Scyld Cloud Workstation Documentation

Release 5.0.6

Penguin Computing

Jun 06, 2017

CONTENTS

1 About Scyld Cloud Workstation **3**

2 Introduction **5**

3 Release Notes **7**
- 3.1 v5.0.6 . . . 7
- 3.2 v5.0.5 . . . 7
- 3.3 v5.0.4 . . . 7
- 3.4 v5.0.3 . . . 7
- 3.5 v5.0.2 . . . 7
- 3.6 v5.0.1 . . . 8
- 3.7 v5.0.0 . . . 8
- 3.8 v3.1.0 . . . 8
- 3.9 v3.0.4 . . . 9
- 3.10 v3.0.3 . . . 9
- 3.11 v3.0.2 . . . 9
- 3.12 v3.0.1 . . . 9
- 3.13 v3.0.0 . . . 9
- 3.14 v2.3.2 . . . 9
- 3.15 v2.3.1 . . . 9
- 3.16 v2.3.0 . . . 10
- 3.17 v2.2.0 . . . 10
- 3.18 v2.1.0 . . . 10

4 Server Requirements **11**
- 4.1 Server OS . . . 11
- 4.2 Server Hardware . . . 11
- 4.3 Server NVIDIA Drivers . . . 11
- 4.4 Server Screen Resolutions . . . 12
- 4.5 OpenSSL . . . 12
- 4.6 SSL Certificate . . . 12

5 Client Requirements **13**
- 5.1 Client Hardware and Network . . . 13
- 5.2 Client Web Browsers . . . 13

6 Installation **15**
- 6.1 Required Files . . . 15
- 6.2 CentOS 6 (RPM): Fresh Install . . . 15
- 6.3 CentOS 6 (RPM): Updating an Existing Install . . . 16
- 6.4 Windows 7: Fresh Install . . . 16

6.5 Windows 7: Updating an Existing Install . . . 17
6.6 Client Installation . . . 17

7 Flexera License Management **19**
7.1 Supported License Types . . . 19
7.2 Obtaining a License . . . 19
7.3 Installing a Node-Locked License . . . 19
7.4 Installing a Floating License . . . 20
7.5 Testing your Floating License Install . . . 21

8 Setup **23**
8.1 Applying Config File Changes . . . 23
8.2 Config File Settings . . . 24
8.3 Settings Glossary . . . 27
8.4 Client Settings . . . 34

9 Usage **35**
9.1 Using the Linux Service . . . 35
9.2 Using the Windows Service . . . 35
9.3 Change the Config File Password . . . 36
9.4 Log Output . . . 36
9.5 Selecting a Video Source . . . 37
9.6 Sign In . . . 37
9.7 User Controls . . . 37
9.8 Paste Text from the Local Clipboard . . . 38
9.9 Change Screen Resolution . . . 38
9.10 Downscale Screen Resolution . . . 38
9.11 Sign Out . . . 38

10 Collaboration **39**
10.1 Set the maximum number of concurrent clients . . . 39
10.2 Collaboration Quick Start . . . 39
10.3 Control Buttons . . . 39
10.4 Add New Guests . . . 40
10.5 Pause Guest Video . . . 40
10.6 Ban Guests and Revoke Invites . . . 40
10.7 User Buttons . . . 40
10.8 Give Keyboard and Mouse Control . . . 40

11 Performance **41**
11.1 Network Quality . . . 41
11.2 Client Load . . . 41
11.3 Server Load . . . 41
11.4 Further Help . . . 42

12 Frequently Asked Questions **43**
12.1 How many users can sign in at a time? . . . 43
12.2 What screen resolutions are supported? . . . 43
12.3 Can the sign in page connect to LDAP? . . . 43
12.4 I'm only seeing a gray rectangle. . . . 43
12.5 How do I press Ctrl+Alt+Del? . . . 43
12.6 How do I press Ctrl+N, Ctrl+T, Ctrl+W, Ctrl+Tab, Ctrl+Page Up, or Ctrl+Page Down? . . . 44
12.7 What ports do I need to open? . . . 44
12.8 Can I run my applications? . . . 44
12.9 Will it run on my iPad / mobile device? . . . 44

12.10 Is there audio support? . . . 44
12.11 Can I cut, copy, and paste? . . . 44
12.12 What graphics cards do you support? . . . 45
12.13 How many NVIDIA GRID GPUs do I need? . . . 45

13 Indices and tables **47**

Index **49**

Contents:

CHAPTER

ONE

ABOUT SCYLD CLOUD WORKSTATION

Scyld Cloud Workstation 5.0.6, commit 0f005f56d150d382736199b366fd0bd9be994691.

