display when an RGS connection ends, use the property `Rgsender.Compatibility.Displays.ReEnableVmwareDisplaysOnRGSDisconnect`. The VMware SVGA 3D display can also be re-enabled by logging out of Windows. This ensures that the vSphere console is accessible when no users are logged on.
`Rgsender.Compatibility.Displays.ReEnableVmwareDisplaysOnRGSDisconnect`	**NOTE:** For VMware with a Windows guest operating system only

Property	Description
	When enabled, this property causes the VMware SVGA 3D display to be re-enabled when an RGS connection ends. This allows you to access a VMware virtual machine via the vSphere console without having to log out of Windows first. **NOTE:** HP recommends disabling this setting if you do not use the vSphere console, because Windows might rearrange your application windows between RGS connections.
`Rgsender.Compatibility.Displays.AllowNvidiaResolutionMatching`	**NOTE:** For Windows-based senders with NVIDIA graphics only When enabled, RGS Sender attempts NVIDIA resolution-matching before attempting the default resolution-matching method.
`Rgsender.KerberosLogon`	**NOTE:** Linux only Allows a Kerberos RGS authentication ticket to be used for login. The username must be selected or entered manually. Possible value are as follows: `Off`: The Kerberos ticket will not be used for login. `On`: The Kerberos ticket will be used for login. `Persist`: The Kerberos ticket can be used for login and will continue to be available for the lifetime of the RGS connection. The ticket can potentially be used for other authentication activities such as unlocking the desktop.

Per-session properties (RGS Receiver only)

The per-session properties of RGS Receiver, which are applicable to Directory Mode only, let you specify settings for each RGS session individually.

NOTE: When typing per-session properties, replace `<n>` with the number of the session. The first session is `0`, the second session is `1`, and so on.

Window location and size properties (per-session)

Property	Description
`Rgreceiver.Session.<n>.RemoteDisplayWindow.X`	This property sets the horizontal position of the RGS Receiver window for session number `<n>`, as measured from the left edge of the primary screen. The default is `0`.
`Rgreceiver.Session.<n>.RemoteDisplayWindow.Y`	This property sets the vertical position of the RGS Receiver window for session number `<n>`, as measured from the top edge of the primary screen. The default is `0`.
`Rgreceiver.Session.<n>.VirtualDisplay.IsPreferredResolutionEnabled`	`1`=Enables the preferred resolution properties for session number `<n>`. If the sender is unable to match the resolution preference of the receiver, a warning dialog is displayed on the receiver. `0`=Disables the preferred resolution properties for session number `<n>` (default). **NOTE:** The per-session preferred resolution properties override the global property `Rgreceiver.IsMatchReceiverResolutionEnabled`.

Property	Description
`Rgreceiver.Session.<n>.VirtualDisplay.PreferredResolutionHeight`	This property sets the preferred height of the resolution for session number `<n>`.
`Rgreceiver.Session.<n>.VirtualDisplay.PreferredResolutionWidth`	This property sets the preferred width of the resolution for session number `<n>`.
`Rgsender.Compatibility.Displays.ForceEdidOnHeadless`	**NOTE:** For Windows-based senders with NVIDIA graphics only. When enabled, RGS Sender attempts to load an EDID if the system is determined to have no physical displays attached. **NOTE:** The Sender must not have any physical displays connected when the Sender service starts otherwise the system will not be considered headless and no EDID will be loaded. **NOTE:** This EDID will remain loaded until the property is disabled and the RGS Sender service is restarted.

Clipboard properties (per-session)

Property	Description
`Rgreceiver.Session.<n>.Clipboard.IsEnabled`	`1`=Enables Remote Clipboard for session number `<n>` (default). The global property `Rgreceiver.Clipboard.IsEnabled` must be enabled for this to have any effect. `0`=Disables Remote Clipboard for session number `<n>`.

Auto-launch properties (Windows only)

Auto-launch files for RGS Receiver have the extension `.rgreceiver` and use the same syntax for setting property values as `rgreceiverconfig` (see Setting RGS properties manually on page 68).

When an auto-launch file is opened, RGS Receiver starts automatically and attempts to establish a connection to a single sender, as configured in the file.

NOTE: Auto-launch files do not support starting RGS connections to multiple senders. For information about connecting to multiple senders, see Directory Mode on page 52.

The following table describes the auto-launch properties. Since you can auto-launch only one connection at a time, the session number should always be 0.

Property	Description
`Rgreceiver.Session.0.IsConnectOnStartup`	If this property is enabled, RGS Receiver will attempt to auto-launch the connection when the auto-launch file is opened.
`Rgreceiver.Session.0.Hostname`	This property sets the hostname or IP address for the auto-launch connection.
`Rgreceiver.Session.0.Username`	This property sets the username for the auto-launch connection as a UTF-8 encoded string.
`Rgreceiver.Session.0.Password`	This property sets the password for the auto-launch connection as a UTF-8 encoded string.
`Rgreceiver.Session.0.PasswordFormat`	`Encrypted`=This password format is supported on Windows only and is the hexadecimal string representation of the password

Property	Description
	encrypted using the Windows command `CryptProtectData`. See http://msdn.microsoft.com/en-us/library/aa380261(VS.85).aspx for more information. `Clear`=This password format is unencrypted text. `XOR`=This password format is the hexadecimal string representation of a password encrypted using an XOR cipher using a key of 129.

