ICE RemoteWare Documentation

Release 15.1.0

Penguin Solutions

Aug 13, 2025

CONTENTS

CHAPTER

ONE

ICE REMOTEWARE PREREQUISITES

Learn more about the server and client requirements for using the ICE RemoteWare™ product.

1.1 About the ICE RemoteWare Software

ICE RemoteWare 15.1.0, commit 9c8756db1e26e37c7ad733dca2bc51921059c79f.

1.2 Introduction

The ICE RemoteWare product is a web server that provides secure, easy remote access to teams working on Linux, Windows, and MacOS workstations through standard web browsers, eliminating the need for client-side installations and changes to firewall policies.

1.3 Server Requirements

This section describes the hardware and software requirements for the workstation hosting the ICE RemoteWare server.

1.3.1 Server OS

The ICE RemoteWare software is supported and tested on the following 64-bit operating systems:

- Rocky Linux 8 and 9
- Windows 10, 11, and Windows Server 2019
- Windows Server 2022 (server-side only)
- MacOS Monterey 12 to MacOS Sonoma 14
- Ubuntu 20, 22 and 24

Important

Rocky Linux users: XWayland is not currently supported. Please see *Installing the Server on Rocky Linux* for instructions on enabling Xorg as the default X server.

Attention

There is a known graphics issue with older GNOME 3 Shell based systems (GNOME 3 and GDM) on machines that don't have an attached monitor. We recommend upgrading to GNOME 3.28+ or using the MATE desktop environment and LightDM as a workaround.

If you require other versions of Windows, RedHat, and Debian based flavors of Linux, please contact Penguin Solutions for additional support.

1.3.2 Server Hardware

We recommend the following CPU, Memory, and GPU:

Server-Side	Recommended
CPU	Intel Core i5, one core per monitor + 1
Memory	2 GB
GPU	Any

1.3.3 Server Network

The server's bandwidth (BW) requirements are the sum of the bandwidth required by all connected clients.

A client's bandwidth requirements are the sum of the video bandwidth and the audio bandwidth. Video bandwidth depends on the display resolutions, the selected video encoding, and the number of displays. These bandwidth values can be found in *Client Requirements*. Note that even though multiple clients may be sharing the same desktop, each client needs its own connection to that screen with its own bandwidth usage.

By default, audio bandwidth is 1.411 Mbps when it is enabled by the end-user. When audio is disabled by the end-user, it consumes no bandwidth.

To calculate the maximum server bandwidth (BW) requirements, use the following equations:

```
Video BW Per User = Displays per User * BW per Display
```

```
Audio BW Per User = 1.411 Mbps
```

```
Max Server BW = Users * (Video BW per User + Audio BW per User)
```

For example, if we want to plan for a single user to have video and audio access to a server that has a single display showing at 1080p with our normal (lossy) encoding:

```
Video BW Per User = 1 display * 6 Mbps = 6 Mbps
```

```
Audio BW Per User = 1.411 Mbps
```

```
Max Server BW = 1 user * (6 Mbps + 1.411 Mbps) = 7.411 Mbps
```

As a second example, if we want to plan for three users to have video and audio access to a server that has dual displays showing at 2K with our normal (lossy) encoding:

```
Video BW Per User = 2 displays * 12 Mbps = 24 Mbps
```

```
Audio BW Per User = 1.411 Mbps
```

```
Max Server BW = 3 users * (24 Mbps + 1.411 Mbps) = 76.233 Mbps
```

1.3.4 Server Screen Resolutions

The performance of the remote access is partly dependent on the server's screen resolution and the client's ability to process that resolution quickly.

> The ICE RemoteWare software allows system administrators to pick a maximum screen resolution width and height in the config file (by default 2560x1600). If the user attempts to change the screen resolution above this setting, then the video scales down automatically. This can alleviate situations where users set the screen resolution so high that their client machine becomes unusable.

For most users, we recommend our default values. If you'd like to test higher screen resolutions, we recommend doing so with gradual increases.

Warning

Changing screen resolutions has two known issues:

1. **Multiple rapid resolution changes may lead to service instability.** Changing the screen resolution more than 5 times over a few seconds may cause the service to restart or quit.

For more information about changing screen resolutions, see *Change Screen Resolution*.

1.3.5 Server Audio

The ICE RemoteWare product will stream audio from a remote server if it has a functional audio device and proper drivers. In Linux, Pulseaudio is required and is already installed by default on many Linux systems.

MacOS users must follow the instructions in *Install BlackHole for MacOS Audio* to add MacOS Audio Support.

1.3.6 OpenSSL

OpenSSL is an open source implementation of the SSL and TLS protocols and must be installed on the server host. Most Linux distributions have this installed by default, but in Windows this is installed by the ICE RemoteWare server-side installer.

1.3.7 SSL Certificate

An SSL certificate signed by a trusted certificate authority is used to provide encryption and authentication for a client's HTTPS connection to the ICE RemoteWare web server. By default, the ICE RemoteWare product comes with a self-signed SSL certificate and private key that should not be used in secure production environments.

For more information on generating SSL certificates, see *Setup*.

1.4 Client Requirements

You can connect to the server using either an HTML5 browser or our native client (ICE RemoteWare Client).

1.4.1 Client Hardware and Network

Client-side hardware and network requirements are largely based on the server's screen resolution and the number of pixels changing on the screen at a given time.

The table below shows CPU and Network requirements when remoting a single full screen movie using our normal video encoder at 24-30 frames per second. Turning on audio streaming will consume an additional 1.411 Mbps of bandwidth.

Table 1: Normal Video Recommendations

Server Resolution	Network (Mbps)	CPU, Native Client	CPU, Chrome
1280 x 720	3	Intel Core i5	Intel Core i5
1920 x 1080	6	Intel Core i5	Intel Core i7-3520M
2560 x 1440	12	Intel Core i7-3520M	Intel Core i7-2600K
3840 x 2160	25	Intel Core i7-2600K	Intel Core i7-5775C

The tables below show recommendations for visually lossless and lossless video encodings, respectively. These options are only accessible with the native client.

Table 2: Visually Lossless Video Recommendations

Server Resolution	Network (Mbps)	CPU, Native Client
1280 x 720	11	Intel Core i7-3520M
1920 x 1080	22	Intel Core i7-3520M
2560 x 1440	32	Intel Core i7-3520M
3840 x 2160	64	Intel Core i7-2600K

Table 3: Lossless Video Recommendations

Server Resolution	Network (Mbps)	CPU, Native Client
1280 x 720	65	Intel Core i7-2600K
1920 x 1080	125	Intel Core i7-2600K
2560 x 1440	200	Intel Core i7-5775C
3840 x 2160	400	Intel Core i7-5775C

Note

The ICE RemoteWare Client is more optimized than the Chrome Browser so it requires lower CPU resources to achieve the same frame rate.

Note

Acceptable network latency is application and workflow dependent. In some cases, 150ms may be acceptable. Performance may degrade if the client is running background applications that consume significant amounts of CPU time, memory, or network bandwidth.

1.4.2 Web Browser Support

The following web browsers are supported and listed in order of performance:

- Chrome 59+
- FireFox 56+
- Microsoft Edge Legacy 44.17763.1.0+
- Microsoft Edge 79+
- Safari 7+

Note

Chrome provides the best performance and is recommended.

These browsers by default enable TLS 1.2, WebGL and WebSocket features that are necessary for security and optimal ICE RemoteWare performance. While WebSocket support is a hard requirement, the ICE RemoteWare software is capable of running without WebGL support at reduced performance levels.

The following links can be used to determine if your browser supports necessary features for an optimal ICE RemoteWare experience:

Browser Feature	Test for Browser Support
Security Protocol TLS 1.2	https://www.ssllabs.com/ssltest/viewMyClient.html
WebGL	https://get.webgl.org/
WebSockets	http://websocketstest.com/

Note

TLS 1.2 is the current standard used to secure HTTPS connections as of the writing of this document.

1.4.3 ICE RemoteWare Client

ICE RemoteWare Client is a native client that requires a separate application installation on the client side. It is similar to the web browser, but it includes some additional benefits:

- faster frame rates at higher screen resolutions
- lossless and visually lossless video support
- support for keyboard shortcuts reserved by web browsers (for example: `Ctrl + T`, `Ctrl + N`, `Ctrl + W`)

ICE RemoteWare Client is supported and tested on the following 64-bit operating systems:

- Rocky Linux 8 and 9

- Windows 10, 11, and Windows Server 2019
- MacOS Big Sur 11 to MacOS Sonoma 14
- Ubuntu 20, 22 and 24

Note

OpenGL 2.1 support is required.

Note

New in v11.2: ICE RemoteWare Client can also be launched from URI links such as: `irw://<server>`

1.5 Feature Requirements and Setup

ICE RemoteWare features are designed to be ready to use across all platforms that meet the recommended hardware and operating systems listed above. Some of these features include:

- Authentication over Active Directory, LDAP, PAM, SCAuth, RHV OAuth2, and more
- Secure HTTPs communication
- Video playback up to 4k
- Audio
- Multi-display support
- Text copy & paste
- Quality of Service adaptation
- File up- and download
- Collaboration

Some features have additional requirements. These are organized by server-side operating system below:

1.5.1 All Operating Systems

Enabling 4K Video on all OSes

1. Set `Server.Video.MaxWidth` and `Server.Video.MaxHeight` to `-1` in the XML config file.
2. Connect with the native client instead of a browser for best performance.

Enabling Lossless and Visually Lossless Video on all OSes

1. Connect with the native client instead of a browser.

1.5.2 Rocky Linux

Enabling USB Forwarding on Rocky Linux

USB devices can be forwarded between native clients and remote servers that meet the following requirements:

1. The server's license file must have a valid 'irw-usb' entitlement. If you do not see this entitlement in your license file, please contact Penguin Solutions sales for more information.
2. The Server-USB module must be installed on the remote server. See *Installing Server-USB Module on Rocky Linux* for more information on this step.
3. The Client-USB module must be installed on the client side. See *Installing Client-USB Module on the Client* for more information on this step.

Enabling Xorg X server as the default on Rocky Linux

XWayland is not currently supported. Please see *Installing the Server on Rocky Linux* for instructions on enabling Xorg as the default X server.

1.5.3 MacOS

Enabling Audio on MacOS

1. Download and install BlackHole 0.2.9. See *Install BlackHole for MacOS Audio* for more information.
2. Note: Audio is not supported on MacOS Virtual Machines.

Re-Enabling USB Forwarding after Updating to MacOS Monterey

If you have an existing ICE RemoteWare installation and you've updated from Big Sur (or earlier) to Monterey (or later), follow these steps to install 'VirtualHereUniversal' and re-enable USB Forwarding:

1. Use a Finder window to open the Applications folder
2. Right-click on 'ICE RemoteWare' and select 'Show Package Contents'
3. Open 'Contents' and then 'Resources'
4. Open the VirtualHereUniversal dmg by double-clicking on 'VirtualHereUniversal.dmg'
5. Drag the 'VirtualHereUniversal' application into the Applications folder
6. Move the deprecated 'VirtualHere' application to the Trash

CHAPTER

TWO

RELEASE NOTES

This page lists the version history of ICE RemoteWare™ releases.

You can access the latest ICE RemoteWare™ documentation here as well as the latest version of the release notes.

2.1 What's New in v15.1.0

- **Updated bundled OpenSSL to version 3.5.0 on all platforms**
- **MultiSession: Added audio support for guest sessions**
- MultiSession: Added a tool for transparently starting GPU-enabled applications
- MultiSession: Added security options to hide other users process ids and to mount a private /tmp filesystem
- Fixed an issue preventing the server from starting up due to a problem finding the configuration file on Linux
- Simplified audio setup on Rocky Linux 9 and Ubuntu 24
- Resolved an issue, preventing loading the library for VirtualHere integration
- Various improvements to File Up- and Download

2.2 Known Issues

- MacOS Sonoma: USB integration on server is not supported (#4820)
- MacOS Ventura: USB integration install on server requieres manual steps to complete (#4819)
- Guest sessions on Ubuntu system can't execute snap installed applications from GUI (#4799)
- Server does not start up, when a NIVIDA driver is installed but no supported hardware is found (#4780)
- MacOS: NativeClient does not continue mouse dragging when mouse leaves window (#3970)
- MacOS: Sometimes audio gets corrupted when connected requiring the user to reconnect (#3122)
- Safari on BigSur (macOS 11) and earlier doesn't support connecting to servers with self-signed certificates. Please use Chrome as a workaround (#3971)
- Windows systems with no mouse devices will not show a mouse cursor. Please enable the Microsoft 'Mouse Keys' feature to force Windows to show a cursor as a workaround (#1079)
- Disconnecting Wacom Tablets from the USB Forwarding Menu will disable 'Mouse Keys' on Windows and this may cause the cursor to disappear if there are no mouse devices. Please re-enable 'Mouse Keys' or reconnect the Wacom Tablet as a workaround (#3986)

- Wayland based display servers are not supported. A X11 based windowing system must be enabled (#4132)

2.3 Version History

2.3.1 v15.0.3

- **Added Clipboard Auto-Sync support to the Native Client**
- **MultiSession: Starting guest sessions as services for better security isolation**
- Expanded the options to customized the sign-in screen
- Added a setting to harden the server by disabling all optional features
- Restricted access to Advanced Settings to active controller only
- Expanded the documentation of setup variables
- Added a separate log file for tracking server access
- Improved support for multiple server instances on one machine (Linux only)
- MultiSession: Added UI element to show and control guest sessions
- MultiSession: Added a config entry to enable a user to connect to the host and not to a guest server
- MultiSession: Removed dependency on ssh connections to start servers
- MultiSession: Improved documentation
- MultiSession: Now exposing all variables in Advanced Settings Tool even when MultiSession is currently not enabled
- Made UI elements on client window movable
- Fixed an issue preventing Safari from copying the Remote Clipboard
- Fixed video flickering occurring from time to time on Windows and Linux
- Fixed an issue on cloud instances when a slow X11 setup was causing the server to get stuck during boot until it gets manually restarted
- Windows: Fixed a race condition leading to a server crash when too many users connect at the same time
- Improved and extended documentation of setup variables

2.3.2 v15.0.2

- Fixed an issue when Server.Auth.Enabled is false leading an endless loop of client reconnecting to server during a setup problem
- Fixed smaller issues on the client UI, especially on the Advanced Settings page

2.3.3 v15.0.1

- Fixed an issue preventing the Native Client to download files from server
- Fixed an issue preventing the USB integration from installing on certain Linux systems

2.3.4 v15.0.0

- **Scyld Cloud Workstation has been renamed and rebranded to ICE RemoteWare**
- **Redesigned and updated the documentation**
- **Multi Session support on Linux. The multi session feature allows multiple users to run their own sessions concurrently**
- **Added scripts on Linux distribution to set up secure password- less connections**
- Option added to control and set keep-alive settings on TCP sockets
- Showing network address in addition to user name in connect notifications
- Added the server's hostname on sign-page and it's page title
- Fixed an issue where the details of the path to the SSL certificates in the configuration file was deleted
- Fixed an error in the installation validation where a missing VH license triggered a misleading error report
- Improved the dependency information for Linux packages
- Fixed a problem with clients where they might stop working during user login on Linux systems
- Improved sign-in and -out experiences
- Removed CentOS7 from the list of supported OSes
- Fixed a problem where sometimes clients lost keyboard and mouse access when connecting to a server with multiple displays

2.3.5 v14.0.1

- Fix for Linux system without a proper display manager

2.3.6 v14.0.0

- **Added Ubuntu 24 support**
- **Added File Download from server**
- **Added File Upload to server**
- **Added Trial Mode, user can evaluate ICE RemoteWare for a limited time without a trial license**
- **Added Network Address Filter to server**
- **Added USB Allow List to server**
- Command line option added to load additional config file
- Improvements to trial mode
- Added a warning when the user space server is not running
- Removed ctrl-alt-del button in the client UI when connected to a MacOS server

2.3.7 v13.2.0

- Disabled Audio forwarding on OS login screens
- Fixed Ctrl+F12 keyboard shortcut for users who aren't controllers
- Multiple fixes to the Advanced Setting page, e.g. for systems without any authorization, added an option to allow guest access, client UI changes reflecting configuration changes
- Advanced Setting page has default mode for commonly used settings and an expert mode for more advanced configuration
- Fixed Log Viewer for systems without authorization, added an option for guest access
- Fixes for multi-display systems for Log Viewer and Advanced Setting pages
- Enabled "window-manager-less" mode on Linux
- Added a configuration setting to turn off license upload
- Fixes for keyboard handling of Japanese characters
- Server logs any unrecognized settings in config file
- MacOS audio: Fixed server crash and improved audio handling
- Fixed an issue during log into a server when authentication is disabled

2.3.8 v13.1.0

- **Added Advanced Settings page for configuration file editing**
- **Added License Management page for managing missing, outdated, and invalid licenses**
- **Added a Log Viewer for viewing server and service log files (To enable, set Server.LogViewer.Enabled to true)**
- **Added Kiosk Mode to the Native Client to create a locked-down experience (use command line flag –kiosk or /kiosk for windows)**
- **Added MacOS Sonoma 14 support**
- **Deprecated MacOS Catalina 15 support**
- Enabled copying from remote clipboards of Windows servers
- Added Allow list to control the types of USB devices that are allowed to be forwarded to the server (see *Server.VirtualHere.AllowedUsbDevices* for more information)
- Added notifications when a USB device is forwarded to the server
- Improved Japanese language handling on Native Client
- Fixed race condition during USB forwarding
- Fixed an issue preventing the Native Client from copying the server clipboard to the client
- Fixed Windows issue preventing domain account users from logging in twice into the server
- Fixed cursor not displaying on Linux when using the nvfbc video source

2.3.9 v13.0.1

- Fixed Japanese text input on MacOS and added a key mapping example
- Added autodetection of keyboard layout change to MacOS server
- Made missing audio support error message on demand (MacOS only)

2.3.10 v13.0.0

- **Added remote clipboard copying (Linux and MacOS only)**
- **Added 'Fit to Window' view**
- **Added support for Windows Server 2022 (server-side only)**
- **Added beta support for MacOS Sonoma 14**
- Deprecated USB Forwarding on MacOS Big Sur 11
- Added clipboard synchronization notification
- Added notification for when MacOS copy-paste server is not running
- Updated VirtualHere server to 4.5.9 and VirtualHere client to 5.5.4
- Improved mouse responsiveness when client is overloaded
- Fixed keyboard handling of Shift+Insert, Shift+Delete, Shift+NumPad, Shift+Cancel/Stop, and Ctrl+Alt
- Fixed handling of user defined port numbers
- Fixed several issues with installation on Google Cloud instances
- Added workaround for Linux systems where SELinux has made shared memory inaccessible

2.3.11 v12.3.0

- **NOTE:** Existing ICE FlexLM installations must be updated to ICE FlexLM v11.19.3
- **Added support for Rocky Linux 9**
- **Added support for Ubuntu 22.04 LTS**
- **Added support for MacOS Ventura 13**
- **Added beta support for Windows Server 2022**
- **Added Japanese keyboard support**
- Updated VirtualHere server to 4.5.6 and VirtualHere client to 5.4.7
- Updated recommended BlackHole version to 0.5.0 for MacOS audio
- Updated to OpenSSL 3.1 on Windows and MacOS
- Improved stability of VirtualHere integration on Linux
- Improved MacOS Installer
- Improved page loading times
- Improved Windows RDP disconnect handling
- Improved handling of Google Cloud using Google Graphics Array on Windows

- Fixed handling of Ubuntu service shutdown
- Fixed graphics capturing bug on Optimus systems in Windows
- Fixed graphics capturing bug when logging into Linux systems
- Fixed copy-paste on MacOS servers not working on first attempt
- Fixed potential lockout when MacOS lock screen Cancel button causes host to sleep
- Fixed server crash on ARM-based Monterey hosts when switching audio source to Blackhole 16ch
- Fixed Windows native client not shutting down cleanly
- Fixed Windows validation tool unable to run without admin rights
- Fixed service log gets too many messages when server restart fails

2.3.12 v12.2.0

- **Added keyboard support for all Latin and Cyrillic languages**
- **Reduced CPU load when screen window is minimized or in background tab**
- **Reintegrated NvFBC in Linux** to reduce server CPU load
- **Changed Fullscreen keyboard shortcut on native client to Ctrl+F11**
- **Added hardware color conversion for Windows**
- Improved login and logout loading transitions
- Added IPv6 support in native clients
- Added support for sending Cmd+Q to server from MacOS clients
- Changed QoS to be more conservative
- Fixed error page link to home page
- Updated Linux package dependencies

2.3.13 v12.1.1

- **Fixed URI scheme** not registered after performing RPM update of native client
- Fixed internal ping time counter
- Reduced debug level messaging in MacOS
- Fixed Linux 'x11' videosource config option
- Fixed server '–setConfig' command line option
- Removed 'Jointly engineered with Colorado Code Craft' from sign in page

2.3.14 v12.1.0

- **Added support for up to 60 fps frame rate on Linux servers**. Configuration file update is required to enable. See *Server.Video.Encoding.H264.MaxFrameRate* for more information.
- **Added support for Windows 11 and Windows Server 2019**
- **Added support for Ubuntu 20.04 LTS**
- Added beta support for Ubuntu 22.04 LTS (requires: OpenSSL 1.1.1)
- Deprecated support for Ubuntu 16.04 LTS
- Deprecated support for MacOS High Sierra 10.13 and MacOS Mojave 10.14
- Improved user interface load time
- Improved keyboard and mouse response times
- Improved handling of non-English keyboards in Linux
- Fixed Rocky Linux Client's USB Forwarding instability
- Fixed native client video instability during scrolling
- Fixed race condition in service restart tool for Windows
- Fixed race condition in handling CentOS 7 logouts
- Fixed MacOS video sources not always being available after reboot
- Fixed native client crash when adding a third display
- Prevent multiple users from connecting when lossless or visually lossless video encoding is active

2.3.15 v12.0.1

- **Added support for Rocky Linux 8**
- Changed USB Forwarding to only be available by installing an optional module
- **Added support for up to 60 fps frame rate on Windows servers** using the new default video source ('windda')
- **Added support for up to 60 fps frame rate on ARM-based Mac servers**
- Improved handling of Windows sign-out confirmation screen
- Updated VirtualHere server to 4.4.2 and VirtualHere client to 5.3.6
- Fixed Windows active directory domain logins
- Fixed Windows and Linux keyboard handling
- Fixed Linux pactl zombie processes
- Fixed MacOS caffeinate zombie processes
- Fixed USB Forwarding menu not reflecting WACOM tablet unplug events
- Fixed remote cursor not hiding when disconnecting a WACOM tablet
- Fixed missing ShadowPassword fields in default MacOS and Windows configuration files
- Fixed Windows configuration file handling of 'auto' values
- Dropped support for Windows 7 and 8
- Dropped support for NvFBC

- Dropped support for Internet Explorer 11
- Dropped USB Forwarding support for MacOS Big Sur servers

2.3.16 v11.3.3

- Fixed MacOS installer alerts

2.3.17 v11.3.2

- Fixed crash of Windows server

2.3.18 v11.3.1

- Added support for MacOS server updates without a desktop login
- Added support for MacOS client clean installs and updates without a desktop login
- Fixed stuck video on MacOS login screen
- Improved MacOS server and client installer log messages
- Fixed Windows server validation tool
- Fixed Windows client unable to reopen screens
- Fixed missing Windows client DLLs msvcp140_1.dll and vcruntime140_1.dll
- Bug fixes for USB Forwarding
- Updated to VirtualHere server v4.3.8
- Updated to VirtualHere client v5.3.1

2.3.19 v11.3.0

- Added MacOS Monterey 12 client and server side support
- Added Apple Silicon M1 support for client and server
- Added 60 fps support for servers using Apple Silicon M1
- Fixed MacOS client caps lock
- Fixed MacOS client copy and paste
- Removed support for USB Forwarding to Big Sur servers due to a change in Big Sur. Please update to MacOS Monterey for USB Forwarding support. Big Sur clients can still forward USB devices to other servers
- Improved Windows USB Forwarding start-up
- Improved Windows sign out handling
- Improved Windows install verification tool
- Updated Windows and MacOS OpenSSL to 1.1.1l
- Added ability for native clients to auto resize to video
- Added support for **Server.Audio.Output.SampleRate** values 48000 and 96000

- Fixed issue with scrollbars being inaccessible in fullscreen

2.3.20 v11.2.1

- **Added MacOS Big Sur client support (x86 only)**
- Updated USB Forwarding installation for MacOS Catalina and later

2.3.21 v11.2.0

- **Added ability to launch the native client using new URI scheme:** `irw://<server>`
- Added an application launcher for GNOME systems
- Changed native client command line to accept URL argument without flags
- Fixed Ubuntu client installer issue that prevented USB Forwarding

2.3.22 v11.1.1

- Fixed MacOS and Windows client white screen issue

2.3.23 v11.1.0

- **Added USB Forwarding (includes Wacom Tablet support)**
- Upgraded QT on Windows and MacOS to 5.14.2
- Improved audio quality on MacOS and Windows
- CentOS and RHEL customers encouraged to install using YUM repository (see documentation for more information)
- Added PrintScreen and Ctrl+Alt+Del to keyboard shortcuts
- Removed Windows installer menu for config file credential setup
- Changed minimum length of config file passwords to be six characters
- Added FAQ to help users who have WebGL blocked by their browser for certain graphics cards and driver combinations
- Fixed escape key down issue
- Added –broker-passwd flag for MacOS
- Changed ScyldCloudAuth based usernames to be case insensitive

2.3.24 v11.0.1

- **NOTE:** This release is not compatible with earlier versions. Please update all server and client components
- **Added CentOS 8 with GDM support (Xorg must be enabled)**
- **NOTE:** Windows users should use the NVIDIA Control Panel to change screen resolution
- Discontinued CentOS 6 support
- Added notarization and code signing of MacOS packages
- Updated recommended BlackHole version to 0.2.9 for MacOS audio
- Added CSP policy
- Added Users API
- Added 'broker' account for API access
- Disabled 'admin' account by default on Linux and Windows
- Fixed initial static audio in MacOS
- Fixed multiple users not able to access audio streams in Linux
- Fixed MacOS copy-paste
- Changed service architecture for all Linux platforms
- Updated Windows and MacOS OpenSSL to 1.1.1k
- Removed ability to customize Linux screensaver launcher
- Changed background color to a slight gray
- Optimized cursor loading
- Bug fixes and security updates

