HP Remote Graphics 4.2.0
User's Guide

Copyrights and trademarks

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.

Microsoft, MS-DOS, Windows, Windows NT, Windows 2000, Windows XP, and DirectX are registered trademarks or trademarks of Microsoft Corporation in the U.S. and other countries.

Intel, Pentium, Intel Inside, and Celeron are registered trademarks of Intel Corporation or its subsidiaries in the U.S. and other countries.

Java is a trademark or registered trademark of Sun Microsystems, Inc.

AMD and AMD64 are trademarks of Advanced Micro Devices, Inc.

OpenGL is a registered trademark of Silicon Graphics, Inc.

Red Hat and Enterprise Linux are registered trademarks of Red Hat, Inc.

Linux is the registered trademark of Linus Torvalds in the United States and other countries.

InstallShield® is a registered trademark and service mark of Macrovision Corporation and/or Macrovision Europe Ltd. in the United States and/or other countries.

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation.

pcAnywhere is a trademark of Symantec Corporation.

ZeroC, Ice, and Internet Communications Engine are trademarks of ZeroC, Inc.

CORBA is a trademark or registered trademark of the Object Management Group, Inc.

Audigy is a trademark of Creative Technology Ltd. in the United States and/or other countries.

Python and PyCon are trademarks or registered trademarks of the Python Software Foundation.

All other product names mentioned herein may be trademarks of their respective companies.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material. The information in this document is provided “as is” without warranty of any kind, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, and is subject to change without notice. The warranties for HP products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

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). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

log4cplus: This product includes software developed by the Apache Software Foundation (http://www.apache.org/). log4cplus is available from http://log4cplus.sourceforge.net/

Advanced Linux Sound Architecture (ALSA): ALSA provides audio and MIDI functionality to the Linux operating system. ALSA is released in source code format under the GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999. ALSA is used in the HP Remote Graphics Software Receiver for Linux.

Jack Audio Connection Kit (JACK): JACK is a low-latency audio server, written for POSIX conformant operating systems such as GNU/Linux and Apple's 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.

Libsndfile: Libsndfile is a C library for reading and writing files containing sampled sound (such as MS Windows WAV and the Apple/SGI AIFF format) through one standard library interface. Libsndfile is released in source code format under the GNU LESSER GENERAL PUBLIC LICENSE. Libsndfile is used in the HP Remote Graphics Software Receiver for Linux.

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

Table Of Contents

Welcome to HP Remote Graphics Software

Welcome to HP Remote Graphics Software (RGS). This document provides a complete overview of the RGS product including the RGS Receiver, RGS Sender, and RGS Enterprise Service.

About Remote Graphics Software

What is Remote Graphics Software?

Remote Graphics Software (RGS) is software that allows a user to access the desktop of a remote computer over a standard computer network. The software is conceptually similar to other remote access solutions such as Microsoft Remote Desktop, Symantec pcAnywhere™ and others.

Remote Graphics Software is composed of three major software components:

1. RGS Sender is a software application that runs as a service or background process on a remote computer and transmits graphics updates, audio, and USB data to one or more RGS Receivers. The Sender receives keyboard events, mouse events, and USB data from the Receiver, and processes them locally.

2. RGS Receiver is a software application that runs on a local computer or thin-client. The Receiver establishes a connection to one or more Senders, requests graphics updates from the Sender, and displays the desktop of the remote computer inside a window on the local system. Keyboard and mouse events in the Remote Display Window are transmitted to a Sender. USB data is also transmitted and received from the Sender. The Receiver connects to the RGS Enterprise Service if enabled.

3. RGS Enterprise Service is an optional software component that runs as a service or daemon on a remote computer. The Enterprise Service (ES) manages centralized system lookup and user enterprise properties for the RGS Receiver over a standard computer network. The Enterprise Service is delivered as a Software Development Kit (SDK).

Features

HP Remote Graphics Software includes the following features:

- Application transparency: No modification to applications is necessary to access them remotely.
- Audio follows focus: The RGS Receiver can be configured to enable audio for the session displayed in the Remote Display Window that currently has focus and is muted for all other remote sessions/windows.
- Collaboration: Multiple users can simultaneously connect to the same Sender. This allows several users to view and interact with the same desktop. For example, several users at different remote locations can simultaneously view 3D OpenGL applications using a RGS Receiver.
- Collaboration Notification: The RGS Sender displays a collaboration notification dialog when one or more non-primary connections are active. The dialog displays the users currently connected to the Sender. This provides a reminder to the user that multiple connections to the desktop exist. Individual users can be disconnected using the collaboration notification dialog. See Collaboration Notification for more details.
- Directory Mode: Directory Mode enables the Receiver to locally lookup pre-assigned systems for a user from a file.
- Direct3D: Direct3D 8.0 and Direct3D 9.0 applications are supported. Remote access users and remote collaborators can easily interact with Direct3D applications running on a remote desktop. Direct3D applications run using the full power of the graphics adapter. See Enabling Direct3D Applications on Windows for further information.
- Disconnect primary or non-primary users: The RGS Sender desktop GUI provides the ability to selectively disconnect either non-primary users or all users (both primary and non-primary).
- Easy Login: Enables fewer authentication steps when connecting to an HP Blade Workstation running Windows XP Pro. See Using Easy Login for more details.
- Enterprise Service Mode: The Remote Graphics Software Enterprise Service enables a customer to integrate remote graphics into their enterprise directory infrastructure to support assignment of systems to users as well as managing user settings and properties. The Enterprise Service enables roaming usage. Users can work from any location on the network and easily access their assigned systems and settings without re-entering them. The Remote Graphics Software Enterprise Service also allows IT organizations to easily manage user system assignment with their current enterprise directory infrastructure.
- Hotkeys: The RGS Receiver supports setting user-defined hotkeys for entering Setup Mode as well as other operations.

- Image-based remote visualization technology: Proprietary HP image compression/decompression algorithms enable real-time remote visualization that is visually lossless and fast. Interactive remote visualization of 2D and 3D OpenGL graphics are possible using hardware acceleration. DirectX applications are not supported.
- Logging: The RGS Sender for Windows logs to the Windows Event Log connection status changes such as when a new connection is established, when a disconnect occurs, the user that is assigned to a connection, and whether that user is a primary or non-primary user.
- Multi-head Display: Single-headed receivers can view multi-headed senders. Multi-headed receivers can view single-headed senders. Multi-headed receivers can view multi-headed senders. The view can expand to contain the entire area on the receiver's desktop. This gives the user the impression of direct connection and full utilization of the sender's desktop.
- Multi-platform support: Senders and Receivers are supported on Microsoft Windows, Linux and HP-UX systems. See System Requirements for more details.
- Network Connection Warning Notification: The RGS Receiver visually warns the user when network connectivity between a Receiver and Sender is potentially lost. If network connectivity recovers, normal operation should continue. See Network Options and Using Timeouts for more details.
- OpenGL 3-D OpenGL applications are supported. Remote access users and remote collaborators can easily interact with 3-D applications running on a remote desktop. 3-D applications run using the full power of the graphics adapter. See Enabling OpenGL Applications for further information. :
- Properties: The RGS Receiver and Sender provide an easy to use public interface that allows users and administrators to specify properties either on the command-line, a configuration file, or using the RGS Enterprise Service. See Properties for more details.
- Remote Application Termination (RAT): Network outages or loss of connectivity between a Receiver and Sender 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. Remote Application Termination is only available with the RGS Sender for Windows. See Remote Application Termination on Windows for more details.
- Remote Audio: Smooth, continuous, low-latency, high-quality remote audio is possible from RGS Senders to RGS Receivers. See System Requirements for more details on the supported systems.
- Remote & Local Cursor Tracking: In a collaboration session (multiple users connected to the same remote desktop) the shape of the local hardware cursor is modified for the floor owner (the user that is currently in control of the mouse and keyboard). For the other remote users, the local cursor is left unchanged and a remote cursor is displayed in the Remote Display Window.

- Remote USB: The HP Blade Workstation with RGS Sender supports multiple USB devices connected from an HP Workstation Blade Client. See System Requirements for more details on the supported systems.
- Screen lock: When the primary user disconnects the desktop of the remote system is locked.
- Single Sign-on: Enables fewer authentication steps and automatic login and unlocking of the desktop when connecting to a HP Blade Workstation running Windows XP Pro. Activation of RGS Single Sign-on requires enabling the RGS Sender for Windows GINA module (*hprgina.dll*) which can be selected during installation.
- Status Bar: A status bar in the RGS Receiver Control Panel provides status notification such as connecting, authenticated, authorizing, and connected messages. The banner in the RGS Control Panel also animates when a connection is in progress.
- Stateless client: Connections are completely stateless. No data is persistently stored in the Receiver.
- Timeout Configuration: Network and dialog timeouts can be controlled to meet various network and user requirements. See Network Options and Using Timeouts for more details.
- Virtual KVM: A single Receiver can establish multiple remote connections to several remote systems simultaneously when run in Directory or Enterprise Service Mode. Virtual KVM (V-KVM) emulates the functionality of a KVM switch in software to provide a convenient method to map workstations to specific displays and switch between them. This feature emulates the capabilities found in a physical KVM switch by allowing the user to easily switch between remote session by "raising" the selected Remote Display Window in a manner similar to the "alt-tab" capability provided in Windows. The receiver can also switch audio between active sessions as described in the Controlling Receiver Settings section using the audio follows focus option.

Security Features

HP Remote Graphics Software has the following features to maintain security:

- Authentication: When a Receiver attempts to connect to a Sender, user credentials are validated using the native authentication method on the sender system. If the credentials are not authenticated, the connection is closed. On Windows operating systems authentication uses NTLM or Kerberos. On UNIX (Linux and HP-UX) authentication uses the Pluggable Authentication Module (PAM).
- Authorization: Multiple connections to the same Sender are only allowed if the user logged into the desktop of the Sender system (primary user) allows the connection. When a non-primary user attempts to connect to a Sender an authorization dialog is displayed on the desktop of the remote system that asks whether the user should be allowed to connect.
- Automatic Desktop Locking: The desktop of the Sender system locks when the primary user disconnects. This prevents non-primary users from being able to interact with a remote session after the primary user has disconnected.

  This feature is supported on Windows systems, and on Linux and HP-UX, this feature is supported on the Gnome, KDE, and CDE desktop environments.
- Automatic Disconnect: On Linux and HP-UX systems all Receivers will disconnect when the primary user disconnects. This prevents non-primary users from interaction with a remote session after the primary user disconnects.
- Automatic Disconnect of non-primary users on Login: All non-primary 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 Log Off: All Receivers are disconnected when the primary user logs off of the remote desktop. This can be disabled by setting the "IsDisconnectOnLogoutEnabled" sender property to "0". See Sender Properties for more information.
- Connection Status: On Windows a desktop icon in the application tray animates when other users are connected. Likewise, on Linux and HP-UX the Sender GUI animates.
- Collaboration notification: See Features.
- Connections are not allowed when an iLO remote console is enabled: If the iLO remote console is enabled on a HP Blade Workstation, connections to the blade using RGS are denied.
- Disconnect All: All Receivers can be easily disconnected using the Sender GUI. This is useful when hosting a collaboration session, such as in a classroom environment, and the session ends. On Windows system, the GUI is an icon

located in the system tray. On Unix systems, the GUI is an application on the desktop. Simply right-click on the GUI and select "Disconnect All Receivers".

- Enable/Disable I/O: The Sender GUI can enable or disable mouse and keyboard input for all non-primary 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 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 Receiver and Sender pair.

System Requirements

Sender

Feature	Supported Components
Supported Platforms	• Microsoft Windows 2000 or XP Professional 32-bit (Intel x86 and x86-64 processor families. AMD x86 and AMD64 processor families.) • Microsoft Windows XP Professional x64 Edition (Intel x86-64 processor families. AMD64 processor families.) • Red Hat Enterprise Linux WS3 32-bit & 64-bit (Intel x86 and x86-64 processor families. AMD x86 and AMD64 processor families. HP Personal Workstations only.) • HP-UX 11.0 and 11i V1 HP PA-RISC 2.0 architecture (PA-8500 or later)
Supported Graphics	Windows & Linux: • Any graphics adapter (nVIDIA, ATI, Matrox) HP-UX: • HP Visualize fx5, fx10 • ATI FireGL-UX, FireGL T2-128p • FireGL X1-256p, FireGL X3-256
Display Settings	Supports the following Display Settings: • 32 bit at 1024x768 resolution or higher • On Windows, video overlay planes, DirectX and full-screen exclusive mode access not supported. • On Windows, OpenGL overlay planes are not supported.
Remote Audio	• Microsoft Windows XP Professional 32-bit and 64-bit • Microsoft Windows 2000 Professional

Remote USB	Remote USB is only supported on an HP Blade Workstation Client when connected to an HP Blade Workstation sender system. 1. Any number of USB devices can be simultaneously connected. 2. HP Remote Graphics Software requires matched versions of the RGS Sender and RGS Receiver systems. For example, RGS Sender and Receiver at version 4.0 work together. If they are both version 3.1, they will work together. Versions 3.1 and 4.0 in any combination will not work together. 3. Not all USB devices are supported. Refer to the HP Blade Workstation documentation for more details.
Easy Login	HP Blade Workstation running Microsoft Windows XP Professional 32-bit.
Remote Application Termination	Microsoft Windows 2000 Professional or XP Professional 32-bit and 64-bit.
Collaboration Notification	Microsoft Windows 2000 Professional or XP Professional 32-bit and 64-bit.
Networking	• Standard TCP/IP. • 10/100/1000BASE-T (Gigabit) Ethernet. • Full-duplex recommended.

Receiver

Feature	Supported Components
Supported Platforms	• Microsoft Windows 2000 or XP Professional 32-bit (Intel x86 and x86-64 processor families. AMD x86 and AMD64 processor families.) • Microsoft Windows XP Professional x64 Edition (Intel x86-64 processor families. AMD64 processor families.) • HP Compaq t5720 Thin Client with Microsoft Windows XP Embedded (SP2) • Red Hat Enterprise Linux WS3 32-bit & 64-bit (Intel x86 and x86-64 processor families. AMD x86 and AMD64 processor families. HP Personal

	Workstations only.) • HP-UX 11.0 and 11i V1 HP PA-RISC 2.0 architecture (PA-8500 or later)
Supported Graphics	Any system graphics
Display Settings	Supports the following Windows XP Color Quality settings: • 16 bit • 24 bit • 32 bit All Linux or HP-UX Color Quality settings are supported at 1024x768 resolution or higher
Remote Audio	• Microsoft Windows XP Professional 32-bit and 64-bit • Microsoft Windows 2000 Professional • HP Compaq t5720 Thin Client with Microsoft Windows XP Embedded (SP2) • Linux 32-bit & 64-bit
Remote USB	Remote USB is only supported on an HP Blade Workstation Client when connected to an HP Blade Workstation sender system. 1. Any number of USB devices can be simultaneously connected. 2. HP Remote Graphics Software requires matched versions of the RGS Sender and RGS Receiver systems. For example, RGS Sender and Receiver at version 4.0 work together. If they are both version 3.1, they will work together. Versions 3.1 and 4.0 in any combination will not work together. 3. Not all USB devices are supported. Refer to the HP Blade Workstation documentation for more details.

Networking	• Standard TCP/IP. • 10/100/1000BASE-T (Gigabit) Ethernet. • Full-duplex recommended.
Keyboard Locales	The following keyboard localizations are supported: • U.S. English • U.K. English • Japanese • German • French The following keyboard localizations are supported on the HP Blade Workstation Client: • U.S. English • U.K. English • German (ABD) • Italian (ABH) • French (ABF) • Spanish (ABE) • International keyboard (ABZ) • Swedish • Finnish • Danish, • German Swiss • French Canadian • Norwegian.

Enterprise Service

Feature	Supported Components
Operating System	• Microsoft Windows XP Professional 32-bit & 64-bit • Microsoft Windows 2000 Professional

Getting Started with Remote Graphics Software

Installing the Receiver

Installation of the HP Remote Graphics Software Receiver is required on all systems that will be connecting to a HP Remote Graphics Software Sender.

Installing the RGS Receiver for Windows

To begin the installation of the RGS Receiver for Windows login to an account with administrator privileges:

1. Insert the HP Remote Graphics Software CD and in Explorer change to the directory `win32\receiver` on your CD-ROM drive.
2. Double-click or select `Setup.exe` to start the installer.
3. Follow the instructions on the screen.

The installer will add a menu item folder to the Programs folder called HP Remote Graphics. In this folder will be two items:

- Receiver
- Receiver **`-directory`**

Unattended Installations

If you need to install the Windows RGS Receiver on several systems, please refer to Creating Unattended Installers.

Installing the RGS Receiver for Linux

To install:

1. Login as root.
2. Insert the HP Remote Graphics Software CD and mount the CD, if it is not automatically mounted.
3. Go to the mount point of the CD, which is usually `/mnt/cdrom` and change directories to `lin32/receiver`.
4. Execute the following command:

   ```
   ./install.sh
   ```

   Note: If remote audio is installed the HP Remote Graphics Software requires certain audio support utilities be available for remote audio support from

appropriate senders. This software (based upon ALSA sound libraries and JACK-Audio-Connection-Kit libraries) must be built and installed on the target system as a part of the install.sh script. The install script assumes a supported set of ALSA sound libraries from HP or Red Hat Enterprise Linux (release 4 or greater) already exist on the platform. Only the JACK-Audio-Connection-Kit is built during install and it requires ALSA sound library support.

Note: The files contained within hp_rgs_4_audiosupport.tar.gz can also be built and configured for RPM package creation. See script rgs_audio_support for details.

5. The Receiver will be installed into `/opt/hpremote/rgreceiver`. To start the Receiver, execute the following command:

   ```
   /opt/hpremote/rgreceiver/rgreceiver.sh
   ```

   To start the Receiver in directory mode, execute the following command:

   ```
   /opt/hpremote/rgreceiver/rgreceiver.sh -directory
   ```

6. Optionally, add the directory `/opt/hpremote/rgreceiver` to your PATH environment variable.
7. Refer to Installing & Enabling Remote Audio to complete the Receiver installation.

Installing the RGS Receiver for HP-UX

To install:

1. Login as root.
2. Insert the HP Remote Graphics Software CD and mount the CD.
3. Go to the mount point of the CD, which is usually `/mnt/cdrom` and change directories to hpux-pa/receiver.
4. Execute the following command:

   ```
   ./install.sh
   ```

5. The Receiver will be installed into `/opt/hpremote/rgreceiver`. To start the Receiver, execute the following command:

   ```
   /opt/hpremote/rgreceiver/rgreceiver.sh
   ```

   To start the Receiver in directory mode, execute the following command:

   ```
   /opt/hpremote/rgreceiver/rgreceiver.sh -directory
   ```

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

Uninstalling the RGS Receiver

Uninstalling the RGS Receiver for Windows:

To uninstall the RGS Receiver for Windows use the Windows 2000 or Windows XP Add or Remove Programs feature from the Control Panel. Select Remote Graphics Receiver and click Change/Remove.

Uninstalling the RGS Receiver for Linux:

To uninstall the RGS Receiver for Linux find the name of the RedHat RPM package for the Remote Graphics Receiver, by typing:

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

If the Receiver is installed on the system, you will see `rgreceiver_linux_32-4.0-0` or a similar Receiver package. To remove the Receiver's RPM package, become root and type:

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

Uninstalling the RGS Receiver for HP-UX

To uninstall the RGS Receiver for HP-UX, become root and type:

```
/usr/sbin/swremove rgreceiver_hpux_pa
```

Installing the Sender

Installation of the RGS Sender for Windows, Linux and HP-UX is easily done by following the directions specific to each platform in the following sections.

Installing the RGS Sender for Windows

To install the RGS Sender for Windows, login to an account with administrator privileges:

1. Insert the HP Remote Graphics Software CD and change to the directory `win32\sender` on your CD-ROM drive.
2. Double-click or select **`Setup.exe`** to start the installer.
3. Follow the instructions on the screen.

   NOTE: The Remote Graphics Diagnostic tool runs during installation to detect common setup issues (Windows XP firewall settings, Guest Account security policies, RDP interoperability, Easy Login configuration, etc). The tool will only display a window if it detects a potential problem. Use the tool anytime after installation to determine installation problems. See Utilities for more details.
4. You will be prompted to restart the system after the installation is complete. Select yes when asked to restart the system.

The Sender is installed as a Windows Service. In fact, this is necessary to enable some features, such as the ability to send `Ctrl-Alt-Del` key sequences and also view locked screens. Additionally, installing the Sender as a service allows the Microsoft Windows operating system to automatically start the Sender when the system is started.

NOTE: To enable OpenGL applications see Enabling OpenGL Applications for more details.

NOTE: To enable remote audio see Installing & Enabling Remote Audio for more details.

Installing the RGS Sender on HP Blade Workstations

The RGS Sender for Windows installer `setup.exe` will automatically upgrade software versions prior to 4.0.0 when run. Upgrading the Sender is possible while connected to a HP Blade Workstation. After completing the upgrade restart the system when prompted. This will disconnect the current RGS connection and require a reconnect after the Blade Workstation restarts.

First-time installs of the RGS Sender on Blade Workstations require installation via the iLO Remote Console. This requires use of the administrative console in Setup Mode (from the boot BIOS) to complete the RGS Sender installation. After the install completes, return the iLO Remote Console Mode to User Mode. Please refer to the HP Blade Workstation iLO documentation for further details about the iLO administrative console.

Installing the RGS Sender and Remote Desktop

Using Microsoft Remote Desktop to remotely install the RGS Sender for Windows is not supported. If attempted, the installation process displays an error message and stops the installation process. If installing the RGS Sender on a HP Blade Workstation, use the iLO Remote Console Mode in Setup Mode (from the boot BIOS) instead.

Unattended Installations

If you need to install the Windows RGS Sender on several systems, please refer to Creating Unattended Installers.

Installing the RGS Sender for Linux

Linux Sender Installation

1. Login as root.
2. Insert the HP Remote Graphics Software CD and mount the CD, if it is not automatically mounted.
3. Go to the mount point of the CD, which is usually `/mnt/cdrom` and change directories to `lin32/sender`.
4. Execute the following command:

   ```
   ./install.sh
   ```

5. The Sender will be installed to `/opt/hpremote/rgsender`.
6. Add the "rge" extension to the X Server configuration file. Edit the `/etc/X11/XF86Config`, `/etc/X11/XF86Config-4` or the appropriate `XF86Config` file on your system for XFree86 X servers. Edit the `xorg.conf` file for X.Org X Servers. In the Modules section of this file, add the following line:

   ```
   Load "rge"
   ```

7. The `Module` section should read as follows:

   ```
   Section "Module"
        ...
        Load "rge"
        ...
   ```

```
EndSection
```

8. The Sender will be installed to `/opt/hpremote/rgsender` and will be started automatically when the X Server or system is restarted, provided the appropriate `XF86Config/xorg.conf` file was correctly modified.

9. The Linux Sender uses the Pluggable Authentication Module (PAM) for authentication. If you are using the GNOME Desktop Manager or KDE Desktop Manager you must manually add the following lines to the files `/etc/pam.d/gdm`, `/etc/pam.d/kde`, and `/etc/pam.d/xdm`:

```
session    optional    pam_rg.so
```

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

11. 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 may 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 may need to add the following to the file "`/etc/pam.d/rgsender`".

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

12. The default on RedHat Linux is to bind the machine name to the loopback interface in the `/etc/hosts` file. 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.bigmoney.com
```

Linux Sender GUI Installation

The Sender GUI will automatically starts on Linux when the Sender process starts. If you prefer to start the Sender GUI on a per-user basis, then edit the file `/opt/hpremote/rgsender/rgsender.sh`, and add the `-noautostartgui` command line option as follows

```
exec ./rgsender $* -noautostartgui -l logSetup
```

and then proceed to follow the directions below.

KDE RedHat GUI setup

To section describes how to manually start the Sender GUI when KDE is the desktop manager.

1. Open the Konqueror file manager (the desktop icon that is named "Home").

2. On the menu bar select "Go/Autostart".
3. A new Konqueror window will open. Right click and select "Create New" and choose "Link to Application".
4. A dialog box will open. On the General Tab page, give it a name such as "rgsender".
5. On the Execute Tab page, add the following in the Command text edit box :

   /opt/hpremote/rgsender/rgsender_gui.sh
6. Click the "OK" button to save the changes.
7. Logout and log back in and you should see the RG Sender GUI.

GNOME RedHat Enterprise GUI setup

To section describes how to start the Sender GUI when Gnome is the desktop manager.

1. Open the Nautilus file manager (the desktop icon that is named "Start Here")
2. Select the "Preferences" icon.
3. Select the "Session" icon.
4. Select the "Session Properties & Startup Programs" icon. A new dialog window will open.
5. Select the "Startup Programs" Tab in the new dialog window
6. Click the "Add" button. A new dialog window will open.
7. In the "Startup Command" text edit box in the new dialog window enter:

   ```
   /opt/hpremote/rgsender/rgsender_gui.sh --display :0.0
   ```
8. Select the "OK" button.
9. Select the "Apply" button.
10. Logout and log back in and you should see the RG Sender GUI.

Optionally, you can also setup Gnome so the icon does not show up on the task bar - the following instructions do not apply for RedHat Enterprise Edition systems.

1. Go back to the Nautilus file manager, select "Preferences" and then select "Sawfish window manager."
2. Select "Matched Windows". A new dialog window will open.
3. Click the "Add" button. A new dialog window will open.
4. In the "Matchers" window select the down arrow button and select "Name" in the left text edit window.
5. In the corresponding text edit window on the right enter the following "rgsender_gui"

6. On the "Other" tab in this window select the "Skip tasklist" button.
7. On the "State" tab in this window select the "Cycle skip" button and the "Window list skip" button.
8. Click on OK
9. Click on OK
10. Logout and log back in and you should not see the rgsender_gui listed in the task bar although you should see the icon on the desktop.

Installing the RGS Sender for HP-UX

HP-UX Sender Installation

1. Login as root.
2. Insert the HP Remote Graphics Software CD and mount the CD.
3. Go to the mount point of the CD, which is usually `/mnt/cdrom`, and change directoryies to `hpux-pa/sender`.
4. Execute the following command:

   ```
   ./install.sh
   ```

5. The Sender will be installed to `/opt/hpremote/rgsender` and will be started automatically when the X Server or system is restarted.
6. The HP-UX Sender uses the Pluggable Authentication Module (PAM) for authentication. Add the following lines to the file `/etc/pam.conf`:

   ```
   gdm     session optional /usr/lib/security/libpam_rg.1
   dtlogin session optional /usr/lib/security/libpam_rg.1
   ```

7. 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 always consult your HP-UX documentation when configuring PAM. If you are using a custom PAM authentication module called "`libpam_custom.1`" then you may need to edit the PAM configuration file "`/etc/pam.conf`" to specify the PAM authentication module to be used by the RGS Sender. For example, may need to add to the file "`/etc/pam.conf`" the following:

   ```
   rgsender auth optional /usr/lib/security/libpam_custom.1
   ```

NOTE: The system must contain the December 2002 or newer X server patches. HP-UX 11.0 requires X server patch PHSS_26637 or newer. HP-UX 11.11 requires X server patch PHSS_26638 or newer.

The system must also contain the September 2004 OpenGL patch (PHSS_30882) or newer for proper 3D OpenGL operation.

HP Remote Graphics Software is not supported the HP-UX 10.20 or HP-UX 11i V2 operating system, and is only supported on PA-RISC 2.0 architecture.

HP-UX Sender GUI Installation

The Sender GUI will automatically start on HP-UX when the Sender process starts. If you would rather start the GUI on a per-user basis, then edit the /opt/hpremote/rgsender/rgsender.sh file, and add the -noautostartgui option as follows:

```
exec ./rgsender $* -noautostartgui -l logSetup
```

Uninstalling the RGS Sender

Uninstalling the RGS Sender for Windows:

To uninstall the Windows Sender use the Windows 2000 or Windows XP Add or Remove Programs feature from the Control Panel. Select Remote Graphics Sender and click Change/Remove.

Uninstalling the RGS Sender for Linux:

To uninstall the Linux Sender find the name of the RedHat RPM package for the Remote Graphics Sender, by typing:

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

If the Sender is installed on the system, you will see rgsender_linux_32-4.0-0 or something similar. To remove the Sender's rpm package, become root and type:

```
rpm -e --allmatches rgsender_linux_32
```

Uninstalling the RGS Sender for HP-UX:

To uninstall the HP-UX Sender, become root and type:

```
/usr/sbin/swremove -x autoreboot=true rgsender_hpux_pa
```

Creating Unattended Installers

Unattended installers can be created for the RGS Receiver and Sender for Windows. Unattended installers are useful when an enterprise needs to install RGS without user interaction.

Creating an Unattended Receiver Installer for Windows

The RGS Receiver installer is created using InstallShield and normally requires user interaction when run. To create unattended installers for the RGS Receiver install the RGS Receiver by creating an installation script with the following commands:

1. First install the RGS Receiver by running the `Setup.exe` for the RGS Receiver with the `/r` (record mode) and `/f1` ("ef-one", alternative response filename) flags. For example:

   ```
   Setup.exe /r /f1"C:/TEMP/ReceiverInstall.iss"
   ```

   This creates the InstallShield response file `ReceiverInstall.iss` which can be used for unattended installs on other systems.

2. Install the RGS Receiver on other systems using the `/s` (silent mode) flag and the response file created in the previous step. For example:

   ```
   Setup.exe /s /f1"C:/TEMP/ReceiverInstall.iss"
   ```

Creating an Unattended Sender Installer for Windows

The RGS Sender installer is created using InstallShield and normally requires user interaction when run. To create unattended installers for the RGS Sender install the RGS Sender by creating an installation script with the following commands:

1. Install the RGS Sender by running the `Setup.exe` for the RGS Sender with the `/r` (record mode) and `/f1` ("ef-one", alternative response filename) flags. For example:

   ```
   Setup.exe /r /f1"C:/TEMP/SenderInstall.iss"
   ```

   This creates the InstallShield response file `SenderInstall.iss` which can be used for unattended installs on other systems.

2. Install the RGS Sender on other systems using the `/s` (silent mode) flag and the response file created in the previous step. For example:

   ```
   Setup.exe /s /f1"C:/TEMP/SenderInstall.iss"
   ```

Installing & Enabling Remote Audio

Remote Graphics Software supports remote audio. Refer to the System Requirements section for the list of supported RGS Sender and Receiver operating systems.

The Receiver Control Panel enables remote audio. When remote audio is enabled the Sender records and transmits audio to the Receiver for playback. Audio controls in the Receiver Control Panel allow you set the audio volume, quality, and stereo/mono format. Note that audio quality and stereo settings will affect your overall network usage and bandwidth.

The following sections assume the Remote Graphics Software is installed.

Installing Audio on a Receiver for Windows

The Receiver uses the default audio device. If you do not have an audio device installed or if it is currently disabled, the audio controls in the receiver are disabled.

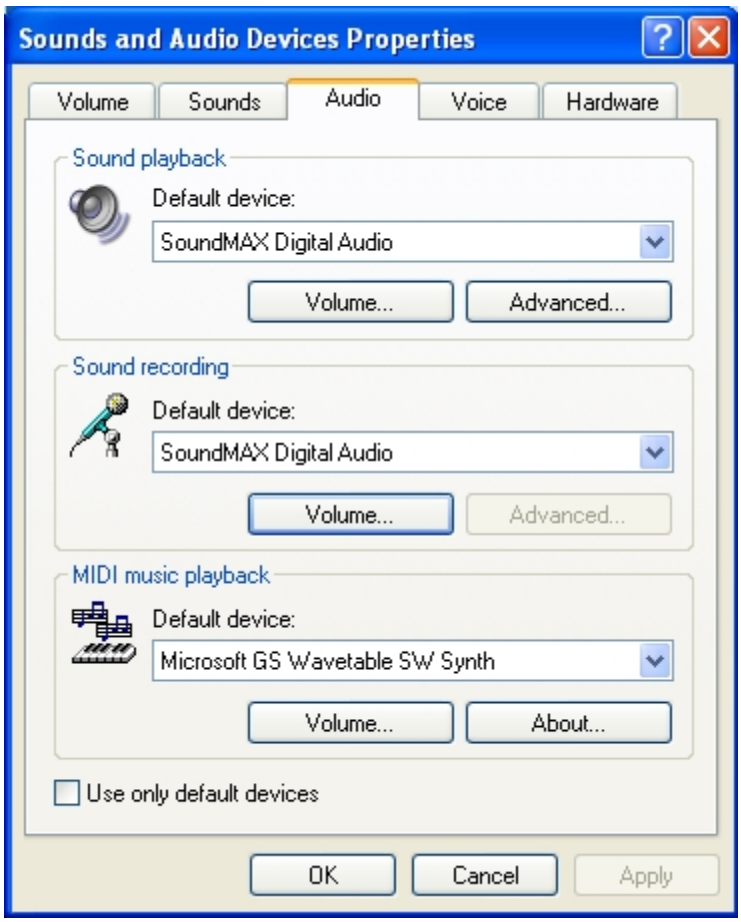
Note: The audio controls in the Receiver Control Panel can be disabled by setting properties in the Receiver if the administrator does not want to allow the user to modify the audio settings.

Installing and Calibrating Audio on a Sender for Windows

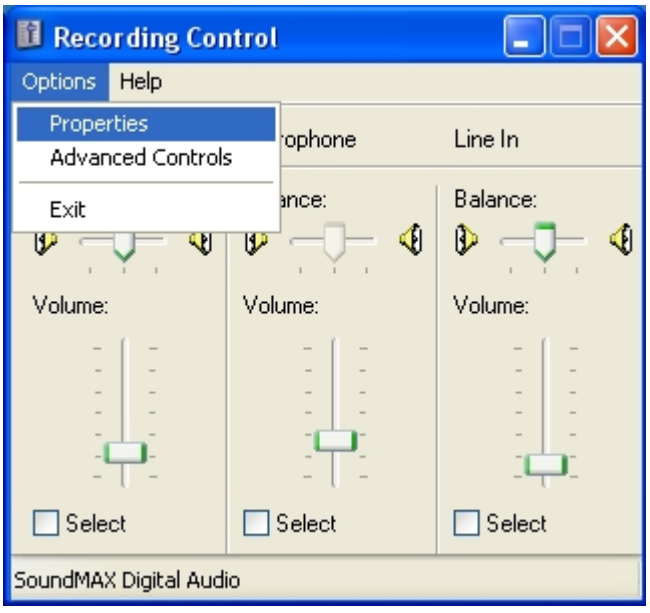
Installing Audio on a Sender for Windows

The RGS Sender records from the audio device mixer and sends this information to the receiver. If an audio device is not detected during installation, the HP Remote Audio device will be installed. The HP Remote Audio device has only the mixer available in the recording control panel and the volume level for this line cannot be adjusted. If an audio device is detected during installation, an attempt is made to select the mixer as the recorder input. Due to wide variations in naming and volume levels, it is likely that the mixer line will need to be selected by hand.

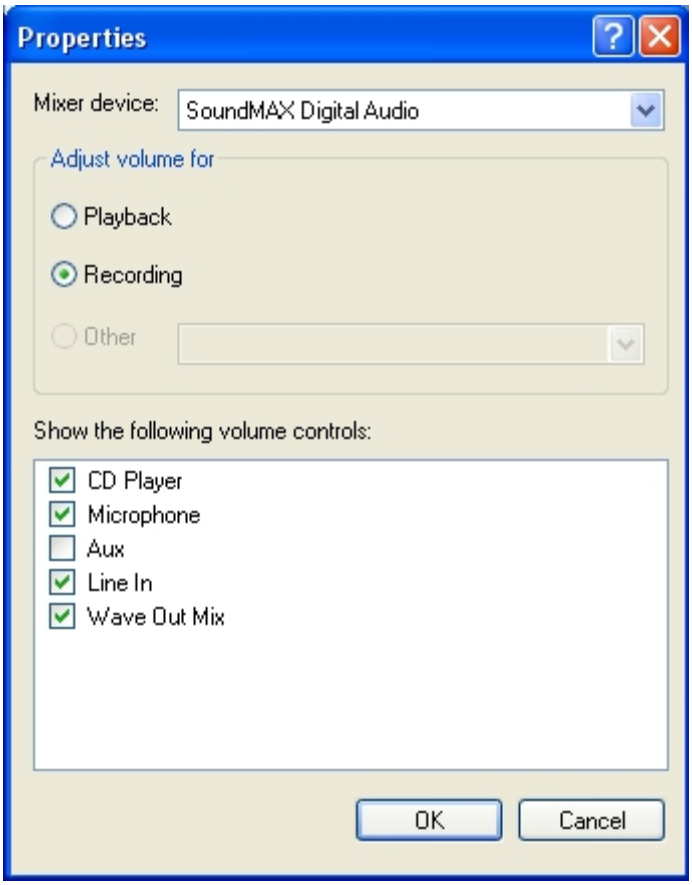
To select the mixer as the input line, open the Sounds and Audio Devices control panel. You can find this by opening the Windows Control Panel in the Start menu. The following picture shows an example of a Control Panel with the Audio tab selected.



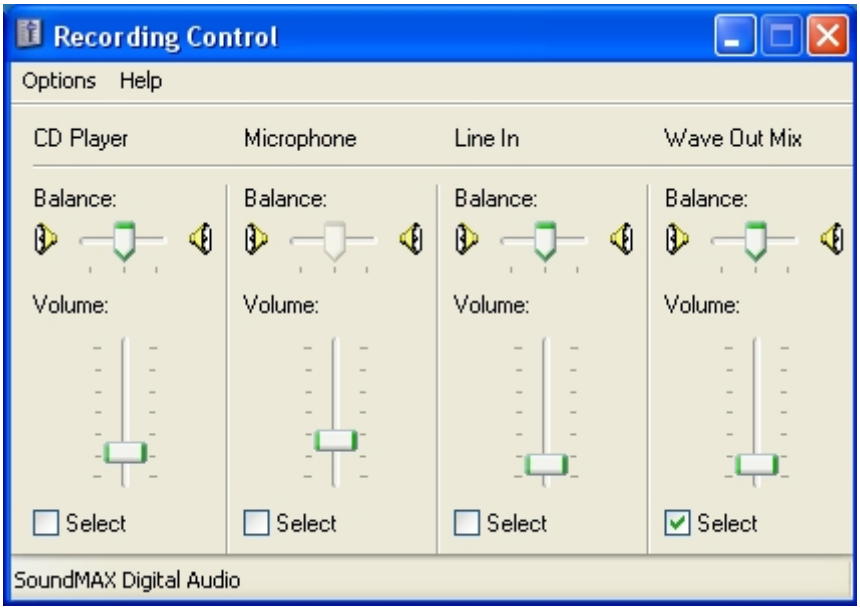
Press the Volume button in the Sound recording section in the middle of this window. This brings up the Recording Control window. Many audio device drivers do not show all available inputs by default. The mixer line is often one of the control lines that are not visible by default. To make it visible, click on the Options item in the menu and then click on the Properties item as shown in the following picture.



This brings up another window showing all available controls. The control associated with the mixer is often called “Wave Out Mix”, “Stereo Mix”, or some variation on “Mixer”. The Creative Audigy driver calls this the “What U Hear” control. Make sure this control is enabled similar to the following.



Press the OK button and you should see that the Recording Control window now has the mixer line as one of the controls. Make sure this item is selected and that the volume level is not at the bottom. The following picture shows an example of a selected mixer line.

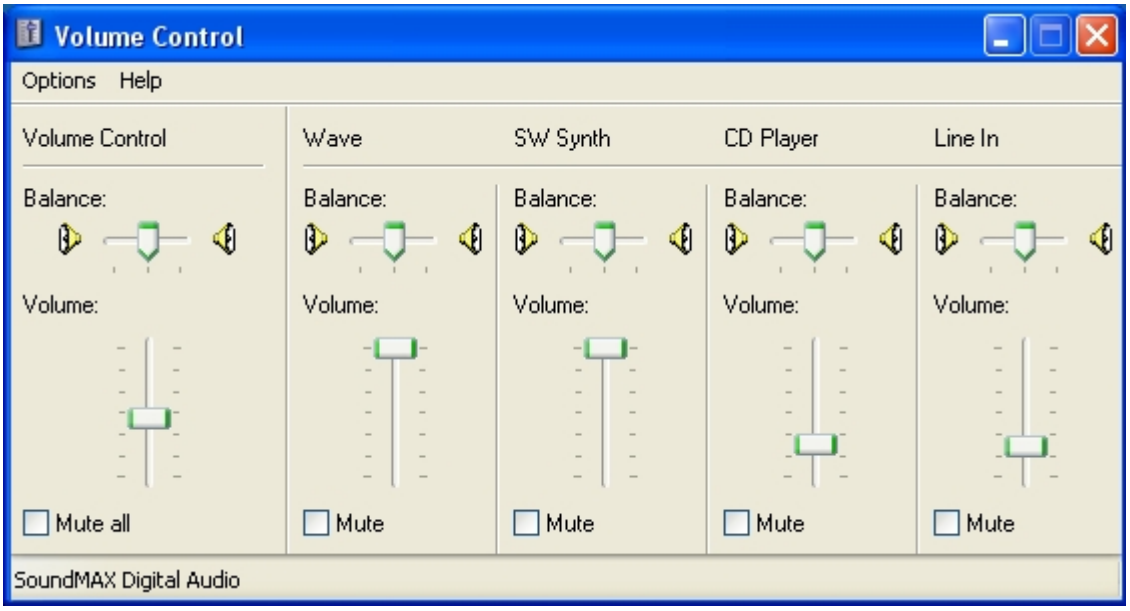


After you have selected the mixer, the Sender should record audio information and send it to the Receiver. Refer to the Windows RGS Sender Audio Calibration section to improve the audio quality. If you are not getting an audio signal, refer to the Windows Audio Troubleshooting section.

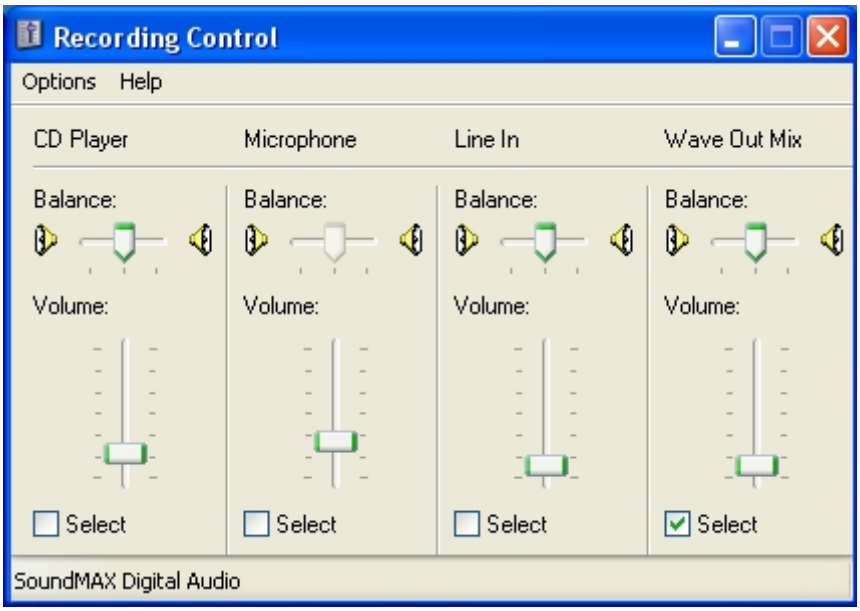
Calibrating Audio on a Sender for Windows

The audio signal captured by the sender is modified by two different device driver volume controls and then the master volume level is artificially inserted into the signal. If these volume controls are too low, you might hear the audio signal. If they are too high, the signal may be distorted. This section describes a technique to hand tune the controls to reduce the amount of distortion. These operations should be performed while connected to the sender through the receiver.

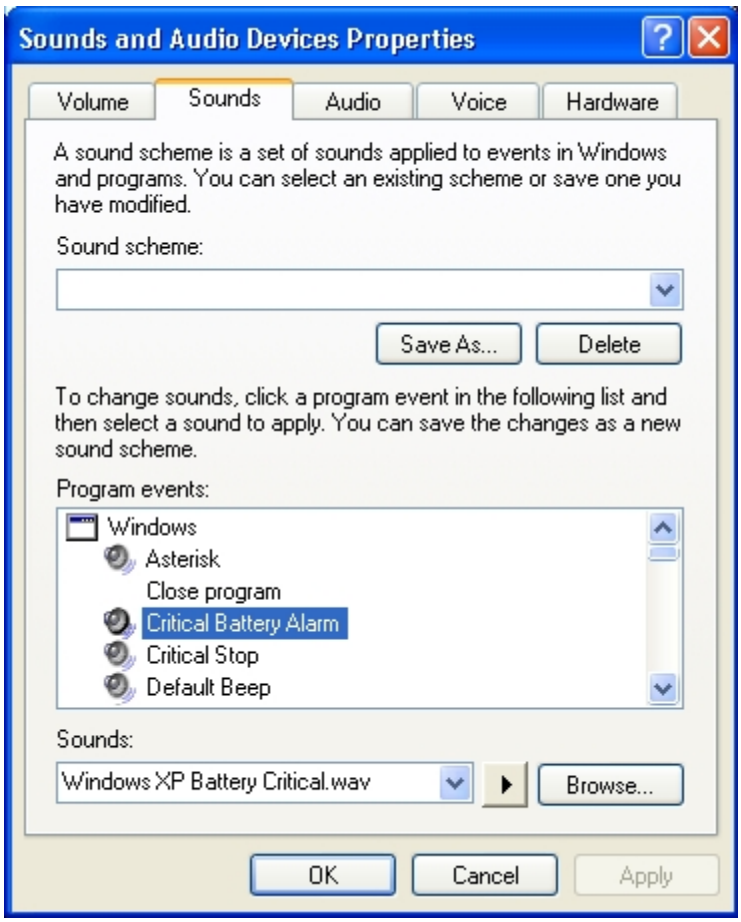
The Wave line of the Volume Control is the first volume control to impact the audio signal outside of the application that generates the signal. Setting this value to the maximum level gives you the most resolution in your audio signal. The following image shows an example of this control at its maximum level.



The next volume control to adjust is the mixer line of the Recording Control. The name of this line varies with different audio devices. See the Windows Sender Audio Installation section for information on how to determine the name of this control. For our example, the control is called Wave Out Mix. Adjust this volume control while playing a sound. At higher levels, the audio signal gets clamped and the signal becomes distorted. Decrease the level until the sound becomes clear. On some devices, the mixer volume control does not go to zero. In this case, the Wave line of the Volume Control will need reduction. The following image demonstrates the Wave Out Mix level needed to eliminate distortion. Note that this is in the Recording Control.



The best sound to play to calibrate your audio device is a low frequency sound with high amplitude. By default, Windows assigns a program event that meets these requirements. To play this sound, open up the Sound and Audio Devices control panel and click on the Sounds tab as shown in the following windows.



Select the Critical Battery Alarm program event and press the play button (the triangle located next to the Browse button). The wav file associated with this event is recorded at near maximum intensity. If you can play this sound without distortion, you should play mosts sounds without distortion. Some media applications modify their audio signal prior to sending it to the audio device. The Windows Media Player may appear to distort some audio files. This is due to signal modification by some kind of enhancement such as an equalizer.

Installing Audio on a Receiver for Linux

If you install audio on a Receiver for Linux the audio component uses the JACK sound server API. JACK is a low late ncy sound server that works in conjunction with the ALSA sound drivers to mix and direct audio on your system. It runs as a daemon in the background and acts as a “patch bay” for audio connections and applications that use the JACK interface.

For reliable audio support with the Receiver for Linux, the bundled versions of the ALSA sound libraries and JACK Audio Connection Kit software must be built and installed. Versions of ALSA prior to the version provided with the installer may yield unsupportable results. Removal of these previous versions is advised prior to reinstallation of ALSA software.

If multiple audio devices are installed in a system, administrators should identify the target audio system prior to installing the included ALSA software.

Properly configured kernel headers for the running kernel must be available from the directory `/lib/modules/<version>/build` for proper installation. The example installation script provided only builds/installs for the currently active kernel.

The installation and configuration scripts require administrator privileges on the target system. If you cannot become root on your system, ask an administrator for assistance.

Once ALSA and JACK are installed and correctly configured, you are ready to use remote audio with the RGS Receiver for Linux.

Audio Requirements

For reliable audio support with the Receiver for Linux, the bundled version of the JACK Audio Connection Kit software must be built and installed. ALSA sound libraries must be HP-supported or Red Hat Enterprise Linux (release 4 or greater) versions for best results. Manual installation of prior ALSA libraries may yield unpredictable results on older releases of Linux. Do not mix versions of ALSA software.

If multiple audio devices are installed in a system, administrators should identify the target audio system prior to installing the included ALSA software.

Properly configured kernel headers for the running kernel must be available from the directory /lib/modules/<version>/build for proper installation. The example installation script provided only builds/installs for the currently active kernel.

The installation and configuration scripts require administrator privileges on the target system. If you cannot become root on your system, ask an administrator for assistance.

System Preparation

It is recommended to remove all previously installed versions of JACK before installation. If the RPM package manager was utilized, then the packages are located by:

- `rpm -qa | grep -i jack`

Removal by RPM involves utilizing the above search results with:

- `rpm -e --nodeps --allmatches {pkg-name}`

The install script `rgs_audio_support` may detect residual directories from previous installations. Respond as prompted during installation.

Customized Installation

The following remote audio installation for Linux process is used when the RGS Receiver is installed (through the `./install.sh` script). For those installations that require customization or wish to use other features from the `rgs_audio_support` script, here are additional details for its use.

The audio support bundle ships as `hp_rgs_4_audiosupport.tar.gz`. It is accessed by the RGS `install.sh` script in `/opt/hpremote` or may be utilized for manual installations / RPM package building.

The install process requires a locally writable directory in which to build. Locate the support bundle in an appropriate directory before installation.

Use the following command to unpack the file manually if desired:

- `tar xzf hp_rgs_4_audiosupport.tar.gz`

As the user root, change directory into the one created by the command above. It will contain important files such as:

- `README.txt` - basic instructions and file manifest
- `rgs_audio_support` - shell installation script for ALSA/JACK libraries
- `alsa-*.tar.bz2` - recent validated tar archives from the ALSA project (provided only for open source requirements and legacy installations) - `http://alsa-project.org`
- `jack-*.tar.gz` - recent validated tar archives from the JACK-Audio-Connection-Kit project - `http://jackit.sourceforge.net`
- `libsndfile-*.tar.gz` - recent validated tar archives from the libsndfile project (JACK dependency) - `http://www.mega-nerd.com/libsndfile`

The sample installation script, `rgs_audio_support`, offers three installation scenarios:

1. `install` - This command unpacks all tar archives into a local build directory in the current directory [`./localroot`], configures, builds, and installs the required ALSA/JACK libraries appropriate for the host system and active kernel. It is a good choice for local installations or system development. A system reboot is recommended for best results.
2. `remove` - This command removes and un-configures an installation provided by the above install command.
3. `build_rpms` - This command runs an install command first and then attempts to create a compatible set of binary RPMs for installation on matched system configurations. This will greatly reduce the work of enterprise administrators duplicating this install process across multiple nodes. After a successful build, the following files are created:
    - `./RPMS/*.rpms` - binary RPMs copied from `/usr/src/redhat/RPMS`
    - `./RPMS/RGS_audio_install.sh` - customized install and configuration script to associate with RPMs

Note: The build log created by this script is located in `/var/log/hpaudio.log`

Note: The install command does not yield results visible by the RPM package manager, `rpm`. The `rpm` database is not updated nor will inquiries with `rpm -q` report the installation. Only installations performed with the results of `build_rpms` are manageable by the `rpm` command.

The sample installation script, `rgs_audio_support`, supports limited customization capabilities for newer source deliveries as they become available. See the script internals for more details.

Installing and Enabling Single Sign-on

Installing and Enabling Single Sign-on on Windows

Installing RGS Single Sign-on is for experienced users and IT administrators only. Please read all the directions completely before proceeding and exercise caution when installing.

The RGS shared library, `hprgina.dll`, enables Single Sign-on. The file `hprgina.dll` is a GINA (Graphical Identification and Authentication) module that is loaded by the Window's `WinLogon.exe` process. There are three ways to install and enable RGS Single Sign-on.

1. Install time:

The `hprgina.dll` can be installed and enabled during the RGS Sender installation. This is the preferred method and is the safest and easiest way to enable RGS Single Sign-on. The default during installation is to not enable Single Sign-on. The user must answer two questions before Single Sign-on is properly enabled. If enabled, the system must be rebooted before RGS Single Sign-on is operational.

2. Using the **`rgadmin`** Tool:

The RGS Rgadmin Tool can be used to enable or disable the `hprgina.dll`. The `rgadmin` tool can also be run from the command line with the proper options to enable or disable the GINA module. This method is preferred over the manual method.

3. Manual Method:

Although this is not the preferred method to enable RGS Single Sign-on, it is here so that administrators will know exactly what parts of the system are modified. To manually enable `WinLogon` to load the `hprgina` module, do the following steps in the exact order listed:

1. Install the RGS Sender on the HP Workstation. If the RGS Sender is not installed or installs with errors, DO NOT perform the remaining steps. Doing so puts the system in a state that requires a complete re-installation of the operating system.
2. After the RGS Sender is installed confirm that the `hprgina.dll` exists in the `C:\WINDOWS\system32` directory. The RGS Sender installer copies `hprgina.dll` into the `system32` directory directly. If it does not exist, DO NOT perform the remaining steps. Doing so puts the system in a state that requires a complete re-installation of the operating system.
3. Add the `GinaDLL` registry key if it does not already exist. This can be done through the use of `regedit`, the Windows Registry Editor. Create the key as type `REG_SZ` (a string type). The full path of the key is

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\GinaDll
```

4. Set the value of the GinaDll key to the text "hprgina.dll". Confirm the spelling before closing.
5. Add the GinaDllMode registry key if does not already exist. This can be done through the use of regedit as well. Create the key as type RGS_SZ (a string type). The full path of the key is

   ```
   HKEY_LOCAL_MACHINE\Software\Hewlett-Packard\Remote Graphics
   Sender\GinaDllMode
   ```

6. Set the value of the GinaDllMode key to the text "HprSso". Confirm the spelling before closing.
7. Restart the system. The hprgina.dll will be loaded by WinLogon when started.

   WARNING: If the hprgina.dll does not exist in C:\WINDOWS\system32, do not perform steps three and four. Doing so puts the system in a state that requires a complete re-installation of the operating system.

If the GinaDLL key does not currently exist in the registry then Microsoft's default GINA DLL (msgina.dll) is currently loaded by WinLogon. Adding the GinaDLL registry key and setting its value to hprgina.dll tells WinLogon to load the hprgina.dll instead of the default msgina.dll.

If the GinaDllMode key does not exist in the registry, or if the key does not contain the text "HprSso", then RGS Single Sign-on will be enabled by default.

Setting the Local Security Policy

The local security policy "Interactive logon: Do not require CTRL-ALT-DEL" must be disabled to support Single Sign-on. This can be set in the Windows "Local Security Settings" under "Security Options." The RGS Diagnostic Tool programmatically detects if this local security policy is set correctly. See the RGS Diagnostic Tool section for more information.

Note: Creating the GinaDLL registry key disables Window's "Fast User Switching" and "Welcome Screen" features.

Uninstalling and Disabling Single Sign-on

There are two methods used to disable Single Sign-on:

1. Using the **rgadmin** Tool:

The RGS Rgadmin Tool contains command-line options to disable RGS Single Sign-on. This method is preferred over the manual method.

2. Manual Method:

To disable Single Sign-on without the use of the rgadmin tool, delete or rename the value of the GinaDLL registry key. If there is no other custom GINA module on the system, simply removing the GinaDLL key definition from the registry disables Single Sign-on. The GinaDLL key:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\GinaDll
```

is removed through the use of regedit, the Windows Registry Editor. Be certain to actually remove the key by selecting the GinaDLL key in regedit and select the Delete entry in the Edit menu. Once the key is deleted, it no longer shows up as a key in the WinLogon subkey. When the system reboots, the default GINA module, msgina.dll, will be loaded by the WinLogon.exe process.

If there is a custom GINA DLL module on the system and it replaces the default msgina.dll, change the value of the GinaDLL value from hprgina.dll to the name of the custom GINA module. To change the value of the GinaDLL key, select the GinaDLL key in regedit and then select the Modify entry in the Edit menu. A dialog box appears allowing the value of the key to be changed. Type the name of the custom GINA module in the "Value data:" area. Confirm that the custom GINA module entered actually exists on the system in C:\WINDOWS\system32. When the system reboots the custom GINA module is loaded by the WinLogon.exe process.

WARNING: If the value of the GinaDLL key contains the name of a custom GINA DLL, and the file does not exist in C:\WINDOWS\system32, the system will not start correctly upon the next reboot. The system will then require a complete re-installation of the operating system.

Installing and Enabling Easy Login

Installing and Enabling Easy Login on Windows

Easy Login is only supported on HP Blade Workstations running the RGS Sender. Installing Easy Login is for experienced users and IT administrators. Please read all the directions completely before proceeding and exercise caution when installing.

The RGS shared library, `hprgina.dll`, enables Easy Login. The file `hprgina.dll` is a GINA (Graphical Identification and Authentication) module that is loaded by the Window's `WinLogon.exe` process. There are three ways to install and enable RGS Easy Login.

1. Install time:

The `hprgina.dll` can be installed and enabled during the RGS Sender installation. This is the preferred method and is the safest and easiest way to enable RGS Easy Login. The default during installation is to not enable Easy Login. The user must answer two questions before Easy Login is properly enabled. If enabled, the system must be rebooted before RGS Easy Login is operational.

2. Using the **`rgadmin`** Tool:

The RGS Rgadmin Tool can be used to enable or disable the `hprgina.dll`. The `rgadmin` tool can also be run from the command line with the proper options to enable or disable the GINA module. This method is preferred over the manual method.

3. Manual Method:

Although this is not the preferred method to enable RGS Easy Login, it is here so that administrators will know exactly what parts of the system are modified. To manually enable `WinLogon` to load the `hprgina` module, do the following steps in the exact order listed:

1. Install the RGS Sender on the HP Blade Workstation. If the RGS Sender is not installed or installs with errors, DO NOT perform the remaining steps. Doing so puts the system in a state that requires a complete re-installation of the operating system.
2. After the RGS Sender is installed confirm that the `hprgina.dll` exists in the `C:\WINDOWS\system32` directory. The RGS Sender installer copies `hprgina.dll` into the `system32` directory directly. If it does not exist, DO NOT perform the remaining steps. Doing so puts the system in a state that requires a complete re-installation of the operating system.
3. Add the `GinaDLL` registry key if it does not already exist. This can be done through the use of `regedit`, the Windows Registry Editor. Create the key as type REG_SZ (a string type). The full path of the key is

   ```
   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
   NT\CurrentVersion\Winlogon\GinaDll
   ```

4. Set the value of the GinaDll key to the text "hprgina.dll". Confirm the spelling before closing.
5. Add the GinaDllMode registry key if does not already exist. This can be done through the use of regedit as well. Create the key as type RGS_SZ (a string type). The full path of the key is

   HKEY_LOCAL_MACHINE\Software\Hewlett-Packard\Remote Graphics Sender\GinaDllMode

6. Set the value of the GinaDllMode key to the text "HprEasyLogin". Confirm the spelling before closing.
7. Restart the system. The hprgina.dll will be loaded by WinLogon when started.

   WARNING: If the hprgina.dll does not exist in C:\WINDOWS\system32, do not perform steps three, four and five. Doing so puts the system in a state that requires a complete re-installation of the operating system.

If the GinaDLL key does not currently exist in the registry then Microsoft's default GINA DLL (msgina.dll) is currently loaded by WinLogon. Adding the GinaDLL registry key and setting its value to hprgina.dll tells WinLogon to load the hprgina.dll instead of the default msgina.dll.

The hprgina module is a chaining GINA DLL. When the RGS hprgina.dll is loaded by WinLogon, the hprgina module then loads the msgina.dll shared library. The hprgina module chains (forwards) all GINA requests to the msgina.dll module.

Chaining custom GINA modules

If it is discovered in step #3 above that the GinaDLL registry key does exist, and the value of the key is not msgina.dll, then a custom GINA module is currently loaded and being used by WinLogon. Custom GINA modules provide custom authentication dialogs or even custom user authentication methods. If it is determined that functionality of both the RGS Easy Login and a custom GINA module is necessary, then the hprgina.dll needs further configuration. The hprgina.dll module needs to be setup to load the custom GINA module rather than the default msgina.dll as described above.

To enable the hprgina module to load a custom GINA module, create a new registry key, ChainedGinaDLL, on the system with the value of the key containing the name of the chained custom GINA module. Do steps #1 through #4 shown above (the reboot will be done below) plus the following steps to chain custom modules:

1. Create the ChainedGinaDLL registry key. Create the key as type REG_SZ (a string type). The full path of the key is:

   HKEY_LOCAL_MACHINE\Software\Hewlett-Packard\Remote Graphics Sender\ChainedGinaDLL

2. Set the value of the new ChainedGinaDLL key to the name of the custom GINA module. For instance, if the name of the custom GINA module is foogina.dll, then the value of the key is foogina.dll. The value should

match the string originally discovered in the registry key GinaDLL. Confirm the spelling before closing.

3. Restart the system.

When the RGS hprgina.dll is loaded by WinLogon, hprgina loads the chained GINA DLL foogina.dll. The hprgina module then chains all GINA requests to the foogina module.

If the custom foogina.dll is also a chaining GINA module, foogina, in turn, chains itself to the msgina module. Three GINA DLLs will be loaded as part of the WinLogon.exe process: 1) hprgina.dll, 2) foogina.dll, and 3) msgina.dll.

Setting the Local Security Policy

The local security policy "Interactive logon: Do not require CTRL-ALT-DEL" must be disabled to support Easy Login. This can be set in the Windows "Local Security Settings" under "Security Options." The RGS Diagnostic Tool programmatically detects if this local security policy is set correctly. See the RGS Diagnostic Tool section for more information.

Note: Creating the GinaDLL registry key disables Window's "Fast User Switching" and "Welcome Screen" features.

Uninstalling and Disabling Easy Login

There are two methods used to disable RGS Easy Login.

1. Using **rgadmin** Tool:

The RGS Rgadmin Tool contains command-line options to disable RGS Easy Login. This method is preferred over the manual method.

2. Manual Method:

To disable Easy Login without the use of the rgadmin tool, delete or rename the value of the GinaDLL registry key. If there is no other custom GINA module on the system, simply removing the GinaDLL key definition from the registry disables Easy Login. The GinaDLL key:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\GinaDll
```

is removed through the use of regedit, the Windows Registry Editor. Be certain to actually remove the key by selecting the GinaDLL key in regedit and select the Delete entry in the Edit menu. Once the key is deleted, it no longer shows up as a key in the WinLogon subkey. When the system reboots, the default GINA module, msgina.dll, will be loaded by the WinLogon.exe process.