Settings from the RGS Receiver Configuration tool (and the `rgreceiverconfig` file) are ignored when you use an auto-launch file, so you need to add any desired property settings to the auto-launch file. See below for an example.

```
Rgreceiver.Session.0.IsConnectOnStartup=1
Rgreceiver.Session.0.Hostname=192.168.0.47
Rgreceiver.Session.0.Username=MyUserName
Rgreceiver.Session.0.Password=MyPassword
Rgreceiver.Session.0.PasswordFormat=Encrypted
Rgreceiver.Network.Timeout.Error=60000
Rgreceiver.Network.Timeout.Warning=4000
Rgreceiver.Network.Timeout.Dialog=30000
Rgreceiver.IsBordersEnabled=0
```

9 Performance optimization

General

The following suggestions apply to all operating systems:

- Enable HP Velocity (see HP Velocity (Windows/Linux only) on page 33 for more information).
- Set the sender desktop background to a solid color to minimize the amount of image data that needs to be sent.
- Set both the receiver and the sender display depth to 32-bits per pixel.
- Lower the sender's display resolution.
- Increase the Max Image Update rate from 30 to 60 using the RGS Sender Configuration tool.
- Reduce the Remote Audio quality setting in RGS Receiver, or disable Remote Audio if it is not needed.

The following suggestion applies to Windows only:

- Adjust the Windows system performance settings in Control Panel. The **Adjust for best performance** option will minimize the bandwidth requirements for RGS.

Network

RGS depends on low network latency and reasonably high network bandwidth. There are several methods to test and measure the network bandwidth, latency, and the number of hops between the receiver and the sender:

- Use the `ping` command to measure network latency.
- Use the `Traceroute` (Linux) or `tracert` (Windows) command, which will report the number of hops it takes to reach a computer in addition to the network latency.
- Use the tools NTttcp Utility, ipref, or something similar, which are available at https://gallery.technet.microsoft.com/NTttcp-Version-528-Now-f8b12769.

Once you've characterized your network performance, you can decide if improvement is required.

The network interface will auto-negotiate the network speed with the network switches on the local network. Most modern network interfaces and switches will negotiate the highest possible speed available. However, unless the network has been carefully designed for maximum throughput, the network interfaces and switches might auto-negotiate to a sub-optimal speed.

If the network interface and switches are configured to auto-negotiate properly, you can leave the settings to auto-negotiate. If you want to force the network to operate at a particular speed, the settings in the network interface and switches can be hard-coded. You must be careful with these settings, however. If the network interface and switch settings don't complement each other, the network will have poor performance.

To configure a network interface to force a particular network speed on Windows:

1. In Control Panel, select **Device Manager**.
2. Expand **Network adapters**.
3. Right-click the network adapter you want to configure, and then select **Properties**.

4. Click the **Advanced** tab.
5. In the list of properties, locate the property that controls the speed and duplex setting. The name can vary, but it is usually something like **Speed & Duplex** or **Link Speed & Duplex**.
6. From the **Value** drop-down list, select the fastest speed your network can support, and be sure to select the **Full Duplex** version of that speed.

To configure a network interface to force a particular network speed on Linux:

- As root, use a command like in the following example. This example sets network interface 0 as a 100 Mb/sec connection running full duplex mode:

```
$ /usr/local/sbin/ethtool -s eth0 speed 100 duplex full autoneg off
```

If you are not satisfied with your network performance, look at the log files on your network switch (if the receiver is connected to one). A significant number of errors on the switch port may indicate that the computer or network is not configured correctly. Work with your IT organization to optimize your computer and network configuration.

10 Troubleshooting

Failed connection attempts

This section describes the most common issues that cause RGS connection attempts to fail.

Receiver checklist

Use the following checklist to troubleshoot failed connection attempts from the receiver side:

1. Verify that you are entering the correct hostname or IP address for the sender.

   If you changed the port that RGS Sender listens on from its default of 42966, you must specify the port number along with the hostname or IP address like in the following examples:

   ```
   MyHostName:12345
   ```

   ```
   192.168.0.10:12345
   ```

2. Verify that the receiver is on the same network as the sender.
3. Verify that the receiver can ping the sender.
4. If the receiver is behind a firewall, verify that the firewall supports network address translation (NAT).

Sender checklist

Use the following checklist to troubleshoot failed connection attempts from the sender side:

NOTE: After going through this checklist, make sure you log out of the sender before attempting an RGS connection again.

1. Verify the credentials for the user account you are trying to access from the receiver. The account password cannot be blank.
2. Verify that RGS Sender has started on the sender (see RGS Sender overview on page 24 for more information).
3. Verify that all tests pass on the Diagnostics panel of the RGS Sender Configuration tool.
4. If the sender is behind a firewall, verify that the firewall supports network address translation (NAT) and port forwarding.
5. If you changed the network interface binding of RGS Sender from its default of listening to all network interfaces, verify that the sender is listening on the correct network interface (see Sender network interface binding on page 77 for more information).
6. **(Windows only)**

   Verify that the sender is not using Automatic Private IP Addressing (APIPA) by typing the following in a command window:

   ```
   netstat -n -a
   ```

If the IP address associated with the RGS Sender listening port (42966 by default) is private, APIPA is the likely cause. For information about how to disable APIPA, go to http://support.microsoft.com/kb/220874.