CHAPTER

TWO

INTRODUCTION

Scyld Cloud Workstation is a web server that provides secure, easy remote access to teams working on Windows and Linux 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.

CHAPTER

THREE

RELEASE NOTES

Attention: We recommend moving changes from your old config file to the latest config file.

3.1 v5.0.6

- Fixed “too many files open” error for generic stream video source
- Improved error handling for disconnects during inactivity
- Changed default idle user timeout to 2 hours

3.2 v5.0.5

- Fixed black winlogon screen for stream video source

3.3 v5.0.4

- Fixed screen size changing in Windows

3.4 v5.0.3

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

3.5 v5.0.2

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

3.6 v5.0.1

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

3.7 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 **boot.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

3.8 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

3.9 v3.0.4

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

3.10 v3.0.3

- Fixed QoS adaptive frame rate algorithm

3.11 v3.0.2

- Fixed IE11 fullscreen keyboard and scrollbars

3.12 v3.0.1

- Fixed unexpected multi-user client timeouts

3.13 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

3.14 v2.3.2

- Updated default SSL ciphers

3.15 v2.3.1

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

3.16 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

3.17 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

3.18 v2.1.0

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

CHAPTER

FOUR

SERVER REQUIREMENTS

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

4.1 Server OS

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

- Windows 7, 8
- CentOS 6, 7

Beta support is available for:

- Ubuntu 12, 14, 16

Attention: There is a known graphics issue with GNOME Shell based systems (GNOME 3 and GDM) on machines that do not have an attached monitor. For these systems, MATE desktop environment and LightDM can be used as a workaround.

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

4.2 Server Hardware

Scyld Cloud Workstation is supported on the following server hardware configurations:

Server-Side	Recommended	Minimum
CPU	> Intel Core i5, Dual-Core	> Intel Core i3, Dual-Core
Memory	> 2 GB	> 2 GB
GPU	NVIDIA GRID K1, K2, M60	NVIDIA GRID K1, K2, M60

4.3 Server NVIDIA Drivers

Scyld Cloud Workstation runs on NVIDIA GRID GPUs such as the NVIDIA GRID K2 and Tesla M60. Drivers that support the NVIDIA GRID SDK are required. The following combinations have been successfully tested with version 5.0.6:

OS	NVIDIA Driver Release
Windows 7	347.88 354.99 369.49
CentOS 6	354.41 361.42

Warning: The following issues are known for NVIDIA device drivers in Linux:

- 331.62: the remote mouse cursor is not hidden when the local mouse cursor is active.
- 340.46: changing the screen resolution via the xrandr command halts video stream.
- 367.35, 367.57: changing the screen resolution via the xrandr command halts video stream.

4.4 Server Screen Resolutions

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

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

For most users, we recommend a resolution of 1600x900. 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*.

4.5 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 this should be downloaded and installed manually in Windows before you can install Scyld Cloud Workstation.

For Windows hosts, download the latest Win64 OpenSSL package (either full or light versions will work) from Shining Light Productions: https://slproweb.com/products/Win32OpenSSL.html

4.6 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*.

CHAPTER

FIVE

CLIENT REQUIREMENTS

This section describes the hardware and software requirements for the connecting client.

5.1 Client Hardware and Network

We recommend using clients with the following minimum specs.

Client-Side	Recommended
CPU	> Intel Core i5, Dual-Core
Memory	> 2 GB
Network Bandwidth	> 5.5 Mbps
Network Latency	< 80 ms

Note: Acceptable network latency is application dependent. For certain applications, users may find 150 ms to be acceptable. Performance may degrade if the client is running background applications that consume significant amounts of CPU time, memory, or network bandwidth.

5.2 Client Web Browsers

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

- Chrome 30+
- FireFox 27-37, 39+
- Internet Explorer 11+
- Safari 7+

Note: Chrome 30+ provides the best performance and is recommended.

These browsers by default enable TLS 1.2, WebGL and WebSocket features that are necessary for security and optimal 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.

CHAPTER

SIX

INSTALLATION

The Scyld Cloud Workstation server can be installed as a Windows 7 or CentOS 6 service.