If there is a custom GINA DLL module on the system and it replaces the default msgina.dll, change the value of the GinaDLL value from hprgina.dll to the name of the custom GINA module. To change the value of the GinaDLL key, select the

GinaDLL key in regedit and then select the Modify entry in the Edit menu. A dialog box appears allowing the value of the key to be changed. Type the name of the custom GINA module in the "Value data:" area. Confirm that the custom GINA module entered actually exists on the system in C:\WINDOWS\system32. When the system reboots the custom GINA module is loaded by the WinLogon.exe process.

WARNING: If the value of the GinaDLL key contains the name of a custom GINA DLL, and the file does not exist in C:\WINDOWS\system32, the system will not start correctly upon the next reboot. The system will then require a complete re-installation of the operating system.

Installing the Enterprise Service SDK

The RGS Enterprise Service SDK can be easily installed by following the directions below. The Enterprise Service SDK is meant to be installed by IT administrators and is not normally installed by end-users. The SDK is a Software Development Kit that can be used to implement a RGS Enterprise Service. A sample implementation is delivered with the SDK.

Installing the Enterprise Service SDK on Windows

To begin the installation, log in to an account with administrator privileges:

1. Insert the HP Remote Graphics Software CD and in Window's Explorer change to the directory `win32\enterprise-service` on your CD-ROM drive.
2. Double-click or select `Setup.exe` to start the installer.
3. Follow the instructions on the screen.

The installer will add a menu item to the HP Remote Graphics Programs folder called Start Enterprise Service.

Note: The Enterprise Service is a Python program and requires Python Version 2.4 for proper operation. For convenience, the Python installation package `python-2.4.msi` is included in the Enterprise Service installation directory (`C:\Program Files\Hewlett-Packard\Remote Graphics Enterprise Service`).

Enabling the Enterprise Service in the Receiver

All of the functionality necessary to communicate with the Enterprise Service is in the RGS Receiver. Refer to the Installing the Receiver section to install the RGS Receiver. To use the Enterprise Service, refer to the Using the Enterprise Service section.

Enabling OpenGL Applications

HP Remote Graphics Software supports remote viewing of 3D applications. The OpenGL 3D API is supported on all sender platforms. The HP-UX Sender supports all HP-UX 3D APIs.

Enabling OpenGL Applications on Windows

Automatically Enabling 3D Updates from OpenGL Applications:

HP Remote Graphics Software will automatically receive updates from 3D OpenGL applications. Automatic 3D updates are enabled by default during RGS Sender installation. On a Windows's 64-bit OS (XP Professional x64 Edition), automatic 3D updates are enabled for 32-bit and 64-bit OpenGL applications. Previous versions of HP Remote Graphics Software required a library called `OpenGL32.dll` to be manually placed into the OpenGL application directory to obtain 3D updates. This file should be removed from the OpenGL application directory to obtain maximum performance. Do not remove the `OpenGL32.dll` library from the system directory (`"C:\WINDOWS\system32"`).

Manually Enabling 3D Updates from OpenGL Applications:

If automatic updates are disabled through the RGS Admin Tool, 3D updates will only be received from OpenGL applications that have the HP Remote Graphics Software `OpenGL32.dll` library manually copied into the OpenGL application directory. For example, suppose you want to enable remote viewing for the 3D OpenGL application "`foo3d.exe`". If the executable "`foo3d.exe`" is installed in the directory "`C:\Program Files\foo3d`", you will need to manually copy the HP Remote Graphics Software `OpenGL32.dll` from "`C:\Program Files\Hewlett-Packard\Remote Graphics Sender\OpenGL\32-bit`" to "`C:\Program Files\foo3d`". This must be done before the application "`foo3d.exe`" is started.

On a Window's 64-bit OS (XP Professional x64 Edition) system, there are two RGS `OpenGL32.dll` libraries - a 32-bit library and a 64-bit library. They are both named `OpenGL32.dll` and are use to enable viewing of OpenGL 32-bit or 64-bit applications. The libraries are located in the RGS Sender install directory "`C:\Program Files\Hewlett-Packard\Remote Graphics Sender\OpenGL\32-bit`" and "`C:\Program Files\Hewlett-Packard\Remote Graphics Sender\OpenGL\64-bit`". For remote viewing of 32-bit OpenGL applications running on a 64-bit OS, use the instructions above. For remote viewing of 64-bit OpenGL applications, the 64-bit RGS `OpenGL32.dll` must be manually copied to the same directory as the 64-bit OpenGL application executable.

Enabling OpenGL Applications on Linux

There are two supported methods to enable remote viewing of OpenGL applications on Linux. The first, and preferred method, requires an nVidia graphics device present on the system. The second method requires the use of the `LD_PRELOAD` environment variable.

1. nVidia method: nVidia graphics drivers have extensions that enable remote viewing of OpenGL applications using a Remote Graphics Software. This method requires no user configuration other than making sure the proper nVidia drivers (version 1.0-5336 and beyond) are properly installed on the system.

2. LD_PRELOAD method: The LD_PRELOAD method is used for systems that do not have nVidia graphics installed. Set the LD_PRELOAD environment variable as follows:

   ```
   $ export LD_PRELOAD=/opt/hpremote/lib/librgopengl.so
   ```

   Once the LD_PRELOAD variable is properly set, any OpenGL application can be started. The application should then properly display in a Remote Graphics Software environment. To automate the setting of the environment variable, the variable can be set in the users .profile. For example, for those using bash, add the following to the system or users .bash_profile:

   ```
   $ export LD_PRELOAD=/opt/hpremote/lib/librgopengl.so
   ```

   Adding this to the .profile will enable remote viewing of 3D OpenGL screensavers.

Enabling OpenGL, PHIGS, PEX and Starbase Applications on HP-UX

OpenGL, PHIGS, PEX, and Starbase applications are automatically setup for remote access within an HP Remote Graphics Software environment. No extra setup steps are necessary. All that is required is that the proper X server and OpenGL libraries to be installed on the system.

Enabling Direct3D Applications on Windows

HP Remote Graphics Software will automatically receive updates from Direct3D 8.0 and Direct3D 9.0 applications. Automatic updates are enabled by default during RGS Sender installation. On a Windows's 64-bit OS (XP Professional x64 Edition), automatic updates are enabled for 32-bit and 64-bit applications.

Versions of the Direct3D API other than 8.0 and 9.0 are not supported. If automatic updates are disabled using the RGS Admin Tool, updates from all Direct3D applications will be unavailable.

Using Remote Graphics Software

Using the Receiver

Overview of the Remote Graphics Receiver

Receiver Terminology

The Receiver is composed of three main components:

1. Control Panel: The main Receiver window that is used to connect and control many Receiver settings.
2. Remote Display Window: The window that displays the desktop of the remote computer.
3. Remote Display Window Toolbar: A toolbar that is displayed at the top of the Remote Display Window that provides status information and has several controls.

Modes of operation

There are three modes of operation for the Receiver - Normal Mode, Directory Mode, and Enterprise Service Mode.

1. Normal Mode: Enables a user to connect to a system by specifying the hostname or IP address in the Receiver Control Panel:
   - On Windows, to start the HP Remote Graphics Software Receiver from the Start menu, select Start -> HP Remote Graphics -> Receiver
   - On Linux or HP-UX, execute

     ```
     /opt/hpremote/rgreceiver/rgreceiver.sh
     ```
2. Directory Mode: Enables a user to automatically open connections to several systems based on the systems assigned to each user. These assignments are saved in the RGS directory file on a shared file server or network mapped drive. This file is normally created and maintained by the system administrator or an IT support engineer.
   - On Windows, to start the HP Remote Graphics Software Receiver -directory version from the Start menu, select:

     ```
     Start -> HP Remote Graphics -> Receiver -directory
     ```
   - On Linux or HP-UX, type:

     ```
     /opt/hpremote/rgreceiver/rgreceiver.sh -directory [file]
     ```

     where the optional "file" is the path to the directory file. If the file path is not entered, then the user can enter the directory file through the use of the "Set Directory File" button on the user interface.

3. Enterprise Service Mode: Is similar to Directory Mode, but rather than looking up the systems assigned to a user in a file, they are looked up using the RGS Enterprise Service. The RGS Enterprise Service is a network service that is accessible over a standard computer network. Before the rgreceiver is started in Enterprise Service Mode, the Enterprise Service must be installed and running on the network and visible to the Receiver. After the Enterprise Service is started, the location of the Enterprise Service is entered on the command-line when starting the Receiver.

    - On Windows, to start the HP Remote Graphics Software Receiver in Enterprise Service Mode:

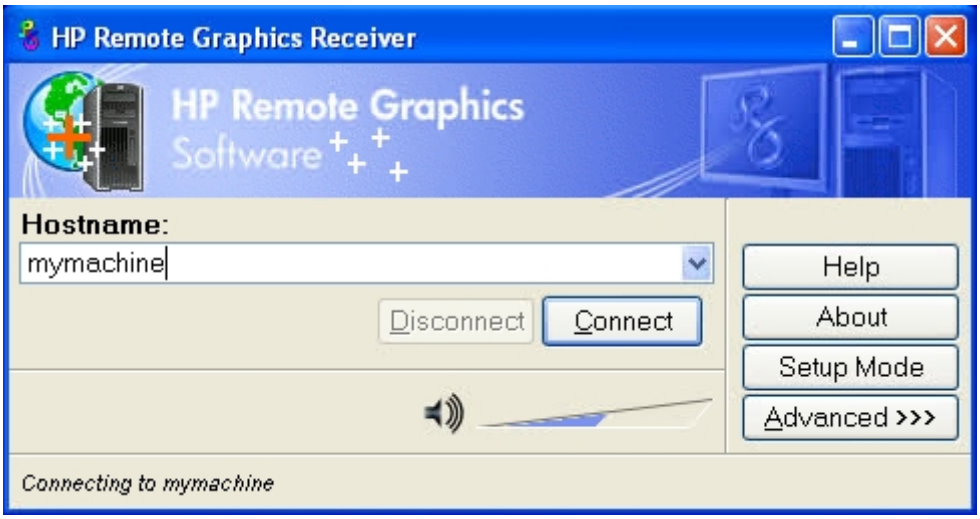
      ```
      cd "C:\Program Files\Hewlett-Packard\Remote Graphics
      Receiver"

      rgreceiver.exe -esdir service1 [service2 ... serviceN]
      ```

    - On Linux or HP-UX, execute:

      ```
      /opt/hpremote/rgreceiver/rgreceiver.sh -esdir service1
      [service2 ... serviceN]
      ```

    where "service1" is either the hostname or ipaddress of the system that the Enterprise Service is running on. Multiple hostnames or ipaddresses can be entered, each separated by white space.

Opening and Closing Connections



To connect to a Sender using the Receiver:

1. Enter the hostname or IP address of the Sender.
2. Press Enter or select the Connect button to connect.

The RGS Receiver Control Panel is used to perform the following tasks:

- Open a connection: To open a connection to a system, enter the hostname or IP address of the system running the RGS Sender in the Hostname field. Press Enter or select the Connect buttonto connect. The selector on the right side of the text box displays a history of previously connected systems that can be selected.
- Close a connection: To close a connection, select the Disconnect button.
- Authentication during a connection: When the Receiver connects to a Sender the user must be authenticated and authorized. The Receiver displays authentication dialogs where the user enters their credentials, such as username and password. If the Sender validates the credentials and the user is authorized, then the connection is established.
- Enable Setup Mode: Select the Setup Mode button to configure the local Remote Display Window. In Setup Mode, the Receiver suspends mouse and keyboard input to the remote system. This allows the user to move or resize the Remote Window Display Window. The Remote Display Window should also dim when Setup Mode is enabled. See Setup Mode and Hotkeys for more information.
- Display Help: Click Help to display the online help. The online help is displayed separately in a WEB browser, such as Internet Explorer or Mozilla.
- Display Program Information: Select the About button to display program and copyright information.

The RGS Receiver Control Panel contains a status bar at the bottom of the window.

The status bar provides information that describes the current state of the RGS receiver. For example, it displays messages that indicate “connection in progress”, “connection succeeded”, and “connection failed.” The status bar can be useful in diagnosing connection problems because it displays the general reason for the failure, for example, “Authorization Failed”, “Authentication Failed”, and more.

Controlling Receiver Settings

Receiver settings are controlled as follows:

- Via a tabbed set of options accessible by pressing the Advanced button on the Receiver Control Panel. The following groups of options are available: General Options, Audio Options, USB Options, Network Options, Hotkey Options, Logging Options, Statistics Options.
- The Remote Display Window Toolbar.

General Options:

Prompt for username and password under specific scenarios this option enables or disables prompting the user for domain, username and password credentials for each connection. When deselected, the current domain user credentials are sent to

the Sender. When selected, the Receiver can prompt and send an alternate user domain and password to the Sender. This is advantageous on Sender/Receiver pairs running Windows and Enterprise Service Mode with different connection needs for each session. Note: If Easy Login is installed on the Sender system, the user is sometimes not prompted for the connection.

Enable global image updates updates selects a different image update algorithm. When enabled, the Remote Display Window updates with all accumulated Sender updates as a single operation (commonly referred to as a BLockTransfer, or BLT). When disabled, the Remote Display Window updates with each intermediate change sent rather than accumulating results. The tradeoff is time versus quality. Global image updates reduces artifacts such as image tearing but sometimes at a higher data transfer cost (especially for large display resolutions).

Select help browser allows the user to specify a Web browser, such as mozilla, to display online help. This option is not available on Windows because the default Web Browser is automatically read from the Windows Registry.

Audio Options:

The Audio follows focus checkbox modifies the handling of the audio streams when connected to multiple remote systems. Checking the box enables only the audio stream corresponding to the Remote Display Window that currently has the keyboard focus. When unchecked, the Receiver combines the audio from all active connections into a single stream.

The Stereo checkbox enables or disables stereo audio. Stereo audio sends independent audio streams for the left and right channels. Stereo mode requires greater network bandwidth.

The Quality box allows the user to select one of three different audio quality settings:

- Low specifies a sampling rate of 11 KHz.
- Medium specifies a sampling rate of 22 KHz.

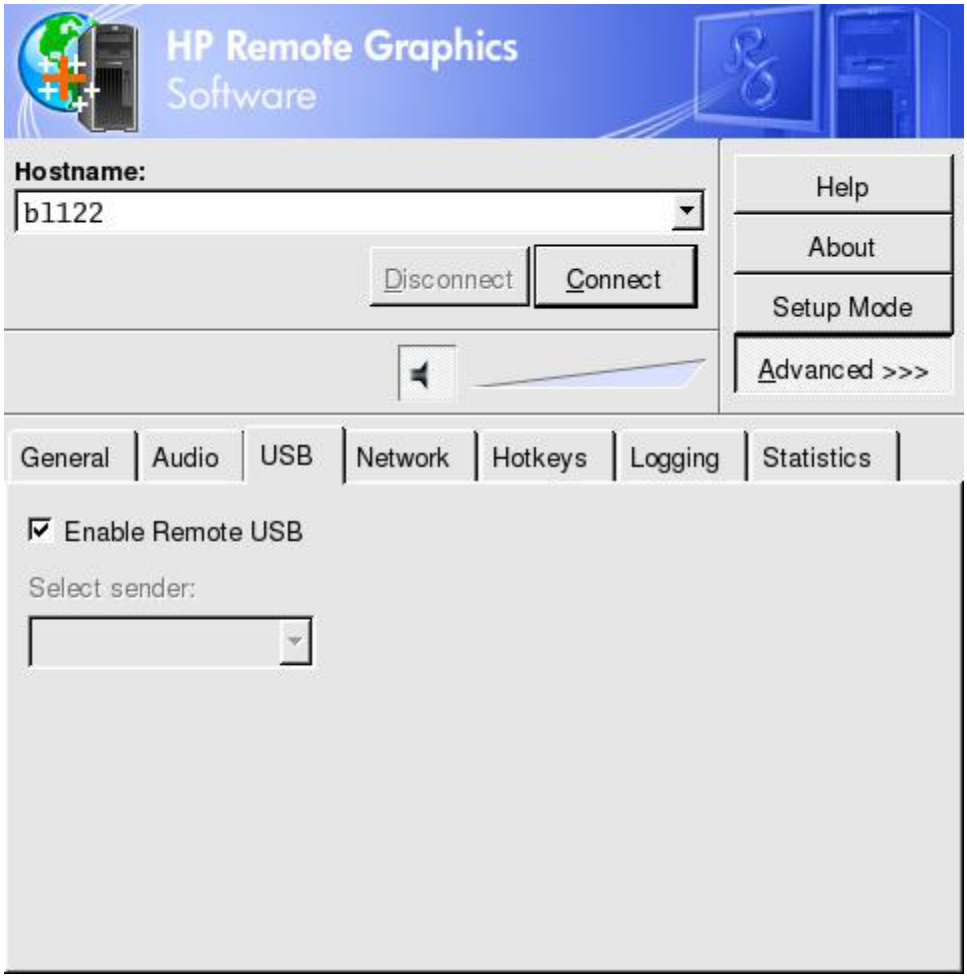
- High specifies a sampling rate of 44 KHz which equivalent to CD quality audio.

Higher quality settings (sampling rates) require more network bandwidth and can impact the performance of HP Remote Graphics especially over bandwidth-constrained networks.

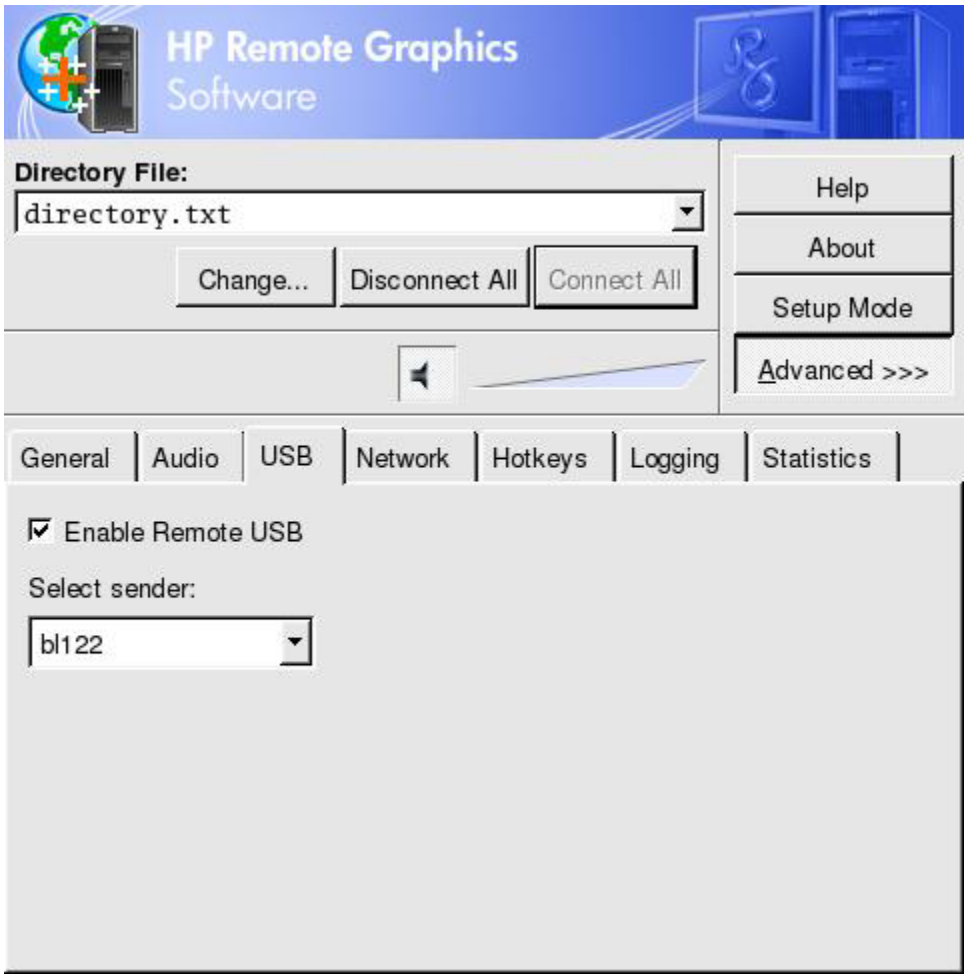
USB Options:

Remote USB is only supported on a HP Blade Workstation Client and a HP Blade Workstation sender. See System Requirements for further details.

HP Remote Graphics Software supports a Remote USB capability. This allows a user to connect any number of USB devices to a local RGS Receiver system and have the devices appear connected to the RGS Sender system.



The toggle button labeled Enable Remote USB selectively enables or disables Remote USB capability. When enabled, USB devices plugged into the local system appear to the remote system as locally attached devices. Remote USB can dynamically enable or disable USB connections while connected to a Sender system. Remote USB supports hotplug events, so it is not necessary to disable Remote USB before plugging or unplugging USB devices.



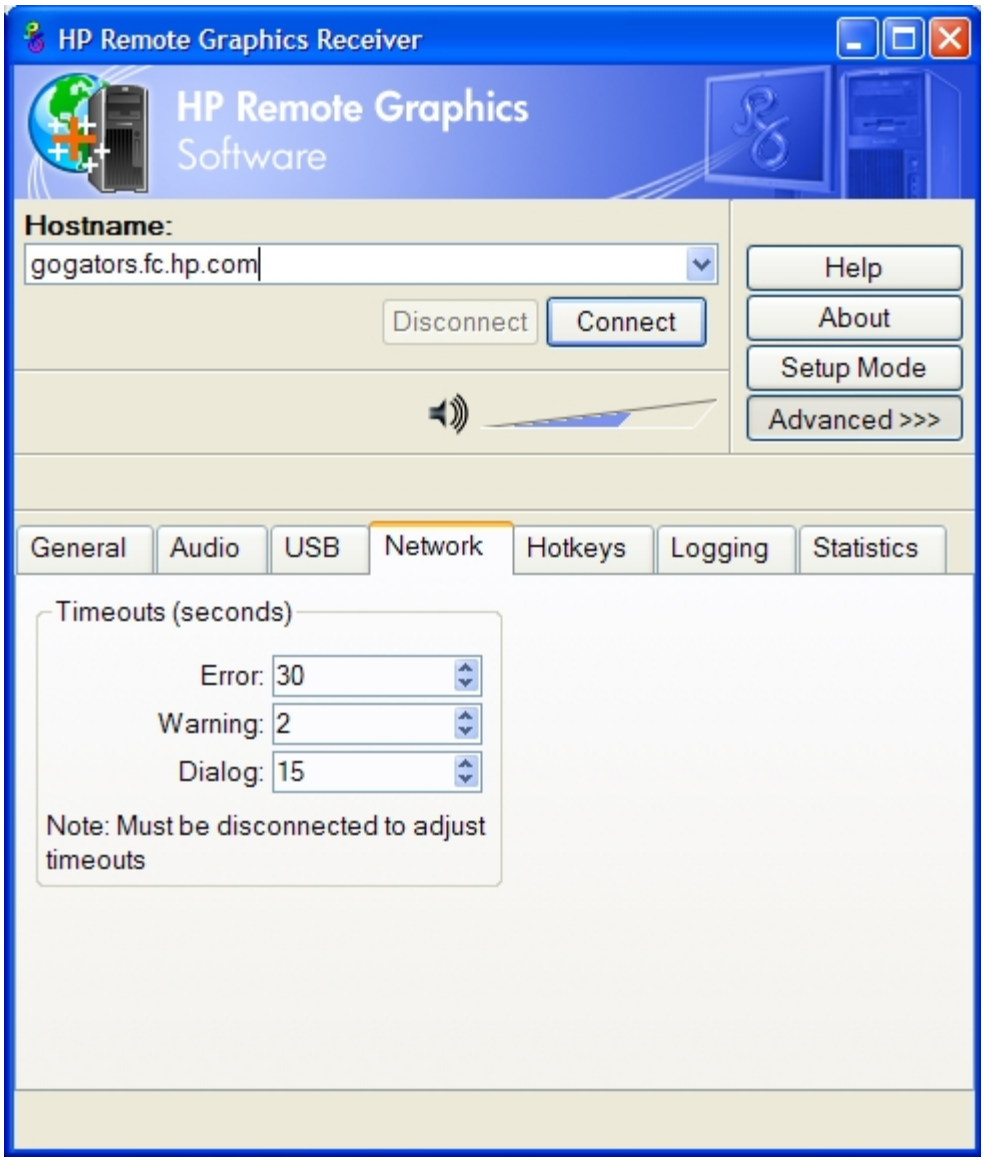
When the Receiver uses Directory Mode or Enterprise Service Mode with multiple Senders specified, the `Select sender` drop down box manages which system receives the active Remote USB connection. The example above shows a RGS Receiver setup for directory mode using the Directory File "`directory.txt`" and the system `bl122` selected for Remote USB devices at the next connection.

NOTE: In Directory Mode or Enterprise Service Mode, Remote USB requires selection of one Sender system before connecting to any systems. Remote USB can only be enabled to one Sender at a time. During an active connection, if users want to change their Remote USB devices to another Sender system, they must

1. disconnect all systems using the "Disconnect All" button
2. use the "Select sender" box to select a new Remote USB system
3. reconnect to their remote systems using the "Connect All" button.

During device discovery, the new sender system will report the USB connection as a hotplug event for the Remote USB devices.

Network Options:



The network timeouts control various timeouts that may occur within HP Remote Graphics.

- Error: Specifies the timeout in seconds used to detect and disconnect an inactive connection.
- Warning: Specifies the timeout in seconds used to detect and notify the user of a potential network disruption. If network connectivity is restored before reaching the error timeout, the warning notification disappears and the user can continue often without interruption.
- Dialog: Specifies the timeout in seconds used to display and wait for input dialog responses from input, such as the authorization or PAM authentication dialogs.

The Receiver must be disconnected from all Senders to change timeouts. See Using Timeouts for a detailed discussion on setting timeouts.

Hotkeys Options:

Ctrl-Alt-End Hotkey: On some platforms the local host operating-system intercepts the Ctrl-Alt-Delete key sequence and does not forward it to the Receiver. For example, on a Windows system Ctrl-Alt-Del displays a dialog box instead of sending the sequence to the Receiver. With this option checked, the Receiver recognizes Ctrl-Alt-End as a signal to send a Ctrl-Alt-Delete sequence directly to the Sender. The Ctrl-Alt-Delete sequence is also available via the Remote Display Window Toolbar.

Send First Key: The Receiver filters keystrokes and does not send hotkey sequences to the Sender. For example, the default setup mode hotkey consists of a shift press, space press, and space release. When the Receiver sees a shift key press, the event does not pass immediately through to the Sender. The Receiver holds the event to determine if the next keystroke forms a hotkey sequence. If the next key pressed is not space, the Receiver immediately forwards all events to the Sender.

Some applications require the first key press event to arrive separately from subsequent events to function properly. If this is the case, check the 'Send First Key' option to immediately pass the first key in a hotkey sequence.

Setup Mode Hotkey: While in a Remote Display Window, the remote desktop can sometimes completely cover and hide your local desktop. If you need access to your local desktop or Receiver, use the Setup Mode Hotkey to expose them. See Setup Mode documentation for more information on other options available in Setup Mode.

By default, to access Setup Mode:

- Press and hold down the Shift key.
- At the same time, press then release the space bar to activate Setup Mode.

You will remain in Setup Mode until you release the Shift key.

Pressing the Set button on the GUI begins redefinition of the Setup Mode Hotkey sequence. Typing any combinations of Ctrl, Alt, Shift, and Space defines a new sequence. Every sequence must begin with Ctrl, Alt, or Shift, and the first key pressed remains held down through the entire sequence. When the first key is released, the sequence is considered complete. When activating Setup Mode via this hotkey, it remains active until release of the first key in the sequence. Pressing the Reset button on the GUI restores the Setup Mode Hotkey sequence to its original default values.

When defining a hotkey sequence via the GUI, the sequence becomes left-side and right-side sensitive when multiple keys exist. For example, left-side shift key strokes differ from right-side shift key strokes. To define a sequence that is side insensitive, you must modify the property value from outside of the GUI while RGS is not running. See the Hotkeys Properties documentation for information on modifying the sequence from outside of the GUI.