2.3.25 v10.2.2

- Added security patch to MacOS server
- Fixed missing MacOS client icon

2.3.26 v10.2.1

- **NOTE:** Existing ICE FlexLM installations should be updated to ICE FlexLM v11.17.0.1
- Added audio support for Safari
- Fixed MacOS issue with starting service from command line
- Fixed MacOS issue with audio toggle
- Fixed MacOS issue with video device detection on reboot

2.3.27 v10.2.0

- Improved audio settings to CD-Audio quality
- Improved audio-video sync by lowering default **Audio.Output.BufferTime** to 0.020s
- Added support for 8, 16, and 24 values to **Audio.Output.BitsPerSample**
- Added support for additional **Server.Audio.Output.SampleRate** values
- Added ability to restart audio by toggling audio button
- Updated documentation for bandwidth and hardware requirements
- Fixed OS credentials login conflicts
- Fixed Linux user name detection
- Fixed Linux "Test AudioSource: pipe failed 'Too many files open'"
- Fixed Windows NvFBC multi-screen mouse cursor positioning
- Fixed Windows adding config file credentials dynamically
- Fixed MacOS for multiple user accounts
- Fixed MacOS login
- Fixed MacOS audio detection
- Fixed MacOS launcher

2.3.28 v10.1.1

- Fixed issue with Chrome not being able to sign in over HTTP
- Fixed issue with incomplete Config File Credentials preventing other sign ins

2.3.29 v10.1.0

- Added **server support for MacOS** 10.13, 10.14, and 10.15
- Added **client support for MacOS** 10.13, 10.14, and 10.15
- Added **on-screen performance monitor** to client
- Improved audio-video sync by lowering **Audio.Output.BufferTime** to 0.045s

2.3.30 v10.0.0

- Added **two-channel audio** for Windows 10, CentOS 7, and Ubuntu 16 servers. See the *Server Audio* section for more information
- Increased **Server.Video.MaxWidth** and **Server.Video.MaxHeight** to 1440p (2560x1440)
- Added **RHV Authentication Support**
- Added **support for IPv6**
- Updated Windows OpenSSL to 1.1.1g
- Fixed issue with High DPI scaling in Windows native client

- Fixed browser support for NvFBC at 4K resolutions

2.3.31 v9.2.1

- Fixed issue with visually lossless slider not updating in multi-display, multi-user situation

2.3.32 v9.2.0

- Added support for **visually lossless video** (single user, native client only)
- Improved lossless video performance
- Added support for Chrome 80's new SameSite cookie policy
- Fixed display detection error handling in Linux startup script

2.3.33 v9.1.11

- Fixed custom application cursors not showing in Windows
- Fixed fullscreen button not showing for Guest users
- Changed UI to inform when no users have keyboard and mouse control

2.3.34 v9.1.10

- Added security patch to Server.Auth.OSAuth.Enabled for Windows
- Fixed screen resolution changing in CentOS 7.7
- Fixed pausing and resuming guest video
- Fixed video halting when switching to Ctrl+Alt+Del menu in Windows 7
- Fixed black box cursor when connecting over a VM
- Added error messaging for missing PEM file
- Fixed ERR_BAD_SSL_CLIENT_AUTH_CERT connection error
- Improved log file messaging
- Improved screen scaling support

2.3.35 v9.1.9

- Fixed QoS to react faster to network changes
- Increased default **Server.Video.AvgBitRate** to `1280x720=3000k,1920x1080=6000k`
- Changed **Server.Video.AvgBitRate** to optionally accept a single `<resolution>=<bit-rate>` value and use the given bit-rate for all resolutions
- Disabled low bandwidth warning messages by default

2.3.36 v9.1.8

- **NOTE:** This release is not compatible with earlier versions. Please update all server and client components.
- Added a new video decoder for **significant video improvement in modern browsers**
- Added **security patch to WebSocket protocol**
- Added support for **ScyldCloudAuth Token Authentication**
- Added ability to use a custom sign-in page by setting **Server.Auth.ExternalSignInPage** to a URL
- Improved QoS algorithm
- Added feature to halt server if port is already being used
- Fixed issue with setting Server.Video.VideoSource to 'nvfbc' resulting in 'stream' video source
- Changed frame rate to reflect actual frames per second instead of decode time
- Fixed Mac Cmd key
- Fixed text paste not working in Chrome browser

2.3.37 v9.0.0

- Added single-user support for toggling **lossless video** (native client only)
- Added beta support for GNOME 3.28+ on CentOS 7
- Dropped server and client support for Ubuntu 14
- Reorganized main toolbar
- Added lossless video checkbox to new settings menu
- Added scaled video status message to new settings menu
- Upgraded QT to 5.9.7
- Updated Windows OpenSSL to 1.0.2r
- Fixed multi-display issues when enabling and disabling displays
- Improved user warning alerts
- Fixed multi-user slow-user warning icons
- Fixed alternative mouse cursor visibility
- Fixed mouse scrolling behavior in Chrome 73
- Fixed multi-display issue with double-clicking on screen buttons
- Fixed misleading "Another user is signed in" message
- Fixed issue where clicking on external links created a black window (native client only)
- Reduced mouse context menu options (native client only)
- Fixed "You need to enable cookies in order to log in" issue (native client only)

2.3.38 v8.1.5

- Fixed CentOS 6 issue with setting **Server.Video.VideoSource** to `auto` or `nvfbc`
- Fixed minor multi-screen interface issues
- Fixed documentation by changing **Server.ConcurrentClients.MaxClientCount** to **Server.Collaboration.MaxClientCount**
- Hide Guest Invite buttons when **Server.Collaboration.MaxClientCount** is set to 1
- Fixed QoS stability issues

2.3.39 v8.1.4

- Added support for mouse dragging between tiled screens
- Switched to overlay scrollbars
- Updated QoS algorithm
- Fixed JavaScript error in IE11

2.3.40 v8.1.3

- Fixed crash related to screen size changing
- Fixed flickering caused by decoder library and stream video source
- Fixed QoS stability issues

2.3.41 v8.1.2

- Fixed downscaling when resolution height is not divisible by 4

2.3.42 v8.1.1

- Added `--check` command line option to help test installation
- Added version compatibility checking to native client and server
- Added support for adding or removing displays
- Added Windows start menu shortcuts for easier access to log file and service restart
- Updated Windows OpenSSL to 1.0.2p
- Fixed Ubuntu 14 issue where video outputs swapped after screen size change
- Fixed resolution scale down message text and added fade-out behavior
- Fixed button behavior for opening screens
- Fixed mouse location after display re-positioning
- Fixed support for Windows systems with multiple NvFBC GPUs

2.3.43 v8.0.1

- **NOTE:** This release is not compatible with earlier versions
- **NOTE:** A clean install of the Server is required (Windows only)
- Added ability to show **multiple screens** across **multiple displays**
- Renamed boot.log log file to win-service.log
- Added confirmation prompts to prevent accidental session closing
- Added ability to change PAM Service name by changing the **Server.Auth.OSAuth.PAM.Service** config option
- Fixed max video scaling issues that occurred after resolution changes
- Removed unneeded libraries from Server MSI installer
- Fonts are now hosted by the Server
- Client window bug fixes

2.3.44 v7.1.8

- Fixed native client blank connect dialogue appearing after service restarts
- Fixed native client black screen when reconnecting after Windows 10 service restarts
- Fixed native client scroll bars not appearing when reconnecting after Windows 10 service restarts
- Fixed Windows 10 service becoming unavailable after signing out
- Suppressed mouse cursors always shows in Windows 10
- Added HiDPI support for Windows stream encoder
- Fixed Linux log file location

2.3.45 v7.1.1

- Improved handling of scenarios where Windows has no console session
- Improved handling of scenarios where RDP session is active
- Documented 'Escape' workaround for black windows login screen issue
- Changed default XML config file value for **Server.Misc.IdleUserTimeout** to 120
- Fixed missing OpenSSL libraries in Windows
- Fixed client EULA

2.3.46 v7.1.0

- Changed **video bit-rate selection** to be based on screen resolution
- **Lower latency** for native client due to optimizations on color conversion and frame rendering

2.3.47 v7.0.2

- Added OpenSSL v1.0.2n libraries to Windows native-client

2.3.48 v7.0.1

- Fixed Windows password changing documentation
- Fixed config file automatically inserting StreamVideoSource tags
- Removed Windows wrapper batch script

2.3.49 v7.0.0

- Added **4K resolution support to native-client**. Additional server-side setup is required. See the *Enable 4K Support* section for more information.
- Improved **frame-rate performance of native-client**
- Added **MD5 hash of configuration file to start-up output**
- Upgraded QT to 5.9.2
- Improved **native-client window resize behavior**
- Improved **native-client fullscreen behavior** to downscale graphics when remote desktop is larger than the client screen size

2.3.50 v6.1.1

- Fixed image blurring when enabling unique frames

2.3.51 v6.1.0

- Added ability to **sign in with Linux and Windows OS credentials**
- Added ability to **transmit only unique video frames** with **Server.Video.UniqueFramesOnly** config setting (true by default)

2.3.52 v6.0.3

- Added browser-less 'Native Client' for CentOS 7 and Windows 7
- Fixed relative paths for Server.License.FileName
- Updated fonts, icons, and colors
- Changed from Windows NSIS installer to MSI installer
- All **Server.ConcurrentClients** configuration settings changed to **Server.MultiUser**

2.3.53 v5.0.7

- Fixed "too many files open" error for generic stream video source

2.3.54 v5.0.6

- Improved error handling for disconnects during inactivity
- Changed default idle user timeout to 2 hours

2.3.55 v5.0.5

- Fixed black winlogon screen for stream video source

2.3.56 v5.0.4

- Fixed screen size changing in Windows

2.3.57 v5.0.3

- Fixed handling of poor network connections
- Windows installer preserves *.dat, *.lic files on update

2.3.58 v5.0.2

- Fixed blackscreen when using IE 11 over a VPN
- Fixed systemd service status check

2.3.59 v5.0.1

- Fixed init script false-positive when license checkout fails
- Fixed systemd service script
- Reduced log output on license checkout retries

2.3.60 v5.0.0

- Added CPU-based (**stream**) video source option
- Added **idle user timeout** (**Server.Misc.IdleUserTimeout** takes minutes. Disabled by default)
- Added ability to **update Server.Auth settings at runtime** (except Server.Auth.Enabled)
- Added ability to **auto-select a video source**
- Added **Flexera License Management**
- Added ability to specify license file with **Server.License.FileName** config setting
- Added ability to delay service start with **Server.Misc.StartDelay** config setting
- Renamed **Server.WebSocketServer.Secure** to **Server.Network.Secure**
- Renamed **Server.WebSocketServer.Port** to **Server.Network.Port**
- Renamed **Server.ServiceLogFile** to **Server.Log.ServiceLogFile**
- Renamed **debug0.txt** to **ice-remoteware-service.log** and **debug1.txt** to **ice-remoteware.log**
- Changed Windows install directory to **C:\Program Files\Penguin Solutions\ICE RemoteWare**
- Changed Windows service startup from Automatic to Delayed
- Changed log messages
- Fixed guests getting kicked out if one of multiple hosts signs out
- Fixed handling of IPv6 addresses
- Fixed guest toolbar being hidden while paused
- Fixed duplication of guest alerts
- Fixed guest video when starting out paused

2.3.61 v3.1.0

- Added **support for CentOS 7** (requires LightDM / MATE desktop environment)
- Added **Floating UI**
- Added **adjustable screen resolutions limits**
- Added **Server.Video.MaxWidth** and **Server.Video.MaxHeight** to config file
- Updated **QoS algorithm**
- Windows installer preserves *.crt, *.cer, *.pem, *.key, and *.der files on update
- Set default max frame rates to 30
- Fixed Firefox keyboard issue for remote Windows services

2.3.62 v3.0.4

- Increased send timeout values
- Added **Server.Network.Timeouts.VideoSend**, **Server.Network.Timeouts.CtrlSend**, and **Server.Network.Timeouts.Receive** to config file

2.3.63 v3.0.3

- Fixed QoS adaptive frame rate algorithm

2.3.64 v3.0.2

- Fixed IE11 fullscreen keyboard and scrollbars

2.3.65 v3.0.1

- Fixed unexpected multi-user client timeouts

2.3.66 v3.0.0

- Added **keyboard and mouse sharing** for collaboration
- Added **guest invites** for collaboration
- Added **text paste from local clipboard** support
- Added **remote desktop auto-lock on disconnect**
- Updated **QoS algorithm**
- Updated user interface style
- Updated default SSL ciphers
- Compatible with v2.3 config file

2.3.67 v2.3.2

- Updated default SSL ciphers

2.3.68 v2.3.1

- Fixed Command/Windows key getting stuck
- Fixed cursor disappearing during Windows UAC

2.3.69 v2.3.0

- Improved **decode performance**
- Improved **QoS responsiveness**
- Improved mouse scrolling. Ticks are now server-dependent
- Added code authenticity check
- Fixed OS X command key
- Improved version number system
- Fix for null cursor
- Fix for missing HTML icons
- Added support for 16x16 cursors in Windows
- Improved web-page refresh

2.3.70 v2.2.0

- Added **local cursor**
- Added **basic QoS /** dynamic frame rate updates
- Simplified configuration file by relying more on defaults
- Updated interface controls to be centered, sleeker
- Updated default openSSL.server.cipherList string to include !RC4
- Updated default openSSL.server.verificationMode to relaxed
- Fixed cursor in Firefox Fullscreen
- Fixed mouse wheel
- Fixed screen crop
- Added auto-lock (disabled by default)
- Authentication screen can now be disabled in config
- RPM installer preserves old config file by default

2.3.71 v2.1.0

- Added **screen resolution change support** (Windows, Linux)
- ScyldCloudAuth "JSON Syntax Error" fix
- Silent / Quiet Windows installer

CHAPTER

THREE

INSTALLATION

Learn more about installing the ICE RemoteWare™ server and client.

3.1 Server Installation

The ICE RemoteWare server can be installed on the following operating systems:

- Rocky Linux 8 and 9
- Windows 10, 11, and Windows Server 2019
- Windows Server 2022 (server-side only)
- MacOS Monterey 12 to MacOS Sonoma 14
- Ubuntu 20, 22 and 24

3.1.1 Required Files

Installation packages and documentation can be downloaded from: https://updates.penguincomputing.com/irw/download/. Rocky, CentOS and RHEL users should add the repository as a YUM repo using the OS-specific instructions that follow.

Installation of the ICE RemoteWare server requires the following files:

- The ICE RemoteWare server installation package for your operating system:
  - Rocky Linux 8: `ice-remoteware-15.1.0-0.el8.x86_64.rpm`
  - Rocky Linux 9: `ice-remoteware-15.1.0-0.el9.x86_64.rpm`
  - Ubuntu 20: `ice-remoteware_15.1.0.0-0ubuntu1.20_amd64.deb`
  - Ubuntu 22: `ice-remoteware_15.1.0.0-0ubuntu1.22_amd64.deb`
  - Ubuntu 24: `ice-remoteware_15.1.0.0-0ubuntu1.24_amd64.deb`
  - Windows 10, 11, and Windows Server 2019, 2022: `ICE RemoteWare-15.1.0.0.msi`
  - MacOS Monterey 12 to MacOS Sonoma 14: `ice-remoteware-15.1.0.0.pkg`
- One of the following:
  - A trial license file (`ice-remoteware.lic`)
  - A floating license file (`ice-flexlm.lic`) and the license server (ICE FlexLM).

3.1.2 Installing the Server on Rocky Linux

Follow the steps below to install the ICE RemoteWare server, replace the default SSL key and certificate files, install the license file, and change your X server from XWayland to Xorg. After a service restart, you should be able to sign in with standard OS credentials.

1. Use the `wget` command to install the ICE RemoteWare YUM repository for your version of Rocky Linux:

```
% ## Rocky Linux 8 only
% sudo wget https://updates.penguincomputing.com/irw/irw-el8.repo -P /etc/yum.repos.
↪d

% ## Rocky Linux 9 only
% sudo wget https://updates.penguincomputing.com/irw/irw-el9.repo -P /etc/yum.repos.
↪d
```

2. Use the `yum install` command to install `ice-remoteware`.

```
% sudo yum install -y ice-remoteware
```

   The installer does the following:

   - Installs ICE RemoteWare files to `/opt/ice-remoteware`
   - Installs ice-remoteware.service to `/lib/systemd/system/`
   - Reloads the systemd manager configuration using `systemctl daemon-reload`
   - Enables the unit file with `systemctl enable ice-remoteware.service`

3. If you have a trusted SSL certificate for your server's domain, open the configuration file (`/opt/ice-remoteware/ice-remoteware.xml`) and set the value of `openssl.server.privateKeyFile` and `openssl.server.certificateFile` to its path. Using a trusted SSL certificate is recommended for maximum security.

4. Install the license.

   - If you have a trial license (`ice-remoteware.lic`), copy it into `/opt/ice-remoteware/bin`.
   - If you have a floating license (`ice-flexlm.lic`), proceed to *Flexera License Management* for instructions on installing ICE FlexLM.

5. Verify that your firewall rules allow traffic over HTTPS (port 443).

6. ONLY IF you are using XWayland as your X server (enabled by default in Rocky Linux), enable Xorg by following these steps:

   a. Open editor to open: `/etc/gdm/custom.conf`

   b. Look for the lines below:

```
[daemon]
# Uncomment the line below to force the login screen to use Xorg
#WaylandEnable=false
```

   c. Uncomment (remove the '#') preceding the 'WaylandEnable' variable.

   d. Save the file and reboot the system. The service will start after the reboot.

7. Use the `systemctl restart` command to restart the service:

```
% sudo systemctl restart ice-remoteware.service
```

8. OPTIONAL: To enable USB Forwarding features, see *Installing Server-USB Module on Rocky Linux*.

The ICE RemoteWare product should now be reachable over HTTPS at your server's hostname or IP address. For advanced configuration options, please see *Setup*.

3.1.3 Installing Server-USB Module on Rocky Linux

USB devices can be forwarded between native clients and remote servers that meet the following requirements:

1. The server's license file must have a valid 'irw-usb' entitlement. If you do not see this entitlement in your license file, please contact Penguin Solutions sales for more information.
2. The Server-USB module must be installed on the remote server.
3. The Client-USB module must be installed on the client side. See *Installing Client-USB Module on the Client* for more information on this step.

To install the Server-USB modules:

1. Use the `yum` command to install `ice-remoteware-server-usb-module`.

```
% sudo yum install -y ice-remoteware-server-usb-module
```

2. Use the `systemctl restart` command to restart the service:

```
% sudo systemctl restart ice-remoteware.service
```

3.1.4 Installing the Server on Windows

Note

For virt-manager users: virt-manager's graphical console will no longer work after installing the NVIDIA GRID driver and restarting Windows.

To get the virt-manager graphical console to work again, start the Windows VM in 'Safe Mode' by restarting the VM, commanding it to "Force Off", and restarting the VM again. Select "Safe Mode with Networking" from the menu that appears.

1. Download `ICE RemoteWare-15.1.0.0.msi` from https://updates.penguincomputing.com/irw/download/
2. Double-click on the `ICE RemoteWare-15.1.0.0.msi` installer.
3. Follow the instructions in the GUI.
4. If your server's domain has a trusted SSL certificate, open the configuration file (`C:\Program Files\Penguin Solutions\ICE RemoteWare\ice-remoteware.xml`) and set the value of `openssl.server.privateKeyFile` and `openssl.server.certificateFile` to its path. Using a trusted SSL certificate is recommended for maximum security.
5. Install the license.
    - If you have a trial license (`ice-remoteware.lic`), copy it into `C:\Program Files\Penguin Solutions\ICE RemoteWare`.

- If you have a floating license (`ice-flexlm.lic`), proceed to *Flexera License Management* for instructions on installing ICE FlexLM.

6. OPTIONAL: To enable USB Forwarding features, see *Installing Server-USB Module on Windows*.

The ICE RemoteWare product should now be reachable over HTTPS at your server's hostname or IP address. For advanced configuration options, please see *Setup*.

3.1.5 Installing Server-USB Module on Windows

USB devices can be forwarded between native clients and remote servers that meet the following requirements:

1. The server's license file must have a valid 'irw-usb' entitlement. If you do not see this entitlement in your license file, please contact Penguin Solutions sales for more information.
2. The Server-USB module must be installed on the remote server.
3. The Client-USB module must be installed on the client side. See *Installing Client-USB Module on the Client* for more information on this step.

To install the Server-USB modules on the remote server:

1. Download `ICE RemoteWare Server USB Module-15.1.0.0.msi` from https://updates.penguincomputing.com/irw/download/
2. Double-click on the `ICE RemoteWare Server USB Module-15.1.0.0.msi` installer.
3. Follow the instructions in the GUI.

3.1.6 Installing the Server on Ubuntu

Follow the steps below to install the ICE RemoteWare server, replace the default SSL key and certificate files, and install the license file. After a service restart, you should be able to sign in with standard OS credentials.

1. Download the debian installer for your Ubuntu version from https://updates.penguincomputing.com/irw/download/
   - Ubuntu 20: `ice-remoteware_15.1.0.0-0ubuntu1.20_amd64.deb`
   - Ubuntu 22: `ice-remoteware_15.1.0.0-0ubuntu1.22_amd64.deb`
   - Ubuntu 24: `ice-remoteware_15.1.0.0-0ubuntu1.24_amd64.deb`
2. Use the `apt install` command to install the DEB file (adjust the file path if necessary):

```
% ## Ubuntu 20 only
% sudo apt install ./ice-remoteware_15.1.0.0-0ubuntu1.20_amd64.deb

% ## Ubuntu 22 only
% sudo apt install ./ice-remoteware_15.1.0.0-0ubuntu1.22_amd64.deb

% ## Ubuntu 24 only
% sudo apt install ./ice-remoteware_15.1.0.0-0ubuntu1.24_amd64.deb
```

   The installer does the following:

   - Installs ICE RemoteWare files to `/opt/ice-remoteware`
   - Installs ice-remoteware.service to `/lib/systemd/system/`
   - Reloads the systemd manager configuration using `systemctl daemon-reload`

- Enables the unit file with `systemctl enable ice-remoteware.service`

3. If your server's domain has a trusted SSL certificate, open the configuration file (`/opt/ice-remoteware/ice-remoteware.xml`) and set the value of `openssl.server.privateKeyFile` and `openssl.server.certificateFile` to its path. Using a trusted SSL certificate is recommended for maximum security.
4. Install the license.
   - If you have a trial license (`ice-remoteware.lic`), copy it into `/opt/ice-remoteware/bin`.
   - If you have a floating license (`ice-flexlm.lic`), proceed to *Flexera License Management* for instructions on installing ICE FlexLM.
5. Verify that your firewall rules allow traffic over HTTPS (port 443).
6. Use the `systemctl restart` command to restart the service:

```
% sudo systemctl restart ice-remoteware.service
```

7. OPTIONAL: To enable USB Forwarding features, see *Installing Server-USB Module on Ubuntu*.

The ICE RemoteWare product should now be reachable over HTTPS at your server's hostname or IP address. For advanced configuration options, please see *Setup*.

3.1.7 Installing Server-USB Module on Ubuntu

USB devices can be forwarded between native clients and remote servers that meet the following requirements:

1. The server's license file must have a valid 'irw-usb' entitlement. If you do not see this entitlement in your license file, please contact Penguin Solutions sales for more information.
2. The Server-USB module must be installed on the remote server.
3. The Client-USB module must be installed on the client side. See *Installing Client-USB Module on the Client* for more information on this step.

To install the Server-USB modules on the remote server:

1. Download the debian installer for your Ubuntu version from https://updates.penguincomputing.com/irw/download/
   - Ubuntu 20: `ice-remoteware-server-usb-module_15.1.0.0-0ubuntu1.20_amd64.deb`
   - Ubuntu 22: `ice-remoteware-server-usb-module_15.1.0.0-0ubuntu1.22_amd64.deb`
   - Ubuntu 24: `ice-remoteware-server-usb-module_15.1.0.0-0ubuntu1.24_amd64.deb`
2. Use the `apt install` command to update the DEB file (adjust the file path if necessary):

```
% ## Ubuntu 20
% sudo apt install ./ice-remoteware-server-usb-module_15.1.0.0-0ubuntu1.20_amd64.deb

% ## Ubuntu 22
% sudo apt install ./ice-remoteware-server-usb-module_15.1.0.0-0ubuntu1.22_amd64.deb

% ## Ubuntu 24
% sudo apt install ./ice-remoteware-server-usb-module_15.1.0.0-0ubuntu1.24_amd64.deb
```

3. Use the `systemctl restart` command to restart the service:

```
% sudo systemctl restart ice-remoteware.service
```

3.1.8 Installing the Server on MacOS

1. Download the `ice-remoteware-15.1.0.0.pkg` from https://updates.penguincomputing.com/irw/download/
2. Double-click on `ice-remoteware-15.1.0.0.pkg` to launch the installer and follow the GUI instructions.
3. Click OK when the prompt for microphone access appears.
4. **MacOS Monterey 12 and earlier:** Click `Open System Preferences` when the `Screen Recording` prompt appears.

   MacOS Ventura 13 and later: Click `Open System Settings` when the `Screen Recording` prompt appears.
5. **MacOS Monterey 12 and earlier:** Click on the Lock icon in the `Security & Privacy` dialog and enter your password.
6. In the menu on the right locate the checkbox labelled ice-remoteware and make sure this box is checked.
7. If you do not see a box for ice-remoteware, click on the + symbol, manually add ice-remoteware to the list, and then make sure the box is checked.
8. Repeat steps 4-7 when the prompt for `Accessibility Access` appears.
9. If your server's domain has a trusted SSL certificate, open the configuration file (`/Applications/ICE RemoteWare.app/Contents/Resources/ice-remoteware.xml`) and set the value of `openssl.server.privateKeyFile` and `openssl.server.certificateFile` to its path. Using a trusted SSL certificate is recommended for maximum security.
10. Install the license.

    - If you have a trial license (`ice-remoteware.lic`), copy it into `/Applications/ICE RemoteWare.app/Contents/Resources`.
    - If you have a floating license (`ice-flexlm.lic`), proceed to *Flexera License Management* for instructions on installing ICE FlexLM.

    Once the license file has been installed, the server will start automatically and be accessible with a web browser or our native client.
11. OPTIONAL: Proceed to *Install BlackHole for MacOS Audio* for information on adding audio support.
12. OPTIONAL: To enable USB Forwarding features, see *Installing Server-USB Module on MacOS*.

