Scyld Cloud Workstation Documentation

Release 11.3.1

Penguin Computing

Mar 28, 2022

CONTENTS

Contents:

ONE

ABOUT SCYLD CLOUD WORKSTATION

Scyld Cloud Workstation 11.3.1, commit 062f9c390b01c3482b87f54a7a2eb72751f5d545.

INTRODUCTION

Scyld Cloud Workstation 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.

This document describes system requirements, installation, configuration, and usage.

SERVER REQUIREMENTS

This section describes the hardware and software requirements for the workstation hosting the Scyld Cloud Workstation server.

3.1 Server OS

Scyld Cloud Workstation is supported and tested on the following 64-bit operating systems:

- CentOS 7 and 8

- Windows 7, 8, and 10

- MacOS High Sierra 10.13 to Monterey 12

Beta support is available for:

- Ubuntu 16 and 18

Important: CentOS 8 users: XWayland is not currently supported. Please see *Installing the Server on CentOS 8* 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 Computing for additional support.

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

3.3 Server NVIDIA NVFBC Support (Optional)

Scyld Cloud Workstation can autodetect and utilize the NVFBC feature available on servers with GRID, Tesla, and Quadro 2000+ NVIDIA GPUs.

For older GRID GPUs, we recommend NVIDIA driver version 369.49 on Windows and 361.42 in Linux.

For Tesla and Quadro 2000+ GPUs, we recommend NVIDIA driver version 392.37 for Windows and 410.66 or later for Linux.

3.4 Server Network

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

A client's bandwidth requirements is 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
```

3.5 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.

Scyld Cloud Workstation allows system administrators to pick a maximum screen resolution width and height in the config file (by default 1920x1080). 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*.

3.6 Server Audio

Scyld Cloud Workstation 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 in CentOS 7+ and Ubuntu 16+.

If Scyld Cloud Workstation is installed on a Windows VM, you may need to install Screen Capture Recorder to enable audio support. Screen Capture Recorder has been tested in Windows 10 and can be downloaded from the URL below:

https://github.com/rdp/screen-capture-recorder-to-video-windows-free/releases/download/0.12.10/Setup.Screen.Capturer.Recorder.v0.12.10.exe

MacOS users must follow the instructions in *Install BlackHole for MacOS Audio* for instructions on adding MacOS Audio Support.

3.7 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 Scyld Cloud Workstation server-side installer.

3.8 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 Scyld Cloud Workstation web server. By default, Scyld Cloud Workstation 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*.

CLIENT REQUIREMENTS

You can connect to the server using either an HTML5 browser or our native client (Scyld Cloud Workstation Client).

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 Scyld Cloud Workstation Client is more optimized than the Chrome Browser so it requires lower CPU resources to achive 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.

4.2 Web Browser

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

- Chrome 59+

- FireFox 56+

- Internet Explorer 11+

- Microsoft Edge Legacy 44.17763.1.0+

- Microsoft Edge 79+

- Safari 7+

Note: Chrome provides the best performance and is recommended.

Note: FireFox 52.4.0 in CentOS 7 is known to have screen flickering issues. Please update to 60.8 and above.

These browsers by default enable TLS 1.2, WebGL and WebSocket features that are necessary for security and optimal Scyld Cloud Workstation performance. While WebSocket support is a hard requirement, Scyld Cloud Workstation 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 Scyld Cloud Workstation 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.

4.3 Scyld Cloud Workstation Client

Scyld Cloud Workstation Client is a native client that requires a separate application installation on local machines. It is nearly identical to the web browser, but it includes some additional benefits:

- faster frame rates at higher screen resolutions

- lossless and visually lossless video support

- audio support

- support for keyboard shortcuts reserved by web browsers (for example: `Ctrl + T`, `Ctrl + N`, `Ctrl + W`)

Scyld Cloud Workstation Client is supported and tested on the following 64-bit operating systems:

- CentOS 7 and 8

- Windows 7, 8, and 10

- MacOS High Sierra 10.13 to Monterey 12

Beta support is available for:

- Ubuntu 16 and 18

Note: OpenGL 2.1 support is required.

Note: New in v11.2! Scyld Cloud Workstation Client can also be launched from URI links such as: `scw://<server>`

FIVE

SERVER-CLIENT VERSION COMPATABILITY

Scyld Cloud Workstation and Scyld Cloud Workstation Client versions are compatible if they are from the same compatible range. The current list of compatible version ranges is given below.

- v11.0 and later
- v9.1 until v11.0

FEATURE REQUIREMENTS AND SETUP

Scyld Cloud Workstation 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 1440p

- Audio

- Multi-display support

- Text paste

- Quality of Service adaptation

- US keyboard and mouse support

- Collaboration

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

- *All Operating Systems*
    - *Enabling 4K Video on all OSes*
    - *Enabling Lossless and Visually Lossless Video on all OSes*
- *CentOS 7*
    - *Enabling USB Forwarding on CentOS 7*
- *CentOS 8*
    - *Enabling USB Forwarding on CentOS 8*
    - *Enabling Xorg X server as the default on CentOS 8*
- *Windows*
    - *Enabling Audio on Windows VMs*
- *MacOS*
    - *Enabling Audio on MacOS*
    - *Enabling USB Forwarding on MacOS Big Sur*
    - *Re-Enabling USB Forwarding after Updating to MacOS Monterey*

6.1 All Operating Systems

- *Enabling 4K Video on all OSes*
- *Enabling Lossless and Visually Lossless Video on all OSes*

6.1.1 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.

6.1.2 Enabling Lossless and Visually Lossless Video on all OSes

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

6.2 CentOS 7

- *Enabling USB Forwarding on CentOS 7*

6.2.1 Enabling USB Forwarding on CentOS 7

ONLY IF you have a `scw-usb` feature in your license file: Install the scw-el7 repository and then use the `yum` command to install `kmod-usbip` and `usbip-utils`. These packages are needed to enable USB forwarding.

```
% sudo wget https://updates.penguincomputing.com/scw/scw-el7.repo -P /etc/yum.repos.d
% sudo yum install -y kmod-usbip usbip-utils
```

6.3 CentOS 8

- *Enabling USB Forwarding on CentOS 8*
- *Enabling Xorg X server as the default on CentOS 8*

6.3.1 Enabling USB Forwarding on CentOS 8

ONLY IF you have a `scw-usb` feature in your license file: Install the scw-el8 repository and then use the `yum` command to install `kmod-usbip` and `usbip-utils`. These packages are needed to enable USB forwarding.

