



# HP Remote Graphics Software 7.0

User Guide

© Copyright 2014 Hewlett-Packard  
Development Company, L.P.

Microsoft, Windows, and Windows Vista are  
trademarks of the Microsoft group of  
companies.

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

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

Third Edition: December 2014

First Edition: June 2014

Document Part Number: 773127-003

## Acknowledgments

**HP Remote Graphics Software was developed using several third party products including, but not limited to:**

**OpenSSL:** This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)). This product includes cryptographic software written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com))

**Jack Audio Connection Kit (JACK):** JACK is a low-latency audio server, written for POSIX conformant operating systems such as GNU/Linux and Apple OS X. JACK is released in source code format under the GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999. JACK is used in the HP Remote Graphics Software Receiver for Linux.

The HP Remote Graphics Sender for Windows uses Microsoft Detours Professional 2.0. Detours is Copyright 1995-2004, Microsoft Corporation. Portions of the Detours package may be covered by patents owned by Microsoft corporation.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

Portions of this software were originally based on the following: software copyright (c) 1999, IBM Corporation, <http://www.ibm.com>.

Where required, related source code and licenses are re-distributed with HP Remote Graphics Software.



## About this guide

This guide uses the following styles to distinguish elements of text:

Style	Definition
<code>&lt;variable&gt;</code>	Variables or placeholders are enclosed in angle brackets. For example, replace <code>&lt;pathname&gt;</code> with the appropriate path, such as <code>C:\Windows\System</code> . When typing the actual value for the variable, omit the brackets.
<code>[optional parameters]</code>	Optional parameters are enclosed in square brackets. When specifying the parameters, omit the brackets.
<code>"literal value"</code>	Command line text that appears inside quotation marks should be typed exactly as shown, including the quotation marks.



---

# Table of contents

<b>1 Getting started in Windows .....</b>	<b>1</b>
<b>2 RGS overview .....</b>	<b>2</b>
Typical RGS deployment .....	3
User interface overview .....	4
RGS Receiver Control Panel .....	4
Remote Display Window .....	5
Remote Display Window toolbar .....	6
RGS features .....	7
RGS Sender and RGS Receiver interoperability .....	9
RGS licensing .....	9
Connection types .....	9
Multi-monitor configurations .....	10
RGS login methods .....	10
Standard Login .....	10
Easy Login .....	11
Single Sign-on .....	11
Deciding between Easy Login and Single Sign-on .....	11
<b>3 Installing and activating RGS .....</b>	<b>12</b>
Installing RGS on Windows .....	12
Installing the RGS Receiver on Windows .....	12
Manual installation of the RGS Receiver on Windows .....	12
Automatic installation of the RGS Receiver on Windows .....	13
Command line syntax .....	13
RGS Receiver installation command line options .....	14
RGS Receiver installation log file .....	15
Uninstalling the RGS Receiver on Windows .....	15
Installing the RGS Sender on Windows .....	15
Prerequisites for RGS Sender installation on Windows .....	15
Manual installation of the RGS Sender on Windows .....	16
Automatic installation of the RGS Sender on Windows .....	16
Command line syntax .....	16
RGS Sender installation command line options .....	17
RGS Sender installation log file on Windows .....	18
Uninstalling the RGS Sender on Windows .....	18

Installing RGS on Linux .....	18
Installing the RGS Receiver on Linux .....	19
RGS Receiver audio requirements on Linux .....	19
Uninstalling the RGS Receiver on Linux .....	19
Installing the RGS Sender on Linux .....	20
Manually disabling Easy Login on Linux .....	21
Uninstalling the RGS Sender on Linux .....	22
<b>4 Pre-connection checklist .....</b>	<b>23</b>
Local computer checklist .....	23
Remote computer checklist .....	23
RGS Sender network interface binding .....	25
Reconfiguring network interface binding manually .....	26
Reconfiguring network interface binding using RGS Sender properties .....	26
Using RGS through a firewall .....	26
Remote computer power saving states .....	27
<b>5 Using the RGS Receiver .....</b>	<b>28</b>
Starting the RGS Receiver .....	28
RGS Receiver command line options .....	28
Creating an RGS connection .....	29
Using touch features (Windows 8 only) .....	30
Setup Mode (non-touch displays only) .....	31
<b>6 RGS Receiver Control Panel settings .....</b>	<b>32</b>
Connection settings .....	33
Performance settings .....	34
Gesture settings (Windows 8 only) .....	35
Audio settings .....	35
Network settings .....	36
Hotkey settings .....	36
Changing the Setup Mode hotkey sequence (non-touch displays only) .....	37
Logging settings .....	37
Statistics .....	38
<b>7 Using the RGS Sender .....</b>	<b>39</b>
Starting and stopping the RGS Sender on Windows .....	39
RGS Sender command line options on Windows .....	39
Starting the RGS Sender on Linux .....	40
RGS Sender GUI (Windows only) .....	41



Setting the RGS Sender process priority (Windows only) .....	41
Using the RGS Diagnostics Tool (Windows only) .....	41
Using the RGS Admin Tool (Windows only) .....	42
RGS Sender logging (Windows only) .....	42
<b>8 Advanced RGS features .....</b>	<b>43</b>
Collaboration .....	44
Creating a collaboration session .....	44
Collaboration notification dialog .....	45
Optimizing RGS performance .....	45
Advanced performance features .....	45
Performance tuning for all operating systems .....	46
Performance tuning for Windows .....	46
Configuring your network for optimal performance .....	46
Display resolution and layout matching .....	47
Matching display resolution and layout on Windows .....	47
Creating and applying an EDID file on Windows .....	48
Adding custom resolutions on Windows .....	48
Matching display resolution and layout on Linux .....	49
Configuring the X server .....	49
Scenario 1: All receiving computers have the same configuration .....	50
Scenario 2: Receiving computers have different configurations .....	50
Creating an EDID file on Linux .....	51
Remote Audio .....	51
Remote Audio on Windows .....	51
Remote Audio on Linux .....	52
Configuring audio on Linux .....	53
Disabling audio on the remote computer .....	54
Remote Clipboard .....	54
Remote USB .....	54
Local/Remote USB overview .....	55
Auto-remoting .....	55
Supported USB devices .....	56
Remoting USB microphones .....	56
Unique smart card handling .....	57
Remote USB Access Control List .....	58
Determining USB device information .....	59
Determining USB device information for Windows .....	59
Determining USB device information for Linux .....	60
Verifying the USB data .....	60
Using RGS in Directory Mode (non-touch displays only) .....	61

Directory file format .....	61
Starting the RGS Receiver in Directory Mode .....	62
Game Mode (non-touch displays only) .....	63
Auto-launching connections .....	64
RGS Sender event logging (Windows only) .....	64
Viewing the HPRemote log .....	64
Additional information on event logging .....	65
Remote application termination .....	65
HPRemote log format .....	65
Agent design issues .....	69
Desktop session logout .....	69
Selective environment shutdown .....	69
Wrapping applications of interest .....	69
Administrator alerts .....	70
Anticipating user disconnects and reconnects .....	70
General agent design guidelines .....	70
Additional features for Windows systems .....	70
RGS Sender Service Recovery Settings .....	70
Microsoft Remote Desktop Recovery .....	71
Sample agent .....	71
Interoperability of RGS and Microsoft Remote Desktop Connection .....	76
RGS security features .....	76
Remote computer monitor blanking operation .....	77
Linux connection considerations .....	78
Full-screen crosshair cursors .....	78
Gamma correction on the local computer .....	78
Black or blank connection session with the RGS Sender on Linux .....	78
<b>9 RGS properties .....</b>	<b>80</b>
Property syntax .....	81
Setting property values in a configuration file .....	81
Setting properties on the command line .....	81
RGS Receiver properties .....	82
RGS Receiver property setting hierarchy .....	82
RGS Receiver global properties .....	82
Remote Display Window properties .....	82
Experience properties .....	84
Browser properties .....	85
Audio properties .....	85
Microphone properties .....	85
USB properties .....	86

Network properties .....	86
Hotkey properties .....	87
Clipboard properties .....	88
Logging properties .....	88
Registration properties .....	89
Proxy server properties .....	89
RGS Receiver per-session properties .....	89
Auto-launch properties (per-session) .....	89
Window location and size properties (per-session) .....	90
Clipboard properties (per-session) .....	91
RGS Sender properties .....	91
<b>Appendix A Supported hardware and software .....</b>	<b>95</b>
RGS support matrix .....	95
Advanced Video Compression requirements .....	96
Remote Audio device support on Linux .....	96
Keyboard locale support .....	97
Application support .....	98
Video overlay surfaces .....	98
<b>Appendix B Troubleshooting .....</b>	<b>99</b>
Potential issues and suggestions .....	99
Troubleshooting network timeouts .....	99
RGS Receiver network timeout .....	99
RGS Sender network timeout .....	100
Network timeout issues .....	101
Troubleshooting graphics performance .....	102
Troubleshooting Remote Audio .....	102
Troubleshooting Remote Clipboard .....	103
Troubleshooting Remote USB .....	104
Computers supporting Remote USB .....	104
Supported USB devices .....	104
Enable Remote USB .....	104
Check USB cable connections .....	104
Reset the USB device .....	105
HP Remote Virtual USB Driver .....	105
USB device drivers and program support .....	105
RGS error messages .....	105

<b>Appendix C HP support .....</b>	<b>108</b>
Obtaining HP support .....	108
Additional RGS documents .....	108
<b>Index .....</b>	<b>109</b>


---

# 1 Getting started in Windows

The chapter provides a quick guide for Windows users to install and use HP Remote Graphics Software (RGS) in common scenarios.

To install RGS:


---

 **IMPORTANT:** Be sure you are logged in to an account with administrator privileges before performing installation:

---

1. Install the RGS Sender on the remote computer using the default options.
2. Install the RGS Receiver on the local computer using the default options.

---

 **NOTE:** For information about more advanced installation options, see [Installing RGS on Windows on page 12](#).

---

To start the RGS Receiver:


▲ Windows 7: Select **Start > All Programs > HP > HP Remote Graphics Software > HP RGS Receiver**.

Windows 8: Select the **HP RGS Receiver** tile on the Start screen.

To create an RGS connection:

1. In the **Hostname or IP address** field, type the hostname or IP address of the remote computer that is on the same network and has the RGS Sender installed, and then press **Enter** or click **Connect**.
2. Type the username and password in the fields, and click **OK**.


---

 **NOTE:** The username and password are the same credentials that you would use to log in to Windows on the remote computer.

---

If the connection succeeds, the Remote Display Window will appear and display the desktop session of the remote computer.

---

 **NOTE:** If the remote desktop is locked, you will need to enter your credentials a second time to unlock it. If the prompt instructs you to press **Ctrl+Alt+Del** to initiate this process, you must instead press **Ctrl+Alt+End** to trigger the desired response on the remote computer. Pressing **Ctrl+Alt+Del** will always trigger a response on the local computer.

---

---

## 2 RGS overview

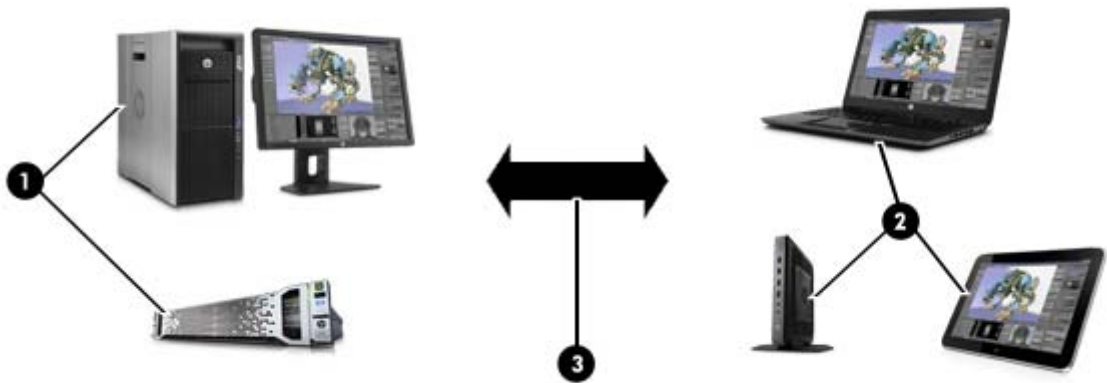
This chapter discusses the following topics:

- [Typical RGS deployment](#)
- [User interface overview](#)
- [RGS features](#)
- [RGS Sender and RGS Receiver interoperability](#)
- [RGS licensing](#)
- [Connection types](#)
- [Multi-monitor configurations](#)
- [RGS login methods](#)

# Typical RGS deployment

RGS is the collaboration and remote desktop solution for serious workstation users and their most demanding applications. All applications 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 a window on a local computer using advanced image compression technology specifically designed for digital imagery, text, and high frame rate video applications. Local keyboard, mouse, and touch inputs are supported, as well as redirection of most USB devices to provide an interactive, high-performance workstation experience.

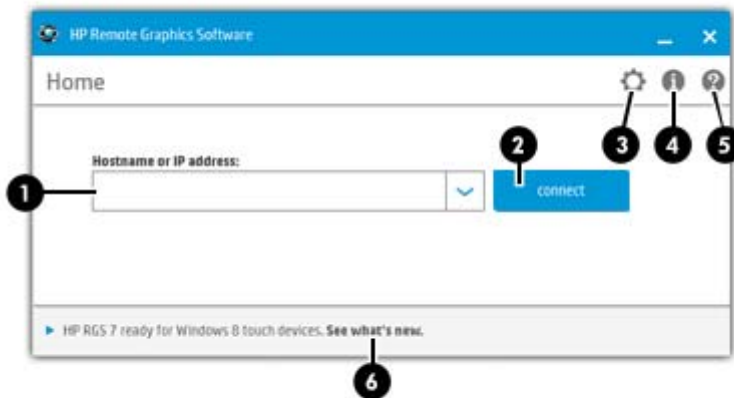
The following image shows a typical RGS deployment.



- 
- 1 Remote computer**—A high-performance workstation, virtual workstation, blade, or server hosts the user's applications and the RGS Sender, which transmits graphics, audio, and USB data to the RGS Receiver on the local computer. The remote computer receives and processes keyboard events, mouse events, and USB data from the local computer.  
**NOTE:** The RGS Sender operates independently of whether or not a monitor is actually connected to the remote computer.
  - 2 Local computer**—A desktop, notebook, tablet, or thin client hosts the RGS Receiver, which establishes a connection to the remote computer and displays the desktop of the remote computer inside a window or full screen on the local computer. The local computer transmits keyboard and mouse events to the remote computer, allowing the user to interact with their applications remotely.
  - 3 TCP/IP network**—Serves as the communication link between the remote computer and local computer.
-

# User interface overview

## RGS Receiver Control Panel




- 
- 1 In this field, enter the hostname or IP address of the remote computer running the RGS Sender. You can also click the down arrow to display a list of recent entries.
  - 2 Initiates the RGS connection.
  - 3 Displays advanced options.  
**NOTE:** For more information, see [RGS Receiver Control Panel settings on page 32](#).
  - 4 Displays the RGS version number, technical information, and the End User License Agreement (EULA).
  - 5 Displays the *HP Remote Graphics Software User Guide* (this document).
  - 6 Displays information about RGS touch features.  
**NOTE:** For more information, see [Using touch features \(Windows 8 only\) on page 30](#).
-



## Remote Display Window

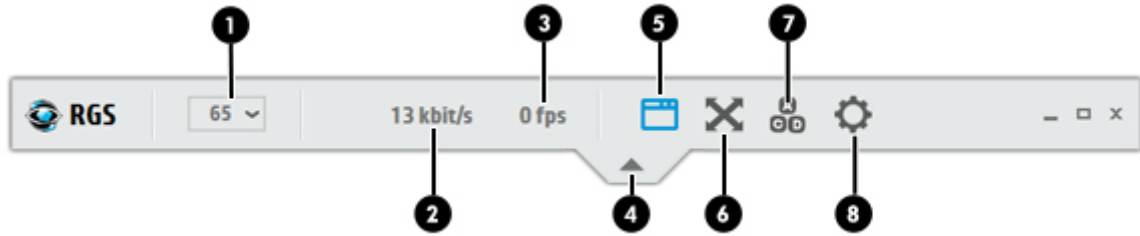


 **NOTE:** The Remote Display Window might look slightly different on touch displays.

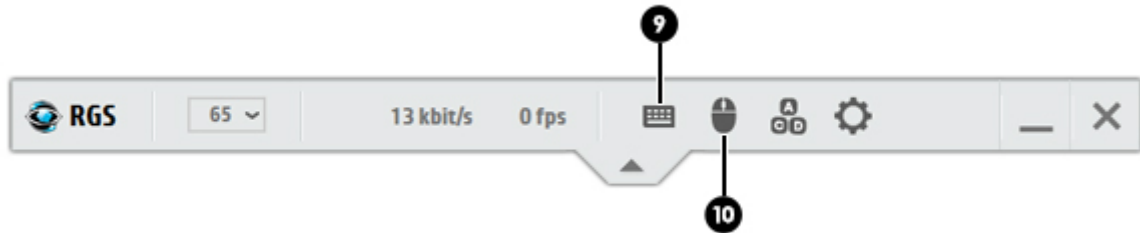
- 1 The Remote Display Window toolbar provides easy access to the most frequently used options. For more information about the individual toolbar items, see [Remote Display Window toolbar on page 6](#).
- 2 Scroll bars appear if the resolution of the remote computer is larger than the size of the Remote Display Window.

# Remote Display Window toolbar

## Non-touch displays



## Touch displays



- 
- 1 Sets the image quality and the amount of compression. Higher image quality reduces the amount of compression and therefore consumes greater network bandwidth.  
**NOTE:** This control is duplicated in the **Performance** tab of the RGS Receiver settings.

---

  - 2 Displays the current network bandwidth consumed by the connection.

---

  - 3 Displays the number of image updates in frames per second for the connection.

---

  - 4 Shows or hides the toolbar.  
**TIP:** The position of this button on the toolbar can be moved by dragging it.

---

  - 5 Adds or removes window borders on the Remote Display Window (non-touch displays only).

---

  - 6 Toggles Setup Mode (non-touch displays only). For more information, see [Setup Mode \(non-touch displays only\) on page 31](#).

---

  - 7 Sends the **Ctrl+Alt+Del** key sequence to the remote computer.  
**NOTE:** Some key sequences, such as **Ctrl+Alt+Del**, are trapped by the local computer and are not forwarded to the remote computer. This button allows you to send a **Ctrl+Alt+Del** sequence to the remote computer without using the keyboard.

---

  - 8 Displays advanced options. For more information, see [RGS Receiver Control Panel settings on page 32](#).

---

  - 9 Opens the virtual keyboard (touch displays only). For more information, see [Using touch features \(Windows 8 only\) on page 30](#).

---

  - 10 Enables the virtual mouse (touch displays only). For more information, see [Using touch features \(Windows 8 only\) on page 30](#).  
**TIP:** The virtual mouse can also be enabled and disabled using the 4-finger tap gesture.
-

# RGS features

The following tables describe many of the RGS features that are designed to optimize functionality, performance, and security.

**Table 2-1 RGS functionality features**

Feature	Description
3D application support	OpenGL 3D applications can be run on the remote computer. Direct3D applications are also supported if they are not in full-screen mode.
Collaboration	Multiple users can simultaneously connect to the same remote computer, allowing them to view and interact with the same desktop session and applications.  See <a href="#">Collaboration on page 44</a> for more information on using and specific support this feature.
Directory Mode	Directory Mode enables you to connect to multiple remote computers at the same time.  See <a href="#">Using RGS in Directory Mode (non-touch displays only) on page 61</a> for more information on using and specific support this feature.
Login methods	RGS provides several different login methods to support various deployments.  See <a href="#">RGS login methods on page 10</a> for more information.
Remote Audio	Smooth, continuous, low-latency, high-quality audio is transmitted from the remote computer to the local computer.  See <a href="#">Remote Audio on page 51</a> for more information on using and specific support this feature.
Remote Clipboard	This feature allows you to cut, copy, and paste data between the local and remote computers or between two different remote computers.  See <a href="#">Remote Clipboard on page 54</a> for more information on using and specific support this feature.
Remote USB	USB devices connected to the local computer can be virtually attached to and accessed by the remote computer.  See <a href="#">Remote USB on page 54</a> for more information on using and specific support this feature.
Touch support	The RGS Receiver supports touch displays and a variety of gestures. Hotkey sequences can also be mapped to gestures for keyboard-less environments.  See <a href="#">Using touch features (Windows 8 only) on page 30</a> for more information on using and specific support this feature.

**Table 2-2 RGS performance features**

Feature	Description
Advanced Video Compression	This option uses a modern video codec to greatly reduce the network bandwidth needed for high-quality video streams.  <b>IMPORTANT:</b> See <a href="#">Advanced performance features on page 45</a> for information about the recommended usages of this feature.
HP Velocity	This option improves performance over poor network connections.

**Table 2-2 RGS performance features (continued)**

Feature	Description
	See <a href="#">Advanced performance features on page 45</a> for more information.
Selective screen updates	When Advanced Video Compression is not selected, only the portions of the screen that change are captured, compressed, and transmitted from the remote computer to the local computer, further improving performance.

**Table 2-3 RGS security features**

Feature	Description
Encryption	RGS supports AES 256 encryption of the pixel data sent from the remote computer to the local computer.
Event logging	Network outages or loss of connectivity between a local and a remote computer can leave a desktop session running without supervision. To safeguard running applications, customer-designed agents can monitor the status of connections to determine if termination of applications is required. Event logging provides a mechanism for agents to determine the status of the connection.  See <a href="#">RGS Sender event logging (Windows only) on page 64</a> for more information about using this feature.
Remote computer monitor blanking	The remote computer's monitor will blank to black by default when an RGS connection is established.  See <a href="#">Remote computer monitor blanking operation on page 77</a> for more information.

For a more detailed list of RGS security features, see [RGS security features on page 76](#).

# RGS Sender and RGS Receiver interoperability

RGS provides interoperability between an RGS Sender and RGS Receiver that have the same primary version number. A connection should only be attempted when their primary version numbers are the same.

See below for a description of the RGS version number components.



---

1	<b>Primary release number</b> —A primary release contains sufficient changes such that interoperability with the prior primary release is not guaranteed. For example, RGS Sender version 6.x.x is not guaranteed to interoperate with RGS Receiver version 7.x.x.
2	<b>Minor release number</b> —Minor releases introduce new RGS features and functionality. Minor releases will also include (roll up) the changes in any prior patch releases.
3	<b>Patch release number</b> —Patch releases are generated only for a security issue or for a major defect in a feature. A patch release is indicated by this number being non-zero.

---

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

---

## RGS licensing


For information about RGS licensing, see the *HP Remote Graphics Software Licensing Guide*, available at <http://www.hp.com/go/rgs>.

## Connection types

The following connection types are supported by RGS:

- **One-to-one connection**—The simplest RGS connection type is between an RGS Receiver on a single local computer and an RGS Sender on single remote computer. The entire frame buffer of the remote computer is displayed in the Remote Display Window on the local computer. See [Creating an RGS connection on page 29](#) for more information.
- **One-to-many connection (collaboration)**—This RGS connection type allows the entire frame buffer of a remote computer to be transmitted by the RGS Sender to multiple local computers, each running the RGS Receiver. This configuration is ideal for collaboration because multiple users can simultaneously view and interact with the same desktop session and applications. See [Collaboration on page 44](#) for more information.
- **Many-to-one connection (Directory Mode)**—This RGS connection type allows an RGS Receiver on a single local computer to connect to multiple remote computers, each running the RGS Sender. The frame buffer of each remote computer is displayed in a separate Remote Display Window on the local computer. This connection type is achieved using Directory Mode. See [Using RGS in Directory Mode \(non-touch displays only\) on page 61](#) for more information.

## Multi-monitor configurations

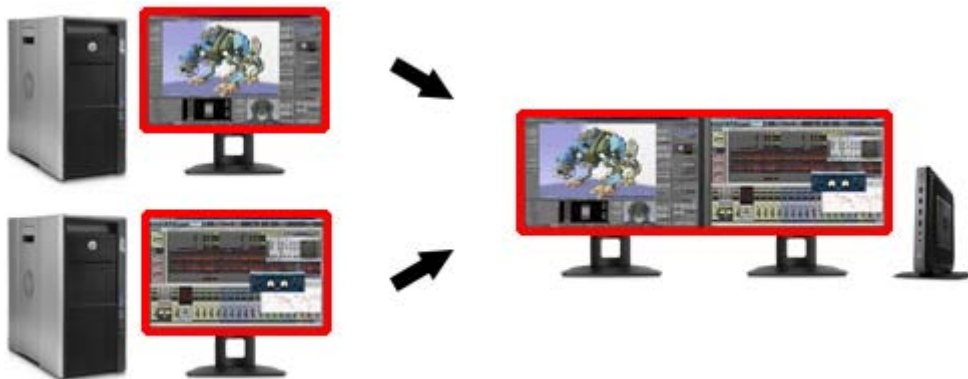
 **NOTE:** Advanced Video Compression is not supported on multi-monitor configurations.