Important

Putting your remote MacOS server to sleep (for example: by closing the lid of the laptop, selecting "Sleep" from the Apple menu) will make the ICE RemoteWare software inaccessible.

Important

The ICE RemoteWare product prevents Display Sleep from happening in MacOS using an application called caffeinate. This is to prevent the server from going to sleep.

The ICE RemoteWare product should now be reachable over HTTPS at your server's hostname or IP address. For advanced configuration options, please see *Setup*.

Install BlackHole for MacOS Audio

To add remote audio capture, perform the following steps on your ICE RemoteWare MacOS server:

1. **Download and install `BlackHole 0.2.9` from** https://existential.audio/blackhole/.
2. Select `BlackHole 16ch` as the Sound Output device.
   - **MacOS Monterey 12 and earlier: Open `System Preferences` > `Sound` > `Output`** and select `BlackHole 16ch`.
   - **MacOS Ventura 13 and later: Open `System Settings` > `Sound` > `Output`** and select `BlackHole 16ch`.

   Note

   Selecting `BlackHole 16ch` will disable audio playback on `Internal Speakers`, but this can be changed using the steps above. To change devices more easily, check the `Show volume in menu bar` box. You can now click on the volume control and select one from the Output Device list.

3. Add the ICE RemoteWare software to the `Login Items` list for each MacOS user.
   - MacOS Monterey 12 and earlier: Open `System Preferences` > `Users & Groups`. Select your username and then the `Login Items` tab. Click on the Lock icon and enter your password. Now click on the + button and use the Finder window to add the ICE RemoteWare software to the list.
   - MacOS Ventura 13 and later: Open `System Settings` > `General` > `Login Items`. Click on the + button and use the Finder window to add the ICE RemoteWare software to the list.
4. Logout of MacOS and log back in.

The steps above will make audio accessible to clients that connect to your ICE RemoteWare MacOS server and click on the audio icon.

Note

More information about BlackHole can be found at: https://github.com/ExistentialAudio/BlackHole

3.1.9 Installing Server-USB Module on MacOS

USB devices can be forwarded between native clients and remote servers that meet the following requirements:

1. The server's license file must have a valid 'irw-usb' entitlement. If you do not see this entitlement in your license file, please contact Penguin Solutions sales for more information.
2. The Server-USB module must be installed on the remote server.
3. The Client-USB module must be installed on the client side. See *Installing Client-USB Module on the Client* for more information on this step.

To install the Server-USB modules on the remote server:

1. Download `ice-remoteware-server-usb-module-15.1.0.0.pkg` from https://updates.penguincomputing.com/irw/download/
2. Double-click on the `ice-remoteware-server-usb-module-15.1.0.0.pkg` installer.

3. Follow the instructions in the GUI.

3.2 Client Installation

Users can connect to the ICE RemoteWare server using commonly available web browsers or the native client, ICE RemoteWare Client. The native client is similar to the web browser in many ways, but it is also capable of faster video frame rates and additional features, such as:

- USB Forwarding
- Lossless and Visually Lossless Video

ICE RemoteWare Client can be installed on the following operating systems:

- Rocky Linux 8 and 9
- Windows 10, 11, and Windows Server 2019
- MacOS Big Sur 11 to MacOS Sonoma 14
- Ubuntu 20, 22 and 24

3.2.1 Web Browser Support

The following commonly available web browsers can be used to get fast access to ICE RemoteWare servers:

- Chrome 59+
- FireFox 56+
- Microsoft Edge Legacy 44.17763.1.0+
- Microsoft Edge 79+
- Safari 7+

> **Note**
>
> Chrome provides the best performance of all the web browsers.

3.2.2 Installing the Client

The native client is capable of additional features and faster video frame rates.

- Rocky Linux 8 users:
  1. Use the `wget` command to install the ICE RemoteWare YUM repository for Rocky Linux 8.

     ```
     % sudo wget https://updates.penguincomputing.com/irw/irw-el8.repo -P /etc/yum.
     ↪repos.d
     ```

  2. Use the `yum install` command to install `ice-remoteware-client`.

     ```
     % sudo yum install -y ice-remoteware-client
     ```

- Rocky Linux 9 users:

1. Use the `wget` command to install the ICE RemoteWare YUM repository for Rocky Linux 9.

```
% sudo wget https://updates.penguincomputing.com/irw/irw-el9.repo -P /etc/yum.
↪repos.d
```

2. Use the `yum install` command to install `ice-remoteware-client`.

```
% sudo yum install -y ice-remoteware-client
```

- Windows, MacOS, and Ubuntu users: Download and install the Client installer for your OS from

  https://updates.penguincomputing.com/irw/download/

3.2.3 Installing Client-USB Module on the Client

USB devices can be forwarded between native clients and remote servers that meet the following requirements:

1. The server's license file must have a valid 'irw-usb' entitlement. If you do not see this entitlement in your license file, please contact Penguin Solutions sales for more information.
2. The Server-USB module must be installed on the remote server.
3. The Client-USB module must be installed on the client side.

- Rocky Linux 8 users:

  1. Use the `wget` command to install the ICE RemoteWare YUM repository for Rocky Linux 8.

```
% sudo wget https://updates.penguincomputing.com/irw/irw-el8.repo -P /etc/yum.
↪repos.d
```

  2. Use the `yum install` command to install `ice-remoteware-client-usb-module`.

```
% sudo yum install -y ice-remoteware-client-usb-module
```

- Rocky Linux 9 users:

  1. Use the `wget` command to install the ICE RemoteWare YUM repository for Rocky Linux 9.

```
% sudo wget https://updates.penguincomputing.com/irw/irw-el9.repo -P /etc/yum.
↪repos.d
```

  2. Use the `yum install` command to install `ice-remoteware-client-usb-module`.

```
% sudo yum install -y ice-remoteware-client-usb-module
```

- Windows, MacOS, and Ubuntu users: Download and install the Client-USB module installer for your OS from

  https://updates.penguincomputing.com/irw/download/

CHAPTER

FOUR

FLEXERA LICENSE MANAGEMENT

As of version 5.0.0, the ICE RemoteWare™ software uses the Flexera License Management system to ensure compliance with the terms and regulations described in the End-User License Agreement. This section talks about the types of licenses, how to obtain a license, and how to use your license.

4.1 Obtaining a License

Licenses can be requested by contacting Penguin Solutions (`http://www.penguinsolutions.com`) at `support@penguinsolutions.com`.

4.2 Installing a Trial License

Use a terminal or command prompt to copy the trial license `ice-remoteware.lic` into ice-remoteware using one of the following commands:

- Linux: `sudo cp ice-remoteware.lic /opt/ice-remoteware/bin`
- Windows: `copy ice-remoteware.lic C:\Program Files\Penguin Solutions\ICE RemoteWare`
- MacOS: `sudo cp ice-remoteware.lic /Applications/ICE RemoteWare.app/Contents/Resources`

4.3 Installing a Floating or Node-Locked License

Follow these steps on the ICE FlexLM host:

1. Install the ICE FlexLM license server package (distributed by Penguin Solutions) on a host that has network access to all ICE RemoteWare hosts.
2. Use a terminal or command prompt to copy the trial license named `ice-flexlm.lic` into ICE FlexLM using one of the following commands:
   - Linux: `sudo cp ice-flexlm.lic /opt/ice-flexlm/bin`
   - Windows: `copy ice-flexlm.lic C:\Program Files\Penguin Solutions\ICE FlexLM`
   - MacOS: `sudo cp ice-flexlm.lic /Applications/ice-flexlm.app/Contents/Resources`
3. For Linux users only, change the owner of the file to ice-flexlm using the chown command and make sure the owner has read permission:

```
chown ice-flexlm /opt/ice-flexlm/bin/ice-flexlm.lic
chmod o+r /opt/ice-flexlm/bin/ice-flexlm.lic
```

4. In `ice-flexlm.lic`, find the line that looks like: `VENDOR PENGUIN PORT=<port>`. The last token is the vendor port number (typically `28282`). Change your firewall to allow incoming connections to the vendor port.
5. Now find the line that looks like: `SERVER this_host ANY <port>`. The last token is the license server port number. If the port is not listed, assume it is `27002`. Change your firewall to allow incoming connections the license server port.
6. Restart your firewall and the ICE FlexLM service.

Follow these steps on each ICE RemoteWare host:

1. Use a text editor to open the configuration file located at:
   - Linux: `/opt/ice-remoteware/ice-remoteware.xml`
   - Windows: `C:\Program Files\Penguin Solutions\ICE RemoteWare\ice-remoteware.xml`
   - MacOS: `/Applications/ICE RemoteWare.app/Contents/Resources/ice-remoteware.xml`
2. Find the `Server.License.FileName` setting in the configuration file. If it does not exist you will need to add a `<LicenseFile></LicenseFile>` tag inside the `<Server></Server>` tag.
3. Set the value of `Server.License.FileName` to the port and host of the license server using the `port@host` syntax (or just `@host` if the ICE FlexLM server is using the default port (`27002`).

   For example, if ICE FlexLM was running on port `27002` on a host with hostname `iceberg`:

```
<Server>
  ...
  <LicenseFile>27002@iceberg</LicenseFile>
  ...
</Server>
```

   If you are unsure what port and hostname (or IP address) to use, look at the `SERVER` line in the `ice-flexlm.lic` file. The host name will be second token and the port will be the forth token. In the example above this would look like:

```
SERVER iceberg 0011223344 27002
```

Important

If the hostname or port of your license server has changed, you will need to update this setting and restart the ICE RemoteWare service.

Note

Flexera typically creates a `$HOME/.flexlmrc` file in Linux or a Windows registry setting to cache successful license checkout locations for future use.

The order of precedence for license searching paths is as follows:

1. PENGUIN_LICENSE_FILE environment variable
2. LM_LICENSE_FILE environment variable

3. Server.License.FileName configuration setting
4. Flexera cache

4.4 Testing your Floating / Node-Locked License Install

To test if the ICE RemoteWare host can checkout licenses from the ICE FlexLM host, sign into the ICE RemoteWare host and use the `lmutil` tool:

```
lmutil lmdiag [-c license-file]
```

For example, if your ICE FlexLM server is running on port 27002 and the IP address is 192.168.1.7, a successful test will look like:

```
lmutil lmdiag -c 27002@192.168.1.7

lmutil - Copyright (c) 1989-2016 Flexera Software LLC. All Rights Reserved.
FlexNet diagnostics on Fri 12/1/2010 08:00

-------------------------------------------------------
License file: 27002@192.168.1.7
-------------------------------------------------------
"irw" v1.000, vendor: PENGUIN, expiry: 01-aug-2027
  License server: 192.168.1.7
  nodelocked license locked to NOTHING (hostid=ANY)  starts: 1-jan-1990,   expires: 01-
↪aug-2027

This license can be checked out
-------------------------------------------------------
```

If license checkout fails, the output of this command can be useful for troubleshooting license checkout issues. If you would like additional support, please contact Penguin Solutions at support@penguinsolutions.com.

Once the license file is installed, proceed to: *Setup*.

CHAPTER

FIVE

SETUP

Attention

We recommend using the latest config file as a starting point and moving changes from your old config file into the new one.

Configuration values are defined by nested XML elements in the `ice-remoteware.xml` config file. This can be found:

- Linux: `/opt/ice-remoteware/ice-remoteware.xml`
- MacOS: `/Applications/ICE RemoteWare.app/Contents/Resources/ice-remoteware.xml`
- Windows: `C:\Program Files\Penguin Solutions\ICE RemoteWare\ice-remoteware.xml`.

This section describes properties in the config file.

For the purpose of this document, we refer to properties by using dot notation. For example, `config.Server.Log.Level` indicates that `LogLevel` is a property within `Server`, which is a property within `config`. Since all properties begin with 'config', for brevity we ignore it. Properties are case-sensitive.

Warning

The config file and private key files contains sensitive information that can compromise security if an attacker can read it. We strongly recommend limiting read and write access to the root / system administrator account.

Warning

The ICE RemoteWare™ software includes a default private key, certificate file, username, and password that are not secure and should be changed.

5.1 Applying Config File Changes

Saved changes to the config file are only applicable once the service restarts. The Server.Auth.ShadowPassword setting is the one exception to this rule - saved changes to it are applicable immediately.

In Linux you can restart the service using the `systemctl restart` command:

```
systemctl restart ice-remoteware.service
```

In Windows you can restart the service using the Services tool. First open the Task Manager by right-clicking on the Task Bar and select `Start Task Manager`. At the Task Manager, go to the `Services` tab and click on `Services`. Right-click on `ice-remoteware` in the list of services and select `Restart` from the dropdown of actions.

In MacOS you can restart the service by calling the application with the `--service restart` flag. For example:

```
# Change to the application directory
cd /Applications/ICE RemoteWare.app/Contents/MacOS

# Restart the service
sudo ./ice-remoteware --service restart
```

The ICE RemoteWare sign-in page should return after a few seconds.

> **Attention**
>
> We recommend using the latest config file as a starting point and moving changes from your old config file into the new one.

The default config file comes with appropriate values for nearly all of the server settings.

In this section we discuss config settings that are commonly changed from the default config file.

5.2 License Management

For more information on license management, please see: *Flexera License Management*.

5.3 Server Authentication

Users are authenticated using credentials defined by the config file or by the ScyldCloudAuth web service. To disable any of these, simply comment out these elements by wrapping them with `<!--` and `-->`.

Authentication is enabled by default and in should not be disabled in production systems. *Server.Auth.Enabled* should always be set to `true`.

There are several authentication schemes supported by the ICE RemoteWare software. Each system is independent and can be enabled in parallel.

- Config File Authentication
- ScyldCloudAuth Authentication
- OS Credential Authentication

5.3.1 Config File Authentication

In addition to OS credentials, you can setup a username and hashed password in the config file to sign in to the ICE RemoteWare software. These config file credentials can sign into the ICE RemoteWare product at any time. This differs from OS credentials, which can only sign into the ICE RemoteWare software if the OS greeter screen or that user's desktop is showing. Config file credentials are independent from LDAP, the remote operating system, and ScyldCloudAuth.

Config file credentials are only enabled if `Server.Auth.Username` and `Server.Auth.ShadowPassword` tags exist, are uncommented, and both have values. The following settings control Config File Authentication:

- *Server.Auth.Username*
- *Server.Auth.ShadowPassword*
- *Server.Auth.MinPasswordLength*

Config File Authentication can be disabled by commenting or removing *Server.Auth.Username* and *Server.Auth.ShadowPassword*.

To set the password, verify that the `Server.Auth.Username` and `Server.Auth.ShadowPassword` tags exist **and are uncommented** in the config file (that is, they are not surrounded by `<!--` and `-->`). If the value of either tag is blank, the account is considered disabled.

If these tags do not already exist, insert both of them and set a value for `Server.Auth.Username`. For example:

```
<Server>
  ...
  <Auth>
    ...
    <Username>admin</Username>
    <ShadowPassword></ShadowPassword>
    ...
  </Auth>
  ...
</Server>
```

You can now set this password by opening a terminal, changing to the directory of the ICE RemoteWare binary, and running ice-remoteware with an OS-specific `passwd` flag:

```
# Linux:
sudo ice-remoteware.sh --passwd

# Windows (as an Administrator):
ice-remoteware.exe /passwd

# MacOS:
sudo ice-remoteware --passwd
```

The password change takes effect immediately.

Password strength requirements are described in the Setup chapter under *Server.Auth.ShadowPassword*.

Important

This only changes the Server.Auth.ShadowPassword entry in the config file. It does not change the passwords used by the remote operating system, LDAP, or ScyldCloudAuth.

5.3.2 ScyldCloudAuth Authentication

ScyldCloudAuth Authentication uses the ScyldCloudAuth proxy service for authentication. To enable ScyldCloudAuth for authentication, set:

- *Server.Auth.ScyldCloudAuth.URL*
- *Server.Auth.ScyldCloudAuth.Allow*
- *Server.Auth.ScyldCloudAuth.Deny*
- *Server.Auth.ScyldCloudAuth.ApiKey*
- *Server.Auth.ScyldCloudAuth.ApiSecret*

ScyldCloudAuth can be disabled by commenting or removing *Server.Auth.ScyldCloudAuth.URL*.

5.3.3 OS Credential Authentication

The credentials accepted by your remote Linux, Windows, or MacOS host can be used to sign into the ICE RemoteWare product. This supports ActiveDirectory for Windows, and LDAP / PAM for Linux.

Important

While config file or ScyldCloudAuth usernames can be used to sign in to the ICE RemoteWare product at any time, only a single set of OS credentials can be used to sign-in at a time. This prevents different OS credentials from signing in at the same time.

This feature can be disabled by setting *Server.Auth.OSAuth.Enabled* to `false` or removing it from the config file.

5.3.4 External Sign-In Pages

If your organization wants to use an external webpage for signing into the ICE RemoteWare product, you can set the *Server.Auth.ExternalSignInPage* setting to the URL. The ICE RemoteWare sign-in page will show a link to the external sign-in page instead of the default sign-in interface.

5.4 Server Security

5.4.1 HTTPs Security

The cipher list will determine what ciphers are used to encrypt communication between your clients and your server. It is always a good idea to keep your server's OpenSSL updated to the latest version.

We recommend using the default values for *openSSL.server.cipherList*.

5.5 Client Security

Clients and browsers that meet the requirements listed in *Client Requirements* support TLS 1.2, WebGL, and WebSockets by default and require no further setup.

> **Attention**
>
> Contact your system administrator if TLS 1.2, WebGL, or WebSockets are disabled.

5.6 Firewall

Your server host's firewall needs to allows incoming connections to the server over port 443 if you are using use HTTPS or port 80 if you are using HTTP.

In Linux, you will have to update your firewall using iptables. In most cases, adding the following line to your rules file (Rocky/CentOS/RHEL: `/etc/sysconfig/iptables`) and restarting the iptables service will allow incoming HTTPS traffic.

```
# Allow all https
-A INPUT -p tcp --dport 443 -j ACCEPT
```

Change 443 to 80 in the line above to accept incoming HTTP traffic over port 80 instead.

In Windows these rules are automatically set by the installer and removed by the uninstaller.

5.7 HTTPS / SSL Certificates

HTTPS and trusted SSL certificates are required to make all of your interactions with the server secure.

To ensure that connections are using the latest TLS protocol (as of 2015), set *openSSL.server.requireTLSv1_2* to `true` and enable HTTPS by setting *Server.Network.Secure* to `true`.

Set *openSSL.server.privateKeyFile* and *openSSL.server.certificateFile* to the appropriate private key and SSL certificate paths.

If you have set a passphrase for your private key you will need to set *openSSL.server.privateKeyPassphraseHandler.options.password*.

An SSL certificate signed by a trusted certificate authority (CA) is used to encrypt and authenticate communication between a browser and server. To obtain an SSL certificate from a CA, you need to generate a certificate signing request (CSR) and submit it to the CA. A list of popular CA's is given below:

- https://www.digicert.com/
- http://www.entrust.com/ssl-certificates/
- http://www.geotrust.com/
- https://www.thawte.com/

Linux users need to install OpenSSL on the server to complete setup. For example:

```
# Rocky, CentOS and RHEL Linux
sudo yum install openssl

# Ubuntu
sudo apt-get install openssl
```

The following sections describe how to use the openSSL command to create a new private key and CSR, a new CSR from an existing private key, and a self-signed SSL certificate (not recommended).

5.7.1 Create a Private Key and a CSR

Use the openssl command to creates a 2048-bit private key (domain.key) and a CSR (domain.csr). If your CA supports SHA-2, add the -sha256 option to sign the CSR with SHA-2.

```
openssl req -newkey rsa:2048 -nodes -sha256 -keyout domain.key -out domain.csr
```

Fill out the prompted questions to complete the CSR.

> **Warning**
>
> The contents of your private key should never be shared with anyone.

5.7.2 Create a CSR from an Existing Private Key

To create a CSR from an existing private key:

```
openssl req -key domain.key -new -out domain.csr
```

Fill out the prompted questions to complete the CSR.

5.7.3 Create a Private Key and Self-Signed SSL Certificate

You can create a self-signed SSL certificate instead of having one signed by a CA. The disadvantage to this is that in order to establish trust between the browser and the server, you must make a security exception for this certificate when you visit the page or install it in every browser.

```
openssl req \
        -newkey rsa:2048 -nodes -sha256 -keyout domain.key \
        -x509 -days 365 -out domain.crt
```

Fill out the prompted questions to complete the CSR.

> **Warning**
>
> The contents of your private key should never be shared with anyone.

5.7.4 Create a Self-Signed SSL Certificate from an Existing Private Key

To create a self-signed certificate from an existing private key:

```
openssl req \
        -key domain.key -new \
        -x509 -sha256 -days 365 -out domain.crt
```

Fill out the prompted questions to complete the CSR.

5.8 Video Setup

5.8.1 Selecting a Video Source and Max Frame Rate

The ICE RemoteWare software currently supports these video sources: `x11`, `nvfbc`, `stream`, `windda`, and `default`.

- The `x11` video source uses software encoding and only works for Linux systems. It supports a max frame rate of up to 60 fps.
- The `nvfbc` video source is for Linux systems with an NVIDIA GPU and driver that support NVIDIA GRID or NVIDIA NvFBC. It supports a max frame rate of up to 60 fps.
- The `windda` video source is optimized for Windows and supports a max frame rate of up to 60 fps.
- The `stream` video source uses software encoding and is available on all operating systems. This video source supports a max frame rate of up to 60 fps on ARM-based Macs and 30 fps on all other systems.
- The `default` video source selects the default video source for your system:
  - On Windows systems, `windda` is selected.
  - On Linux systems, `x11` is selected. .
  - On MacOS systems, `stream` is selected.

The table below summarizes the default and configurable maximum frame rate settings for each video source:

Video Source	Default MaxFrameRate	Configurable MaxFrameRate
x11 (Linux)	30	60
stream (Linux)	30	30
nvfbc (Linux)	30	60
default (Linux)	see: x11	see: x11
windda (Windows)	30	60
stream (Window)	30	30
default (Windows)	see: windda (Windows)	see: windda (Windows)
stream (MacOS)	30	60
default (MacOS)	see: stream (MacOS)	see: stream (MacOS)

By default, the maximum frame rate is set to 30. To enable a maximum frame rate of 60 fps for the supported cases listed above, set `Server.Video.Encoding.H264.MaxFrameRate` in the config file. See *Server.Video.Encoding.H264.MaxFrameRate* for more information.

To change the video source, see *Server.Video.VideoSource* for more information.

5.8.2 Change Screen Resolution

> **Warning**
>
> Changing screen resolutions has these known issues:
>
> 1. **Multiple rapid resolution changes may lead to service instability.** Changing the screen resolution more than 5 times over a few seconds may cause the service to restart or quit.
> 2. **Windows users with an NVIDIA graphics card should use the NVIDIA Control Panel to change screen resolution.**

Change your screen resolution by using the provided Linux OS tools (dependent on distribution).

In Windows, right-click on the desktop and select `Screen resolution`. Change the resolution dropdown to your desired resolution and then click `OK`.

5.8.3 Downscale Screen Resolution

System administrators have the ability to restrict the maximum screen resolution in the config file at `ice-remoteware.xml` using the `Server.Video.MaxWidth` and `Server.Video.MaxHeight` settings. This is useful for preventing clients from being overwhelmed by the processing power required to work with high-resolution video.

If the user attempts to use a higher screen resolution, the user will get an alert and the video will be scaled down.

5.8.4 Enable 4K Support

As of v7.0.0 it is possible to support 4K desktops with the native, non-browser based client. This feature is not enabled by default and requires a configuration file change to disable the default screen size and bitrate caps. We recommend having a downlink of at least 20 Mbps to support the increased screen size.

In future releases 4K support will be enabled automatically.

> **Note**
>
> If you are not going to use 4K resolutions, then leave the following settings at their defaults by commenting them out or deleting them from the config file. The default screen size and bitrate caps are used to ensure a good user experience for slower clients.

To enable 4K support:

1. Open the xml config file.
2. Uncomment the `Server.Video.MaxWidth` and `Server.Video.MaxHeight` tags and set the values to `-1` to disable the resolution cap.
3. Save the config file and restart the service.

5.8.5 Configure Video Bit-Rate

As of v9.1.9, the default video bit-rate is calculated by using a linear regression of two values: 3000 kbps at 1280x720 and 6000 kbps at 1920x1080. A system administrator can customize bit-rates for different resolutions by adding two or more resolution and bit-rate pairings within the `Server.Video.AvgBitRate` config file setting. The syntax is as follows:

```
<width>x<height>=<bitrate>,<width>x<height>=<bitrate>,...
```

Example 1: The following is equivalent to the default bit-rate values: `1280x720=3000k,1920x1080=6000k`.

Example 2: The following can be used to specify a single average bit-rate setting across all resolutions: `1024x768=2m, 1600x900=2m`.

The linear regression algorithm is based on the two closest resolutions to allow a fine-grained bit-rate control. If the value only specifies one resolution and bit-rate, the service will use the specified average bit-rate for all resolutions.

5.9 Local-site Customization

You can modify the text and header fields on the ICE RemoteWare sign-in page. This allows you to guide users when connecting to the remote server by adding text for special purpose servers or by reminding users of special policies on a host. You can also change sign-in page if you have a customized authentication method like using a smart card generated key login token rather than a password.

See *Server.Customization* for a list of possible adjustments.

5.10 User Notifications

ICE RemoteWare displays by default a message on the server OS when a new user connects to the server mentioning user name and remote ip address. This behavior and the timeout of the notifications can be controlled by the configuration.

See *Server.UserNotifications*

5.11 Multi Server (Linux only)

The ICE RemoteWare™ system can be set up to run multiple server instances as services on a single host machine. For example, this can be used to provide access to different X11 sessions on the same machine. In order to configure an installation this way, a few steps have to be undertaken:

1. Choose short and descriptive names for the services.

   In the following text, we will use ‘gpu0’ and ‘gpu1’ to identify the services.