```
% sudo wget https://updates.penguincomputing.com/scw/scw-el8.repo -P /etc/yum.repos.d
% sudo yum install -y kmod-usbip usbip-utils
```

6.3.2 Enabling Xorg X server as the default on CentOS 8

XWayland is not currently supported. Please see *Installing the Server on CentOS 8* for instructions on enabling Xorg as the default X server.

6.4 Windows

- *Enabling Audio on Windows VMs*

6.4.1 Enabling Audio on Windows VMs

Only if you are running the server on a Windows Virtual Machine: Download and install Screen Capture Recorder 0.12.10.

6.5 MacOS

- *Enabling Audio on MacOS*
- *Enabling USB Forwarding on MacOS Big Sur*
- *Re-Enabling USB Forwarding after Updating to MacOS Monterey*

6.5.1 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.

6.5.2 Enabling USB Forwarding on MacOS Big Sur

USB Forwarding to Big Sur servers is no longer supported due to a change in Big Sur. Please update to MacOS Monterey for USB Forwarding support. NOTE: Big Sur clients can still forward USB devices to other servers.

6.5.3 Re-Enabling USB Forwarding after Updating to MacOS Monterey

If you have an existing Scyld Cloud Workstation 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 'scyld-cloud-workstation' 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

RELEASE NOTES

This page lists the version history of Scyld Cloud Workstation releases.

7.1 What's New in 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

7.2 Version History

7.2.1 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
- **Known Issue:** Updating the server-side to MacOS Monterey or later will disable USB fowarding for existing Scyld Cloud Workstation installations. This can be re-enabled by following the steps in *Re-Enabling USB Forwarding after Updating to MacOS Monterey*

- 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 **Audio.Output.SampleRate** values 48000 and 96000
- Fixed issue with scrollbars being inaccessible in fullscreen

7.2.2 v11.2.1

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

7.2.3 v11.2.0

- **Added ability to launch the native client using new URI scheme:** `scw://<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
- **Known Issue:** For MacOS Clients, when you forward or unforward a USB device you may get a pop-up that says: "Driver Installation problem. Failed to install the Server driver. Ensure you have approved the Kernel Extension and/or reboot and try again and/or turn off SIP." This message can be safely ignored
- **Known Issue:** Enabling Avast Antivirus can crash or cause unstable behavior with the native client. Possible workarounds include creating an exception for the native client or disabling Avast

7.2.4 v11.1.1

- Fixed MacOS and Windows client whitescreen issue

7.2.5 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 keydown issue
- Added –broker-passwd flag for MacOS
- Changed ScyldCloudAuth based usernames to be case insensitive
- **Known Issue:** The remote cursor on some Windows servers are sometimes offset
- **Known Issue:** Copy and Paste is not currently working with the MacOS client

7.2.6 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
- **Known Issue:** Audio forwarding can only be enabled after logging into the GDM screen
- **Known Issue:** We do not support the XWayland X server. Xorg must be enabled

7.2.7 v10.2.2

- Added security patch to MacOS server
- Fixed missing MacOS client icon
- Known issue: Copy-Paste to a MacOS server is currently not supported

7.2.8 v10.2.1

- **NOTE:** Existing Scyld FlexLM installations should be updated to Scyld 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

7.2.9 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 **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

7.2.10 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

7.2.11 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

7.2.12 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

7.2.13 v9.2.1

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

7.2.14 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

7.2.15 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

7.2.16 v9.1.10

- Added security patch to Server.Auth.OSAuthEnabled 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

7.2.17 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

7.2.18 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.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

- **Known Issue:** The Windows native client does not properly fullscreen

7.2.19 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)

7.2.20 v8.1.5

- Fixed CentOS 6 issue with setting **Server.VideoSource** to `auto` or `nvfbc`

- Fixed minor multi-screen interface issues

- Fixed documentation by changing **Server.ConcurrentClients.MaxClientCount** to **Server.MultiUser.MaxClientCount**

- Hide Guest Invite buttons when **Server.MultiUser.MaxClientCount** is set to `1`

- Fixed QoS stability issues

7.2.21 v8.1.4

- Added support for mouse dragging between tiled screens

- Switched to overlay scrollbars

- Updated QoS algorithm

- Fixed Javascript error in IE11

7.2.22 v8.1.3

- Fixed crash related to screen size changing

- Fixed flickering caused by decoder library and stream video source

- Fixed QoS stability issues

7.2.23 v8.1.2

- Fixed downscaling when resolution height is not divisible by 4

7.2.24 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 scaledown 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

7.2.25 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.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

7.2.26 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

7.2.27 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.IdleUserTimeout** to 120
- Fixed missing OpenSSL libraries in Windows
- Fixed client EULA

7.2.28 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

7.2.29 v7.0.2

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

7.2.30 v7.0.1

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

7.2.31 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

7.2.32 v6.1.1

- Fixed image blurring when enabling unique frames

7.2.33 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)

7.2.34 v6.0.3

- Added browserless 'native' client for CentOS 7 and Windows 7
- Fixed relative paths for Server.LicensePath
- Updated fonts, icons, and colors
- Changed from Windows NSIS installer to MSI installer
- All **Server.ConcurrentClients** configuration settings changed to **Server.MultiUser**

7.2.35 v5.0.7

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

7.2.36 v5.0.6

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

7.2.37 v5.0.5

- Fixed black winlogon screen for stream video source

7.2.38 v5.0.4

- Fixed screen size changing in Windows

7.2.39 v5.0.3

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

7.2.40 v5.0.2

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

7.2.41 v5.0.1

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

7.2.42 v5.0.0

- Added CPU-based (**stream**) video source option
- Added **idle user timeout** (**Server.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.LicenseFile** config setting
- Added ability to delay service start with **Server.StartDelay** config setting
- Renamed **Server.WebSocketServer.Secure** to **Server.Secure**
- Renamed **Server.WebSocketServer.Port** to **Server.Port**
- Renamed **Server.ServiceLogFile** to **Server.BootLogFile**
- Renamed **debug0.txt** to **service.log** and **debug1.txt** to **scyld-cloud-workstation.log**
- Changed Windows install directory to **C:\Program Files\Penguin Computing\Scyld Cloud Workstation**
- 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

7.2.43 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

7.2.44 v3.0.4

- Increased send timeout values
- Added **Server.VideoSendTimeout**, **Server.DataSendTimeout**, and **Server.ReceiveTimeout** to config file

7.2.45 v3.0.3

- Fixed QoS adaptive frame rate algorithm

7.2.46 v3.0.2

- Fixed IE11 fullscreen keyboard and scrollbars

7.2.47 v3.0.1

- Fixed unexpected multi-user client timeouts

7.2.48 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

7.2.49 v2.3.2

- Updated default SSL ciphers

7.2.50 v2.3.1

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

7.2.51 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

7.2.52 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

7.2.53 v2.1.0

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

INSTALLATION

The Scyld Cloud Workstation server can be installed on the following operating systems:

- CentOS 7 and 8

- Ubuntu 16, 18, 20

- Windows 7, 8, and 10

- MacOS High Sierra 10.13 to Monterey 12

8.1 Required Files

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

Installation of the Scyld Cloud Workstation server requires the following files:

- The Scyld Cloud Workstation server installation package for your operating system:

    - CentOS 7: `scyld-cloud-workstation-11.3.1-1.el7.x86_64.rpm`

    - CentOS 8: `scyld-cloud-workstation-11.3.1-1.el8.x86_64.rpm`

    - Ubuntu 16 and 18: `scyld-cloud-workstation_11.3.1.1-0ubuntu1.16_amd64.deb`

    - Ubuntu 20: `scyld-cloud-workstation_11.3.1.1-0ubuntu1.20_amd64.deb`

    - Windows 7, 8 and 10: `Scyld Cloud Workstation-11.3.1.1.msi`

    - MacOS High Sierra 10.13 to Monterey 12: `scyld-cloud-workstation-11.3.1.1.pkg`

- One of the following:

    - A trial license file (`scyld-cloud-workstation.lic`)

    - A floating license file (`scyld-flexlm.lic`) and the license server (Scyld FlexLM).

Note: CentOS 7 and CentOS 8 customers who have a `scw-usb` feature in their license file will also want to install `kmod-usbip` and `usbip-utils` packages.

Note: If you have an NVIDIA graphics card, download and install the appropriate NVIDIA drivers from http://www.nvidia.com/download/index.aspx

8.2 Installing the Server on CentOS 7

Follow the steps below to install Scyld Cloud Workstation, 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. Use the `wget` command to install the Scyld Cloud Workstation YUM repository for CentOS 7.

   ```
   % sudo wget https://updates.penguincomputing.com/scw/scw-el7.repo -P /etc/yum.
   ↪repos.d
   ```

2. Use the `yum install` command to install `scyld-cloud-workstation`.

   ```
   % sudo yum install -y ./scyld-cloud-workstation-11.3.1-1.el7.x86_64.rpm
   ```

   The installer does the following:

   - Installs Scyld Cloud Workstation files to `/opt/scyld-cloud-workstation`
   - Installs scyld-cloud-workstation.service to `/lib/systemd/system/`
   - Reloads the systemd manager configuration using `systemctl daemon-reload`
   - Enables the unit file with `systemctl enable scyld-cloud-workstation.service`

3. If your server's domain has a trusted SSL certificate, open the configuration file (`/opt/scyld-cloud-workstation/bin/scyld-cloud-workstation.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 (`scyld-cloud-workstation.lic`), copy it into `/opt/scyld-cloud-workstation/bin`.
   - If you have a floating license (`scyld-flexlm.lic`), proceed to *Flexera License Management* for instructions on installing Scyld FlexLM.

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

6. ONLY IF you have a `scw-usb` feature in your license file: use the `yum` command to install `kmod-usbip` and `usbip-utils`. These packages are needed to enable USB forwarding.

   ```
   % sudo yum install -y kmod-usbip usbip-utils
   ```

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

   ```
   % sudo systemctl restart scyld-cloud-workstation.service
   ```

Scyld Cloud Workstation should now be reachable over HTTPS at your server's hostname or IP address. For advanced configuration options, please see *Setup*.

8.3 Updating the Server on CentOS 7

1. Use the `yum update` command to update an existing installation:

```
% sudo yum update -y ./scyld-cloud-workstation-11.3.1-1.el7.x86_64.rpm
```

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

```
% sudo systemctl restart scyld-cloud-workstation.service
```

8.4 Installing the Server on CentOS 8

Follow the steps below to install Scyld Cloud Workstation, 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 Scyld Cloud Workstation YUM repository for CentOS 8.

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

2. Use the `yum install` command to install `scyld-cloud-workstation`.

```
% sudo yum install -y ./scyld-cloud-workstation-11.3.1-1.el8.x86_64.rpm
```

   The installer does the following:

   - Installs Scyld Cloud Workstation files to `/opt/scyld-cloud-workstation`
   - Installs scyld-cloud-workstation.service to `/lib/systemd/system/`
   - Reloads the systemd manager configuration using `systemctl daemon-reload`
   - Enables the unit file with `systemctl enable scyld-cloud-workstation.service`

3. If you have a trusted SSL certificate for your server's domain, open the configuration file (`/opt/scyld-cloud-workstation/bin/scyld-cloud-workstation.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 (`scyld-cloud-workstation.lic`), copy it into `/opt/scyld-cloud-workstation/bin`.
   - If you have a floating license (`scyld-flexlm.lic`), proceed to *Flexera License Management* for instructions on installing Scyld FlexLM.

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

6. ONLY IF you have a `scw-usb` feature in your license file: use the `yum` command to install `kmod-usbip` and `usbip-utils`. These packages are needed to enable USB forwarding.

```
% sudo yum install -y kmod-usbip usbip-utils
```

7. ONLY IF you are using XWayland as your X server (enabled by default in CentOS 8), enable Xorg by following these steps:

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

b. Look for the lines below:

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

c. Uncomment (remove the '#') preceeding the 'WayLandEnable' variable.

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

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

```
% sudo systemctl restart scyld-cloud-workstation.service
```

Scyld Cloud Workstation should now be reachable over HTTPS at your server's hostname or IP address. For advanced configuration options, please see *Setup*.

8.5 Updating the Server on CentOS 8

1. Use the `yum update` command to update an existing installation:

```
% sudo yum update -y ./scyld-cloud-workstation-11.3.1-1.el8.x86_64.rpm
```

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

```
% sudo systemctl restart scyld-cloud-workstation.service
```

8.6 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 `Scyld Cloud Workstation-11.3.1.1.msi` from https://updates.penguincomputing.com/scw/download/

2. Double-click on the `Scyld Cloud Workstation-11.3.1.1.msi` installer.

3. Follow the instructions in the GUI. Confirm that you'd like to start Scyld Cloud Workstation as a service to have Scyld Cloud Workstation start automatically.

4. If your server's domain has a trusted SSL certificate, open the configuration file (`C:\Program Files\ Penguin Computing\Scyld Cloud Workstation\scyld-cloud-workstation.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 (`scyld-cloud-workstation.lic`), copy it into `C:\Program Files\ Penguin Computing\Scyld Cloud Workstation`.

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

On some systems (such as those using virt-manager's graphical console), a reboot may be required after installation to ensure that the NVIDIA GRID card is activated.

Scyld Cloud Workstation is intended to run automatically as a service in Windows. While it is possible to start it up as a normal application, Scyld Cloud Workstation must be run as a service in order to support:

- Windows sign out and sign in

- screensavers with passwords

- Windows User Access Control

If Scyld Cloud Workstation is installed on a Windows VM, you may need to install Screen Capture Recorder to enable audio support. Screen Capture Recorder has been tested in Windows 10 and can be downloaded from the URL below:

https://github.com/rdp/screen-capture-recorder-to-video-windows-free/releases/download/0.12.10/Setup.Screen.Capturer.Recorder.v0.12.10.exe

Scyld Cloud Workstation should now be reachable over HTTPS at your server's hostname or IP address. For advanced configuration options, please see *Setup*.

8.7 Updating the Server on Windows

1. Download `Scyld Cloud Workstation-11.3.1.1.msi` from https://updates.penguincomputing.com/scw/download/

2. Double-click on the `Scyld Cloud Workstation-11.3.1.1.msi` installer.

3. Follow the instructions in the GUI. Confirm that you'd like to start Scyld Cloud Workstation as a service to have Scyld Cloud Workstation start automatically.

8.8 Installing the Server on Ubuntu

Follow the steps below to install Scyld Cloud Workstation, 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/scw/download/

   - **Ubuntu 16 and 18:**

     - `scyld-cloud-workstation_11.3.1.1-0ubuntu1.16_amd64.deb`

   - **Ubuntu 20:**

     - `scyld-cloud-workstation_11.3.1.1-0ubuntu1.20_amd64.deb`

2. Use the `apt install` command to install the DEB file (adjust the file path if necessary):