Hotkey definitions are formed by strings of comma-separated word pairs. The first word represents the key while the second represents a specific action for that key. Each pair represents an event token. For example, the default Setup Mode Hotkey sequence is defined by:

- `Shift Down, Space Down, Space Up`

The valid words for the keys are:

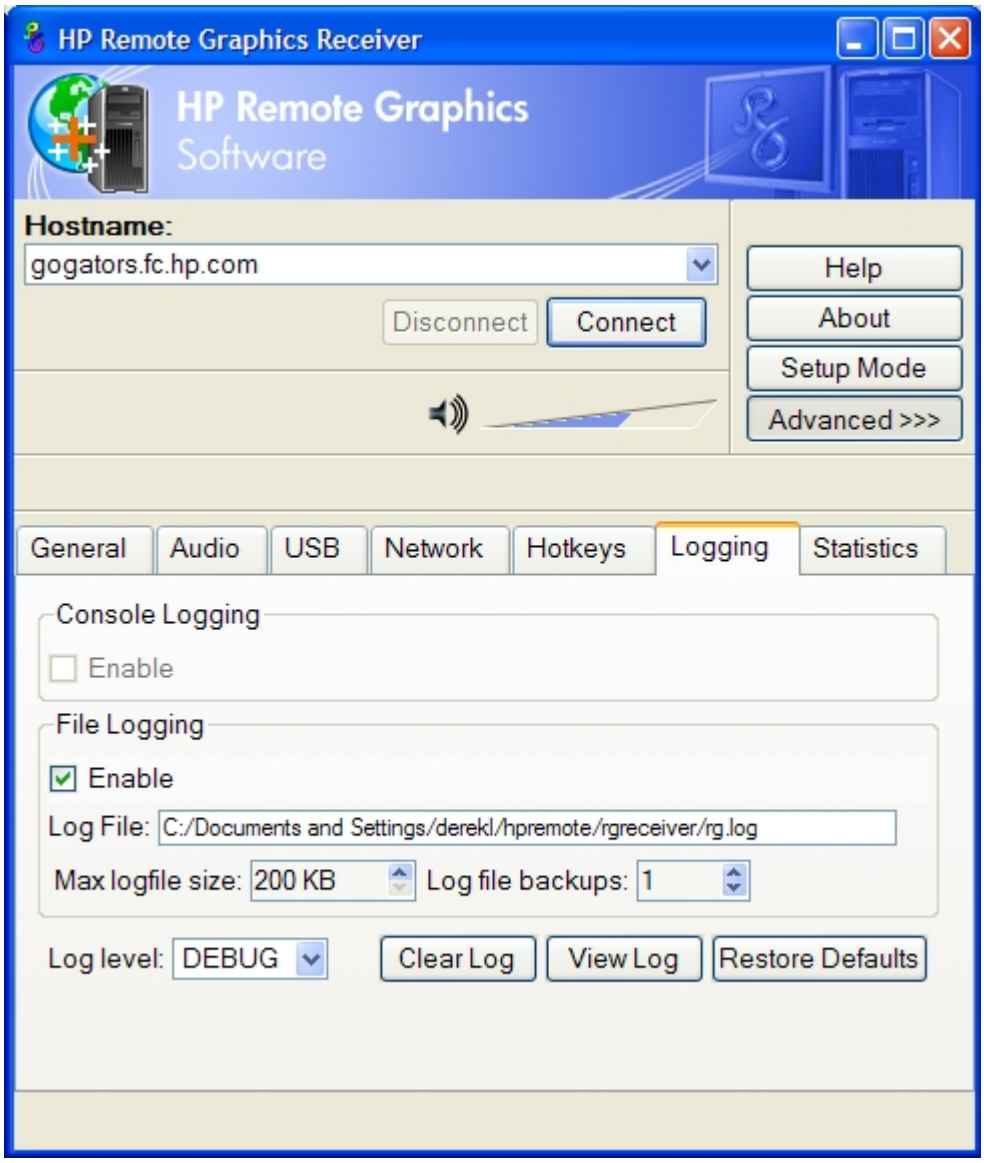
- `LCtrl, RCtrl, Ctrl`: Specifies a left, right or side insensitive ctrl key, respectively.
- `LAlt, RAlt, Alt`: Specifies a left, right or side insensitive alt key, respectively.
- `LShift, RShift, Shift`: Specifies a left, right or side insensitive shift key, respectively.
- `Space`: To specify a space key.

The valid words for the actions are:

- `Down`: Specifies a key press.

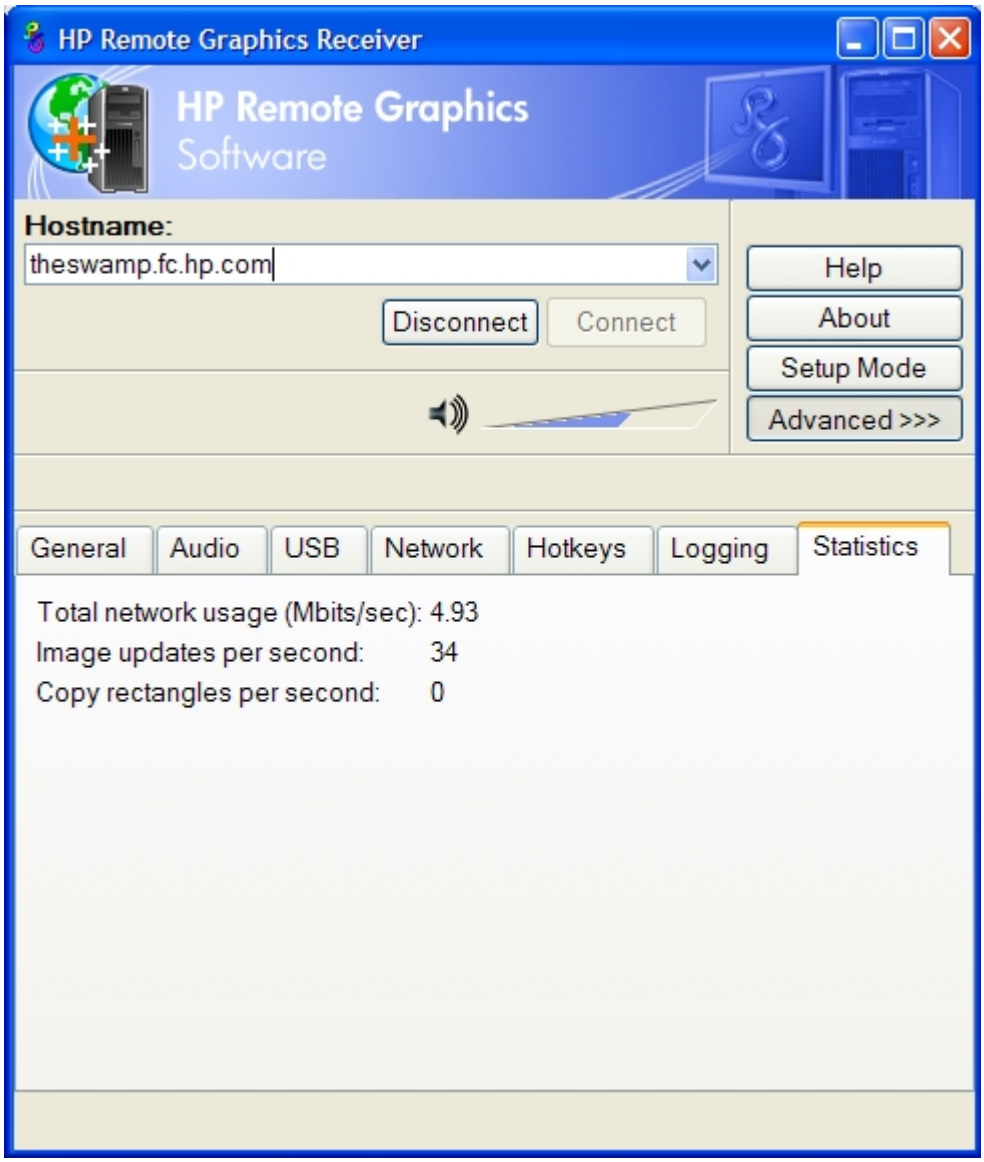
- Up: Specifies a key release.

Logging Options:



- Console logging: enables logging to the console (standard output). This option is only available on Linux and HP-UX. It is not supported on Windows.
- File logging: enables logging to the specified file. The spinboxes for Max logfile size and Log file backups limit the maximum logfile size and the number of backup logfiles respectively.
- Log level: determines the type and amount of information logged.
- Clear Log: clears the contents of the log file.
- View Log: displays the contents of the log file in a window.
- Restore Defaults: resets all logging settings to default values.

Statistics Options:



The statistics tab displays aggregate data for all connected sessions.

- Total network usage: The combined network bandwidth received from all remote systems per second.
- Image updates per second: The combined number of image updates per second received from all connections.
- Copy rectangles per second: The combined number of copy updates per second received from all connections.

Remote Display Window Toolbar:

The Remote Display Window toolbar contains controls and information for the session. The toolbar is made visible by entering Setup Mode (using the key

sequence defined in the Hotkeys tab) and then pressing the "H" key. The toolbar window appears at the top of the Remote Display Window:

The toolbar displays the following controls and information:

- hostname: the hostname of the remote Sender
- disconnect button: disconnects the current session
- CTRL-ALT-DEL button: sends the CTRL-ALT-DEL key sequence to the Sender. Some key-sequences, such as `Ctrl-Alt-Del`, are trapped by the local system and therefore do not forward to the remote system using normal methods. The user cannot send a `Ctrl-Alt-Del` key sequence using a keyboard on the Receiver. The `Ctrl-Alt-Del` button in the toolbar sends this key sequence to the Sender.
- Borders button: adds or removes window borders and decorations to the Remote Display Window.
- Snap button: when selected, this option causes the Remote Display Window to snap to the edges of the screen whenever the boundaries of the window are within 10 pixels of the edge of the screen.
- Image quality slider: sets the compression level. Higher settings require greater bandwidth.
- Network bandwidth: displays the current network bandwidth received by this session.
- Image update rate: displays the number of image updates per second received by this session.

Setup Mode

The RGS Receiver enters Setup Mode via a hotkey sequence or button in the Receiver Control Panel. See the hotkeys documentation for more information on accessing Setup Mode with a standard PC keyboard. Note that within a Remote Display Window, the Setup Mode Hotkey may sometimes be the only way to access your local desktop.

When Setup Mode is active, the Receiver captures and interprets all keystrokes and mouse events on your local computer. No mouse or keyboard events pass to the Sender.

In Setup Mode, you can:

- Easily move and resize Remote Display Windows - Use the left mouse button in any Remote Display Window to drag or resize the window on the desktop.
- Show the Receiver Control Panel - Press M to show the control panel.
- Show or hide the Receiver Toolbar - Press H to show or hide the toolbar.
- Activate the Remote Display Window selection dialog – Press TAB to display the dialog

  The Remote Display Window selection dialog allows the user to quickly navigate between multiple active connections. The dialog displays a thumbnail representing each Remote Display Window. Display the dialog by pressing TAB while in Setup Mode. The dialog remains active while the initial Setup Mode hotkey is depressed. Releasing the initial Setup Mode key closes the selection dialog and switches focus to the selected Remote Display Window. The currently selected Remote Display Window is highlighted with a red border.

  While the Remote Display Window selection dialog is active, navigate between windows by:

  - Pressing TAB to select the next window.
  - Pressing the numeric key displayed beneath the thumbnail.
  - Clicking the mouse on a thumbnail.
  - Double clicking the mouse on a thumbnail (this will also immediately close the selection dialog).

  To directly switch to a window without activating the selection dialog, simply press the number that corresponds to the identifier of the window (the same identifier displayed in the dialog).

Directory Mode

Starting the Receiver in Directory Mode

When the Receiver starts in Directory Mode the Receiver looks up the name and location of a directory file containing the names of users and their assigned systems.

The Receiver reads this file to identify the systems assigned to the current user and attempts to automatically connect to them. The directory file may contain multiple users with a list of Senders assigned to each user.

The first time the Receiver starts in Directory Mode, if the command line (`-directory "filename"`) specifies a filename the Receiver will use that file as the directory. If no file name is specified, the user is prompted to select the location and name of the directory file.

After the location of the directory file is set, the Receiver automatically connects to the Senders assigned to the user specified in the file. The locations of the directory file can be reset using the Receiver control panel.

Configuring a directory file for Directory Mode

When the Receiver runs in Directory Mode, it requires a properly configured directory file. Normally, the directory file is a common file for an entire group, department, organization, or entire company. The directory file can manage and administer the assignment of systems for any number of users. This file is specified as a normal ASCII text file as follows:

```
domainName userName1 sender1 sender2 ... senderN

domainName userName2 sender1 sender2 ... senderN
```

For example, the following text specifies the directory for the users Sally and Joe.

```
Domain1 sally sender1 sender2 sender3

Domain1 joe sender4 sender5 sender6
```

In this example:

- Sally is assigned sender1, sender2, and sender3
- Joe is assigned sender4, sender5, sender6

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

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

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

When using the directory file for users on either Linux or HP-UX systems, the "domain name" does not apply. Simply use the keyword "UNIX" in place of the domain name. For example:

```
UNIX  sally  sender1   sender2   sender3
```

Save the directory file on a readily accessible network file share or mapped drive so that each Receiver can read the file at start-up.

Organizing Displays

Directory Mode is usually intended for a system with multiple displays attached. For example, if the Receiver connects to two Senders, then at least two displays should be available on the local system. Each Sender can then display on its own monitor.

The Receiver allows the user to easily move and position the Remote Display Window on the local desktop using Setup Mode. For optimal viewing the display resolution of the Sender and Receiver should be set to the same values. If the resolution of the display connected to the local system is less than display resolution of the remote system, the image will be cropped by the local display.

Enterprise Service Mode

Using the Enterprise Service

The Enterprise Service (ES) supports assignment of systems to users and management of user settings and properties through a standard network service. The advantages of the Enterprise Service over using Directory Mode are:

- Using a network service, a centralized database or enterprise directory infrastructure can store systems assigned to a user. A service can support dynamic and complex business logic for system assignment.
- Users authenticate against the Enterprise Service.
- The Receiver can also read and write the user's properties.

The Enterprise Service comes as a Software Development Kit (SDK). Developers use the SDK to adapt and customize their required enterprise solution. Consequently, the ES SDK does not directly implement the specific functionality required for assigning and looking up user systems and settings. For example, the SDK does not provide ready-to-use Active Directory or LDAP integration itself. The SDK provides the ICE interfaces and a sample implementation written in Python. ICE (Internet Communications Engine - see http://www.zeroc.com/ice.html) is a modern alternative to object middleware such as CORBA™ or COM/DCOM/COM+, with support for C++, Java, Python, PHP, C# and Visual Basic.

The sample implementation demonstrates a simple XML file as the enterprise directory. Associated with the XML is a DTD that specifies a precise and legal set of XML elements and attributes that represent syntax to specify the user to machine mappings as well as the user RGS Properties. This sample implementation can be used to test the Enterprise Service and become familiar with its capabilities. Simply add a set of test users and user settings to the XML file, start the Enterprise Service, and connect to RGS Senders from a RGS Receiver using the service. After the sample is working, the job of creating an implementation that interacts with a customers enterprise directory can begin.

To learn more about the SDK, review the README.txt file in the ES installation. It explains the purpose and usage of each file in the installation.

Starting the RGS Receiver in Enterprise Service mode

When the RGS Receiver starts in Enterprise Service Mode using the command line option -esdir, the Receiver connects to the Enterprise Service. The user will then authenticate with the ES.

After the user authenticates, the Receier reads from the Enterprise Service a list of systems assigned to the user and specified by hostname or ipadress. The Receiver will try to connect to the specified systems.

If the command line option also specifies option `-esdirsettings`, the Receiver gets the properties that the Receiver should use from the ES. The properties specify

settings such as the location of each Remote Display Window on the local desktop, codec quality settings, audio settings, and others. See Properties for more details.

If the command line options `-esdirsettings` is not specified, then the users settings are read from the local system. When the Receiver closes, the users settings are saved, either locally or remotely in the Enterprise Service, depending on the specification of the command line option `-esdirsettings`.

When a connection to each of the RGS Senders is initiated, the credentials gathered during the ES authentication are used to authenticate the connection. If "`Prompt for username and password`" is enabled in the Receiver Control Panel, then the credentials used to authenticate with the ES are not used and the user is prompted to enter credentials for each connection.

Organizing Displays in Enterprise Service Mode

Refer to "Organizing Displays in Directory Mode" section.

Starting the Enterprise Service

To run the sample Enterprise Service, the system must have Python 2.4 installed. See Installing the Enterprise Service for more information.

Once Python is installed, the user starts the ES as follows:

From the command line:

```
python C:\Program Files\Hewlett-Packard\Remote Graphics Enterprise
Service\HprEsPrivate.py
```

From the Start menu, select:

```
Start --> Hp Remote Graphics --> Start Enterprise Service
```

Configuring the Enterprise Service

As mentioned before, the current SDK provides a sample implementation using a simple XML file as an enterprise directory. This is only a sample to learn how the Enterprise Service operates. It is up to the customer to implement the ES interfaces, by providing an implementation that communicates with their enterprise infrastructure.

The README.txt file in the ES installation can help learn how to use the SDK. The current ES is written in the Python language. Python is an interpreted object-oriented (OO) language well suited for this problem and readily available on a wide variety of platforms. All of the Python code is human readable and can be used to understand the workings of the ES.

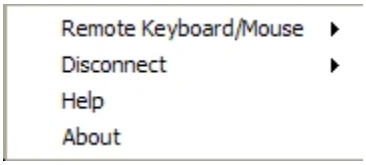
Using the Sender

Controlling Sender Settings:

Controlling Settings on Microsoft Windows

Sender GUI

The Sender for Windows registers an HP Remote Graphics Software icon in the application tray. On Windows the icon animates when Receivers are connected to the Sender. By right clicking on the icon, the user can display the Sender GUI



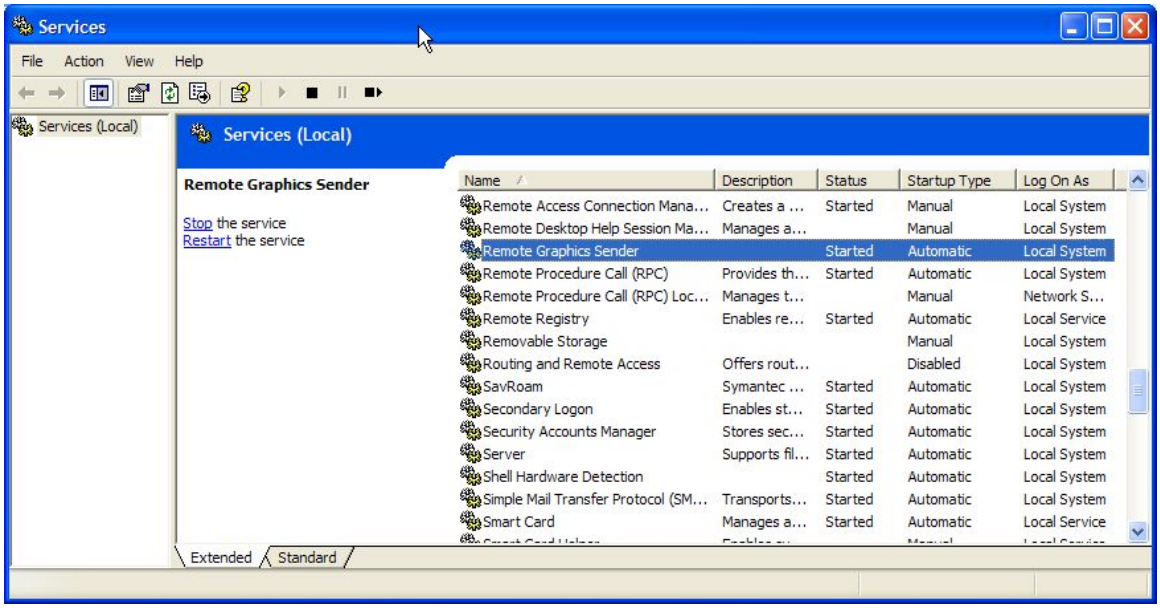
and select one of the following options:

- "Remote Keyboard/Mouse --> Enable or Disable" - If "Disable" is selected, all non-primary users are in "view-only" mode. Only the primary user, the user that is logged into the desktop, will control the remote desktop remotely using the Receiver. If "Enable" is selected, all users connected to the Sender can interact with the remote desktop. All keyboard and mouse activity will be injected into the Sender allowing non-primary users control of the remote desktop.
- "Disconnect --> Non-Primary Users or All Users" – disconnects receiver sessions for either non-primary users or all users.
- "Help" displays the Remote Graphics Help system.
- "About" displays Remote Graphics program information.

Manually Starting & Stopping the Sender

By default the Sender installs as a Windows Service and configures to automatically start on system startup. The user can control Windows Services by accessing the "Services" panel. The "Services" panel can be accessed from the Windows "Control Panel" and selecting "Administrative Tools".

The following diagram shows the Administrative Tool for Services. The Remote Graphics Sender is highlighted. The status of the service is "started" and the service is configured to startup automatically. By right clicking on the Sender, the service can be stopped, started, or resumed. Additionally, the properties of the service can be controlled such as the start-up type, and the recovery mode.



Controlling Settings on Linux and HP-UX

Sender GUI

By default, the Sender GUI automatically starts on Linux and HP-UX when the Sender process starts. The Sender GUI displays with the HP Remote Graphics Software icon on the desktop. By right clicking on the icon, the user can select one of the following options:

- "Remote Keyboard/Mouse --> Enable or Disable" - If "Disable" is selected, all non-primary (A user of a RGS connection that does not match the user logged into the desktop of the remote computer. If no one is logged into the desktop of the remote computer, then all connections are non-primary.) users are in "view-only" mode. Only the primary user, the user that is logged into the desktop, will control the remote desktop remotely using the Receiver. If "Enable" is selected, all users connected to the Sender can interact with the remote desktop. All keyboard and mouse activity will be injected into the Sender allowing non-primary users control of the remote desktop.
- "Disconnect --> Non-primary Users or All Users" – disconnects receiver sessions for either non-primary users or all users.
- "Help" displays the Remote Graphics Help system.
- "About" displays Remote Graphics program information.

It is possible to disable the GUI from automatically starting. See Installing the Sender for more details.

Starting & Stopping

The Remote Graphics Software Sender on UNIX automatically starts when the X server on the system starts. Starting the Sender process in any other way is not supported. Typing the following command in a terminal emulator will show the Sender's process information:

```
ps -ef | grep rgsender
```

If multiple X servers are running on the system, there will be one Sender running for each X server.

If the Sender process is stopped or killed, the X server will attempt to restart the Sender. When the X server is shutdown, the Sender will also stop running. If the X server is recycled, the Sender process is stopped and a new Sender is started.

If for some reason the X server cannot start, and a Sender process is running, killing the Sender will allow the X server to restart.

Setting the Windows Sender Process Priority

This section describes how to adjust the process priority of the Windows Sender. The default process priority of the Windows Sender is normal. Under some situations, however, increasing the process priority of the Windows Sender may improve interactivity. In some cases, the Windows operating system scheduling algorithms do not give the RGS Sender sufficient CPU time to maintain smooth interactivity. Erratic updates from a Windows Sender can sometimes result from a process load and scheduling situation. (Networking performance can also contribute to poor interactivity.)

RGS Sender for Windows on some laptops has exhibited erratic behavior. Increasing the Sender priority to high usually improves interactivity in this case. This enables the Sender more frequent access to the CPU and improve updates to the Receiver.

Process priority for the Sender is command-line accessible for the Windows Sender. Four command-line options are available: `-belownormal`, `-normal`, `-abovenormal`, or `-high`. Priorities low and realtime cannot be selected for the Windows Sender. Please see Command Line Options for further information.

Currently, there are two ways of setting the process priority for a Windows Sender:

- using `regedit` to modify the rgsender service start up parameters in the Windows Registry
- using HP Performance Tuning Framework (PTF) to configure Windows Sender priority (available only on HP Workstations)

Both methods are covered below.

WARNING: Adjusting the process priority of the sender to a level higher than `-normal` can cause other normally privileged processes to get fewer CPU cycles than usual. Please adjust the priority of the sender with caution.

Setting the Sender process priority using regedit

This section describes how to use the Windows `regedit` command to increase the process priority of the Sender service when it starts. Under normal operation the Windows Sender runs as a Windows Service. When the system starts up, the installed services are usually started. When the RGS Sender is installed an entry is added in the Windows Registry for the Remote Graphics Sender service. `regedit` can be used to modify the command line that is used for starting the Sender service:

1. `Start regedit` - this can be done by opening a Windows command prompt and executing the command “regedit” or using the "run" command line from the Start menu
2. Using `regedit` navigate to the key

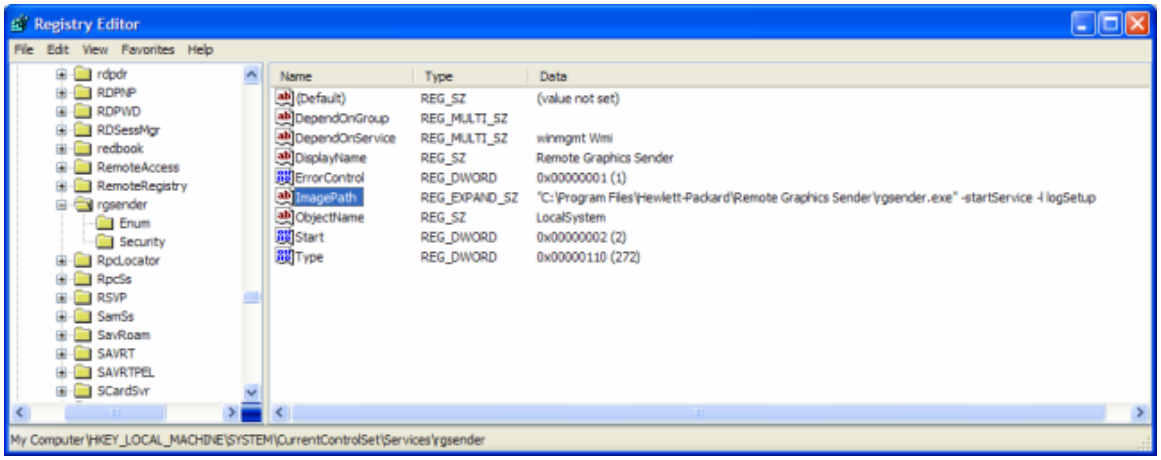
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\rgsender`

3. Add the desired process priority command-line option for starting the Remote Graphics Sender service. For example, to increase the process priority to high add the “-high” option to the key “ImagePath” as follows:

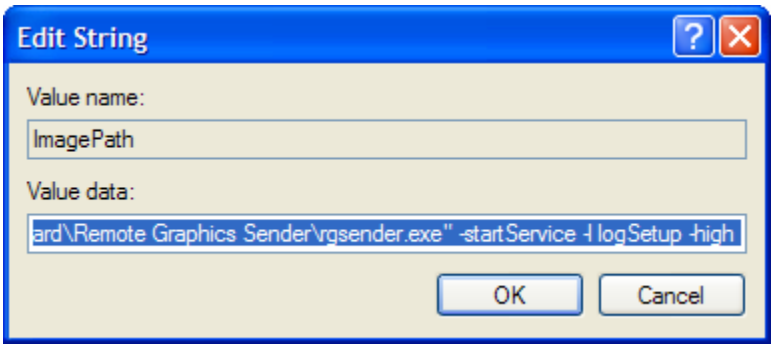
```
"C:\Program Files\Hewlett-Packard\Remote Graphics
Sender\rgsender.exe" -startService -l logSetup –high"
```

4. Restart the Sender service with the new option. This can be done using the Windows Service Control Manager or re-starting the system.

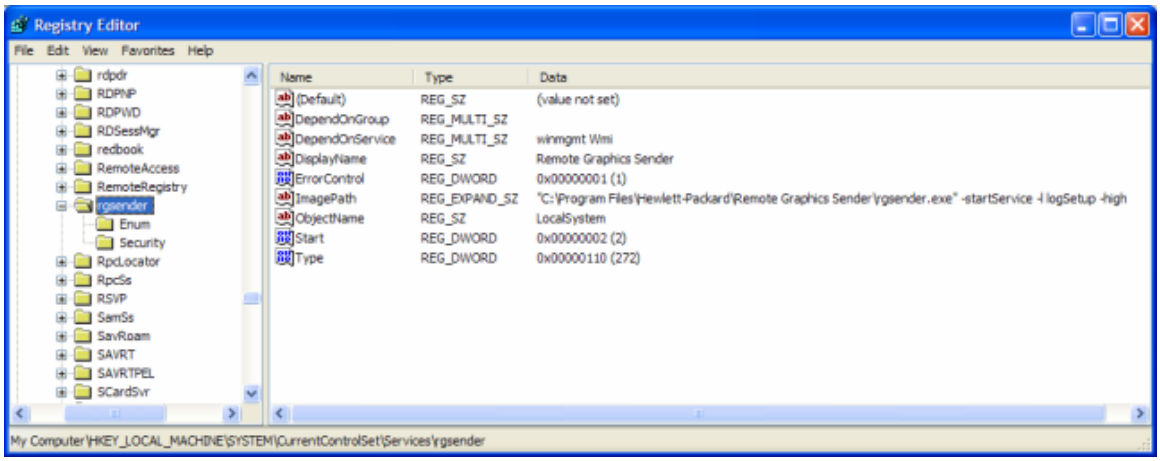
Regedit should look like this prior to making any changes.



Double-clicking on the “ImagePath” key should bring up the following dialog which allows the user to edit the value. The screen-shot shows the “-high” option already added.



After the changes are made the registry should look like this



Note the addition of the "`-high`" command line option to the end of the command-line.

Setting the Sender process priority using PTF

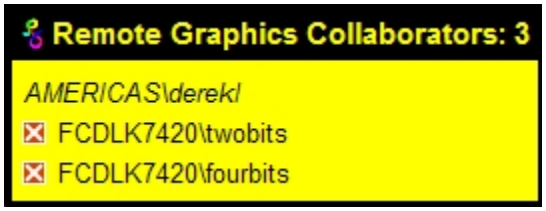
The HP Performance Tuning Framework (PTF) can adjust the priority of the Sender without having to use regedit. PTF is available for HP Workstations only from this location:

`http://www.hp.com/workstations/software/framework/index.html`

Please see the PTF help and documentation for further information.

Collaboration Notification

The Remote Graphics Sender for Windows displays a notification dialog when non-primary users are connected. The dialog displays a list of domain\usernames representing each user connected to the Sender:



Two types of connections to a Sender are possible, primary and non-primary. A primary connection is one where the login credentials match those of the user logged into the desktop of the Sender system. A non-primary connection is defined as any connection to the Sender with a login other than the primary. Within the collaboration notification dialog, primary and non-primary users are identified using different fonts. Primary users are italicized and listed first. Non-primary usernames follow and are displayed using a normal font. The example screen-shot above shows two connections are active, one a primary user and the other a non-primary. A small button with an “X” is displayed next to all non-primary usernames. Pressing this button disconnects the corresponding non-primary user. All non-primary users may be disconnected with a single command using the Sender GUI as described in Controlling Sender Settings.

When the collaboration notification dialog is displayed, it indicates that there are multiple connections to the remote desktop. The collaboration notification dialog cannot be dismissed. It is possible to move the dialog within the boundaries of the desktop by clicking anywhere within the dialog and dragging it. The Sender removes the dialog when all non-primary connections terminate.

Command Line Options

This section describes the options that can be specified on the command line of the Receiver and Sender. In addition, many properties can also be set on the command line.

RGS Receiver Command Line Options

The Windows Receiver (`rgreceiver.exe`) or the Linux/HP-UX Receiver (`rgreceiver.sh`) command line options are:

[-directory [file] | -esdir serv1 [serv2 ... servN [-esdirsettings]]]

[-nosplash]

[-v | -ver | -version]

[-h | -help | -?]

`-directory [file]` starts the Receiver in -directory mode. If the optional "file" file path is specified, then the file is opened and used to lookup systems assigned to the user. If the "file" is not specified, the user is prompted to enter a path to the directory file. See Starting the Receiver in Directory Mode for more details.

`-esdir serv1 [serv2 ... servN]` starts the Receiver in enterprise service mode using service 1 and service 2 through service N where serv1, serv2, and servN are the hostnames or ipaddresses of the enterprise service. Setting the –esdir option allows the Remote Graphics Software Receiver to lookup the systems assigned to the user using a RGS Enterprise Service. See Using The Enterprise Service for more details.

`-esdirsettings` enables the Receiver to get and set the Receiver settings from the enterprise service. If this option is used, -esdir must also be set.

`-nosplash` disables display of the splash screen when the Receiver starts.