6.1 Required Files

Installation of Scyld Cloud Workstation requires the following files:

- The Scyld Cloud Workstation installation package for your operating system:
  - CentOS 6 and 7: `scyld-cloud-workstation-5.0.6-1.x86_64.rpm`
  - Windows 7: `Scyld Cloud Workstation-5.0.6-1-setup.exe`
- The Scyld Cloud Workstation license file

If you wish to use a license server to centralize management of system licenses you will also require the following files:

- The Flexera license manager daemon, (optional):
  - CentOS 6 and 7: `lmgrd`, `lmadmin`, and `PENGUIN`
  - Windows 7: `lmgrd.exe`, `lmadmin.exe`, and `PENGUIN.exe`

6.2 CentOS 6 (RPM): Fresh Install

Download and install the latest NVIDIA GRID drivers for your OS: http://www.nvidia.com/download/index.aspx

Use the `rpm` command to install the Scyld Cloud Workstation RPM.

Important: Scyld Cloud Workstation includes a default private key, certificate file, username, and password that are not secure and should be changed. See *Setup* for more information once installation is complete.

The installer performs the following actions:

- Scyld Cloud Workstation files are installed to `/opt/scyld-cloud-workstation`.
- scyld-cloud-workstation.init is installed to `/etc/init.d` and has its security context changed to `system_u:object_r:bin_t:s0`.
- A line of code is added to `/etc/gdm/Init/Default` that allows scyld-cloud-workstation to restart when the service is enabled by chkconfig and gdm restarts. To prevent scyld-cloud-workstation from starting when gdm starts, use the chkconfig command: `chkconfig --del scyld-cloud-workstation`.

The name of the RPM may be different depending on the version of Scyld Cloud Workstation.

Use the `rpm -ivh` command:

```
% sudo rpm -ivh scyld-cloud-workstation-5.0.6-1.x86_64.rpm
```

Follow the quickstart instructions that appear on the terminal and then proceed to: *Flexera License Management*.

6.3 CentOS 6 (RPM): Updating an Existing Install

If you are performing an update, use the `rpm -Uvh` command:

```
% sudo rpm -Uvh scyld-cloud-workstation-5.0.6-1.x86_64.rpm
```

The new RPM may include new settings that are not present in your existing XML config file. You must merge the settings found in `scyld-cloud-workstation.xml.rpmnew` into your existing `scyld-cloud-workstation.xml` file.

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

Important: If you are updating over an existing Scyld Cloud Workstation installation, your old config file will be preserved. The new package may include an XML config file with newer / updated settings. Merge the new settings found in `scyld-cloud-workstation.xml.rpmnew` with the existing `scyld-cloud-workstation.xml` file.

Once this update is successful, proceed to: *Flexera License Management*.

6.4 Windows 7: Fresh Install

Download and install the following:

- the latest Win64 OpenSSL package (either full or light versions will work) from Shining Light Productions: https://slproweb.com/products/Win32OpenSSL.html
- the latest NVIDIA GRID driver for your OS from: http://www.nvidia.com/download/index.aspx

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.

Double-click on the Scyld Cloud Workstation-5.0.6-1-setup.exe installer. Follow the instructions in the GUI to complete installation. Hit "Cancel" at any time to abort. Confirm that you'd like to start Scyld Cloud Workstation as a service to have Scyld Cloud Workstation start automatically.

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

Once this update is successful, proceed to: *Flexera License Management*.

6.5 Windows 7: Updating an Existing Install

Double-click on the Scyld Cloud Workstation-5.0.6-1-setup.exe installer. Follow the instructions in the GUI to complete installation. Hit "Cancel" at any time to abort. Confirm that you'd like to start Scyld Cloud Workstation as a service to have Scyld Cloud Workstation start automatically.

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

Important: If you are updating over an existing Scyld Cloud Workstation installation, your old config file will be preserved. The new package may include an XML config file with newer / updated settings. Merge the new settings found in `C:\Program Files\Penguin Computing\Scyld Cloud Workstation\Defaults\scyld-cloud-workstation.xml` with the existing `C:\Program Files\Penguin Computing\Scyld Cloud Workstation\scyld-cloud-workstation.xml` file.

Once this update is successful, proceed to: *Flexera License Management*.

6.6 Client Installation

Install any of the following browsers:

- Chrome 30+
- Internet Explorer 11+
- FireFox 27+
- Safari 7+

Note: Chrome 30+ provides the best performance and is recommended.

CHAPTER

SEVEN

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.

7.1 Supported License Types

Scyld Cloud Workstation currently supports node-locked licenses and floating licenses. Licenses take the form of plain text that can be copied and pasted from one license file to another license file.

7.1.1 Node-Locked License

A node-locked license enables one unique computer to use the software.

7.1.2 Floating License

A floating license enables anyone on the network to use the licensed software, up to the limit specified in the license file.

Floating license files are typically named: `scyld-flexlm.lic`.

7.2 Obtaining a License

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

7.3 Installing a Node-Locked License

If you are using a file named `scyld-cloud-workstation.lic` from Penguin Computing, you are most likely using a Node-Locked license.