7. **(Linux only)**

   Verify that the sender is not using an X desktop started on the command line. Outside connection attempts might fail because of incomplete PAM session management and permissions for the console. Login management should be handled by the display manager started by `init` run level 5.

   RGS Sender natively supports the following display managers:

   - GNOME Display Manager (GDM)
   - KDE Display Manager (KDM)
   - LightDM

   If the sender system uses a different PAM-based display manager, you can try the following:

   NOTE: This configuration might not work for some display managers.

   a. Find the configuration files for the display manager in `/etc/pam.d/`.

   b. Add the following line to the end of each file (create a backup of each file before modifying it):

      ```
      session optional pam_rg.so
      ```

   c. Restart the sender system.

Kerberos

Kerberos authentication is available only on a Windows receiver. The receiver must be connected to the same Windows domain as the Windows or Linux sender. Kerberos authentication requires that the RGS Receiver and RGS Sender systems have synchronized clocks. Some tolerance is allowed for clock differences. The tolerance is dependent on parameters setup on the domain controller. In order to allow the Kerberos ticket to be used for login on the sender, the `Rgsender.KerberosLogon` property needs to be set and the domain controller needs to have delegation enabled for the computer. This feature may not be configured for all services. Other PAM services may be able to authenticate with the Kerberos ticket by adding `auth sufficient pam_rg.so` to the associated PAM service in `/etc/pam.d`. This must be added before the authentication line that includes `password-auth` or `system-auth`.

A Linux sender must be identified by the hostname and not an IP address in order for the receiver to obtain the necessary service ticket. The service ticket for a host with the name `hostname.example.com` can be seen by running the command line program `klist` on the receiver. This ticket will be listed with the server name `host/hostname.example.com`.

Sender network interface binding

RGS Sender is set by default to listen to all network interfaces present on the sender. If this is undesirable, the network interface binding can be manually reconfigured.

There are three methods to reconfigure RGS Sender network interface binding:

- Disable the network interfaces that you do not want RGS Sender to listen to, and then restart the sender. RGS Sender will then bind to the remaining enabled network interface. The disadvantage of this method is that the other network interfaces will no longer be usable.
- Manually configure the desired network interface to be the one listened to by RGS Sender. See Reconfiguring network interface binding manually on page 78 for more information.
- Use the RGS Sender Configuration tool to specify which network interface to listen to. See Reconfiguring network interface binding using the RGS Sender Configuration tool on page 78 for more information.

If you enter a hostname instead of an IP address when establishing an RGS connection, it is possible that the hostname will resolve to the IP address of an incorrect network interface. This could be caused by a number of factors, including how your DHCP and DNS servers are configured.

If the hostname resolves to the IP address of an incorrect network interface, do one of the following:

- Enter the IP address that RGS Sender is bound to instead of the hostname when establishing an RGS connection.
- Reconfigure your DHCP and DNS servers so that the hostname resolves to the correct IP address.
- Use the `nslookup` command to determine the IP address that the hostname resolves to, and then follow the steps in Reconfiguring network interface binding manually on page 78 to set the corresponding network interface to be listed first in the list of connections.

Reconfiguring network interface binding manually

To manually configure which network interface the sender binds to:

1. Disable the **Listen for RGS connections on all network interfaces** option in the RGS Sender Configuration tool.

   NOTE: See Using the RGS Sender Configuration tool on page 62 for more information.

2. Click the network icon in the Windows notification area, and then click **Open Network and Sharing Center**.
3. Click **Change adapter settings** in the left pane.
4. Press the Alt key to show the menu bar, select **Advanced**, and then select **Advanced Settings**.
5. In the **Adapter and Bindings** panel, use the arrow buttons next to the **Connections** pane to move the desired network interface to the top of the list.

   The network interface at the top of the list will be the one listened to by RGS Sender.

Reconfiguring network interface binding using the RGS Sender Configuration tool

Before configuring options in the RGS Sender Configuration tool, you'll need to determine the number that corresponds to the network interface you want RGS Sender to listen to. To do this, follow these steps:

1. Click the network icon in the Windows notification area, and then click **Open Network and Sharing Center**.
2. Click **Change adapter settings** in the left pane.

3. Press the Alt key to show the menu bar, select **Advanced**, and then select **Advanced Settings**.
4. In the **Adapter and Bindings** panel, look at the list of network interfaces in the **Connections** pane.

   The number that corresponds to the network interface at the top of the list is **0**. The number for the next network interface in the list is **1**, and so on.

After determining the number that corresponds to the desired network interface, follow these steps to configure the appropriate RGS Sender settings:

1. Disable the **Listen for RGS connections on all network interfaces** option in the RGS Sender Configuration tool.
2. Set the value of the **Listen to a specific network interface** option in the RGS Sender Configuration tool to the number of the desired network interface.

NOTE: See Using the RGS Sender Configuration tool on page 62 for more information.

Network timeouts

The network timeout properties of RGS Receiver and RGS Sender provide a way to handle network disruptions. Although TCP/IP is reliable, it does not guarantee network packet delivery. Possible issues include the following:

- Network over-subscription, resulting in congestion and packet loss
- CPU utilization by other processes and tasks, starving the TCP/IP network stack
- Incorrectly configured or malfunctioning network switches, routers, and network interfaces

See below for a list of timeout-related issues and solutions.

The RGS Receiver window repeatedly dims and displays a connection warning message.