```
% ## Ubuntu 16 and 18
% sudo apt install ./scyld-cloud-workstation_11.3.1.1-0ubuntu1.16_amd64.deb

% ## Ubuntu 20
% sudo apt install ./scyld-cloud-workstation_11.3.1.1-0ubuntu1.20_amd64.deb
```

The installer does the following:

- Installs Scyld Cloud Workstation files to `/opt/scyld-cloud-workstation`

- Installs scyld-cloud-workstation.service to `/lib/systemd/system/`

- Reloads systemd manager configuration using `systemctl daemon-reload`

- Enables the unit file with `systemctl enable scyld-cloud-workstation.service`

3. If your server's domain has a trusted SSL certificate, open the configuration file (`/opt/scyld-cloud-workstation/bin/scyld-cloud-workstation.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 (`scyld-cloud-workstation.lic`), copy it into `/opt/scyld-cloud-workstation/bin`.

- If you have a floating license (`scyld-flexlm.lic`), proceed to *Flexera License Management* for instructions on installing Scyld 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 scyld-cloud-workstation.service
```

Scyld Cloud Workstation should now be reachable over HTTPS at your server's hostname or IP address. For advanced configuration options, please see *Setup*.

8.9 Updating the Server on Ubuntu

1. Download the debian installer for your Ubuntu version from https://updates.penguincomputing.com/scw/download/

- **Ubuntu 16 and 18:**

  - `scyld-cloud-workstation_11.3.1.1-0ubuntu1.16_amd64.deb`

- **Ubuntu 20:**

  - `scyld-cloud-workstation_11.3.1.1-0ubuntu1.20_amd64.deb`

2. Use the `apt install` command to update the DEB file (adjust the file path if necessary):

```
% ## Ubuntu 16 and 18
% sudo apt install ./scyld-cloud-workstation_11.3.1.1-0ubuntu1.16_amd64.deb

% ## Ubuntu 20
% sudo apt install ./scyld-cloud-workstation_11.3.1.1-0ubuntu1.20_amd64.deb
```

The installer does the following:

- Installs Scyld Cloud Workstation files to `/opt/scyld-cloud-workstation`

- Installs scyld-cloud-workstation.service to `/lib/systemd/system/`

- Reloads systemd manager configuration using `systemctl daemon-reload`

- Enables the unit file with `systemctl enable scyld-cloud-workstation.service`

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

```
% sudo systemctl restart scyld-cloud-workstation.service
```

8.10 Installing the Server on MacOS

1. Download the `scyld-cloud-workstation-11.3.1.1.pkg` from https://updates.penguincomputing.com/scw/download/

2. Double-click on `scyld-cloud-workstation-11.3.1.1.pkg` to launch the installer and follow the GUI instructions.

   MacOS Mojave and later: a series of "Security and Privacy" windows will appear for granting permissions to "Microphone" and "Accessibility". MacOS Catalina and later will need to grant permissions to "Screen Recording".

   Perform the following for each "Security and Privacy" window:

   a. Click on the Lock icon to allow changes

   b. Click on the checkbox next to the Scyld Cloud Workstation application

   c. Close the window

3. If your server's domain has a trusted SSL certificate, open the configuration file (`/Applications/scyld-cloud-workstation.app/Contents/Resources/scyld-cloud-workstation.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 (`scyld-cloud-workstation.lic`), copy it into `/Applications/scyld-cloud-workstation.app/Contents/Resources`.

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

   Once the license file has been installed, the server will start automatically and be accessible with a web browser or our native client.

5. Proceed to *Install BlackHole for MacOS Audio* for information on adding audio support (Optional).

Important: Putting your remote MacOS server to sleep (for example: by closing the lid of the laptop, selecting "Sleep" from the Apple menu, or scheduling sleeps through `System Preferences > Energy Saver`) will make Scyld Cloud Workstation inaccessible.

Important: Scyld Cloud Workstation prevents Display Sleep from happening in MacOS using an application called caffeinate. This is to prevent the server from going to sleep.

8.10.1 Install BlackHole for MacOS Audio

To add remote audio capture, perform the following steps on your Scyld Cloud Workstation MacOS server:

1. Download and install `BlackHole 0.2.9` from https://existential.audio/blackhole/.

2. Open the `System Preferences > Sound > Output` window to make `BlackHole 16ch` the Sound Output device.

3. **MacOS Mojave and later:** Add Scyld Cloud Workstation to the `Login Items` list for each MacOS user.

4. Logout of MacOS and log back in.

Start by downloading BlackHole 0.2.9 from https://existential.audio/blackhole/ (note: you may be required to subscribe to their mail list) to your MacOS server. Double-click the installer and follow the GUI instructions.

Next, go to `System Preferences > Sound > Output` and select `BlackHole 16ch` as the Sound Output device.

Note: Selecting `BlackHole 16ch` will disable audio playback on `Internal Speakers`, but this can be changed back when necessary. 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.

MacOS Mojave and later: Add Scyld Cloud Workstation to the `Login Items` list for each user by doing the following:

1. Go to `System Preferences > Users & Groups`.

2. Click on your username in the list of accounts.

3. Select the `Login Items` tab.

4. Click the Lock icon to make changes.

5. Click the + button to open a Finder window.

6. Use the Finder window to go to `Applications` and add `scyld-cloud-workstation`.

7. When you are finished repeating the steps above for each remote user, log out of MacOS and log back in.

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

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

---

8.11 Updating the Server on MacOS

1. Download the `scyld-cloud-workstation-11.3.1.1.pkg` from https://updates.penguincomputing.com/scw/download/

2. Double-click on `scyld-cloud-workstation-11.3.1.1.pkg` to launch the installer and follow the GUI instructions.

Note: If you are updating over an existing Scyld Cloud Workstation installation, your old config file and license files will still be used.

8.12 Installing the Client

You can connect to Scyld Cloud Workstation by installing the native client, Scyld Cloud Workstation Client, or using any of these web browsers:

- Chrome 59+

- FireFox 56+

- Internet Explorer 11+

- Microsoft Edge Legacy 44.17763.1.0+

- Microsoft Edge 79+

- Safari 7+

The native client enables more features and enhanced performance. Native client installation packages for each OS can be downloaded from

- https://updates.penguincomputing.com/scw/download/

Note: Chrome provides the best performance of all the web browsers.