Many computers have a frame buffer that is larger in size (as measured in horizontal pixels by vertical pixels) than what can be displayed on a single monitor. During an RGS connection, the remote computer transmits its entire frame buffer.

For the local user to view the complete desktop of the remote computer, the local computer must have a comparably-sized frame buffer, which will typically require two monitors to view (see the image below).



Multiple monitors on the local computer are also useful for a many-to-one connection. If the local computer is connected to two remote computers, each remote computer frame buffer can be displayed on its own monitor if the local computer has two monitors (see the image below).



## RGS login methods

RGS provides three methods for the local user to log in to a remote computer:

- **Standard Login**—supported for the Windows and Linux versions of the RGS Sender.
- **Easy Login**—supported for the Windows and Linux versions of the RGS Sender.
- **Single Sign-on**—supported for the Windows version of the RGS Sender.

On Windows, the login method is selected during installation of the RGS Sender and can be changed later using the RGS Admin Tool (see [Using the RGS Admin Tool \(Windows only\) on page 42](#)).

On Linux, Easy Login can be enabled during installation and disabled using an RGS Sender property (see [Manually disabling Easy Login on Linux on page 21](#)).

### Standard Login

Standard Login is the process by which a local user attempts to connect to a remote computer 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 local computer to a remote computer. The two steps are as follows:

1. The first authentication step is from the RGS Receiver to the RGS Sender. The dialog for this authentication step is generated and displayed by the RGS Receiver on the local computer.
2. The second authentication step is when logging in to or unlocking the remote computer desktop session. The login or unlock dialog is generated by the remote computer and is displayed in the Remote Display Window on the local computer.



**NOTE:** If another user is already logged in to the remote computer, 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 44](#) for more information).

## Easy Login

With Easy Login, the RGS authentication step is skipped, and you only need to log in to the remote desktop once the Remote Display Window appears.

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 connection to the RGS Sender. The RGS Diagnostics Tool can help troubleshoot these issues. See [Using the RGS Diagnostics Tool \(Windows only\) on page 41](#) for more details.

## Single Sign-on

With Single Sign-on, the RGS authentication step is used and automatically unlocks the remote desktop once you are authenticated.

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.

## Deciding between Easy Login and Single Sign-on

When selecting between Easy Login and Single Sign-on, there are some factors to consider:

- **Windows**

Easy Login on Windows uses credential providers to allow the user to be authenticated through their standard username/password mechanism or using smart card or ActivKey technologies. Single Sign-on does not support smart card or ActivKey technologies. The only credential providers supported when using Easy Login are the Microsoft Password Credential Provider and the Microsoft Smartcard Credential Provider.

For example, if a smart card or ActivKey is not connected to the system, the user will be authenticated through their standard username/password mechanism. However if a smart card or ActivKey is connected to the system, Easy Login will use that device to authenticate the user.

- **Linux**

If the RGS Sender is on Linux, Easy Login is supported but Single Sign-on is not.

---

## 3 Installing and activating RGS

This chapter describes the following aspects of installing RGS:

- [Installing RGS on Windows](#)
- [Installing RGS on Linux](#)

### Installing RGS on Windows

This section describes installation of the RGS Receiver and RGS Sender on Windows. See [Supported hardware and software on page 95](#) for a list of the Windows operating systems that support the RGS Receiver and Sender.

If you plan to use Advanced Video Compression, see [Advanced Video Compression requirements on page 96](#). Meeting these requirements is essential to having a quality experience when using this feature.


### Installing the RGS Receiver on Windows

This section describes manual and automatic installation of the RGS Receiver on Windows.

#### Manual installation of the RGS Receiver on Windows

To install the RGS Receiver on Windows:

---

 **IMPORTANT:** Be sure you are logged in to an account with administrator privileges before performing installation:

---

1. Run the RGS Receiver installer, and follow the on-screen instructions.
2. During the installation, the Remote USB Configuration dialog is displayed.


The three Remote USB Configuration options are:

- **USB devices are Local**—All USB devices will remain local and will be accessible only by the local computer. None of the USB devices will be accessible by a remote computer.
- **USB devices are Remote**—All USB devices can be accessed by the remote computer, and none of the USB devices can be accessed by the local computer.
- **USB devices are Local/Remote**—Whether USB devices are locally or remotely accessible depends on when they are plugged into the local computer relative to establishment of an RGS connection (see [Auto-remoting on page 55](#) for more information).


Select the USB configuration option that meets your needs, and click **Next**.


To see additional information, select **I'm not sure, I want more information**, and click **Next**.

---


 **NOTE:** The Remote USB configuration cannot be changed after installation of the RGS Sender and Receiver. To select a different USB configuration option, the RGS Sender or Receiver must be uninstalled and reinstalled.



 **NOTE:** The "auto" option described in [Auto-remoting on page 55](#) alters the behavior you select during installation. It will re-enumerate any device marked as auto on connect and disconnect. For instance, you have a USB key device that you have marked "auto". Until the local computer is started, it will be attached to the local system. Once the local computer starts and makes a connection to a remote computer, it will be remoted to the remote system. Upon disconnect, it will be given back to the local system.


 **NOTE:** For many USB devices, the Windows operating system provides default USB drivers. While these default drivers may, in fact, work with your USB devices, it is recommended that you install the manufacturer supplied USB drivers to optimize functionality and performance of your USB devices. The manufacturer supplied driver should be installed on the computer, local or remote, where the USB devices will be *logically* (not physically) attached.

3. The Remote Clipboard Configuration dialog is displayed next. To see additional information, select **I'm not sure, I want more information**, and click **Next**. Select the desired Remote Clipboard Configuration option, and click **Next**.

 **NOTE:** Selecting "Yes" will cause the hprclipboard.dll library to be installed with the RGS Receiver. If you select "No", this DLL won't be installed and you won't be able to use Remote Clipboard. To enable Remote Clipboard later, you would need to reinstall the RGS Receiver, and select "Yes" in the above dialog.


4. The next dialog allows you to install HP Velocity:


- **Yes**—This option installs HP Velocity, which improves data communication to and from a remote computer for better performance over a wide area network.

 **NOTE:** HP Velocity may increase network bandwidth usage.

- **No**—This option leaves the current network setting as is.
- **I'm not sure. I want more information**—This option displays more information about HP Velocity.

5. Next, you may be prompted to configure proxy settings. If you access the Internet through a proxy server, these settings are required to activate advanced RGS features such as Advanced Video Compression and HP Velocity.

 **IMPORTANT:** The activation process uses anonymous access, so you must add the IP address 192.151.30.9 to your proxy server's list of allowed anonymous access.

 **NOTE:** If Windows already has proxy settings configured in Internet Explorer, those settings will be used and this installation step will be skipped.

6. The final installation step will normally prompt you to restart your computer.

## Automatic installation of the RGS Receiver on Windows

The RGS Receiver can be installed or removed in automatic mode. Automatic mode allows the RGS Receiver to be installed or removed without any user interaction. Automatic mode will also restart the computer, if required, after the installation process completes.

If an illegal combination of command line options is specified or another error occurs during the installation, the installation will abort and the error will be logged to the RGS Receiver installation log file. Setup will exit without making any changes if automatic installation of the same version currently installed is attempted.

### Command line syntax

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:

```
ReceiverSetup.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:

```
ReceiverSetup.exe /z"/autoinstall /agreetolicense /folder=\"C:\Program Files\Hewlett-Packard\Remote Graphics Receiver\""
```



**NOTE:** Command line options intended for the MSI installer should precede the /z flag, be separated by a space, and not be enclosed in quotes. MSI command line options should be used by advanced users only. The only suggested option is /s, which hides prompts and dialogs.

## RGS Receiver installation command line options

**Table 3-1 RGS Receiver installation command line options**

Command	Description
/autoinstall	This option performs one of the following: <ul style="list-style-type: none"><li>• Installs the RGS Receiver if it is not currently installed.</li><li>• Updates the RGS Receiver if a prior version is currently installed.</li><li>• Exits without changes if the version being installed is the same as the version that is currently installed.</li></ul> The RGS Receiver will not be reinstalled if the version being installed is older than the version currently installed.
/agreetolicense	Use of this option indicates that the user agrees to the license for use of this software. This option is required when doing an installation.
/autoremove	Removes the RGS Receiver.
/folder=\"<フォルダー>\" Example: /folder=\"C:\RGS Receiver\"	Specifies the destination folder. <b>NOTE:</b> The default is C:\Program Files\Hewlett-Packard\Remote Graphics Receiver.
/usb=local	Installs USB in Local Mode.
/usb=remote	Installs USB in Remote Mode. The system will automatically restart after the installation completes.
/usb=localRemote	Installs USB in Local/Remote Mode. The system will automatically restart after the installation completes. <b>NOTE:</b> USB is installed in Local/Remote Mode by default if no mode is specified.
/clipboard	Enables Remote Clipboard.
/noreboot	Causes the system to not reboot after an installation or uninstallation.
/viewlicense	Displays the EULA (End User License Agreement) for use of this software. <b>NOTE:</b> Using this option will negate all other options used.
/help	Displays usage text. <b>NOTE:</b> Using this option will negate all other options used.
/proxy=<アドレス>:<ポート>	Configures proxy settings to allow RGS to establish an HTTP session during Advanced Features registration.

**Table 3-1 RGS Receiver installation command line options (continued)**

Command	Description
Example: /proxy=123.456.78.90:4321	
/wanimprovement	Installs HP Velocity.

## RGS Receiver installation log file

Installation of the RGS Receiver creates the following log file:

```
%TEMP%\rgreceiverInstaller.log
```


This log file can be viewed by the user to obtain details about what operations were performed and errors that occurred during the installation process.


The log file is especially useful for automatic installations because installer errors are not displayed on the screen and are only viewable using the log file. If the log file already exists when the installer is run, the installer will remove the current contents of the log file before writing to it.

## Uninstalling the RGS Receiver on Windows

To uninstall the RGS Receiver on Windows:


- ▲ Go to the Windows **Control Panel > Programs and Features**, and uninstall **Remote Graphics Receiver**.


 **IMPORTANT:** After the RGS Receiver is uninstalled, you may be prompted to restart your computer. This restart is very important—if it is not performed, installation of a later version of the RGS Receiver may not succeed.

 **TIP:** On certain client computers, simply rerun the installation program to uninstall the RGS Receiver.

## Installing the RGS Sender on Windows


This section covers the manual and automatic installation of the RGS Sender on Windows.

 **NOTE:** The RGS Sender can only be installed on the computers and operating systems shown in [Supported hardware and software on page 95](#). Installing the RGS Sender on a non-supported computer will prevent an RGS connection from being established.


 **NOTE:** Installation of the RGS Sender on Windows may be performed remotely using Remote Desktop Connection.

## Prerequisites for RGS Sender installation on Windows

Prior to installing the RGS Sender on Windows, if an NVIDIA driver is not currently installed and is required, the NVIDIA graphics driver must be installed first. The latest NVIDIA driver for your product is available at <http://www.hp.com/support>. Windows systems require driver version 191.56 and later.

 **NOTE:** For some features, it is recommended to have an NVIDIA Quadro 2000 or better graphics card with driver version 305.29 or greater.


Install the NVIDIA graphics driver following the instructions in the download package.

 **NOTE:** Installing the NVIDIA graphics driver after the RGS Sender has been installed may prevent the use of Windows Aero on Windows.

## Manual installation of the RGS Sender on Windows

To install the RGS Sender on Windows:


---

 **IMPORTANT:** Be sure you are logged in to an account with administrator privileges before performing installation:

---

1. Run the RGS Sender installer, and follow the on-screen instructions.
2. During the installation, the RGS Sender configuration dialog is displayed. Check the boxes appropriate to your requirements, as follows:
  - **Enable Remote USB**—Check this box if USB devices attached to the local computer need to be accessible by the remote computer. For further information, see [Remote USB on page 54](#).
  - **Enable Remote Clipboard**—Check this box if your Local Users will need Remote Clipboard capability. For further information, see [Remote Clipboard on page 54](#)
  - **Enable HP Velocity**—Check this box to install HP Velocity, which improves data communication to and from a remote computer for better performance over a wide area network.


---

 **NOTE:** HP Velocity may increase network bandwidth usage.

---

- **I'm not sure, I want more information**—For further information, check this box, and click **Next**.
3. If you are installing the RGS Sender on HP workstations running Windows, you will be presented with a dialog to enable either Single Sign-on or Easy Login. If you're not sure, you will be able to configure them later using the rgadmin.exe tool.
4. If you are on an HP desktop Z series workstation, HP EliteBook mobile workstation, or HP ZBook mobile workstation, skip to the next step. If not, the RGS Sender installer will prompt you for an RGS Sender license. If you have an RGS Sender license file, click the appropriate radio button, click **Next**, and provide the requested information. If you don't yet have a license file, click **I do not yet have a license file**, and click **Next**. You can install your license file later.

---

 **NOTE:** Absent a license file, the RGS Sender will still function correctly, and you'll be able to establish a connection from the RGS Receiver. However, an error dialog will be displayed in the Remote Display Window. Installation of the license file is described in detail in the *HP Remote Graphics Software Licensing Guide*, available at <http://www.hp.com/support/rgs>.

---

5. You will be prompted to restart your computer after the RGS Sender installation is complete. Select **Yes** when asked to restart the system.

## Automatic installation of the RGS Sender on Windows

The RGS Sender can be installed or removed in automatic mode. Automatic mode allows the RGS Sender to be installed or removed without any user interaction. Automatic mode will also restart the computer, if required, after the installation process completes.

If an illegal combination of command line options is specified or another error occurs during the installation, the installation will abort and the error will be logged to the RGS Sender installation log file. Setup will exit without making any changes if automatic installation of the same version currently installed is attempted.


### Command line syntax

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:

```
SenderSetup.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:

```
SenderSetup.exe /z"/autoinstall /agreetolicense /folder="C:\Program Files
\Hewlett-Packard\Remote Graphics Sender\""
```

 **NOTE:** Command line options intended for the MSI installer should precede the /z flag, be separated by a space, and not be enclosed in quotes. MSI command line options should be used by advanced users only. The only suggested option is /s, which hides prompts and dialogs.

## RGS Sender installation command line options

**Table 3-2 RGS Sender installation command line options**

Command	Description
/autoinstall	This option performs one of the following: <ul style="list-style-type: none"> <li>Installs the RGS Sender if it is not currently installed.</li> <li>Updates the RGS Sender if a prior version is currently installed.</li> <li>Exits without changes if the version being installed is the same as the version that is currently installed.</li> </ul> <p>The RGS Sender will not be reinstalled if the version being installed is older than the version currently installed.</p>
/agreetolicense	Use of this option indicates that the user agrees to the license for use of this software. This option is required when doing an installation.
/autoremove	Removes the RGS Sender.
/folder="<フォルダー>" Example: /folder="C:\RGS Sender\"	Specifies the destination folder. <b>NOTE:</b> The default is C:\Program Files\Hewlett-Packard\Remote Graphics Sender.
/usb	Enables Remote USB.
/remotemic	Enables Remote Microphone.
/clipboard	Enables Remote Clipboard.
/sso	Enables Single Sign-on. <b>NOTE:</b> Only one of /e1 or /sso can be specified. If neither is specified, the Standard Login method will be used.
/e1	Enables Easy Login. <b>NOTE:</b> Only one of /e1 or /sso can be specified. If neither is specified, the Standard Login method will be used.
/gina="<ファイル名>"	Specifies the chaining GINA module to use and can only be specified if /e1 is used. The default is msgina.dll.
/rgslicensserver=<ポート>@<ホスト> Example: /rgslicensserver=4321@123.456.78.90	Specifies the listening port and host of the license server where RGS should acquire a license during installation. <b>NOTE:</b> The port and the trailing @ symbol are optional, in which case the default port is used for the given host. <b>NOTE:</b> Only one of /rgslicensserver or /rgslicensefile can be specified. If neither is specified, RGS will be installed without a license.

**Table 3-2 RGS Sender installation command line options (continued)**

Command	Description
<code>/rgslicensefile=\&lt;ファイル名&gt;\</code> <b>Example:</b> <code>/rgslicensefile=\"license.lic\"</code>	Specifies the file where RGS should acquire a license during installation.  <b>NOTE:</b> Only one of <code>/rgslicensesserver</code> or <code>/rgslicensefile</code> can be specified. If neither is specified, RGS will be installed without a license.
<code>/noreboot</code>	Causes the system to not reboot after an installation or uninstallation.
<code>/viewlicense</code>	Displays the EULA (End User License Agreement) for use of this software.  <b>NOTE:</b> Using this option will negate all other options used.
<code>/help</code>	Displays usage text.  <b>NOTE:</b> Using this option will negate all other options used.
<code>/wanimprovement</code>	Installs HP Velocity.

## RGS Sender installation log file on Windows

Installation of the RGS Sender creates the following log file:

```
%TEMP%\rgsenderInstaller
```

This log file can be viewed by the user to obtain details about what operations were performed and errors that occurred during the installation process.

The log file is especially useful for automatic installations because installer errors are not displayed on the screen and are only viewable using the log file. If the log file already exists when the installer is run, the installer will remove the current contents of the log file before writing to it.

## Uninstalling the RGS Sender on Windows

To uninstall the RGS Sender on Windows:

- ▲ Go to the Windows **Control Panel > Programs and Features**, and uninstall **Remote Graphics Sender**.



**TIP:** **Retain User Settings** will leave user-specific settings in the registry.




**IMPORTANT:** After the RGS Sender is uninstalled, you will be prompted to restart your computer. This restart is very important—if it is not performed, installation of a later version of the RGS Sender may not succeed.

## Installing RGS on Linux

This section describes installation of the RGS Receiver and RGS Sender on Linux. See [Supported hardware and software on page 95](#) for a list of the Linux operating systems that support the RGS Receiver and RGS Sender.

If you plan to use Advanced Video Compression, see [Advanced Video Compression requirements on page 96](#). Meeting these requirements is essential to having a quality experience when using this feature.

## Installing the RGS Receiver on Linux

 **NOTE:** The Linux RGS Receiver is available in both 32-bit and 64-bit versions. The Xlib version 1.1.5 is not supported.

RGS only supports multi-head displays on Linux systems that have NVIDIA cards in TwinView mode. ATI dual-head is not supported.

To install the RGS Receiver on Linux:


1. Log in as root.
2. Go to the directory where you downloaded RGS, and navigate to the directory `lin32/receiver` (32-bit version) or `lin64/receiver` (64-bit version).


3. Execute the following command:

```
./install.sh
```

The RGS Receiver will be installed into `/opt/hpremote/rgreceiver`.

4. You may be prompted to configure proxy settings. If you access the Internet through a proxy server, these settings are required to activate advanced RGS features such as Advanced Video Compression and HP Velocity.

 **IMPORTANT:** The activation process uses anonymous access, so you must add the IP address 192.151.30.9 to your proxy server's list of allowed anonymous access.

 **NOTE:** If the Linux operating system already has proxy settings configured, it will be suggested to use the settings from the operating system.

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

## RGS Receiver audio requirements on Linux

The RGS Receiver installer will install a version of JACK Audio Connection Kit if one is not already installed on the system. JACK is a low-latency sound server that works in conjunction with an ALSA sound driver to mix and direct audio on the RGS Receiver system. The version of JACK provided with the RGS Receiver installer is the version that is expected to be started by the script in `/opt/hpremote/rgreceiver/hprgsaudio`. A different version may require adjustments to this script to provide different options for the JACK daemon.

The JACK Audio Connection Kit is installed as an RPM package. The RGS Receiver will run on systems without audio hardware, but the RGS Receiver will not run without the libraries provided by the JACK RPM package. If the RGS Receiver is being removed from the system, JACK can also be removed using the following command:

```
rpm -e jack-audio-connection-kit
```

## Uninstalling the RGS Receiver on Linux


To uninstall the RGS Receiver on Linux find the name of the RedHat RPM package for the RGS Receiver by typing the following:

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

If the RGS Receiver is installed on the system, you will see `rgreceiver_linux_32-5.1-0` or a similar package. To remove the RGS Receiver's RPM package, become root and type:

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


## Installing the RGS Sender on Linux

 **NOTE:** The Linux version of the RGS Sender can only be installed on the computers and Linux operating systems shown in [Supported hardware and software on page 95](#). Installing the RGS Sender on a non-supported computer will prevent an RGS connection from being established.

The RGS Sender requires a license key to establish an RGS connection (except on HP desktop Z series workstations, HP EliteBook mobile workstations, and HP ZBook mobile workstations). For information on RGS Sender licensing on Linux, see the *HP Remote Graphics Software Licensing Guide*, available at <http://www.hp.com/support/rgs>.


To install the RGS Sender on Linux:

1. Log in as root.
2. Install the accelerated NVIDIA graphics driver. This is required prior to installing the RGS Sender. The NVIDIA driver installation creates the file `/etc/X11/xorg.conf`, which is used by the RGS Sender installation.

 **NOTE:** For some features, it is recommended to have an NVIDIA Quadro 2000 or better graphics card with driver version 305.29 or greater.

The minimum NVIDIA driver version for RHEL6 is 256.53. The latest NVIDIA driver for your product is available at <http://www.hp.com/support>.

Install the driver using the Linux `rpm` command.


 **TIP:** Installing the driver while the system is at **run level 3** allows the installation to complete without restarting. Installing while at **run level 5** will require restarting.


3. Go to the directory where you downloaded RGS, and change to the directory `lin64/sender`.
4. Execute the following command:

```
./install.sh
```

This command will give you a choice of performing a manual installation or a partially automated installation (automating steps 5 and 6). The RGS Sender will be installed to `/opt/hpremote/rgsender`.

5. This last step of the installation is optional and will ask if you would like to automatically customize the following files to enable proper function of the RGS Sender:
  - `/etc/X11/xorg.conf`—The configuration file for the X Server will be modified to load the `rge` extension.
  - `/etc/pam.d/rgsender`—This configuration file will be modified to allow the RGS Sender to interact with the currently supported PAM authentication.
  - `/etc/pam.d/gdm*`, `/etc/pam.d/kdm*`, `/etc/pam.d/xdm*`—These configuration files will be modified to ensure proper PAM authentication window manager support for the RGS Sender process. If a different window manager is in use, that file must be manually configured.

 **NOTE:** The file `rgsender_config_64-*.rpm` that performs these automated customizations can also be run independently of the installation script.

 **IMPORTANT:** This automated step must be performed after any actions that install their own X Server configuration files because these files are modified to load the `rge` module required for proper RGS Sender functionality. If these files are replaced or modified later, then the modifications must be performed manually as described below.



If you choose not to use the automatic customization, perform the following steps:

1. Add the "rge" extension to the X Server configuration file (`/etc/X11/xorg.conf`). In the Module section of this file, add the following line:

```
Load "rge"
```

Next, you need to disable the Composite extension. To do this, add this line in the Extensions section:

```
Option "Composite" "Disable"
```

2. If you are using the GNOME Desktop Manager or KDE Desktop Manager, add the following line to the files listed below:

```
session optional pam_rg.so
```

Files (and all related derivatives):

```
/etc/pam.d/gdm
```

```
/etc/pam.d/kdm
```

```
/etc/pam.d/xdm
```

3. Some Linux distribution versions utilize newer or older PAM support modules and support conventions. The file `rgsender_config_64-*.rpm` performs configuration analysis to determine types of `pam_unix*.so`, `pam_env*.so`, `common-auth`, and `pam_stack` that might apply to your configuration for the `/etc/pam.d/rgsender` configuration file. If you choose to do all of your own customizations manually, please run `rgsender_config_64-*.rpm` at least once on a test system to determine an example of any customizations that you might need in your current environment.

If another desktop manager, such as Enlightenment, is being used, you will need to make similar changes to the PAM configuration file used by it. Consult your Linux and Desktop Manager documentation for further information.