`[-v | -ver | -version]` prints the Receiver's version information.

`[-h | -help | -?]` prints a listing of the various command line options, those that are listed on this page.

RGS Sender Command Line Options

The Windows Sender (rgsender.exe) or the Linux/HP-UX Sender (rgsender.sh) command line options are:

[-nocollab]

[-timeout value]

[-authtimeout value]

[-l logSetupFile]

[-v | -ver | -version]

[-h | -help | -?]

[-installService | -startService | -uninstallService]

[-belownormal | -normal | -abovenormal | -high]

[-noautostartgui]

[-display value]

Under normal operation the Windows Sender runs as a Windows Service. When the system starts up, the installed services are usually started. When the RGS Sender is installed an entry is added in the Windows Registry for the Remote Graphics Sender service. `regedit` can be used to modify the command line that is used for starting the Sender service:

1. `Start regedit` - this can be done by opening a Windows command prompt and executing the command “regedit” or using the "run" command line from the Start menu
2. Using `regedit` navigate to the key

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\rgsender
   ```

3. Add the desired process priority command-line option for starting the Remote Graphics Sender service. For example, to increase the process priority to high add the “-high” option to the key “ImagePath” as follows:

   ```
   "C:\Program Files\Hewlett-Packard\Remote Graphics
   Sender\rgsender.exe" -startService -l logSetup –high"
   ```

4. Restart the Sender service with the new option. This can be done using the Windows Service Control Manager or re-starting the system.

On HP-UX and Linux the Sender is started by the X Server. The file `rgsender.sh` can be edited to set the command line options.

Platform independent command line options

The following options are available on all platforms.

`-nocollab` Disables collaboration. When specified, only the primary user can connect to the Sender.

`-timeout value`The timeout in milliseconds used to detect and disconnect an inactive connection. This option sets the property “Rgsender.Network.Timeout.Error.” See Using Timeouts for more details.

`-authtimeout value`The timeout in milliseconds used to detect and notify the user of a network disruption. This option sets the property “Rgsender.Network.Timeout.Dialog.” See Using Timeouts for more details.

-l logSetupFile Specifies the "logSetupFile" file used to describe various logging parameters for Sender's error and informational output. Use this file to determine where the output goes (to a file or to standard error) as well as the type of output logged (INFO or DEBUG). At installation, the Sender default is with "-l logSetup"

turned on, where the logSetup file in the installation directory is set for output to a file named rg.log at INFO debug level.

[-v | -ver | -version] prints the Senders's version information.

[-h | -help | -?] prints a listing of the various command line options, those that are listed on this page.

Windows specific command line options

The following options are only available on Windows.

-installService Installs the “Remote Graphics Sender” service.

-startService Starts the “Remote Graphics Sender” service. The Sender must be installed as a service first.

-uninstallService Uninstalls the “Remote Graphics Sender” service.

-belownormal Sets the process priority of the Sender to below normal.

-normal Sets the process priority of the Sender to normal. This is the default priority.

-abovenormal Sets the process priority of the Sender to above normal.

-high Sets the process priority of the Sender to high.

Linux/HP-UX specific command line options

The following options are only available on Linux and HP-UX.

-noautostartgui The RGS Sender GUI automatically starts on Linux when the Sender process starts. To start the GUI on a per-user basis, edit the /opt/hpremote/rgsender/rgsender.sh file, and add the -noautostartgui option. Refer to the Linux Sender GUI Installation or HP-UX Sender GUI Installation sections for more information.

-display value where value is the display number of the X server that the RGS Sender will share. For example, if both X servers hostname:0 and hostname:1 are running, use -display 1 to share the X server running at display hostname:1.

Properties

Remote Graphics Software has a configuration mechanism that allows specifying many controls. This configuration mechanism is called Properties. Properties are name/value pairs. Properties are created with default values and can enable or disable window borders, set the codec quality, set the audio quality, adjust the connection timeouts, etc.

Properties are set in a configuration file, on the command line, or using the RGS Enterprise Service. Properties specified on the command line override properties set in a configuration file or RGS Enterprise Service.

Syntax

Properties are name/value pairs and can contain any non whitespace characters except "=" and "#". The property name and property value are separated by an "=". For example:

```
Rgreceiver.Network.Timeout.Warning=10
```

The name of this property is `Rgreceiver.Network.Timeout.Warning`, and the value of the property is `10`.

All RGS Receiver properties begin with "`Rgreceiver`". All RGS Sender properties begin with "`Rgsender`". Property values cannot contain the "`=`" or "`#`" characters.

Properties can contain values of the following types: `string`, `int`, `bool`, `string vector` and `int vector`. Properties of type `bool` are set to either "1" or "0" - representing `true` or `false`.

Any property set to an empty value,

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

initializes as follows: if the value of the property is of type STRING, the value will be set to an empty string. If the value of the property is of type INT or BOOL, the value will be set to "0". This can be used to initialize properties in a configuration file or on the command line.

Configuration Files

All RGS properties can be set in a configuration file. The RGS Receiver uses a file named `rgreceiverconfig` to read for its properties. The RGS Sender uses a file named `rgsenderconfig` to read for its properties. On Windows these files are installed in the directory where RGS is installed. On Linux and HP-UX these files are installed in `/etc/opt/hpremote/rgreceiver` and `/opt/opt/hpremote/rgsender` respectively.

The configuration files contain properties (name/value pairs) with only one property per line. Empty lines (containing only whitespace characters) 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.

Setting Properties on the Command Line

In addition to setting properties in a configuration file, properties can be set on the command line. Properties entered on the command line override all properties set in a configuration file. All properties must begin with a "-" on the command line to be recognized as a valid property. For example:

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

will starts the RGS Receiver with the `Rgreceiver.Network.Timeout.Warning` property set to 10000 milliseconds. If any property is set more than once on the command line, the value of the last entry is used. There cannot be any whitespace between the property name, the "=" character, and the property value. The following example:

```
rgreceiver.sh -Rgreceiver.IsSnap = 1
```

is invalid, due to the whitespace on either side of the "=" character.

Properties of type `string vector` and `int vector` cannot be set on the command line.

RGS Receiver Properties

All of the following properties are used by the RGS Receiver, and available on the command line or using the RGS Receiver property configuration file (rgreceiverconfig).

All RGS Receiver properties are automatically saved away in a "Properties Archive" when the receiver exits. They are used again with the next invocation of the receiver.

General Properties:

`Rgreceiver.IsBordersEnabled=bool`

If set to "1", the borders on the Remote Display Window will be enabled. If set to "0" the borders will be removed creating a borderless windows to display the remote session. The default value is "1" - borders are on.

`Rgreceiver.IsSnapEnabled=bool`

If set to "1", as the Remote Display Window is being positioned on the display, the window will snap to the edge of the screen when top edge of the window moves within 10 pixels of the top of the display, or when the left edge of the window moves within 10 pixels of the left edge of the display. The default value is "1" - snap is on.

`Rgreceiver.IsAlwaysPromptCredentialsEnabled=bool`

If set to "1", when connecting to an RGS Sender, the user will always be prompted for the domain, username and password. There will be no attempt to automatically

verify the users credentials. The default value is "0" - prompting for credentials is off.

Rgreceiver.Directory=string

Used to set the name and location of the directory to use for determining the Sender systems that are assigned to the current user. This property is only used then the RGS Receiver is in Directory Mode. The default value is "*directory.txt".*

Rgreceiver.ConnectionWarningColor=string

This is the color the Remote Display Window will be composited with when the RGS Receiver detects a network disruption. The value is a hexadecimal number, with four components (alpha, red, green, blue). The alpha component is used to specify the level of transparency the color will take. An alpha value of zero will be totally transparent, where no warning color will be visible by the user. An alpha value of one will be totally opaque, completely covering the image in the remote sender.

The default value is "0x80b40000". The alpha component is 0x80 (128 decimal). The red component is 0xb4 (180 decimal). The blue and green components are both zero. Therefore, the color is a red of strength 180/256, or around 70% of full red. The alpha value is 128/256, or 50% transparent.

Rgreceiver.IsGlobalImageUpdateMutable=bool

If set to "1", the user will be able to modify the Enable global image updates check box in the Receiver Control Panel. If set to "0", the user will be unable to modify the checkbox. This property can be used to permanently enable or disable global image updates in the Receiver. The default value is "1" - global image updates can be configured by the user.

Rgreceiver.IsGlobalImageUpdateEnabled=bool

If set to "1", the Receiver updates the area of the screen with the extents of all the areas of the screen that have changed. If set to "0", the Receiver updates the screen to just the areas of the screen that have changed - using individual update rectangles. If image updates in the Remote Display Window seem to show image tearing, setting the value to "1", enabling global image updates, might reduce the tearing. Tearing usually occurs on large images that are updated quite frequently, such as a model of a 3D object being rotated in an large window. Setting the value to '"0", disabling global image updates, is usually best for large Remote Display Windows (5120 x 1024 resolution) that display mostly text based applications. The default value is "0" - global image updates are disabled.

Rgreceiver.RecentWindowPositions=int vector

This property can be used to initialize the positions of the Remote Display Windows. The position of each Remote Display Window is controlled by an (xpos,ypox) tuple. The following example contains two tuples, one for each of two Remote Display Windows:

```
Rgreceiver.RecentWindowPositions=0 0 1280 0
```

This property will set the coordinates of the first Remote Display Window to (0,0), and the second Remote Display Window to (1280, 0). In this example, if each Remote Display Window was at resolution 1280x1024, the first window would show up at the far left of the receiver's display, and the second window would be placed right next to the right edge of the first window, making them appear as one large 2560x1024 display.

Audio Properties:

Rgreceiver.Audio.IsMutable=bool

If set to "1", the user will be able to modify all audio controls in the RGS Receiver. If set to "0", none of the controls can be modifed by the user. The default value is "1" - audio can be configured by the user.

This property only applies to the Windows or Linux versions of the RGS Receiver.

Rgreceiver.Audio.IsEnabled=bool

If set to "1", the audio subsystem in RGS will be enabled. If set to "0", all remote audio will be disabled and no network bandwidth will be consumed for remote audio. The default value is "1" - audio is enabled.

This property only applies to the Windows or Linux versions of the RGS Receiver.

Rgreceiver.Audio.IsInStereo=bool

If set to "1", stereo is enabled and both left and right channels are transmitted. The highest quality setting with stereo enabled is equivalent to CD quality audio but consumes more network bandwidth. The default value is "1" - stereo is enabled.

This property only applies to Windows or Linux versions of the RGS Receiver.

Rgreceiver.Audio.IsFollowsFocusEnabled=bool

If set to “1”, enables only the audio stream corresponding to the Remote Display Window that currently has the keyboard focus. The audio stream from all other active connections is disabled. Setting the property to “0” combines the audio from all active connections into a single stream. The default value is “0” – combine audio from all active connections and play in a single stream.

Rgreceiver.Audio.Quality=int

The AudioQuality can be set to low (0), medium (1) or high (2) quality. This property is used to adjust the sample rate of the streaming audio. The lower the sample rate, the less information that is sent over the network thereby reducing the amount of consumed bandwidth. The default value is "1" - medium audio quality.

This property only applies to Windows or Linux versions of the RGS Receiver.

Browser Properties:

`Rgreceiver.Browser.IsMutable=bool`

If set to "1", the name of the browser used to display online help, can be changed by the user in the Receiver Control panel. If set to "0", the name of the browser cannot be changed by the user. This can be used to permanently set the browser to be used before the RGS Receiver is started. This setting only applies to the Linux and HP-UX versions of the RGS Receiver. The default value is "1".

For Window's versions of the RGS Receiver, the default browser that is set in the Windows Registry is used to display the online help.

This property only applies to the Linux or HP-UX versions of the RGS Receiver.

`Rgreceiver.Browser.Name=string`

Use this property to set the name of the browser to be used to display online help. For example, setting `Rgreceiver.Browser.Name=mozilla` will start up the Mozilla browser when the "Help" button is selected in the Receiver Control Panel.

This property only applies to Linux or HP-UX versions of the RGS Receiver.

Hotkeys Properties:

`Rgreceiver.Hotkeys.IsMutable=bool`

If set to "1", all Hotkey settings in the Receiver Control Panel will be able to be changed by the user. If set to "0", none of the settings can be changed by the user. This can be used to permanently enable or disable Hotkey settings before the RGS Receiver is started. The default value is "1" - Hotkeys can be configured by the user.

`Rgreceiver.Hotkeys.SetupModeSequence=string`

Defines the Setup Mode hotkey sequence. The sequence may only consist of Ctrl, Alt, Shift and Space keys. The sequence must also start with either a Ctrl, Alt or Shift key. The first key must also be held down through the entire hotkey sequence. The default value is "`Shift Down, Space Down, Space Up`".

`Rgreceiver.Hotkeys.IsSendCtrlAltEndAsCtrlAltDeleteEnabled=bool`

When enabled a `Ctrl-Alt-End` key sequence in the Remote Display Window is sent to the RGS Sender as a `Ctrl-Alt-Del` key sequence. The default value is "1" - send a `Ctrl-Alt-Del` when the user enters `Ctrl-Alt-End`.

`Rgreceiver.Hotkeys.IsSendFirstKeyInSequenceEnabled=bool`

When enabled the first key in the hotkey sequence is sent to the RGS Sender. The default value is "0" - don't send the first key in the hotkey sequence.

ImageCodec Properties:

`Rgreceiver.ImageCodec.IsMutable=bool`

If set to "1", the image quality can be changed by the user in the Receiver Control Panel. If set to "0", the user cannot change the image quality. This can be used to permanently set the image quality before the RGS Receiver is started. The default value is "1" - image quality can be adjusted by user.

`Rgreceiver.ImageCodec.Quality=int`

The CodecQuality can be set to a value between and including 0 and 100. This property is used to set the quality of the image in the Remote Display Window. A value of 100 is the highest image quality and should be visually lossless. A value of 0 is the lowest image quality. Under most circumstances a value of 65 should be sufficient. Often, lowering the quality will reduce the bandwidth on the network. The default value is 65.

Logging Properties:

`Rgreceiver.Log.IsMutable=bool`

If set to "1", the logging settings in the Receiver Control Panel can be changed by the user. If set to "0", the user will not be able to change any of the logging settings. This can be used to permanently enable or disable logging settings before the RGS Receiver is started. The default value is "1" - logging settings can be changed.

`Rgreceiver.Log.IsFileLoggerEnabled=bool`

If set to "1", logging output from the RGS Receiver will be sent to a file. The default value is "1" - log to a file.

`Rgreceiver.Log.IsConsoleLoggerEnabled=bool`

If set to "1", logging output from the RGS Receiver will be sent to a console window. The RGS Receiver must be started in a console window to see the logging output. The default value is "1" - log to the console.

This property only applies to the Linux and HP-UX versions of the RGS Receiver.

`Rgreceiver.Log.Filename=string`

This is the path to the log file. This will only be used if `RgReceiver.Log.IsFileLoggerEnabled` is set to "1". The default path on Windows is located in the directory where the RGS Receiver is installed, normally `C:/Program Files/Hewlett-Packard/Remote Graphics Receiver/rg.log`. The default path on Linux or HP-UX is `$HOME/.hpremote/rgreceiver/rg.log`.

`Rgreceiver.Log.Level=string`

There are five logging levels: DEBUG, INFO, WARN, ERROR and FATAL. If DEBUG level is chosen, then all level of output from DEBUG to FATAL will be output to the

log file. If WARN level is chosen, then all levels from WARN to FATAL will be output. The default value is INFO - all DEBUG output is turned off.

Rgreceiver.Log.MaxFileSize=int

This sets the maximum size of the log file in kilobytes (Kbytes). The default maximum size is 1024 Kbytes.

Rgreceiver.Log.NumBackupFiles=int

If the log file exceeds its maximum size, the log file will be saved and a new log file will be created. This sets the number of extra files that will be saved. The default number of saved files is five.

Networking Properties:

Rgreceiver.Network.Timeout.IsMutable=bool

If set to "1", the user can modify all network timeout values in the RGS Receiver Control Panel. If set to "0", the user cannot modify the values. This property can be used to permanently set network timeouts before the RGS Receiver is started. The default value is "1" - timeout values are changeable by the user.

Rgreceiver.Network.Timeout.Warning=int

The timeout in milliseconds used to detect and notify the user of a network disruption. The default value is 2000 milliseconds - two seconds.

Rgreceiver.Network.Timeout.Error=int

The timeout in milliseconds used to detect and disconnect an inactive connection. The default value is 30000 milliseconds - thirty seconds.

Rgreceiver.Network.Timeout.Dialog=int

The timeout in milliseconds used to display and wait on responses from input dialogs, such as the authorization dialog and PAMauthentication dialog. The default value is 15000 milliseconds - fifteen seconds.

USB Properties:

Rgreceiver.Usb.IsMutable=bool

If set to "1", the user will be able to modify all USB controls in the RGS Receiver Control Panel. If set to "0", none of the controls can be changed by the user. This can be used to permanently enable or disable remote USB before the RGS Receiver is started. The default value is "1".

This property only applies to HP Blade Workstation Client.

`Rgreceiver.Usb.IsEnabled=bool`

If set to "1", remote USB will be enabled. If set to "0", all remote USB will be disabled and no network bandwidth will be consumed for remote USB.

This property only applies to HP Blade Workstation Client.

`Rgreceiver.Usb.ActiveSession=int`

When the RGS Receiver is in Directory Mode or Enterprise Service Mode, the Receiver can connect to one or more RGS Senders. This property will specify the RGS Sender that remote USB will be connected to. To have all remote USB go to the first sender, use value zero. To have all remote USB go to the second sender, use value one, and so on. Remote USB can only go to one sender at a time. To change the sender, all senders must be disconnected. Then, enter a new value and reconnect all senders. The default value is zero - the first sender to be connected.

This property only applies to HP Blade Workstation Client.

RGS Sender Properties

All of the following properties are used by the RGS Sender, and can be set from the command line or from the RGS Sender property configuration file (`rgsenderconfig`).

General Properties:

`Rgsender.IsRdpLogoutDetected=bool`

The methods provided by Microsoft to close a connection through Remote Desktop Protocol (RDP) work quickly when the user disconnects from the RDP session. If the user logs out of the RDP session, the RGS Sender will be unable to access the desktop for about 60 seconds. If set to "1", the desktop will be available to the user through RGS as soon as possible. The RGS Sender will monitor the RDP session for a logout and begin the process of making the desktop available as soon as the logout is detected. If set to "0", the RGS Sender will not monitor the RDP session for a logout.

This property only applies to Windows versions of the RGS Sender.

`Rgsender.IsCopyRegionEnabled=bool`

If set to "1", RGS Copy Regions are sent from the Sender to the Receiver. If set to "0", RGS Copy Regions are turned off and will be sent to the Receiver as Image Update Regions. This is for advanced use and should not be set. The default value is "1" - send RGS Copy Regions.

`Rgsender.IsRegionLimitEnabled=bool`

Used to limit the number of update rectangles in a update region. This is for advanced use and should not be set. The default value is 0 - don't limit regions.

Rgsender.IsDisconnectOnLogoutEnabled=bool

If set to "1", the RGS connection will be disconnected when the user logs out. If set to "0", the RGS connection will remain connected to the sender when the user logs out. The default value is 1 - always disconnect when the user logs out.

Rgsender.IsSnapToCodecEnabled=bool

If set to "1", the HP Codec will be aligned or snapped to tile boundaries. This will avoid persistent visual artifacts at the expense of potentially increased bandwidth usage. If set to "0", the alignment of the codec with respect to the screen will be arbitrary, as determined by the exposed or modified region. For user desktops that contain primarily 2D applications, turning off this property can save network bandwidth. The default value is "1" - always snap the codec to tile boundaries.

Rgsender.MaxImageUpdateRate=int

Used to limit the number of image updates per second transmitted from the Sender to the Receiver. The value is the maximum number of updates per second. If the image update rate is too high, and using too much network bandwidth, the MaxImageUpdateRate can be set to limit the number of image updates per second. The default value is 0 - don't limit the image update rate.

Networking Properties:

Rgsender.Network.Timeout.Error=int

The timeout in milliseconds used to detect and disconnect an inactive connection. The default value is 30000 milliseconds - thirty seconds. See Using Timeouts for more details.

Rgsender.Network.Timeout.Dialog=int

The timeout in milliseconds used to display and wait on responses from input dialogs, such as the authorization dialog and PAM authentication dialog. The default value is 15000 milliseconds - fifteen seconds. See Using Timeouts for more details.

How to Collaborate

The HP Remote Graphics Software allows users to share a desktop with several users simultaneously. For example, a user can allow multiple connections to the same system enabling multiple-desktop collaboration with several users. This feature can be used for a variety of scenarios including classroom, design reviews, and support. All users must use a unique username and cannot share usernames.

Multiple connections between Senders and Receivers are only allowed if the user logged into the Sender system, referred to as the primary user, allows the connection. A question dialog, stating the domain and user name of the user attempting a connection, is displayed on the Sender's desktop when a new Receiver attempts to connect. All currently connected users are given the option to allow or disallow the connection using buttons in the message box.

- If a user allows the connection, the new user is allowed to connect to the Sender and view the desktop.
- If the connection is not allowed, the new Receiver will be unable to connect.
- If no one is logged into the Sender's desktop (in other words there is no primary user) then all authenticated connections are connected and able to view the Windows login desktop. However, when a user logs into the Sender desktop, all non-primary users, are disconnected. This is a security precaution.
- On Windows, if the primary user disconnects, the desktop is locked, but the Receivers will remain connected.
- On HP-UX and Linux, if the primary user disconnects, the desktop is locked and all users are disconnected.
- If the remote user connecting is the same user as the user logged in the desktop, the collaboration dialog is not displayed and the connection is allowed.

On Microsoft Windows, a Sender desktop icon in the system application tray displays the status of connections. The icon animates when Receivers are connected. Additionally, a collaboration notification dialog is displayed on the desktop whenever a non-primary user is connected.

On Linux and HP-UX, the Sender GUI is present on the desktop, but does not display connection status.

The Sender icon or GUI can be used to enable and disable mouse and keyboard for non-primary users. For example, if you wish to grant "view only" access to users simply right-click on the icon or GUI and select "Remote IO" and then select "Enable" or "Disable"

All Receivers can be easily disconnected from the HP Remote Graphics icon located in the system tray or from the Sender GUI by right-clicking on the icon or GUI. This is useful when hosting collaborative session, such as in a classroom environment, and the session ends.

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 owner must not use the keyboard or mouse for a short period of time (0.5 seconds). If any other user attempts to use the mouse or keyboard while the current owner is not using the input devices for this short period of time, the floor ownership transfers to the new user.

The mouse and keyboard can be disabled for non-primary users. The primary user is the user that is logged into the desktop of the Sender system. A non-primary user is a user that is connected, but is not logged in. For example, if UserA is logged into the Sender system and UserB is connected in, the with I/O disabled, UserB cannot control the mouse and keyboard.

Using Single Sign-on

When RGS Single Sign-on is not installed, users are normally required to authenticate twice when connecting - once to connect from the RGS Receiver to the RGS Sender (RGS connection) and another to log into or unlock the remote desktop (Desktop session).

When Single Sign-on is installed, users will normally need to enter their credentials only once. The user will be prompted on the RGS Receiver to enter their credentials. These credentials will be used to authenticate the connection to the RGS Sender. If the user is authenticated on the sender, the same credentials will be used to silently log into or unlock the user onto the users desktop.

Single Sign-on will only occur when the Sender is in one of two states - the logged off state or the locked desktop state. These two states are `WinLogon` states, and are controlled by the `WinLogon.exe` process running on the Sender system. `WinLogon.exe` is the Window's logon manager and is the process responsible for managing user logon and logoff. The `WinLogon.exe` process controls these states, more formally known as `WlxDisplaySASNotice` and `WlxDisplayLockedNotice` states.

When the remote desktop is in the logged off state (`WlxDisplaySASNotice`), the following dialog is present on the remote desktop:

When the remote desktop is in the locked desktop state (`WlxDisplayLockedNotice`), the following dialog is present on the remote desktop:

If the remote desktop displays either of these two states, then an RGS Single Sign-on connection will work. If the remote desktop state differs from these requirements, Single Sign-on will not work and the user will need to enter their credentials twice.

To support Single Sign-on in the RGS Sender, the custom RGS GINA (Graphical Identification and Authentication) module, `hprgina.dll`, must be installed and loaded by Window's `WinLogon` process. The RGS GINA module resides in the `C:\WINDOWS\system32` directory of the Sender's system. The `hprgina.dll` module is loaded by Window's `WinLogon.exe` process at system boot up.

The RGS Sender enables Single Sign-on functionality with a correctly installed and configured `hprgina.dll` module. Please refer to Installing & Enabling Single Sign-on section to learn more about enabling RGS Single Sign-on.

Using Easy Login

Easy Login is only supported on HP Blade Workstations running Windows XP.

If Easy Login is not installed, users are normally required to authenticate twice when connecting - once to connect from the RGS Receiver to the RGS Sender (RGS connection) and another to log into or unlock the remote desktop (Desktop session).

When Easy Login is installed, users will normally need to enter their credentials only once. The user will directly connect to the RGS Sender and immediately enter their credentials to log in or unlock the remote desktop in the Remote Display Window.

Easy Login works only with one RGS connection - no other prior / simultaneous RGS connections are allowed. Easy Login works only with the Sender in one of two states - the logged off state or the locked desktop state. These two states are `WinLogon` states, and are controlled by the `WinLogon.exe` process running on the Sender system. `WinLogon.exe` is the Window's logon manager and is the process responsible for managing user logon and logoff. The `WinLogon.exe` process controls these states, more formally known as `WlxDisplaySASNotice` and `WlxDisplayLockedNotice` states.

When the remote desktop is in the logged off state (`WlxDisplaySASNotice`), the following dialog is present on the remote desktop:

When the remote desktop is in the locked desktop state (`WlxDisplayLockedNotice`), the following dialog is present on the remote desktop:

These two WinLogon states requires the user to type in **Ctrl-Alt-Del**, the standard WinLogon SAS (Secure Attention Sequence), to enter in their credentials. If the remote desktop displays either of these states with no other RGS connections present, then an Easy Login connection will work. If the remote desktop state differs from these requirements, Easy Login will not work and the user will need to enter their credentials twice.

To support Easy Login in the RGS Sender, the Sender must know about the various WinLogon states. The Sender uses a custom RGS GINA (Graphical Identification and Authentication) module, hprgina.dll, to determine these states. It resides in the C:\WINDOWS\system32 directory of the Sender's system. The hprgina.dll module is loaded by Window's WinLogon.exe process at system boot up. Once the module is loaded, the Sender receives notifications of all WinLogon state changes.

The RGS Sender enables Easy Login functionality with a correctly installed and configured hprgina.dll module. Please refer to Installing & Enabling Easy Login section to learn more about enabling Easy Login.

Microsoft Remote Desktop and Easy Login

Microsoft Remote Desktop and RGS Easy Login ideally coexist and work well together under certain situations. The following scenarios demonstrate how a user and an IT administrator can work together using their preferred methods:

- UserA uses RGS to connect to his HP Blade Workstation.
- UserB is an IT administrator and uses Microsoft Remote Desktop to connect to UserA's Blade Workstation.

Careful orchestration keeps Easy Login enabled. Under certain scenarios, it can become disabled. The following section describes several of the possible key scenarios.

UserB never connects in - RGS Easy Login remains enabled for UserA:

This is the primary scenario assumed for day-to-day operations.

1. UserA logs off and then disconnects the RGS Receiver from the sender before leaving work for the evening. UserA might also lock the workstation rather

than logging off before disconnecting the RGS Receiver. A screen saver might also be used to force the desktop to be locked after a certain amount of elapsed time. In this case, UserA would just disconnect the RGS Receiver and let the screen saver kick in to lock the desktop.

2. UserB never uses Remote Desktop to connect into UserA's Blade Workstation.
3. UserA returns the next morning and connects to his Blade Workstation using the RGS Receiver. UserA connects directly to his workstation with an Easy Login connection. He enters his credentials only once.

UserB logs off of the Blade Workstation when finished - RGS Easy Login remains enabled for UserA:

This is the standard scenario assumed for IT support.

1. UserA logs off and then disconnects the RGS Receiver before leaving work for the evening.
2. That night UserB connects into UserA's workstation using Remote Desktop Connection. He logs in using an administrator account to update a software package. Once UserB finishes, he logs off from the Blade Workstation. No Remote Desktop session remains.
3. UserA returns the next morning and connects to his Blade Workstation using the RGS Receiver. UserA connects directly to his workstation with an Easy Login connection. He enters his credentials only once.

UserB connects in, but does not log in - RGS Easy Login remains enabled for UserA:

This scenario should rarely occur.

1. UserA logs off and then disconnects the RGS Receiver before leaving work for the evening.
2. That night UserB connects to UserA's Blade Workstation using Remote Desktop Connection, but UserB does not log in. A Remote Desktop connection remains active although no login exists.
3. UserA returns the next morning and connects to his Blade Workstation using the RGS Receiver. UserA connects directly to his workstation with an Easy Login connection. He enters his credentials only once.

UserB connects in, and then disconnects without logging out - RGS Easy Login is disabled for UserA:

This scenario is possible but not recommended. IT administrators should always log off (not just disconnect) when finished working with a Microsoft Remote Desktop Connection. When a user only disconnects with Microsoft Remote Desktop, but the user doesn't logoff, it leaves a terminal services session open and this interferes with Easy Login.

1. UserA logs off and then disconnects the RGS Receiver before leaving work for the evening.

2. That night UserB connects into UserA's workstation using Remote Desktop Connection. He logs in using an administrator account to update a software package. Once UserB finishes, he disconnects from the Blade Workstation. Since UserB just disconnected and did not logoff, a Remote Desktop or Windows terminal services session remains active.

3. UserA returns the next morning and attempts to connect to his Blade Workstation using the RGS Receiver. UserA must enter his credentials to connect into the workstation. Due to the active session left by UserB (who did not log off), UserA cannot connect to his workstation because UserB owns the desktop session on UserA's Blade Workstation.

4. UserA must call up IT and seek help. IT must discover the Remote Desktop or Windows terminal services session and log out the administrator session for UserA to connect.

Remote Application Termination on Windows

Remote Application Termination (RAT) is only supported on Windows.

Network outages or loss of connectivity between a RGS Receiver and Sender 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. This support is available through the RGS Sender for Windows.

This section describes how to interpret RGS connectivity status, decode Windows Event Log messages from the Sender, and create effective control agents for remote application management and termination during disconnects.

RGS Connection and User Status

The RGS Sender reports status of connections through a custom Windows Event Log called HPRemote. RGS connections normally occur in two phases:

- Phase 1: RGS Connection - a connection over a standard computer network between an RGS Sender and RGS Receiver
- Phase 2: Desktop Session - a logged-in session that gives access to a desktop workspace on a remote workstation using a RGS connection

Desktop Sessions can operate independently of active RGS Connections. This allows the user to disconnect and reconnect to Desktop Sessions as part of a normal workflow. However, when a connection is unintentionally disconnected, a user may require remote applications to be terminated after Desktop Sessions are left unattended for a period of time to prevent them from operating unsupervised.

Ownership of a Desktop Session on Windows defines the type of user status in effect for a RGS connection. Events posted to the HPRemote Windows Event Log reflect the following control priorities:

- Primary User - The user of a RGS Connection that matches the user logged into the Desktop Session.
- Non-primary User (also Collaborating User) - A user of a RGS Connection that does not match the user logged into the Desktop Session. If no one is logged into a Desktop Session, then all connections are non-primary.

Primary user status defines control and the need for a monitoring agent to take action against running applications of interest. When the number of primary user connections drops to zero, then the Desktop session may require user-defined actions.

HPRemote - the RGS Windows Event Log

The RGS Sender posts events in the HPRemote Windows Event Log. Event messages are directly viewable with the Windows Event Viewer or by an application

using the Event Log Service API. Data in the Event Log consists of a Message ID followed by optional data contained 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. Review each message type in the table below for exact field and usage descriptions. Details for using the Event Viewer follow after the table.

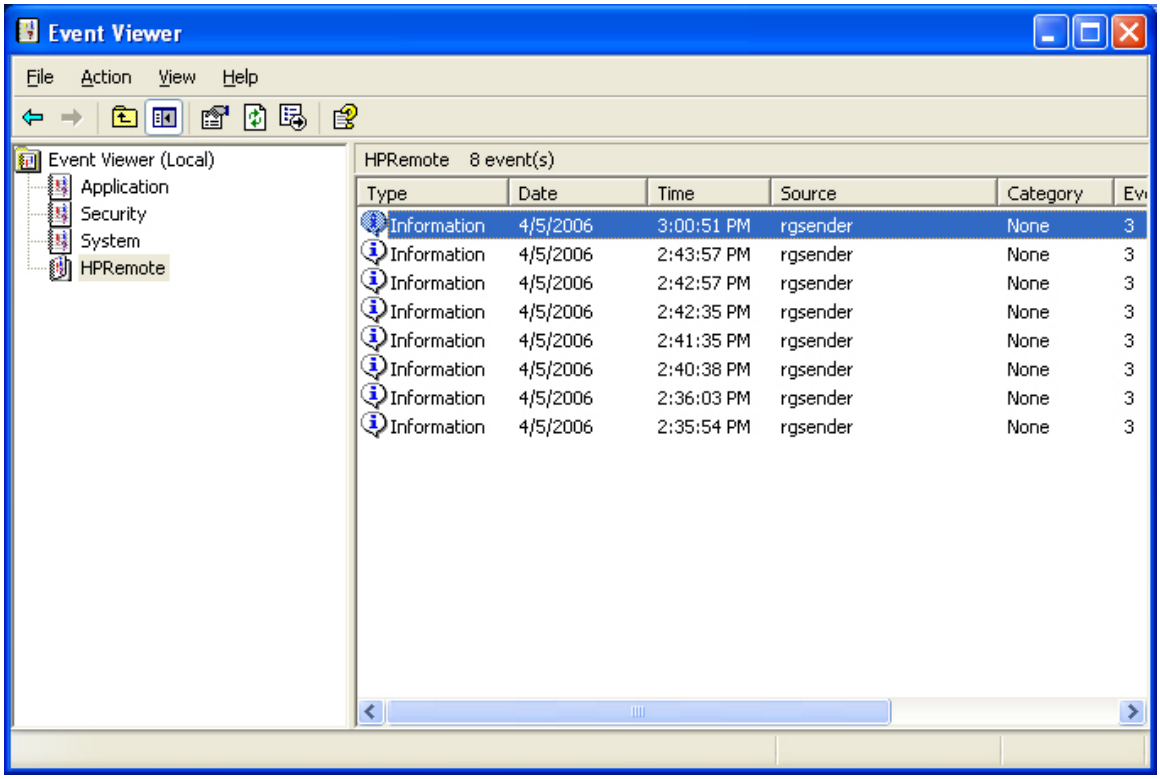
Message ID	Description
RGSENDER_CONNECT_STATE	The connection state consists of zero or more primary connections and zero or more non-primary connections. Each event entry records the current number of active connections in each category. Events appear when the connection status of these users changes. 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. Event Viewer Message: Primary connections: %1. Non-primary connections: %2. Strings: %1 = number of primary connections %2 = number of non-primary connections Data: UINT32 numPrimary UINT32 numNonprimary Event Viewer Example: Primary connections: 1 Non-primary connections: 0

RGSENDER_CONNECT	A new connection was established with an associated name. If Easy Login is enabled, the name assignment will be deferred until login and the associated name may be “Anonymous”. Event Viewer Message: Connect %1. Strings: %1 = name associated with connection Data: None Event Viewer Example: Connect MYDOMAIN\myusername.
RGSENDER_DISCONNECT	A receiver has disconnected. The message will contain the name associated with the connection. If Easy Login is enabled and the receiver disconnects prior to a login, the associated name may be “Anonymous”. Event Viewer Message: Disconnect %1. Strings: %1 = name associated with connection Data: None Event Viewer Example: Disconnect MYDOMAIN\myusername.
RGSENDER_STARTUP	Reference event registered to aid in interpretation of the event log by Event Viewer. Signifies proper startup of the RGS Sender service. Event Viewer Message: RGS Sender startup.

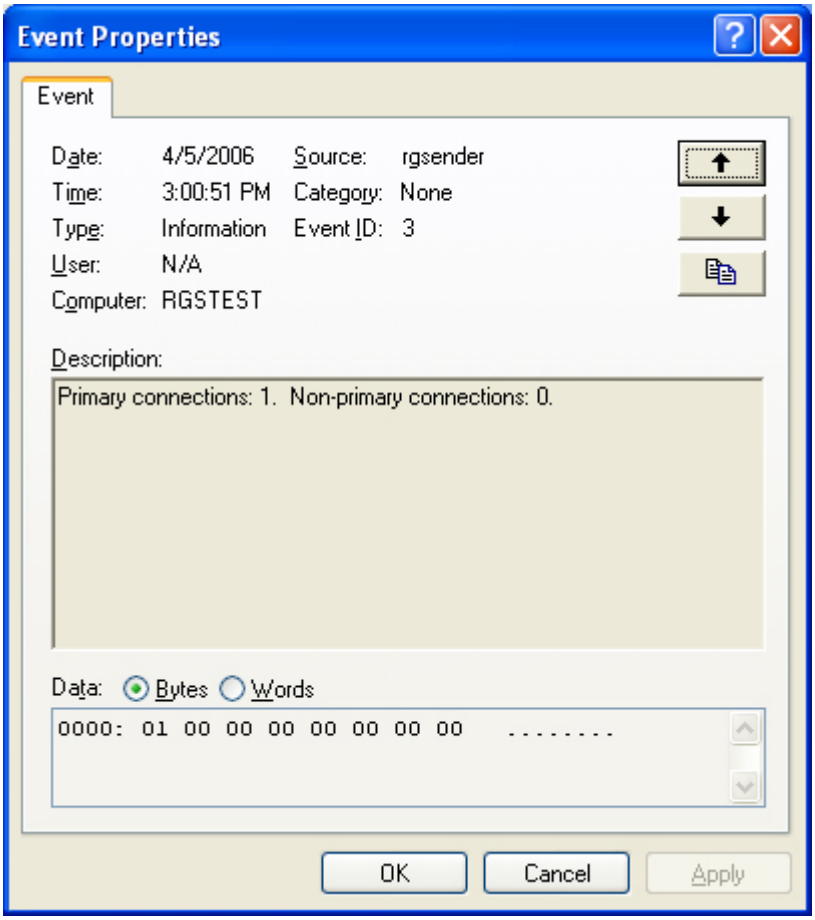
	Strings: None Data: None
RGSENDER_SHUTDOWN	Reference event registered to aid in interpretation of the event log by Event Viewer. Signifies proper shutdown of the RGS Sender service. Event Viewer Message: RGS Sender shutdown. Strings: None Data: None
RGSENDER_SET_PRIMARY	A connection with an associated name is set as the primary connection. Event Viewer Message: Set %1 as primary connection. Strings: %1 = name associated with connection Data: None Event Viewer Example: Set MYDOMAIN\myusername as primary connection.

RGSENDER_SET_NONPRIMARY	A connection with an associated name is assigned to a non-primary status. This may happen as a result of a logout. Event Viewer Message: Set %1 as non-primary connection. Strings: %1 = name associated with connection Data: None Event Viewer Example: Set MYDOMAIN\myusername as non-primary connection.
RGSENDER_ASSIGN_USER	If Easy Login is enabled, the assignment of the name will be deferred until login. When the name is assigned, this message will be generated. Event Viewer Message: Assign %1 connection to %2. Strings: %1 = original name of connection %2 = new name of connection Data: None Event Viewer Example: Assign Anonymous connection to MYDOMAIN\myusername.

The Event Viewer is available as an "Administrative Tools" option in the Windows system Control Panel. Invoking the Event Viewer makes the HPRemote log available along with the standard system event logs:



Assuming the RGS Sender is properly installed and active, an HPRemote Event Log is created and reflects recent connection activity. By default, the most recent events display first. Clicking any record allows inspection of that event. The next image shows the detail of the 3:00:51 event. Note the radio button option to view the UINT32 connection data in byte and word formats. The word format is selected below. The HPRemote Event Log is also a fixed-size event log. All entries are "Last In, First Out" (LIFO) order when it fills.



Basic Application Control Agents

Basic Windows monitoring agents must have the ability to monitor the HPRemote event log and interpret its events. When the number of primary user connections drops to zero, an agent should execute its actions tied to applications of interest running in the Desktop Session. Broader design issues for a control agent are covered in the next section.

This section outlines a simple fixed-polling Windows agent that reads and interprets a local HPRemote event log. The basic structure involves two simple core functions:

- `processEvent(eventServer, eventSource, dwEventNum)`
    - open event log, read event `dwEventNum`, close event log
    - if valid read, process recognized `EventIDs`, then return
- `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 mSec

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

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

The programming header file, `RGSenderEvents.h`, is located with the RGS Sender installed software at:

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

A simple pseudo-code agent using these functions looks like this:

```
#include <windows.h>
#include <stdio.h>
#include "RGSenderEvents.h"
#define BUFFER_SIZE 1024    // safe EVENTLOGRECORD size for now
#define EVENT_SERVER NULL   // remote server = "\\\\nodename";  local = NULL
#define EVENT_SRC "rgsender"   // specifies specific event name source in
                               // HPRemote
BOOL processEvent(LPCTSTR eventServer, LPCTSTR eventSource, DWORD dwEventNum)
{
    HANDLE h;
    EVENTLOGRECORD *pevlr;
    BYTE bBuffer[BUFFER_SIZE];
    DWORD dwRead, dwNeeded;
    BOOL result;
  //  Open, read, close event log ============================================

    if ((h = OpenEventLog(eventServer, eventSource)) == NULL)
    {
        ... report error status ...
        return true;
    }

    // Set the pointer to our buffer. Strings and data will get appended
    // to the EVENTLOGRECORD structure.
    pevlr = (EVENTLOGRECORD *) &bBuffer;

    // Read the event specified by dwEventNum

    result = ReadEventLog(h,            // event log handle
                EVENTLOG_SEEK_READ |    // start at specific event
                EVENTLOG_FORWARDS_READ, // advance forward
                dwEventNum,             // record to read
                pevlr,                  // pointer to buffer
                BUFFER_SIZE,            // size of buffer
```

```
                &dwRead,                // number of bytes read
                &dwNeeded);             // bytes in next record
    if (CloseEventLog(h) == false)
    {
        ... report error status ...
        return true;
    }
  //  Process event (example: print out event) ============================
    if (result)
    {
        // We only know how to process specific events
        if (pevlr->EventID == RGSENDER_CONNECT_STATE)
        {
            // Retrieve the two UINT32 fields of this message
            // representing primary and non-primary connections.

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

        // If an event is added, either the start or count will change.
```

```
        // Get the start and count. Microsoft does not specify what
        // reasons these functions could fail, so we cannot ensure
        // success. Check the return value.
        if (GetOldestEventLogRecord(h, &dwCurrentStart) == false ||
            GetNumberOfEventLogRecords(h, &dwCurrentCount) == false)
        {
            CloseEventLog(h);
            ... report error - unable to obtain event logs ...
            return;
        }
        if (CloseEventLog(h) == false)
        {
            ... report error status here ...
            return;
        }
      //  Determine state of log change ====================================
        // Compute the index of the last event. If the count is zero, then
        // there are no events and the index is 0.
        if (dwCurrentCount == 0)
        {
            dwNewIndex = 0;
        }
        else
        {
            dwNewIndex = dwCurrentStart + dwCurrentCount - 1;
        }
        // If the new index is different than the current, update the current
        // and process the current event. Otherwise, we sleep for a while.
        if (dwNewIndex != dwCurrentIndex)
        {
            // We have at least one new event. Print out the last event.
            dwCurrentIndex = dwNewIndex;
            if (dwNewIndex)
            {
                if (processEvent(eventServer, eventSource, dwCurrentIndex))
                {
                    ... event processing error here ...
                    return;
                }
            }
        }
        else
        {
            // No new events. Sleep for 1 second.
            Sleep(1000);
            waitedFor += 1;
        }
    }
    return;
}
main( ... )
{
    ... setup and initialize agent ...
```

```
    monitorEvents(EVENT_SERVER, EVENT_SRC, seconds);
    ... cleanup agent here or send alerts ...
    ... may wish to return status from monitorEvents ...
}
```

NOTE: The parameter EVENT_SRC above defines the name of an event generator here, not necessarily the Windows Event Log name HPRemote as suggested by external documentation. Supported event source names include:

RGS Event Source Name (**LPCTSTR**)	Description
"rgsender"	Events generated by the RGS Sender service

More information and examples for Event Log readers is available at:

```
http://msdn.microsoft.com/library
```

Search on the topic OpenEventLog for a function description and additional examples.

Agent Design Issues

Windows Application Agents for RGS remote session require careful design to maximize their effectiveness. Issues and tradeoffs can minimize data loss and determine when a last resort shutdown of a disconnected Windows session is required.

The following list introduces topics of interest 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. In general, remote administration of an arbitrary application environment will require some pioneering work.

Desktop Session Logout

- Issues - 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 specific time allowance for reconnection has expired). This action would drop all connections to the remote session.
- Benefits - Implementing a full session shutdown / logout ensures that all connection activity ceases immediately and 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 session management. Agent relies upon Windows logout routines to terminate environment - simple in design and result.
- Concerns - Forcing a 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 intervention at restart.

Selective Environment Shutdown

- Issues - Partial shutdown of an environment only terminates certain applications of interest. It does not implement a full Desktop Session logout. It selectively protects only the most critical applications requiring oversight and control.
- Benefits – 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.
- Concerns - Potentially more complicated to implement. Can require coordination of multiple agents to handle layered shutdown. Can still result in data loss for specific applications. May require a master semaphore to halt / terminate multiple agents if user reconnects and wants to stop the shutdown process.

Wrapping Applications of Interest

- Issues - Agents can be launched and supervise only specific applications in a given environment. Tying agents to specific applications is a selective safety net for every user.
- Benefits - 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.
- Concerns - 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

- Issues - 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.
- Benefits - System agents are not required to take destructive action - they serve only as alarms and monitors for alternate human intervention.

- Concerns - May require redundant networking channel. Requires administrator or operator availability to support.

Anticipating User Disconnects and Reconnection

- Issues - Users must first be warned about the consequences of disconnection. Agents that provide protection for a disconnected session can also provide 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.
- Concerns - Users should not be able to disable or specify their own timeouts due to potential irreversible data loss.

General Design Issues

- All active agents should externally log their decisions and actions for post mortem 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 Safeguard Features for Windows systems

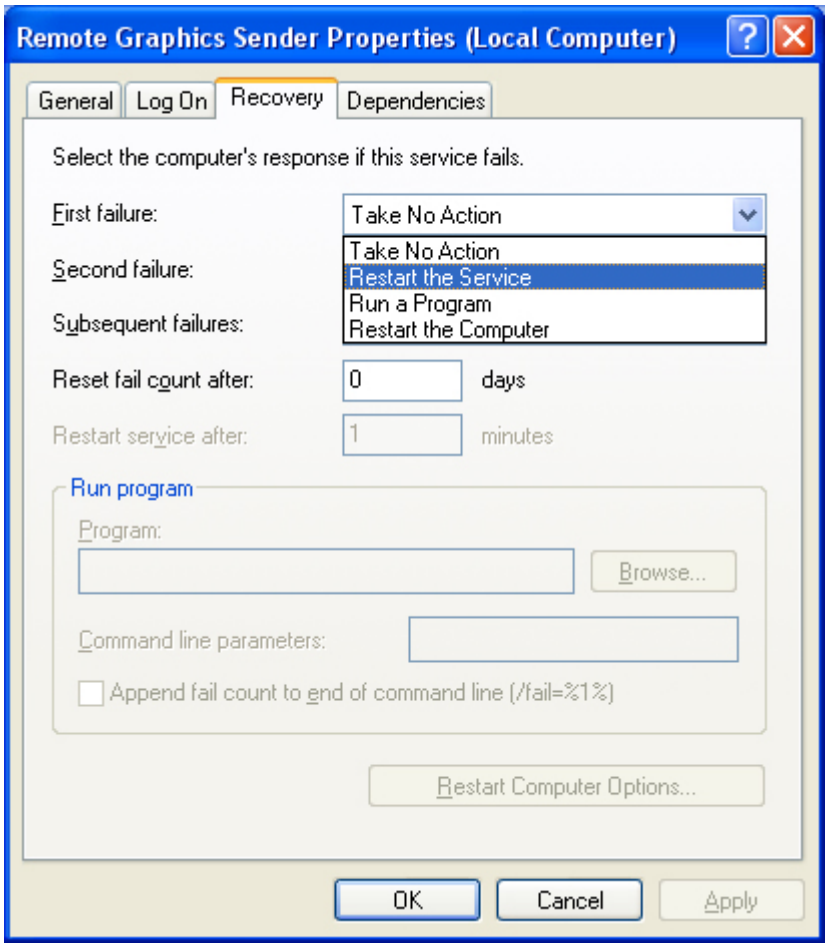
The following optional procedures for the RGS Sender service can improve the reliability of your remote agent solution if required in your environment.

RGS Sender Service Recovery Settings

- 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 Windows defaults (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).
- Agent designs should take into account 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. Recovery options seen in the properties panel below 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 Receiver can no longer connect to the Sender, a Windows system with Remote Desktop services enabled can also access the remote system to diagnose the issue.

Using Timeouts

Various network conditions as well as end-user needs require the ability to specify network warning, error and dialog timeouts. RGS enables relatively fine-grained control over the network and dialog timeout values as well as an innovative form of user notification when a warning timeout expires. This allows tuning for specific network conditions and environments, such as low-bandwidth or high-latency conditions. At the same time the user is notified of potential issues involving more catastrophic or transient network conditions. This section describes the purpose, type, function, and recommended settings for RGS timeouts.

The RGS Receiver and Sender have command-line options and properties that can specify the network warning and error timeouts. The RGS Receiver also enables timeout values available from the Receiver Control Panel.

There are several types or classifications of timeouts in the RGS product:

- Network Warning Timeouts: The Receiver uses network warning timeouts to display a warning or notification of potential network connectivity loss if the timeout expires.
- Network Error Timeouts: The Receiver and Sender use network error timeouts to control the following:
    - The maximum time that a Sender and Receiver will wait for or retry a network invocation before reporting a network error and fully closing the connection.
    - The maximum time that a Receiver and Sender will wait for a sync-pulse prior to fully closing the connection.
- Dialog Timeouts: The maximum time that a Receiver and Sender will display a message/response dialog or wait for an invocation response between the pair.

RGS uses TCP/IP over a standard computer network to transmit data. TCP/IP is a reliable transport mechanism, but it still offers no guarantees on network packet delivery. This is in contrast to the reliable connection that a keyboard, mouse, and monitor enjoy when using a PS/2, USB, or video cable on a computer. (A complete discussion of TCP/IP is beyond the scope of this document. Interested readers should refer to any number of excellent references on this subject to fully cover this material.)

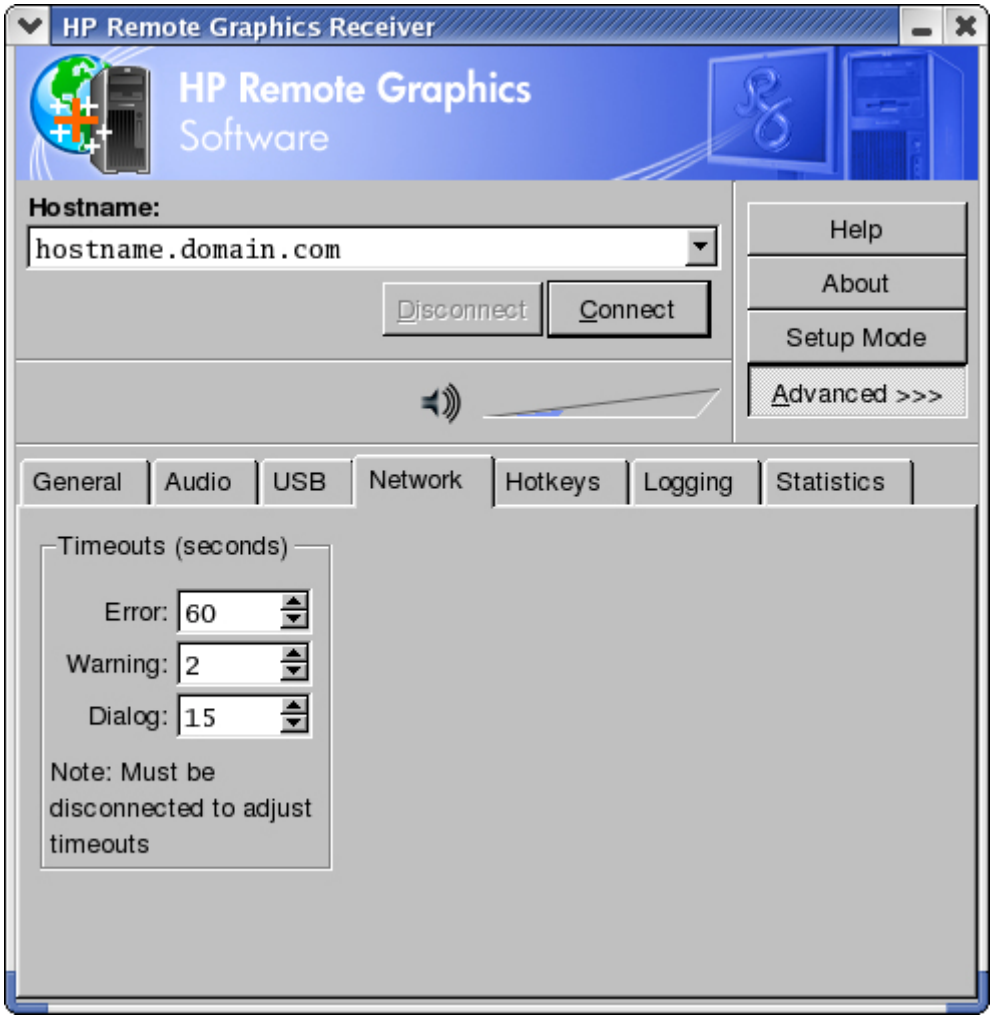
The TCP/IP network stack typically performs well on a relatively stable network. However, issues outside of RGS can affect the probability and timing of network packet delivery that ultimately impact system performance. Issues such as

- network over-subscription results in congestion and packet loss
- CPU utilization from other processes/tasks starves the network stack
- send and receive response time fails due to inadequate bandwidth
- network switches, routers, and NICs can fail or be incorrectly configured

- a network cable can be pulled (done often during testing) from its port
- other failures are possible, too.

In some network scenarios, a disruption is transient while in other networks the connectivity loss is more permanent. For example, a network cable can be accidentally pulled and then plugged in again resulting in the network being restored. If a network disruption is temporary, a network stack may wait and attempt to recover connectivity before giving up and fully disconnecting. This is what the TCP layer of the TCP/IP network stack automatically does. If a temporary network disruption occurs, the network stack often detects the condition and continues to retry, subject to the timeout parameters set in the TCP/IP network stack. However, during these intervals of network inactivity, it is often important that the user receive notification of a potential network connectivity loss, especially if important decisions depend upon the temporal accuracy of the data presented to the user in the Remote Display Window.

If connectivity is restored after a disruption, the RGS Receiver should continue to receive updates and operate normally. In many cases, the user should experience little or no inconvenience if connectivity is restored in a short amount of time. However, if network connectivity loss persists, then a connection decision is required to either wait, retry, or permanently close a connection. If the error timeout expires, the RGS Receiver and Sender will fully close their connections and a new connection must be initiated by the Receiver to restore connectivity.



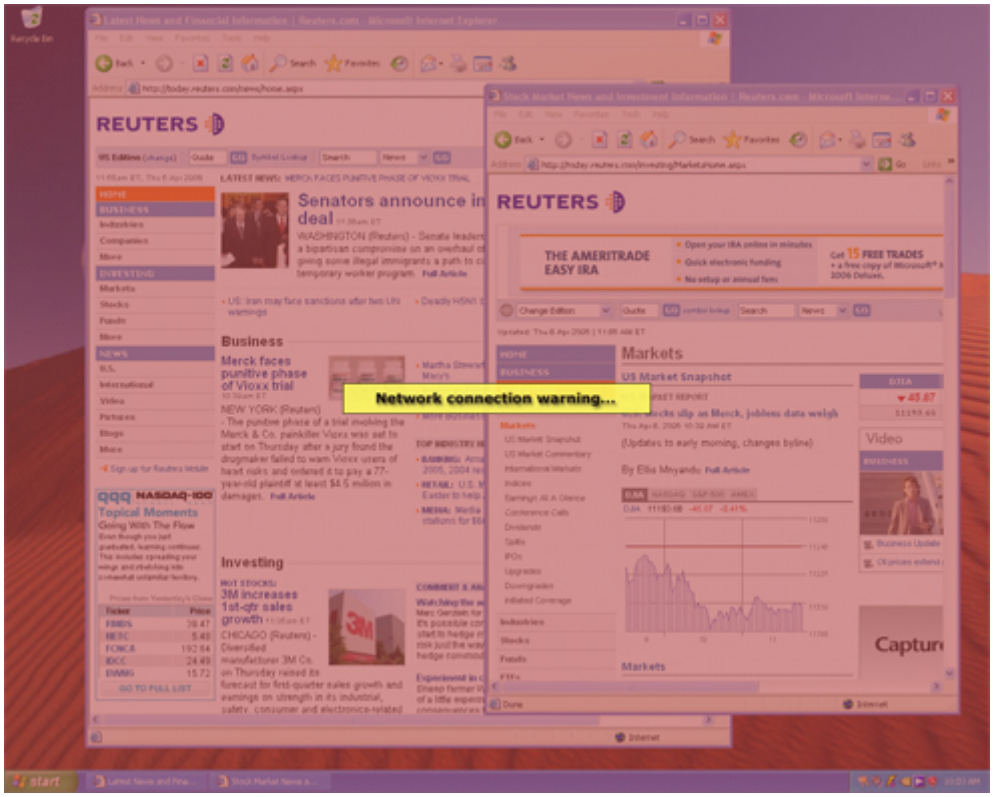
In the network section of the RGS Receiver Control Panel, the warning timeout controls user notification if a potential network issue occurs. Under normal conditions, the RGS Receiver and Sender use sync-pulses to establish connection integrity. Sync-pulses are messages or, more appropriately, method invocations between the Receiver and Sender. If the Receiver fails to detect a sync-pulse beyond the warning timeout value, the Receiver's Remote Display Window will dim and display a warning to the user. This serves to notify the user of stale contents in the Remote Display Window. Users making critical decisions based upon data displayed in the Remote Display Window should wait until their network returns. If connectivity returns prior to reaching the error threshold (implying return of sync-pulses between applications), the Remote Display Window becomes undimmed on the next image update and normal operation continues.

If loss of sync-pulses and connectivity continues or a network invocation fails, the error timeout will trigger the Receiver to close its connection. After this action, the Receiver displays the "Connection Lost" error dialog.

A useful timeout strategy for end-users is to set short warning timeouts and longer error timeouts. With these settings the end-user detects potential network disruptions relatively quickly while allowing connections enough time to possibly recover upon network restoration. The default warning timeout for RGS Receiver is

two seconds (two-thousand milliseconds). The default error timeout is thirty seconds (thirty-thousand milliseconds).

In a practical example, if a temporary network disruption occurs for less than two seconds, the Receiver does not display a user notification and the user only experiences a brief drop in Remote Display Window interactivity. This means that, for a user moving or scrolling a window, the window will appear unresponsive or hung. If no interaction with the display occurred while the network stalls, the event is usually not even notable unless dynamic content such as video fails to update in a reasonable amount of time.



If the disruption continues for greater than two seconds, then the Remote Display Window dims and a warning appears. During this time the Remote Display Window appears unresponsive to users. If connectivity returns, then the Remote Display Window returns to its normal appearance and interactivity. A full loss of connection beyond the error timeout results in closure of the Remote Display Window and display of the "Connection Lost" error dialog as previously described.

Receiver properties are fully settable from the Receiver properties resource file or command line. The default value for the Receiver property, Rgreceiver.Network.Timeout.Warning, is 2,000 milliseconds (two seconds). This value works well for most installations. For networks with less stable connectivity and disruptions greater than two seconds, higher warning timeout values will lessen the appearance of network warning as a nuisance to user productivity.

The recommended default value for the Receiver property, Rgreceiver.Network.Timeout.Error, is 30,000 milliseconds (thirty seconds). In practice, this works well, although some users adjust this value lower to force connections to close sooner. Higher settings of one minute (60,000 milliseconds or

60 seconds) or greater are not necessarily practical as the connection usually becomes useless and only frustrates the user with a waiting time that tries their patience.

In the case of the Sender, the RGS Sender property, Rgsender.Network.Timeout.Error, also defines a required maximum network timeout value independent of Receiver settings. Due to legacy issues, the Sender first starts up using the maximum of either the Rgsender.Network.Timeout.Error or Rgsender.Network.Timeout.Dialog property (discussed later) to set an internal error timeout for method invocations between the Sender and Receiver as well as sync-pulse detection.

When the Receiver negotiates its connection, it notifies the Sender of its error timeout value. The Sender adopts the lesser of both timeouts to use for sync-pulse error detection. If the user later adjusts the Receiver value greater than the Sender error timeout, the Sender caps itself to its own timeout value. The total combined error timeout can never exceed the Sender's error timeout value. If a sync-pulse or an invocation between the Receiver and Sender exceeds the lesser of either limit above, then the Sender will disconnect the Receiver. The user must initiate a re-connect to the Sender to restore connectivity. Note that there is no equivalent timeout warning in the Sender that the Receiver will display. The Sender does not inform the Receiver of its error timeout value. The connection simply drops at the end of the computed timeout unless the network stack responds to an earlier network error.

The following examples demonstrate the final behavior. When the Sender error timeout is 30 seconds and the Receiver error timeout is 5 seconds, then the Sender uses 5 seconds for its sync-pulse detection since this is the minimum of both. If the Receiver error timeout is adjusted to 60 seconds, then the Sender uses a value of 30 seconds for sync-pulse detection since this is, again, the minimum of both timeouts. The timeout for invocations between the Sender and Receiver is 30 seconds in both cases.

A larger error timeout for the Sender is not recommended. If the Receiver and Sender connection terminates ungracefully, then the Sender could possibly take as long as its error timeout value to determine the connectivity loss and fully terminate the connection. From the time of actual network disruption until the error timeout expires, the Sender will not send image updates to all other Receivers (if it is serving multiple Receiver connections). This will hang the interactivity of other users for no apparent reason. After the error timeout expires, the Sender removes the one connection and continues updating all other Receivers.

If the network stack determines a network failure has occurred, it can shutdown the connection or entire network interface prior to expiration of the error timeout. For example, if a network cable is pulled on a Receiver system, the Receiver system might determine that it has lost its network and shutdown networking completely. In this case the Receiver application might catch the network exception more quickly than its timeout because the system error flows back to the receiver instead of waiting for recovery. Consequently, this results in a full Receiver disconnection before reaching its timeout threshold.

Dialog timeouts specify the maximum time that a message/response dialog appears or is waited upon between the Receiver and Sender. Invocations between the Receiver and Sender requiring user interaction often need much higher timeout

values than normal steady-state timeouts. Authentication or authorization dialogs often require more display time than standard messages and alerts due to their importance. The RGS system supports alternate timeouts for user interaction to separate them from operations such as sending graphics and audio content. This enables usable authentication and authorization experiences as well as more reasonable limits for standard messages and invocations.

The Receiver property, Rgreceiver.Network.Timeout.Dialog, (also available from the Receiver Control Panel Network tab), limits the display of incoming and outgoing query dialogs from the Sender requiring user input and interaction. Similarly, the Sender property, Rgsender.Network.Timeout.Dialog, specifies from its side similar limits for Receiver messages and queries. At startup the Sender uses the maximum of either Rgsender.Network.Timeout.Error or Rgsender.Network.Timeout.Dialog properties to define its networking timeout between the Sender and Receiver.

An example of dialog timeouts follows. If User A attempts to connect to User B's desktop, an authorization dialog prompts User B. The RGS Sender prompts User B on the Sender desktop asking for permission to connect User A to the desktop. The RGS Receiver property Rgreceiver.Network.Timeout.Dialog limits how long the Receiver waits on the invocation between the Receiver and Sender before returning failure. The RGS Sender property Rgsender.Network.Timeout.Dialog limits the display of the authorization dialog on the Sender. If either timeout expires without action, the dialog exits and connection is denied by default or it defaults secure. If the Sender timeout is shorter than the Receiver's timeout, the authorization invocation from the Receiver to the Sender usually times out faster that the dialog times out, so the authorization fails. If the Sender timeout is longer than the Receiver's timeout, the authorization dialog expires faster than the invocation from the Receiver to the Sender and the authorization still fails.

Another example follows for a different type of authentication. When a Receiver connects to a Sender running a Linux or HP-UX operating system, the Pluggable Authentication Module (PAM) authenticates the connection. In this case, the PAM subsystem invokes a PAM conversation/callback function that results in the Sender making invocations back to the Receiver to prompt the user with PAM message dialogs. The Sender receives the responses. Typically the dialogs request a username and password, but any message is possible. The timeout for the PAM message/response dialog invoked by the Sender and displayed by the Receiver is the Receiver's Rgreceiver.Network.Timeout.Dialog value.

The maximum of either the Rgsender.Network.Timeout.Error or Rgsender.Network.Timeout.Dialog properties limits how long the Sender will wait for a response. The Receiver controls the display time for the PAM message/response dialog and the Sender controls how long to wait for a response from the Receiver. If either timeout expires, the connection is denied by default or defaults secure if the timeout is exceeded. If the Sender timeout is shorter than the Receiver's timeout, then the authentication invocation from the Sender to the Receiver expires faster than the PAM Authentication Dialog, resulting in a PAM authentication failure. If the Receiver timeout is larger than the Sender's timeout, then the PAM authentication dialog times out faster than the invocation from the Receiver to the Sender and the PAM authentication still fails.

The property Rgreceiver.Network.Timeout.Dialog does not control all dialogs displayed by the Receiver. For example, the authentication dialog for a Windows Sender connection displayed by the Receiver for username and password does not

have an associated timeout since it is not an incoming invocation from the Sender to the Receiver. This dialog displays indefinitely until the user responds "OK" or "Cancel" to its requests.

The default property for Rgreceiver.Network.Timeout.Dialog and Rgsender.Network.Timeout.Dialog is fifteen thousand milliseconds (15 seconds). This should support most user authorization scenarios or PAM authentication dialogs displayed by the Receiver. In cases of more complex scenarios requiring additional time, the user should adjust both Receiver and Sender timeouts appropriately through the Receiver Control Panel, specifying properties on the command line, or using a properties configuration file.

In summary, the Receiver and Sender properties Rgreceiver.Network.Timeout.Dialog and Rgsender.Network.Timeout.Dialog similarly control the duration of response wait time requiring user interaction while making outgoing connections and dialog display time as a result of incoming messages/invocations.

Remote Graphics and Microsoft Remote Desktop Interaction

Prior to release 4.0, RGS Sender for Windows could not coexist on systems enabled for Windows Remote Desktop connections. At release 4.0, connections made with either HP Remote Graphics or Windows Remote Desktop will work. Simultaneous desktop sharing, however, is not possible.

A RGS connection to a sender already occupied with a Remote Desktop connection only works if the user credentials match for both connections. This implies that the same user wants access to transition from Remote Desktop to a RGS connection. If allowed, the current Remote Desktop connection disconnects and the RGS Receiver takes control of the current Windows desktop session. The current user does not log off and work continues with the new connection. The reverse works as well. A user who connects to his or her RGS session with a Remote Desktop connection displaces the first connection. In this case, the Remote Desktop connection causes the RGS Sender to disconnect all of its receivers (including all RGS collaborators). The Windows desktop session remains active during the switch.

If a user disconnects from a system using the Windows Remote Desktop disconnect button, the session remains logged in and all applications continue to run. The session, however, locks its screen. Remote Graphics connections only work if the credentials match the currently logged-in user.

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

A Remote Desktop connection made to a 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 logout other users. Non-administrators are refused with a warning message about permissions. If Remote Desktop logs out the current RGS user, then the sender disconnects all of its receivers (including all RGS collaborators). Note: Under reverse circumstances for the above, RGS connections will not logout an existing Remote Desktop user regardless of authority. RGS will report an authorization failure message concerning a different user owning the desktop.

Optimizing Performance

This section provides suggestions on how to optimize performance in RGS.

Performance Tuning for all platforms:

1. Set the network to operate in Full-Duplex mode

   To get the best performance, the network between the RGS Sender and RGS Receiver should run in Full-duplex mode. Read the section on Network information to learn how to turn on Full-duplex mode.

2. Set the background of the desktop to a solid color on the Sender

   One Windows using the Display Properties panel, select the Desktop tab. Set the background to None.

3. Set the Sender and Receiver to 32 bits-per-pixel

   On Windows, using the Display Properties panel, select the Settings tab and set the highest color setting in the color quality box.

4. Lower the display resolution

   HP Remote Graphics Software is an image-based remote visualization technology. Consequently, lowering the display resolution can significantly improve performance.

Performance Tuning for Windows:

This section provides performance tuning tips for RGS on Windows.

1. Use the Windows Classic desktop theme on the Sender

   The Windows XP themes are more complicated and hence require more data to be sent. From the Display Properties panel, select the Themes tab. Select Windows Classic in the Theme box.

2. Lock desktop icons on the Sender

   From with the Display Properties panel select the Desktop tab. Select Customize Desktop. On the Web tab, check Lock desktop items.

3. Disable transition effects

   Don't use color or animated cursors on the Sender. Although HP Remote Graphics Software displays color and animated cursors very well, this can take up more network bandwidth and CPU utilization.

4. Sender Process Priorities

   Sometimes, for example, rotating a model in a 3D mechanical design program using the mouse appears sluggish and image updates are inconsistent. One

possible reason for the problems is network performance. If the Sender runs on a Windows operating system, it can be an operating system scheduling issue. Sometimes this can be resolved by increasing the process priority of the Sender. See Setting Sender Priorities for further details.

Performance Tuning for Linux and HP-UX:

1. On a HP-UX sender move the window position feedback window to the edge of the screen

   On HP-UX systems running the CDE window manager, a window position feedback dialog is displayed in the middle of the screen when windows are moved around. Configure the window to be placed to the edge of the screen. Doing this will allow windows to move more quickly.

   There are two Dtwm resources that can be changed: `feedbackGeometry` or `showFeedback`. To move the feedback window to the upper-left portion of the screen, add one of the following entries to the Xdefaults file:

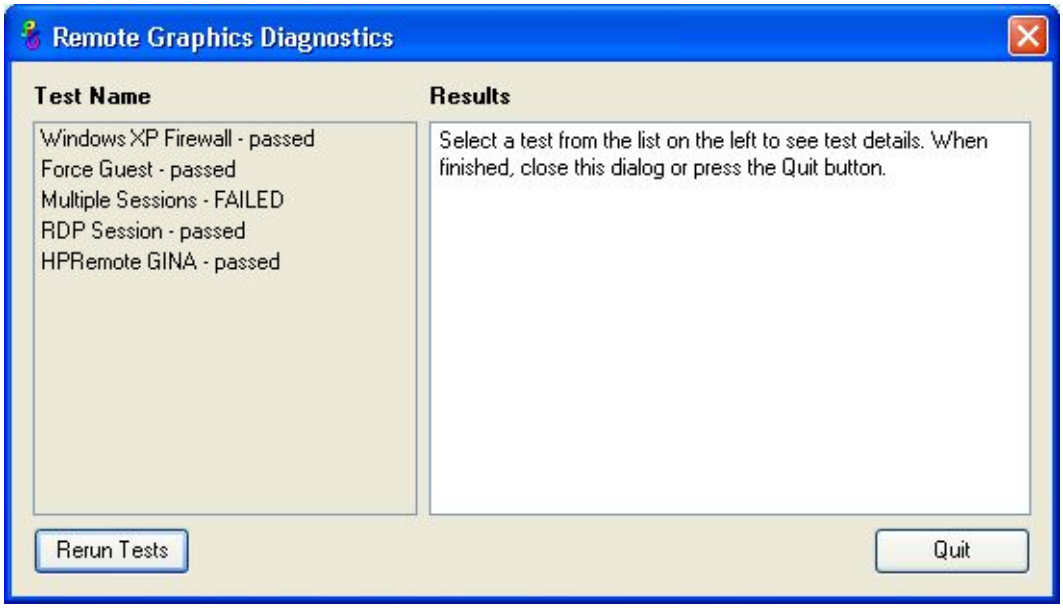
   - `Dtwm*feedbackGeometry: +0+0` - This will force the feedback window to the upper-left portion of the screen
   - `Dtwm*showFeedback: none` - This will totally turn off the feedback window
   - `Dtwm*showFeedback: -move` - This will disable the feedback window during window moves.

Utilities

The HP Remote Graphics Software comes with the following utilities to help the user set-up their systems.

Microsoft Windows Specific Utilities:

- RGS Diagnostic Tool: At the end of a normal installation of the Windows version of the RGS Sender, the RGS Diagnostic Tool runs to detect common issues that can prevent remote connections. This tool does not run as a part of an unattended install. The tool is installed in the RGS Sender installation folder and is available for running any time after an installation.



The left panel with the title Test Name shows the list of tests that run. Selecting a test with the mouse will display additional information in the right panel with the title Results. The Rerun Tests button on the bottom left reruns all tests. The example window shows that all tests have passed with the exception of the Multiple Sessions test. To determine what this test looked for, why it failed, whether this failure would prevent connections and how to fix the problem on this system, simply select the Multiple Sessions test title to display its details in the Results panel.

The RGS Diagnostic tool can be run any time after RGS Sender installation. To execute, use Windows Explorer to display the RGS Sender installation folder and locate a program called rgdiag.exe with the RGS icon. On a 32-bit Windows system, this is normally located at:

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

On a 64-bit Windows system, this is normally located at:

```
C:\Program Files (x86)\Hewlett-Packard\Remote Graphics
Sender\rgdiag.exe
```

Double click the application to launch the diagnostic tool. If the tool runs while connected to the sender through Windows Remote Desktop, the RDP Session tests will fail. This is normal. Viewing the test results will show that the currently active Remote Desktop session caused the failure. The current session will prevent the sender from allowing further connections if attempted using usernames that differ from the current session.

- RGS Admin Tool: The RGS Admin Tool can be used to enable and disable automatic updates from OpenGL and Direct3D applications.

  On a 32-bit Windows system, this is normally located at:

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

  On a 64-bit Windows system, this is located at:

  ```
  C:\Program Files (x86)\Hewlett-Packard\Remote Graphics
  Sender\rgadmin.exe
  ```

  Double-click the application to launch the RGS Admin tool. This application must be run using an account with Administrator permissions.

Troubleshooting

Troubleshooting Usage and Performance

This section covers troubleshooting networking configuration, graphics, cpu, remote audio, and remote USB.

Troubleshooting Network Configuration

This section describes troubleshooting the network.

1. Image update rate appears slow:

   Troubleshooting network issues is difficult. Although the HP Remote Graphics Software is capable of excellent performance, if your network does not support the required bandwidth and latency, Remote Graphics Software will not run efficiently. If your network is not configured optimally, you may experience problems.

   The computer's NIC will auto-negotiate the network speed with the network switches that are present on the local network. The negotiated speed can vary from 10Mb half duplex (HD) to 10Gb full duplex (FD). Ideally most modern NICs and switches negotiate the highest possible speed available. In the real world, unless the network was carefully designed for maximum throughput, the settings in the NICs and switches will auto-negotiate to a sub-optimal speed. By understanding this effect, the NIC and switches can be configured properly such that the highest speed possible is achieved. If the NICs 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 NICs and switches can be hard-coded. You must be careful with these settings though. If they are not setup such that the NICs and switch settings complement each other, the network will operate with poor performance.

   - Configuring the NIC on Windows

     You change the link speed and duplex on Microsoft Windows by opening the Device Manager. Open up the Control Panel -> System -> Hardware Tab -> Device Manager button. Once the Device Manager dialog is open, click the + next to Network adapters. Then, right-click on the adapter that you want to change and select Properties. Click the Advanced tab. Each network adapter has its own properties/settings that can be changed. The property that affects the link speed and duplex is usually named "Link Speed & Duplex". Click that property. If you decide that Auto-negotiation is what you want, pick the Auto Detect entry in the "Value" box. If you want to hard-code the speed and duplex, always choose the fastest link your network can support and always choose the Full-duplex setting.

   - Configuring the NIC on Linux

On Linux systems, there are two tools that can be used (`mii-tool` & `ethtool`) to configure networking. If the `mii-tool` does not work for a particular system, use `ethtool`. Do the following to get and set the network characteristics on Linux:

To get the LAN characteristics for interface 0, as root, type:

```
$ /sbin/mii-tool eth0
```

or

```
$ /usr/local/sbin/ethtool eth0
```

To set the LAN characteristics for a 100 Mbit connection running full-duplex mode, as root, type:

```
$ /sbin/mii-tool -F 100baseTx-FD
```

or

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

- Configuring the NIC on HP-UX

  On HP-UX systems, do the following to get and set the network characteristics:

  To get the LAN characteristics type:

  ```
  $ /usr/sbin/lanadmin -x 0
  ```

  To set the LAN characteristics for a 100 Mbit connection running in full-duplex mode, as root type:

  ```
  $ /usr/sbin/lanadmin -X 100FD 0
  ```

Remote Graphics Software depends on low network latency and reasonably fast network bandwidth.

There are several methods to test and measure the network bandwidth, latency, and the number of hops between Sender and Receiver computers:

- Use the ping command to measure network latency. From a command prompt on Windows or a terminal window on UNIX, execute `ping hostname`. This will report the network latency.

  Note: Be sure the ping protocol (ICMP) is not blocked by a firewall. Windows can also be setup with IPSec filters - be sure there is no IPSec filter policy disabling ICMP traffic.

- Use Traceroute or tracert to measure the network latency between two systems. Traceroute will report the number of hops it takes to get to a system in addition to the network latency. (Traceroute is available on Unix systems; tracert is available on Windows systems.)

- Use ttcp to measure the network bandwidth. ttcp should be available here: `http://www.pcausa.com/Utilities/pcattcp.htm`

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

2. Can't connect from an RGS Receiver to a Linux Sender:

   The default on RedHat Linux is to bind the machine name to the 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.bigmoney.com
   ```

Troubleshooting Graphics and CPU Performance

The single most dominant factor impacting performance on the sender is the frame-buffer read performance of the graphics card. Frame-buffer read performance of at least ten frames-per-second is recommended for optimum performance of HP Remote Graphics Software.

The HP Remote Graphics Software uses the graphics card to accelerate the rendering of the image being displayed on the monitor. After the desktop on the remote system is modified, the Sender reads the rendered image from the frame-buffer, and then compresses and transmits the image to the Receiver.

On Windows systems, use BltTest to test the frame-buffer read performance of the server. This application is available here: `http://www.stereopsis.com/blttest/`.

If image updates from the Sender to the Receiver appear slow and erratic, the Sender might not be getting enough of the CPU to do timely image updates. If the Sender is running on a Windows operating-system, it can be an operating-system scheduling issue. Sometimes this can be resolved by increasing the process priority of the Sender. Please see the section Setting Sender Priorities for further details.

Troubleshooting Remote Audio

This section describes troubleshooting remote audio.

1. Disabling Audio on a Sender for Windows:

   Most audio devices will allow the sender speakers to be disabled while still allowing audio to arrive at the receiver. 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 arriving at the receiver. The Realtek audio device used in the HP xw4300 is known to have this issue. One possible solution when running the 32 bit version of Windows XP is to disable the audio device prior to installing the 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 sender will connect to the first audio device it detects, which may not be the device that is selected by the user.

2. RGS Receiver Audio Controls Are Disabled on a Receiver for Linux:

   The audio controls will be disabled when the receiver cannot open or communicate with the JACK audio server (jackd). The status can be determined with the hprgsaudio script:

   - `/opt/hpremote/rgreceiver/hprgsaudio status`

     This reports the existence of a user-owned jackd audio server.

   - `/opt/hpremote/rgreceiver/hprgsaudio start`

     This will attempt to manually start of the jackd audio server if it is not running.

   - `/opt/hpremote/rgreceiver/hprgsaudio stop`

     This will attempt to manually stop the jackd audio server if unused by rgreceiver.

   - `/opt/hpremote/rgreceiver/hprgsaudio restart`

     This will attempt to shutdown and restart jackd if possible.

   The hprgsaudio script should always be the preferred method of managing jackd.

   Note: Audio is not supported on HP-UX.

3. No Audio on Windows Receiver:

   Verify that your local audio device is working. The volume control slider on the Receiver should play the default beep when released. Make certain that the mute is not enabled. Refer to the Windows Sender Audio Installation section for information on selecting the mixer as the input line. Refer to the Windows Sender Audio Calibration for information on how to ensure the volume levels are not too low. Make sure the mute is not enabled on the Wave line of the sender or receivers Volume Control.

4. No Audio on Linux Receiver:

   Installations that fail to yield any sound should observe the following checklist:

   1. Verify the sender system is configured properly to use the correct recording device and is recording from the correct source.

2. Verify the JACK and ALSA components are installed and configured properly on the receiver system. To see if the modules are present, as root, type `/sbin/lsmod`. The modules show up as `snd-*-*` names. They usually appear by either direct loading or system initialization in the `/etc/modules.conf` [2.4 kernel] and `/etc/modprobe.conf` [2.6 kernel]. Examine these files for extraneous or duplicate configuration lines.

3. Unset the channel "mute" and increasing "volume" settings with volume controls such as `/usr/bin/alsamixer` - channels are un-muted with the "`m`" command and volume is increased by using arrow keys in a terminal window.

4. Check alternate audio ports on your workstation with audio earphones (in case the speaker is not active or provided).

5. The chipset was unrecognized by the provided source bundles - visit the project sites to update your systems (after updating the script `rgs_audio_support`).

6. On some sound hardware, ALSA mixer controls do not work as expected. Try running `alsamixer` in a terminal window or your favorite sound mixer application. Manually adjust the volume sliders in conjunction with the volume slider in the Receiver's Control Panel. Sometimes a sound device “Master Volume” will get mapped to the wrong slider.

7. If you have a sound card installed in your system with multiple line-outs, be sure you are plugged into the correct one.

8. On some hardware, the headphones JACK might be inactive when running ALSA sound drivers. Try plugging into the line-out in the back of your machine.

5. Validating the JACK/ALSA installation on a Linux Receiver:

   When the RGS Receiver starts it invokes the jack sound server (`jackd`) in the background. When JACK is running it has control of the ALSA drivers on your system and prevents other applications from being able to access the ALSA drivers. Attempting to use another audio application that uses ALSA while the RGS Receiver is active may cause unknown behavior. The behavior could be observed as the audio from an application appearing to stop or causing the application to hang. The `rgreceiver.sh` script attempts to minimize the use of the `jackd` sound server.

   Users can check the state of the ALSA sound drivers by playing any WAV file. On most Linux installations there are WAV files in `/usr/share/sounds`. Use the simple ALSA player `/usr/bin/aplay` to test the audio. Be sure to try this when `rgreceiver.sh` is not in use and the RGS Receiver application has halted.

   The script hprgsaudio can determine the state of the JACK sound server (jackd). Users who own the jackd process can inquire:

   - `/opt/hpremote/rgreceiver/hprgsaudio status`

With ALSA working, users can validate JACK by performing the following steps:

1. Ensure that the ALSA device is properly configured and can be heard through the desired port, i.e., headphone jack, speaker, etc.
2. Determine that no other jackd process is running:
3. `ps -ef | grep jackd`

The following steps connect a simple beeping client to a JACK sound server daemon:

4. `jackd -d alsa hw:0 &  # start jackd`
5. `jack_metro -b 120 &  # audio client`
6. `jack_lsp -c    # display connections`
7. `jack_connect "metro:120_bpm" \ "alsa_pcm:playback_1"`

   Note: jack_lsp may suggest an alternate PCM playback channel based on your hardware - use that for the jack_connect command

Other JACK tutorial ideas can be found at:

`http://dis-dot-dat.net/jacktuts/starting/compiling.html`

6. Cannot connect to running jackd process on Lunux Receiver:

   You may not own the executing sound server process (i.e., your user Ids (UID) may not match). Currently JACK systems only support client-server combinations where the UIDs match. If UIDs do not match, you will often see a client connection failure message:

   `jack server not running?`

Troubleshooting Remote USB

HP Remote Graphics Software supports a Remote USB capability. This allows a user to connect any number of USB devices to a local RGS Receiver system and have the devices appear connected to the RGS Sender system.

Currently only a single Sender can receive the Remote USB device connections. If you have problems connecting a Remote USB device, the following checklist may help to identify the problem:

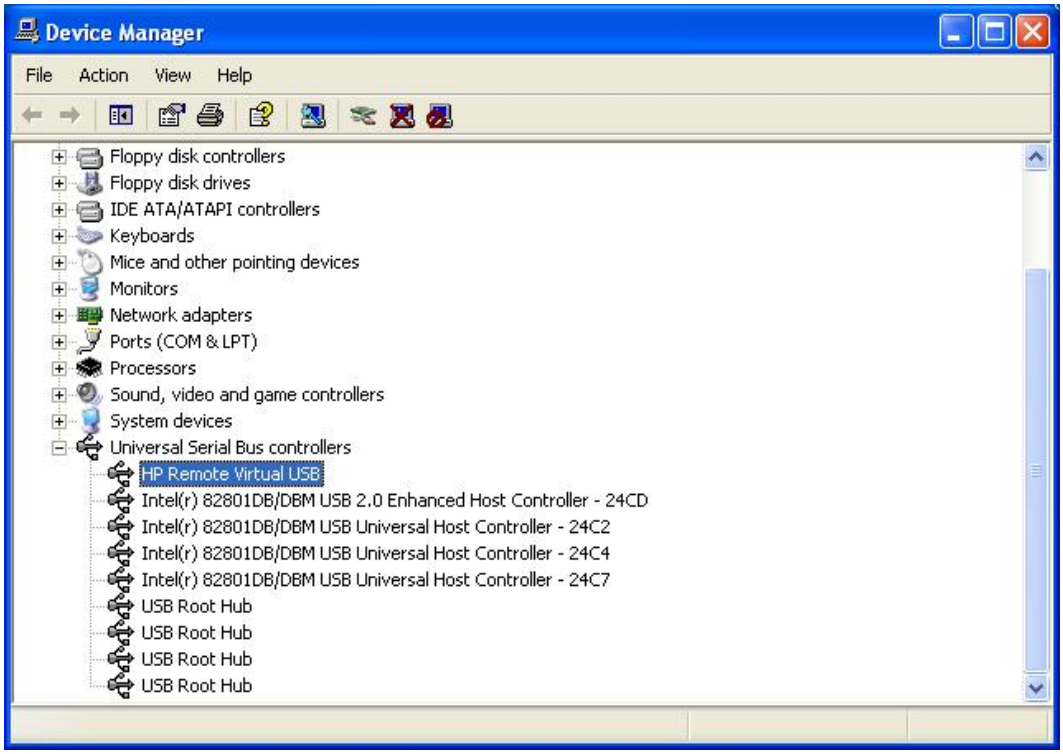
1. HP Blade Workstations Only:

   Remote USB is only supported on an HP Blade Workstation Client receiver system connected to a HP Blade Workstation sender system. In addition, the Sender and Receiver versions must match. See the USB Remote Requirements section for further details.

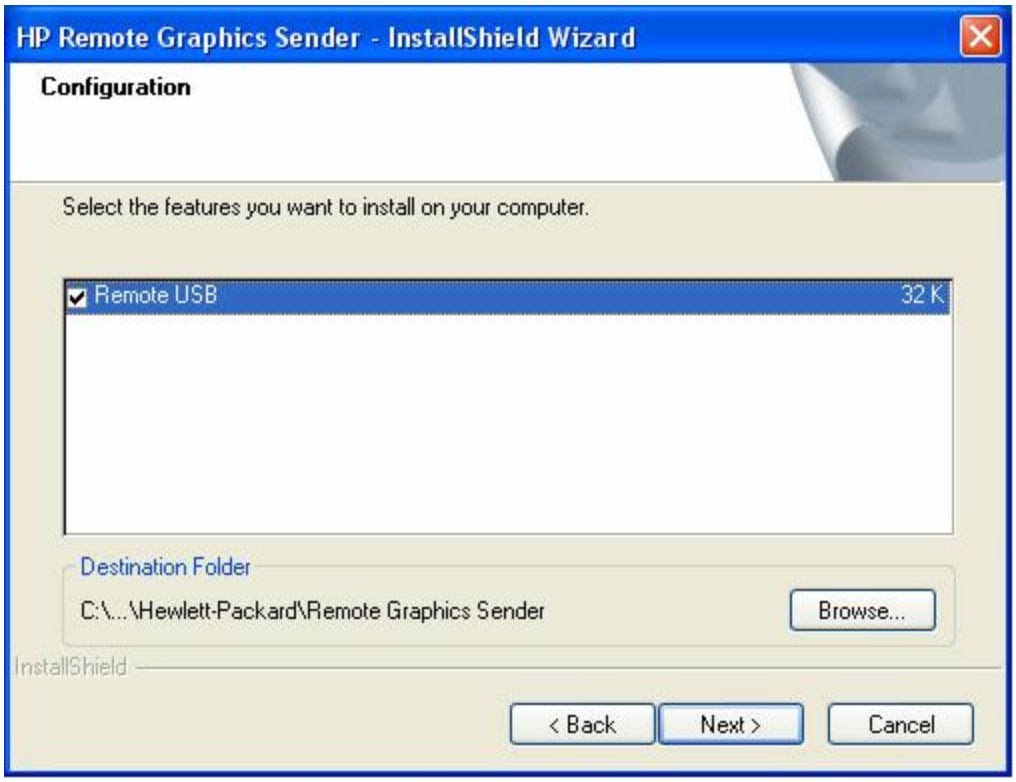
2. HP Remote Virtual USB Driver:

   Verify that the HP Remote Virtual USB driver is installed and active on the HP Remote Graphics sender system. Open the Windows XP Device Manager and

verify that HP Remote Virtual USB is listed under Universal Serial Bus Controllers. The following panel shows the HP Remote Virtual USB is properly installed and configured.

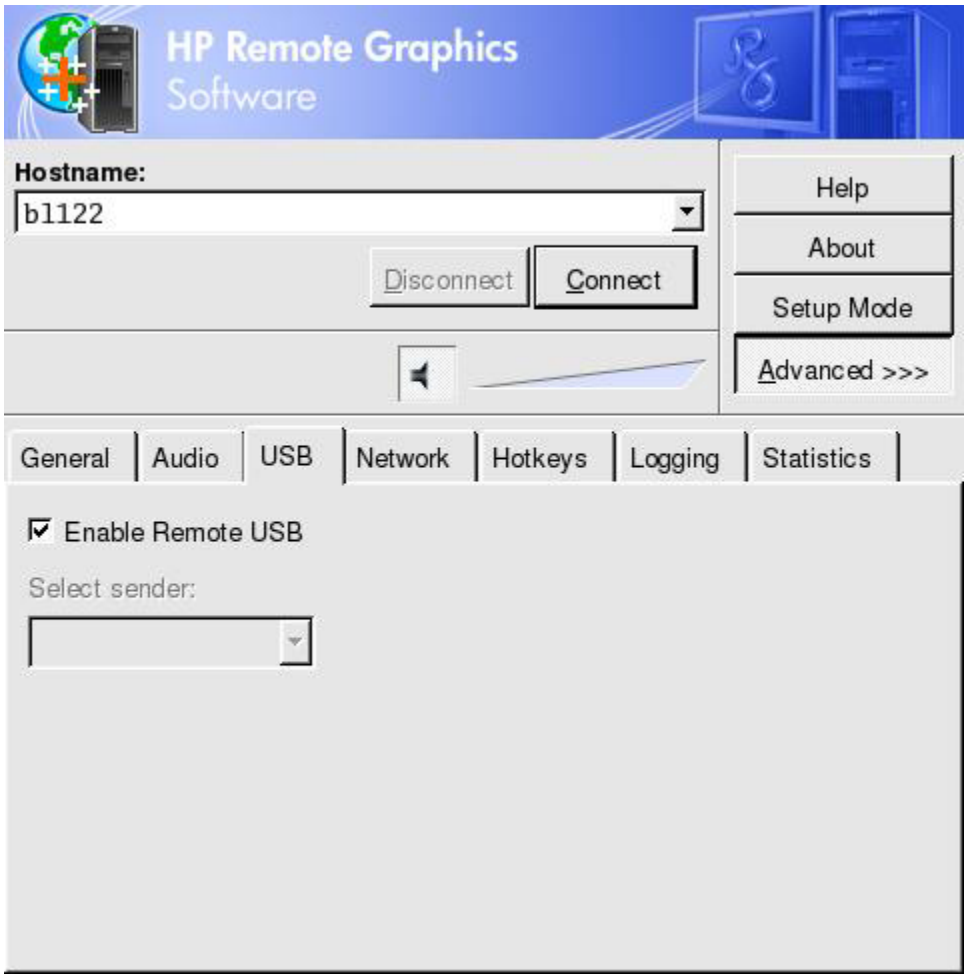


If the driver is not reported, reinstall the RGS Sender Software on the HP Blade Workstation sender system. During installation, verify that the Remote USB box is checked in the Configuration window as shown in the next panel:



3. Enable Remote USB:

   Verify that the receiver has enabled Remote USB. Make certain that the "Enable Remote USB" box is checked under the USB option tab of the RGS Control Panel as shown below:



4. Supported USB Devices:

   Verify that the USB device is supported for remote connection. Not all USB devices are supported by the current version of HP Remote Graphics Software.