Cause	Solution
There are frequent network disruptions between RGS Receiver and RGS Sender.	If the notifications are occurring too frequently, increase the RGS Receiver warning timeout value.

The RGS Receiver window dims, and RGS Receiver disconnects and displays a connection error, but you can connect again immediately.

Cause	Solution
The length of the network disruption exceeded the error timeout value of either RGS Receiver or RGS Sender. **NOTE:** This could also occur if RGS Sender was stopped unexpectedly.	Increase the error timeout value of RGS Receiver, RGS Sender, or both.

When connecting to a Linux-based sender, the PAM authentication dialog on the receiver does not display long enough for credentials to be entered.

Cause	Solution
The RGS Receiver dialog timeout value is too low.	Increase the dialog timeout value of RGS Receiver.

When connecting to the sender, the authorization dialog is not displayed long enough for the user to respond to it.

Cause	Solution
The collaboration request timeout value of RGS Sender is too low.	Increase the collaboration request timeout value of RGS Sender.

The RGS Receiver window is not updating.

Cause	Solution
A network disruption occurred, but the warning and error timeout values of RGS Receiver are set too high.	Decrease the warning and error timeout values of RGS Receiver.

Increasing the error timeout value of RGS Receiver does not appear to have an effect, and RGS Receiver still disconnects.

Cause	Solution
The error timeout value of RGS Sender is less than that of RGS Receiver.	Increase the error timeout value of RGS Sender so that its higher than that of RGS Receiver.

Graphical issues (Linux)

Full-screen crosshair cursors

Some software uses large crosshair cursors that might not display correctly on the receiver. Full-screen crosshair cursors can be disabled by typing the following in an X terminal:

```
X11xprop -root -remove _SGI_CROSSHAIR_CURSOR
```

Gamma correction on the receiver

The color in a 3D application on the sender can look incorrect when displayed on a receiver. This is because the gamma of the receiver monitor does not match the gamma of the sender monitor.

Any tool that can adjust the gamma for a display can help resolve this issue. Some tools adjust the gamma for the entire display, while others adjust the gamma on a per-window basis. A per-window tool that can adjust the RGS Receiver window only should provide the best results.

Black or blank RGS Receiver window

If the sender is set to less than 24-bit or 32-bit color depth (depending on the graphics adapter), the RGS Receiver window might display a black or blank desktop session. Increase the color depth of and restart the sender usually resolves the issue.

Remote Audio issues

See below for a list of audio-related issues and solutions.

RGS Receiver is not outputting audio.

Cause	Solution
Various	• Verify that Remote Audio is enabled in the RGS Receiver settings. • Verify that audio is not muted by the operating system. • Verify that the audio device of the receiver is working.

Audio is disrupted.

Cause	Solution
The audio quality settings are too high for a low-bandwidth connection.	• Reduce the audio quality. • Disable stereo audio.
The RGS Sender process priority is too low.	Increase the RGS Sender process priority.

Audio causes continuous network traffic.

Cause	Solution
The noise level is too high and being interpreted by RGS as an audio signal.	Lower the volume input setting on or disable any active external devices connected to the Line In audio jack on the sender.

There is no audio on a sender or a receiver with multiple audio devices.

Cause	Solution
RGS is not using the correct audio device.	Disable extra audio devices to make sure RGS uses the correct device.

Remote USB issues

The following information describes Remote USB troubleshooting tips:

- Verify that Remote USB is enabled in RGS Receiver.
- Verify that the USB device is physically connected to the receiver, powered, and turned on.
- Verify that the USB device is detected by the receiver.
  - Windows: Verify that the USB device is listed in Device Manager.
  - Linux: Verify that the USB device is listed in `/proc/devices/usb_remote/devices`. If only one USB device is recognized by the receiver, the `devices` file will have a single file descriptor named `192`, which is the Remote USB device. Dumping this file with the command `cat 192` displays data about the device. If multiple devices are connected, then each will have a file descriptor numbered consecutively starting at `192`.
- Verify that both the sender and the receiver support Remote USB (see Remote USB (Windows/ThinPro only) on page 49).

- Verify that the USB device is supported (see Remote USB (Windows/ThinPro only) on page 49).
- Uninstall and reinstall RGS Receiver to make sure that Remote USB is configured correctly during installation (see Installing RGS Receiver (Windows) on page 6).
- Uninstall and reinstall RGS Sender and make sure that Remote USB is enabled during installation (see Installing RGS Sender (Windows) on page 8).
- Verify that the drivers and software required by the USB device are installed and available on the sender. Many USB devices require manufacturer-supplied software to work. This software must often be installed before the USB device is connected to the computer.

Smart card redirection issues

Consider the following when troubleshooting smart card redirection:

- Verify that the smart card works standalone on both ends of a connection.
- Verify that vendor drivers are installed for the smart card reader and the smart card devices.
- Be sure that only the primary user is attempting to use a smart card.
- Verify that there is only one active smart card connected to the receiver. A virtual smart card is counted as an active smart card.
- If the smart card service on RHEL 7 does not start correctly, you might need to modify the pcscd startup script located at `/usr/lib/systemd/system/pcscd.service`. Open the script for editing and change the ExecStart option to the following:

  ```
  ExecStart=/usr/sbin/pcscd --foreground --auto-exit -c /etc/
  reader.conf.d/hpremotescr.conf
  ```

Mouse Cursor issues on Servers/Blades (Windows Sender)

VMouseSetup.exe must be installed on systems without a physical pointer device (e.g. servers or blade workstations) on Windows 8 and later. VMouseSetup.exe will install a Virtual Pointer Driver to enable HP RGS to correctly display the mouse cursor on systems without a pointer device. VMouseSetup.exe is included in the RGS Install package for the Windows Sender.