If the PAM system has been configured to use custom PAM authentication modules, then you may need to manually configure the PAM module that is used by the RGS Sender. You should consult your Linux documentation when configuring PAM. If you are using a custom PAM authentication module called `libpam_custom.1`, you might need to edit the PAM configuration file `/etc/pam.d/rgsender` to specify the PAM authentication module to be used by the RGS Sender. For example, you might need to add the following line to the file:

```
auth optional /lib/security/pam_custom.1
```

The RGS Sender will not accept remote connections when a DNS name inquiry does not resolve to a valid/active IP address—it expects to fully resolve the machine name to an active network connection IP. To test this, the command `hostname -i` should report an active IP address for the qualified hostname. Failure to resolve this address from a qualified hostname may result in remote connection errors. One way to address the hostname/IP name resolution is to edit the `/etc/hosts` file, and bind the machine name to its proper IP address as follows:

```
127.0.0.1 localhost localhost.localdomain
```

```
88.1.89.122 blade2 blade2.datacenter.com
```

## Manually disabling Easy Login on Linux

Easy Login can be disabled on Linux by adding the following property to the `rgsenderconfig` file:

```
Rgsender.IsClassicEasyLogonEnabled=0
```

## Uninstalling the RGS Sender on Linux

To uninstall the RGS Sender on Linux:

1. Log in as root.
2. If the default `install.sh` was used, then the following command reports some variation of the following packages:

```
# rpm -qa | grep -i rgsender
rgsender_linux_64-5.4.8-1
rgsender_config_64-5.4.8-1
```

3. To remove the `rgsender` package (and corresponding configuration rpm if used), execute the command:  

```
rpm -e --allmatches rgsender_linux_64 rgsender_config_64
```
4. If `rgsender_config_64-*.rpm` was installed, it must be removed first (or together as demonstrated above) before removing the `rgsender_linux_64-*.rpm` package. This resolves dependencies between the packages and undoes the previous customizations performed by this rpm. If you are upgrading your system from a previous version of RGS, it is suggested that you remove both packages and apply the new software rpms for supported results.

---

## 4 Pre-connection checklist

Establishing an RGS connection from an RGS Receiver to an RGS Sender requires that the local and remote computers be in the correct state. This chapter provides a checklist of items that should be verified before attempting an RGS connection.



**NOTE:** This chapter can also be used as a troubleshooting aid. If a connection attempt fails, the checklists below can be used to help diagnose the problem.

---

### Local computer checklist

Verify the following items on the local computer before attempting to establish a connection.

1. If using Advanced Video Compression, make sure that the local computer system meets the requirements described in [Advanced Video Compression requirements on page 96](#) (essential for a quality experience when using this feature).
2. Ensure that you are on the same network as the remote computer.
3. **Verify the hostname or IP address of the remote computer**—Verify that you have the correct hostname or IP address of the remote computer. If the remote computer hostname fails to resolve to the correct IP address, address this problem before continuing.
4. **Verify that, from the local computer, you can ping the remote computer**—If you're unable to ping the remote computer, you won't be able to establish an RGS connection. Ping the remote computer using the same computer designator you'll be using to establish an RGS connection, either the hostname or the IP address of the remote computer. Open a Command window and execute either:

```
ping hostname
```

or

```
ping <IP address>
```

If no ping reply is received, the remote computer is unreachable or is not running—resolve this problem before continuing. If a ping reply is received, the remote computer is reachable by RGS.



**NOTE:** Ensure that firewall settings are not preventing the ping command from working.

---

### Remote computer checklist

Modification and verification of the RGS Sender state can be performed either by connecting a keyboard, mouse, and monitor directly to the remote computer, or by using Remote Desktop Protocol to log in remotely to the remote computer. In either case, verify each of the following items:

1. If using Advanced Video Compression, make sure that the remote computer system meets the requirements described in [Advanced Video Compression requirements on page 96](#) (essential for a quality experience when using this feature).
2. **OPTIONAL: Ensure RGS Sender licensing is set up**—For detailed information on RGS licensing, see the HP Remote Graphics Software Licensing Guide, available at <http://www.hp.com/support/rgs>.



**NOTE:** This step is optional because you can establish a connection from the RGS Receiver to the RGS Sender without an RGS Sender license. However, an error dialog will be displayed in the Remote Display Window if the RGS Sender license file is missing or invalid. If you don't set up RGS licensing now, you can do it after you've verified you can establish an RGS connection.

3. **Ensure you have a login account on the remote computer**—When establishing an RGS connection, the remote computer will prompt you for a user name and password. Ensure that you have a login account on the remote computer.
4. **Verify the remote computer login account does not have a blank password**—The remote computer will not allow a connection for any account with a blank or undefined password. Any accounts on the remote computer used for connection by the local computer must have password protection.
5. **OPTIONAL: Disable Guest login access**—By default, Windows allows any user who can access a computer over the network to log in with Guest access. Because this is a potential security issue, HP recommends that you disable Guest logins on the remote computer. To disable this policy, open the "Control Panel", selecting "Administrative Tools", selecting "Local Security Policy", expanding the "Local Policies", expanding "Security Options", and setting "Network access: Sharing and security model for local accounts" to "Classic – local users authenticate as themselves". For more information on this topic, go to: <http://support.microsoft.com/kb/103674>.
6. **Ensure that the RGS Sender is running on the remote computer**—This can be done on Windows as follows:
  - a. Click **Start**
  - b. Right-click **My Computer**
  - c. Select **Manage** from the menu.
  - d. In the **Computer Management** console, click the + sign to expand **Services and Applications** and select **Services**. The service **Remote Graphics Sender** should be listed as **Started**.
7. **Verify that the rgdiag.exe diagnostics tool passes all tests on the RGS Sender on Windows**—This tool may be run any time after RGS Sender installation. See [Using the RGS Diagnostics Tool \(Windows only\) on page 41](#) for information on running this tool.
8. **Network Interface binding**—The RGS Sender defaults to listening to multiple network interfaces if the computer is so equipped. If the remote computer has multiple network interfaces, the RGS Sender will dynamically add or remove network interfaces without restarting the remote computer. See [RGS Sender network interface binding on page 25](#) for more information.
9. **Linux RGS Sender machine name and IP address**—The default on Linux is to bind the machine name to the following loopback interface in the /etc/hosts file:

```
127.0.0.1 blade2 localhost.localdomain
```

The RGS Sender will not accept remote connections with this configuration. Edit the /etc/hosts file and bind the machine name to its proper IP address as follows:

```
127.0.0.1 localhost localhost.localdomain
88.1.89.122 blade2 blade2.datacenter.com
```

For Linux systems with multiple network interfaces, each IP address must be listed in the `/etc/hosts` file, for example:

```
192.168.89.122 blade2 blade2.datacenter.com
192.168.90.111 blade2b blade2b.datacenter.com
```

- 10. User-started X environments do not reliably support outside connections**—Users who manually start X desktops (such as with `startx`) from the console command line will find that outside access attempts may not properly connect or be authenticated. This stems primarily from incomplete PAM session management and permissions to the console. Users should avoid this condition, and achieve login management through the display manager launched in `init-level 5` of the system.
- 11. Windows APIPA (Automatic Private IP Addressing)**—APIPA can cause the RGS Sender to open sockets on private IP addresses. This can occur, for example, if the RGS Sender computer is unable to connect to a DHCP server. Because the private IP addresses are not visible to the RGS Receiver, RGS connections will not work. You can verify if the RGS Sender is using private IP addresses by typing the following in a command window:  

```
netstat -n -a
```

If the IP address associated with the RGS Sender port (listening port 42966) is private, APIPA is the likely cause. For more information on this topic, go to: <http://support.microsoft.com/kb/220874>.
- 12. Log out**—If you do log into the remote computer to verify any of the above items, ensure that you log out when you're done.

## RGS Sender network interface binding

The RGS Sender is set by default to listen to all network interfaces present on the remote computer. 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 the RGS Sender to listen to, and then restart the remote computer. The 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.
- Disable the RGS Sender property that causes it to listen to all network interfaces, and then manually configure the desired network interface to be the one listened to by the RGS Sender. See [Reconfiguring network interface binding manually on page 26](#) for more information.
- Disable the RGS Sender property that causes it to listen to all network interfaces, and then use the RGS Sender network interface binding property to specify which network interface to listen to. See [Reconfiguring network interface binding using RGS Sender properties on page 26](#) 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 the 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 26](#) 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 remote computer binds to:

1. Set the property `Rgsender.Network.IsListenOnAllInterfacesEnabled` to 0.



**NOTE:** See [RGS properties on page 80](#) 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, and then click **Advanced > Advanced Settings**.
5. In the **Adapter and Bindings** tab, 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 the RGS Sender.

## Reconfiguring network interface binding using RGS Sender properties

Before configuring the RGS Sender network interface binding properties, you'll need to determine the number that corresponds to the network interface you want the 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, and then click **Advanced > Advanced Settings**.
4. In the **Adapter and Bindings** tab, 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 properties:

1. Set the property `Rgsender.Network.IsListenOnAllInterfacesEnabled` to 0.
2. Set the property `Rgsender.Network.Interface.<n>.IsEnabled` to 1, where `<n>` is replaced by the number that corresponds to the desired network interface.



**NOTE:** See [RGS properties on page 80](#) for more information.

## Using RGS through a firewall

The RGS Receiver can use the public IP address of the remote computer so that RGS can be used through a simple firewall. To take advantage of this feature, the remote and local computer firewalls must both support Network Address Translation (NAT). In addition, the remote computer firewall must support port forwarding.



**NOTE:** For more information on how to set up port forwarding on your firewall, see the documentation for your firewall.

The port used by the RGS Receiver is assigned by the operating system of the local computer and can vary.

The RGS Sender listens on port 42966 by default, but the port number can be changed using the `Rgsender.Network.Port` property as described in [RGS properties on page 80](#). If this property is used to change the port number from its default value of 42966, the port number must then be specified when establishing an RGS connection. Either of the following formats are accepted:

```
<hostname>:<port>
```

```
<IPAddress>:<port>
```

## Remote computer power saving states

In order for a local computer to establish connection to a remote computer, the remote computer cannot be in a power saving state, such as Windows hibernate or standby. Furthermore, the remote computer cannot utilize wake-on-LAN in an attempt to power-up in order to respond to a connection request from the local computer—the remote computer must be powered-up, and able to respond to an RGS connection request at all times.

# 5 Using the RGS Receiver

This chapter discusses the following topics:

- [Starting the RGS Receiver](#)
- [Creating an RGS connection](#)
- [Using touch features \(Windows 8 only\)](#)
- [Setup Mode \(non-touch displays only\)](#)

## Starting the RGS Receiver

To start the RGS Receiver on Windows:

- ▲ Windows 7: Select **Start > All Programs > HP > HP Remote Graphics Software > HP RGS Receiver**.
- Windows 8: Select the **HP RGS Receiver** tile on the Start screen.

To start the RGS Receiver on Linux:

- ▲ Run the executable `rgreceiver.sh`.

## RGS Receiver command line options

The following table describes the valid command line options for the Windows executable (`rgreceiver.exe`) and the Linux executable (`rgreceiver.sh`).


**Table 5-1 RGS Receiver command line options**

Option	Description
<code>-config &lt;ファイル名&gt;</code> Example: <code>-config rgreceiverconfig</code>	Specifies the name of the RGS Receiver configuration file to use.
<code>-directory &lt;ファイル名&gt;</code> Example: <code>-directory directory.txt</code>	Starts the RGS Receiver in Directory Mode. If the optional filename is specified, the file is opened and used to look up the remote computers assigned to you. If a file is not specified, you are prompted to enter a path to the directory file. <b>NOTE:</b> For information on Directory Mode, see <a href="#">Using RGS in Directory Mode (non-touch displays only) on page 61</a> .
<code>-nosplash</code>	Disables the splash screen that displays by default when the RGS Receiver starts.
<code>-v   -ver   -version</code>	Displays the RGS Receiver version information.
<code>-h   -help   -?</code>	Displays the command line options that are listed in this section.
<code>-Rgreceiver.&lt;プロパティ&gt;=&lt;番号&gt;</code> Example: <code>-Rgreceiver.IsBordersEnabled=1</code>	Sets the specified RGS Receiver property to the specified value. <b>NOTE:</b> See <a href="#">RGS properties on page 80</a> for general information on RGS properties. For information specifically on RGS Receiver properties, see <a href="#">RGS Receiver properties on page 82</a> .



# Creating an RGS connection

---


 **NOTE:** Before attempting to connect to a particular remote computer for the first time, HP recommends that you verify that the remote and local computers satisfy the [Pre-connection checklist on page 23](#). The checklist can also be used as a troubleshooting aid if a connection attempt fails.

---

To create an RGS connection:

1. In the **Hostname or IP address** field, type the hostname or IP address of the remote computer that is on the same network and has the RGS Sender installed, and then press **Enter** or click **Connect**.
2. Type the username and password in the fields, and click **OK**.


---

 **NOTE:** The username and password are the same credentials that you would use to log in to Windows on the remote computer.

---

If the connection succeeds, the Remote Display Window will appear and display the desktop session of the remote computer.

---

 **NOTE:** If the remote desktop is locked, you will need to enter your credentials a second time to unlock it. If the prompt instructs you to press **Ctrl+Alt+Del** to initiate this process, you must instead press **Ctrl+Alt+End** to trigger the desired response on the remote computer. Pressing **Ctrl+Alt+Del** will always trigger a response on the local computer.

---


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 the HP Velocity and Advanced Video Compression features. For more information on these features, see [Advanced performance features on page 45](#).
- Using the standard method of creating an RGS connection (with the RGS Receiver Control Panel), you cannot connect to more than one remote computer at a time. If an attempt is made to connect to a second remote computer using the RGS Receiver Control Panel, the connection to the first remote computer is terminated. For information about how to connect to more than one remote computer at a time, see [Using RGS in Directory Mode \(non-touch displays only\) on page 61](#).
- If your RGS Sender is not licensed, a warning dialog will be displayed in the Remote Display Window. For information on RGS Sender licensing, see the *HP Remote Graphics Software Licensing Guide*, available at <http://www.hp.com/go/rgs>.
- On Linux, the RGS Receiver Control Panel will not stay on top of other windows in the desktop and can therefore get lost. Also, for session managers that support multiple desktops, the RGS Receiver Control Panel will not, by default, show up in all desktops. See [Setup Mode \(non-touch displays only\) on page 31](#) to understand how to raise the RGS Receiver Control Panel to the top of the window stack.

## Using touch features (Windows 8 only)


RGS supports the following touch features:

- **Gestures**—See [Table 5-2 RGS touch gestures on page 30](#) for more information.
- **Virtual keyboard and virtual mouse**—The virtual keyboard and virtual mouse can be accessed using the Remote Display Window toolbar. The virtual mouse provides a visual indication of the remote cursor position, which is normally not present in tablet mode. 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 [Gesture settings \(Windows 8 only\) on page 35](#) 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.

**Table 5-2 RGS touch gestures**

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
	<b>NOTE:</b> 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	These gestures can be customized. See <a href="#">Gesture settings (Windows 8 only) on page 35</a> for more information.
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	

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

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

## Setup Mode (non-touch displays only)

If the Remote Display Window is configured to cover the entire local monitor and also has its title bar and borders hidden, then a number of questions arise, including the following:

- How do you move or resize the window absent a title bar and borders?
- In Directory Mode, if multiple Remote Display Windows are covering each other, how do you select a particular Remote Display Window to view?

Complicating the situation is that all keyboard and mouse events in the Remote Display Window are sent to the remote computer for processing. Therefore, the keyboard and mouse cannot be readily used to interact with the locally-displayed Remote Display Window.

To address this situation, RGS provides Setup Mode. In Setup Mode, transmission of keyboard and mouse events to the remote computer is suspended. Instead, the keyboard and mouse can be used to interact with the Remote Display Window on the local computer. In Setup Mode, you can perform a number of operations, including the following:

- You can move a Remote Display Window that has its title bar and borders hidden.
- In Directory Mode, you can select (bring to the front) a particular Remote Display Window that is being obscured by another Remote Display Window.

Setup Mode can be activated in two ways:

- Click the Setup Mode button on the Remote Display Window toolbar to toggle the state of Setup Mode.
- Type the default hotkey sequence as follows:

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



**NOTE:** The default hotkey sequence can be changed in the RGS Receiver settings (see [Changing the Setup Mode hotkey sequence \(non-touch displays only\) on page 37](#)).

---

---

# 6 RGS Receiver Control Panel settings

This chapter discusses the advanced settings available in the RGS Receiver Control Panel:

- [Connection settings](#)
- [Performance settings](#)
- [Gesture settings \(Windows 8 only\)](#)
- [Audio settings](#)
- [Network settings](#)
- [Hotkey settings](#)
- [Logging settings](#)
- [Statistics](#)

# Connection settings

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

**Table 6-1 Connection settings**

Setting	Description
Prompt for username and password	<p>Forces the authentication prompt to display when starting an RGS connection.</p> <p>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.</p> <p><b>TIP:</b> This is advantageous when using RGS in Directory Mode where there are different connection needs for each session.</p>
Match Receiver display resolution	<p>Attempts to set the remote computer's resolution to match the local computer's resolution.</p> <p><b>NOTE:</b> 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 <a href="#">Matching display resolution and layout on Linux on page 49</a> for more information.</p>
Match Receiver display layout	<p>Attempts to set the remote computer's display layout to match the local computer's display layout.</p> <p>For example, if the local computer has two physical displays side-by-side and an overall display resolution of 2560x1024, RGS will attempt to set the remote computer to the same layout and resolution. If that fails, RGS will attempt to set a resolution of 2560x1024 on a single remote computer display.</p> <p><b>NOTE:</b> This option is not supported if the sending computer is running Linux.</p>
Enable remote USB	<p>Enables Remote USB.</p> <p><b>NOTE:</b> For more information on Remote USB, see <a href="#">Remote USB on page 54</a>.</p>
Select Sender	<p>For use with Directory Mode only, this settings specifies the remote computer to mount USB devices on with Remote USB.</p>
Enable remote clipboard	<p>Enables Remote Clipboard.</p> <p><b>NOTE:</b> For more information on Remote Clipboard, see <a href="#">Remote Clipboard on page 54</a>.</p>

# Performance settings

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** tab.

**Table 6-2 Performance settings**

Setting	Description
Force full screen image updates	<p>Forces the entire screen to update when any part of it changes.</p> <p>Select this option if image tearing is present. This option can, however, reduce the update rate.</p> <p><b>NOTE:</b> This option is disabled when Advanced Video Compression is enabled.</p>
Advanced Video Compression on Sender	<p>Enables Advanced Video Compression.</p> <p><b>IMPORTANT:</b> See <a href="#">Advanced performance features on page 45</a> for information about the recommended usages of this feature.</p>
Image Quality	<p>Sets the maximum image quality.</p> <p>When not using <b>Adaptive image quality</b>, RGS will maintain the image quality specified by this option. When selecting <b>Adaptive image quality</b>, RGS will use this option's setting as the target image quality when the updates-per-second value allows.</p> <p><b>NOTE:</b> This option is duplicated on the Remote Display Window toolbar.</p>
Increase text rendering quality	<p>Improves image quality for images containing significant amounts of text or lines.</p> <p>Because of the high contrast ratio between adjacent pixels, images containing text or lines often don't compress well. Such high contrast cases will be compressed in a manner to better preserve their visual quality, but at the possible expense of higher network bandwidth and/or lower image update rates. HP recommends that you experiment with different settings of the image quality slider and this checkbox to find the optimal settings for your environment.</p> <p><b>NOTE:</b> This option is disabled when Advanced Video Compression is enabled.</p>
Adaptive image quality Minimum image quality Target update rate	<p>When <b>Adaptive image quality</b> is enabled, RGS will begin to degrade the image quality down to the <b>Minimum image quality</b> setting (from 0–100) anytime the updates-per-second value falls below the <b>Target update rate</b> (from 0–30 updates per second).</p> <p><b>NOTE:</b> These options are disabled when Advanced Video Compression is enabled.</p>

**TIP:** See [Optimizing RGS performance on page 45](#) for more information about ways to optimize RGS performance.

## Gesture settings (Windows 8 only)

 **NOTE:** The **Gestures** tab is only available if the local computer is running Windows and has a touch display.

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 \(Windows 8 only\) on page 30](#).

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 settings

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

**Table 6-3 Audio settings**

Setting	Description
Don't stream audio from Sender	Prevents the remote computer's audio stream from being sent to the local computer.
Stereo	Enables stereo audio for the audio stream sent from the remote computer to the local computer. <b>NOTE:</b> Stereo audio requires more network bandwidth.
Quality	Sets the quality for the audio stream being transmitted by the remote computer. <b>NOTE:</b> Higher-quality audio requires more network bandwidth.
Volume	Controls the volume level on the local computer.

## Network settings

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

**Table 6-4 Network settings**

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

**IMPORTANT:** The activation process uses anonymous access, so you must add the IP address 192.151.30.9 to your proxy server's list of allowed anonymous access.

## Hotkey settings

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

**Table 6-5 Hotkey settings**

Setting	Description
Send First Key	<p>Forces the first key of a local hotkey sequence to be transmitted to the remote computer.</p> <p>By default, if a key press matches the first key of a local hotkey sequence (such as the default Setup Mode sequence of <b>Shift</b> press, <b>Space</b> press, and <b>Space</b> release), the first key press event is not transmitted to the remote computer until RGS determines that the next key press is not completing the sequence. Upon that determination, all of the key press events are then transmitted simultaneously to the remote computer.</p> <p>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.</p> <p><b>NOTE:</b> In addition to transmitting the first key press to the remote computer, the key is also still processed by the local computer.</p>
Send CTRL-ALT-END key sequence as CTRL-ALT-DEL	<p>Enables the use of a <b>Ctrl+Alt+End</b> key sequence as a <b>Ctrl+Alt+Delete</b> sequence for the remote computer.</p> <p>This is useful when logging into the remote computer because, on some computers, the local operating system will interrupt the standard <b>Ctrl+Alt+Delete</b> key sequence and bring up local Windows security options instead.</p> <p><b>TIP:</b> The <b>Ctrl+Alt+Del</b> sequence can also be sent using the Remote Display Window toolbar.</p>



**Table 6-5 Hotkey settings (continued)**

Setting	Description
Key Repeat	<p>Enables the processing of key repeats for when the <a href="#">Shift</a> key is held down.</p> <p>By default, key repeat processing is disabled by RGS, but some remote applications might require this functionality.</p> <p><b>NOTE:</b> If this option is enabled, the default Setup Mode hotkey sequence will not trigger unless it is typed fast enough.</p>
Setup Mode Sequence	<p>Sets the hotkey sequence for switching to Setup Mode.</p> <p>For more information, see <a href="#">Changing the Setup Mode hotkey sequence (non-touch displays only) on page 37</a>.</p> <p><b>NOTE:</b> This option applies to non-touch displays only.</p>

## Changing the Setup Mode hotkey sequence (non-touch displays only)

RGS allows you to change the Setup Mode hotkey sequence from its default value of [Shift](#) press, [Space](#) press, and [Space](#) release.

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

- [LCtrl](#), [RCtrl](#), [Ctrl](#)—Specifies a left, right, or side-insensitive [Ctrl](#) key, respectively.
- [LAlt](#), [RAlt](#), [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** tab 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.

To define a sequence that is side-insensitive, you'll need to modify the property value from outside of the GUI while RGS is not running. See [Hotkey properties on page 87](#) for information on modifying the sequence from outside of the GUI.

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

## Logging settings

The RGS Receiver logs various types of information during its operation. The logging settings allow you to set a number of parameters, such as whether logging is enabled and the location and name of the log file.

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

**Table 6-6 Logging settings**

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 <b>WARN</b> is selected, the log file will contain information of the type <b>WARN</b> and also anything more serious than that type ( <b>ERROR</b> and <b>FATAL</b> ).  To log all information generated by the RGS Receiver, select <b>DEBUG</b> .
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

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

**Table 6-7 Statistics**

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.
Copy rectangles per second	Displays the combined number of copy updates per second received from all connections.
Image compression	Displays the compression ratio of the update stream.  In a multi-connection environment, the value is from the Remote Display Window that currently has the keyboard focus. If none of the Remote Display Windows have focus, the value will be zero. In a single-connection environment, the value will be always available even if the Remote Display Window does not have focus.

# 7 Using the RGS Sender

This chapter discusses the following topics:

- [Starting and stopping the RGS Sender on Windows](#)
- [Starting the RGS Sender on Linux](#)
- [RGS Sender GUI \(Windows only\)](#)
- [Setting the RGS Sender process priority \(Windows only\)](#)
- [Using the RGS Diagnostics Tool \(Windows only\)](#)
- [Using the RGS Admin Tool \(Windows only\)](#)
- [RGS Sender logging \(Windows only\)](#)

## Starting and stopping the RGS Sender on Windows

The Windows version of the RGS Sender is comprised of two processes, one of which runs as a Windows service. The service is configured by default to start when Windows starts. The service process, `rgsendersvc.exe`, will then start the RGS Sender executable `rgsender.exe`.

To manually start or stop the RGS Sender:

- ▲ In the Windows **Services** utility, right-click **Remote Graphics Sender Service** and select the desired option.

## RGS Sender command line options on Windows

The RGS Sender executable supports command line options that are passed to it via a registry key for the service process `rgsendersvc.exe`.

To modify RGS Sender command line options using the registry:

1. Open the Windows **Registry Editor**.
2. Navigate to the following folder:  
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\rgsender`
3. Add the desired parameters to the **ImagePath** registry key. For example, to increase the process priority to high, change the registry key data to the following: `C:\Program Files\Hewlett-Packard\Remote Graphics Sender\rgsendersvc.exe -l logSetup -high`
4. Restart the RGS Sender service.