5. USB Device Drivers and Program Support:

   Verify that the device drivers and programs required by the device are installed and available on the Sender system. 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.

6. Check USB cable Connections:

   Verify that the USB device is physically connected to the Receiver system. Check to see that it has power and is turned on. Some devices may require that the user initiate an action before it connects. For example, Palm PDA devices require starting a HotSync operation for the device to connect and appear on the remote Sender system.

   To further verify your connections, recognized devices on the Receiver system 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:

a. `/proc/devices/usb_remote/devices` - File contains a list of recognized devices by the Receiver system.

b. `/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.

7. Directory Mode and Enterprise Service Mode:

   If running in Directory Mode or Enterprise Service mode, the sender system must be selected before connecting to any systems. If a different sender system is required after connection, then all systems must be disconnected, a new sender system selected in the Receiver Control Panel, and then all senders can be reconnected.

8. Reset the USB Device:

   Press the reset button on the device if it has a reset button. If the device has entered into a bad state, it may fail to connect. Pressing the reset may allow the device to connect.

Known Issues and Limitations

This section describes a list of known issues and limitations of the HP Remote Graphics Software.

General Issues:

1. Switching Network Interfaces:

   The Sender does not transition well when switching network interfaces or hopping from one network interface to another. The Sender must be re-started so that it can re-discover the correct interface.

2. Multi-homed Systems:

   Receivers that run on systems that are multi-homed might not work correctly. The following multi-homed scenarios are presented:

   - Suppose a laptop is connected into the LAN through an Ethernet NIC with a CAT5 cable and another Wireless NIC running 802.11b. When the Receiver running on the laptop connects to the Sender, the system sometimes gets confused as to what NIC should support the connection. Disabling one of the NICs will allow the Receiver to properly connect to the Sender.

   - The Sender is running on a system that is using the LAN through an Ethernet NIC with a CAT5 cable. Then, if the LAN cable is unplugged and a Wireless NIC is started, the Sender will no longer function properly, since it is listening to connections from RGS Receivers on a "dead" NIC. Simply restarting the RGS Sender will enable the Sender to use the Wireless NIC, and will allow the RGS Receiver to connect again.

   - Suppose a Sender is running on a machine with two Ethernet NICs, where each NICs is using a CAT5 cable. The NIC that is listed first, for example when the Windows command `ipconfig /all` is run, will be the NIC that the Sender binds to. If it is desirable that the Sender runs using the other NIC, change the binding order of the NIC in the system. On Windows this is done by bringing up the "Network Connections" dialog in the Control Panel. In the Advanced menu, select "Advanced Settings" to bring up the "Advanced Settings" dialog. Select the "Adapter and Bindings" tab. Here you can move the preferred NIC to the top of the binding order.

3. Remote Audio Issues:

   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 Sender will capture 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 sender and will not be transmitted.

Audible Pops and Glitches in Sound:

Most likely this is because the network bandwidth and 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 sender detects an audio signal, that signal is sent to the receiver. If the audio device on the sender 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 get interpreted as an audio signal and get sent to the receiver. This may occur when something is connected to the "Line In" port of the audio device. Reducing volume levels or disconnecting these external devices may help reduce the interference.

4. Network Timeout Issues:

   The Remote Display Window repeatedly dims out and displays a connection warning message:

   This is likely caused by frequent network disruptions between the Receiver and Sender. The dimming of the display serves as a notification to the end-user that the Remote Display Window may reflect stale information. If frequent notifications are annoying and the network issues do not improve, then the user should refer to the section “Using Timeouts” and adjust the Receiver’s warning timeout value found on the Receiver Control Panel or the property Rgreceiver.Network.Timeout.Warning.

   The Remote Display Window dims, the Receiver disconnects, and it displays a “Connection closed” error dialog, but the user can often immediately connect in again:

   Most likely network connectivity between the Receiver and Sender was temporarily lost for some reason. Other possibilities include

   - the Sender has ungracefully terminated
   - the Sender system experienced some sort of failure
   - the Sender system’s cpu utilization prevented the Sender from making progress, or
   - the length of this connectivity loss exceeds the Receiver’s error timeout value, controlled by the Receiver’s

Rgreceiver.Network.Timeout.Error property so the Receiver disconnected.

If this condition persists, then it is likely that network disruptions are exceeding the Receiver's error timeout value. If this is a network issue and is not resolvable, then the user might consider adjusting the error timeout of the Receiver to reduce Receiver disconnection. Additionally, the Sender timeout might need to be increased too. Please refer to the section Using Timeouts for further details.

When connecting to a Linux or HP-UX system, the PAM authentication dialog displayed by the Receiver does not appear long enough to enter the user's credentials such as username and password:

This is likely caused by too small of a Receiver's dialog timeout value. Please refer to the section "Using Timeouts" for further details on setting timeouts. The user should first check the Receiver Control Panel to determine the Network dialog timeout setting and adjust as appropriate.

When connecting to a Sender, the authorization dialog is not displayed long enough for the user to respond to it:

This is likely caused by too small of a Sender's dialog timeout value. Please refer to the section Using Timeouts for further details on the property Rgsender.Network.Timeout.Dialog. The default value for this property is 15 seconds.

When connecting to a Linux or HP-UX system 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, or
- the timeouts are too short.

Please refer to the section Installing the Sender to understand if PAM is correctly configured. Please refer to the section Using Timeouts for further details on setting timeouts. The user could try increasing the Receiver's network dialog timeout as well as the 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:

Most likely a network disruption. The user can adjust the warning timeout to get notification when this occurs. The user 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. Please refer to the section Using Timeouts for further details on setting the Receiver timeouts.

Increasing the Receiver error dialog timeout doesn't appear to have an effect and the Receiver still disconnects:

Either a network failure results in detecting lost connectivity by the Receiver (resulting in disconnected connections) or the Sender's timeouts are shorter than the Receiver's timeouts and the Sender disconnects the 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 system determines that network connectivity is lost and an error returns by the network stack to the Receiver, then the connection will disconnect sooner than the error timeout setting. If the Sender's timeout values are shorter than the Receiver's, then the Sender may close the connection sooner than the Receiver, disconnecting the Receiver. If the issue continues, the user can consider increasing the Sender's error timeout value. Please refer to the section Using Timeouts for further details on setting timeouts.

Microsoft Windows Specific Issues:

1. Cannot Connect to Sender:

   There are several common system setup issues that can prevent a connection to the RGS Sender. The RGS Diagnostic Tool programmatically detects some of these problems and suggests possible solutions. Please refer to the RGS Diagnostic Tool section.

2. Guest Login Access:

   By default, Microsoft Windows XP allows any user who can access your computer over the network to login with Guest access. We believe this represents a security risk. 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". Click here for more information on this issueGo to http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/lpe_overview.mspx for more information on this issue.

3. Blank Password:

   The RGS Sender will not allow a connection for an account with a blank or undefined password. All accounts on the machine running the RGS Sender should have password protection prior to connection.

4. Microsoft XP SP2 Firewall:

   Installation of Microsoft Windows XP SP2 prevents Remote Graphics Software from starting. Microsoft Windows XP SP2 by default enables a firewall. When the Receiver trys to connect to a Sender, if the firewall is not configured correctly, the firewall will ask the user to allow the connection. On the Sender, the firewall blocks the Sender from starting. This can also be configured. Please refer to the engineering advisory(http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp

?objectID=PSD_WO040917_CW01) for more details on how to resolve this issue.

5. OpenGL Applications Not Starting:

   Previous versions of HP Remote Graphics required the manual placement of the HP Remote Graphics `OpenGL32.dll` library into the application's directory. This library may cause some applications to fail on startup. Automatic updates of OpenGL applications are now supported and the HP Remote Graphics `OpenGL32.dll` library is no longer required. See Enabling OpenGL Applications On Windows for more details.

   If the use of the HP Remote Graphics `OpenGL32.dll` is still required (the method for enabling automatic 3D updates is disabled), some OpenGL applications (e.g.: PTC ProEngineer or Google Earth) will not start with the Window's HP Remote Graphics Software Sender installed.

   Only the following versions of ProEngineer are compatible with Remote Graphics `OpenGL32.dll`:

   Pro/E Wildfire 2.0 - all datecodes

   Pro/E WildFire 1.0 - datecodes 2003051 or later

   Pro/E 2001 - datecodes 2004290 or later

6. Accelerated DirectDraw Not Available:

   The HP Remote Graphics Driver will cause accelerated DirectDraw to become disabled. Many DirectDraw applications though, will continue to work as expected. Your mileage may vary.

7. Video Overlay Planes Are Not Supported:

   Video overlay planes are not supported. Some media players that use video overlay planes will not update. This can often be resolved by disabling the use of video overlay planes in the media player.

8. OpenGL Overlay Planes Are Not Supported:

   OpenGL overlay planes are not support using RGS Sender for Windows. The use of overlay planes can be often be disabled.

9. Full-screen and DOS Applications Are Not Supported:

   Full-screen applications, such as DOS prompts and games, are not supported. If you attempt to create a full-screen DOS window, the window will be reset to the normal size.

10. Inability to Connect to Senders on HP xw6200 and xw8000 System:

    Connections to the Sender may not appear to work on HP xw8200/xw6200 systems. This can sometimes be related to Microsoft Window's APIPA (Automatic Private IP Addressing). APIPA can cause the Remote Graphics Sender to open sockets on private IP addresses. The private IP addresses are not visible from the RGS Receiver so connections will not work. You can verify if the Sender is using private IP addresses by typing `netstat -n -a` in a

command window. If the IP address associated with the Sender ports (listening port 42966) are private, then APIPA is probably at fault. Consult the Microsoft's APIPA WEB site for further information, including how to disable APIPA here(http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/Default.asp?url=/resources/documentation/windows/xp/all/reskit/en-us/prjj_ipa_eiih.asp).

11. Remote Cursors Not Available During Login:

    When a user on the Sender system is using the mouse on the Login Desktop, mouse updates will not be visible on any Receiver.

12. Remote Audio Issues:

    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 receiver because it is played through the PC Speaker. See the section on PC Speaker Sounds Not Working.

    No Audio With Multiple Audio Devices:

    The HP Remote Graphics Software sender will open up the device that is registered as the default audio device. The sender is a service that is running in a different context. If you have multiple audio devices, it may choose a different device than what the user has selected as the default. Disable the extra audio device to ensure the sender uses the correct device. See the Windows Sender Audio Installation section to setup the audio device after disabling the extra audio device.

13. Image updates from the Sender to the Receiver appear slow and erratic:

    For example, rotating a model in a 3D mechanical design program using the mouse appears sluggish and image updates are inconsistent. One possible reason for the problems is network performance. If the Sender is running on a Windows operating-system, it can be an operating-system scheduling issue. Sometimes this can be resolved by increasing the process priority of the Sender. Please see the section Setting Sender Priorities for further details.

14. Easy Login Connections Don't Seem to be Enabled:

    There are several common system setup issues that can prevent an Easy Login connection to the RGS Sender. The RGS Diagnostic Tool programmatically detects some of these problems and suggests possible solutions. Please refer to the RGS Diagnostic Tool section.

Linux or HP-UX Specific Issues:

1. Hidden Receiver Control Panel:

   The 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 Receiver control panel will not, by default, show up in

all desktops. Read the Setup Mode section to learn how to bring the Receiver control panel to the front.

2. Geometry Feedback Window And Performance:

   Performance of window moves using a HP-UX Sender over a low-bandwidth network connection is slow. This is related to the geometry feedback window placed on top of the window that you are moving. This can be resolved by disabling the geometry feedback window or moving the geometry feedback window to a corner of the screen. Read the Optimizing Performance section to learn how to relocate the feedback window.

3. 3D Animation Loops And Performance (Linux only):

   When sharing an application that is running a 3D animation loop, such as a continuously rotating object, the application seems to run smoothly at first for a period of time (5 to 30 seconds), and then abruptly slows down. It will run smoothly, then stop, then run smoothly again, then stop again, over and over. The periodicity of the abruptness is around 1 to 2 seconds. The interval of stopping is around 250 msec and is quite noticeable.

   The problem is with the Linux scheduler, such that after a period of time, the scheduler decides to give the animation loop process a higher priority and therefore more CPU cycles, which effectively gives the X server process less cycles. To temporarily fix the problem, simply reduce the priority of the animation loop process (i.e. - "`renice priority pid`"). By default, priority is set to 0. Simply bump the priority one at a time until the application runs smoothly again.

4. Full-screen Crosshair Cursors:

   Some applications that use large crosshair cursors (e.g.: PTC's ICEM Surf - uses a full-screen crosshair cursor) don't display correctly on the Receiver. The full-screen crosshair cursors can be disabled by typing the following a terminal window:

   ```
   /usr/contrib/bin/X11xprop -root -remove
   _SGI_CROSSHAIR_CURSOR
   /usr/contrib/bin/X11xprop -root -remove _HP_CROSSHAIR_CURSOR
   ```

   This will force the application to use a real X cursor, which will display correctly on the Receiver.

5. Gamma Correction On Receiver:

   The gamma in a 3D Application on the Sender can look incorrect when displayed on a Receiver. This is because the gamma of the Receiver's monitor does not correctly match the gamma of the monitor on the Sender. 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. Those that can adjust only the Receiver's window will provide the best results.

6. Transparent Overlay Windows (aka Glass-bottom windows) Are Not Supported (HP-UX only):

Transparent Overlay Windows - Certain applications, primarily 3D applications, create windows in the overlay planes that entirely cover the main application windows that exist in the image planes. These overlay windows are primarily transparent and are used to contain text or other rendered images that should not be drawn into the image planes of the application. These overlay transparent windows are also called glass-bottom windows, as they can be used to "see into" the image planes. Applications that use glass-bottom windows do not currently share well with Remote Graphics Software.

This problem is present only on HP-UX systems with graphics devices that 1) support overlay planes, 2) have the overlay planes enabled, and 3) run applications that create glass-bottom windows. As a work-around, to enable these applications to share properly over a Remote Graphics Software connection, the overlay planes can be disabled. Most applications will still run correctly with the overlays disabled. To disable the overlays, the X server's configuration file must be edited. The following table shows where the various configuration files exist:

X server (platform)	Configuration File
Xhp (PA HP-UX)	/etc/X11/X0screens
Xf86 (PA HP-UX)	/etc/X11/XF86Config

The following X0screens entries will disable the overlays for an Xhp X server:

```
Screen /dev/crt
    ScreenOptions
          SuppressPseudoColorOverlayVisual
```

The following XF86Config entries will disable the overlays for an Xf86 X server running ATI Fire GL-UX graphics:

```
Section "Device"
    Identifier      "hp Fire GL-UX"
    Driver          "firegl123"
    VendorName      "hp"
    BoardName       "Fire GL-UX"
    Card            "Fire GL-UX"
    Option          "Overlay"      "false"
    Option          .... other options ....
#EndSection
```

7. Remote Audio Issues (Linux only):

   ALSA Quirks:

   ALSA drivers can have problems mapping correct mixer channels to the correct sliders. This means that on some more advanced or proprietary sound hardware, the “Master Volume” control might incorrectly get mapped to the “Headphones” slider or “Wave Mix” slider for example. The Receiver tries to do its best to remedy these situations by adjusting common sliders like “PCM,” “WAVE,” and “LINE” to appropriate levels, then attaching the volume slider to “Master Volume” and the “Headphone” mixer channels. This should

work for most systems… but if not, try manually playing with mixer settings via the `alsamixer` in a terminal window or via your favorite mixer application.

JACK Sound Server:

JACK is a sound server that interfaces with the ALSA drivers. Once installed and configured on your machine, this is your sound.

8. User-started X environments (startx) 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 init-level 5 of the X server.

9. Improperly configured /etc/hosts table (Linux only):

   The default on RedHat Linux is to bind the machine name to the 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.bigmoney.com
   ```

10. Advanced Linux Sound Architecture (ALSA) support:

    Release 4.0.0 for Linux requires Advanced Linux Sound Architecture (ALSA) support to be installed prior to RGS installation. If the RGS installation script runs on a system without ALSA installed, the subsequent JACK Audio Connection Kit (JACK) built will not be compatible with ALSA loaded anytime after the fact. If this occurs, first install the necessary ALSA support drivers and libraries and then re run the JACK install script as:

    ```
    /opt/hpremote/rgreceiver/hp_rgs_4_audiosupport/rgs_audio_sup
    port  install
    ```

    and answer "yes" to the prompts to re-install JACK.

For information on any additional issues and limitations, see the release notes on the HP Remote Graphics Software CD.

Error Messages

The following table lists the errors that are reported by the HP Remote Graphics Software Receiver.

Error	Description
Connection lost!	The RGS Sender has closed the connection. Possible reasons include: 1. The Sender may have explicitly disconnected your connection. For example a user may have selected disconnect all connections from the Sender icon or Sender GUI or the user may have logged off. 2. Another user has connected to the Sender using the same username and password. 3. If you connected to a desktop that was not logged in and another user logged in your connection will be disconnected. 4. If you were connected to a logged in desktop and the logged in user disconnects your connection will be disconnected too. 5. The network may have been disconnected, closed, or temporarily disrupted. 6. The Sender service/daemon may have been stopped, re-started, or killed. 7. The Sender system may have been stopped/shutdown, or re-started. 8. If connecting to a UNIX system the X Server may have been stopped or re-started. 9. The Sender or X Server may have experienced a failure.
Unable to connect to Sender!	1. The Receiver is unable to find the hostname or IP address that was entered. Verify that the hostname or ipaddress that you entered is correct. If this does not correct the problem then make sure you can reach the Sender over the network. Opening a Command Prompt, then execute: *ping hostname* or

	`ping` *`IP address`* If no ping reply is received, the Sender is unreachable or is not running. If a ping reply is received, the Sender software may not be running on the remote computer. 2. A Sender is not running on the system you are attempting to reach. Verify that the Sender is running on the system. 3. The Sender system is not started or connected to the network. You could try a basic connectivity test, such as ping. 4. The network is not configured correctly. For example, DNS may not have resolved the name of the Sender system correctly or your /etc/hosts file, if using UNIX, does not have the proper ipaddress mapped to the hostname. Try entering the ipaddress of the Sender. 5. The Sender is started and listening on a different network interface than the one you are attempting to reach. This could be the case if the Sender system has multiple NICs, it is a multi-homed system, or there is a virtual ethernet device installed. If this is true you may need to specify the binding order of hostnames to ipaddress. 6. If you are attempting to connect to a UNIX system you may have entered an incorrect screen number. 7. If the Sender system has changed networks and been assigned a new ipaddress after the Sender was started then you'll need to re-start the Sender service/daemon.
Authentication failed!	The Remote Graphics Software Sender has refused to allow a connection. Possible reasons include the following: 1. The authentication credentials that you entered, such as domain name, user name and password, are not valid or recognized by the Sender system. 2. The Sender's authentication is not configured appropriately. Please consult the User's manual and README.txt for the latest directions and issues with respect to configuring authentication.

Directory not found or not accessible!	The directory file is not available. Possible reasons include: 1. The directory file name or location has been mistyped. 2. The file has been moved or is no longer available. 3. The network is down or experiencing a disruption. 4. The user does not have read permission on the file.
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: 1. The username entered in the directory file does not exactly match the real username. 2. 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.
Authorization failed!	The connection was authenticated, but another user is already logged into the desktop of the Sender system. When a connection is attempted to another user's desktop, a dialog is displayed on the Sender 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: Receiver License Not Found!	A license was not found for the RGS Receiver.
Error: Receiver License Invalid!	The license is invalid for the RGS Receiver.
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	The license has expired for the RGS Sender.

to!	
Error: License Invalid for the sender you are trying to connect to!	The license is invalid for the RGS Sender.
Could not create an Enterprise Directory Session!	The Receiver was started in Enterprise Service Mode and it could not connect to the RGS Enterprise Service. There are several possibilities including the following: • The hostname or ipaddress of the RGS Enterprise Service specified on the command line is incorrect. • The RGS Enterprise Service is not running.
Authentication to the Enterprise Directory Service failed!	The Receiver was started in Enterprise Service Mode and the user was not authenticated. There are several possibilities including the following: • The user entered incorrect credentials. • The Enterprise Service cannot validate the users credentials.
Could not lookup the users systems on the Enterprise Directory Service!	The Receiver was started in Enterprise Service Mode, but the user was not found.
No systems were assigned to the user in the Enterprise Directory Service!	The Receiver was started in Enterprise Service Mode, but no systems were assigned to the user.
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, property configuration file, or RGS Enterprise Service, 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, property configuration file, or RGS Enterprise Service, is invalid and the property Rgreceiver.Hotkeys.IsMutable is disabled. Therefore hotkeys have been disabled.
Connection denied! The iLO remote console is enabled.	The iLO remote console is enabled on the HP Blade Workstation. The Blade must be configured in User Mode before connections are allowed.
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 pubic IP address and is not blocked by a firewall.	The Receiver was able to lookup and resolve the specified hostname or IP address. However, the Receiver was unable to establish a connection to the Sender. There are several possibilities such as the Sender is not installed, the Sender is not running, the Sender is listening on the wrong network interface, or a firewall is blocking the Sender.

License and Support

End-user License Agreement

PLEASE READ CAREFULLY BEFORE USING THIS EQUIPMENT:

This End-User license Agreement ("EULA") is a legal agreement between (a) you (either an individual or a single entity) and (b) Hewlett-Packard Company ("HP") that governs your use of any Software Product, installed on or made available by HP for use with your HP product ("HP Product"), that is not otherwise subject to a separate license agreement between you and HP or its suppliers. Other software may contain a EULA in its online documentation. The term "Software Product" means computer software and may include associated media, printed materials and "online" or electronic documentation. An amendment or addendum to this EULA may accompany the HP Product.

RIGHTS IN THE SOFTWARE PRODUCT ARE OFFERED ONLY ON THE CONDITION THAT YOU AGREE TO ALL TERMS AND CONDITIONS OF THIS EULA. BY INSTALLING, COPYING, DOWNLOADING, OR OTHERWISE USING THE SOFTWARE PRODUCT, YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT ACCEPT THESE LICENSE TERMS, YOUR SOLE REMEDY IS TO RETURN THE ENTIRE UNUSED PRODUCT (HARDWARE AND SOFTWARE) WITHIN 14 DAYS FOR A REFUND SUBJECT TO THE REFUND POLICY OF YOUR PLACE OF PURCHASE.

1. GRANT OF LICENSE. HP grants you the following rights provided you comply with all terms and conditions of this EULA:

a. Use. You may use the Software Product on a single computer ("Your Computer"). If the Software Product is provided to you via the internet and was originally licensed for use on more than one computer, you may install and use the Software Product only on those computers. You may not separate component parts of the Software Product for use on more than one computer. You do not have the right to distribute the Software Product. You may load the Software Product into Your Computer's temporary memory (RAM) for purposes of using the Software Product.

b. Storage. You may copy the Software Product into the local memory or storage device of the HP Product.

c. Copying. You may make archival or back-up copies of the Software Product, provided the copy contains all of the original Software Product's proprietary notices and that it is used only for back-up purposes.

d. Reservation of Rights. HP and its suppliers reserve all rights not expressly granted to you in this EULA.

e. Freeware. Notwithstanding the terms and conditions of this EULA, all or any portion of the Software Product which constitutes non-proprietary HP software or software provided under public license by third parties ("Freeware"), is licensed to you subject to the terms and conditions of the software license agreement accompanying such Freeware whether in the form of a discrete agreement, shrink wrap license or electronic license terms accepted at time of download. Use of the

Freeware by you shall be governed entirely by the terms and conditions of such license.

f. Recovery Solution. Any software recovery solution provided with/for your HP Product, whether in the form of a hard disk drive-based solution, an external media-based recovery solution (e.g. floppy disk, CD or DVD) or an equivalent solution delivered in any other form, may only be used for restoring the hard disk of the HP Product with/for which the recovery solution was originally purchased. The use of any Microsoft operating system software contained in such recovery solution shall be governed by the Microsoft License Agreement.

2. UPGRADES. To use a Software Product identified as an upgrade, you must first be licensed for the original Software Product identified by HP as eligible for the upgrade. After upgrading, you may no longer use the original Software Product that formed the basis for your upgrade eligibility.

3. ADDITIONAL SOFTWARE. This EULA applies to updates or supplements to the original Software Product provided by HP unless HP provides other terms along with the update or supplement. In case of a conflict between such terms, the other terms will prevail.

4. TRANSFER.

a. Third Party. The initial user of the Software Product may make a one-time transfer of the Software Product to another end user. Any transfer must include all component parts, media, printed materials, this EULA, and if applicable, the Certificate of Authenticity. The transfer may not be an indirect transfer, such as a consignment. Prior to the transfer, the end user receiving the transferred product must agree to all the EULA terms. Upon transfer of the Software Product, your license is automatically terminated.

b. Restrictions. You may not rent, lease or lend the Software Product or use the Software Product for commercial timesharing or bureau use. You may not sublicense, assign or transfer the license or Software Product except as expressly provided in this EULA.

5. PROPRIETARY RIGHTS. All intellectual property rights in the Software Product and user documentation are owned by HP or its suppliers and are protected by law, including but not limited to United States copyright, trade secret, and trademark law, as well as other applicable laws and international treaty provisions. You shall not remove any product identification, copyright notices or proprietary restrictions from the Software Product.

6. LIMITATION ON REVERSE ENGINEERING. You may not reverse engineer, decompile, or disassemble the Software Product, except and only to the extent that the right to do so is mandated under applicable law notwithstanding this limitation or it is expressly provided for in this EULA.

7. TERM. This EULA is effective unless terminated or rejected. This EULA will also terminate upon conditions set forth elsewhere in this EULA or if you fail to comply with any term or condition of this EULA.

8. CONSENT TO USE OF DATA. You agree that HP and its affiliates may collect and use technical information you provide in relation to support services related to the

Software Product. HP agrees not to use this information in a form that personally identifies you except to the extent necessary to provide such services.

9. DISCLAIMER OF WARRANTIES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, HP AND ITS SUPPLIERS PROVIDE THE SOFTWARE PRODUCT “AS IS” AND WITH ALL FAULTS, AND HEREBY DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, EITHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF TITLE AND NON-INFRINGEMENT, ANY IMPLIED WARRANTIES, DUTIES OR CONDITIONS OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, AND OF LACK OF VIRUSES ALL WITH REGARD TO THE SOFTWARE PRODUCT. Some states/jurisdictions do not allow exclusion of implied warranties or limitations on the duration of implied warranties, so the above disclaimer may not apply to you in its entirety.

10. LIMITATION OF LIABILITY. Notwithstanding any damages that you might incur, the entire liability of HP and any of its suppliers under any provision of this EULA and your exclusive remedy for all of the foregoing shall be limited to the greater of the amount actually paid by you separately for the Software Product or U.S. $5.00. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL HP OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT, OR OTHERWISE IN CONNECTION WITH ANY PROVISION OF THIS EULA, EVEN IF HP OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF THE REMEDY FAILS OF ITS ESSENTIAL PURPOSE. Some states/jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

11. U.S. GOVERNMENT CUSTOMERS. 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 HP's standard commercial license.

12. COMPLIANCE WITH EXPORT LAWS. You shall comply with all laws and regulations of the United States and other countries ("Export Laws") to assure that the Software Product is not (1) exported, directly or indirectly, in violation of Export Laws, or (2) used for any purpose prohibited by Export Laws, including, without limitation, nuclear, chemical, or biological weapons proliferation.

13. CAPACITY AND AUTHORITY TO CONTRACT. You represent that you are of the legal age of majority in your state of residence and, if applicable, you are duly authorized by your employer to enter into this contract.

14. APPLICABLE LAW. This EULA is governed by the laws of the State of California, U.S.A.

15. ENTIRE AGREEMENT. This EULA (including any addendum or amendment to this EULA which is included with the Product) is the entire agreement between you and HP relating to the Software Product and it supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to the Software Product or any other subject matter covered by this EULA. To the extent the terms of any HP policies or programs for support services conflict with the terms of this EULA, the terms of this EULA shall control.

Rev. 10/03

355096-001

Amendment to End User License Agreement For HP Remote Graphics Software

For HP Remote Graphics Software, Section 1.a. is replaced by the following:

1.a. Use. You may use the Software Product on a single computer (“Your Computer”) which is supported by the Software Product. If the Software Product is provided to you via the internet and was originally licensed for use on more than one computer, you may install and use the Software Product only on those computers. You may not separate component parts of the Software Product for use on more than one computer. You do not have the right to distribute the Software Product. You may load the Software Product in Your Computer’s temporary memory (RAM) for purposes of using the Software Product.

382263-003

Contacting HP

Technical Support

For technical support, visit our web site here:
`http://welcome.hp.com/country/us/en/support.html`.

Corporate Headquarters

Hewlett-Packard
3000 Hanover Street
Palo Alto, CA 94304-1185 USA
Phone: (650) 857-1501
Fax: (650) 857-5518

Open between 8:00 a.m. and 5:00 p.m. Pacific Time, Monday through Friday.

Regional Headquarter Offices

For the HP sales office nearest you, please refer to your local phone directory, or call the HP sales office in your region.

Latin America
Hewlett-Packard
Waterford Building, 9th Floor
5200 Blue Lagoon Drive
Miami, Florida 33126 USA
Phone: (305) 267-4220

Open between 8:00 a.m. and 6:00 p.m. local time, Monday through Friday.

Europe, Africa, Middle East
Hewlett-Packard
Route du Nant-d'Avril 150
CH-1217 Meyrin 2
Geneva, Switzerland
Phone: (41/22) 780-8111

Open between 9:00 a.m. and 6:00 p.m. local time, Monday through Friday.

Asia Pacific
Hewlett-Packard Asia Pacific Ltd.
Hewlett-Packard Hong Kong Ltd.
19/F, Cityplaza One
1111 King's Road
Taikoo Shing
Hong Kong
Phone: (852) 2599-7777

Open between 9:00 a.m. and 6:00 p.m. local time, Monday through Friday.