A Switching between RGS and Remote Desktop Connection (Windows only)

You can switch between an RGS session and a Windows Remote Desktop Connection session without having to log out of the remote desktop on the sender as long as you use the same credentials for both sessions. The existing session is ended when you start the new session using the other program.

If you try to use *different* credentials to start a Remote Desktop Connection session with a sender that is already in an RGS session, Remote Desktop Connection allows you to force a log off for the remote user account currently in the RGS session. Forcing a log off requires Windows administrator privileges and ends the RGS session.

If you try to use *different* credentials to start an RGS session with a sender that is already in a Remote Desktop Connection session, RGS will display an authorization failure message. You cannot force a log off in this scenario.

IMPORTANT: See the following information about security and authentication concerns:

- If you switch from an active Remote Desktop Connection session to an RGS session, the remote desktop might enter into a logged on and unlocked state. This might not be desirable if an unlocked remote desktop is a security concern. To avoid this, log off of the remote desktop using Remote Desktop Connection before starting the RGS session.
- If you have an active Remote Desktop Connection session that you authenticated using a smart card and try to switch to an RGS session using Easy Login on a receiver other than the one that started the active Remote Desktop Connection session, RGS will prompt you for your username and password, which is not normally required for Easy Login authentication. If you do not know your username and password because you normally use smart card authentication, then you will not be able to switch to an RGS session. In this scenario, the Remote Desktop Connection session must be ended manually to release the smart card reader for use by RGS.

B Creating an agent for remote application termination (Windows only)

When an RGS session is unintentionally ended, you might want applications on the sender to be terminated to prevent them from operating unsupervised.

This appendix describes how to create an agent on the sender that provides remote application termination by monitoring events in the RGS Sender event log `HPRemote`.

Viewing the HPRemote log

To view the HPRemote log:

1. Select **Start**, select **Control Panel**, select **Administrative Tools**, and then select **Computer Management**.
2. In the left pane, select **System Tools**, select **Event Viewer**, and then select **HPRemote**.

The HPRemote log contains information about recent RGS connection activity. By default, the most recent events are listed first.

To view the properties of an event, double-click it to open the Event Properties window.

NOTE: For additional information on Windows event logging, go to Microsoft Developer Network (MSDN) at http://msdn.microsoft.com/.

HPRemote log format

Data in the HPRemote log consists of a message ID followed by optional data in both string and binary formats.

The following table describes the events logged in the HPRemote log. The message IDs are defined in the header file `RGSenderEvents.h` and are 32-bit values. The `EventID` is from the `Code` field within the message ID and, for the HPRemote log, ranges from 1 to 13.

Message ID	Description

`RGSENDER_CONNECT_STATE`
 	
Event ID: 3
	The connection state consists of zero or more **primary** connections and zero or more **non-primary** connections. Each event entry records the current number of active connections in each category. Events appear when the connection status of these of a particular connection changes.
	
	The first field represents the number of primary connections. The second field represents the number of non-primary connections. Each state field provides a string and a 32-bit unsigned integer.
	
	Event viewer message:
	
	`Primary connections: %1. Non-primary connections: %2.`
	
	Strings:
	
	`%1 = number of primary connections`
	
	`%2 = number of non-primary connections`

Message ID	Description

	Data:
	`UINT32 numPrimary`
	`UINT32 numNonprimary`
	Event viewer example:
	`Primary connections: 1. Non-primary connections: 0.`

`RGSENDER_CONNECT`
Event ID: 4
	A new connection was established with an associated name. If Easy Login is enabled, the name assignment will be deferred until login and the associated name may be Anonymous.
	Event viewer message:
	`Connect %1.`
	Strings:
	`%1 = name associated with connection`
	`%2 = IP address and port number of receiver`
	Data:
	`None`
	Event viewer example:
	`Connect MYDOMAIN\myusername.`

`RGSENDER_DISCONNECT`
Event ID: 5
	A receiver has disconnected. The message will contain the name associated with the connection. If Easy Login is enabled and the receiver disconnects prior to a login, the associated name may be Anonymous.
	Event viewer message:
	`Disconnect %1.`
	Strings:
	`%1 = name associated with connection`
	`%2 = IP address and port number of receiver`
	Data:
	`None`
	Event viewer example:
	`Disconnect MYDOMAIN\myusername.`

`RGSENDER_STARTUP`
Event ID: 1
	Reference event registered to aid in interpretation of the event log by Event Viewer. Signifies proper startup of the RGS Sender service.
	Event viewer message:
	`RGS Sender startup.`
	Strings:
	`None`
	Data:
	`None`

`RGSENDER_SHUTDOWN` Event ID: 2	Reference event registered to aid in interpretation of the event log by Event Viewer. Signifies proper shutdown of the RGS Sender service. Event viewer message:

Message ID	Description
	RGS Sender shutdown. Strings: None Data: None
RGSENDER_SET_PRIMARY Event ID: 6	A connection with an associated name is set as the primary connection. Event viewer message: Set %1 as primary connection. Strings: %1 = name associated with connection Data: None Event viewer example: Set MYDOMAIN\myusername as primary connection.
RGSENDER_SET_NONPRIMARY Event ID: 7	A connection with an associated name is assigned to a non-primary status. This may happen as a result of a logout. Event viewer message: Set %1 as non-primary connection. Strings: %1 = name associated with connection Data: None Event viewer example: Set MYDOMAIN\myusername as non-primary connection.
RGSENDER_ASSIGN_USER Event ID: 8	If Easy Login is enabled, the assignment of the name will be deferred until login. When the name is assigned, this message will be generated. Event viewer message: Assign %1 connection to %2. Strings: %1 = original name of connection %2 = new name of connection Data: None Event viewer example: Assign Anonymous connection to MYDOMAIN\myusername.
RGSENDER_USB_CONNECT_DEVICE Event ID: 9	Remote USB mounted a USB device to the sender. Event viewer message:

Message ID	Description
	`USB Device Connect:Class=%1, Vendor ID=%2, Product ID=%3, Manufacturer=%4, Product=%5` Strings: %1 = USB device class %2 = USB device vendor ID %3 = USB device product ID %4 = USB device manufacturer string %5 = USB device product string Data: None
`RGSENDER_USB_DISCONNECT_DEVICE` Event ID: 10	Remote USB unmounted a USB device from the sender. Event viewer message: `USB Device Connect:Class=%1, Vendor ID=%2, Product ID=%3, Manufacturer=%4, Product=%5` Strings: %1 = USB device class %2 = USB device vendor ID %3 = USB device product ID %4 = USB device manufacturer string %5 = USB device product string Data: None
`RGSENDER_CONNECT_USB_DENIED` Event ID: 13	A USB device connection was denied by the USB access control list. Event viewer message: `USB Device Connect:Class=%1, Vendor ID=%2, Product ID=%3,` Strings: %1 = USB device class %2 = USB device vendor ID %3 = USB device product ID Data: None

Agent design guidelines

Designing an agent to provide Remote Application Termination requires consideration of a number of issues in order to minimize data loss and determine when a last-resort shutdown of a disconnected desktop session is required. Listed below are several topics to consider when designing application control agents for your environment. The topics are not exhaustive—use them as a starting point for a more complete design that meets your business requirements.

Desktop session logout

- **Situation**—In some circumstances, loss of a primary user connection should trigger a full shutdown of all applications and force a logout of the desktop session (perhaps after a specified time limit for reconnection has expired). This action would drop all connections to the remote session.
- **Benefit**—Implementing a full desktop session shutdown/logout ensures that all connection activity ceases immediately and ensure that applications are prevented from further unattended actions. Shutdown of a remote session frees the workstation for connection by other users. This approach is the most absolute and secure solution for desktop session management. Agent relies upon Windows logout routines to terminate environment—simple in design and result.
- **Issue**—Forcing a desktop session shutdown/logout can result in data loss for any open applications on the desktop session. Forcing session logouts can result in application alert prompts requiring user interaction to save altered data. These prompts can delay or halt an interactive logout. Session termination also destroys memory of window placement on the desktop, and requires user intervention at restart.

Selective environment shutdown

- **Situation**—Partial shutdown of an environment only terminates specific applications of interest. It does not implement a full desktop session logout. It selectively protects only the most critical applications requiring oversight and control.
- **Benefit**—Preserves the active desktop session for connection at a later time. Selectively terminates the applications of interest. Preserves data not governed by an automated shutdown policy. Supports session recovery with an arbitrary connection time. If done in layers (giving some applications more time to live than others), then a gradual "soft landing" shutdown can occur that ultimately results in a full logout. Idle resources over a specific amount of time can be returned to a remote server pool.
- **Issue**—Potentially more complicated to implement. Can require coordination of multiple agents to handle layered shutdown. May still result in data loss for specific applications. May also require a master semaphore to halt/terminate multiple agents if the user reconnects and wants to stop the shutdown process.

Wrapping applications of interest

- **Situation**—Agents can be launched that supervise only specific applications in a given environment. Tying agents to specific applications is a selective safety net for every user.
- **Benefit**—Application-specific agents can be implemented as plug-ins or support utilities for a given application. In the future, certain software providers may provide custom interfaces for safe shutdown messages from an agent or the operating system. Custom agents can be independently maintained and tied to specific application releases for greater support flexibility. Independent agent design supports unit testing and decouples environmental dependencies.
- **Issue**—Users need specific recourse to disarm an agent if they reconnect. Applications may not interact well with a dedicated agent (and only shutdown due to a global shutdown request). Dedicated agents could possibly be compromised.

Administrator alerts

- **Situation**—Instead of shutting down an environment, an agent can be designed to alert an administrator or operator to determine the status of the user before taking action. This watchdog

approach can further be defined to exploit redundant network connection support to a remote system to allow user-directed shutdowns to occur.

- **Benefit**—System agents are not required to take destructive action—they serve only as alarms and monitors for alternative human intervention.
- **Issue**—May require redundant networking channel. Requires administrator or operator availability to support.