The following table describes the valid command line options.

**Table 7-1 RGS Receiver command line options (Windows)**

<code>-nocollab</code>	Disables collaboration.
<code>-timeout &lt;時間 (ミリ秒) &gt;</code> Example: <code>-timeout 30000</code>	Specifies the timeout in milliseconds used to detect and disconnect an inactive connection.

**Table 7-1 RGS Receiver command line options (Windows) (continued)**

	<b>NOTE:</b> This option sets the value of the property <code>Rgsender.Network.Timeout.Error</code> and overrides the <b>Error</b> value set in the RGS Receiver network settings.
<code>-authtimeout &lt;時間 (ミリ秒) &gt;</code> Example: <code>-authtimeout 15000</code>	Specifies the timeout in milliseconds used to detect and notify the user of a network disruption.
	<b>NOTE:</b> This option sets the value of the property <code>Rgsender.Network.Timeout.Dialog</code> and overrides the <b>Dialog</b> value set in the RGS Receiver network settings.
<code>-l &lt;ファイル名&gt;</code> Example: <code>-l logSetup</code>	Specifies the file that is used to control RGS Sender logging. For more information, see <a href="#">RGS Sender logging (Windows only) on page 42</a> .
<code>-v   -ver   -version</code>	Displays the RGS Sender version information.
<code>-h   -help   -?</code>	Displays the command line options that are listed in this section.
<code>-belownormal</code> <code>-normal</code> <code>-abovenormal</code> <code>-high</code>	Sets the process priority of the RGS Sender to the specified value. The default is <code>normal</code> .
<code>-Rgsender.&lt;プロパティ&gt;=&lt;番号&gt;</code> Example: <code>-Rgsender.Clipboard.IsEnabled=1</code>	Sets the specified RGS Sender property to the specified value. <b>NOTE:</b> See <a href="#">RGS properties on page 80</a> for general information on RGS properties. For information specifically on RGS Sender properties, see <a href="#">RGS Sender properties on page 91</a> .

## Starting the RGS Sender on Linux

The RGS Sender on Linux is started by the `rge` X server extension. The RGS Sender cannot be started manually. Proper configuration and startup of the RGS Sender can be verified by examining the X server log file (`Xorg.0.log`). The log file will show that the extension is loaded, and that the extension has started the RGS Sender.

The log file content looks like the following:

```
(II) LoadModule: "rge"
(II) Loading /usr/lib64/xorg/modules/extensions/librge.so
.
.
.
(RG) 10:29:52.654 HP Remote Graphics extension. Build date : Jul 15 2009
(RG) 10:29:53.002 Listening for RG connections at /var/opt/hpremote/rgsender/sockets/rgsender-rge:0
(RG) 10:29:53.631 Started rgsender process PID = 5780
```

The `rgsender.sh` command has two options that can be executed from the command line. The `rgsender.sh` command does not start the RGS Sender if either of these options are used.

The options are described in the following table.

**Table 7-2 RGS Receiver command line options (Linux)**

<code>-v   -ver   -version</code>	Displays the RGS Sender version information.
<code>-h   -help   -?</code>	Displays the command line options that are listed in this section.

## RGS Sender GUI (Windows only)

The RGS Sender icon appears in the notification area. The icon animates when RGS Receivers are connected to the RGS Sender. Right-click the icon to display the RGS Sender GUI.

The following options are provided by the RGS Sender GUI:


- **Collaborator Input**—If **Disable** is selected, all local users are in view-only mode, meaning that only the primary user can control the remote computer desktop using a keyboard and mouse. If **Enable** is selected, all local users (and the primary user) can interact with the remote computer desktop.
- **Disconnect**—Disconnects RGS Receiver sessions for either collaboration users or all users.
- **About**—Displays information about the RGS Sender.

## Setting the RGS Sender process priority (Windows only)

The default process priority of the RGS Sender is **normal**. In some cases, increasing the process priority of the RGS Sender will improve interactivity by providing it more frequent access to the CPU and improving the update frequency to the RGS Receiver.

There are two ways to set the process priority of the RGS Sender:

- Use the Registry Editor to modify the rgsender service startup parameters in the Windows Registry (see [RGS Sender command line options on Windows on page 39](#)).
- Use HP Performance Advisor to configure the RGS Sender priority (available only on HP workstations). Go to <http://www.hp.com/go/performanceadvisor> for more information.

 **IMPORTANT:** Adjusting the process priority of the RGS Sender to a level higher than **normal** can cause other processes to receive fewer CPU cycles than normal. Therefore, caution should be observed in adjusting the priority of the RGS Sender.

## Using the RGS Diagnostics Tool (Windows only)


During the installation of the RGS Sender on Windows, the RGS Diagnostics Tool (rgdiag.exe) is installed. This tool can be used to detect potential issues (such as Windows firewall settings, guest account security policies, RDC interoperability, and Easy Login settings) that might prevent a remote connection.

The **Test Name** list shows the tests that have been run. Selecting a test with the mouse will display additional information in the **Results** list. The **Rerun Tests** button on the bottom left reruns all tests. The example window shows that all tests have passed. If a test failed, click the test title to display its details in the **Results** panel. This information can be used to determine what the test looked for, why it failed, whether the failure will prevent connections, and suggestions on how to fix the problem.

The RGS Diagnostics Tool can be run any time after RGS Sender installation. To run the RGS Diagnostics Tool, use Windows Explorer to display the RGS Sender installation folder, and locate rgdiag.exe. This tool is normally located at:

C:\Program Files\Hewlett-Packard\Remote Graphics Sender\rgdiag.exe

---

 **TIP:** For 64-bit systems, use Program Files (x86).


---

## Using the RGS Admin Tool (Windows only)

The RGS Admin Tool can be used to enable and disable both Single Sign-on and Easy Login. For a normal RGS Sender installation, this tool can be found at:

C:\Program Files\Hewlett-Packard\Remote Graphics Sender\rgadmin.exe

---

 **TIP:** For 64-bit systems, use Program Files (x86).

---


## RGS Sender logging (Windows only)

RGS Sender logging is not controlled by a GUI—instead, RGS Sender logging is controlled by a particular file in the RGS Sender installation directory. The default file used is **logSetup**. See [RGS Sender command line options on Windows on page 39](#) for information on how to specify a different file using the command line.

The logSetup file is used to specify where the log output goes (to a file or to a standard error) as well as the type of output logged. By default, the logSetup file is set to send output to a file named rg.log at the INFO level.

If another logging level is required, edit the file to replace INFO with any of the following: DEBUG, WARN, ERROR, or FATAL.

 **NOTE:** The logSetup file is set to read-only during RGS Sender installation, so you'll need to uncheck the **Read-only** property to edit the file.

 **NOTE:** To log Remote Clipboard activities on the RGS Sender, DEBUG-level logging (not the default INFO-level logging) must be specified in the logSetup file.

---

---

## 8 Advanced RGS features

This chapter discusses the following topics:

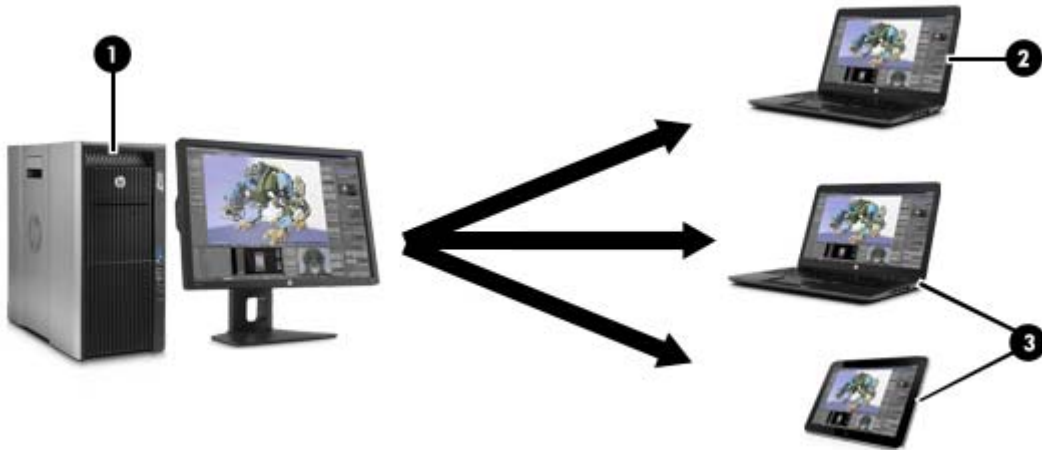
- [Collaboration](#)
- [Optimizing RGS performance](#)
- [Display resolution and layout matching](#)
- [Remote Audio](#)
- [Remote Clipboard](#)
- [Remote USB](#)
- [Using RGS in Directory Mode \(non-touch displays only\)](#)
- [Game Mode \(non-touch displays only\)](#)
- [Auto-launching connections](#)
- [RGS Sender event logging \(Windows only\)](#)
- [Remote application termination](#)
- [Interoperability of RGS and Microsoft Remote Desktop Connection](#)
- [RGS security features](#)
- [Linux connection considerations](#)

# 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.

## Creating a collaboration session

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.



- 
- |   |  |
|---|--|
| 1 | <b>Remote computer</b> —Hosts the RGS Sender, which transmits the remote computer's desktop session to the RGS Receivers on the local computers. |
| 2 | <b>Primary local user</b> —This user is logged into the remote computer and must authenticate any secondary local users joining the session.     |
| 3 | <b>Secondary local users</b> —These users can view the primary local user's remote desktop session if that user authenticates them.              |
- 


**NOTE:** The image above is just an example of one possible configuration. Any combination of hardware supported by the RGS Receiver can be used by the primary and secondary local users.

**NOTE:** Collaboration requires unique login credentials on the remote computer for each participant.

**NOTE:** 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.

---

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.

 **NOTE:** The delay's value of 0.5 seconds can be changed using the property `Rgsender.RequestFloorControlTime`. See [RGS Sender properties on page 91](#) for more information.

---



The primary user can disable collaborator input using the RGS Sender GUI. Authorized local users will still be able to view the primary user's desktop but will be unable to interact with it.

To disable collaborator input:

- ▲ Right-click the RGS Sender icon in the notification area and select **Collaborator Input > Disable**.

All collaboration users can be disconnected simultaneously using the RGS Sender GUI.

To disconnect all collaboration users:

- ▲ Right-click the RGS Sender icon in the notification area and select **Disconnect > Collaborators**.

Note the following additional information about collaboration:

- 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 rates of all collaborators is limited by the lowest update rate of any one collaborator. This is required for content synchronization. Collaborators with low update rates can use the performance settings to improve their update rate, which will improve the experience for all collaborators. See [Performance settings on page 34](#) for more information.

## Collaboration notification dialog

The RGS Sender on Windows displays a collaboration notification dialog that displays a list of usernames for each user connected to the remote computer.

Primary and collaboration users are identified using different fonts in the notification dialog. The primary user is italicized and listed first. Collaborator usernames follow and are displayed using a non-italicized font.

Individual users can be disconnected by clicking the **X** icon next to their username.

## Optimizing RGS performance

### Advanced performance features

The following features can be used to optimize RGS performance:

- **Advanced Video Compression**—This option enables the use of a modern video codec to greatly reduce the network bandwidth needed for high-quality video streams. It 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. This option can be enabled via the **Performance** tab of the RGS Receiver Control Panel settings.



**IMPORTANT:** CPU consumption might be higher on both the remote and local computers when using Advanced Video Compression. This feature is not recommended for customers who do not require reduced network bandwidth consumption. If using Advanced Video Compression, be sure the remote and local computers meet the requirements described in [Advanced Video Compression requirements on page 96](#).



**NOTE:** Advanced Video Compression is not supported on multi-monitor configurations.

- **HP Velocity**—Improves RGS performance over poor network connections. HP Velocity must be enabled during installation of both the RGS Receiver and RGS Sender.



**NOTE:** HP Velocity may increase network bandwidth usage.



**NOTE:** These features will be activated during the first RGS connection, and this activation will require Internet access. Please make sure your proxy settings are correctly configured (see [Network settings on page 36](#)).

## Performance tuning for all operating systems

The following suggestions apply to all operating systems:

- Set the network to full-duplex mode
- Do not use color or animated cursors on the remote computer. Although RGS displays color and animated cursors very well, this typically requires more network bandwidth and CPU resources.
- Set the remote computer desktop background to a solid color to minimize the amount of image data that needs to be sent.
- Set the remote and local computers to 32-bits per pixel.
- Lower the remote computer's display resolution.

## Performance tuning for Windows

The following suggestions apply to Windows:

- Increase the process priority of the RGS Sender. See [Setting the RGS Sender process priority \(Windows only\) on page 41](#) for more information.
- Mute the audio on the local computer if it is not needed using the local computer's mute button (not the system mute function). Alternatively, set the local computer's audio to play in mono at either 11 KHz or 22 KHz.
- Adjust the Windows system performance settings in the Windows Control Panel. The **Adjust for best performance** option will minimize the bandwidth requirements for RGS.

## Configuring your network for optimal performance

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 remote and local computers:

- 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 Test TCP (TTCP) tool, which is available at <http://www.pcausa.com/Utilities/pcattcp.htm>.

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. Open **Device Manager** in the Windows Control Panel.
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 local computer 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.

## Display resolution and layout matching

Many RGS scenarios require that the resolution and display layout transmitted by the sending computer match the display configuration on the receiving end. The following sections describe how to configure the sending computer for both Windows and Linux scenarios if RGS is unable to match the resolution and display layout by default.

### Matching display resolution and layout on Windows

When using the Windows version of the RGS Sender, RGS will automatically try to set the resolution and display layout of the sending computer to match that of the receiving computer (see [Connection settings on page 33](#) for more information about the settings that enable this functionality by default). However, there are some scenarios where some manual configurations might be required to achieve the desired result, such as when the sending computer has no monitor attached.

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

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 sending computer's resolution to the match the receiving computer'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 hardware and driver you are using, you might need to perform additional configurations on the sending computer. The required configurations can vary depending on the hardware, as described below:

- **Blade workstation**—If the sending computer is a blade workstation, then its NVIDIA driver exposes all display outputs 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 Windows on page 48](#).
- **Virtual workstation**—If the sending computer 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 receiving computer, no further action is required. If you need to configure additional resolutions and/or make additional displays available, see [Creating and applying an EDID file on Windows on page 48](#).
- **Traditional workstation**—If the sending computer 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. If you do not have a display attached, the NVIDIA driver reverts to a single VGA output with basic display resolutions. If you want to rack mount a workstation of this type in a data center, you need to attach an EDID emulator device to the graphics card outputs you want to use or provide an EDID file from a display you want to emulate. See [Creating and applying an EDID file on Windows on page 48](#) for more information.

## Creating and applying an EDID file on Windows

There are software tools available to create and edit an EDID file, but the easiest method is to use an existing monitor from the receiving side and temporarily attach it to the sending system, which should be Windows-based with NVIDIA graphics. If you have several different displays that you use on the receiving side, HP recommends that you capture the EDID information of the one that has the highest display resolution. This will address all other resolution needs.

To create and apply an EDID file:

1. Attach a monitor to the sending computer.



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

2. Open the NVIDIA Control Panel and click **View system topology**.
3. Click the **EDID** link for the port where you connected the monitor.
4. In the Manage EDID dialog box, click **Export** and save the output to a file.
5. Disconnect the monitor and establish an RGS connection to the sending computer.
6. In the Manage EDID dialog box, click **Browse** and select the EDID file you created.
7. Under **Connector type (video signal)**, select **DisplayPort (Digital)**.
8. Select the checkboxes for the DisplayPort connectors you want to apply the EDID file to. If you apply the file to multiple DisplayPort connectors, RGS will be able to support dual-display configurations.
9. Click **Load**. The EDID information will be applied.
10. Click **OK**, and then click **Cancel** to exit the Manage EDID dialog box.


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 screen resolution and display layout.

## Adding custom resolutions on Windows

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 on Linux

RGS can automatically try to set the resolution and display layout of a sending computer running Linux to match that of the receiving computer, but because RGS only supports a single remote X screen, the method for doing so is different from when the RGS Sender is on Windows. RGS will try to set the desktop resolution of the sending computer to the combined resolution of all displays attached to the receiving computer.

---

 **NOTE:** This is the default action when the **Match Receiver display resolution** setting is disabled, even when the sending computer is running Windows.

---


For example, if the receiving computer has a dual-display setup with both monitors set at a 1280x1024 resolution, RGS will ask the sending computer to set its desktop resolution to 2560x1024. The sending computer must support this resolution for this to be successful. If the resolution is not supported, the RGS session defaults to the sending computer's preferred resolution from the file `xorg.conf`.

Also, as with Windows, the easiest way to check if the sending computer can match the receiving computer's resolution is to attempt to set the resolution on the sending computer manually. If you can set the resolution manually, then RGS can also 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 the Linux version of the RGS Sender.

---

Once you establish an RGS session, open an X terminal window and use the `xrandr` command to list all the currently supported resolutions for the X server.

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 receiving computer's resolution in an RGS session where the X server cannot determine the capabilities of the receiving computer's monitors.

## 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 receiving computers have the same configuration

If all receiving computers 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 receiving computers 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, every time you connect via RGS, the X server is configured to have a single screen running at a resolution of 5120x1024, which covers all four of the receiving computer's monitors. You can use this method to support a very large virtual display limited only by frame buffer memory.

## Scenario 2: Receiving computers 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 receiving computers 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 receiving computers. 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 Linux on page 51](#)) and making the following additions to the file `xorg.conf`.



**NOTE:** This example uses dual HP LP2465 displays.

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

```
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 on Linux


To create an EDID file on Linux:

- ▲ Use the NVIDIA tool `nvidia-settings`.

---

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

 **NOTE:** The EDID file can be in either `.bin` or `txt` format.

 **NOTE:** You can also use the method described in [Creating and applying an EDID file on Windows on page 48](#) and just copy the EDID file to the Linux system.

---

## Remote Audio

### Remote Audio on Windows

The following table describes the paths taken by both application-generated audio output and microphone audio on Windows.

**Table 8-1 Windows RGS audio data paths**

---

Audio playback from the remote computer to the local computer	Sending of microphone audio from the local computer to the remote computer
---	--

---

**Table 8-1 Windows RGS audio data paths (continued)**

<ol style="list-style-type: none"><li>1. An application on the remote computer generates audio output.</li><li>2. If an audio device is installed, the application-generated audio is routed through it.</li><li>3. If there is no audio device, the application-generated audio is routed through the HP Remote Audio virtual device.</li><li>4. Audio from either the audio device or the HP Remote Audio virtual device is sent to the RGS Audio Recorder.</li><li>5. The RGS Audio Recorder captures the audio, which is sent by RGS to the local computer.</li><li>6. The RGS Audio Player on the local computer decodes the received audio and sends it to the audio mixer.</li><li>7. The output of the audio mixer is sent to the local computer audio device.</li><li>8. The audio device drives an audio output device, such as a speaker.</li></ol>	<p><b>USB devices are Remote or Local/Remote:</b></p> <p>Certain USB microphones can be attached to the remote computer using the Remote USB functionality.</p> <p>For more information, see <a href="#">Remoting USB microphones on page 56</a>.</p> <hr/> <p><b>USB devices are Local:</b> RGS on Windows does not support locally-mounted USB microphones.</p>
--	---

## Remote Audio on Linux

The following table describes the paths taken by both application-generated audio output and microphone audio on Linux.

**Table 8-2 Linux RGS audio data paths**

<b>Audio playback from the remote computer to the local computer</b>	<b>Sending of microphone audio from the local computer to the remote computer</b>
<ol style="list-style-type: none"><li>1. An application on the remote computer generates audio output.</li><li>2. If an audio device is installed, the application-generated audio is routed through it.</li><li>3. If there is no audio device, the application-generated audio is routed through the Virtual Audio Driver.</li><li>4. Audio from either the audio device or the Virtual Audio Driver is sent to the RGS Audio Recorder.</li><li>5. The RGS Audio Recorder captures the audio, which is sent by RGS to the local computer.</li><li>6. The RGS Audio Player on the local computer decodes the received audio and sends it to the audio mixer.</li><li>7. The output of the audio mixer is sent to the local computer audio device.</li><li>8. The audio device drives an audio output device, such as a speaker.</li></ol>	<p><b>USB devices are Remote or Local/Remote:</b> Certain USB microphones can be attached to the remote computer using the Remote USB functionality. The remote computer must be running Windows.</p> <p><b>NOTE:</b> For more information, see <a href="#">Remoting USB microphones on page 56</a>.</p> <hr/> <p><b>USB devices are Local:</b> RGS on Linux does not support locally-mounted USB microphones.</p>

The device the audio is recorded from can be specified in the RGS Sender 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 playbac
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
```

There are two important things. The first is the content between the “[ ]”. The first number is the “card” (denoted “c” below) and the second number is the “device” (denoted “d” below). The second important thing is the word “capture” in the description.

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

In the example above, depending upon which audio device you would like to capture the audio from, you could specify the device with:

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

or

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

## Configuring audio 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. See [Remote Audio device support on Linux on page 96](#) for a list of supported audio devices. 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 program 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.

The Audigy2ZS and Audigy 4 audio devices require the controls labeled **PCM Capture** to have a non-zero volume. Other volume controls will not impact the volume of the signal captured through RGS. Since the master control does not impact RGS, the volume of the speakers on the remote computer can be muted without preventing RGS from capturing an audio signal.

The Sound Blaster Live! needs to have recording enabled on the Wave control in addition to having a non-zero volume level. Similar to the Audigy cards, the master control does not impact RGS.

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**.

## Disabling audio on the remote computer

Most audio devices will allow the remote computer's speakers (if present) to be disabled while still allowing audio to be sent to the local computer. This is done by enabling the mute for the master volume control through the Sounds and Audio Devices control panel or through the Volume icon in the taskbar. The Volume icon in the taskbar will change when mute is enabled.

Enabling mute on some devices will prevent audio from reaching the local computer. The Realtek audio device used in the HP xw4300 has this issue. One possible solution when running the 32-bit version of Windows is to disable the audio device prior to installing the RGS Sender. This will cause the HP Remote Audio device driver to be installed. The real audio device and the HP Remote Audio device should not be enabled at the same time. The remote computer will connect to the first audio device it detects, which might not be the device that is selected by the user.

## Remote Clipboard

Remote Clipboard allows you to cut, copy, and paste data between the local and remote computers or between two different remote computers.

Remote Clipboard is supported in the following scenarios:

- **Between the local computer and the remote computer**—The remote computer can be running either Windows or Linux, but the local computer must be running Windows.
- **Between two different remote computers**—Both the remote and local computers can be running either Windows or Linux.

On Windows, Remote Clipboard must be enabled during both the RGS Sender and RGS Receiver installations (see [Installing RGS on Windows on page 12](#)).

On Linux, Remote Clipboard is installed by default.

On both Windows and Linux, Remote Clipboard must also be enabled in the RGS Receiver Control Panel (see [Connection settings on page 33](#)).

## Remote USB

Remote USB allows USB devices that are connected to the local computer to be attached (mounted) to a remote computer. The remote computer will have direct access to the local USB devices as if they were connected directly to the remote computer.

Note the following information about Remote USB:

- Local USB devices can be collectively attached to a single remote computer. Local USB devices cannot be split between multiple remote computers nor can they be collectively attached to multiple remote computers.
- Devices that adhere to the USB 1.x or 2.x standard should work; however, devices that are sensitive to timing may not work or performance may be impacted. HP recommends thoroughly testing any USB device needed for RGS deployments.
- USB 3.x is not supported.
- Remote USB is not supported with the Linux version of the RGS Sender.

## Local/Remote USB overview

This section describes Remote USB behavior if you have selected the **USB devices are Local/Remote** option described in [Manual installation of the RGS Receiver on Windows on page 12](#).

USB device accessibility depends on when the USB device is plugged into the local computer. If a USB device is inserted while no RGS connection is established, the device will be locally accessible only. If a USB device is inserted while an RGS connection is established, the device will be remotely-accessible only.

Once a USB device is established as locally-accessible or remotely-accessible, its status can only be changed by removing and inserting the device while in the alternate RGS connection state (either connected or not connected). For example, to make a locally accessible USB device remotely accessible, the USB device needs to be removed and inserted after an RGS connection is established.

## Auto-remoting

In addition to the general default settings for Remote USB configurations, RGS supports auto-remote and auto-return of user-specified USB devices when using Windows on both the RGS Sender and Receiver platforms. An auto-remote configuration syntax for the Windows Registry entries allows specified USB devices to be automatically attached to a remote computer at RGS connection and then returned to the local computer at RGS disconnect.



**IMPORTANT:** Enabling auto-remoting of specific USB devices requires modifications to the Windows Registry. Registry modifications should only be made by experienced personnel. Because an incorrect Registry setting can cause serious problems, you should always make a backup of the Registry prior to making any changes.