FLEXERA LICENSE MANAGEMENT

As of version 5.0.0, Scyld Cloud Workstation 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.

9.1 Obtaining a License

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

9.2 Installing a Trial License

Trial licenses are named `scyld-cloud-workstation.lic` and must be copied to the Scyld Cloud Workstation host at `/opt/scyld-cloud-workstation/bin` for Linux hosts or `C:\Program Files\Penguin Computing\Scyld Cloud Workstation` for Windows hosts.

9.3 Installing a Floating or Node-Locked License

Follow these steps on the Scyld FlexLM host:

1. Install the Scyld FlexLM license server package (distributed by Penguin Computing) on a host that has network access to all Scyld Cloud Workstation hosts.

2. Copy the license file (`scyld-flexlm.lic`) to `/opt/scyld-flexlm/bin` for Linux hosts or `C:\ Program Files\Penguin Computing\Scyld FlexLM` for Windows hosts.

3. For Linux users only, change the owner of the file to scyld-flexlm using the chown command and make sure the owner has read permission:

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

4. In `scyld-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 Scyld FlexLM service.

Follow these steps on each Scyld Cloud Workstation host:

1. Open the configuration file located at `/opt/scyld-cloud-workstation/bin/scyld-cloud-workstation.xml` for Linux and `C:\Program Files\Penguin Computing\Scyld Cloud Workstation\scyld-cloud-workstation.xml` for Windows.

2. Find the `Server.LicenseFile` 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.LicenseFile` to the port and host of the license server using the `port@host` syntax (or just `@host` if the Scyld FlexLM server is using the default port (`27002`).

   For example, if Scyld 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 `scyld-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 Scyld Cloud Workstation 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.LicenseFile configuration setting

4. Flexera cache

9.4 Testing your Floating / Node-Locked License Install

To test if the Scyld Cloud Workstation host can checkout licenses from the Scyld FlexLM host, sign into the Scyld Cloud Workstation host and use the `lmutil` tool:

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

For example, if your Scyld 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
-----------------------------------------------------
"scw" v1.000, vendor: PENGUIN, expiry: 01-aug-2017
  License server: 192.168.1.7
  nodelocked license locked to NOTHING (hostid=ANY)  starts: 1-jan-1990,   expires:␣
→01-aug-2017

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 Computing at support@penguincomputing.com.

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

Chapter 9. Flexera License Management

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 `scyld-cloud-workstation.xml` config file. In Linux this can be found at `/opt/scyld-cloud-workstation/bin/scyld-cloud-workstation.xml` and in Windows this can be found at `C:\Program Files\Penguin Computing\Scyld Cloud Workstation\scyld-cloud-workstation.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.LogLevel` 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:** Scyld Cloud Workstation includes a default private key, certificate file, username, and password that are not secure and should be changed.

10.1 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 CentOS and Ubuntu you can restart the service using the `systemctl restart` command:

```
systemctl restart scyld-cloud-workstation.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 `scyld-cloud-workstation` in the 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/scyld-cloud-workstation.app/Contents/MacOS

# Restart the service
sudo ./scyld-cloud-workstation --service restart
```

The Scyld Cloud Workstation sign-in page should return after a few seconds.

10.2 Config File Settings

> **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.

10.2.1 License Management

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

10.2.2 Server Authentication

User's 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 Scyld Cloud Workstation. Each system is independent and can be enabled in parallel.

- Config File Authentication
- ScyldCloudAuth Authentication
- OS Credential Authentication

Config File Authentication

Config File Authentication uses credentials stored in the config file. The following settings control Config File Authentication:

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

The ShadowPassword is set by calling `scyld-cloud-workstation.sh --passwd` in Linux with sudo privileges, `scyld-cloud-workstation.exe /passwd` in Windows as an Administrator, or `sudo scyld-cloud-workstation --passwd`.

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

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*.

OS Credential Authentication

The credentials accepted by your remote Linux, Windows, or MacOS host can be used to sign into Scyld Cloud Workstation. This supports ActiveDirectory for Windows, and LDAP / PAM for Linux.

Important: While config file or ScyldCloudAuth usernames can be used to sign in to Scyld Cloud Workstation 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.

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

10.2.3 External Sign-In Pages

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

10.2.4 Server 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*.

10.2.5 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 (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.