2. Disable the ‘default service’ using the `systemctl` command:

   ```
   sudo systemctl stop ice-remoteware.service
   sudo systemctl disable ice-remoteware.service
   ```

3. Run the following script with the service name as a parameter to configurate each service:

   ```
   sudo /opt/ice-remoteware/bin/setup-service-instances.sh <SERVICE_ID>
   ```

   e.g.:

```
sudo /opt/ice-remoteware/bin/setup-service-instances.sh gpu0
sudo /opt/ice-remoteware/bin/setup-service-instances.sh gpu1
```

The script creates a configuration file for each service. The file is named /opt/ice-remoteware//opt/ice-remoteware-<SERVICE_ID>.xml. For the example services, it creates /opt/ice-remoteware//opt/ice-remoteware-gpu0.xml and /opt/ice-remoteware//opt/ice-remoteware-gpu1.xml

4. Update the parameters of the newly created configuration file(s).

A. Define a unique port number under which the services are readable. See *Server.Network.Port* for details.

B. Adjust firewall settings to allow external hosts to reach the services.

C. If the services should access different X11 servers, change either the X11 display ID or the X11 seat. See *Server.X11.Seat* and *Server.X11.Display* for details.

5. Enable and start the newly defined services using the `systemctl` command:

```
sudo systemctl enable ice-remoteware@<SERVICE_ID>.service
sudo systemctl start ice-remoteware@<SERVICE_ID>.service
```

e.g.:

```
sudo systemctl enable ice-remoteware@gpu0.service
sudo systemctl start ice-remoteware@gpu0.service

sudo systemctl enable ice-remoteware@gpu1.service
sudo systemctl start ice-remoteware@gpu1.service
```

5.12 Multi Session (Linux only)

The Multi Session feature allows multiple users to run their own sessions concurrently. When Multi Session is enabled, an X-server and an ICE RemoteWare server are started for each user. After the start of the X-server, the ICE RemoteWare software connects the user to the user's specific X-server. This feature is different from the collaboration feature, which allows multiple users to connect to the same X-server.

The spawned sessions can be monitored by standard tools, e.g. querying the status using systemctl:

```
[root@localhost]# systemctl list-units | grep irw
  irw-session-user-a-9202.service  loaded active running   "ICE RemoteWare guest session,
↪ user user-a"
  irw-session-user-b-9203.service  loaded active running   "ICE RemoteWare guest session,
↪ user user-b"
```

or shutting a single session down:

```
[root@localhost]# systemctl stop irw-session-user-b-9203.service
```

5.12.1 Installation

Multi Session requires the installation of one additional X11 server, named Xvfb.

1. Install virtual X-server:

```
sudo dnf install xorg-x11-server-Xvfb -y    # RedHat/Rocky

sudo apt install xvfb -y                    # Ubuntu
```

2. Disable Wayland and replace with X11 by either editing `/etc/gdm*/custom.conf` and uncommenting '#WaylandEnable=false/WaylandEnable=false' or by executing the following command:

```
sudo sed -i 's/\#WaylandEnable=false/WaylandEnable=false/' /etc/gdm*/custom.conf
```

3. Temporarily disable firewall for testing purposes:

```
sudo systemctl stop firewalld     # RedHat/Rocky

sudo systemctl stop ufw           # Ubuntu
```

> **Attention**
>
> If you run the server on a cloud system, check if the cloud service provider uses a global firewall independent of the host's settings. If there is a global firewall, you need to open individual ports depending on the server's setup.
>
> See *Server.MultiSession.PortNumbersBegin* and *Server.MultiSession.PortNumbersEnd*

4. Enable the ICE RemoteWare Multi Session feature by using the `Advanced Settings Tool` in the client UI or by editing `/opt/ice-remoteware/ice-remoteware.xml` and adding the following lines:

```
<Server>
 ...
  <MultiSession Enabled="true">
 ...
</Server>
```

5. Restart the `ice-remoteware` service:

```
sudo systemctl restart ice-remoteware
```

6. Patch the Gnome Display Manager setup:

```
sudo bash /opt/ice-remoteware/bin/setup-multisession-host.sh
```

   This will enable the guest sessions to run in parallel with any host X11 sessions

By default, users connect to the newly spawned sessions. Only the configuration file user (if set up) can access the host X server by default. Use the *Server.MultiSession.HostAdmins* configuration setting to grant access to the host X session to selected users.

5.12.2 Configuration

We provide an example configuration file at `examples/configs/ice-remoteware.MultiSession.xml`. This file can be used as a starting point to configure the server.

- Port Range

  After a user logs in, the ICE RemoteWare software assigns a dedicated port to the user's session. The range of available ports is set using the *Server.MultiSession.PortNumbersBegin* and *Server.MultiSession.PortNumbersEnd* settings.

- Number of Allowed Concurrent User Sessions

  The maximum number of users who can login concurrently is set using the *Server.MultiSession.MaxClients* setting.

- Desktop Resolution of User Sessions

  The dimensions of the desktop size for all user sessions is set using the *Server.MultiSession.Guests.DefaultWidth* and *Server.MultiSession.Guests.DefaultHeight* settings.

5.12.3 Security

By running the guest session as a service, the user session is isolated from the rest of the system. Currently there are two settings natively supported by the server:

- HidePIDs

  This setting will trigger the server to remount the `/proc` filesystem with the option `hidepid=2` as soon as the first guest session starts. This will hide all process entries in the directory from other users. Please note that the changes apply to all users on the server. If certain users need to see all pids, you need to create a group and add these users to it. Then set the value of *Server.MultiSession.Secure.HidePIDs.GroupID* to the newly created group id.

  See *Server.MultiSession.Secure.HidePIDs.Enabled*

- PrivateTmp

  This setting will create an overlay of the `/tmp` and `/var/tmp` directories for the service process. This way no data is shared between the users of the server in these directories.

  See *Server.MultiSession.Secure.PrivTmp.Enabled*

5.12.4 Usage

1. Open a browser and connect to the remote server.
2. Enter the user's credentials.

The user is connected to their desktop.

Note

- For each user who connects, a new X-server is started. When the user stops the session, the X-server is shut down. When the user decides to sign out, the session will be kept alive after the user disconnects. This way the user can reconnect to the session later.
- The number of users that can connect concurrently is not limited other than by the resource limitations of the remote server.

5.12.5 GPU Forwarding

When GPU Forwarding is enabled, set by *Server.MultiSession.GPUForwarding.Enabled*, the host server assumes that X11 Xscreens are assigned to a separate GPU and uses this information to distribute the GPUs evenly to the guest sessions.

The guest session defines the `VGL_DISPLAY` environment variable which routes all OpenGL calls to the appropriate GPU.

Setup

To take advantage of the assigned GPU, the user needs to start any OpenGL program with the helper tool `vglrun`. This tool will route any OpenGL call to the assigned GPU.

To install `vglrun` on RPM-based Linux systems:

```
sudo dnf install VirtualGL -y
```

To install `vglrun` on Debian-based Linux systems, download the latest package from the official VGL website and install the downloaded package:

```
sudo apt install ./virtualgl_<VERSION>_amd64.deb -y
```

Test GPU Forwarding

1. Log in to the server as a guest user.
2. In the guest session, open a terminal and run the `glxgears` program in a terminal:

   ```
   glxgears
   ```

The program reports the frames per second it can render. Because this is done in software, the numbers should be low.

3. Run the program again with GPU support:

   ```
   vglrun glxgears
   ```

Because the OpenGL calls are processed by the assigned GPU, the number of frames per second should be significantly higher.

Transparent launch of OpenGL programs

As it is not always possible to prefix all calls to programs with vglrun, we provide a simple launcher application called `vgllauncher` to simplify automatic GPU assignment.

Depending on your setup, `vgllauncher` operates in two modes to support different usage scenarios. Both modes is in common, that the administrator creates a link on the launcher, which is named like the executable which should be assigned to a GPU. The launcher will then locate the target and start it with `vglrun` support

- Configuration based on PATH variable

  This is the preferable setup method, but it is more dependent on the way the applications are started. Two steps are required. First, the administrator needs to create a directory and links to the target executables, e.g.:

```
mkdir /usr/share/vgl-bin
cd  /usr/share/vgl-bin
ln -s /opt/ice-remoteware/bin/vgllauncher glxgears
```

In a second step, the users' environments have to be altered to make the newly created directory the first directory in the path variable, e.g.:

```
export PATH=/usr/share/vgl-bin:${PATH}
```

After reloading the environment all calls to glxgears will be intercepted by the launcher and handed over to `vglrun`.

- Configuration based on modifying file names

  When the application is started by scripts which modify the PATH variable themselves, the setting up the system like descripted before might impose various problems. In these cases, it might be easier to follow this approach:

  The system administrator has to rename the executables within the original application directory by appending the fixed extension `.vgl-orig` to the file name. In a second step a link to the launcher is created with the original name of the executable, e.g.:

```
cd /usr/bin
mv glxgears glxgears.vgl-orig
ln -s /opt/ice-remoteware/bin/vgllauncher glxgears
```

  This way the launcher is called independently of the user's path setting. This is more invasive than the first method and will require some clean-up before updating or after deinstalling the application.

When problems show up, set `VGL_LOG_INFO` or `VGL_LOG_DEBUG` and run the program again. The output shows in detail which paths are considered and where the executables are found.:

```
VGL_LOG_INFO=1 glxgears
```

Security Considerations with GPU Forwarding

As the guest sessions have access to the host's X11 server to render on their assigned GPU, the host's X11 user session might expose resources to the users of the guest sessions.

When *Server.MultiSession.SecureAdminLogin* is set to true, the host server goes into maintenance mode as soon as an unlocked X11 session is running on the host. In this mode it will disable all guest sessions in order to prevent any risks of malicious user trying to access any private resources of the host session . When the host server's X11 session is terminated, it will then allow users to create guest sessions again, but disable any pasting of passwords into the OS to secure the login session as well.

Any remote `ssh` access is unaffected as no X11 resources will be shared.

Limitations

When Multi-Session is enabled, audio is not supported on the host session.

On Ubuntu guest sessions can't execute any applications which are installed as `snap(8)` applicaton from the GUI. There is a disagreement between the `snapd` and the guest gnome-session about the proper dbus address. There are two work arounds

- Install the non-snapped version of the applications
- Modify the users' shell environment and start the application from a terminal.

The guest server sets an environment variable `DBUS_SESSION_BUS_ADDRESS_SNAP` to simplify user setup. Add the following code to the resource file of the users' shell, e.g. into `~/.bashrc`:

```
if [[ ! -z "${DBUS_SESSION_BUS_ADDRESS_SNAP}" ]] ; then
  export DBUS_SESSION_BUS_ADDRESS=${DBUS_SESSION_BUS_ADDRESS_SNAP}
fi
```

This will enable the user to start any applications from a terminal.

5.12.6 Troubleshooting

Make sure:

- Firewall is disabled while testing
- All required tools are installed (see Setup)

CHAPTER

SIX

USAGE

In this section we describe how to start and stop the ICE RemoteWare™ service in either Linux or Windows on the remote server. We then talk about how to connect and interact with the remote desktop interface.

6.1 Using the Linux Service

To start, stop, or restart the ice-remoteware, open a terminal with root or sudo privileges and use the `service` command:

```
# Start the service
service ice-remoteware start

# Stop the service
service ice-remoteware stop

# Restart the service
service ice-remoteware restart
```

To run ice-remoteware directly rather than as a service, on Linux and Windows you have the option to run the server ice-remoteware from the command line. This is usually only useful for debugging purposes.

Windows (options shortened):

```
usage: ice-remoteware OPTIONS

/help                                   Display help information on command line␣
↪arguments
/logLevel=level                         Set the log level (ex: trace, debug,␣
↪information, notice, warning, error,
                                                                critical, none)
/version                                Display the version number
/application                            Run in application/console)
/validate                               Validate installation (text or html)
/passwd                                 Change the admin password
/broker-passwd                          Change the broker password
/check-license                          Check, if valid license is installed
/writeConfigFull=[filename]             Write configuration file (all options)
/config=filename                        Load additional configuration from file
/setConfig=<path>=<value>               Set a specific config value
/disableMouse                           Disable capture of mouse movements
```

Linux (options shortened):

```
usage: ice-remoteware OPTIONS
ice-remoteware -- a GPU accelerated remote desktop web service.

--help                                  Display help information on command line␣
↪arguments
--logLevel=level                        Set the log level (ex: trace, debug,␣
↪information, notice, warning, error,
                                                                critical, none)
--version                               Display the version number
--application                           Run in application/console)
--validate                              Validate installation (text or html)
--passwd                                Change the admin password
--broker-passwd                         Change the broker password
--check-license                         Check, if valid license is installed
--writeConfigFull=[filename]            Write configuration file (all options)
--config=filename                       Load additional configuration from file
--setConfig=<path>=<value>              Set a specific config value
--disableMouse                          Disable capture of mouse movements
```

6.2 Using the Windows Service

To use the ice-remoteware service, verify that the service is registered with the OS and then start the service.

6.2.1 Open a Command Prompt as an Administrator

1. Sign in as a user with Administrator permissions.
2. Open the Windows Start menu.
3. In the Search box, type `Command Prompt`, but don't hit `Enter` just yet.
4. Right-click on the Command Prompt and select `Run as administrator`.

6.2.2 Register the Windows Service

To register the windows service, use the `ice-remoteware.exe` command:

```
ice-remoteware.exe /registerService /startup=automatic
```

The ice-remoteware service will now automatically start on reboot.

Note

Service registration should already be handled by the installer. If you see the message below, verify that ice-remoteware has been properly installed. This is usually a sign that the PATH environment variables are not pointing at the ice-remoteware.exe file.

```
'ice-remoteware.exe' is not recognized as an internal or
 external command, operable program or batch file.
```

6.2.3 Start and Stop the Windows Service

To start and stop the registered windows service without rebooting, use the `net` command:

```
# Start the service
net start ice-remoteware

# Stop the service
net stop ice-remoteware
```

6.3 Using the MacOS Service

To start, stop, restart, or check the status of the ICE RemoteWare service, open a terminal and go to the `/Applications/ICE RemoteWare.app/Contents/MacOS` directory. Next, run the application with the `--service` flag with sudo privileges:

```
# Change to the application directory
cd "/Applications/ICE RemoteWare.app/Contents/MacOS"

# Start the service
sudo ./ice-remoteware --service start

# Stop the service
sudo ./ice-remoteware --service stop

# Restart the service
sudo ./ice-remoteware --service restart

# Check the status of the service
sudo ./ice-remoteware --service status
```

6.4 Manually running the MacOS audio server (advanced)

The ICE RemoteWare audio server is usually launched after a user logs in to MacOS (assuming it has been added to Login Items for that user). If this is not the case, one alternative way to temporarily launch the audio server is to open a terminal and run these commands:

```
# Change to the application directory
cd /Applications/ICE RemoteWare.app/Contents/MacOS

# Start the audio server
./ice-remoteware --audio-server
```

6.5 Log Output

Log output is organized by priority levels (from highest to lowest: Fatal, Critical, Error, Warning, Notice, Information, Debug, and Trace). By default, ice-remoteware prints Information level messages to `/var/log/messages`.

Setting `LogLevel` to `information` will log all server starts/stops, sign-in attempts, socket connects/disconnects, video source plays/pauses, and additional warning/error messages. This is usually sufficient for production usage.

To see debug and higher-level output, open the ice-remoteware.xml config file and set `LogLevel` to `debug`.

The most useful log files for the ICE RemoteWare software can be found at these locations:

```
# Linux:
/opt/ice-remoteware/ice-remoteware.log.

# Windows:
C:\Program Files\Penguin Solutions\ICE RemoteWare\log\ice-remoteware.log
C:\Program Files\Penguin Solutions\ICE RemoteWare\log\ice-remoteware-service.log.

# MacOS:
/var/log/com.penguinsolutions.ice-remoteware/ice-remoteware.log
```

Note

You can change the path of the output by opening the `ice-remoteware.xml` config file and setting `Server.Log.FileName` to a new destination.

By default, the ICE RemoteWare software displays a timestamp with each log message. To change the timestamp to all of your output, open the `ice-remoteware.xml` and set `LogFormat`. For more information, see *Server.Log.Format*.

6.6 Sign In

Once the ICE RemoteWare server starts, users can connect their networked client to the server by typing the server's URL into a web browser. Servers using the HTTPS protocol (default) have URLs like this: `https://<server-hostname-or-ip>`.

This will take you to the ICE RemoteWare sign-in page. Enter the either the OS username and password, the username and password encrypted in the config file or by ScyldCloudAuth to sign in.

Consult *Server Authentication* on how to setup server access

Important

While config file or ScyldCloudAuth usernames can be used to sign in to the ICE RemoteWare software at any time, only a single set of OS credentials can be used to sign-in at a time. This prevents different OS credentials from signing in at the same time.

After signing in, you will see a loading screen that will turn into a remote visualization display within a few seconds. At this point you can interact with the remote operating system. Other user accounts are prevented from signing into the web service until you sign out. This doesn't apply to the account specified in the config file.

6.7 Main Toolbar

The main toolbar gives access to additional ICE RemoteWare features such as signing out. This menu can be hidden or shown by pressing `Ctrl+F12` or using the hide/show button at the bottom of the screen.

6.7.1 Toggle Audio

Click the `Toggle Audio Streaming` button to begin streaming the default audio output device of the remote server. The default output device is managed through your remote operating system's audio device interface.

> **Note**
>
> For Linux users, Puleaudio version 10.0+ is required.

6.7.2 Keyboard Menu

The Keyboard Menu contains a list of special actions and keyboard button presses to transmit to the remote system. The keyboard buttons are `Ctrl-Alt-Del` (Linux and Windows) and `Print Screen`.

Copy Remote To Local Clipboard

`Copy From Remote Clipboard` copies plain text contents from the remote clipboard to the local clipboard.

This feature can be disabled by setting *Server.Clipboard.Copy.Enabled* to `false`.

When multiple clients are connected, only the current Controller (see *Collaboration*) can copy from the server's into the local clipboard.

> **Note**
>
> Only characters that are supported by both the client and server can be copied/pasted.

> **Important**
>
> Due to the design of X11, Linux users might experience warnings about failing to copy the clipboard. Most of the time copying the buffer again will fix the problem.

Paste Local To Remote Clipboard

`Paste To Remote Clipboard` copies plain text contents from the local clipboard to the remote clipboard.

Some browsers require the user to confirm the control of the clipboard contents to the browser. In this case the browser will show a message which requires the user to confirm the transaction. While Chrome remembers the user's answer, Firefox shows every time a small pop-up asking for confirmation.

When multiple clients are connected, only the current Controller (see *Collaboration*) can paste text into the server's clipboard.

This feature can be disabled by setting *Server.Clipboard.Paste.Enabled* to `false`

Note

Paste with keyboard shortcuts see *Server.Clipboard.Paste.KeyboardShortcut*

6.7.3 File Handling Menu

The File Handling Menu contains support for uploading and downloading files to and from the server. When either of those actions is active, the server displays information about the transfer progress.

When multiple clients are connected, this control is only accessible to the current Controller (see *Collaboration*).

`Upload Files to Server` opens a file explorer on the client to select one or multiple files to be uploaded to server. Alternatively, you can select the files in the client OS file explorer and drag a selection of files to the canvas to be uploaded.

Configuration options can be found at *Settings File Upload*

`Download Files from Server` initiates a transfer of a list of files from the server to the client. The user selects files to be copied to the client by selecting the files in a file browser and pressing the [CTRL] + [C] keys (Windows & Linux). If no files are selected, the server will try to copy all files in the upload directory.

Configuration options can be found at *Settings File Download*

6.7.4 USB Menu

The USB Menu contains a list of USB devices that can be forwarded to the remote server. This menu only appears if you've purchased a license for USB Forwarding, you are a host user, and you are the controller of the remote keyboard.

When multiple clients are connected, this control is only accessible to the current controller.

Note

USB Forwarded devices will disconnect every time a user:

- disconnects from the ICE RemoteWare service
- signs in or signs out of the remote OS
- adds or removes a monitor on the remote server
- loses controller status (gives up remote keyboard control)

```
sudo modprobe -r hid_wacom wacom wacom_w8001
sudo modprobe -a hid_wacom wacom wacom_w8001
```

6.7.5 Settings Menu

The Settings Menu provides options for adjusting view, monitoring performance, and selecting between three video quality settings (this last option is available to native client users only). If video is being downscaled it also provides a status message.

You can adjust the view settings by toggling `Fit to Window` view or `Full Screen` view.

`Performance Monitor` adds a pop-up at the bottom of the remote desktop window that displays current frames per second (FPS), ping speed (in ms), and video bandwidth (in Kbps). You can close the pop-up by either clicking the X on the pop-up or by toggling `Performance Monitor` under the `Settings` menu.

`Advanced Settings` allows administrator to configure the server from the client. Clicking on the icon opens the Advanced Settings page which exposes most of configuration variables of the server. Initially showing only the common settings, the view can be customized to show more advanced settings or show only modified values. Changing some of the values require a server restart which will disconnect all guest users and session.

When multiple clients are connected, this control is only accessible to the current Controller (see *Collaboration*).

When the `LogViewer` feature is enabled, administrators can open the log files of the server from the client window. A new page will be opened with the current log file loaded. While the user is logged in this page can be refreshed by the browser to update the log file shown.

Configuration options can be found at *Settings LogViewer*

`Auto-Sync Clipboard` is only accessible in the Native Client. When enabled the Client will sync server and client clipboards. When disabled the Keyboard Menu will show the `Copy From Remote Clipboard` and `Paste To Remote Clipboard` controls.

When multiple clients are connected, this control is only accessible to the current Controller (see *Collaboration*). The Client will remember the setting.

Configuration options can be found at *Settings Clipboard*

See also *Copy Remote To Local Clipboard*

The `Video Quality` slider is enabled when connecting with the Native Client and the display is not shared with other users.

Higher quality video settings result in better color accuracy at the cost of higher bandwidth usage and lower frame-rates. The three video quality settings are: `normal` (lossy with best frame-rate and lowest bandwidth usage), `visually lossless` (close to lossless quality with better frame rates and lower bandwidth usage), and `truly lossless`.

Important

Enabling lossless video on a downscaled video may improve image quality, but is not truly lossless.

Important

Currently only `normal` video quality is available when multiple users are signed in.

6.7.6 User Tools Menu

The User Tools Menu provides options for inviting guests, pausing guest video streams, and removing all guests and cancelling guest invites.

6.8 UI Keyboard Shortcuts

The following keyboard shortcuts are supported:

- `Ctrl+F11`: Toggle Fullscreen (Native Clients only)
- `Ctrl+F12`: Toggle Main Toolbar

6.9 Sign Out

Linux, Windows, and MacOS users change users by using the remote OS's log out / log in feature. The ICE RemoteWare software does not support "fast user switching" and the service must be restarted if this happens.

Closing your browser or signing out of the ICE RemoteWare session does not sign you out of the remote operating system. Use the remote OS's signing-out capability to sign out of the remote OS.

6.10 End Session (Linux, MultiSession only)

When the user is connected to a Guest Session, signing out keeps the session alive to connect at a later time. `End Session` will log out the user and end the session. A later connection will initiate a new session for the user to connect to.

See *Multi Session (Linux only)*

CHAPTER

SEVEN

COLLABORATION

7.1 Introduction

Multiple users can share control of the same desktop. There are two types of users in this case: regular Host users and temporary Guest users.

Hosts

Hosts are fully trusted users who have an account on the system and have complete control over what a Guest can access. An ongoing session begins when one Host is signed in and ends when the last Host leaves. All Guests and Invites are removed when an ongoing session ends.

Guests

Guests are users who are invited to join an ongoing session. As a Host, this can be useful when you want to share a workstation with a remote colleague who should not have a permanent account on the system.

Controller

When sharing the same desktop with multiple clients exactly one client controls the session's remote keyboard and mouse. This `Controller` has some additional privileges like e.g. remote clipboard access. This status can be transferred from one client to another. See *Give Keyboard and Mouse Control*

This section describes how a Host adds and manages Guest users.

Important

The Guest alerts and interface buttons described below are not visible in Fullscreen mode.

7.2 Set the maximum number of concurrent clients

By default, the server only allows 6 users to be signed on at any given time. This number can be changed by a system administrator by adding a `Server.Collaboration.MaxClientCount` setting in the config file at `ice-remoteware.xml`.

7.3 Collaboration Quick Start

At a high level, adding a new guest involves three steps:

1. A Host creates an Invite Link and sends it to Guest users.
2. A Guest opens the Invite Link, enters a Guest name, and requests to sign in.
3. A Host accepts the Guest's sign in request.

Hosts can use the control buttons to pause video to all Guests or ban all Guests and revoke all pending Invites. Hosts can also click on user buttons to remove individual Guests or give keyboard and mouse control.

7.4 Control Buttons

At the top of the screen there are a row of buttons that allow you to type special keys such as `Ctrl-Alt-Del`, add guests, pause all guest video, ban all guests, and sign out. Press `Ctrl+F12` to show / hide these buttons.

7.5 Add New Guests

Hosts can invite a group of guests by creating an Invite Link.

1. Click the `Invite Guests` button.
2. In the window that appears, specify how many guest sign ins you'd like this link to be accommodate. It is recommended to select the minimum number you will need.
3. The generated Invite Link is shown. Copy and send this link to Guest users and then close the window.

Warning

Anyone who receives an Invite Link can request Guest access to your system. While these links expire over time and are limited by how often they can be used, it is best practice to keep this link confidential.

When Guests use this link to request a sign in, an alert appears to all Hosts asking whether the user should be Accepted or Declined.

Important

It is best practice to verify the incoming user's identity via a phone call, text message, or other trusted communication channel.

When a Guest signs in, their username is reserved until all Hosts sign out. Guest usernames must be unique and consist of only letters, numbers, and underscores. Once the session ends, all Guest usernames are freed for use again.

7.6 Pause Guest Video

Guest video can be toggled by clicking on the `Pause Guests` button. Guest usernames will be greyed out when guest video is paused. Click `Resume Guests` to re-enable guest video.

7.7 Remove Guests and Cancel Invites

Guests can be removed from the session either individually using the `Kick` action from their username or all at the same time using the `Remove Guests and Cancel Invites` button from the User Tools menu. Hosts cannot be banned.

7.8 User Buttons

At the bottom of the screen there are a row of buttons containing usernames and status icons. The first button will always be "You", indicating the user button for the user signing in. Clicking on the user button will show status information (including frame rate) and actions that can be taken on that user, such as kicking or giving keyboard / mouse control.

Usernames that end with an asterisk are Hosts. Press `Ctrl+F12` to show / hide these buttons.

7.9 Give Keyboard and Mouse Control

A Host can give any other user control of the keyboard and mouse using the `Give Keyboard and Mouse Control` button from the username. The host can regain control using the `Take Keyboard and Mouse` button from their own user buttons (You).

CHAPTER

EIGHT

PERFORMANCE

Playback performance depends on three bottlenecks (in order of significance): network quality, client load, and server load. In this section we talk about each of these and how to determine which bottleneck requires attention.