To auto-remote a particular USB device, perform the following steps:

1. Get the vendor ID and device ID for your USB device using the following steps. For this example assume that you found the vendor id is 0x1234 and device id is 0x5678.

- a. Open Device Manager and find the USB device to be auto-remoted.
- b. Right-click the USB device and select **Properties**.
- c. Select the **Details** tab and select **Hardware IDs** in the drop-down menu. The Hardware IDs format will be:

```
USB\Vid_xxxx&Pid yyyy
```

where xxxx is the VendorID and yyyy is the ProductID

The VendorID and ProductID are reported in hexadecimal format, and should be entered in hexadecimal format in the new key created below.

2. Create the following Registry key:

```
HKLM\System\CurrentControlSet\Services\hprpush\Parameters\Device
```

3. Create the following Registry key, where the vendor and device IDs like Vid\_1234&Pid\_5678 are added to the end of the Device key:

```
HKLM\System\CurrentControlSet\Services\hprpush\Parameters\Device  
\Vid_1234&Pid_5678
```

4. In the key created in Step 3, create a string value (REG\_SZ) named Mode:

```
HKLM\System\CurrentControlSet\Services\hprpushb\Parameters\Device  
\Vid_1234&Pid_5678\Mode
```

5. Set the Mode data value to one of the following:

default—Allows the device to work in local, then remote mode.

local—Allows the device to be used on the local computer only.

remote—Allows the device to be used on a remote computer only.

auto—Allows the device to be used on the local computer until there is a connection to a remote computer. Once the connection has been made, the device will be removed from the local computer and remoted to the remote computer.

## Supported USB devices

RGS supports all USB transfer types (bulk, isochronous, interrupt and control). This support means that a wide range of USB devices will work remotely with RGS.

RGS works very closely with the Windows USB driver stack. Any USB device that exclusively uses the Windows USB driver stack for functionality should work with RGS. The less a USB device's driver complies with the Windows USB driver stack, the less likely it will work with RGS.



**NOTE:** Devices that adhere to the USB standard should work. Because RGS is a remote graphics protocol and is emulating the USB protocol over a network, devices that are sensitive to timing may not work at all. This includes USB devices with security and encryption mechanisms built into them. The additional network delay could be looked at as a threat. Other devices that are known to break the USB standard, such as webcams, may also not function at all. Performance of USB devices over RGS will not be equal to that of a locally connected device. File copies may take longer due to the additional overhead of the network protocol sitting on top of the USB protocol.

HP recommends that customers thoroughly test any USB device they are considering to use with RGS as Hewlett-Packard cannot certify and or guarantee it will work over a Remote USB protocol. Because many USB vendors do not support their devices over any Remote USB protocol, HP recommends that you contact the USB vendor for support concerns first.

## Remoting USB microphones

The Remote USB driver (on the local computer) 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 remote computer in the same manner as other USB devices.

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



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

## Unique smart card handling

Smart card readers are handled in a unique manner, as follows:

- Both the sending and receiving computers should be running Windows.
- Easy Login must be enabled.
- Smart card readers will always be accessible by the local computer prior to establishing a connection to a remote computer, unless the smart card reader is explicitly marked by the user as a "classic" device.
- The **USB devices are Remote** and **USB devices are Local/Remote** settings are effectively ignored for smart card readers. Smart cards readers are accessible locally if there is no RGS connection established, and they automatically become remotely accessible when an RGS connection is established.
- If a smart card reader is plugged in after an RGS connection is established, it will be available remotely.
- If there is a break in the RGS connection, the smart card reader will become locally accessible.

If RDC is used to connect from the local computer to the remote computer, it is possible to get into a situation where the smart card reader cannot be used to log into the remote computer (for details on the interoperability of RGS and RDC, see [Interoperability of RGS and Microsoft Remote Desktop Connection on page 76](#)). This situation can arise as follows:

1. The user uses a smart card reader to log into the remote computer with RDC. Assume that this login session is established from the user's home.
2. Assume further that the user inadvertently leaves the RDC login session established, and departs for work.
3. From work, the user attempts to log into the remote computer with RGS using an at-work smart card reader in Easy Login mode. Because the home RDC login session is still active, RGS will require the user to authenticate the connection, which is not normally required with Easy Login.

However, the user may not have a login name and password—the user may be totally relying on smart card readers at home and at work to log into the remote computer. If the user is unable to authenticate the connection with a user name and password, the USB smart card reader will not be remotely mounted to the remote computer, and the user will not be able to log into the remote computer.

4. To prevent this situation, the user should log out from the RDC session prior to leaving home.
5. To address this situation if it occurs, the user can do one of the following:
  - Contact IT, and have an administrator log into the remote computer with RGS, which will terminate the RDC session. After the administrator disconnects the RGS connection, the user can establish an RGS connection using the smart card reader.
  - Restart the remote computer.
  - Return home, and log out from the RDC session.



**NOTE:** Unlike RDC, an RGS user can leave a remote "user session" created from the home RGS connection active and locked, and then log in from work with RGS. The home RGS connection **must be disconnected**, but the remote user login can be left in an active and locked state as previously stated. The smart card reader will operate correctly in both situations, and the work RGS login session will replace the home login session. If the home RGS connection is left connected, an Easy Login connection from work will not succeed because of the existing connection. The user will be required to perform steps similar to the steps in paragraph 5 above to be able to log in from work.

## Remote USB Access Control List

RGS supports a per-remote computer Access Control List (ACL) file that specifies which USB devices are allowed to be remotely attached to the remote computer from a local computer, and which USB devices are denied attachment. The ACL file, which resides on the remote computer, supports allowing/denying USB device attachments based on the following nine USB descriptor fields:

1. Device Class
2. Device Subclass
3. Device Protocol
4. Vendor ID
5. Product ID
6. Device BCD
7. Manufacturer
8. Product Type
9. Serial Number

USB device mounting can also be allowed/denied based on the following two parameters:

1. IP address of the local computer
2. The domain group of the local user

The ACL file supports two rule types: “allow” and “deny.” The rules are evaluated by the remote computer for each USB connection request from a local computer as follows:

- 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.

Therefore, a deny rule takes precedence over an allow rule. The ACL file is implemented as an Extensible Markup Language (XML) file. The ACL schema file is located at:

```
C:\Program Files\Hewlett-Packard\Remote Graphics Sender\hprUsbAcl.xsd
```

For backwards compatibility, the following default ACL file (installed during RGS Sender installation) allows all USB connections to be made:

```
C:\Program Files\Hewlett-Packard\Remote Graphics Sender  
\hprDefaultUsbAcl.xml
```

The names for these files can be changed using the properties described in [RGS Sender properties on page 91](#). The default ACL file contains the following contents, which allows all USB connections to be made:

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="no"?> <hprUsbAcl>  
rule type="allow"> <name>Allow all USB devices (HP default)</name> </  
rule> </ruleset> </hprUsbAcl>
```

The following example ACL file denies all Remote USB attachment requests:

```
<hprUsbAcl> <ruleset> <rule type="deny"/> </ruleset> </hprUsbAcl>
```

Rules may contain filters based on the 11 parameters listed previously. These parameters are repeated below along with the name of the filter element.

1. Device Class—bDeviceClass
2. Device Subclass—bDeviceSubclass
3. Device Protocol—bDeviceProtocol
4. Vendor ID—idVendor
5. Product ID—idProduct
6. Device BCD—bcdDevice
7. Manufacturer—manufacturer
8. Product Type—product
9. Serial Number—serialNumber



**IMPORTANT:** Filtering on device strings (manufacturer, product, and serial number) may not be reliable. Device vendors are not required to add data to these fields, and many do not. Before deploying a solution that depends on a string-based filter, ensure that the devices you wish to use implement the appropriate device strings.

10. IP address of the local computer—peerAddress
11. The domain group of the local user—group

The following ACL file allows only USB devices with a Device Class (bDeviceClass) of 7 to be remotely attached while denying everything else:

```
<hprUsbAcl> <ruleset> <rule type="allow"> <name>Allow printing devices</name> <filter bDeviceClass="07"/> </rule> </ruleset> </hprUsbAcl>
```

The following ACL file denies USB devices for a specific range of local computer IP addresses while allowing all other local computers to use Remote USB:

```
<hprUsbAcl> <ruleset> <rule type="allow"> <name>Allow all devices</name> </rule> <rule type="deny"> <name>Deny 192.168.9.0 subnet</name> <filter peerAddress="192.168.9.0/20"/> </rule> </ruleset> </hprUsbAcl>
```

The following ACL file allows USB connections for members of the DEFAULT-DOMAIN\administrators group while denying all other USB connections:

```
<hprUsbAcl> <ruleset> <rule type="allow"> <name>Allow members of DEFAULT-DOMAIN\administrators</name> <filter group="DEFAULT-DOMAIN\administrators"/> </rule> </ruleset> </hprUsbAcl>
```

## Determining USB device information

This section describes how to obtain several of the most-used USB device parameters.

### Determining USB device information for Windows

To obtain the Vendor ID and the Product ID for a USB device on Windows, perform the following steps:

1. Open the device manager.

- Go to the Control Panel and select **System**.
  - Select the **Hardware** tab.
  - Select **Device Manager**.
2. Double-click the **Universal Serial Bus Controllers**
  3. Double-click the specific device, which brings up a separate window.
  4. Select the **Details** tab and select one of the following properties from the pull down menu:
    - "Hardware Ids" property—This property shows the Vendor ID, Product ID and Revision for the device. The Vendor ID is the 4 hex digits after "Vid\_". The Product ID is the 4 hex digits after "Pid\_". The Revision is the 4 hex digits after "Rev\_". For example, an iPod has a "Hardware Ids" property that looks like this:

```
USB\Vid_05ac&Pid_120a&Rev_0001
```

This gives us the following values:

```
iPod Vendor ID : 0x05AC
```

```
iPod Product ID : 0x120A
```

```
iPod Revision : 0x0001
```

- "Compatible Ids" property—This property shows the class code, subclass code and protocol code for the device. The class code is the 2 hex digits after "Class\_". The subclass code is the 2 hex digits after the "SubClass\_". The protocol code is the 2 hex digits after the "Prot\_". For example, an iPod has a "Compatible Ids" property that looks like this:

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

This gives us the following values:

```
iPod Class Code : 08 (Mass Storage Device)
```

```
iPod Subclass Code : 06 (SCSI transparent command set)
```

```
iPod Protocol Code : 50 (Bulk-only transport)
```

## Determining USB device information for Linux

An open source program called "usbview" is available on the SourceForge website. There are three different programs called "usbview". The one to use is the "original" version. This is the plain usbview that was registered on "1999-12-20" and is administered by "kroah". Do not use "usbview2" or "usbview-1.8". Go to <http://sourceforge.net/projects/usbview>.

## Verifying the USB data

Once a device has been identified using one of the previous methods, you should verify that the correct device was used. This can be done by consulting one of the many USB ID lists. There are documents that contain most of the registered Vendor IDs and Device IDs. There are different documents that contain the different registered classes and subclasses. By comparing the values of the device to these documents, the user can verify that they are looking at the correct device and not some other device that is also plugged into the system.

The linux-usb group keeps an up-to-date list of registered USB Vendor IDs and Device IDs. Go to <http://www.linux-usb.org/usb.ids>.

The registered classes and subclasses are documented by the USB Device Working Group (DWG). The latest document from DWG for 1.0 defined class codes is hosted at: [http://www.usb.org/developers/defined\\_class](http://www.usb.org/developers/defined_class).



## Using RGS in Directory Mode (non-touch displays only)

Directory Mode enables the local user to automatically open connections to multiple remote computers based on the computers assigned to each user. When the user starts the RGS Receiver in Directory Mode, the RGS Receiver looks for a directory file containing user names and their assigned remote computers. The RGS Receiver reads this file to identify the remote computers assigned to the current user, and then attempts to automatically connect to each specified remote computer. The directory file may contain multiple users with a list of remote computers assigned to each user. The default directory file used by the RGS Receiver is:

```
C:\Program Files\Hewlett-Packard\Remote Graphics Receiver\directory.txt
```

After the directory file name is determined, the RGS Receiver automatically connects to the remote computers specified in this file for the named user.

### Directory file format

Often, the directory file is a common file for a group, department, organization, or an entire company. The directory file can manage and administer the remote computer assignments for any number of users. HP recommends that you save the directory file on a readily-accessible network file share or mapped drive so that each RGS Receiver can read the file at start-up.

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

```
domainName localuser remotecomputer1 remotecomputer2 ... remotecomputerN
```

where:

- The `domainName` on a Windows computer depends upon the environment the currently logged-in user is operating within. If the user is logged into their domain account, this means they are logged into an account specified by Microsoft Active Directory directory services. If the domain account is `worldwide\sally`, the name of the Windows domain is `worldwide` and will be used as the `domainName` for directory mode.

If the user is logged into the computer with a local account, `sally_computer\sally` for instance, the `domainName` used for directory mode is `sally_computer`. This typically will be a computer that is either standalone or part of a workgroup not using Active Directory directory services. The computer name, such as `sally_computer`, can be found by executing the command `hostname` in a command window.

For Linux users, use `UNIX` as the `domainName`.

- `localuser` is the name of the local user.
- `remotecomputer1`, `remotecomputer2` ... `remotecomputerN` are the remote computers assigned to the local user, as specified by either a hostname or an IP address.

For example, the following directory file specifies the remote computers for users Sally and Joe in a Microsoft Active Directory directory services environment:

```
worldwide sally RC_1 RC_2 RC_3
```

```
worldwide joe RC_4 RC_5 RC_6
```

In the next example, the directory file specifies the remote computers for users Sally and Joe in a standalone or workgroup environment.

```
sally_computer sally RC_1 RC_2 RC_3
```

```
joe_computer joe RC_4 RC_5 RC_6
```

In the above examples:

- Local user sally is assigned remote computers RC\_1, RC\_2, and RC\_3
- Local user joe is assigned remote computers RC\_4, RC\_5, and RC\_6

If the domain name, user name, or remote computer contains white-space characters, the name can be enclosed in double-quotes, as follows:

```
"domain 1" "sally user" "RC 1" "RC 2" "RC 3"
```

```
"domain 1" "joe user" "RC 4" "RC 5" "RC 6"
```

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 sally RC_1 RC_2 RC_3
```

Comment lines in the directory file are preceded by the “#” character in the first column.

## Starting the RGS Receiver in Directory Mode

Before attempting a connection in Directory Mode for the first time, HP recommends that you verify that RGS can connect to each computer individually (see [Creating an RGS connection on page 29](#)). The [Pre-connection checklist on page 23](#) can be used to verify that the computer and network parameters are set correctly. After individual connectivity is verified, start the RGS Receiver in Directory Mode.

To start the RGS Receiver in Directory Mode on Windows:

- ▲ Windows 7: Select **Start > All Programs > HP > HP Remote Graphics Software > HP RGS Receiver Directory Mode**.

Windows 8: Select the **HP RGS Receiver Directory Mode** tile on the Start screen.

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


```
C:\Program Files\Hewlett-Packard\Remote Graphics Receiver\rgreceiver.exe -
directory <filename>
```

```
C:\Program Files\Hewlett-Packard\Remote Graphics Receiver\rgreceiver.exe -
directory
```

If a file name is specified after -directory, the RGS Receiver will use that file as the directory file. If no file name is specified, the user is prompted by RGS to specify the path and name of the directory file.

In Directory Mode, the RGS Receiver Control Panel 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 remote computers listed in the directory file.

---

 **NOTE:** The RGS Sender is configured to start when the remote computer starts (or, in the case of Linux, also when the X server starts).

---

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

If Setup Mode is activated by the hotkey sequence (see [Setup Mode \(non-touch displays only\) on page 31](#)), and you have multiple Remote Display Windows on your computer, you can bring up the Remote Display Window selection dialog to view a thumbnail image of each Remote Display Window.

**Figure 8-1** Remote Display Window selection dialog



To display the selection dialog, press the **Tab** key while in Setup Mode—again, Setup Mode must have been previously activated by the hotkey sequence. The selection dialog is displayed as long as the initial Setup Mode hotkey (normally the **Shift** key) remains pressed. The currently-selected Remote Display Window is highlighted with a red border.

The Remote Display Window selection dialog is only displayed in Directory Mode—this is the mode that supports multiple Remote Display Windows. While the Remote Display Window selection dialog is active, navigate between windows (thumbnails) by:

- Pressing **Tab** to select the next window.
- Clicking on the number displayed beneath the thumbnail.
- Clicking directly on a thumbnail.
- Double-clicking the mouse on a thumbnail (this will also immediately close the selection dialog).

When the initial Setup Mode hotkey is released, the selected Remote Display Window is brought to the forefront and displayed.

## Game Mode (non-touch displays only)

**Game Mode** is a feature accessed via an RGS Receiver property (see [RGS Receiver properties on page 82](#) for more information).

When operating in normal cursor mode, RGS synchronizes the cursor movements of a remote computer to a controlling local computer by placing the remote computer's cursor at the same absolute coordinates as the local computer's cursor. Some applications rely on a relative movement of the cursor to interact with a 3D environment. These applications may programmatically readjust the cursor position after a movement is detected. In the default mode of operation where RGS is moving the cursor to an absolute position, these applications may have erratic behavior or cause a loss of cursor control. Game Mode is an attempt to provide better cursor control for such applications.

Game Mode is a toggle on the RGS Receiver to supply the remote computer with relative cursor movements. This will enable applications that rely on relative movements to be controlled with RGS. Game Mode is enabled and disabled by pressing the hot key followed by the **G** key. By default, the key sequence is **Shift** press, **Space** press, **Space** release, **G**.

When Game Mode is enabled, the cursor will be locked to the local computer's Remote Display Window. The Remote Display Window toolbar can be enabled, but interacting with the Remote Display Window toolbar is not possible when Game Mode is enabled. The local computer is dependent on the remote computer for updating the cursor position. Network connections with a high latency may not be suitable for use with Game Mode. The Remote Display Window can be repositioned without leaving Game Mode. When a connection is terminated, Game Mode will be disabled.

RGS may not be suitable for full screen games. The techniques used by games to quickly draw to the screen will often prevent RGS from being able to extract the contents of the remote frame buffer for display. This is often seen as partially rendered scene or a completely scrambled scene. A game that works in a windowed mode may be able to be controlled when Game Mode is enabled. However, the extremely high frame rates and low latencies required to successfully operate some games are not possible with the current RGS protocol. See [Application support on page 98](#) for the official description of supported applications.

## Auto-launching connections

On Windows, the RGS Receiver supports file association. You can create property files with the extension `.rgreceiver` using the same format as the RGS Receiver configuration file.



**NOTE:** See [Setting property values in a configuration file on page 81](#) for more information.

For example, the file `hostname.rgreceiver` could be used for creating a property configuration file for connecting to the system with name **hostname**.

If the user double-clicks or opens a file with the `.rgreceiver` extension, the RGS Receiver will be automatically started and the property file will be read and applied. Create a folder in the user's home folder to safely store Auto Launch configuration files.



**NOTE:** See [Auto-launch properties \(per-session\) on page 89](#) for property details.

## RGS Sender event logging (Windows only)

The RGS Sender event log file is named `HPRemote` and has several important usages:

- **Troubleshooting**—The `HPRemote` log can be used to aid troubleshooting of connection issues between the RGS Sender and Receiver. If you're unable to view the `HPRemote` log because of RGS connection difficulties, Remote Desktop can be used to connect to the remote computer to view the `HPRemote` log.
- **Remote application termination**—See [Remote application termination on page 65](#) for more information.
- **Other automated actions**—The basic principle behind using the `HPRemote` log to perform remote application termination can also be used to create an agent to automatically monitor and process other events logged by the RGS Sender.

## Viewing the HPRemote log

To view the `HPRemote` log:

1. Select **Start > Control Panel > Administrative Tools > Computer Management**.
2. In the left pane, navigate to **System Tools > Event Viewer > HPRemote**.

The `HPRemote` log reflects recent RGS connection activity. The log entries are in "Last In, First Out" (LIFO) order. By default, the most recent events are listed first.



**NOTE:** RGS event logging is supported only on the RGS Sender on Windows. It is not supported on the RGS Receiver.

To view the properties of a particular event, double-click the event of interest to open the Event Properties window.

This window displays the connection data in byte and word formats. The section [HPRemote log format on page 65](#) provides more details on the supported data formats.

## Additional information on event logging

For additional information on Windows event logging, search Microsoft Developer Network (MSDN) at <http://msdn.microsoft.com/>.

## Remote application termination

This section describes how to create a Windows agent on the remote computer that provides remote application termination.

A desktop session can operate independently of the RGS connection. This allows you to disconnect and reconnect to desktop sessions as part of a normal workflow. However, when an RGS connection is unintentionally disconnected, you might want remote applications to be terminated to prevent them from operating unsupervised.

For a sample agent, see [Sample agent on page 71](#).

## HPRemote log format

Data in the HPRemote log consists of a Message ID followed by optional data in both character string and binary data formats. Binary data provides direct access to data without requiring application parsing. Character strings format the binary data into human-readable messages compatible with the Windows Event Viewer. [Table 8-3 RGS Sender events logged in the HPRemote log on page 65](#) shows 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.

**Table 8-3 RGS Sender events logged in the HPRemote log**

Message ID	Description
RGSENDER_CONNECT_STATE EventID: 3	<p>The connection state consists of zero or more <b>primary</b> connections and zero or more <b>non-primary</b> connections. Each event entry records the current number of active connections in each category. Events appear when the connection status of these users 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 text string and binary, 32-bit unsigned integer for application use.</p> <p>Event Viewer Message:</p> <pre>Primary connections:%1. Non-primary connections:%2.</pre> <p>Strings:</p> <pre>%1 = number of primary connections %2 = number of non-primary connections</pre> <p>Data:</p> <pre>UINT32 numPrimary UINT32 numNonprimary</pre> <p>Event Viewer Example:</p> <pre>Primary connections:1 Non-primary connections:0</pre>

**Table 8-3 RGS Sender events logged in the HPRemote log (continued)**

Message ID	Description
RGSENDER_CONNECT EventID: 4	<p>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.</p> <p>Event Viewer Message:</p> <p>Connect %1.</p> <p>Strings:</p> <p>%1 = name associated with connection</p> <p>%2 = IP address and port number of local computer</p> <p>Data:</p> <p>None</p> <p>Event Viewer Example:</p> <p>Connect MYDOMAIN\myusername.</p>
RGSENDER_DISCONNECT EventID 5	<p>A local computer has disconnected. The message will contain the name associated with the connection. If Easy Login is enabled and the local computer disconnects prior to a login, the associated name may be Anonymous.</p> <p>Event Viewer Message:</p> <p>Disconnect %1.</p> <p>Strings:</p> <p>%1 = name associated with connection</p> <p>%2 = IP address and port number of local computer</p> <p>Data:</p> <p>None</p> <p>Event Viewer Example:</p> <p>Disconnect MYDOMAIN\myusername.</p>
RGSENDER_STARTUP EventID: 1	<p>Reference event registered to aid in interpretation of the event log by Event Viewer. Signifies proper startup of the RGS Sender service.</p> <p>Event Viewer Message:</p> <p>RGS Sender startup.</p> <p>Strings:</p> <p>None</p> <p>Data:</p> <p>None</p>
RGSENDER_SHUTDOWN EventID: 2	<p>Reference event registered to aid in interpretation of the event log by Event Viewer. Signifies proper shutdown of the RGS Sender service.</p> <p>Event Viewer Message:</p> <p>RGS Sender shutdown.</p>

**Table 8-3 RGS Sender events logged in the HPRemote log (continued)**

Message ID	Description
	<p><b>Strings:</b></p> <p>None</p> <p><b>Data:</b></p> <p>None</p>
RGSENDER_SET_PRIMARY EventID: 6	<p>A connection with an associated name is set as the primary connection.</p> <p><b>Event Viewer Message:</b></p> <p>Set %1 as primary connection.</p> <p><b>Strings:</b></p> <p>%1 = name associated with connection</p> <p><b>Data:</b></p> <p>None</p> <p><b>Event Viewer Example:</b></p> <p>Set MYDOMAIN\myusername as primary connection.</p>
RGSENDER_SET_NONPRIMARY EventID: 7	<p>A connection with an associated name is assigned to a non-primary status. This may happen as a result of a logout.</p> <p><b>Event Viewer Message:</b></p> <p>Set %1 as non-primary connection.</p> <p><b>Strings:</b></p> <p>%1 = name associated with connection</p> <p><b>Data:</b></p> <p>None</p> <p><b>Event Viewer Example:</b></p> <p>Set MYDOMAIN\myusername as non-primary connection.</p>
RGSENDER_ASSIGN_USER EventID: 8	<p>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.</p> <p><b>Event Viewer Message:</b></p> <p>Assign %1 connection to %2.</p> <p><b>Strings:</b></p> <p>%1 = original name of connection</p> <p>%2 = new name of connection</p> <p><b>Data:</b></p> <p>None</p> <p><b>Event Viewer Example:</b></p> <p>Assign Anonymous connection to MYDOMAIN\myusername.</p>

**Table 8-3 RGS Sender events logged in the HPRemote log (continued)**

Message ID	Description
RGSENDER_USB_CONNECT_DEVICE EventID: 9	<p>A new USB device was connected to the remote computer via Remote USB.</p> <p>Event Viewer Message:</p> <p>USB Device Connect:Class=%1, Vendor ID=%2, Product ID=%3, Manufacturer=%4, Product=%5</p> <p>Strings:</p> <p>%1 = USB device class</p> <p>%2 = USB device vendor ID</p> <p>%3 = USB device product ID</p> <p>%4 = USB device manufacturer string</p> <p>%5 = USB device product string</p> <p>Data:</p> <p>None</p>
RGSENDER_USB_DISCONNECT_DEVICE EventID: 10	<p>A new USB device was disconnected from the local computer and connected to the remote computer via Remote USB.</p> <p>Event Viewer Message:</p> <p>USB Device Connect:Class=%1, Vendor ID=%2, Product ID=%3, Manufacturer=%4, Product=%5</p> <p>Strings:</p> <p>%1 = USB device class</p> <p>%2 = USB device vendor ID</p> <p>%3 = USB device product ID</p> <p>%4 = USB device manufacturer string</p> <p>%5 = USB device product string</p> <p>Data:</p> <p>None</p>
RGSENDER_CONNECT_USB_DENIED EventID: 13	<p>A USB device connection was denied by the USB access control list.</p> <p>Event Viewer Message:</p> <p>USB Device Connect:Class=%1, Vendor ID=%2, Product ID=%3,</p> <p>Strings:</p> <p>%1 = USB device class</p> <p>%2 = USB device vendor ID</p> <p>%3 = USB device product ID</p> <p>Data:</p> <p>None</p>



## Agent design issues

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.