10.2.6 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.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:

```
# CentOS
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).

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.

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.

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.

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.

10.3 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.

10.3.1 Server.LogLevel

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'.

10.3.2 Server.LogFormat

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)
%a	date/time am/pm
%A	date/time AM/PM

Table 1 – continued from previous page

Pattern	Description
%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

10.3.3 Server.LogFile

A path to the log file of the Scyld Cloud Workstation server. By default this can be found in the directory of the Scyld Cloud Workstation executable and is named `scyld-cloud-workstation.log`. For more information on log output, see *Log Output*.

Changed in v5.0.0. Default value changed.

10.3.4 Server.BootLogFile

Windows only. A path to the log file of the Scyld Cloud Workstation meta-server. By default this can be found in the directory of the Scyld Cloud Workstation executable and is named `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

10.3.5 Server.LocalCursor

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.

10.3.6 Server.AutoLock

Determines if Scyld Cloud Workstation calls on the OS to lock the desktop upon disconnecting from the web page. Experimental. Defaults to `false`.

> **Warning:** NOTE: 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.

Updated in v5.0.0.

10.3.7 Server.IdleUserTimeout

The length of time (in minutes) that users must be inactive before all users are disconnected. This feature is disabled if value is `0.0` or less. Defaults to `120`.

Added in v5.0.0.

10.3.8 Server.Port

The port number used by the server. Defaults to `443` if *Server.Secure* is `true` or `80` if *Server.Secure* is `false`.

10.3.9 Server.Secure

Determines if the server operates over HTTPS (recommended). Defaults to `true`.

10.3.10 Server.LicenseFile

Specifies a license file path or a `port@host` address where a Scyld FlexLM license server is hosted. If the default license server port is being used (`27002`), then `@host` is also acceptable. Defaults to `scyld-cloud-workstation.lic`.

For more information on installing license files, see *Flexera License Management*

Added in v5.0.0.

10.3.11 Server.StartDelay

Specifies a sleep time to delay the start-up of Scyld Cloud Workstation in seconds. Defaults to 0.

Added in v5.0.0.

10.3.12 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.

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

10.3.13 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.

10.3.14 Server.Auth.Username

Declares a username to be used in combination with the password defined by Server.Auth.ShadowPassword at the Scyld Cloud Workstation sign in page.

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

10.3.15 Server.Auth.ShadowPassword

A shadowed password used to sign in to the Scyld Cloud Workstation 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, please change your password immediately using our password update utility:

- Linux: `sudo scyld-cloud-workstation.sh --passwd`
- Windows: `scyld-cloud-workstation.exe /passwd`
- MacOS: `sudo scyld-cloud-workstation --passwd`

Note: Changing this value takes effect without a service restart.

Changed in v11.1.0.

10.3.16 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*. This defaults to 6.

Note: Changing this value takes effect without a service restart.

Changed in v11.1.0.

10.3.17 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.

10.3.18 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.

10.3.19 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.

10.3.20 Server.Auth.ScyldCloudAuth.Allow

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

Note: Changing this value takes effect without a service restart.

Changed in v11.0.0.

10.3.21 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.

Usernames elements can use asterisk wildcard characters (i.e. `*@penguincomputing.com` will enable all usernames that end in `@penguincomputing.com`).

Note: Changing this value takes effect without a service restart.

Changed in v11.0.0.

10.3.22 Server.Auth.ScyldCloudAuth.ApiKey

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

Added in v9.1.

10.3.23 Server.Auth.ScyldCloudAuth.ApiSecret

A string that represents a shared secret between Scyld Cloud Workstation and the Scyld Cloud Auth server. This is required to make priviledged Scyld Cloud Auth web service calls.

Added in v9.1.

10.3.24 Server.Auth.Session.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.

10.3.25 Server.Auth.OSAuthEnabled

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 Scyld Cloud Workstation 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.

10.3.26 Server.Auth.Session.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.

10.3.27 Server.Auth.PAM.Service

The name of the PAM (Pluggable Authentication Module) service. Defaults to `login`.

Added in v8.0.0.

10.3.28 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.

10.3.29 Server.Broker.ShadowPassword

A shadowed password used to sign in to the Scyld Cloud Workstation 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, please change your password immediately using our password update utility:
>
> - Linux: `sudo scyld-cloud-workstation.sh --passwd`
> - Windows: `scyld-cloud-workstation.exe /passwd`
> - MacOS: `sudo scyld-cloud-workstation --passwd`

Note: Changing this value takes effect without a service restart.

Changed in v11.1.0.

10.3.30 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 can not be streamed.

Added in v10.0.0.

10.3.31 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.

10.3.32 Server.Audio.Output.SampleRate

Determines the audio sample rate in Hz. Higher sample rates lead to better audio quality, but consumes 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.

10.3.33 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.

10.3.34 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.

10.3.35 Server.VideoSource

The video capture mechanism. Currently supports `nvfbc`, `stream`, and `auto`. The default is `auto`.

Set to `auto` if you'd like the system to use `nvfbc` when the service detects an NVIDIA GRID compatible card and `stream` in all other cases.

Set to `nvfbc` only if you have an NVIDIA GRID SDK compatible graphics card and driver.

Set to `stream` to use our CPU-based encoding solution.

Changed in v5.0.0.

10.3.36 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 can not process them fast enough.

A value of `-1` disables this threshold.

Defaults to `2560`.

Updated in v5.0.0. Changed default.

10.3.37 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 can not process them fast enough.

A value of `-1` disables this threshold.

Defaults to `1440`.

Updated in v5.0.0. Changed default.

10.3.38 Server.Video.StartFrameRate

Initial frame rate. Measured in frames per second. Defaults to `24`.

Added in v2.2.0.

10.3.39 Server.Video.MinFrameRate

The lowest valid frame rate for a connection. Measured in frames per second. Defaults to `2`.

Added in v2.2.0.

10.3.40 Server.Video.AvgBitRate

This setting can be 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, please see: *Configure Video Bit-Rate*

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

Updated in v9.1.9. Increased defaults.

10.3.41 Server.Video.MaxFrameRate

The highest allowable frame rate for a connection. Measured in frames per second. Defaults to `30`.

10.3.42 Server.MultiUser.MaxClientCount

The maximum number of clients that can be connected at a time. Defaults to `6`.

Added in v3.0.0.

10.3.43 Server.QoS.Enabled

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

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

Defaults to `true`.

10.3.44 openSSL

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

10.3.45 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.

10.3.46 openSSL.server.certificateFile

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

10.3.47 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.

10.3.48 openSSL.server.loadDefaultCAFile

Boolean value. Specifies wheter the builtin CA certificates from OpenSSL are used. Defaults to `true`.

10.3.49 openSSL.server.cipherList

Specifies the supported ciphers in OpenSSL notation.

Changed in v3.0.0. Default value changed.

10.3.50 openSSL.server.privateKeyPassphraseHandler.name

Defaults to `KeyFileHandler`. 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.

Added in v2.2.0. Default value changed.

10.3.51 openSSL.server.privateKeyPassphraseHandler.options.password

The private key passphrase (ignored if there is no passphrase for the private key).

10.3.52 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.

10.3.53 openSSL.server.cacheSessions

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

10.3.54 openSSL.server.extendedVerification

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

10.3.55 openSSL.server.requireTLSv1_2

Require a TLSv1.2 connection. Defaults to `true`.

Added in v2.2.0. Default value changed.

10.3.56 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.

10.3.57 openSSL.fips

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

10.4 Client Settings

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

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

USAGE

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

11.1 Using the Linux Service

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

```
service scyld-cloud-workstation start
service scyld-cloud-workstation stop
service scyld-cloud-workstation restart
```

To run scyld-cloud-workstation directly rather than as a service (this is usually only useful for debugging purposes), use the scyld-cloud-workstation.sh start-up script. Usage information can be obtained by passing the `--help` flag.

```
usage: scyld-cloud-workstation OPTIONS
scyld-cloud-workstation -- a GPU accelerated remote desktop web service.

--daemon                                 Run application as a daemon.
--pidfile=path                           Write the process ID of the
                                         application to given file.
-h, --help                               display help information on command
                                         line arguments
-vsvideosource, --videosource=videosource  choose videosource (nvfbc, stream)
-q, --quiet                              hide the console when running
-pwd, --passwd                           update the password
```

11.2 Using the Windows Service

To use the scyld-cloud-workstation service, we must verify that the service is registered with the OS and then start the service.

11.2.1 Open a Command Prompt as an Administrator

1. Sign in as a user that is an Administrator.

2. Click on 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`.

11.2.2 Register the Windows Service

To register the windows service, use the `scyld-cloud-workstation.exe` command:

```
scyld-cloud-workstation.exe /registerService /startup=automatic
```

The scyld-cloud-workstation service will now automatically start on reboot.

Note: Service registration should already be handled by the installer. If you the message below, verify that scyld-cloud-workstation has been properly installed. This is usually a sign that the PATH environment variables are not pointing at the scyld-cloud-workstation.exe.