8.1 Network Quality

Network quality can be measured as a combination of latency, throughput, and stability. When determining network quality, you may want to run the ICE RemoteWare™ software on its own to guarantee that other applications or clients are not consuming large amounts of network resources at the same time.

Latency between the client and server can be measured using `ping` times. Acceptable latency depends on the applications being used. CAD users, for example, may find ping times up to 150 ms to be quite usable and 300 ms to be usable for sporadic use. Testing and demoing of applications like Google Earth are typically over 802.11g connections with ping times of 30-80 ms.

When running fullscreen animations at 1440x900, the ICE RemoteWare software has a typical throughput consumption of 4 Mbps. Throughput consumption drops dramatically when pixels on the screen do not change. We conservatively recommend 5.5 Mbps. This is typically not a bottleneck for the ICE RemoteWare software since it's common for clients and servers to have more than 4 Mbps of bandwidth, but it is still worth remembering.

8.2 Client Load

Decoding is largely dependent on the web browser implementation and the CPU performance of the client. We recommend using Chrome as it performs best with ICE RemoteWare in testing.

CPU performance depends on the hardware and the load on the system. We test on modern CPUs such as the multi-core Intel i5s and i7s from 2011 and later. When evaluating playback performance, verify that other applications are not also consuming large amounts of CPU time.

Decreasing screen resolution on the server-side is another option for reducing load on the client. While we recommend 1600x900, users may find that 1280x720 offers a better overall experience.

If you are running the non-WebGL version of the ICE RemoteWare software, performance is expected to be considerably slower (depending on the CPU). Lowering the remote server's screen resolution and using Chrome is strongly recommended in this case.

8.3 Server Load

In our tests, a server forwarding a 1080p video with audio enabled typically uses between 50% to 85% of a single Intel Xeon E5 2.1GHz core from 2012. We recommend running with at least two cores for a single-display system.

8.4 Further Help

If you have additional questions about performance, please contact Penguin Solutions at support@penguinsolutions.com.

CHAPTER

NINE

SETTINGS GLOSSARY

In this section we describe all of the settings available in the config file.

> **Note**
>
> All changes to Scyld.Auth settings except Scyld.Auth.Enabled take effect without a service restart.

9.1 Server.AdvancedSettings

Advanced Settings, see *Settings Menu*

9.1.1 Server.AdvancedSettings.Enabled

Set to `true` to enable the Advanced Settings Tool on the client. A client connected as an OS user who is member of the administrator group (Windows) or the irw-wheel (Linux, MacOS) can use this tool to configure the server.

Defaults to `true`.

9.1.2 Server.AdvancedSettings.AdminOnly

When set to true access to the Advanced Settings Tool is limited to the configuration file user. See *Config File Authentication*

Defaults to `false`.

9.1.3 Server.AdvancedSettings.GuestAccess

Controls the access of guest to the Advanced Settings Tool on the client. When set to `true`, any guest can access this feature when they get control, such as access to the server's keyboard.

Be aware that a server restart will disconnect any guests, so the host has to issue a new invite.

Defaults to `false`.

9.2 Server.Audio

Audio forwarding related settings, see *Toggle Audio*

9.2.1 Server.Audio.Enabled

Determines if fetching the remote server's audio is allowed. Defaults to `true`.

If `true`, the remote server's audio can be streamed.

If `false`, the remote server's audio cannot be streamed.

When Multi-Session is enabled, audio is not supported on the host session.

Added in v10.0.0.

9.2.2 Server.Audio.Output.BufferTime

The buffering time (in seconds) for the audio output stream.

Lowering the time improves synchronization with the video stream, but may result in more playback skipping.

Increasing the time results in a more stable playback, but adds latency to audio playback and causes it to be less synchronized with the video stream.

> **Note**
>
> If you are using devices that add additional latency (such as Bluetooth speakers), then lowering this value may be beneficial.

Defaults to `0.020`.

Changed in v10.2.0.

9.2.3 Server.Audio.Output.SampleRate

Determines the audio sample rate in Hz. Higher sample rates lead to better audio quality, but consume more bandwidth. Supported values are `96000`, `48000`, `44100`, and `22050`.

> **Note**
>
> CD audio quality can be achieved with a sample rate of `44100` Hz and a format of `s16le`.

Defaults to `44100`.

Updated in v11.3.0. Added new supported values.

9.2.4 Server.Audio.Output.Stream.Format

Determines the audio output format. Note that audio bit depth (i.e., bits per sample) differs for each of the supported PCM formats below. Higher bit depth may improve audio quality, but will consume more bandwidth.

> **Note**
>
> CD audio quality can be achieved with a sample rate of `44100` Hz and a format of `s16le`.

Format	Description
`s8`	PCM 8-bit signed integer little endian
`s16le`	PCM 16-bit signed integer little endian
`s24le`	PCM 24-bit signed integer little endian
`f32le`	PCM 32-bit floating point little endian

Defaults to `s16le`.

Added in v10.2.0.

9.2.5 Server.Audio.Output.Stream.Device

Linux Only.

Determines the Pulseaudio monitor sink to fetch audio from on the server. These names must end with `.monitor`. Usually this value is automatically detected and updated to reflect the operating system's default audio device.

To force the system to use a specific device, use the command: `pactl list short sinks` to see a list of the device names. In the example below, there are two available sinks:

```
[root@server ~]# pactl list short sinks
0   alsa_output.pci-0000_00_04.0.analog-stereo  ...(additional text)...
1   alsa_output.pci-0000_00_05.0.analog-stereo  ...(additional text)...
```

To select the first device, set the value of this setting to: `alsa_output.pci-0000_00_04.0.analog-stereo.monitor`.

Defaults to `auto`.

Added in v10.0.0.

9.2.6 Server.Audio.Output.SampleRateAdjust

Sets the adjustment for the sample rate when server and client rates drift.

Defaults to `1.01`.

Added in v10.0.0.

9.2.7 Server.Audio.Output.StartDelay

Sets the initial delay (in fractions of a second) before the playback starts. A higher value may prevent noise due to empty sample buffer, but also adds delay to the playback.

Defaults to `0.050`.

Added in v10.0.0.

9.2.8 Server.Audio.Output.BitsPerSample

Sets the bits per sample.

Defaults to `16`.

Added in v10.0.0.

9.2.9 Server.Audio.Output.SamplesPerFrame

Defines the chunk size used during the transmission of audio data.

Defaults to `4096`.

Added in v10.0.0.

9.2.10 Server.Audio.Output.Threshold

Sets the audio output threshold.

Defaults to `0.150`.

Added in v10.0.0.

9.3 Server.Auth

Authentication Settings, see *Server Authentication*

9.3.1 Server.Auth.Enabled

Determines if authentication is enabled and valid credentials are required to sign-in (recommended).

Defaults to `true`.

If `false`, then all authentication is disabled and any credentials can be used to sign-in. Guest invites are also disabled in this case.

> **Note**
>
> Changing this value only takes effect after a service restart.

9.3.2 Server.Auth.AllowedGroups

Limits access to the server to users which are members of any group listed by this setting (currently Linux only).

By default not set.

9.3.3 Server.Auth.ExternalSignInPage

A URL to your organization's custom sign-in page. When this value is set to a non-empty string, the normal sign-in user interface is replaced with a link to the custom sign-in page.

> **Note**
>
> Setting this value does not enable or disable any authentication protocols. Users may still be able to sign in using ajax calls even if the normal sign-in user interface is disabled.

Added in v9.1.

9.3.4 Server.Auth.Username

Declares a username to be used in combination with the password defined by Server.Auth.ShadowPassword at the ICE RemoteWare sign-in page.

Config File Authentication can be disabled by commenting or removing *Server.Auth.Username* and *Server.Auth.ShadowPassword*. This must be specified with Server.Auth.ShadowPassword and is not necessarily the same as the username used by the remote operating system.

> **Note**
>
> Changing this value takes effect without a service restart.

Changed in v5.0.0.

9.3.5 Server.Auth.ShadowPassword

A shadowed password used to sign-in to the ICE RemoteWare sign-in page. Config File Authentication can be disabled by commenting or removing *Server.Auth.Username* and *Server.Auth.ShadowPassword*. The format is as follows:

```
$6$<salt>$<hash>
```

The initial 6 value should never be changed and signals that SHA-512 should be used. The <salt> and the plain text password are used to create the hashed password using the UNIX crypt method. See http://linux.die.net/man/3/crypt for more information on UNIX crypt.

> **Warning**
>
> Even though the ShadowPassword value encrypts your password, its contents should remain private. If you suspect that any part of the ShadowPassword has been compromised, change your password immediately using the password update utility:

- Linux: `sudo ice-remoteware.sh --passwd`
- Windows: `ice-remoteware.exe /passwd`
- MacOS: `sudo ice-remoteware --passwd`

Note

Changing this value takes effect without a service restart.

Changed in v11.1.0.

9.3.6 Server.Auth.MinPasswordLength

The built-in password updater uses this value to require a minimum password length for *Server.Auth.ShadowPassword* and *Server.Broker.ShadowPassword*.

Defaults to 6.

Note

Changing this value takes effect without a service restart.

Changed in v11.1.0.

9.3.7 Server.Auth.FailAttempts

The number of unsuccessful sign in attempts a client is allowed before the server temporarily rejects future requests from that client for a time period specified by Server.Auth.FailDelay. This helps reduce brute force attacks.

Note

Changing this value takes effect without a service restart.

Changed in v5.0.0.

9.3.8 Server.Auth.FailDelay

The length of time that the server will reject sign in requests from clients that repeatedly fail to sign in. See Server.Auth.FailAttempts for more information.

Note

Changing this value takes effect without a service restart.

Changed in v5.0.0.

9.3.9 Server.Auth.OnlyOSUser

When set to `true`, only the currently logged in username can be used to log into the server. If no user is logged in, any available username can be chosen.

This does not affect the configuration file admin user.

Defaults to `true`.

9.3.10 Server.Auth.HardenedConfig

If set to `true`, the server disables the following configuration settings by default:

- *Server.Clipboard.Copy.Enabled*: Copying clipboard from server to client
- *Server.Clipboard.Paste.Enabled*: Pasting client clipboard to server
- *Server.FileDownload.Enabled*: Downloading files from the server
- *Server.FileUpload.Enabled*: Uploading files to the server
- *Server.AdvancedSettings.Enabled*: Advanced settings editor
- *Server.LogViewer.Enabled*: Showing log files on the client
- *Server.License.Upload.Enabled*: Uploading licenses to the server
- *Server.Collaboration.Guests.Enabled*: Inviting guest clients to current session
- *Server.VirtualHere.Enabled*: USB forwarding

If any of the listed features should be supported by the server, they need to be explicitly activated in the configuration.

The server also sets the defaults to `true` for the following features:

- *Server.Misc.AutoLock.Enabled*: OS locking of the desktop
- *Server.UserNotifications.Enabled*: Notify OS user of events

Defaults to `false`.

9.3.11 Server.Auth.ScyldCloudAuth.URL

The URL to the Scyld Cloud Auth authentication web service. Only applies to Scyld Cloud Manager products.

> **Note**
>
> Changing this value takes effect without a service restart.

Changed in v5.0.0.

9.3.12 Server.Auth.ScyldCloudAuth.Allow

A list of <Username></Username> elements. Case insensitive. Each <Username> element enables a username to be authenticated by ScyldCloudAuth. Username elements can use asterisk wildcard characters (i.e. *@penguinsolutions.com enables all usernames that end in @penguinsolutions.com).

> **Note**
>
> Changing this value takes effect without a service restart.

Changed in v11.0.0.

9.3.13 Server.Auth.ScyldCloudAuth.Deny

A list of <Username></Username> elements. Case insensitive. Each <Username> element disables a username to be authenticated by ScyldCloudAuth. Usernames that are mentioned by both the Deny and Allow list are denied.

Username elements can use asterisk wildcard characters (i.e. *@penguinsolutions.com enables all usernames that end in @penguinsolutions.com).

> **Note**
>
> Changing this value takes effect without a service restart.

Changed in v11.0.0.

9.3.14 Server.Auth.ScyldCloudAuth.ApiKey

A string that uniquely identifies the server. This is required to make privileged Scyld Cloud Auth web service calls.

Added in v9.1.

9.3.15 Server.Auth.ScyldCloudAuth.ApiSecret

A string that represents a shared secret between the ICE RemoteWare product and the Scyld Cloud Auth server. This is required to make privileged Scyld Cloud Auth web service calls.

Added in v9.1.

9.3.16 Server.Auth.DefaultTimeout

The lifetime (in seconds) of a session token that starts upon successfully signing in. Session tokens let you access protected resources from the server such as creating a new remote-visualization connection. Increasing this value means a longer period of time you can access the resources without signing in again.

Existing remote-visualization connections are unaffected by session token timeouts. Defaults to 60 seconds.

> **Note**
>
> Changing this value takes effect without a service restart.

Changed in v5.0.0.

9.3.17 Server.Auth.OSAuth.Enabled

Determines if authentication using OS credentials is enabled. Defaults to `true`.

Important

While config file or ScyldCloudAuth usernames can be used to sign in to the ICE RemoteWare software at any time, only a single set of OS credentials can only be used to sign-in at a time. This prevents different OS credentials from signing in at the same time.

Note

Changing this value takes effect after a service restart.

Added in v6.1.0.

9.3.18 Server.Auth.OnSignIn

The path of a script to execute immediately after signing in. The script is passed the system account name of the user as an argument. By default, this is not set, but it can be used for custom sign-in initialization.

Note

Changing this value takes effect without a service restart.

Changed in v5.0.0.

9.3.19 Server.Auth.OSAuth.PAM.Service

The `service name` of the PAM (Pluggable Authentication Module) service. The service is defined by the file `/etc/pam.d/service name` or in /etc/pam.conf.

Defaults to `login`.

When changing the PAM method, it might be necessary to change the login hints on the sign-in page, see *Server.Customization.UserNameInput* and *Server.Customization.PasswordInput*

Added in v8.0.0.

9.4 Server.Broker

9.4.1 Server.Broker.Username

Declares a username to be used in combination with the password defined by Server.Broker.ShadowPassword for accessing API calls only.

Config File Authentication can be disabled by commenting or removing *Server.Broker.Username* and *Server.Broker.ShadowPassword*. This must be specified with Server.Broker.ShadowPassword and is not necessarily the same as the username used by the remote operating system.

Note

Changing this value takes effect without a service restart.

Changed in v11.0.0.

9.4.2 Server.Broker.ShadowPassword

A shadowed password used to sign in on the ICE RemoteWare sign-in page. Config File Authentication can be disabled by commenting or removing *Server.Broker.Username* and *Server.Broker.ShadowPassword*. The format is as follows:

```
$6$<salt>$<hash>
```

The initial 6 value should never be changed and signals that SHA-512 should be used. The <salt> and the plain text password are used to create the hashed password using the UNIX crypt method. See http://linux.die.net/man/3/crypt for more information on UNIX crypt.

Warning

Even though the ShadowPassword value encrypts your password, its contents should remain private. If you suspect that any part of the ShadowPassword has been compromised, change your password immediately using the password update utility:

- Linux: `sudo ice-remoteware.sh --broker-passwd`
- Windows: `ice-remoteware.exe /broker-passwd`
- MacOS: `sudo ice-remoteware --broker-passwd`

Note

Changing this value takes effect without a service restart.

Changed in v11.1.0.

9.5 Server.Clipboard

9.5.1 Server.Clipboard.AutoSync.Enabled

When set to `true users of the Native Client can choose to automatically sync server and client clipboards. This setting requires copy and paste of clipboards to be enabled.

Defaults to `true`.

9.5.2 Server.Clipboard.AutoSync.Notifications

When set to `true` all clipboard copy operations will trigger a notification on the client UI.

Defaults to `false`.

9.5.3 Server.Clipboard.Copy.Enabled

Enables copying the clipboard from the server to the client.

See *Copy Remote To Local Clipboard*

Defaults to `true`.

9.5.4 Server.Clipboard.Copy.MaxSize

This setting controls the maximum size of clipboard content allowed to be copied from the server to the client.

Default is `10m`.

9.5.5 Server.Clipboard.Copy.Bandwidth

Controls the maximum bandwidth used when copying server clipboard content to the client.

Default is `64m`.

9.5.6 Server.Clipboard.Copy.FragSize

Defines the size of the fragments sent during the transfer of the server clipboard to the client. This can be used to control the traffic patter during this operation as smaller fragments prevent peaks in bandwidth consumption Keep in mind that a smaller value puts more load on the clients.

Default is `131072`.

9.5.7 Server.Clipboard.Paste.Enabled

When set to `true`, clients can paste the contents of their clipboard to the server's clipboard.

See *Paste Local To Remote Clipboard*

Default is `true`.

9.5.8 Server.Clipboard.Paste.KeyboardShortcut

When set to `true` the user can use OS shortcuts to paste the server clipboard:

To paste text from a local Linux/Windows clipboard into a remote Linux/Windows desktop, press `Ctrl+v`.

To paste text from a local MacOS clipboard to a remote Linux/Windows desktop, use your browser's menu system to select `Edit > Paste`. This transfers the local clipboard to the remote clipboard. Once this is done, you can use `Ctrl+v` or use your remote application's paste feature.

This feature is disabled by default as it would interfere with a server-only workflow. Only when combining a MacOS server/client with a Linux/Windows client/server the system can distinguish between a local and a remote paste action.

Default is `false`.

Also, see notes at *Keyboard Menu*

9.5.9 Server.Clipboard.Paste.Bandwidth

Controls the maximum bandwidth used when copying the client clipboard to the server.

Default is `64m`.

9.5.10 Server.Clipboard.Paste.FragSize

Defines the size of the fragments sent during the transfer of the client clipboard to the server. This can be used to control the traffic patter during this operation as smaller fragments prevent peaks in bandwidth consumption Keep in mind that a smaller value puts more load on the clients.

Default is `131072`.

9.6 Server.Collaboration

Collaboration framework related setting, see *Collaboration*

9.6.1 Server.Collaboration.Guests.Enabled

When set to `true`, clients can invite guests to log in via a unique server-generated link. Guests are not authentificated by the server. This feature can be turned off by setting the value to `false`.

Defaults to `true`.

9.6.2 Server.Collaboration.Guests.MaxInviteTime

Time (in seconds) an invite link to join the session as guest is valid.

Defaults to `7200`.

9.6.3 Server.Collaboration.Guests.Reconfirm

When set to `false`, a guest using the invite link can connect to the server without a confirmation by the client that generated the invite.

Defaults to `true`.

9.6.4 Server.Collaboration.MaxClientCount

The maximum number of clients that can be connected at a time.

Note: This doesn't only apply to guests, but also to other connected users.

Defaults to `6`.

Added in v3.0.0.

9.7 Server.Customization

Server Web page customizations, for more information see *Local-site Customization*

When you are altering fields or labels on the sign-in page with HTML statements, use < for "<" and > for ">". Use for example "<h2>" instead of "<h2>".

The Advanced Settings page will translate any tags automatically.

The css file `signin-cust.css` in the wwwroot directory provides some editable style classes. While all other files in this directory are static, this one can be changed.

9.7.1 Server.Customization.MainPageTitle

Sets the title of the main page.

Default is `${HOSTNAME} - ${BRAND_TM_HTML}`.

9.7.2 Server.Customization.SignInCaption

Defines the caption displayed on the sign-in page.

Default is `${HOSTNAME}`.

9.7.3 Server.Customization.SignInTitle

Sets the title on the sign-in page and on the tabs of the connecting browser.

Default is `Sign In - ${HOSTNAME}`.

9.7.4 Server.Customization.UserNameInput

Sets the description of the user field on the sign-in page. Use this setting to adapt the sign-in page to your authentication method.

Default is `Username or Email`.

9.7.5 Server.Customization.PasswordInput

Sets the description of the password field on the sign-in page. Use this setting to adapt the sign-in page to your authentication method.

Default is `Password`.

9.7.6 Server.Customization.SignInFailWarning

Sets the warning message after an unsuccessful sign-in attempt. Use this guide the user based on your authentication method.

Default is `Incorrect username or password`.

9.7.7 Server.Customization.SignInWrongGroupWarning

Sets the warning message after an unsuccessful sign-in attempt, when a user is not a member of any group allowed to connect.

Default is `User is not member of any group allowed to sign-in`.

9.7.8 Server.Customization.SignInHint

The text of this setting will be shown on the sign-in page to guide the user based on the authentication method used. It accepts HTML code to format the message.

Default is not set.

9.7.9 Server.Customization.SignInCaptionGuests

Defines the caption displayed on the sign-in page for guest logins.

Default is `${HOSTNAME}`.

9.7.10 Server.Customization.SignInTitleGuests

Sets the title on the sign-in page for guests and on the tabs of the connecting browser.

Default is `Guest Sign In - ${HOSTNAME}`.

9.7.11 Server.Customization.Message.Text

Allows the system admin to show each user a small message when they log in, such as reminding the user of important policies on this specific machine.

Not set by default.

9.7.12 Server.Customization.Message.Timeout

Timeout (in seconds) of the initial welcome message.

Default is `5`.

9.8 Server.FileUpload

Upload files to server, see *File Handling Menu*

9.8.1 Server.FileUpload.Enabled

When set to `true`, users are allowed to upload files from the client to the server.

When set to `false`, no files can be uploaded.

Defaults to `true`.

Added in v13.2.1.

9.8.2 Server.FileUpload.Directory

Directory to store uploaded files on the server.

Defaults to `${HOME}/Downloads`.

Added in v13.2.1.

9.8.3 Server.FileUpload.MaxFileSize

Maximum file size a client is allowed to upload to the server.

Defaults to `100M`.

Added in v13.2.1.

9.8.4 Server.FileUpload.CreateDirectory

When set to `true`, the server creates the download directory on behalf of the user. See *Server.FileUpload.Directory*

When set to `false`, no directory is created.

Defaults to `true`.

Added in v13.2.1.

9.9 Server.FileDownload

Download files from server, see *File Handling Menu*

9.9.1 Server.FileDownload.Enabled

When set to `true`, clients are allowed to download files they have access to.

When set to `false`, no file downloads from the server are supported.

Defaults to `true`.

Added in v13.2.1.

9.9.2 Server.FileDownload.Directory

Directory of files to be downloaded to client.

The server monitors this directory and, when a new file is detected during an active client session, the server automatically downloads the file(s) to the client. Any files found in the directory at the start of the client session are ignored until the user clicks on `Download Files from Server` in the File Menu on the client UI. The server will then download all files in the directory to the client.

For details, see *File Handling Menu*

Defaults to `$ {HOME}/Desktop/Uploads`.

Added in v13.2.1.

9.9.3 Server.FileDownload.CreateDirectory

When set to `true`, the server creates the monitored directory on behalf of the user. See *Server.FileDownload.Directory*

When set to `false`, no directory is created.

Defaults to `false`.

Added in v13.2.1.

9.9.4 Server.FileDownload.MonitorDirectory

When set to `true`, the server monitors a special directory on behalf of the user. When `false` the server ignores the contents of this directory.

. See *Server.FileDownload.Directory*

9.9.5 Server.FileDownload.MaxFileSize

The maximum size a file might have when being downloaded to the client.

Defaults to `100M`.

9.10 Server.License

For information on license management, please see: *Flexera License Management*.

9.10.1 Server.License.Upload.Enabled

When set to `true`, the user can upload a new or updated license from the client.

Defaults to `true`.

Added in v13.2.1.

9.10.2 Server.License.FileName

Specifies a license file path or a `port@host` address where an ICE FlexLM license server is hosted. If the default license server port is being used (`27002`), then `@host` is also acceptable.

Defaults to `ice-remoteware.lic`.

Added in v5.0.0.

9.11 Server.LocalCursor

9.11.1 Server.LocalCursor.Enabled

Determines if the client's local cursor should be shown instead of the remote cursor. Enabling local cursor typically improves the user experience.

Defaults to `true`.

Added in v2.2.0.

9.12 Server.Log

9.12.1 Server.Log.Level

The verbosity of output in the log file.

The LogLevel value can be any one of the following (ordered least-to-most verbose): 'none', 'fatal', 'critical', 'error', 'warning', 'notice', 'information', 'debug', and 'trace'.

9.12.2 Server.Log.ServiceLogFile

A path to the log file of the ICE RemoteWare service. By default, this can be found in the directory of the ICE RemoteWare executable and is named `ice-remoteware-service.log`. For more information on log output, see *Log Output*.

Changed in v5.0.0. Previously named Server.ServiceLogFile in v2.2.0. Default value changed

9.12.3 Server.Log.Format

Format of the output. Defaults to: `%Y-%m-%d %H:%M:%S.%i:%q%q:%t`

The format pattern is used as a template to format the message and is copied character by character except for the following special characters, which are replaced by the corresponding value.

Table 1: Log Format Special Characters

Pattern	Description
%s	message source
%t	message text
%l	priority level (1 .. 7)
%p	priority (Fatal, Critical, Error, Warning, Notice, Information, Debug, Trace)
%q	abbreviated message priority (F, C, E, W, N, I, D, T)
%P	process identifier
%T	thread name
%I	thread identifier (numeric)
%N	node or host name
%U	source file path (empty string if not set)
%u	source line number (0 if not set)
%w	date/time abbreviated weekday (Mon, Tue, ...)
%W	date/time full weekday (Monday, Tuesday, ...)
%b	date/time abbreviated month (Jan, Feb, ...)
%B	date/time full month (January, February, ...)
%d	date/time zero-padded day of month (01 .. 31)
%e	date/time day of month (1 .. 31)
%f	date/time space-padded day of month (1 .. 31)
%m	date/time zero-padded month (01 .. 12)
%n	date/time month (1 .. 12)
%o	date/time space-padded month (1 .. 12)
%y	date/time year without century (70)
%Y	date/time year with century (1970)
%H	date/time hour (00 .. 23)
%h	date/time hour (00 .. 12)

continues on next page

Table 1 – continued from previous page

Pattern	Description
%a	date/time am/pm
%A	date/time AM/PM
%M	date/time minute (00 .. 59)
%S	date/time second (00 .. 59)
%i	date/time millisecond (000 .. 999)
%c	date/time centisecond (0 .. 9)
%F	date/time fractional seconds/microseconds (000000 - 999999)
%z	time zone differential in ISO 8601 format (Z or +NN.NN)
%Z	time zone differential in RFC format (GMT or +NNNN)
%L	convert time to local time (must be specified before any date/time specifier; does not itself output anything)
%E	epoch time (UTC, seconds since midnight, January 1, 1970)
%v[width]	the message source (%s) but text length is padded/cropped to 'width'
%[name]	the value of the message parameter with the given name
%%	percent sign

9.12.4 Server.Log.FileName

A path to the log file of the ICE RemoteWare server. By default, this can be found in the directory of the ICE RemoteWare executable and is named `ice-remoteware.log`. For more information on log output, see *Log Output*.