## Additional features for Windows systems

The following optional procedures for the RGS Sender service can improve the reliability of your remote agent solution.

### RGS Sender Service Recovery Settings

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

By default, most Windows services are installed without any automatic restart/recovery settings. This means that, when a service terminates, Windows will, by default, not restart the service unless explicitly set. When RGS Sender software is first installed, it is installed with the Windows default (do not restart).

Restarting the RGS Sender service can support RGS reconnection with a RGS Receiver client (unless a system error prevents the RGS service from restarting).

In designing the agent, you should consider whether or not 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 for automatic restart, you must adjust its **Recovery Property** through the **Administrative Tools** and **Services** control panel options.

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

## Microsoft Remote Desktop Recovery

If the RGS Sender becomes unavailable and the RGS Receiver can no longer connect to the RGS Sender, a Windows system with Remote Desktop services enabled can access the remote computer to diagnose the issue.

## 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 remote computer.

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 backslashes 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 with the RGS Sender and is located at:

```

C:\Program Files\Hewlett-Packard\Remote Graphics Sender\include
\RGSEvents.h

#include <windows.h>
#include <stdio.h>
#include "RGSEvents.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 ...  
}
```

## Interoperability of RGS and Microsoft Remote Desktop Connection

This section discusses interoperability considerations for RGS and Remote Desktop Connection (RDC). Because RGS and RDC both provide connection to a remote desktop, their interoperation is important to understand.

If a local user is connected to a remote computer using RDC and then attempts to establish an RGS connection, the RGS connection only works if the local user credentials match for both connections. This implies that the same user wants access to transition from RDC to an RGS connection. If the credentials match, the current RDC session disconnects, and the RGS Receiver takes control of the remote computer Windows desktop session. The current user does not log off, and work continues with the new connection.

The reverse works as well. If a user is connected with RGS and then connects with RDC (using the same credentials as the RGS connection), the RDC session displaces the RGS connection. In this case, the RGS Sender will disconnect all RGS Receivers (including all RGS collaborators). The Windows desktop session remains active during the switch.

If an RDC user disconnects from a remote computer using the RDC disconnect button, the session remains logged in, and all applications continue to run. The session, however, locks its screen. An RGS connection works only if the credentials match the currently logged-in user.

If a user logs out of their session while using RDC, the RGS Sender returns the system to its initial logged out state. Any authorized user can connect and log into this system using RGS.

An RDC connection made to a RGS Sender already occupied with a RGS connection by a non-matching user prompts the new user to logout the current RGS user. Only administrators can log out other users. Non-administrators are refused with a warning message about permissions. If RDC logs out the current RGS user, then the RGS Sender disconnects all of RGS Receivers (including all RGS collaborators).

Under reverse circumstances for the above, RGS connections will not log out an existing RDC user, regardless of authority. RGS will report an authorization failure message concerning a different user owning the desktop

**When RGS displaces an existing RDC session on Windows, the desktop may enter into a temporary logged in and unlocked state due to these operations. The user should exercise caution in situations where even a temporarily unlocked desktop is a security concern.**

Cause	Solution
Windows performs session operations that are outside the control of RGS.	This issue can be avoided by logging out of the RDC session before establishing an RGS connection.

## RGS security features

Because of the distributed nature of an RGS connection, providing connection security is critically important. RGS implements many features to provide connection security, including:

- **Authentication:** When a local user attempts to connect to a remote computer, the user credentials are validated using the native authentication method on the remote computer. If the credentials are not



authenticated, the connection is closed. On Windows, authentication uses NTLM or Kerberos. On Linux, authentication uses the Pluggable Authentication Module (PAM).

- **Authorization:** Multiple connections to the same remote computer are only allowed if the user logged into the desktop of the remote computer (primary user) allows the connection. When another user attempts to connect to the remote computer, an authorization dialog is displayed on the desktop of the remote computer that asks whether the new user should be allowed to connect.
- **Automatic desktop locking:** The desktop of the remote computer locks when the primary user disconnects. This prevents collaboration users from being able to interact with a remote session after the primary user has disconnected. This feature is supported on Windows. On Linux, this feature is supported on the Gnome, KDE, and CDE desktop environments.
- **Automatic disconnect:** On Linux, all RGS Receivers will disconnect when the primary user disconnects. This prevents collaboration users from interaction with a remote session after the primary user disconnects.
- **Automatic disconnect of collaboration users on login:** All collaboration users are disconnected when a login event occurs. Only the primary user remains connected when the desktop of the remote computer is logged in.
- **Automatic disconnect on logoff:** All RGS Receivers are disconnected when the primary user logs off of the remote desktop. This can be disabled by setting the `IsDisconnectOnLogoutEnabled` RGS Sender property to 0. See [RGS Sender properties on page 91](#).
- **Connection status:** A desktop icon in the application tray animates when other users are connected.
- **Collaboration notification:** See [Collaboration notification dialog on page 45](#).
- **Disconnect Everyone:** All RGS Receivers can be easily disconnected using the RGS Sender GUI. This is useful when hosting a collaboration session, such as in a classroom environment, and the session ends. The RGS Sender GUI is an icon in the system tray. Simply right-click the GUI and select **Disconnect > Everyone**.
- **Remote Keyboard/Mouse:** The RGS Sender GUI can enable or disable mouse and keyboard input for all collaboration users.
- **Single user connection:** A user, identified by a username, is only allowed one connection to a RGS Sender. If the same username connects more than once to a RGS Sender, the previous connection drops and the new connection continues on. If several users attempt to share a username, only one connection is active at a time.
- **SSL encryption:** SSL securely encrypts all data transmitted between a RGS Receiver and Sender pair.

## Remote computer monitor blanking operation


Monitor blanking on the remote computer is provided for security, so that the primary user's desktop session on the remote computer is not visible if a monitor is connected to the remote computer.

The default behavior is that the remote computer monitor will blank to black when the user connects and logs in. The remote computer monitor will un-blank when the user disconnects or logs out. Below are several additional details on monitor blanking on HP personal workstations:

- The one element on the monitor that does not go blank is the cursor.
- Blanking can take up to two seconds from the time the primary user logs in or reconnects until the time that the monitor is actually blanked.

- The HP personal workstations also block input from a directly connected keyboard and mouse when monitor blanking is occurring. When keyboard or mouse input is received by the remote computer, the monitor will enter the display powersave mode, and the cursor will be blanked as a result.
- An exception to input blocking is the **Ctrl+Alt+Del** key sequence. When this sequence is received by the remote computer from a directly-connected keyboard, the remote computer desktop will display the login dialog in the local computer. The remote computer monitor will remain blank while this occurs but the monitor will exit its powersave mode, and keyboard input will become unblocked until this dialog is dismissed.


---

 **NOTE:** Remote computer monitor blanking is not supported if the remote computer is a virtual machine (e.g., VMware ESX, Citrix Xen, etc).

---

If monitor blanking is enabled but the remote computer is unable to blank the display (because, for example, the computer is not one of the supported computers listed previously), a warning dialog is displayed on the local computer.

---

 **NOTE:** Linux screen blanking functionality is not supported on dual-monitor systems unless NVIDIA TwinView is in use.

---


The remote computer monitor blanking feature can be disabled by setting the following RGS Sender property to 0 (false).

```
Rgsender.IsBlankScreenAndBlockInputEnabled
```

If this property is set to 0, monitor blanking will be disabled, meaning that a monitor connected to the remote computer will display the user's desktop session. Furthermore, because monitor blanking is disabled, the warning dialog will not be displayed. For more details on this property, see [RGS Sender properties on page 91](#).

## Linux connection considerations

---

 **NOTE:** The **Switch User** functionality added to RHEL6 is not supported by RGS.

---

### Full-screen crosshair cursors

Certain applications that use large crosshair cursors (for example, Dassault Systemes ICEM Surf uses a full-screen crosshair cursor) will not display correctly on the local computer. Full-screen crosshair cursors can be disabled by typing the following in a terminal window:

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

This will force the application to use an X cursor, which will display correctly on the local computer.

### Gamma correction on the local computer

The color on a 3D application on the remote computer can look incorrect when displayed on a local computer. This is because the gamma of the local computer monitor may not match the gamma of the remote computer monitor. To correct this, any tool that will adjust the gamma for a display can be used. Some tools will adjust the gamma for the entire monitor, while others will adjust the gamma on a per-window basis. Per-window tools that can be used to adjust only the local computer window will provide the best results.

### Black or blank connection session with the RGS Sender on Linux

Connection to an X Server that is configured with less than 24-bit or 32-bit default visuals (depending on the graphics device) will cause the RGS Sender on Linux to generate a black or blank connection screen. For example, some default installations may configure a 16-bit visual in `/etc/X11/xorg.conf` after the

installation. Reconfiguring the X Server to serve 24-bit (or 32-bit) default visuals, and restarting the X Server will usually fix the black or blank connection situation.

---

# 9 RGS properties

RGS properties provide you with another way to customize RGS settings. Some properties correspond to settings that are also available in the GUI, while other properties correspond to settings that can only be set via a configuration file or the command line.

This chapter discusses the following topics:

- [Property syntax](#)
- [Setting property values in a configuration file](#)
- [Setting properties on the command line](#)
- [RGS Receiver properties](#)
- [RGS Sender properties](#)

## 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 the 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 the RGS Sender. This particular setting is duplicated in the Network tab of the RGS Receiver Control Panel 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 RGS Receiver uses the file `rgreceiverconfig` for its properties, while the RGS Sender uses the file `rgsenderconfig` file for its properties. On Windows, these files are located in the directory where the RGS Receiver and RGS Sender are installed. The defaults are as follows:

```
RGS Receiver: C:\Program Files\Hewlett-Packard\Remote Graphics Receiver  
\rgreceiverconfig
```

```
RGS Sender: C:\Program Files\Hewlett-Packard\Remote Graphics Sender  
\rgsenderconfig
```


On Linux, these files are located as follows:

```
RGS Receiver: /etc/opt/hpremove/rgreceiver/rgreceiverconfig
```


```
RGS Sender: /etc/opt/hpremove/rgsender/rgsenderconfig
```

The configuration files contain one property per line. Empty lines are ignored. The `#` character begins a comment on the line, extending to the end of the line. If a property is listed more than once, the value of the last entry is used.

---

 **NOTE:** 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.

---

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

---

## Setting properties on the command line

Properties can be set on the command line like in the following examples:

Windows: `rgreceiver.exe -Rgreceiver.Network.Timeout.Warning=10000`

Linux: `rgreceiver.sh -Rgreceiver.Network.Timeout.Warning=10000`



**NOTE:** Properties of the type **int vector** cannot be set on the command line.

## RGS Receiver properties

There are two types of RGS Receiver properties:

- **Global properties**—The global properties affect all RGS connections. See [RGS Receiver global properties on page 82](#) for detailed information about these properties.
- **Per-session properties**—The per-session (per-connection) properties allow the user to specify settings for each individual RGS connection. For example, in a many-to-one configuration, per-session properties can be specified for each Remote Display Window displayed by the RGS Receiver. See [RGS Receiver per-session properties on page 89](#) for detailed information about these properties.

## RGS Receiver property setting hierarchy

In this hierarchy, properties set by methods higher on the list override properties set by methods lower on the list (with 1 being the highest and 5 being the lowest):

1. Properties set in the RGS Receiver Control Panel
2. Properties set on the command line
3. Properties set in the RGS Receiver configuration file
4. Property settings retrieved from an archive file



**NOTE:** Properties set using the RGS Receiver Control Panel are saved in an archive file when the RGS Receiver is closed.

5. Default settings



**TIP:** All RGS Receiver properties can be restored to their default values by uninstalling and reinstalling the RGS Receiver.

## RGS Receiver global properties

### Remote Display Window properties

**Table 9-1 Remote Display Window properties**

`Rgreceiver.IsBordersEnabled`

1=Borders are enabled on the Remote Display Window (default).

0=Borders are disabled on the Remote Display Window.

`Rgreceiver.IsSnapEnabled`

1=The Remote Display Window will snap when close to the top or left edge of the screen (default).

0=Snapping is disabled.

`Rgreceiver.ImageCodec.IsMutable`

1=The image quality slider can be adjusted by a user, either in the RGS Receiver Control Panel or on the Remote Display Window toolbar (default).

**Table 9-1 Remote Display Window properties (continued)**

---

<code>0</code>	The image quality slider is disabled and cannot be adjusted by a user.
<code>Rgreceiver.ImageCodec.Quality</code>	
	The image quality can be set from a minimum of 0 to a maximum of 100. The default is 65.
<code>Rgreceiver.ImageCodec.IsBoostEnabled</code>	
<code>1</code>	Improves image quality for images containing significant amounts of text or lines (default).
<code>0</code>	Disables this setting.
<b>NOTE:</b>	This option is disabled when Advanced Video Compression is enabled.
<code>Rgreceiver.ImageCodec.IsH264Enabled</code>	
<code>1</code>	Enables the use of the H264 codec (Advanced Video Compression) to reduce network bandwidth consumption. See <a href="#">Advanced performance features on page 45</a> for more information about Advanced Video Compression.
<code>0</code>	Disables Advanced Video Compression (default).
<code>Rgreceiver.MaxSenderListSize</code>	
	This property specifies the size of the list of recent remote computers in the RGS Receiver. The default is 5.
<code>Rgreceiver.Directory</code>	
	This property specifies the file used for Directory Mode. The default is <code>directory.txt</code> .
<code>Rgreceiver.MaxImageUpdateRequests</code>	
	This property controls the maximum number of outstanding image update requests between the RGS Receiver (requestor) and the RGS Sender (responder).
	For example, a setting of 2 will allow the RGS Receiver to issue a second image update request to the RGS Sender prior to receiving the first image update response. This allows the RGS Sender and RGS Receiver to operate more in parallel, but at the potential expense of increased network bandwidth consumption.
	The maximum and default value is 4.
<code>Rgreceiver.ConnectionWarningColor</code>	
	This property sets the warning color that overlays the Remote Display Window when the RGS Receiver detects a network disruption. The warning color is a four byte number that specifies the alpha, red, green, and blue components of the color.
	The default value of the warning color is <code>0x80b40000</code> , representing the following:
	<ul style="list-style-type: none"><li>• The alpha component is <code>0x80</code> (128 decimal). This is 50% of full transparency (<code>0xFF</code>).</li><li>• The red component is <code>0xb4</code> (180 decimal). This is about 70% of full red (<code>0xFF</code>).</li><li>• The green component is <code>0x00</code>. There is no green component.</li><li>• The blue component is <code>0x00</code>. There is no blue component.</li></ul>
<code>Rgreceiver.IsMouseSyncEnabled</code>	
<code>1</code>	Mouse cursor snaps (such as to the default button of a dialog box) will be communicated by RGS (default).
<code>0</code>	Mouse cursor snaps are disabled.
<code>Rgreceiver.IsMenubarEnabled</code>	
<code>1</code>	The Remote Display Window toolbar is enabled (default).
<code>0</code>	The Remote Display Window toolbar is disabled.
<code>Rgreceiver.IsDisconnectWarningEnabled</code>	

---

**Table 9-1 Remote Display Window properties (continued)**

---

1=The RGS Receiver will display a warning that disconnecting an RGS connection will not automatically log them out of the remote computer.

0=This warning is disabled.

---

Rgreceiver.IsAlwaysPromptCredentialsEnabled

1=The RGS Receiver will always prompt for the domain, username, and password when establishing a connection.

0=The RGS Receiver will attempt to automatically verify the user's credentials in certain situations (default).

---

Rgreceiver.IsGlobalImageUpdateEnabled.IsMutable

1=The **Force full screen image updates** option in the RGS Receiver Control Panel can be modified by a user (default).

0=The **Force full screen image updates** option in the RGS Receiver Control Panel cannot be modified by a user.

---

Rgreceiver.IsGlobalImageUpdateEnabled

1=Enables the **Force full screen image updates** option.

0=Disables the **Force full screen image updates** option (default).

---

Rgreceiver.IsMatchReceiverResolutionEnabled

1=Enables the **Match Receiver display resolution** option.

0=Disables the **Match Receiver display resolution** option (default).

---

Rgreceiver.IsMatchReceiverPhysicalDisplaysEnabled

1=Enables the **Match Receiver display layout** option.

0=Disables the **Match Receiver display layout** option (default).

---

## Experience properties

**Table 9-2 Experience properties**

---

Rgreceiver.Experience.IsMutable

1=A user can use the RGS Receiver Control Panel to change the settings under the **Experience** heading (default).

0=A user cannot change the settings under the **Experience** heading.

---

Rgreceiver.Experience.Mode

FixedImageQuality=RGS does not utilize the **Adaptive image quality** settings (default).

AdjustImageQuality=RGS will utilize the **Adaptive image quality** settings.

---

Rgreceiver.Experience.MinImageQuality

The minimum image quality can be set from a minimum of 0 to a maximum of 100. The default is 20.

---

Rgreceiver.Experience.MinUpdateRate

The minimum update rate can be set from a minimum of 0 to a maximum of 30. The default is 30.

---



## Browser properties

**Table 9-3 Browser properties**

---

`Rgreceiver.Browser.IsMutable`

**NOTE:** This property only applies to Linux.

1=A user can use the RGS Receiver Control Panel to specify the name of the browser that is used to display this document.

0=The browser name cannot be changed by a user.

---

`Rgreceiver.Browser.Name`

**NOTE:** This property only applies to Linux.

This property specifies the name of the browser that is used to display this document. The default is `mozilla`.

---

## Audio properties

**Table 9-4 Audio properties**

---

`Rgreceiver.Audio.IsMutable`

1=A user can modify the audio settings in the RGS Receiver Control Panel (default).

0=A user cannot modify the audio settings in the RGS Receiver Control Panel.

---

`Rgreceiver.Audio.IsEnabled`

1=Remote Audio is enabled (default).

0=Remote Audio is disabled.

---

`Rgreceiver.Audio.IsInStereo`

1=Stereo audio is enabled (default).

0=Stereo audio is disabled.

---

`Rgreceiver.Audio.IsFollowsFocusEnabled`

1=The audio will play from whichever Remote Display Window has the current focus.

0=The audio will play combined from all Remote Display Windows (default).

---

`Rgreceiver.Audio.Quality`

2=Audio plays at the CD quality of 44 KHz.

1=Audio plays at the medium quality of 22 KHz (default).

0=Audio plays at the low quality of 11 KHz.

---

## Microphone properties

**Table 9-5 Microphone properties**

---

`Rgreceiver.Mic.IsEnabled`

1=Microphones can be removed.

0=Microphones cannot be removed (default).

---

## USB properties

**Table 9-6 USB properties**

---

`Rgreceiver.Usb.IsMutable`

1=A user can modify the Remote USB settings in the RGS Receiver Control Panel (default).

0=A user cannot modify the Remote USB settings in the RGS Receiver Control Panel.

---

`Rgreceiver.Usb.IsEnabled`

1=Remote USB is enabled (default).

0=Remote USB is disabled.

---

`Rgreceiver.Usb.ActiveSession`

This property specifies which remote computer to attach USB devices to for Directory Mode. 0 is the first remote computer, 1 is the second remote computer, and so on.

**NOTE:** After changing this setting, you must disconnect and then reconnect all RGS connections.

---

## Network properties

**Table 9-7 Network properties**

---

`Rgreceiver.Network.Timeout.IsMutable`

1=A user can modify the network timeout settings in the RGS Receiver Control Panel (default).

0=A user cannot modify the network timeout settings in the RGS Receiver Control Panel.

---

`Rgreceiver.Network.Timeout.IsGuiEnabled`

1=Enables the warning dialog for when the RGS connection is about to time out due to the inability to contact the RGS Sender (default).

0=Disables this warning dialog.

---

`Rgreceiver.Network.Timeout.Error`

This property sets the time in milliseconds that the RGS Receiver will wait before ending the connection after failing to detect the RGS Sender. The default is 30000 milliseconds (30 seconds).

---

`Rgreceiver.Network.Timeout.Warning`

This property sets the time in milliseconds that the RGS Receiver will wait before displaying a warning dialog to the local user after failing to detect the RGS Sender. The default is 2000 milliseconds (2 seconds).

---

`Rgreceiver.Network.Timeout.Dialog`

This property sets the time in milliseconds that the RGS Receiver will wait for a response to a dialog being displayed on the remote computer (such as an authentication dialog). The request will be canceled if there is no response. The default is 15000 milliseconds (15 seconds).

---

`Rgreceiver.Network.Port`

This property specifies the port used for communication between the RGS Receiver and RGS Sender. This setting must match the port setting on the RGS Sender. The default is 42966.

---

`Rgreceiver.Network.HPVelocity.Mode`

3=HP Velocity operates in Active mode (default).

1=HP Velocity operates in Monitor mode.

**Table 9-7 Network properties (continued)**

---

<code>0=HP Velocity is disabled.</code>
<b>NOTE:</b> See HP Velocity documentation for more information.
<code>Rgreceiver.Network.HPVelocity.TargetLossRate</code>
<code>3=The target loss rate used by HP Velocity is 0.04% (default).</code>
<code>2=The target loss rate used by HP Velocity is 0.1%.</code>
<code>1=The target loss rate used by HP Velocity is 0.2%.</code>
<code>0=The target loss rate used by HP Velocity is 0.4%.</code>
<b>NOTE:</b> See HP Velocity documentation for more information.
<code>Rgreceiver.Network.HPVelocity.NetworkInterface</code>
<b>NOTE:</b> This property only applies to Linux.
This property specifies the active network interface. The default is <code>eth0</code> .

---

## Hotkey properties

**Table 9-8 Hotkey properties**

---

<code>Rgreceiver.Hotkeys.IsMutable</code>
<code>1=A user can modify the hotkey settings in the RGS Receiver Control Panel (default).</code>
<code>0=A user cannot modify the hotkey settings in the RGS Receiver Control Panel.</code>
<code>Rgreceiver.Hotkeys.IsSetupModeEnabled</code>
<code>1=Enables the Setup Mode hotkey sequence (default).</code>
<code>0=Disables the Setup Mode hotkey sequence.</code>
<code>Rgreceiver.Hotkeys.SetupModeSequence</code>
Specifies the Setup Mode hotkey sequence. The default is <code>Shift Down, Space Down, Space Up</code> .
<code>Rgreceiver.Hotkeys.IsSendCtrlAltEndAsCtrlAltDeleteEnabled</code>
<code>1=Enables the <b>Send CTRL-ALT-END key sequence as CTRL-ALT-DEL</b> option (default).</code>
<code>0=Disables the <b>Send CTRL-ALT-END key sequence as CTRL-ALT-DEL</b> option.</code>
<code>Rgreceiver.Hotkeys.IsSendFirstKeyInSequenceEnabled</code>
<code>1=Enables the <b>Send First Key</b> option.</code>
<code>0=Disables the <b>Send First Key</b> option (default).</code>
<code>Rgreceiver.Hotkeys.IsKeyRepeatEnabled</code>
<code>1=Enables the <b>Key Repeat</b> option.</code>
<code>0=Disables the <b>Key Repeat</b> option (default).</code>
<code>Rgreceiver.Hotkeys.IsCtrlAltDeletePassThroughEnabled</code>
<code>1=Both the remote and local computers will process a <b>Ctrl+Alt+Delete</b> sequence.</code>

**Table 9-8 Hotkey properties (continued)**

---

0=Only the local computer will process a **Ctrl+Alt+Delete** sequence. (default).