```
'scyld-cloud-workstation.exe' is not recognized as an internal or
 external command, operable program or batch file.
```

11.2.3 Start and Stop the Windows Service

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

```
net start scyld-cloud-workstation
net stop scyld-cloud-workstation
```

11.3 Using the MacOS Service

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

```
# Change to the application directory
cd /Applications/scyld-cloud-workstation.app/Contents/MacOS

# Start the service
sudo ./scyld-cloud-workstation --service start

# Stop the service
sudo ./scyld-cloud-workstation --service stop

# Restart the service
sudo ./scyld-cloud-workstation --service restart

# Check the status of the service
sudo ./scyld-cloud-workstation --service status
```

11.4 Manually running the MacOS audio server (advanced)

The Scyld Cloud Workstation 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/scyld-cloud-workstation.app/Contents/MacOS

# Start the audio server
./scyld-cloud-workstation --audio-server
```

11.5 Creating Config File credentials

OPTIONAL. In addition to OS credentials, you can setup a username and hashed password in the config file to sign in to Scyld Cloud Workstation. These Config File cedentials can sign into Scyld Cloud Workstation at any time. This differs from OS credentials, which can only sign into Scyld Cloud Workstation 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.

To set the password, verify that the `Server.Auth.Username` and `Server.Auth.ShadowPassword` tags exist **and are uncommented** in the config file (i.e., 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 Scyld Cloud Workstation binary, and running scyld-cloud-workstation with an OS-specific `passwd` flag:

```
# Linux:
sudo scyld-cloud-workstation.sh --passwd

# Windows (as an Administrator):
scyld-cloud-workstation.exe /passwd

# MacOS:
sudo scyld-cloud-workstation --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.

11.6 Log Output

Log output is organized by priority levels (from highest to lowest: Fatal, Critical, Error, Warning, Notice, Information, Debug, and Trace). scyld-cloud-workstation by default 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 scyld-cloud-workstation.xml config file and set `LogLevel` to `debug`.

The most useful log files for Scyld Cloud Workstation can be found at these locations:

```
# Linux:
/opt/scyld-cloud-workstation/bin/scyld-cloud-workstation.log.

# Windows:
C:\Program Files\Penguin Computing\Scyld Cloud Workstation\log\scyld-cloud-
↪workstation.log
C:\Program Files\Penguin Computing\Scyld Cloud Workstation\log\service.log.

# MacOS:
/var/log/com.penguincomputing.scyld-cloud-workstation/scyld-cloud-workstation.log
```

Note: You can change the path of the output by opening the `scyld-cloud-workstation.xml` config file and setting `Server.LogFile` to a new destination.

By default, Scyld Cloud Workstation displays a timestamp with each log message. To change the timestamp to all of your output, open the `scyld-cloud-workstation.xml` and set `LogFormat`. For more information, see: *Server.LogFormat*.

11.7 Selecting a Video Source

Scyld Cloud Workstation currently supports two video sources:`nvfbc` and `stream`.

For most users an appropriate default video source will be automatically detected based on the system's configuration. Hosts that have an NVIDIA GRID card with a compatible NVIDIA GRID driver installed default to `nvfbc`. All other systems will default to `stream`.

To override the video source, specify `--videosource=<nvfbc|stream>` or change `Server.VideoSource` in the config file.

11.8 Sign In

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

This will take you to the Scyld Cloud Workstation sign in page. Submit the username and password encrypted in the config file or by ScyldCloudAuth to sign in.

As a third option, you can use your OS specific credentials to sign in.

Important: While config file or ScyldCloudAuth usernames can be used to sign in to Scyld Cloud Workstation 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.

After signing in you will see a gray canvas that will turn into a remote visualization display within a few seconds. At this point you can interact with the remote operating system. Other users will be prevented from signing into the web service until you sign out.

11.9 Main Toolbar

The main toolbar gives access to additional Scyld Cloud Workstation 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.

11.10 Toggle Audio

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

Note: Puleaudio version 10.0+ is required for Linux users.

11.11 Keyboard Menu

The Keyboard Menu contains a list of special keyboard button presses to transmit to the remote system, such as `Ctrl+Alt+Del` or `Print Screen`.

11.12 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.

Note: USB forwarded devices will disconnect every time a user:

- disconnects from Scyld Cloud Workstation
- signs in or signs out of the remote OS

- adds or removes a monitor on the remote server

- loses controller status (i.e., gives up remote keyboard control)

Warning: CentOS 7 doesn't always properly load the default USB kernel modules for forwarded Wacom tablets. As a workaround, reload all wacom related modules using the following commands:

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

11.13 Settings Menu

The Settings Menu provides options for toggling the fullscreen state and selecting between three video quality settings (native client users only). If video is being downscaled it will also provide a status message.

Higher quality settings will 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.

11.14 User Tools Menu

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

11.15 Paste Text from the Local Clipboard

Text can be pasted from the local client into the remote desktop.

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

To paste text from a local MacOS clipboard to the 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.

Note: Only characters that are supported by both the client and server can be pasted.

11.16 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.**

In Linux, if you are using a first generation NVIDIA GRID card (i.e., K1, K2) in a headless configuration (i.e. you are using the `UseDisplayDevice none` option in your `/etc/X11/xorg.conf` file), you will have to open a command prompt and use the `xrandr --fb <width>x<height>` command. For example, if you'd like to change the screen resolution to 1920x1080, you would enter: `xrandr --fb 1920x1080`.

Otherwise 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'.

11.17 Downscale Screen Resolution

System administrators have the ability to restrict the maximum screen resolution in the config file at `scyld-cloud-workstation.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.

11.18 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.

The following steps enable 4K support:

1. Open the xml config file.

2. Add the `Server.Video.MaxWidth` and `Server.Video.MaxHeight` tags with the value set to `-1` to disable the resolution cap.

3. Save the config file and restart the service.

Note: NVIDIA GRID products (such as a Tesla M60) require an NVIDIA Quadro Virtual Datacenter Workstation license to use 4K resolutions. Contact NVIDIA for more information.

11.19 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.

11.20 Sign Out

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

Closing your browser or signing out of the Scyld Cloud Workstation 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.

COLLABORATION

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

Hosts are 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 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.

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.

12.1 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.MultiUser.MaxClientCount` setting in the config file at `scyld-cloud-workstation.xml`.

12.2 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 attempts 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 kick individual Guests or give keyboard and mouse control.

12.3 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.

12.4 Add New Guests

Hosts can invite a group of guests by creating an Invite Link. Click on the 'Add Guests' button.

In the form that appears, specify how many guest sign ins you'd like this link to be good for. It is best practice to select the minimum number you will need.

The next form will show the generated Invite Link. Copy and send this link to Guest users and then close the form.

> **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 will appear to all Hosts asking whehter 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 becomes 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 again for use.

12.5 Pause Guest Video

Guest video can be toggled by clicking on the 'Pause Guests' button.

12.6 Ban Guests and Revoke Invites

Guests can be banned for the session either individually or all at the same time using the 'Ban Guests' button. Hosts can not be banned.

12.7 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 banning or giving keyboard / mouse control.

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

12.8 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.

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.

13.1 Network Quality

Network quality can be measured as a combination of latency, throughput, and stability. When determining network quality you may want to run Scyld Cloud Workstation 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, Scyld Cloud Workstation 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 Scyld Cloud Workstation since it's common for clients and servers to have more than 4 Mbps of bandwidth, but it is still worth remembering.

13.2 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 Scyld Cloud Workstation 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 Scyld Cloud Workstation, 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.

13.3 Server Load

Server load is typically not a large bottleneck since Scyld Cloud Workstation does not consume much server-side CPU time. GPU consumption does increase, but for NVIDIA GRID cards the display capture and encoding is done on a part of the GPU that is independent of computation.

13.4 Further Help

If you have additional questions about perormance, please contact Penguin Computing at support@penguincomputing.com.

FREQUENTLY ASKED QUESTIONS / TROUBLESHOOTING

14.1 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.

14.2 Why is USB Forwarding disabled after updating MacOS Big Sur (or earlier) to MacOS Monterey (or later)?

When Scyld Cloud Workstation 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 'VirtualHereUniversal' to re-enable USB Forwarding.

Please see: *Re-Enabling USB Forwarding after Updating to MacOS Monterey* for installation instructions.

14.3 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.

14.4 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 Scyld Cloud Workstation 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!

14.4.1 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.

14.4.2 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.

14.4.3 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.

14.5 Why does my MacOS display not go to sleep?

Scyld Cloud Workstation 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 Scyld Cloud Workstation inaccessible.

14.6 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 CentOS 7 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.

14.7 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 Scyld Cloud Workstation is running.

14.8 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.

14.9 My desktop is flickering between a dark gray screen and my desktop!

This is a known issue with older versions of Firefox (such as 52.4.0) and has been observed in CentOS 7. Please update to 60.8 or whatever the latest available version of Firefox.

14.10 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.

14.11 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.

14.12 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.

14.13 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 dropwdown. Then close and restart Chrome.

14.14 How many users can sign in at a time?

Scyld Cloud Workstation 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.MultiUser.MaxClientCount* option.

14.15 Can LDAP credentials be used at the sign in page?

Yes. There are two ways to support this.

Traditionally support for LDAP currently comes as part of the Scyld-Cloud-Manager package. Scyld Cloud Workstation can be configured to authenticate through Scyld-Cloud-Auth, which can talk to LDAP. To connect to a Scyld-Cloud-Auth service, open the config file, set *Server.Auth.ScyldCloudAuth.URL*, and add one or more Username elements to the *Server.Auth.ScyldCloudAuth.Allow*.

As of v6.1.0, Scyld Cloud Workstation passes credentials directly to the remote operating system. This feature is enabled by default, but it can be disabled by setting *Server.Auth.OSAuthEnabled* to `false`.

14.16 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 Scyld Cloud Workstation 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 CentOS 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` in CentOS.

If you are a Windows user and you are using the NvFBC videosource, verify that NvFBC is enabled by running `NvFBCEnable.exe -checkstatus` as an Administrator. If it is disabled, you can enable it with the `NvFBCEnable.exe -enable` command.

14.17 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.

14.18 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, Scyld Cloud Workstation Client. Chrome users can try another workaround, described below.

By default, Google Chrome (aka Chromium) intercepts certain specific keyboard combinations before Scyld Cloud Workstation 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 Scyld Cloud Workstation. If this is something you will do often, we recommend creating a shortcut with a flag to your Scyld Cloud Workstation 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 Scyld Cloud Workstation interface.

14.19 What ports do I need to open?

By default, Scyld Cloud Workstation must be able to accept incoming requests over HTTPS port 443 (or port 80 if you are using HTTP).

14.20 Can I run my applications?

Scyld Cloud Workstation 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 Scyld Cloud Workstation.

14.21 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.

14.22 Is there audio support?

Yes. As of v10.0 we support dual channel audio.

14.23 Can I cut, copy, and paste?

You can copy text from the local desktop to the remote desktop. See *Paste Text from the Local Clipboard* for more information.

14.24 What graphics cards do you support?

See *Server Hardware*.

14.25 How many NVIDIA GRID GPUs do I need?

As of v5.0, NVIDIA GRID GPUs are no longer required to run Scyld Cloud Workstation.

14.26 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
```