Changed in v5.0.0. Default value changed.

9.12.5 Server.Log.FileSize

Sets the maximal size of the server's log files (in KB).

Defaults to `24576`.

9.12.6 Server.Log.SystemLog.Enabled

When set to true the server will use the operating system logging facility (Linux only).

Defaults to `true`.

9.13 Server.LogViewer

Expose logs on client page, see *Settings Menu*

9.13.1 Server.LogViewer.Enabled

Set to `true` to show a link to the server's logfiles in the Settings menu.

See *Server.LogViewer.ServiceLog* and *Server.LogViewer.AccessLog*.

Defaults to `false`.

9.13.2 Server.LogViewer.AdminOnly

When set to true access to the LogViewer is limited to the configuration file user. See *Config File Authentication*

Defaults to `false`.

9.13.3 Server.LogViewer.GuestAccess

Controls the access of a guest to the exposed log files in the Settings menu. When set to `true`, guests can access the log files.

Defaults to `false`.

9.13.4 Server.LogViewer.ServiceLog

When set to `true`, the service log file is exposed in the client UI.

Defaults to `false`.

9.13.5 Server.LogViewer.AccessLog

When set to `true`, the access log file is exposed in the client UI.

See *Server.Network.Access.Logger.FileName*

Defaults to `false`.

9.14 Server.Misc

9.14.1 Server.Misc.AutoLock.Enabled

Determines if the ICE RemoteWare software calls on the OS to lock the desktop upon disconnecting from the web page.

Defaults to `false`.

> **Warning**
>
> In Linux, screen locking is achieved by entering `Ctrl+Alt+l` on behalf of the user. While this will lock the screen for most, this feature is not guaranteed to work on all Linux systems.

Changed in v15.0.3. Previously named Server.AutoLock

Updated in v5.0.0.

9.14.2 Server.Misc.IdleUserTimeout

The length of time (in minutes) after which an idle user gets automatically disconnected. This feature is disabled if value is `0` or less.

This value does not affect MultiSession guests, see *Server.MultiSession.Guests.MaxIdleTime*

Defaults to `0`.

Changed in v15.0.3. Previously named Server.IdleUserTimeout Added in v5.0.0.

9.14.3 Server.Misc.LocalHostRestricted

When set to `false`, host users that connect to a 'localhost' server are eligible to be automatically assigned control of the keyboard and mouse. This may be useful for certain VPN solutions that map remote addresses to 'localhost' addresses.

When set to `true`, host users that connect to a local machine can only receive control of the keyboard and mouse if it is assigned through the user interface.

Defaults to `true`.

Added in v12.3.0.

9.14.4 Server.Misc.StartDelay

Specifies a sleep time to delay the start-up of the ICE RemoteWare software in seconds.

Windows service only.

Defaults to `2`.

Added in v5.0.0.

9.14.5 Server.Misc.UnlockWelcomeScreen

When set to `true`, the server will automatically send a CTRL-ALT-DEL to the GUI to unlock to OS login.

if not set, the server will enable this feature for Windows server OSes.

Only available on Windows.

9.15 Server.Mouse

9.15.1 Server.Mouse.Enabled

When set to `false`, clients are not given the control over the cursor on the server.

Defaults to `true`.

9.16 Server.MultiSession

Multi Session related variables, see *Multi Session (Linux only)*.

9.16.1 Server.MultiSession.Enabled

Enables Multi-Session on the server. When this feature is enabled, all connecting clients are redirected to their private X11 server, running under the user id of the connected client.

Default is `false`.

9.16.2 Server.MultiSession.HostAdmins

This variable defines a list of OS users who connect directly to the host server and not to a guest X11 server. When this variable is not set all connecting clients will be redirected to their own X11 session. Only the admin user defined in the config file will always directly connect to the host.

Default is not set.

9.16.3 Server.MultiSession.GPUForwarding.Enabled

When this variable is set to true the server will assign a GPU to the guest session of the client. For more details see *Multi Session (Linux only)*.

Default is `true`.

9.16.4 Server.MultiSession.GPUForwarding.NumGPUs

When this variable is set to a value higher than zero, the server will assume that this number represents the number of screens available on the X11 server. This might help when the X11 monitor setup is not detected by the server. For more details see *Multi Session (Linux only)*.

Default is `0`.

9.16.5 Server.MultiSession.MaxClients

This variable limits the maximum number of client sessions started by the server. Note that the number of client sessions might be larger than the number of currently connected clients, as sessions are not stopped when clients disconnect.

Default is `8`.

9.16.6 Server.MultiSession.PortNumbersBegin

This variable defines the minimal port number a connecting client can get assigned to. Use this and the following value to limit the number of ports open on the firewall.

Default is `9200`.

9.16.7 Server.MultiSession.PortNumbersEnd

This variable defines the highest port number a connecting client can get assigned to. A value of `-1` indicates that the highest port number is determined by adding the values of the lowest and the number of clients (*Server.MultiSession.MaxClients*).

Use this and the previous value to limit the number of ports open on the firewall.

9.16.8 Server.MultiSession.DisplayIDsBegin

This variable defines the start value of the range of X11 display ids used for the private X11 servers of the clients.

Default is `32`.

9.16.9 Server.MultiSession.DisplayIDsEnd

This variable defines the end value of the range of X11 display ids used for the private X11 servers of the clients.

Default is `128`.

9.16.10 Server.MultiSession.Service.GracePeriod

This variable sets a grace period after which guest sessions are terminated when they are shut down by the GUI or when the host server stops.

Default is `30`.

9.16.11 Server.MultiSession.Secure.HidePIDs.Enabled

When this variable is set to `true`, the server will `unshare(1)` the filesystems of the host server and remount the `/proc` filesystem after the X11 session has been started but before the guest user is admitted to the system.

Default is `false`.

9.16.12 Server.MultiSession.Secure.HidePIDs.GroupID

This variable defines a Linux group, which allows its users to see all pids in the `/proc` filesystem.

See *Security* for more details.

Default is empty.

9.16.13 Server.MultiSession.Secure.PrivTmp.Enabled

When this variable is set to `true`, the server will start the guest user service with the option `--property=PrivateTmp=yes`. This way the services gets spawned after fresh filesystems have been mounted on the `/tmp` and `/var/tmp` directories. After the service is stopped, the filesystems are discarded.

Default is `true`.

9.16.14 Server.MultiSession.Service.Options

With this variable administrators can customize the settings of guest user services. The value will be added to the call of `systemd-run(1)`, which is used to start the guest services. While the setting `--property=PrivateTmp=yes` can be set using *Server.MultiSession.Secure.PrivTmp.Enabled*, other options are available, e.g. assignment of different slices. For a full list check the manual page of `systemd-run(1)`, the version of the installed `systemd`, and the online documentation.

Additional considerations should be made when changing the service to a `transient scope unit` or the `uid` of the service. This advanced configuration should only be made when fully understood.

Default is not set.

9.16.15 Server.MultiSession.VideoOptimizations

When this variable is set to `true`, the server will directly access the framebuffer from the X11 server. On some systems, certain resolutions cause the host server to lose sync with the X11 server. In these cases the video gets distorted. By setting this variable to `false` the server will operate normally again.

Default is `true`.

9.16.16 Server.MultiSession.Debug

When set to `true` the guest server will create log files for the X11 server and the Gnome window manager. In addition, the log level of the guest server will be set to `debug`. As setting this to `true` will slow down the guest server and produce large log files, use this setting with care.

Default is `false`.

9.16.17 Server.MultiSession.Guests.MaxIdleTime

After a client disconnects, the session is maintained for the number of seconds defined by this setting. A value of `-1` disables this timeout mechanism.

Default is `86400`.

9.16.18 Server.MultiSession.Guests.DefaultWidth

Defines the default width of the guest X11 server's display.

Default is `1440`.

9.16.19 Server.MultiSession.Guests.DefaultHeight

Defines the default height of the guest X11 server's display.

Default is `900`.

9.16.20 Server.MultiSession.Guests.Pixels

Defines the color pixels of the guest X11 server's display (Xephir).

Default is `24`.

9.16.21 Server.MultiSession.Guests.DPI

Defines the DPI of the guest X11 server's display.

Changing this value is not recommended.

Default is `96`.

9.16.22 Server.MultiSession.Guests.LogViewer.Enabled

The server of the guest session has a special logfile. This is by default located in the home directory of the guest session user. Set to `true` to show a link to the guest server's logfile.

Default is `false`.

9.16.23 Server.MultiSession.Guests.Config.Enabled

Setting this value to `true` enables the users of guest session to define individual resolutions of their sessions. To limit the values based on the processing capabilities, see the following two settings.

Default is `true`.

9.16.24 Server.MultiSession.Guests.Config.MaxWidth

When guest users are enabled to change the resolutions of their sessions, a system administrator can limit the maximal width a user can define.

Default is `2560`.

9.16.25 Server.MultiSession.Guests.Config.MaxHeight

When guest users are enabled to change the resolutions of their sessions, a system administrator can limit the maximal height a user can define.

Default is `1600`.

9.16.26 Server.MultiSession.Guests.Config.AdvancedSettings

When *Server.MultiSession.Guests.Config.Enabled* is set to `true` this setting will enable a UI control to assist the users with defining the desired resolution.

Default is `true`.

9.16.27 Server.MultiSession.Custom.MinimizeGuestWindow

When running Xephir as X11 server for the guest session, setting this variable to `true` closes the guest X11 server's window.

Default is `false`.

9.16.28 Server.MultiSession.WindowManager.LogFile

The setting defines the log file path of the window manager of the guest Gnome window manager.

Default is `~/.ice-remoteware/log/window-mgr.log`.

9.16.29 Server.MultiSession.XServer.LogFile

The setting defines the log file path of the window manager of the guest X11 server.

Default is `~/.ice-remoteware/log/xserver.log`.

9.16.30 Server.MultiSession.AllowLongRunningProcesses

When set to `true` the host server will stop all processes spawned by the user after the guest session is terminated. When set to `false` only processes related to the X11 session will be shutdown.

Default is `false`.

9.16.31 Server.MultiSession.SecureAdminLogin

When set to `true` the host server will disable guest access to the server when an unlocked X11 session on the host is running. This prevents any undesired interaction of the host user's session with any guest sessions.

See *Security Considerations with GPU Forwarding* for more details.

When GPU sharing is enabled (*Server.MultiSession.GPUForwarding.Enabled*) it is advisable to set this to true.

Default is `false`.

9.17 Server.Network

9.17.1 Server.Network.Port

The port number used by the server.

Defaults to `443` if *Server.Network.Secure* is `true` or `80` if *Server.Network.Secure* is `false`.

9.17.2 Server.Network.Secure

Determines if the server operates over HTTPS (recommended).

Defaults to `true`.

9.17.3 Server.Network.Address

When set, the server binds its network interface to the given address.

Not set by default.

9.17.4 Server.Network.RedirectHTTP

If set to `true`, the server opens the HTTP port `80` and redirects all requests to the HTTPs port `443`. When the port `80` is taken, it logs an error and continues.

Default is `true`.

9.17.5 Server.Network.UseIPv4

If set to `true`, server listens on IPv4 addresses for client requests.

Defaults to `true`.

9.17.6 Server.Network.UseIPv6

If set to `true`, server listens on IPv6 addresses for client requests.

Defaults to `true`.

9.17.7 Server.Network.Timeouts.Receive

Sets the timeout (in seconds) used in the server when receiving messages from clients. If the network is unstable, a higher value can improve the user experience as connections will be maintained longer. However, it will then take longer to discover when a client is permanently disconnected.

Defaults to `4.0`.

9.17.8 Server.Network.Timeouts.VideoSend

Sets the timeout (in seconds) used in the server when sending the video stream to the clients. If the network is unstable, a higher value can improve the user experience as connections will be maintained longer. However, long delays when sending video frames will lead to a large backlog of frames, which is very noticeable to the user.

Defaults to `8.0`.

9.17.9 Server.Network.Timeouts.Connect

Sets the timeout (in seconds) used during the connection phase of the client. Increasing this value might help when a very slow or overloaded server takes too long to respond to initial setup requests.

Defaults to `8.0`.

9.17.10 Server.Network.Access.Logger.Enabled

Enables logging of connection requests.

Defaults to `true`.

9.17.11 Server.Network.Access.Logger.FileName

Sets the log file to log connection requests.

Defaults to `ice-remoteware-access.log`.

9.17.12 Server.Network.Access.IPAllowList

A comma-separated list of network/host addresses that the server will match incoming client request against to determine if the client is allowed to connect.

When this list is empty, all clients are allowed to connect. Otherwise only clients with matching addresses are allowed to connect.

```
<IPAllowList>86.4.0.0/16,86.5.0.0/16,2001:0db8:3c4d:0015:0000:0000:0000:0000/64,
↪2001:db8:3c66:25::1a2f:1a2b/64</IPAllowList>
```

Not set by default.

9.17.13 Server.Network.Access.IPDenyList

A comma-separated list of network/host addresses that the server will match incoming client request against to determine if the client will be refused to connect.

When this list is empty, all clients are allowed to connect. Otherwise clients with addresses in this list are blocked.

```
<IPDenyList>86.4.0.0/16,86.5.0.0/16,2001:0db8:3c4d:0015:0000:0000:0000:0000/64,
↪2001:db8:3c66:25::1a2f:1a2b/64</IPDenyList>
```

Not set by default.

9.17.14 Server.Network.KeepAlive.Enabled

When set to `true`, all connections set the TCP keep alive flag. This prevents aggressive firewalls from dropping the connections when the session is idle for a while.

Default is `true`.

9.17.15 Server.Network.KeepAlive.IdleTimeout

Set the value for the TCP keep alive idle timeout.

Default is `20`.

9.17.16 Server.Network.KeepAlive.Interval

Set the value for the TCP keep alive interval.

Default is `4`.

9.18 Server.QoS

9.18.1 Server.QoS.Enabled

Enables the automatic adjustment of frame rate to adapt to current performance conditions. Frame rate will start at `Server.Video.Encoding.H264.StartFrameRate` and jump between `Server.Video.Encoding.H264.MinFrameRate` and `Server.Video.Encoding.H264.MaxFrameRate`.

Setting this to `false` will cause the server to send a constant frame rate specified by `Server.Video.Encoding.H264.StartFrameRate`. `Server.Video.Encoding.H264.MinFrameRate` and `Server.Video.Encoding.H264.MaxFrameRate` are ignored in this case.

Defaults to `true`.

9.18.2 Server.QoS.MaxBitRate

The variable controls the maximal outgoing average bandwidth of all connected clients. Due to sudden changes in the video stream this value is a target value which is not always reached.

Defaults to `100g`.

9.18.3 Server.QoS.Debug.Enabled

If set to `true`, the server reports very detailed statistics generated by the QoS algorithm. When enabled, this reporting puts a considerable load on the server and the log files fill up quickly.

Defaults to `false`.

9.19 Server.UserNotifications

See *User Notifications*

9.19.1 Server.UserNotifications.Enabled

If set to `true`, the server notifies the OS user of certain events. For example, when a user or USB device is connected or disconnected.

Default is `true`

9.19.2 Server.UserNotifications.Timeout

Only available in Windows and Linux

Controls the time (in seconds) a user notification is shown.

Default is `4`

9.20 Server.Video

Video streaming related settings.

9.20.1 Server.Video.Encoding.H264.AvgBitRate

Used to improve image quality at the cost of using more bandwidth.

The average video bit-rate is calculated by using a linear regression of two values based on the resolution of the screen and the number of bits per second, respectively. For more information, see *Configure Video Bit-Rate*

Defaults to `1280x720=3000k,1920x1080=6000k`.

Updated in v9.1.9. Increased defaults.

9.20.2 Server.Video.Encoding.H264.StartFrameRate

Initial frame rate. Measured in frames per second.

Defaults to `24`.

Added in v2.2.0.

9.20.3 Server.Video.Encoding.H264.MinFrameRate

The lowest valid frame rate for a connection. Measured in frames per second.

Defaults to `2`.

Added in v2.2.0.

9.20.4 Server.Video.Encoding.H264.MaxFrameRate

The highest allowable frame rate for a connection. Measured in frames per second.

Defaults to `30`.

Windows using the default `windda` video source and ARM-based Mac servers can support frame rates up to 60.

Added in v2.2.0.

9.20.5 Server.Video.MaxWidth

Any server-side video that exceeds this width is scaled down to this value. This is primarily used to prevent clients from receiving video with resolutions so high that the client cannot process them fast enough.

A value of `-1` disables this threshold.

Defaults to `2560`.

Updated in v5.0.0. Changed default.

9.20.6 Server.Video.MaxHeight

Any server-side video that exceeds this height is scaled down to this value. This is primarily used to prevent clients from receiving video with resolutions so high that the client cannot process them fast enough.

A value of `-1` disables this threshold.

Defaults to `1600`.

Updated in v5.0.0. Changed default.

9.20.7 Server.Video.Lossless.Enabled

Enables lossless video streaming within the Native Client. It doesn't have any effect on clients connected with a web browser.

Defaults to `true`.

9.20.8 Server.Video.Refresh.Intra

When enabled the server will not send a single I-Frame to refresh the clients' decoders but spread the stream information over a set of frames. This way peaks in bandwidth consumption are avoided.

Defaults to `true`.

9.20.9 Server.Video.Refresh.Rate

When this setting is set to a value higher than zero the server will update the clients' decoders by sending periodically an I-Frame to refresh their decoding state. This setting is measured in seconds.

Defaults to `4`.

9.20.10 Server.Video.VideoSource

The video capture mechanism. The ICE RemoteWare software currently supports these video sources: `x11`, `nvfbc`, `stream`, `windda`, and `default`.

The `x11` video source uses software encoding and only works for Linux systems. It supports a max frame rate of up to 60 fps.

The `nvfbc` video source is for Linux systems with an NVIDIA GPU and driver that support NVIDIA GRID or NVIDIA NvFBC. It supports a max frame rate of up to 60 fps.

The `windda` video source is optimized for Windows and supports a max frame rate of up to 60 fps.

The `stream` video source uses software encoding and is available on all operating systems. This video source supports a max frame rate of up to 60 fps on ARM-based Macs and 30 fps on all other systems.

The `default` video source selects the default video source for your system, on Windows systems `windda`, on Linux systems, `x11``and on MacOS systems ``stream` is selected.

Changed in v15.0.3. Previously named Server.VideoSource, added ``default``, deprecated ``auto``

Changed in v12.2.0. Added nvfbc.

9.21 Server.VirtualHere

9.21.1 Server.VirtualHere.Enabled

Enables USB forwarding via VirtualHere. Check your license to determine if this feature is available.

Default is `true`.

9.21.2 Server.VirtualHere.AllowedUsbDevices

A comma-separated list of USB device names (or parts of device names) that the server will match against to allow USB forwarding from clients. When this list is empty, all USB devices are allowed to be forwarded.

For example, the following setting in the configuration file would allow the server to only accept USB devices that have the word `Wacom` or `Speedline` in their name:

```
<AllowedUsbDevices>Wacom,Speedline</AllowedUsbDevices>
```

9.21.3 Server.VirtualHere.UsbDevicesWithRemoteCursor

A comma-separated list of USB device names (or parts of device names) that trigger the server to show the cursor on the server as part of the video stream. This is very useful when working with a USB tablet as these devices will not update the local cursor when connected to the server.

Default is `Wacom,Huion,Xencelabs,XP-PEN,Intuos`.

9.22 Server.Web

9.22.1 Server.Web.Caching.Enabled

When set to `true`, the server uses the HTTP cache control mechanism to limit network traffic.

Default is `true`.

9.22.2 Server.Web.PathPrefix

The value of this variable is used as a prefix for the server URIs. This can be used to filter the requests in a multiplier.

Variable is not set by default.

9.22.3 Server.Web.CookiesSameSite

Sets the same site property of the cookies used during the session. Accepted values are `strict`, `lax`, `none`, `auto`.

> **Warning**
>
> Make sure you understand the security implications when changing this value.

Default is `auto`.

9.23 Server.X11

See *Multi Server (Linux only)*

9.23.1 Server.X11.Display

When set the server will connect to the specified display id, `:1`. Otherwise the default display id will be assumed.

Default is not set.

This is a setting for specialized setup and very old installations. Please use *Server.X11.Seat*

9.23.2 Server.X11.Seat

When set the server will connect to the specified seat, which identifies an X11 instance. Linux only

Set the X11 seat that the server should connect to.

Defaults to `seat0`.

9.24 openSSL

HTTPs security settings, see *HTTPS / SSL Certificates*

All elements within the openSSL tag are described in the Poco SSLManager documentation.

9.24.1 openSSL.server.privateKeyFile

The path to the file containing the private key for the certificate in PEM format (or containing both the private key and the certificate). This path can be absolute or relative to the XML config file. Required for HTTPS support.

9.24.2 openSSL.server.certificateFile

The path to the file containing the server's or client's certificate in PEM format. Can be omitted if the file given in privateKeyFile contains the certificate as well. This path can be absolute or relative to the XML config file.

9.24.3 openSSL.server.verificationMode

Specifies whether and how peer certificates are validated. See the Poco Context class for details. Valid values are `none`, `relaxed`, `strict`, and `once`.

Defaults to `none`.

Changed in v3.0.0. Default value changed.

9.24.4 openSSL.server.loadDefaultCAFile

Boolean value. Specifies whether the built-in CA certificates from OpenSSL are used.

Defaults to `true`.

9.24.5 openSSL.server.cipherList

Specifies the supported ciphers in OpenSSL notation.

Changed in v3.0.0. Default value changed.

9.24.6 openSSL.server.privateKeyPassphraseHandler.name

The name of the Poco class used for obtaining the passphrase for accessing the private key. If your private key does not use a passphrase, this value is ignored.

Defaults to `KeyFileHandler`.

Added in v2.2.0. Default value changed.

9.24.7 openSSL.server.privateKeyPassphraseHandler.options.password

The private key passphrase. This setting is ignored if there is no passphrase for the private key.

9.24.8 openSSL.server.invalidCertificateHandler.name

This should be set to `ConsoleCertificateHandler`. The name of the class used for confirming invalid certificates.

Defaults to `RejectCertificateHandler`.

Added in v2.2.0. Default value changed.

9.24.9 openSSL.server.cacheSessions

This should be set to `false`. Enables or disables session caching.

9.24.10 openSSL.server.extendedVerification

Enable or disable the automatic post-connection extended certificate verification.

9.24.11 openSSL.server.requireTLSv1_2

Require a TLSv1.2 connection.

Defaults to `true`.

Added in v2.2.0. Default value changed.

9.24.12 openSSL.client.verificationMode

Specifies whether and how peer certificates are validated when the server acts as a client to a third-party host. See the Poco Context class for details. Valid values are `none`, `relaxed`, `strict`, and `once`. Defaults to `relaxed`. Setting this value to `none` is not recommended.

Added in v3.0.0.

9.24.13 openSSL.fips

Enable or disable OpenSSL FIPS mode. Only supported if the OpenSSL version that this library is built against supports FIPS mode.

CHAPTER

TEN

FREQUENTLY ASKED QUESTIONS / TROUBLESHOOTING

10.1 Uninstalling ICE FlexLM on Windows fails to remove application

Microsoft provides a tool that can help automatically repair issues that prevent existing applications from being uninstalled. See the following URL for more information:

https://support.microsoft.com/en-us/topic/fix-problems-that-block-programs-from-being-installed-or-removed-cca7d1b6-65a9-3d98-4

10.2 Firefox Snap 113 on Ubuntu 22 can't launch ICE RemoteWare Client when opening `irw://` URIs.

This is a known issue with the Firefox Snap package. Install and connect with Chrome to work around this issue.

10.3 Why do I get stuck on the loading page when I sign in with Safari?

If the server is using a self-signed certificate, then Safari will refuse the necessary WebSocket connections from the server. You may also see a message in the JavaScript Console that says:

```
WebSocket network error:  OSStatus Error -9807:  Invalid certificate chain
```

There are a few workarounds:

1. The most secure option is to contact your system administrator about either using a trusted certificate for the server.
2. Add the server's self-signed certificate to your Keychain Access. NOTE: This is not recommended if the server is using the certificate that is included with ICE RemoteWare™.
3. The simplest and least secure workaround is to use a different browser such as Chrome or ICE RemoteWare Client.

10.4 Are there any known conflicts with anti-virus software?

Enabling Avast Antivirus can crash or cause unstable with the native client. Possible workarounds include creating an exception for the native client or disabling Avast.

10.5 Why does pasting into a MacOS terminal result in "^[[200~" being displayed?

Certain terminal-based programs (such as zsh shell) come with a feature called "bracketed paste mode". Bracketed paste mode will wrap your pasted string with a `^[[200~` and `~` so that the program can distinguish pasted text from directly typed text.

Please consult the documentation for these terminal-based programs for more information on bracketed paste mode.

10.6 Why is USB Forwarding disabled after updating MacOS Big Sur (or earlier) to MacOS Monterey (or later)?

When ICE RemoteWare is installed on versions of MacOS older than Monterey, it deploys the 'VirtualHere' application to support USB Forwarding. Monterey will not run this application, however, so it must be replaced with 'VirtualHere-Universal' to re-enable USB Forwarding.

Please see: *Re-Enabling USB Forwarding after Updating to MacOS Monterey* for installation instructions.

10.7 Why do I see two cursors for MacOS with only one user signed in?

There are two reasons this might occur:

1. When Wacom tablets are connected, we intentionally draw the mouse cursor to make stylus navigation easier.
2. MacOS servers that do not have a physical display or display dongle attached will always draw the remote cursor. Installing a display dongle or a physical display should resolve this issue.

10.8 Why is video performance poor in Chrome, Firefox, or Edge?

Hardware acceleration for WebGL can be blocked for certain graphics cards and driver combinations in Microsoft Edge, Google Chrome, and Mozilla Firefox browsers.

Follow the browser specific steps below to determine if your browser is blocking WebGL hardware acceleration and force the browser to enable it. If you continue to have trouble getting WebGL hardware acceleration to work after following the steps below you may need to:

- Update your driver (Intel, AMD, or NVIDIA)
- Switch to a compatible browser
- Switch to ICE RemoteWare Client (Recommended!)