Anticipating user disconnects and reconnects

- **Situation**—Users must first be warned about the consequences of disconnection. Agents that provide protection for a disconnected session may become a nuisance for unsuspecting users if they fail to address protective measures in place for their safety. For example, users must know how much time they have to reconnect before safeguards take action. If a remote agent arms itself for application termination, users should be presented with a large, unmistakable disarming "opt-out" panel that, upon login and discovery, they can halt any agent actions before termination. Organizations should carefully discuss and publicize safety measures due to potential data loss.
- **Issue**— Users should not be able to disable or specify their own timeouts due to potential irreversible data loss.

General agent design guidelines

In developing an agent, HP recommends following these guidelines:

- The agent should externally log its decisions and actions for postmortem analysis.
- Independent agents should provide their own opt-out, disarming dialogs with countdown feedback before taking action.
- Expect the unexpected—where possible, limit your actions to those areas you are certain of the outcomes to minimize loss of data and productivity.
- Always inspect error codes when reading event logs—the reliability of this RGS communication method depends upon the Windows Event Log system. While we have yet to see a failure in this path, we recommend using all information available to its fullest potential.

Recovery settings for the RGS Sender service

This section discusses restart options for RGS Sender and possible interactions of the agent with the sender.

By default, most Windows services are installed without any automatic restart or recovery settings. The same is true for the RGS Sender service.

Restarting the RGS Sender service can help reconnect a lost RGS connection (unless a system error prevents the RGS Sender service from restarting).

When designing the agent, you should consider whether to check for the existence of a running RGS Sender service as an indication of a sufficient primary user connection. If service restarts are programmed for your environment, this test may be unnecessary.

To set the RGS Sender service to restart automatically, you must change its recovery settings on the **Recovery** panel of its properties (right-click the service and select **Properties**).

Actions to take for the first failure, second failure, and subsequent failures are available in the properties menu. The Recovery options include:

- Take No Action
- Restart the Service
- Run a Program
- Restart the Computer

Sample agent

The following sample Windows agent monitors the HPRemote event log and interprets its events. Comments are included in the agent code showing where additional code would be added to determine if the number of primary users has dropped to zero. If so, further code can be added to terminate applications on the sender.

The sample code is a fixed-polling Windows agent that reads and interprets the HPRemote event log. The agent uses two functions:

1. `processEvent(eventServer, eventSource, dwEventNum)`
   - open event log, read event `dwEventNum`, close event log
   - if a valid read, process recognized `EventIDs`, then return
2. `monitorEvents(eventServer, eventSource, seconds)`
   - for a finite number of seconds (or infinite if seconds <= 0) do
   - open event log, read log length, close event log
   - if log has changed, `processEvent()`, else sleep for X ms.

To properly use the function `monitorEvents(...)`, the following strings must be defined in the function call:

- `LPCTSTR eventServer`: if string is defined as "\\\\yourservername", then the log is stored on a remote server - if the string is empty (NULL), then the log is stored locally (note that four backlashes compiles to two in a string constant)
- `LPCTSTR eventSource`: the name of the target event generator, e.g., `rgreceiver`

The sample agent uses Microsoft event logging functions such as `OpenEventLog, ReadEventLog`, and `CloseEventLog`.

The sample agent is listed below. Where noted, user-specific code should be added. The agent header file, `RGSenderEvents.h`, is installed in the RGS Sender installation directory under the following path:

```
\include\RGSenderEvents.h
```

```
#include <windows.h>

#include <stdio.h>

#include "RGSenderEvents.h"

#define BUFFER_SIZE 1024 // safe EVENTLOGRECORD size for now

#define EVENT_SERVER NULL // remote server = "\\\\nodename"; local = NULL

#define EVENT_SRC "rgsender" // specifies specific event name source
in // HPRemote

BOOL processEvent(LPCTSTR eventServer, LPCTSTR eventSource, DWORD
dwEventNum)
```

```
{
HANDLE h;
EVENTLOGRECORD *pevlr;
BYTE bBuffer[BUFFER_SIZE];
DWORD dwRead, dwNeeded;
BOOL result;
// Open, read, close event log ============================================
if ((h = OpenEventLog(eventServer, eventSource)) == NULL)
{
... report error status ...
return true;
}
// Set the pointer to our buffer. Strings and data will get appended to
the EVENTLOGRECORD structure.
pevlr = (EVENTLOGRECORD *) &bBuffer
// Read the event specified by dwEventNum
result = ReadEventLog(h, // event log handle
EVENTLOG_SEEK_READ | // start at specific event
EVENTLOG_FORWARDS_READ, // advance forward
dwEventNum, // record to read
pevlr, // pointer to buffer
BUFFER_SIZE, // size of buffer
&dwRead, // number of bytes read
&dwNeeded); // bytes in next record
if (CloseEventLog(h) == false)
{
... report error status ...
return true;
}
// Process event (example: print out event) ==============================
if (result)
{
// We only know how to process specific events
if (pevlr->EventID == RGSENDER_CONNECT_STATE)
```

```
{
// Retrieve the two UINT32 fields of this message
// representing primary and non-primary connections.
unsigned int *pData = (unsigned int *)
((LPBYTE) pevlr + pevlr->DataOffset);
// Examine state of primary connections here for other
// agent response if number drops to zero...
... example only prints out retrieved record to console ...
printf ("Event: %u Primary: %u Secondary: %u\n",
dwEventNum, pData[0], pData[1]);
}
... Process other events here if desired ...
}
else
{
... report unrecognized event here ...
return true;
}
return false;
}
void monitorEvents(LPCTSTR eventServer, LPCTSTR eventSource, int seconds)
{
DWORD dwCurrentIndex = 0;
DWORD dwCurrentStart;
DWORD dwCurrentCount;
DWORD dwNewIndex;
int waitedFor;
// This function will monitor the log for the specified number of
// seconds. If seconds is less than zero, we will wait forever.
for (waitedFor = 0; seconds < 0 || waitedFor < seconds; )
{
HANDLE h;
// Open, read status of log, close event log ========================
if ((h = OpenEventLog(eventServer, eventSource)) == NULL)
```

```
{
... report error status here ...
return;
}
// If an event is added, either the start or count will change.
// Get the start and count. Microsoft does not specify what
// reasons these functions could fail, so we cannot ensure
// success. Check the return value.
if (GetOldestEventLogRecord(h, &dwCurrentStart) == false ||
GetNumberOfEventLogRecords(h, &dwCurrentCount) == false)
{
CloseEventLog(h);
... report error - unable to obtain event logs ...
return;
}
if (CloseEventLog(h) == false)
{
... report error status here ...
return;
}
// Determine state of log change ====================================
// Compute the index of the last event. If the count is zero, then
// there are no events and the index is 0.
if (dwCurrentCount == 0)
{
dwNewIndex = 0;
}
else
{
dwNewIndex = dwCurrentStart + dwCurrentCount - 1;
}
// If the new index is different than the current, update the current
// and process the current event. Otherwise, we sleep for a while.
if (dwNewIndex != dwCurrentIndex)
{
```

```
// We have at least one new event. Print out the last event.
dwCurrentIndex = dwNewIndex;
if (dwNewIndex)
{
if (processEvent(eventServer, eventSource, dwCurrentIndex))
{
... event processing error here ...
return;
}
}
}
else
{
// No new events. Sleep for 1 second.
Sleep(1000);
waitedFor += 1;
}
}
return;
}
main( ... )
{
... setup and initialize agent ...
monitorEvents(EVENT_SERVER, EVENT_SRC, seconds);
... cleanup agent here or send alerts ...
... may wish to return status from monitorEvents ...
}
```