---

`Rgreceiver.Hotkeys.IsGameModeEnabled`

1=Enables Game Mode (default).

0=Disables Game Mode.

---

## Clipboard properties



**NOTE:** For per-session clipboard properties, see [Clipboard properties \(per-session\) on page 91](#).

**Table 9-9 Clipboard properties**

---

`Rgreceiver.Clipboard.IsMutable`

1=A user can modify the Remote Clipboard setting in the RGS Receiver Control Panel (default).

0=A user cannot modify the Remote Clipboard setting in the RGS Receiver Control Panel.

---

`Rgreceiver.Clipboard.IsEnabled`

1=Enables Remote Clipboard (default).

0=Disables Remote Clipboard.

---

`Rgreceiver.Clipboard.FilterString`

**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.

This property is a string that specifies the clipboard formats that are allowed to be transferred using Remote Clipboard. The default is as follows:

```
|1|7|8|13|16|17|Ole Private Data|Object Descriptor|Link Source Descriptor|HTML Format|Rich Text Format|XML Spreadsheet|
```

For more information about these clipboard formats, see <http://msdn2.microsoft.com/en-us/library/ms649013.aspx>.

---

## Logging properties

**Table 9-10 Logging properties**

---

`Rgreceiver.Log.IsMutable`

1=A user can modify the logging settings in the RGS Receiver Control Panel (default).

0=A user cannot modify the logging settings in the RGS Receiver Control Panel.

---

`Rgreceiver.Log.IsFileLoggerEnabled`

1=Enables logging for the RGS Receiver (default).

0=Disables logging for the RGS Receiver.

---

`Rgreceiver.Log.Level`

DEBUG=Enables logging for all five types of output.

INFO=Enables logging for output type INFO and anything more serious (WARN, ERROR, and FATAL).

WARN=Enables logging for output type WARN and anything more serious (ERROR and FATAL).

---

**Table 9-10 Logging properties (continued)**

---

<code>ERROR</code>	=Enables logging for output type ERROR and anything more serious (FATAL).
<code>FATAL</code>	=Enables logging for only FATAL output.
<hr/>	
<code>Rgreceiver.Log.FileName</code>	
This property specifies the path to the RGS Receiver log file. The defaults are as follows:	
<b>Windows:</b>	<code>C:/Program Files/Hewlett-Packard/Remote Graphics Receiver/rg.log</code>
<b>Linux:</b>	<code>\$HOME/.hpremove/rgreceiver/rg.log</code>
<hr/>	
<code>Rgreceiver.Log.MaxFileSize</code>	
This property sets the maximum size of the log file in kilobytes (KB). The default is 1024 (1 MB).	

---

## Registration properties

**Table 9-11 Registration properties**

---

<code>Rgreceiver.Registration.IsMutable</code>	
1=A user can set whether registration of advanced RGS features is enabled.	
0=A user cannot set whether registration of advanced RGS features is enabled.	
<hr/>	
<code>Rgreceiver.Registration.IsEnabled</code>	
1=Enables registration to the HP registration server, which is required to use advanced RGS features (default).	
0=Disables registration to the HP registration server.	

---

## Proxy server properties

**Table 9-12 Proxy server properties**


---

<code>Rgreceiver.Network.ProxyEnabled</code>	
1=Enables the use of a proxy server for registration of advanced RGS features.	
0=Disables the use of a proxy server for registration of advanced RGS features (default).	
<hr/>	
<code>Rgreceiver.Network.ProxyPort</code>	
This property sets a proxy server port to use for registration of advanced RGS features. There is no default value.	
<hr/>	
<code>Rgreceiver.Network.ProxyAddress</code>	
This property sets a proxy server address to use for registration of advanced RGS features. There is no default value.	

---

## RGS Receiver per-session properties

### Auto-launch properties (per-session)

 **NOTE:** The auto-launch properties are used only on Windows and do not have default settings.

**Table 9-13 Auto-launch properties (per-session)**

---

<code>Rgreceiver.Session.&lt;n&gt;.IsConnectOnStartup</code>
--

**Table 9-13 Auto-launch properties (per-session) (continued)**

1=The RGS Receiver will attempt to auto-launch the connection for session number *n* using settings from the other properties in this table.

0=The RGS Receiver will not attempt to auto-launch the connection for session number *n*.

`Rgreceiver.Session.<n>.Hostname`

This property sets the hostname for session number *n*.

`Rgreceiver.Session.<n>.Username`

This property sets the username for session number *n* as a UTF-8 encoded string.

`Rgreceiver.Session.<n>.Password`

This property sets the password for session number *n* as a UTF-8 encoded string.

`Rgreceiver.Session.<n>.PasswordFormat`

`Encrypted`=Sets the password format for session number *n*. This format is only supported on Windows and is the hexadecimal string representation of the password encrypted using the Windows command `CryptProtectData`. See [http://msdn.microsoft.com/en-us/library/aa380261\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa380261(VS.85).aspx) for more information.

`Clear`=Sets the password format for session number *n*. This format is the password as clear text.

`XOR`=Sets the password format for session number *n*. This format is the hexadecimal string representation of a password encrypted using an XOR cipher using a key of 129.

## Window location and size properties (per-session)

**Table 9-14 Window location and size properties (per-session)**

`Rgreceiver.Session.<n>.RemoteDisplayWindow.X`

This property sets the horizontal position of the Remote Display Window for session number *n*, as measured from the left edge of the screen. The default is 0.

`Rgreceiver.Session.<n>.RemoteDisplayWindow.Y`

This property sets the vertical position of the Remote Display Window for session number *n*, as measured from the top edge of the screen. The default is 0.

`Rgreceiver.Session.<n>.VirtualDisplay.IsPreferredResolutionEnabled`

1=Enables the preferred resolution properties for session number *n*. This resolution is communicated to the remote computer, which will attempt to adapt its resolution to match the resolution preference of the local computer. If the remote computer is unable to match the resolution preference of the local computer, a warning dialog is displayed on the local computer.

0=Disables the preferred resolution properties for session number *n* (default).

**NOTE:** The per-session preferred resolution properties override the global property

`Rgreceiver.IsMatchReceiverResolutionEnabled`.

`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*.

## Clipboard properties (per-session)



**NOTE:** For global clipboard properties, see [Clipboard properties on page 88](#).

**Table 9-15 Clipboard properties (per-session)**

`Rgreceiver.Session.<n>.Clipboard.IsEnabled`

1=Enables Remote Clipboard for session number *n* (default).

0=Disables Remote Clipboard for session number *n*.

**NOTE:** For Remote Clipboard to be enabled for any session, the general clipboard property `Rgreceiver.Clipboard.IsEnabled` must also be set to 1.

## RGS Sender properties

In this hierarchy, properties set by methods higher on the list override properties set by methods lower on the list (with 1 being the highest and 3 being the lowest):

1. Properties set on the command line
2. Properties set in the RGS Sender configuration file
3. Default settings

**Table 9-16 RGS Sender properties**

`Rgsender.MaxImageUpdateRate`

This property sets the maximum number of image updates per second. The default is 30. With a setting of 0, the update rate will be unlimited.

`Rgsender.ImageCodec.Preferred`

NC=This codec (HP3) has been the default since release 5.0.

HP2=This codec was the default prior to release 5.0.

JPEG-LS=This codec is mathematically lossless.

`Rgsender.IsDisconnectOnLogoutEnabled`

1=The RGS Sender will end the RGS connection and disconnect all collaborators when the primary user logs out (default).

0=The RGS connection will not be ended when the primary user logs out.

`Rgsender.IsIloRemoteConsoleEnabled`

**NOTE:** This property only applies to Linux.

1=The iLO console can be simultaneously enabled with an RGS connection, which could allow eavesdropping.

0=The iLO console will be disabled when an RGS connection is established (default).

`Rgsender.PreferredDisplayMethods`

This property sets the order of methods to detect image changes. The default is `GPU ChangeList Comparitron`. If a method is not currently supported with the system, the next method in the string will be tried.

GPU=This method uses the GPU hardware to quickly compare one full screen to a previous full screen

ChangeList=This method uses the RGS mirror-driver on Windows and the RGS X server extension on Linux to detect display changes.

**Table 9-16 RGS Sender properties (continued)**

---

`Comparitron`=This method uses the system's CPU to compare one full screen to a previous full screen. This method is supported on Windows only. Animated cursors will be displayed as a static cursor.

---

`Rgsender.IsCollaborationNotificationEnabled`

1=Enables the collaboration notification dialog (default).

0=Disables the collaboration notification dialog.

**IMPORTANT:** This property should normally remain enabled. When disabled, neither remote users or local users will be notified who is participating in a collaboration session. The warning dialog that is displayed when the remote computer is unable to blank its monitor will also be prevented from being displayed.

---

`Rgsender.IsReconnectOnConsoleDisconnectEnabled`

1=Enables session re-connection after logout or Fast User Switching (default).

0=Disables session re-connection.

---

`Rgsender.ConsoleLogonTimeout`

This property sets the time in seconds to wait for a system login event to complete. The default is 30 seconds. If the login does not occur within this limit, the remote computer will be shut down.

---

`Rgsender.Network.Timeout.Error`

This property sets the time in milliseconds that the RGS Sender will wait before ending the connection after failing to detect the RGS Receiver. The default is 30000 milliseconds (30 seconds).

---

`Rgsender.Network.Timeout.Dialog`

This property sets the time in milliseconds that the RGS Sender will wait for a response to a dialog being displayed on the remote computer (such as an authentication dialog). The request will be canceled if there is no response. The default is 15000 milliseconds (15 seconds).

---

`Rgsender.Network.IsListenOnAllInterfacesEnabled`

1=The RGS Sender will accept connections on all network interfaces (default).

0=The RGS Sender will not accept connections on all network interfaces.

---

`Rgsender.Network.Interface.<n>.IsEnabled`

1=The RGS Sender will accept connections on network interface number *n*.

0=The RGS Sender will not accept connections on network interface number *n*.

On Linux, these values generally correspond with `eth0`, `eth1`, and so on. See [RGS Sender network interface binding on page 25](#) for more information about on how to determine these values on Windows.

---

`Rgsender.Network.AllowIpAddressSubnet`

This property specifies the range of IP addresses that the RGS Sender will listen on for a connection request from the RGS Receiver. A network interface must be enabled using the property `Rgsender.Network.Interface.<n>.IsEnabled`, and its IP address must be in the range specified by this property.

**NOTE:** This property is ignored if `Rgsender.Network.IsListenOnAllInterfacesEnabled` is set to 1.

**NOTE:** This property does not restrict incoming IP addresses from receiving computers. See `ipfilter.txt` for information on how to filter receiving computers by IP address.

---

`Rgsender.Network.Port`

This property specifies the port used for communication between the RGS Sender and RGS Receiver. This setting much match the port setting on the RGS Receiver. The default is 42966.

---

`Rgsender.Network.HPVelocity.Mode`

---



**Table 9-16 RGS Sender properties (continued)**

---

3=HP Velocity operates in Active mode (default).

1=HP Velocity operates in Monitor mode.

0=HP Velocity is disabled.

**NOTE:** See HP Velocity documentation for more information.

---

`Rgsender.Network.HPVelocity.TargetLossRate`

3=The target loss rate used by HP Velocity is 0.04% (default).

2=The target loss rate used by HP Velocity is 0.1%.

1=The target loss rate used by HP Velocity is 0.2%.

0=The target loss rate used by HP Velocity is 0.4%.

**NOTE:** See HP Velocity documentation for more information.

---

`Rgsender.Network.HPVelocity.NetworkInterface`

**NOTE:** This property only applies to Linux.

This property specifies the active network interface. The default is `eth0`.

---

`Rgsender.Network.HPVelocity.EnablePlp`

1=Enables packet loss protection for HP Velocity (default).

0=Disables packet loss protection for HP Velocity.

**NOTE:** See HP Velocity documentation for more information.

---

`Rgsender.Network.HPVelocity.LiveTcpCongestionControlAlgorithm`

1=Friendly.

0=Aggressive (default).

**NOTE:** See HP Velocity documentation for more information.

---

`Rgsender.IsBlankScreenAndBlockInputEnabled`

1=The remote computer's screen will blank and its keyboard and mouse will disable when a primary user connects (default).

0=The remote computer's screen will not blank and its keyboard and mouse will not disable.

---

`Rgsender.Usb.Acl.RuleSetPath`

This property specifies the name of the XML file that implements the Remote USB Access Control List (ACL). The default is `hprDefaultUsbAcl.xml`.

---

`Rgsender.Usb.Acl.SchemaPath`

This property specifies the name of the schema file that accompanies the Remote USB XML file. The default is `hprUsbAcl.xsd`.

---

`Rgsender.Usb.Acl.RuleSetErrorTimeout`

This property sets the amount of time in milliseconds that the RGS Sender will wait before disconnecting all USB devices if the USB ACL file disappears or becomes inaccessible. The default is 5000 milliseconds (5 seconds). If the file is restored prior to expiration of the timeout period, the USB devices remain connected.

---

`Rgsender.Clipboard.IsEnabled`

1=Enables Remote Clipboard (default).

0=Disables Remote Clipboard.

---

**Table 9-16 RGS Sender properties (continued)**

---

`Rgsender.IsClassicEasyLogonEnabled`

1=For Windows, this enables multiple users to connect to a locked desktop before logon. For Linux, this enables Easy Logon.

0=For Windows, this disables the ability for multiple users to connect to a locked desktop before logon. For Linux, this disables Easy Logon. This is the default setting for both Windows and Linux.

---

`Rgsender.Audio.IsEnabled`

1=Enables Remote Audio (default).

0=Disables Remote Audio.

---

`Rgsender.Mic.IsEnabled`

1=Enables Remote Microphone (default).

0=Disables Remote Microphone.

---

`Rgsender.CollabUI.Dialog.Timeout`

This property sets the amount of time in milliseconds that the collaboration authentication dialog is shown. The default is 15000 milliseconds (15 seconds). After that amount of time, the collaboration request is denied.

---

`Rgsender.RequestFloorControlTime`

This property 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 default is 500 milliseconds (0.5 seconds), which is the minimum accepted value. The maximum is 15000 milliseconds (15 seconds).

---

`Rgsender.Collaboration.AlwaysAcceptCollaborators`

1=Collaborators will always be accepted without having to be authorized by the primary user.

0=Collaborators will have to be authorized (default).


---


# A Supported hardware and software

## RGS support matrix

**Table A-1 RGS support matrix**

	Windows 7 Professional, Enterprise	Windows 8.1 Pro, Enterprise	RHEL 5.9, 6.6	SLED 11.3
<b>RGS Sender</b>				
HP Z workstations	✓	✓	✓	✓
HP WS460c (Gen6)	64-bit Bare Metal & Citrix XenServer v6			
HP WS460c (Gen8)	64-bit Bare Metal & Citrix XenServer v6		64-bit Bare Metal & Citrix XenServer v6	
HP SL390 (Gen7)	64-bit Bare Metal & Citrix XenServer v6		64-bit Bare Metal & Citrix XenServer v6	
HP SL250 (Gen8)	64-bit Bare Metal & Citrix XenServer v6		64-bit Bare Metal & Citrix XenServer v6	
HP DL380 (Gen8)	64-bit Bare Metal & Citrix XenServer v6		64-bit Bare Metal & Citrix XenServer v6	
HP Moonshot M700	✓			
<b>RGS Receiver</b>				
Desktops/notebooks	✓	✓	✓	✓
Tablets		✓		
<b>RGS Receiver (HP thin clients)</b>				
	<b>Windows Embedded</b>		<b>Embedded Linux</b>	
HP t610	WES7, WES8		HP ThinPro 4.3, 4.4, 5.0	
HP t620	WES7, WES8		HP ThinPro 4.4, 5.0	
HP t820	WES7, WES8			
HP mt40/mt41	WES7			

 **NOTE:** Both the remote and local computers require 1.5 GHz or greater processor with SSE2 multimedia instruction extension, 32-bit color display adapter, and 512 MB minimum RAM. The RGS Sender supports NVIDIA Quadro and AMD FirePro graphics only. Supported Linux distributions might require specific versions of the kernel, xorg.config, and/or xserver.

 **NOTE:** Remote USB is not supported with the Linux version of the RGS Sender.

# Advanced Video Compression requirements

**Table A-2 Advanced Video Compression requirements**

Remote computer (RGS Sender)	Local computer (RGS Receiver)
<p><b>CPU encoding</b>—4 cores or more running at 2 GHz (minimum); 8 cores or more running at 2 GHz (recommended)</p> <p><b>NOTE:</b> If using GPU encoding, the CPU only needs to meet the requirements listed in <a href="#">RGS support matrix on page 95</a>.</p>	<p><b>CPU decoding</b>—2 cores or more running at 2 GHz</p>
<p><b>GPU encoding</b>—NVIDIA Quadro 2000 or better graphics card with driver version 305.29 or greater</p> <p><b>NOTE:</b> If the GPU requirements are not met, RGS will revert to CPU encoding.</p> <p><b>NOTE:</b> If you are running the RGS Sender on RHEL, RGS will revert to CPU encoding.</p>	
<p><b>IMPORTANT:</b> Internet access on the local computer is required for a one-time Advanced Features activation. If a proxy is required, the system must be set up with manual proxy configuration. Activation will not work with PAC or WAPD (automatic configuration script and automatic proxy detection).</p>	

## Remote Audio device support on Linux

An audio device is required to be installed on Linux-based remote computers for application-generated audio to be sent to the local computer. Furthermore, the audio device installed in the remote computer 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.

RGS will attempt to capture application-generated audio from the remote computer and play the result on the local computer. Not all audio device drivers provide the capability to capture application-generated audio.


The following list of audio devices are known to work on RHEL5:


- SoundBlaster Audigy 4—SB0660
- SoundBlaster Audigy 4—SB0610
- SoundBlaster Audigy 2ZS—SB0350
- SoundBlaster—SB0160
- SoundBlaster Live!—CT4780
- SoundBlaster Live!—CT4760

HP personal workstations have a high-definition audio device on the motherboard. This device is known to use a driver on RHEL5 that does not allow RGS to capture application generated audio.

The virtual audio driver for Linux can be used on systems without audio hardware. In some cases, it might be desirable to disable the physical audio device and install the virtual audio driver. The driver and appropriate libraries need to be compiled and installed to match the current Linux kernel. The source code and instructions for installation are in the file `virtual_audio_driver.tar`.

---

 **IMPORTANT:** The Linux virtual audio driver is the only supported audio device for RHEL 6. Hardware audio devices are not supported.

 **NOTE:** The Linux virtual audio driver is not supported in a virtual machine. Timing information from the kernel in a virtual machine may not be precise enough to ensure consistent audio quality.

---

## Keyboard locale support

The following keyboard localizations are supported when connected to a RGS Sender on Linux:

1. French
2. German
3. Japanese
4. Norwegian
5. Swedish
6. United Kingdom
7. U.S. English

The following keyboard localizations are supported when connected to a RGS Sender on Windows:

1. Belgian French
2. Canadian French
3. Chinese (Simplified)—U.S. Keyboard
4. Chinese (Traditional)—U.S. Keyboard
5. Czech
6. Czech (QWERTY)
7. Danish
8. Dutch
9. Finnish
10. French
11. German
12. Italian
13. Japanese
14. Korean
15. Latin American
16. Norwegian
17. Portuguese
18. Portuguese (Brazilian ABNT)
19. Russian
20. Spanish

21. Swedish
22. Swiss French
23. Swiss German
24. Turkish Q
25. United Kingdom
26. United Kingdom Extended
27. United States—International
28. U.S.

## Application support

RGS supports all applications, except those applications that use full screen exclusive mode. RGS may not be suitable for most full screen games. If a full-screen MS-DOS command prompt window is created on the remote computer (using, for example, `command.com`), the window will be reset to its default size by RGS. Likewise, if a full-screen Windows command prompt window is created (using `cmd.exe` or the command prompt icon), the window will also be reset to its default size by RGS. Full-screen DirectDraw applications are not supported; however, DirectDraw applications in a window might work and can be qualified individually.

On remote computers running Linux, OpenGL-based applications can only be remoted if the remote computer is using NVIDIA graphics.

The RGS Sender and RGS Receiver executables are designed for compatibility with strict anti-virus programs.

## Video overlay surfaces

When the RGS Sender on Windows is installed on a computer, video overlay surfaces (also known as overlay planes) are disabled on the computer. Some media players that use video overlay surfaces will not display correctly. This can often be resolved by disabling the use of video overlay surfaces in the media player.

Most OpenGL applications will detect the disabling of overlay surfaces, and will work correctly. However, if your OpenGL application attempts to use the disabled overlay surfaces, it may display incorrectly. If this is the case, check to see if your OpenGL application provides a mechanism for the user to manually disable the use of overlay surfaces.

# B Troubleshooting

This appendix provides suggestions on troubleshooting potential issues with RGS and also lists the RGS error messages and their possible causes.

## Potential issues and suggestions

**Table B-1 Potential RGS issues and troubleshooting suggestions**

Issue	Suggestion
Cannot connect to the RGS Sender.	Verify that the pre-connection checklist is satisfied as described in <a href="#">Pre-connection checklist on page 23</a> .
A connection is established but it appears to time out.	See the section <a href="#">Troubleshooting network timeouts on page 99</a> .
Graphics performance appears slow.	See <a href="#">Optimizing RGS performance on page 45</a> .
Remote Audio doesn't work.	<ul style="list-style-type: none"><li>• If using a RGS Receiver on Linux, verify that audio has been installed correctly as described in <a href="#">RGS Receiver audio requirements on Linux on page 19</a>.</li><li>• See the troubleshooting suggestions in <a href="#">Troubleshooting Remote Audio on page 102</a>.</li></ul>
Remote USB doesn't work.	<ul style="list-style-type: none"><li>• Verify that USB has been correctly configured during RGS Receiver installation on Windows as described in <a href="#">Installing the RGS Receiver on Windows on page 12</a>.</li><li>• See the troubleshooting suggestions in <a href="#">Troubleshooting Remote USB on page 104</a>.</li></ul>
I want to restore the RGS Receiver properties to factory defaults.	Uninstall and reinstall the RGS Receiver.

### Troubleshooting network timeouts

RGS uses TCP/IP over a standard computer network to transmit data. Although TCP/IP is a reliable transport mechanism, it does not guarantee network packet delivery. The TCP/IP network stack performs well on a relatively stable network. However, network issues beyond RGS can affect the probability and timing of network packet delivery. Possible network issues include:

- 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
- A disconnected network cable

To deal with such network issues, the RGS Receiver and Sender both support network timeout mechanisms to provide notification to the user of network issues.

#### RGS Receiver network timeout

RGS provides two user-settable RGS Receiver timeout properties to allow you to optimize RGS for your particular network conditions (such as low-bandwidth or high-latency conditions). These properties allow

you to specify timeout values that, if exceeded, will cause the RGS Receiver to take specific actions, such as displaying a warning dialog or closing the RGS connection. The two RGS Receiver timeout properties are:

- **RGS Receiver warning timeout property**—If this value is exceeded, the RGS Receiver displays a network connection warning.
- **RGS Receiver error timeout property**—If this value is exceeded, the RGS Receiver closes the connection.

The RGS Receiver error and warning timeout properties can be set in the RGS Receiver Control Panel and are specified in seconds. The RGS Receiver timeout properties can also be set in the `rgreceiverconfig` file or on a command line—in both of these cases, the timeout properties are specified in milliseconds.

If a temporary network disruption occurs for less time than the RGS Receiver warning timeout property, the RGS Receiver will not display a warning, and the user will experience only a brief drop in Remote Display Window interactivity. This means, for example, that a user moving or scrolling a window might see a momentary decrease in interactivity. If the user is not interacting with the Remote Display Window during a temporary network disruption, the network disruption may not even be noticeable (unless dynamic content such as video fails to update at an appropriate rate).



**NOTE:** In many cases, the TCP/IP network stack is able to detect and resolve network errors, such as a transmitted packet not being acknowledged. However, if a more serious problem occurs, such as a network cable being unplugged from the local computer, the TCP/IP stack will notify the RGS Receiver of a network exception. In this case, the RGS connection will be closed immediately, independent of whether a network timeout property has been exceeded.

After the RGS Receiver warning timeout property has been exceeded (two seconds, in this case), the Remote Display Window will dim and display a warning message to the user. The dimmed window and warning message notify the user of the potentially stale contents in the Remote Display Window. During this time, the Remote Display Window will appear unresponsive to the user. If connectivity returns, the Remote Display Window will return to its normal appearance and interactivity.