Important

Forcing WebGL hardware acceleration may cause the browser to be unstable. If you are unsure about any of this, please download and install the native client as a workaround instead!

10.8.1 Forcing WebGL in Google Chrome

1. Open Chrome and go to URL `chrome://gpu`
2. Under `Graphics Feature Status`, look for the lines starting with `WebGL:` and `WebGL2:`
3. If those values are NOT: `Hardware accelerated`, then your browser is likely blocking WebGL hardware acceleration.
4. If you suspect WebGL hardware acceleration is blocked, you can try forcing this feature by following these steps:
   a. Go to URL `chrome://flags/#ignore-gpu-blocklist`
   b. Use the dropdown to set its value to `Enabled`.
   c. Restart the browser by clicking on the `Relaunch` button.

10.8.2 Forcing WebGL in Mozilla Firefox

1. Open Firefox and go to URL `about:support`
2. Scroll down to the `Graphics` section.
3. In the `WebGL 1 Driver Renderer` section, you may see a message about it being `Blocked for your graphics card`.
4. If you suspect WebGL hardware acceleration is blocked, you can try forcing this feature by following these steps:
   a. Go to URL `about:config`
   b. A warning page may appear. Click `I accept the risk!` to go to the `about:config` page.
   c. Search for `webgl.force-enabled` and set the value to `true` by double-clicking on the row.
   d. Search for `layers.acceleration.force-enabled` and set the value to `true` by double-clicking on the row.
   e. Restart Firefox to apply your new settings.

10.8.3 Forcing WebGL in Microsoft Edge

1. Open Microsoft Edge and go to URL `edge://gpu`
2. Under `Graphics Feature Status`, look for the lines starting with `WebGL:` and `WebGL2:`
3. If those values are NOT: `Hardware accelerated`, then your browser is likely blocking WebGL hardware acceleration.
4. If you suspect WebGL hardware acceleration is blocked, you can try forcing this feature by following these steps:
   a. Go to `edge://flags/#ignore-gpu-denylist`
   b. Use the dropdown to set its value to `Enabled`.
   c. Restart the browser by clicking on the `Restart` button.

10.9 Why does my MacOS display not go to sleep?

ICE RemoteWare prevents Display Sleep from happening in MacOS using an application called caffeinate. This is to prevent the computer from going to sleep, which would make ICE RemoteWare inaccessible.

10.10 How do I use reserved keyboard shortcuts such as Command-Space?

Command-Space is a common keyboard shortcut in MacOS used to access Spotlight. This can conflict with the Linux equivalent keyboard combination of Super-Space, which is used to a change of the keyboard layout.

Currently the only workaround that will let you transmit Command-Space and a few other keyboard shortcuts reserved by the OS is to disable the keyboard shortcut locally.

10.11 Starting the service in Linux results in "X11 connection rejected because of wrong authentication."

The message indicates there's an X permissions issue. This may be due to a missing X11 magic cookie in your user's $HOME/.Xauthority file.

To add the missing X11 magic cookie value, first determine the display number used by `linuxuser`:

```
linuxuser@host:~$ echo $DISPLAY
host:21.0
```

In this example it is `21.0`. Next, display linuxuser's list of cookies:

```
linuxuser@host:~$ xauth list
host/unix:1  MIT-MAGIC-COOKIE-1  51a3801fd7776704575752f09015c61d
host/unix:21  MIT-MAGIC-COOKIE-1  0ba2913f8d9df0ee9eda295cad7b1010
host/unix:22  MIT-MAGIC-COOKIE-1  33cd4803819fca0ef8297dba308ceeee
```

The cookie for the `21.0` display is the second in the list.

Next, log in as root and add this particular cookie to the root's .Xauthority file with the `xauth` command:

```
root@host:~$ xauth add host/unix:21 MIT-MAGIC-COOKIE-1 0ba2913f8d9df0ee9eda295cad7b1010
```

Finally, try restarting X and check if ICE RemoteWare is running.

10.12 My image is very pixelated. How do I improve image quality?

Increasing the Server.Video.AvgBitRate values will improve image quality at the cost of higher bandwidth. For example, if you want to increase the average bit rate at 1080p to 10 Mbps and you have sufficient bandwidth on the server and client side, we recommend setting Server.Video.AvgBitRate to the following:

```
1280x720=5000k,1920x1080=10000k
```

You may want to experiment for your particular use case. Setting this value too high may render the system slow or unusable for servers and clients with poor bandwidth.

10.13 When I fullscreen the remote desktop in Firefox my screen is cropped!

As a workaround, first exit Fullscreen. Now try using the Firefox menu to zoom out until the entire remote desktop window fits and then use the Fullscreen option.

10.14 How do I create non-standard resolutions in Windows with an NVIDIA GPU?

It is important to use the NVIDA Control Panel to change to a non-standard resolution. Using the Windows Display Manager will result in a corrupt desktop image.

10.15 What do I do if Windows shows a black screen instead of a login screen?

We've observed in Windows 2012 that the login screen will occasionally not appear until you hit the 'Escape' key.

10.16 Why does Google Chrome 61-62 show inaccurate colors?

Newer versions of Google Chrome (Chrome 61 and 62) use the ICC profile provided by the local OS rather than forcing its own color profile. This may make the colors appear different from what you may see in other browsers or in the Native Client.

As a workaround you can enter `chrome://flags/#force-color-profile` in your Chrome URL bar and select `sRGB` from the dropdown. Then close and restart Chrome.

10.17 How many users can sign in at a time?

ICE RemoteWare currently supports multiple signed in users at a time. Currently this defaults to 6. This value can be changed in the config XML file via the *Server.Collaboration.MaxClientCount* option.

10.18 I'm only seeing a gray rectangle.

This is either caused by caching problems in the browser, an unsupported screen resolution, or an unexpected error between the client and server.

Try signing out, opening a new web browser, and trying again. If the problem persists, check the web browser's JavaScript Console and the ICE RemoteWare log file (Linux: `/var/log/messages`) for errors.

If the JavaScript Console shows an error message containing `net::ERR_CERT_AUTHORITY_INVALID` in Chrome, you may want to try Firefox or reset Chrome to its original factory settings.

If you are a Linux user, verify that Xorg is running on `DISPLAY :0` by running `ps aux | grep X`. If you do not see a line that looks like `Xorg :0`, you may need to restart X by running `init 3` and `init 5` on Linux.

10.19 How do I press Ctrl+Alt+Del or Print Screen?

There is a shortcut button for this keyboard combination in the Keyboard Menu in the top control bar.

10.20 How do I press Ctrl+N, Ctrl+T, Ctrl+W, Ctrl+Tab, Ctrl+Page Up, or Ctrl+Page Down?

This is typically when web browsers reserve these keyboard shortcuts. One workaround is to install the latest version of our native client, ICE RemoteWare Client. Chrome users can try another workaround, described below.

By default, Google Chrome (aka Chromium) intercepts certain specific keyboard combinations before ICE RemoteWare can receive them. There is a special "app mode" available for Chrome users that can be activated at the command line by appending the `--app=<url>` flag. For example:

```
google-chrome --app=https://host/
```

This will open a borderless Chrome browser that will relay many of these key combinations to ICE RemoteWare. If this is something you will do often, we recommend creating a shortcut with a flag to your ICE RemoteWare host.

> **Note**
>
> Certain keyboard combinations, such as Ctrl+Alt+Del and Alt+Tab are intercepted by the client operating system and are not relayed to the ICE RemoteWare interface.

10.21 What ports do I need to open?

By default, ICE RemoteWare must be able to accept incoming requests over HTTPS port 443 (or port 80 if you are using HTTP).

10.22 Can I run my applications?

ICE RemoteWare is completely unaware of what applications are being run on the remote operating system. In other words, if your application can run directly on the remote host, it can be displayed on ICE RemoteWare.

10.23 Will it run on my iPad / mobile device?

We do not yet officially support iPad or mobile devices, but we have had some success getting view-only functionality to work with an iPhone SE.

10.24 Is there audio support?

Yes. As of v10.0 we support dual channel audio.

10.25 Can I cut, copy, and paste?

You can copy text from the local desktop to the remote desktop. See *Keyboard Menu* for more information.

10.26 Linux: Install package without Internet connection

On Fedora based systems, e.g. CentOS and Rocky Linux, installation without Internet connection is possible by executing:

```
rpm -ivh [package].rpm
```

10.27 After installing the service does not start

First check the log files, see *Log Output*.

When the log files don't show any problems, start the server from a terminal manually and check for useful messages.

On Windows open a cmd prompt and go to `C:\Program Files\Penguin Solutions\ICE RemoteWare\run` and execute:

```
ice-remoteware.exe /A /logLevel trace
```

On Linux go to `/opt/ice-remoteware/bin` and run:

```
sudo ice-remoteware -A --logLevel trace
```

If there is no indication where the problem might come from, save the output and contact support.

10.28 What graphics cards do you support?

See *Server Hardware*.

10.29 How many NVIDIA GRID GPUs do I need?

As of v5.0, NVIDIA GRID GPUs are no longer required to run ICE RemoteWare.

10.30 What Xorg.conf options do I need for an NVIDIA GRID / Tesla card over GPU passthrough?

First, find the appropriate BusID for your graphics card using the following command:

```
nvidia-xconfig --query-gpu-info | awk '/PCI BusID/{print $4}'

PCI:27:1:0
```

The BusID in this example is `PCI:27:1:0`. (Note: other tools such as lspci show the bus ID in a hexadecimal format that must be manually converted to decimal format).

For older NVIDIA GRID cards (K1 or K2) add the BusID and the "UseDisplayDevice" "none" option. Modify the Xorg.conf file so that the Device and Screen sections look similar to the following:

```
Section "Device"
    Identifier     "Device0"
    Driver         "nvidia"
    VendorName     "NVIDIA Corporation"
    BusID          "PCI:27:01:0"
EndSection

Section "Screen"
    Identifier     "Screen0"
    Device         "Device0"
    Monitor        "Monitor0"
    DefaultDepth    24
    Option         "UseDisplayDevice" "none"
    SubSection     "Display"
        Virtual     1440 900
        Depth       24
    EndSubSection
EndSection
```

For NVIDIA Tesla M60 users add the BusID (note: the syntax below is also valid). You may also want to specify a DPI (as needed) if images on the screen appear too wide or narrow. Modify the Xorg.conf file so that the Device section looks similar to the following:

```
Section "Device"
    Identifier     "Device0"
    Driver         "nvidia"
    VendorName     "NVIDIA Corporation"
    BoardName      "Tesla M60"
    BusID          "PCI:27:01:0"
    Option         "DPI" "96x96"
EndSection
```

CHAPTER

ELEVEN

END USER LICENSE AGREEMENT

```
Penguin Computing, Inc.
45800 Northport Loop West, Fremont, CA 94538
Tel: 415-954-2800
www.penguincomputing.com

Penguin Computing Software End User License Agreement

Last revised: 2/22/2025

LEGAL NOTICE - READ CAREFULLY BEFORE INSTALLING OR OTHERWISE USING THIS SOFTWARE.

This License Agreement (the "Agreement") is a legal agreement between you, a
single legal entity ("End User"), and Penguin Computing, Inc. ("Penguin"). This
Agreement governs your use of the ICE RemoteWare™ software defined below
(the "Software") and any accompanying written materials (the "Documentation").
You must accept the terms of this Agreement before installing, downloading,
accessing or otherwise using such Software and documentation.

By "ACCEPTING" at the end of this Agreement, you are indicating that you have
read and understood, and assent to be bound by, the terms of this Agreement. If
you are an individual working for a company, then you represent and warrant you
have all necessary authority to bind your company to the terms and conditions of
this Agreement.

If you do not agree to the terms of the Agreement, you are not granted any rights
whatsoever in the Software or Documentation. If you are not willing to be bound
by these terms and conditions, do not "ACCEPT" the EULA and remove the software
from the system immediately.

END USER LICENSE AGREEMENT FOR ICE RemoteWare™ Software

1. Definitions.

1.1 "Clustered System" means a collection of computer systems managed by the
Software and for which the total number of computers in the system is specified
in the End User purchase order.

1.2 "Master Node" means the computer or computers designated as the Master
Node(s) in the applicable End User purchase order, where the Software is
initially installed and from which the total number of computers comprising the
```

(continues on next page)

(continued from previous page)

```
Clustered System are managed.

1.3 "Software" means the software provided under this Agreement by Penguin or
its authorized distributor or reseller and for which the applicable End User
purchase order specifies: (i) the Software to be licensed by End User (ii) the
Master Node(s) (iii) the license fees and (iv) the total number of computers in
the Clustered System for which End User has paid applicable license fees and the
term of the Software usage. The Software is comprised of a collection of software
components that fall into three (3) categories: (a) "Unpublished Software" which
is owned by Penguin and/or its licensors and licensed under the terms of this
Agreement (b) "Published Software" which is owned by Penguin and licensed under
the GPL version 2 open source license or such other open source license as
Penguin may elect in its sole discretion and (c) "Open Source Software" which is
owned by various entities other than Penguin and is subject to the "open source"
or "free software" licenses, including but not limited to General Public
Licenses (GPL), Lesser General Public License (LPGL), Apache, Artistic, BSD,
IBM Public, Mozilla, Omron, Open Group Public License, and Python licenses.

1.4 "Client Connections" means the simultaneous connections between any software
client and Software, where a connection creates a persistent and unique Software
session per software client.

2. License.

2.1 License Grant. Subject to the terms and conditions of this Agreement, Penguin
grants to End User a non- exclusive, non-transferable, non-sublicensable right
and license to (a) reproduce (solely to download and install), perform, and
execute the Unpublished Software on the specified Master Node(s), solely for End
User's internal purposes, and (i) solely for use on the number of computers in
the Clustered System and (ii) not to exceed the maximum number of Client
Connections for which End User has paid the required license fees for the
authorized term and (b) make one (1) copy of the Unpublished Software and
Documentation for backup and/or archival purposes only.

2.2 Restrictions. The End User shall not, and shall not permit any third party
to: (a) sell, lease, license, rent, loan, or otherwise transfer the Unpublished
Software or Documentation, with or without consideration (b) permit any third
party to access or use the Unpublished Software or Documentation (c) permit any
third party to benefit from the use or functionality of the Unpublished Software
via a timesharing, service bureau, or other arrangement (d) transfer any of the
rights granted to End User under this Agreement (e) reverse engineer, decompile,
or disassemble the Unpublished Software (f) modify or create derivative works
based upon the Unpublished Software or Documentation, in whole or in part (g)
reproduce the Unpublished Software or Documentation, except as expressly
permitted in Section 2.1 above (h) remove, alter, or obscure any proprietary
notices or labels on the Unpublished Software or Documentation (i) use the
Unpublished Software for any purpose other than expressly permitted in Section
2.1 above or (j) use the Unpublished Software for more than the total number of
computers, or longer than the authorized term the End User is licensed for
pursuant to Section 2.1 above.

2.3 Open Source Software. The Open Source Software and Published Software are
```

(continues on next page)

(continued from previous page)

```
not subject to the terms and conditions of Sections 2.1, 2.2, or 6. Instead,
each item of Open Source Software and Published Software is licensed under the
terms of the end-user license that accompanies such Open Source Software and
Published Software, as may be located in the product packaging or available
on-line. End User agrees to abide by the applicable license terms for any such
Open Source Software and Published Software. Nothing in this Agreement limits
End User's rights under, or grants End User rights that supersede, the terms and
conditions of any applicable end user license for the Open Source Software or
Published Software. In particular, nothing in this Agreement restricts End
User's right to copy, modify, and distribute any of the Open Source Software and
Published Software that is subject to the terms of the GPL and LGPL. For the
Open Source Software and Published Software subject to the GPL and LGPL, for a
period of three (3) years following End User's receipt of the Software, End User
may contact Penguin at the address below in writing and request a copy of the
source code for such Open Source Software or Published Software at Penguin's
then-current fees.

3. Ownership. The Software is licensed, not sold. Penguin and its licensors
retain exclusive ownership of all applicable worldwide copyrights, trade
secrets, patents, and all other intellectual property rights throughout the
world, and all applications and registrations relating thereto, in and to the
Unpublished Software, Published Software, and Documentation, and any full or
partial copies thereof, including any additions or modifications to the
Unpublished Software and Documentation. End User acknowledges that, except for
the limited license rights expressly provided in this Agreement or the Open
Source Licenses, as applicable, no right, title, or interest to the intellectual
property in the Software or Documentation is provided to End User, and that End
User does not obtain any rights, express or implied, in the Software or
Documentation. All rights in and to the Software not expressly granted to End
User in this Agreement or the Open Source Licenses, as applicable, are expressly
reserved to Penguin and its licensors. The “ICE ClusterWare™” and “ICE RemoteWare”
trademarks and associated logos are the trademarks of Penguin and its affiliates.
This Agreement does not permit End User to use the Penguin trademarks.

4. Limited Warranty. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, THE
SOFTWARE IS PROVIDED AND LICENSED AS-IS WITHOUT WARRANTY OF ANY KIND, EXPRESSED
OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-
INFRINGEMENT, TITLE OR FITNESS FOR A PARTICULAR PURPOSE. PENGUIN DOES NOT
WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET THE END USER'S
REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE ERROR FREE OR APPEAR
PRECISELY AS DESCRIBED IN THE ACCOMPANYING DOCUMENTATION.

5. Limitation of Liability. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW,
PENGUIN NOR ANY OF ITS AUTHORIZED DISTRIBUTORS, RESELLERS AND LICENSORS WILL BE
LIABLE TO END USER FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES, LOST PROFITS,
LOST OPPORTUNITIES, LOST SAVINGS, OR LOST DATA OR COST OF COVER ARISING OUT OF
THE USE OR INABILITY TO USE THE SOFTWARE OR DOCUMENTATION OR ANY SERVICES
HEREUNDER, HOWEVER CAUSED ON ANY THEORY OF LIABILITY (INCLUDING CONTRACT, STRICT
LIABILITY, OR NEGLIGENCE), EVEN IF PENGUIN, ITS AUTHORIZED DISTRIBUTORS,
RESELLERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
IN NO EVENT SHALL PENGUIN'S AGGREGATE LIABILITY UNDER THIS AGREEMENT EXCEED THE
AMOUNT ACTUALLY PAID BY END USER TO PENGUIN FOR THE SOFTWARE GIVING RISE TO THE
```

(continues on next page)

(continued from previous page)

```
CLAIM.  END USER ACKNOWLEDGES THAT THE AGREEMENT REFLECTS AN ADEQUATE AND
ACCEPTABLE ALLOCATION OF RISK.

6. Confidential Information. Unpublished Software and the structure,
organization, and code of the Unpublished Software, including but not limited to
the shell scripts of the Unpublished Software, are confidential and proprietary
information ("Confidential Information") of Penguin and/or its licensors. End
User agrees to safeguard such Confidential Information with a degree of care
commensurate with reasonable standards of industrial security for the protection
of trade secrets and proprietary information such that no unauthorized use is
made of such information and no disclosure of any part of its contents is made
to anyone other than End User's employees whose duties reasonably require such
disclosure in order to effectuate the purposes of this Agreement.

7. Term and Termination. This Agreement will remain in effect until terminated
or for the authorized term of license usage. End User may terminate this
Agreement by removing the Unpublished Software from End User's computers,
ceasing all use thereof, and destroying all copies of the Unpublished Software
and Documentation and certifying to Penguin that it has done so. Any breach of
this Agreement by End User will result in the immediate and automatic
termination of this Agreement and licenses granted by Penguin herein, and End
User shall cease all use of and destroy all copies of the Unpublished Software
and Documentation and certify to Penguin that it has done so. In addition to
termination, Penguin will have the right to pursue any other remedies available
to it under law or in equity.

8. Export Controls. End User acknowledges and agrees that the Software and
Documentation which is the subject of this Agreement may be controlled for
export purposes. End User agrees to comply with all United States export laws
and regulations including, but not limited to, the United States Export
Administration Regulations, International Traffic in Arms Regulations,
directives and regulations of the Office of Foreign Asset Control, treaties,
Executive Orders, laws, statutes, amendments, and supplement thereto. End User
assumes sole responsibility for any required export approval and/or licenses and
all related costs and for the violation of any United States export law or
regulation.

9. U.S. Government End Users. The Software is a "commercial item" as that term
is defined at 48 C.F.R. 2.101 (OCT 1995), consisting of "commercial computer
software" and "commercial computer software documentation" as such terms are
used in 48 C.F.R. 12.212 (SEPT 1995). Consistent with 48 C.F.R. 212 and
48 C.F.R. 227.7202-1 through 227.7202-4 (JUNE 1995), all U.S. Government End
Users acquire the Software with only those rights set forth herein.

10. Miscellaneous. This Agreement is the final, complete and exclusive agreement
between the parties relating to the Software and Documentation, and supersedes
all prior or contemporaneous proposals, representations, understandings, or
agreements relating thereto, whether oral or written. Software shall be deemed
irrevocably accepted by End User upon installation. No waiver or modification
of the Agreement will be valid unless signed by each party. The waiver of a
breach of any term hereof will in no way be construed as a waiver of any other
term or breach hereof. The headings in this Agreement do not affect its
```

(continues on next page)

(continued from previous page)

```
interpretation. End User may not assign or transfer any of its rights or
obligations under this Agreement to a third party without the prior written
consent of Penguin. Any attempted assignment or transfer in violation of the
foregoing will be null and void. If any provision of this Agreement is held by
a court of competent jurisdiction to be unenforceable, the remaining provisions
of this Agreement will remain in full force and effect. This Agreement is
governed by the laws of the State of California without reference to conflict
of laws principles that would require the application of the laws of any other
state. The United Nations Convention on Contracts for the International Sale of
Goods shall not apply to this Agreement. All disputes arising out of this
Agreement will be subject to the exclusive jurisdiction of the state and federal
courts located in San Francisco County, California, and the parties agree and
submit to the personal and exclusive jurisdiction and venue of these courts.
Should you have any questions about this Agreement, or if you desire to contact
Penguin, please contact us by mail at
Penguin Computing, Inc., 45800 Northport Loop West, Fremont, CA 94538.
```

CHAPTER

TWELVE

THIRDPARTY LICENSE AGREEMENTS

```
Third Party Open Source License Terms Guide

All platforms:
==============

This Software incorporates certain open software in its stack.  The
license terms associated with this software require that we give
copyright and license information, and this Third Party Open Source
License Terms Guide (“TPOSLTG”) provides those details.

1. Licensing terms Bootstrap

    The MIT License (MIT)

    Copyright (c) 2011-2016 Twitter, Inc.

    Permission is hereby granted, free of charge, to any person obtaining a copy
    of this software and associated documentation files (the "Software"), to deal
    in the Software without restriction, including without limitation the rights
    to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
    copies of the Software, and to permit persons to whom the Software is
    furnished to do so, subject to the following conditions:

    The above copyright notice and this permission notice shall be included in
    all copies or substantial portions of the Software.

    THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
    IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
    FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
    AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
    LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
    OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
    THE SOFTWARE.

    Source, as of 03/27/17: https://github.com/angular-ui/bootstrap/blob/master/LICENSE

2. Licensing terms Broadway.js

    Copyright (c) 2011, Project Authors (see AUTHORS file)
    All rights reserved.
```

(continues on next page)

(continued from previous page)

```
    Redistribution and use in source and binary forms, with or without
    modification, are permitted provided that the following conditions
    are met:

      *  Redistributions of source code must retain the above
         copyright notice, this list of conditions and the following
         disclaimer.
      *  Redistributions in binary form must reproduce the above
         copyright notice, this list of conditions and the following
         disclaimer in the documentation and/or other materials
         provided with the distribution.
      *  Neither the names of the Project Authors nor the names of its
         contributors may be used to endorse or promote products
         derived from this software without specific prior written
         permission.

    THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
    CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES,
    INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
    MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
    DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS
    BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
    EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED
    TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES LOSS OF USE,
    DATA, OR PROFITS OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON
    ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR
    TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF
    THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
    SUCH DAMAGE.

    --

    The 3-clause BSD above applies to all code except for code
    originating from the Android project (the .cpp files in
    Avc/). Those files are under the Android project's Apache 2.0
    license.


    Source, as of 03/27/17: https://github.com/mbebenita/Broadway/blob/master/LICENSE

3. Licensing terms ffmpeg

    Most files in FFmpeg are under the GNU Lesser General Public
    License version 2.1 or later (LGPL v2.1+). Read the file
    COPYING.LGPLv2.1 for details. Some other files have
    MIT/X11/BSD-style licenses. In combination the LGPL v2.1+ applies
    to FFmpeg.

    Some optional parts of FFmpeg are licensed under the GNU General
    Public License version 2 or later (GPL v2+). See the file
    COPYING.GPLv2 for details. None of these parts are used by
```

(continues on next page)

(continued from previous page)

```
default, you have to explicitly pass --enable-gpl to configure to
activate them. In this case, FFmpeg's license changes to GPL v2+.

Specifically, the GPL parts of FFmpeg are:

    libpostproc
    optional x86 optimization in the files
        libavcodec/x86/flac_dsp_gpl.asm
        libavcodec/x86/idct_mmx.c
        libavfilter/x86/vf_removegrain.asm
    the following building and testing tools
        compat/solaris/make_sunver.pl
        doc/t2h.pm
        doc/texi2pod.pl
        libswresample/swresample-test.c
        tests/checkasm/*
        tests/tiny_ssim.c
    the following filters in libavfilter:
        vf_blackframe.c
        vf_boxblur.c
        vf_colormatrix.c
        vf_cover_rect.c
        vf_cropdetect.c
        vf_delogo.c
        vf_eq.c
        vf_find_rect.c
        vf_fspp.c
        vf_geq.c
        vf_histeq.c
        vf_hqdn3d.c
        vf_interlace.c
        vf_kerndeint.c
        vf_mcdeint.c
        vf_mpdecimate.c
        vf_owdenoise.c
        vf_perspective.c
        vf_phase.c
        vf_pp.c
        vf_pp7.c
        vf_pullup.c
        vf_repeatfields.c
        vf_sab.c
        vf_smartblur.c
        vf_spp.c
        vf_stereo3d.c
        vf_super2xsai.c
        vf_tinterlace.c
        vf_uspp.c
        vsrc_mptestsrc.c

Should you, for whatever reason, prefer to use version 3 of the
(L)GPL, then the configure parameter --enable-version3 will
```

(continues on next page)