(continues on next page)

```
    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
```

END USER LICENSE AGREEMENT

```
Penguin Computing Inc.
45800 Northport Loop West, Fremont, CA 94538
Tel: 415-954-2800 - Fax: 415-954-2899
www.penguincomputing.com


Penguin Computing Software End User License Agreement


Last revised: 1/4/2012


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
("Penguin"). This Agreement governs your use of the Scyld 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 SCYLD 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 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) "Scyld Unpublished
Software" which is owned by Penguin and/or its licensors and licensed
under the terms of this Agreement (b) "Scyld 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-sub licensable right and license to (a)
reproduce (solely to download and install), perform, and execute the
Scyld 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
Scyld 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 Scyld Unpublished Software or Documentation, with or
without consideration (b) permit any third party to access or use the
Scyld Unpublished Software or Documentation (c) permit any third
party to benefit from the use or functionality of the Scyld
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
Scyld Unpublished Software (f) modify or create derivative works
based upon the Scyld Unpublished Software or Documentation, in whole
or in part (g) reproduce the Scyld 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
Scyld Unpublished Software or Documentation (i) use the Scyld
Unpublished Software for any purpose other than expressly permitted in
Section 2.1 above or (j) use the Scyld 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 Scyld Published
Software are not subject to the terms and conditions of Sections 2.1,
2.2, or 6. Instead, each item of Open Source Software and Scyld
Published Software is licensed under the terms of the end-user license
that accompanies such Open Source Software and Scyld 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 Scyld 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 Scyld 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 Scyld Published Software that is subject to the terms of
the GPL and LGPL. For the Open Source Software and Scyld 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 Scyld 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 Scyld Unpublished
Software, Scyld Published Software, and Documentation, and any full or
partial copies thereof, including any additions or modifications to
the Scyld 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
"Scyld, "Scyld Beowulf", "Scyld ClusterWare" and "Scyld Computing"
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 CLAIM.  END USER
ACKNOWLEDGES THAT THE AGREEMENT REFLECTS AN ADEQUATE AND ACCEPTABLE
ALLOCATION OF RISK.

6. Confidential Information. Scyld Unpublished Software and the
structure, organization, and code of the Scyld Unpublished Software,
including but not limited to the shell scripts of the Scyld
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 Scyld Unpublished Software
from End User's computers, ceasing all use thereof, and destroying all
copies of the Scyld 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
Scyld 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 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., 501 2nd Street, Suite 310, San Francisco, CA 94107.
```

THIRDPARTY LICENSE AGREEMENTS

```
Third Party Open Source License Terms Guide


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.

    Redistribution and use in source and binary forms, with or without
    modification, are permitted provided that the following conditions
    are met:
```

(continues on next page)

```
    *  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
 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
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.

    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 OpenSSL


   LICENSE ISSUES
   ==============

   The OpenSSL toolkit stays under a double license, i.e. both the
   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
    * 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
     * 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

6. 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,
    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.

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
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
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
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

7. 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
    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

8. 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
    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.

9. 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.

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
    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
```

SEVENTEEN

INDICES AND TABLES

- genindex
- search