If the connection loss extends beyond the RGS Receiver error timeout property (30 seconds, in this case), the Remote Display Window and the RGS Receiver connection will be closed, and the "Connection Lost!" error dialog will be displayed.

The recommended RGS Receiver timeout strategy is to set a short warning timeout property and a longer error timeout property. With these settings, the user is notified of potential network disruptions relatively quickly while allowing sufficient time for the network to possibly recover. For networks with potential disruptions greater than two seconds, a higher RGS Receiver warning timeout property may be appropriate to lessen distraction of the user.

Experience has demonstrated that 30 seconds is a reasonable RGS Receiver error timeout property, although some users adjust this property lower to force connections to close sooner. Higher settings, such as 60 seconds, are often impractical because they force the user to wait an inordinate amount of time before RGS closes the connection.

## RGS Sender network timeout

The RGS Sender supports the RGS Sender error timeout property, `Rgsender.Network.Timeout.Error`. This property can be set only by using the `rgsenderconfig` file or on a command line—the RGS Sender does not have a dialog to set this property. The RGS Sender error timeout property is independent of the RGS Receiver timeout properties. The RGS Sender begins by using the maximum of the `Rgsender.Network.Timeout.Error` property and the `Rgsender.Network.Timeout.Dialog` property.

When the RGS Receiver negotiates its connection to the RGS Sender, it notifies the RGS Sender of its error timeout property. For sync pulse timeout purposes, the RGS Sender adopts the minimum of:

```
Rgreceiver.Network.Timeout.Error
```



and the maximum of

```
{ Rgsender.Network.Timeout.Error AND Rgsender.Network.Timeout.Dialog }
```

For example, if the RGS Sender error timeout property is 30 seconds and the RGS Receiver error timeout property is 20 seconds, the RGS Sender will use 20 seconds for its sync pulse timeout because 20 seconds is the minimum of both. If the user adjusts the RGS Receiver error timeout property to 60 seconds, the RGS Sender will use a value of 30 seconds for sync pulse timeout because, again, 30 seconds is the minimum of both error timeouts.

If a RGS Sender sync pulse timeout occurs, the RGS Sender will terminate its connection to the RGS Receiver. Unlike the local computer, which displays warning and error messages, the remote computer does not display a message prior to terminating the connection. The user must initiate a reconnection from the RGS Receiver to the RGS Sender to restore connectivity.

A relatively small RGS Sender error timeout property is recommended. If the RGS Receiver and Sender connectivity is impacted by a network disruption, the RGS Sender can take as long as its error timeout property to determine the connectivity loss, and fully terminate the connection. During the time from the actual network disruption until the RGS Sender error timeout expires, the remote computer will not send image updates to any other local computers (if the RGS Server is serving multiple RGS Receiver connections). This will impact the interactivity of other users for no apparent reason. After the RGS Sender error timeout expires, the RGS Sender will terminate the faulty connection, and continue updating the other RGS Receivers.

## Network timeout issues

Listed below are several timeout-related issues and their potential causes.

- **Remote Display Window repeatedly dims and displays a connection warning message**—This is likely caused by frequent network disruptions between the RGS Receiver and Sender. The dimming of the display serves as a notification to the user that the Remote Display Window may contain stale information. If frequent notifications are annoying, and the network issues do not improve, see the section [Network settings on page 36](#) and adjust the RGS Receiver’s warning timeout value found on the RGS Receiver Control Panel or the property `Rgreceiver.Network.Timeout.Warning`.
- **The Remote Display Window dims, and the local computer disconnects, and displays a “Connection closed” error dialog, but the user can often immediately connect again**—Most likely the network connectivity between the RGS Receiver and Sender was temporarily lost. Other possible problems include:
  - The RGS Sender unexpectedly terminated.
  - The remote computer experienced a failure.
  - The remote computer CPU utilization prevented the RGS Sender from making progress.
  - The length of this connectivity loss exceeded the RGS Receiver’s error timeout value, controlled by the RGS Receiver’s `Rgreceiver.Network.Timeout.Error` property, so the RGS Receiver disconnected.

If this condition persists, it is possible that network disruptions are exceeding the RGS Receiver error timeout value. If this is a network issue and is not resolvable, consider adjusting the error timeout of the RGS Receiver to reduce RGS Receiver disconnection. Additionally, the RGS Sender timeout might need to be increased too. See [Network settings on page 36](#) for further details.

- **When connecting to a Linux remote computer, the PAM authentication dialog displayed by the local computer does not appear long enough to enter the user’s credentials such as username and password**—This is likely caused by the RGS Receiver’s dialog timeout value being too small. See the section [Network properties on page 86](#) for further details on setting timeouts. The user should first check the RGS Receiver Control Panel to determine the Network dialog timeout setting and adjust as appropriate.

- **When connecting to the remote computer, the authorization dialog is not displayed long enough for the user to respond to it**—This is likely caused by the RGS Sender’s dialog timeout value being too small. See [RGS Sender properties on page 91](#) for further details on the property `Rgsender.Network.Timeout.Dialog`. The default value for this property is 15 seconds.
- **When connecting to a Linux remote computer, the PAM authentication often fails**—There are several reasons why this might occur:
  - PAM may be configured incorrectly.
  - The user could be entering incorrect credentials.
  - The timeouts are too short.

See [Installing the RGS Sender on Linux on page 20](#) to determine if PAM is correctly configured. See [Network settings on page 36](#) for further details on setting timeouts. The user could try increasing the RGS Receiver’s network dialog timeout as well as the RGS Sender’s error and dialog timeouts to see if this helps. If this does not help and the user is convinced that the timeouts are not being exceeded, then it is likely a PAM authentication configuration problem.

- **The Remote Display Window is not updating and appears to be hung**—This is most likely caused by a network disruption. You can adjust the warning timeout to get notification when this occurs. You can also adjust the error timeout to disconnect and dismiss the Remote Display Window sooner. The default warning timeout is two seconds. The default error timeout is 30 seconds. See [Network settings on page 36](#) for further details on setting the RGS Receiver timeouts.
- **Increasing the RGS Receiver error dialog timeout doesn’t appear to have an effect and the RGS Receiver still disconnects**—This is likely caused by either:
  - A network failure resulting in detecting lost connectivity by the RGS Receiver (resulting in a disconnected connection)
  - The RGS Sender timeouts are shorter than the RGS Receiver’s timeouts, and the RGS Sender disconnects the RGS Receiver.

It is not always the case that network error timeouts are honored. A network error timeout only establishes an upper bound on the duration of retries before returning with an error. If the computer determines that network connectivity is lost and an error returns by the network stack to the RGS Receiver, then the connection will disconnect sooner than the error timeout setting. If the RGS Sender’s timeout values are shorter than the RGS Receiver’s, the RGS Sender may close the connection sooner than the RGS Receiver, disconnecting the RGS Receiver. If the issue continues, consider increasing the RGS Sender’s error timeout value. See [Network settings on page 36](#) for further details on setting timeouts.

## Troubleshooting graphics performance

The dominant factor impacting performance on the remote computer is the frame buffer read performance of the graphics adapter. Frame buffer read performance of at least ten frames per second is recommended for optimum RGS performance.

RGS uses the remote computer’s graphics adapter to accelerate rendering of the image. After the image on the remote computer is modified, the RGS Sender reads the rendered image from the frame buffer, compresses it, and transmits it to the RGS Receiver.

On Windows, use the `BltTest` tool to test the frame buffer read performance of the remote computer. This tool is available at: <http://www.stereopsis.com/blttest/>.

## Troubleshooting Remote Audio

Several potential audio issues are described below along with their potential causes.

- No audio on the RGS Receiver on Windows—Verify that your local computer audio device is working. The volume control slider on the RGS Receiver plays a beep by default when released. Ensure that the Speaker button on the RGS Receiver Control Panel is not in the mute position. Make sure that mute is not enabled on the Wave line of the RGS Sender or RGS Receiver Volume Control.
- No audio on Windows after connecting or disconnecting an audio device—Reconfiguring an audio device while an application is using that device can cause the application to stop working. If an audio device is reconfigured, the RGS Sender may stop transmitting audio. Disconnecting the RGS Receiver and reconnecting will cause the RGS Sender to use the new audio configuration.

Some audio device drivers have the ability to detect when a speaker jack is in use. Plugging in headphones to these devices may cause the device to reconfigure. This can result in temporary loss of Remote Audio. Reconnecting the RGS Receiver may be necessary to restore audio.

If all of the audio devices on a system are configured as not plugged in, the audio device cannot be opened. Some programs, such as Windows Media Player, will display an error indicating that an audio device is not available. Something will need to be plugged into one of the unplugged devices to allow audio to work on these devices.

- Audio not continuous—Low bandwidth connections can cause discontinuities in the audio stream. Reducing the quality and turning off stereo may improve the audio quality. Some high priority CPU intensive tasks may disrupt the audio stream. The Windows Task Manager may help you identify such a task. Another possible problem may be a bad network setup.
- PC speaker sounds not working—The RGS Sender captures all audio information sent through the mixer. This includes most audio alerts, MIDI, Direct Sound and Direct Music. Sounds generated by the PC speaker are not captured by the RGS Sender and will not be transmitted.
- Audible pops and glitches in sound—This is most likely because the network bandwidth or system resources are starving the audio streaming from continuous play.
  - Try a lower audio quality setting to reduce network bandwidth usage.
  - Be sure you system is not doing something so computationally intensive that it is starving RGS from keeping up with graphics and audio processing.
- Enabling audio causes continuous network traffic—When the RGS Sender detects an audio signal, that signal is sent to the local computer. If the audio device on the remote computer is silent, there should not be any network traffic due to audio. If the audio device is generating a large amount of noise, that noise may be interpreted as an audio signal, and be sent to the local computer. This may occur when something is connected to the "Line In" port of the audio device. Reducing volume levels or disconnecting any external devices may help reduce the interference.
- ToggleKeys sound not working—The Accessibility control in Windows will play a sound when some control keys are pressed. This sound is not heard on the local computer because it is played through the PC Speaker.
- No audio with multiple audio devices—The RGS Sender will open up the device that is registered as the default audio device. The RGS Sender is a service that is running in a different context. If you have multiple audio devices, it may choose a different device than you have selected as the default. Disable the extra audio device to ensure that the RGS Sender uses the correct device.

## Troubleshooting Remote Clipboard

Both the RGS Receiver and the RGS Sender have the ability to log various types of information to log files during their operation. If the logging level is set to DEBUG on the RGS Receiver and Sender, Remote Clipboard information will be stored in the RGS Receiver and Sender log files. These log files can then be used to detect and resolve Remote Clipboard problems.

Remote Clipboard entries in the log files have the text below preceding the Remote Clipboard information. In particular, the string "(format filter)" identifies each log file entry that contains Remote Clipboard information. In this section, the text preceding the Remote Clipboard information will not be shown.

#### **11-08-08 00:26:14 DEBUG - (format filter) ...Remote Clipboard information...**

To demonstrate use of the RGS logs to view Remote Clipboard information on the local and remote computers, an example is presented in which a copy and paste is performed from a remote computer to a local computer. The steps in this example are:

1. Set the Rgreceiver.Clipboard.FilterString="|1|2|13|Object Descriptor|HTML Format|"
2. Establish an RGS connection from the RGS Receiver to the RGS Sender.
3. Open Notepad on the local computer.
4. Open Notepad on the remote computer (via the Remote Display Window) and enter some text.
5. Highlight the text in the remote computer's Notepad window, and then select **Copy**.
6. Paste the text into the Notepad window on the local computer.

To set the Rgreceiver.Clipboard.FilterString as shown above, the rgreceiverconfig configuration file is modified to specify the property:

```
Rgreceiver.Clipboard.FilterString="|1|2|13|Object Descriptor|HTML Format|"
```

The RGS Receiver is stopped and then restarted to ensure this property is used. When an RGS connection is established, the RGS Receiver sends this filter string to the RGS Sender. From the RGS Receiver's perspective, it's setting a "remote filter" on the RGS Sender. From the RGS Sender's perspective, it's setting its local filter string when it receives the filter string from the RGS Receiver.



**NOTE:** If the clipboard on either the local or remote computer already contains content at the time the RGS connection is established, a sending formats entry will appear in the log file of that computer preceding the setting filter log entry. The sending formats log entry is due to the clipboard contents being sent to the remote computer when the RGS connection is first established.

## **Troubleshooting Remote USB**

If you have problems connecting a remote USB device from a local computer to a remote computer, the following checklist may help identify the problem.

### **Computers supporting Remote USB**

Ensure that both the remote computer and the local computer support Remote USB.

### **Supported USB devices**

Verify that the USB device you're using is supported. HP has tested a number of USB devices to verify they work correctly when attached to a remote computer from a local computer.

### **Enable Remote USB**

Verify that Remote USB is enabled in the RGS Receiver Control Panel.

### **Check USB cable connections**

Verify that the USB device is physically connected to the local computer. Check to see that it has power and is turned on. Some devices may require that the user initiate an action before it connects.

To further verify your connections, recognized devices on the local computer appear in the Proc file system under the `/proc/devices/usb_remote` directory. At least two files appear in this directory for a single connected device:

- `/proc/devices/usb_remote/devices`—File contains a list of recognized devices by the local computer.
- `/proc/devices/usb_remote/#`—If only one USB device is recognized, the "devices" file will have a single entry, 192. The file descriptor named 192 is the Remote USB device. Dumping this file with 'cat 192', for example, displays specific data about device 192. This should reflect the connected USB device. If multiple devices are connected, then each will have a file descriptor numbered consecutively starting at 192.

## Reset the USB device

If the USB device has a reset button, press the button.

## HP Remote Virtual USB Driver

Verify that the HP Remote Virtual USB driver is installed and active on the remote computer. Open the Windows Device Manager, and verify that **HP Remote Virtual USB** is listed under **Universal Serial Bus Controllers**.

If the HP Remote Virtual USB driver is not reported, reinstall the RGS Sender software. During installation, verify that the Remote USB box is checked in the Configuration window.

## USB device drivers and program support

Verify that the device drivers and programs required by the device are installed and available on the remote computer. Many USB devices require manufacturer-supplied software to work on a system. This software must often be installed before the USB device is connected to the system.

## RGS error messages

This section lists the error messages reported by the RGS Receiver and describes possible reasons for them.

**Table B-2 RGS Receiver error messages**

Error	Description
Connection lost!	<p>The RGS Sender has closed the connection. Possible reasons include:</p> <ul style="list-style-type: none"><li>• The RGS Sender might have explicitly disconnected your connection. For example a user might have selected disconnect all connections from the RGS Sender icon or RGS Sender GUI or the user might have logged off.</li><li>• Another user has connected to the RGS Sender using the same username and password.</li><li>• If you connected to a desktop that was not logged in and another user logged in your connection will be disconnected.</li><li>• If you were connected to a logged in desktop and the logged in user disconnects your connection will be disconnected too.</li><li>• The network may have been disconnected, closed, or temporarily disrupted.</li></ul>

**Table B-2 RGS Receiver error messages (continued)**

	<ul style="list-style-type: none"><li>• The RGS Sender service/daemon may have been stopped, restarted, or killed.</li><li>• The RGS Sender system may have been stopped/shutdown or restarted.</li><li>• If connecting to a Linux computer, the X Server may have been stopped or restarted.</li><li>• The RGS Sender or X Server may have experienced a failure.</li></ul>
Unable to connect to Sender!	If this error is reported, see <a href="#">Pre-connection checklist on page 23</a> for a list of possible causes.
Authentication failed!	The RGS Sender has refused to allow a connection. Possible reasons include the following: <ul style="list-style-type: none"><li>• The authentication credentials that you entered, such as domain name, user name and password, are not valid or recognized by the remote computer.</li><li>• The RGS Sender's authentication is not configured appropriately. See the user's manual and README.txt for the latest directions and issues with respect to configuring authentication.</li></ul>
Directory not found or not accessible!	The directory file is not available. Possible reasons include: <ul style="list-style-type: none"><li>• The directory file name or location has been mistyped.</li><li>• The file has been moved or is no longer available.</li><li>• The network is down or experiencing a disruption.</li><li>• The user does not have read permission on the file.</li></ul>
User not found in directory!	The username of the current user of the HP Remote Graphics Software Receiver is not found in the directory file. Possible reasons include: <ul style="list-style-type: none"><li>• The username entered in the directory file does not exactly match the real username.</li><li>• The domainName entered in the directory file is incorrect. See <a href="#">Directory file format on page 61</a> for information about choosing the correct domainName.</li><li>• The username of the current user is not entered in the directory. If the directory file is on a shared drive with restrictive permissions, consult an IT specialist to add the proper entry.</li></ul>
Authorization failed!	The connection was authenticated, but another user is already logged into the desktop of the remote computer. When a connection is attempted to another user's desktop, a dialog is displayed on the remote computer's desktop asking the logged in user to allow the connection. A user is not allowed to connect to another user's desktop unless they are explicitly allowed/authorized. Either the connection was not granted access, or the dialog timed-out and the connection was implicitly denied.
Error: No license found for the Sender you are trying to connect to!	A license was not found for the RGS Sender.
Error: License Expired for the Sender you are trying to connect to!	The license has expired for the RGS Sender.
Error: License Invalid for the Sender you are trying to connect to!	The license is invalid for the RGS Sender.

**Table B-2 RGS Receiver error messages (continued)**

Setup Mode hotkey sequence too short.	The key sequence specified by the user is too short.
Setup Mode hotkey sequence too long.	The key sequence specified by the user is too long.
Setup Mode hotkey sequence may only consist of Ctrl, Alt, Shift and Space.	The key sequence specified by the user contains invalid keys.
A space may only be entered after Ctrl, Alt or Shift is pressed.	The Setup Mode hotkey sequence cannot start with a space.
Setup Mode hotkey sequence is invalid. The sequence has been reset to the default.	The Setup Mode hotkey sequence specified using a property either on the command-line or in the property configuration file is invalid, and has been reset to the default.
Setup Mode hotkey sequence is invalid. The sequence has been disabled.	The Setup Mode hotkey sequence specified using a property either on the command-line or in the property configuration file is invalid, and the property Rgreceiver.Hotkeys.IsMutable is disabled. Therefore, hotkeys have been disabled.
Unable to connect to Sender: The Receiver was unable to resolve the specified hostname or IP Address. Verify that you entered the value correctly.	This is usually indicative of a DNS error.
Unable to connect to Sender: The Receiver resolved the specified hostname or IP address, but cannot connect to the Sender. Verify that the system is accessible on your network and that the Remote Graphics Sender service has been started and is listening on a public IP address and is not blocked by a firewall.	The RGS Receiver was able to look up and resolve the specified hostname or IP address. However, the RGS Receiver was unable to establish a connection to the RGS Sender. There are several possibilities such as the RGS Sender is not installed, the RGS Sender is not running, the RGS Sender is listening on the wrong network interface, or a firewall is blocking the RGS Sender.

---

# C HP support

## Obtaining HP support

If you encounter an issue that requires support, please do the following prior to contacting HP for assistance:

- Be in front of the local computer or remote computer, whichever one is appropriate.
- Note the operating system.
- Note any applicable error messages.
- Note the applications you were using when you had the issue.
- Be prepared to spend the time necessary to troubleshoot the problem with the service technician.

For a listing of all worldwide technical support phone numbers, visit <http://www.hp.com/support>.



**NOTE:** If your phone call is answered by a voice recognition system and you are asked to provide the name of the product, say Remote Graphics Software, not RGS.

---

## Additional RGS documents

Additional RGS documents such as the *HP Remote Graphics Software Licensing Guide* can be found at: <http://www.hp.com/go/rqs>.



# Index

## A

- advanced performance features, activation 13
- Advanced Video Compression
  - activation 13
  - description 45
  - enabling 34
  - requirements 96
- application support 98
- audio
  - disabling on remote computer 54
  - Remote Audio. *See* Remote Audio
  - RGS Receiver requirements on Linux 19
  - RGS Receiver settings. *See* RGS Receiver settings

## C

- collaboration 44
- command line options
  - RGS Receiver 28
  - RGS Sender on Windows 39
- connections
  - auto-launching 64
  - creating 29
  - creating in Directory Mode 61
  - pre-connection checklist 23
  - settings. *See* RGS Receiver settings
  - types 9

## D

- deployment, typical 3
- Directory Mode 61
- display resolution 47

## E

- Easy Login
  - manually disabling on Linux 21
  - overview 11
- error messages 105
- event logging, RGS Sender 64

## F

- features, list of 7
- firewall, using RGS through 26

## G

- Game Mode 63
- gestures
  - RGS Receiver settings. *See* RGS Receiver settings
- getting started in Windows 1

## H

- hardware, supported 95
- hotkey settings. *See* RGS Receiver settings
- HP support 108
- HP Velocity
  - activation 13
  - description 45
  - installation on RGS Receiver 13
  - installation on RGS Sender 16
- HPRemote log
  - format 65
  - viewing 64

## I

- installation on Linux
  - RGS Receiver 19
  - RGS Sender 20
- installation on Windows
  - log file, RGS Receiver 15
  - log file, RGS Sender 18
  - RGS Receiver 12
  - RGS Sender 15
- installing RGS 12
- interoperability
  - RGS and Microsoft Remote Desktop Connection 76
  - RGS Sender and RGS Receiver 9

## K

- keyboard locale 97

## L

- layout matching 47

- licensing 9
- Linux connection considerations 78
- log files
  - installation, RGS Receiver 15
  - installation, RGS Sender 18
- logging
  - RGS Receiver. *See* RGS Receiver settings
  - RGS Sender 42
- login methods 10

## M

- many-to-one connection 9
- microphones. *See* Remote Microphone
- Microsoft Remote Desktop Connection, interoperability with RGS 76
- monitor blanking 77
- multi-monitor configurations 10

## N

- network interface binding, RGS Sender
  - manual reconfiguration 26
  - overview 25
  - reconfiguration using properties 26
- network settings. *See* RGS Receiver settings

## O

- one-to-many connection 9
- one-to-one connection 9
- operating systems, supported 95
- optimizing RGS performance 45

## P

- performance settings. *See* RGS Receiver settings
- power saving states 27
- pre-connection checklist
  - local computer 23
  - remote computer 23

- properties
  - RGS Receiver 82
  - RGS Sender 91
  - setting in a configuration file 81
  - setting on the command line 81
  - syntax 81

## R

- Remote application termination
  - overview 65
  - sample agent 71
- Remote Audio
  - on Linux 52
  - on Windows 51
  - overview 51
  - support on Linux 96
  - troubleshooting 102
- Remote Clipboard 54
  - troubleshooting 103
- Remote Display Window toolbar 6
- Remote Microphone
  - on Linux 52
  - on Windows 51
- Remote USB
  - Access Control List 58
  - auto-remoting 55
  - determining device information 59
  - overview 54
  - smart cards 57
  - supported devices 56
  - troubleshooting 104
  - verifying data 60
- RGS Admin Tool 42
- RGS Diagnostics Tool 41
- RGS documents, additional 108
- RGS overview 2
- RGS Receiver
  - audio requirements on Linux 19
  - command line options 28
  - Control Panel overview 4
  - interoperability with RGS Sender 9
  - network timeout
    - troubleshooting 99
  - properties 82
  - Remote Display Window
    - overview 5,6
  - starting 28
  - using 28

- RGS Receiver settings
  - audio 35
  - connection 33
  - gestures 35
  - hotkeys 36
  - logging 37
  - network 36
  - performance 34
  - statistics 38
- RGS Sender
  - command line options on Windows 39
  - event logging 64
  - GUI on Windows 41
  - interoperability with RGS Receiver 9
  - logging in Windows 42
  - network interface binding 25
  - network timeout
    - troubleshooting 100
  - process priority on Windows 41
  - properties 91
  - RGS Admin Tool 42
  - RGS Diagnostics Tool 41
  - starting and stopping on Windows 39
  - starting on Linux 40
  - using 39
- RGS support matrix 95

## S

- security features 76
- settings, RGS Receiver. *See* RGS Receiver settings
- Setup Mode
  - changing hotkey sequence 37
  - overview 31
- Single Sign-on 11
- smart cards 57
- software, supported 95
- Standard Login 10
- statistics. *See* RGS Receiver settings
- support
  - applications 98
  - keyboard locale 97
  - Remote Audio device on Linux 96
  - video overlay surfaces 98
- support matrix. *See* RGS support matrix

## T

- touch features 30
- troubleshooting
  - error messages 105
  - graphics performance 102
  - network performance 46
  - network timeouts 99
  - Remote Audio 102
  - Remote Clipboard 103
  - Remote USB 104

## U

- uninstallation on Linux
  - RGS Receiver 19
  - RGS Sender 22
- uninstallation on Windows
  - RGS Receiver 15
  - RGS Sender 18
- USB. *See* Remote USB
- user interface 4

## V

- video overlay surfaces 98
- virtual keyboard 30
- virtual mouse 30