C Uninstalling RGS

Uninstalling RGS Receiver or RGS Sender (Windows)

▲ Open the **Programs and Features** item in Control Panel, and uninstall the entry corresponding to RGS Receiver or RGS Sender (**Remote Graphics Receiver** or **Remote Graphics Sender**).

TIP: You can alternatively perform each uninstallation using the command-line option `/autoremove` for each installer.

Uninstalling RGS Receiver (Linux)

To uninstall RGS Receiver on Red Hat Enterprise Linux or SUSE Linux Enterprise Desktop (SLED):

1. Log in as root.
2. Execute the following command to determine the name of the RPM package for RGS Receiver:

   ```
   rpm -q -a | grep -i rgreceiver
   ```

   The package name will be something similar to `rgreceiver_linux_32-5.1-0`.
3. Execute the following command to remove the RPM package for RGS Receiver:

   ```
   rpm -e --allmatches rgreceiver_linux_32
   ```

To uninstall RGS Receiver on HP ThinPro:

1. Log in as root.
2. Execute the following commands:

   ```
   fsunlock
   ```

   ```
   dpkg -l | grep -i rgs-
   ```

   The RGS Receiver core package and dependency packages are listed.

NOTE: A package named findutils might also be listed because of the letters "rgs" appearing in the package description. Do not remove this package.

3. Execute the following command to remove the listed packages:

   ```
   dpkg -P <package name> [<package name> ...]
   ```

IMPORTANT: When inputting package names, omit the brackets and braces. For syntax help, see User input syntax key on page iii.

4. Execute the following command:

   ```
   ln -snf ../tmp/tmpfs/var/opt /var/opt
   ```

5. Restart the thin client.

NOTE: Beginning with ThinPro 7.0, the hptc-rgs-usb package is installed by default with the OS. Do not remove this package.

Uninstalling RGS Sender (Linux)

1. Log in as root.
2. If the default installer (`install.sh`) was used for installation, then execute the following command to determine the names of the RGS Sender packages to remove:

   ```
   rpm -q -a | grep -i rgsender
   ```

   The package names will be something similar to the following:

   - `rgsender_linux_64-7.3.0-1`
   - `rgsender_config_64-7.3.0-1`
   - `rgsender_smartcard-7.3.0-1`

3. Execute the following command to remove the RGS Sender packages:

   ```
   rpm -e --allmatches rgsender_linux_64 rgsender_config_64
   rgsender_smartcard
   ```

IMPORTANT: If `rgsender_config_64-*.rpm` is installed, it must be removed either simultaneously with or prior to the removal of `rgsender_linux_64-*.rpm`. The above command removes both packages simultaneously. This resolves dependencies between the packages and undoes any configuration file modifications the package made automatically during installation.

Uninstalling RGS Receiver (Mac OS)

1. Log in as an administrator (or be able to provide administrator credentials).
2. Open a Finder window, and then select **Applications**.
3. Drag the **HP RGS Receiver** icon to the trash bin.
4. (Optional) To remove all traces of RGS Receiver after uninstalling it, navigate to **/Library/Application Support/HP/rgreceiver/uninstall.command**, double-click **uninstall.command**, and then follow the on-screen instructions.

Index

S

T

U

V

W