(continued from previous page)

```
activate this licensing option for you. Read the file
COPYING.LGPLv3 or, if you have enabled GPL parts, COPYING.GPLv3 to
learn the exact legal terms that apply in this case.

There are a handful of files under other licensing terms, namely:

    The files libavcodec/jfdctfst.c,
    libavcodec/jfdctint_template.c and libavcodec/jrevdct.c are
    taken from libjpeg, see the top of the files for licensing
    details. Specifically note that you must credit the IJG in the
    documentation accompanying your program if you only distribute
    executables. You must also indicate any changes including
    additions and deletions to those three files in the
    documentation.  tests/reference.pnm is under the expat
    license.

External libraries

FFmpeg can be combined with a number of external libraries, which
sometimes affect the licensing of binaries resulting from the
combination.  Compatible libraries

The following libraries are under GPL:

    frei0r
    libcdio
    librubberband
    libvidstab
    libx264
    libx265
    libxavs
    libxvid

When combining them with FFmpeg, FFmpeg needs to be licensed as
GPL as well by passing --enable-gpl to configure.

The OpenCORE and VisualOn libraries are under the Apache License
2.0. That license is incompatible with the LGPL v2.1 and the GPL
v2, but not with version 3 of those licenses. So to combine these
libraries with FFmpeg, the license version needs to be upgraded by
passing --enable-version3 to configure.  Incompatible libraries

There are certain libraries you can combine with FFmpeg whose
licenses are not compatible with the GPL and/or the LGPL. If you
wish to enable these libraries, even in circumstances that their
license may be incompatible, pass --enable-nonfree to
configure. But note that if you enable any of these libraries the
resulting binary will be under a complex license mix that is more
restrictive than the LGPL and that may result in additional
obligations. It is possible that these restrictions cause the
resulting binary to be unredistributable.
```

(continues on next page)

(continued from previous page)

```
    The Fraunhofer FDK AAC and OpenSSL libraries are under licenses
    which are incompatible with the GPLv2 and v3. To the best of our
    knowledge, they are compatible with the LGPL.

    The NVENC library, while its header file is licensed under the
    compatible MIT license, requires a proprietary binary blob at run
    time, and is deemed to be incompatible with the GPL. We are not
    certain if it is compatible with the LGPL, but we require
    --enable-nonfree even with LGPL configurations in case it is not.

    Source as of 03/27/17: https://github.com/FFmpeg/FFmpeg/blob/master/LICENSE.md

4. Licensing terms of Poco

    The Boost Software License 1.0

    Permission is hereby granted, free of charge, to any person or
    organization obtaining a copy of the software and accompanying
    documentation covered by this license (the "Software") to use,
    reproduce, display, distribute, execute, and transmit the
    Software, and to prepare derivative works of the Software, and to
    permit third-parties to whom the Software is furnished to do so,
    all subject to the following:

    The copyright notices in the Software and this entire statement,
    including the above license grant, this restriction and the
    following disclaimer, must be included in all copies of the
    Software, in whole or in part, and all derivative works of the
    Software, unless such copies or derivative works are solely in the
    form of machine-executable object code generated by a source
    language processor.

    THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
    EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
    MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND
    NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
    ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR
    OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING
    FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR
    OTHER DEALINGS IN THE SOFTWARE.

    Source as of 03/27/17: https://pocoproject.org/license.html

5. Licensing terms of OverlayScrollbars

    MIT License

    Copyright (c) 2017 Rene Haas

    Permission is hereby granted, free of charge, to any person
    obtaining a copy of this software and associated documentation
    files (the "Software"), to deal in the Software without
```

(continues on next page)

(continued from previous page)

```
    restriction, including without limitation the rights to use, copy,
    modify, merge, publish, distribute, sublicense, and/or sell copies
    of the Software, and to permit persons to whom the Software is
    furnished to do so, subject to the following conditions:

    The above copyright notice and this permission notice shall be
    included in all copies or substantial portions of the Software.

    THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
    EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
    MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
    NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
    HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,
    WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
    OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER
    DEALINGS IN THE SOFTWARE.

6. Licensing terms of css-loaders

    The MIT License (MIT)

    Copyright (c) 2014 Luke Haas

    Permission is hereby granted, free of charge, to any person obtaining a copy of
    this software and associated documentation files (the "Software"), to deal in
    the Software without restriction, including without limitation the rights to
    use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of
    the Software, and to permit persons to whom the Software is furnished to do so,
    subject to the following conditions:

    The above copyright notice and this permission notice shall be included in all
    copies or substantial portions of the Software.

    THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
    IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS
    FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR
    COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER
    IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN
    CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

7.  License fonts provided by Google, Inc (https://fonts.google.com/attribution)

    Roboto[wdth,wght].ttf: Copyright 2011 The Roboto Project Authors (https://github.com/
↪googlefonts/roboto-classic)

    Roboto-Italic[wdth,wght].ttf: Copyright 2011 The Roboto Project Authors (https://
↪github.com/googlefonts/roboto-classic)

    DMSans[opsz,wght].ttf: Copyright 2014 The DM Sans Project Authors (https://github.
↪com/googlefonts/dm-fonts)

    DMSans-Italic[opsz,wght].ttf: Copyright 2014 The DM Sans Project Authors (https://
```

(continues on next page)

(continued from previous page)

```
↪github.com/googlefonts/dm-fonts)


   This Font Software is licensed under the SIL Open Font License, Version 1.1.
   This license is copied below, and is also available with a FAQ at:
   https://openfontlicense.org

   -----------------------------------------------------------
   SIL OPEN FONT LICENSE Version 1.1 - 26 February 2007
   -----------------------------------------------------------

   PREAMBLE
   The goals of the Open Font License (OFL) are to stimulate worldwide
   development of collaborative font projects, to support the font creation
   efforts of academic and linguistic communities, and to provide a free and
   open framework in which fonts may be shared and improved in partnership
   with others.

   The OFL allows the licensed fonts to be used, studied, modified and
   redistributed freely as long as they are not sold by themselves. The
   fonts, including any derivative works, can be bundled, embedded,
   redistributed and/or sold with any software provided that any reserved
   names are not used by derivative works. The fonts and derivatives,
   however, cannot be released under any other type of license. The
   requirement for fonts to remain under this license does not apply
   to any document created using the fonts or their derivatives.

   DEFINITIONS
   "Font Software" refers to the set of files released by the Copyright
   Holder(s) under this license and clearly marked as such. This may
   include source files, build scripts and documentation.

   "Reserved Font Name" refers to any names specified as such after the
   copyright statement(s).

   "Original Version" refers to the collection of Font Software components as
   distributed by the Copyright Holder(s).

   "Modified Version" refers to any derivative made by adding to, deleting,
   or substituting -- in part or in whole -- any of the components of the
   Original Version, by changing formats or by porting the Font Software to a
   new environment.

   "Author" refers to any designer, engineer, programmer, technical
   writer or other person who contributed to the Font Software.

   PERMISSION & CONDITIONS
   Permission is hereby granted, free of charge, to any person obtaining
   a copy of the Font Software, to use, study, copy, merge, embed, modify,
   redistribute, and sell modified and unmodified copies of the Font
   Software, subject to the following conditions:
```

(continues on next page)

(continued from previous page)

```
    1) Neither the Font Software nor any of its individual components,
    in Original or Modified Versions, may be sold by itself.

    2) Original or Modified Versions of the Font Software may be bundled,
    redistributed and/or sold with any software, provided that each copy
    contains the above copyright notice and this license. These can be
    included either as stand-alone text files, human-readable headers or
    in the appropriate machine-readable metadata fields within text or
    binary files as long as those fields can be easily viewed by the user.

    3) No Modified Version of the Font Software may use the Reserved Font
    Name(s) unless explicit written permission is granted by the corresponding
    Copyright Holder. This restriction only applies to the primary font name as
    presented to the users.

    4) The name(s) of the Copyright Holder(s) or the Author(s) of the Font
    Software shall not be used to promote, endorse or advertise any
    Modified Version, except to acknowledge the contribution(s) of the
    Copyright Holder(s) and the Author(s) or with their explicit written
    permission.

    5) The Font Software, modified or unmodified, in part or in whole,
    must be distributed entirely under this license, and must not be
    distributed under any other license. The requirement for fonts to
    remain under this license does not apply to any document created
    using the Font Software.

    TERMINATION
    This license becomes null and void if any of the above conditions are
    not met.

    DISCLAIMER
    THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
    EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF
    MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT
    OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL THE
    COPYRIGHT HOLDER BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,
    INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL
    DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
    FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM
    OTHER DEALINGS IN THE FONT SOFTWARE.

MacOS and Windows only:
=======================

8. Licensing terms OpenSSL


      LICENSE ISSUES
      ==============

      The OpenSSL toolkit stays under a double license, i.e. both the
```

(continues on next page)

(continued from previous page)

```
  conditions of the OpenSSL License and the original SSLeay
  license apply to the toolkit.  See below for the actual license
  texts.

  OpenSSL License
  ---------------

/* ====================================================================
 * Copyright (c) 1998-2017 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES
 * LOSS OF USE, DATA, OR PROFITS OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
```

(continues on next page)

(continued from previous page)

```
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */

 Original SSLeay License
 -----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
```

(continues on next page)

(continued from previous page)

```
     * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
     * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
     * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
     * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
     * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
     * OR SERVICES LOSS OF USE, DATA, OR PROFITS OR BUSINESS INTERRUPTION)
     * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
     * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
     * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
     * SUCH DAMAGE.
     *
     * The licence and distribution terms for any publically available version or
     * derivative of this code cannot be changed.  i.e. this code cannot simply be
     * copied and put under another distribution licence
     * [including the GNU Public Licence.]
     */

    Source as of 03/27/17: https://www.openssl.org/source/license.html

Windows only:
=============

9. Licensing terms AW_SAS64

    Source as of 03/27/17:
    https://softltd.wordpress.com/simulate-ctrl-alt-del-in-windows-vista-7-and-server-
↪2008/

    AW_SASxx DLLs and other materials included in the Free
    Distribution Package

    END USER LICENSE AGREEMENT TERMS AND CONDITIONS

    Please read the terms and conditions of this license agreement
    (the "License") before installing the computer software (the
    "Software").  By installing and using the Software you accept and
    agree to the terms of this License.  This License constitutes the
    entire agreement concerning the Software between you and Jose
    Pascoa. If you do not agree with these terms and conditions,
    promptly uninstall or remove the Software.

    The term "Software" includes, and these terms and conditions also
    apply to, any updates, modifications and upgrades to the Software
    that you may receive after the initial release.

    1. License Grant. This License permits you to use the supplied
    aw_sasxx DLLs in any software you develop and distribute, sell or
    give away according to your own criteria, except, Use of the
    Software with with any product that is distributed as Open Source
    or is distributed under the terms of GNU General Public License
    (GPL) or where the Source Code of the application is required to
    be freely distributed is NOT ALLOWED.  You agree that you will not
```

(continues on next page)

(continued from previous page)

```
    modify, adapt, rename or translate, or disassemble, decompile,
    reverse engineer or otherwise attempt to discover the source code
    of any parts of the Software supplied in EXE or DLL form.

    2. Jose Pascoa DISCLAIMS ANY AND ALL WARRANTIES, EXPRESS OR
    IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR
    FITNESS FOR PARTICULAR PURPOSE.  Jose Pascoa does not warrant that
    the Software, its use, operation or your ability to use the
    Software will be uninterrupted or error-free or that all Software
    errors will be corrected. Jose Pascoa does not warrant that the
    Software or service will meet your requirements.

    3. Limitations of Liability.  In no event shall Jose Pascoa be
    liable for any damages to you or any other party whether arising
    out of contract or from tort including loss of data, profits or
    business or other special, incidental, exemplary or consequential
    damages, even if Jose Pascoa has been advised of the possibility
    of such loss or damages.  Jose Pascoa's cumulative liability shall
    not exceed the license fee paid, which is none in this case, for
    use of this Software and Documentation.

    Jose Pascoa is a registered Software Developer, with address in
    Lisbon, Portugal

10. Licensing terms of screen-capture-recorder as agreed upon with Roger Pack on 03/27/17

    Copyright (c) 2017, Roger Pack (rogerpack2005@gmail.com )
    All rights reserved.

    Redistribution and use in source and binary forms, with or without
    modification, are permitted provided that the following conditions
    are met:

    1. Redistributions of source code must retain the above copyright
       notice, this list of conditions and the following disclaimer.
    2. Redistributions in binary form must reproduce the above
       copyright notice, this list of conditions and the following
       disclaimer in the documentation and/or other materials provided
       with the distribution.

    THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
    CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES,
    INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
    MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
    DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS
    BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
    EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED
    TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES LOSS OF USE,
    DATA, OR PROFITS OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON
    ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR
    TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF
    THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
```

(continues on next page)

(continued from previous page)

```
    SUCH DAMAGE.

    The views and conclusions contained in the software and
    documentation are those of the authors and should not be
    interpreted as representing official policies, either expressed or
    implied, of the FreeBSD Project.

    Source as of 03/27/17, modified were copyright year and copyright
    holder: https://en.wikipedia.org/wiki/BSD_licenses

11. Licensing terms of WinToast

    MIT License

    Copyright (C) 2016-2023 WinToast v1.3.0 - Mohammed Boujemaoui <mohabouje@gmail.com>

    Permission is hereby granted, free of charge, to any person obtaining a copy of
    this software and associated documentation files (the "Software"), to deal in
    the Software without restriction, including without limitation the rights to
    use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of
    the Software, and to permit persons to whom the Software is furnished to do so,
    subject to the following conditions:

    The above copyright notice and this permission notice shall be included in all
    copies or substantial portions of the Software.

    THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
    IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS
    FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR
    COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER
    IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN
    CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Linux only:
===========

12. Licensing terms NVIDIA GRID SDK

    NVIDIA GRID Software License Agreement

    IMPORTANT NOTICE - PLEASE READ THIS NVIDIA GRID SOFTWARE LICENSE
    AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE.  USE OF THIS
    SOFTWARE IS SUBJECT TO THIS AGREEMENT.  YOU WILL BE ASKED TO
    REVIEW AND EITHER ACCEPT OR NOT ACCEPT THE TERMS OF THIS
    AGREEMENT.

    This GRID Software License Agreement (“Agreement”) is a legal
    agreement between you (“You” or “Licensee”) and NVIDIA Corporation
    ("NVIDIA") which governs the use of NVIDIA GRID frame capture and
    hardware-accelerated video encoding API’s and associated sample
    source code, header files and documentation provided or otherwise
    made available to you ("Software").  By downloading, installing,
```

(continues on next page)

(continued from previous page)

```
or otherwise using the Software, you agree to be bound by the
terms of this Agreement.  If you do not agree to the terms of this
Agreement, do not download, install or otherwise use the Software.
If You are an entity, You acknowledge that the individual
accepting the Agreement has appropriate authority to do so and to
bind You.

The Software is protected by copyright laws and international
copyright treaties, as well as other intellectual property laws
and treaties. The Software is not sold, and instead is only
licensed for use, strictly in accordance with this document. GRID
hardware products are protected by various patents, and are sold,
but this Agreement does not cover that sale, since it may not
necessarily be sold with the Software. This Agreement sets forth
the terms and conditions of the Software only.  Any other use of
the applicable driver software by Licensee will only be under the
terms of a separate license agreement from NVIDIA.


SECTION 1 - LICENSE

1.1 License Grant.  Provided that Licensee is in compliance with
the terms and conditions of this Agreement, NVIDIA grants to
Licensee a nonexclusive, non-transferable, worldwide, revocable,
limited, royalty-free, fully paid-up license to: (i) use,
reproduce, modify and prepare derivative works of the Software
solely for Your own internal development and testing of the
Software with Licensee's product(s) and/or service(s) ("Licensee
Product") for use with GRID or Quadro 4000+ products only (ii)
reproduce and use the Software internally only with GRID or Quadro
4000+ products to provide the Licensee Product services and (iii)
reproduce and distribute the Software (in object code only)
bundled with Licensee Product for use only with GRID or Quadro
4000+ products to Licensee's customers and grant to Licensee's
customers a sublicense to use the Software as compiled with
Licensee Products for use only with GRID or Quadro 4000+ products
under a written, legally enforceable agreement that has the effect
of protecting the Software and the rights of NVIDIA under terms no
less restrictive than this Agreement.

1.2 Limitations.  Unless otherwise authorized in the Agreement,
Licensee shall not otherwise assign, sublicense, lease, or in any
other way transfer or disclose Software to any third party.
Licensee shall not reverse- compile, disassemble,
reverse-engineer, or in any manner attempt to derive the source
code of the Software from the object code portions of the
Software.  Licensee acknowledges and agrees this Software is
licensed for use only in conjunction with NVIDIA GRID and Quadro
4000+ hardware products. Use of the Software in conjunction with
other NVIDIA hardware products or non-NVIDIA hardware and/or
software products is not licensed hereunder.
```

(continues on next page)

(continued from previous page)

```
1.3 No Other License.  Except as expressly stated in this
Agreement, no license or right is granted to Licensee directly or
by implication, inducement, estoppel or otherwise. NVIDIA shall
have the right to inspect or have an independent auditor inspect
Licensee's relevant records to verify Licensee's compliance with
the terms and conditions of this Agreement.

SECTION 2 - CONFIDENTIALITY

2.1 Confidential Information.  Licensee acknowledges and agrees
that the Software, documentation and other information (if such
other information is identified as confidential or should be
reasonably recognized as confidential under the circumstances)
provided to Licensee by NVIDIA hereunder (collectively,
"Confidential Information") constitute the confidential and
proprietary information of NVIDIA and that Licensee's protection
thereof is an essential condition to Licensee's use and possession
of the Software.  Licensee shall retain all Confidential
Information in strict confidence and not disclose it to any third
party or use it in any way except as permitted by this Agreement.
Licensee shall exercise at least the same amount of diligence in
preserving the secrecy of the Confidential Information as it uses
in preserving the secrecy of its own most valuable confidential
information, but in no event less than reasonable diligence.
Notwithstanding the foregoing, all documents and other tangible
objects containing or representing NVIDIA Confidential Information
and all copies thereof which are in the possession of Licensee
shall be and remain the property of NVIDIA and shall be promptly
returned to NVIDIA upon termination of this Agreement.

2.2 Contractor.  If Licensee wishes to have a third party
consultant or subcontractor ("Contractor") perform work on
Licensee's behalf which involves access to or use of Software,
Licensee shall obtain a written confidentiality agreement from the
Contractor which contains terms and obligations with respect to
access to or use of Software no less restrictive than those set
forth in this Agreement and excluding any distribution or
sublicense rights, and use for any other purpose than permitted in
this Agreement. Otherwise, Licensee shall not disclose the terms
or existence of this Agreement or use NVIDIA's name in any
publications, advertisements, or other announcements without
NVIDIA's prior written consent.  Unless otherwise provided in this
Agreement, Licensee does not have any rights to use any NVIDIA
trademarks or logos.

SECTION 3 - OWNERSHIP OF SOFTWARE AND INTELLECTUAL PROPERTY RIGHTS

3.1 Ownership.  All rights, title and interest to all copies of
the Software remain with NVIDIA, subsidiaries, licensors, or its
suppliers. The Software is copyrighted and protected by the laws
of the United States and other countries, and international treaty
provisions. Licensee may not remove any copyright notices from the
```

(continues on next page)

(continued from previous page)

```
Software. NVIDIA may make changes to the Software, or to items
referenced therein, at any time and without notice, but is not
obligated to support or update the Software. Except as otherwise
expressly provided, NVIDIA grants no express or implied right
under any NVIDIA patents, copyrights, trademarks, or other
intellectual property rights.

3.2 Modifications.  Licensee holds all rights, title and interest
in the modifications to and derivative works of the Software that
Licensee creates, subject to NVIDIA's underlying intellectual
property rights to the Software provided, however that Licensee
grants NVIDIA an irrevocable, perpetual, nonexclusive, worldwide,
royalty-free paid-up license to make, have made, use, have used,
sell, license, distribute, sublicense or otherwise transfer
derivative works to the Software created by Licensee that add
functionality or improvement to the Software.

3.3 Feedback.  Licensee has no obligation to give NVIDIA any
suggestions, comments or other feedback ("Feedback") relating to
the Software.  However, NVIDIA may use and include any Feedback
that Licensee voluntarily provides to improve the Software or
other related NVIDIA technologies.  Accordingly, if Licensee
provides Feedback, Licensee agrees NVIDIA and its licensees may
freely use, reproduce, license, distribute, and otherwise
commercialize the Feedback in the Software or other related
technologies without the payment of any royalties or fees.

3.4 Third Party Technology.  Licensee acknowledges and agrees that
it is Licensee's sole responsibility to obtain any, additional,
third party licenses required to make, have made, use, have used,
sell, import, and offer for sale Licensee Products that include or
incorporate any third party technology and content relating to
audio and/or video encoders and decoders from, including but not
limited to, Microsoft, Thomson, Fraunhofer IIS, Sisvel S.p.A.,
MPEG-LA, and Coding Technologies ("Third Party Technology").
Licensee acknowledges and agrees that NVIDIA has not granted to
Licensee under this Agreement any necessary patent rights with
respect to the Third Party Technology.  As such, Licensee's use of
the Third Party Technology may be subject to further restrictions
and terms and conditions.  Licensee acknowledges and agrees that
Licensee is solely and exclusively responsible for obtaining any
and all authorizations and licenses required for the use,
distribution and/or incorporation of the Third Party Technology.

3.5 Licensee Indemnity.  Licensee shall, at its own expense fully
indemnify, hold harmless, defend and/or settle any claim, suit or
proceeding that is asserted by a third party against NVIDIA and
its officers, employees or agents, to the extent such claim, suit
or proceeding arising from or related to Licensee's failure to
fully satisfy and/or comply with the third party licensing
obligations related to the Third Party Technology (a "Claim").  In
the event of a Claim, Licensee agrees to: (a) pay all damages or
```

(continues on next page)

(continued from previous page)

```
settlement amounts, which shall not be finalized without the prior
written consent of NVIDIA, (including other reasonable costs
incurred by NVIDIA, including reasonable attorneys fees, in
connection with enforcing this paragraph) (b) reimburse NVIDIA
for any licensing fees and/or penalties incurred by NVIDIA in
connection with a Claim and (c) immediately procure/satisfy the
third party licensing obligations before using the Software
pursuant to this Agreement.

SECTION 4 - NO WARRANTIES

THE SOFTWARE IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED
WARRANTY OF ANY KIND, INCLUDING WARRANTIES OF MERCHANTABILITY,
NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. NVIDIA DOES
NOT REPRESENT OR WARRANT THAT THE SOFTWARE WILL MEET LICENSEE'S
REQUIREMENT OR THAT THE OPERATION OF THE SOFTWARE WILL BE
UNINTERRUPTED OR ERROR FREE.

SECTION 5 - LIMITATION OF LIABILITY

IN NO EVENT SHALL NVIDIA, ITS SUBSIDIARIES, LICENSORS, OR
SUPPLIERS BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL
OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT
LIMITATION, LOSS OF USE, LOSS OF DATA, BUSINESS INTERUPTION OR
LOST PROFITS) IN CONNECTION WITH THIS AGREEMENT OR ARISING OUT OF
THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF NVIDIA HAS
BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME
JURISDICTIONS PROHIBIT EXCLUSION OR LIMITATION OF LIABILITY FOR
IMPLIED WARRANTIES OR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE
ABOVE LIMITATION MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER
LEGAL RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION.  IN NO
EVENT SHALL WILL NVIDIA'S AGGREGATE LIABILITY ARISING OUT OF THIS
AGREEMENT EXCEED ONE HUNDRED UNITED STATES DOLLARS (USD$100).  THE
LICENSEE IS SOLELY RESPONSIBLE FOR THE PROTECTION AND BACK-UP OF
ALL DATA AND SOFTWARE.

SECTION 6 - TERM AND TERMINATION

6.1 Term.  This Agreement is effective until (i) automatically
terminated if Licensee fails to comply with any of the terms and
conditions of this Agreement or (ii) earlier terminated by NVIDIA
in accordance with Section 6.2 (Termination).

6.2 Termination.  In the event of actual or threatened breach of
this Agreement by Licensee, NVIDIA may terminate this Agreement
and the licenses granted hereunder, in addition to any other
remedies it may have.  If Licensee commences or participates in
any legal proceeding against NVIDIA, then NVIDIA may, in its sole
discretion, suspend or terminate all license grants and any other
rights provided under this Agreement.  Upon termination, Licensee
shall immediately cease using and immediately return all copies of
the Software to NVIDIA, or destroy the Software and certify to
```

(continues on next page)

(continued from previous page)

```
NVIDIA in writing that such actions have been completed.

6.3 Survival.  Those provisions in this Agreement, which by their
nature need to survive the termination or expiration of this
Agreement, shall survive termination or expiration of the
Agreement, including but not limited to Sections 2, 3, 4, 5, 6.2,
6.3, and 7.

SECTION 7 - MISCELLANEOUS

This Agreement shall be deemed to have been made in, and shall be
construed pursuant to, the laws of the State of Delaware. The
state and/or federal courts residing in Santa Clara County,
California shall have exclusive jurisdiction over any dispute or
claim arising out of this Agreement.  This Agreement is the final,
complete and exclusive agreement between the parties relating to
the subject matter hereof, and supersedes all prior or
contemporaneous understandings and agreements relating to such
subject matter, whether oral or written.  If any provision of this
Agreement is inconsistent with, or cannot be fully enforced under,
the law, such provision will be construed as limited to the extent
necessary to be consistent with and fully enforceable under the
law.  This Agreement, and Licensee's rights and obligations
herein, may not be assigned, subcontracted, delegated, or
otherwise transferred by Licensee without NVIDIA's prior written
consent, and any attempted assignment, subcontract, delegation, or
transfer in violation of the foregoing will be null and void.  The
terms of this Agreement shall be binding upon permitted
assignees. The Parties acknowledge that they are independent
contractors and no other relationship, including partnership,
joint venture, employment, franchise, master/servant or
principal/agent, is intended by this Agreement.  Neither Party
shall have the right to bind or obligate the other.  Failure by
either Party to enforce any provision of this Agreement will not
be deemed a waiver of future enforcement of that or any other
provision.  Licensee shall not ship, transfer or export the
Software into any country, or use the Software in any manner,
prohibited by the United States Bureau of Industry and Security or
any export laws, restrictions or regulations.


1
NVIDIA GRID Software License Agreement v.f.nstr02

Source as of 03/27/17: GRID-SDK 2.2 installer from NVIDIA Corporation
```