Copy this file to `/opt/scyld-cloud-workstation/bin` for Linux hosts or `C:\Program Files\Penguin Computing\Scyld Cloud Workstation` for Windows hosts.

7.4 Installing a Floating License

If you have a file named `scyld-flexlm.lic` from Penguin Computing, you are most likely using a Floating license. You will also need the Scyld FlexLM license server package.

Follow these steps on the license server 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 `scyld-flexlm.lic` to `/opt/scyld-cloud-workstation/bin` for Linux hosts or `C:\Program Files\Penguin Computing\Scyld Cloud Workstation` for Windows hosts.
3. In `scyld-flexlm.lic`, find the line that looks like: `VENDOR PENGUIN PORT=<port>`. The last token is the vendor port number.

   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`.
4. Change your firewall to allow incoming connections to the vendor and license server port numbers you found above.
5. 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 `28282` on a host with hostname `iceberg`:

   ```
   <Server>
     ...
     <LicenseFile>28282@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 28282
   ```

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

7.5 Testing your Floating 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

EIGHT

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.

8.1 Applying Config File Changes

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

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

```
service scyld-cloud-workstation restart
```

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.

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

8.2 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.

8.2.1 License Management

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

8.2.2 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

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 or `scyld-cloud-workstation.bat /passwd` in Windows as an Administrator.

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*

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

8.2.3 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*.

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

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.

8.2.5 HTTPS / SSL Certificates

HTTPS is 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/

Attention: You need to install OpenSSL on your server to complete the setup.

- Windows: https://slproweb.com/products/Win32OpenSSL.html
- Linux: `yum install openssl` or `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.

8.3 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.

8.3.1 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'.

8.3.2 Server.LogFormat

Format of the output. By default, Scyld Cloud Workstation does not display a timestamp with each log message. To add timestamps to all of your output, open the `scyld-cloud-workstation.xml` and set `LogFormat` to: `%Y-%m-%d %H:%M:%S %q%q:  %s:%u:  %t`.

8.3.3 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.

8.3.4 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 `boot.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

8.3.5 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.

8.3.6 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.

8.3.7 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.

8.3.8 Server.Port

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

8.3.9 Server.Secure

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

8.3.10 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.

8.3.11 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.

8.3.12 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 takes effect after a service restart.

8.3.13 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.

8.3.14 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.

Password rules are dependent on length:

Length	Password Restrictions
8-11	Use mixed case characters, numbers, and symbols
12-15	Use mixed case characters and either numbers or symbols
16-19	Use mixed case characters
20+	No restrictions

We recommend using passphrases of four randomly generated english words (i.e. "mail design kick office" for the best combination of usability and security.

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: `scyld-cloud-workstation.sh --passwd`
- Windows: `scyld-cloud-workstation.bat /passwd`

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

Changed in v5.0.0.

8.3.15 Server.Auth.MinPasswordLength

The length of the password that is hashed and stored as *Server.Auth.ShadowPassword*. This may be set as low as 8, but we recommend at least 12 characters.

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

Changed in v5.0.0.

8.3.16 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.

8.3.17 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.

8.3.18 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.

8.3.19 Server.Auth.ScyldCloudAuth.Allow

A list of `<Username></Username>` elements. 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 v5.0.0.

8.3.20 Server.Auth.ScyldCloudAuth.Deny

A list of `<Username></Username>` elements. 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 v5.0.0.

8.3.21 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.

8.3.22 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.

8.3.23 Server.VideoSource

The video capture mechanism. Currently supports `nvfbc` and `stream`.

Set to `nvfbc` only if you have an NVIDIA GRID SDK compatible graphics card and driver. Set to the general purpose `stream` for all other systems.

Defaults to `nvfbc` if the service detects a system that supports NVIDIA's NvFBC capability. Otherwise defaults to `stream`.

Changed in v5.0.0.

8.3.24 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 `1920`.

Updated in v5.0.0. Changed default.

8.3.25 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 `1080`.

Updated in v5.0.0. Changed default.

8.3.26 Server.Video.StartFrameRate

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

Added in v2.2.0.

8.3.27 Server.Video.MinFrameRate

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

Added in v2.2.0.

8.3.28 Server.Video.MaxFrameRate

The highest allowable frame rate for a connection. Measured in frames per second. Defaults to `60`.

8.3.29 Server.ConcurrentClients.MaxClientCount

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

Added in v3.0.0.

8.3.30 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`.

8.3.31 openSSL

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

8.3.32 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.

8.3.33 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.

8.3.34 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.

8.3.35 openSSL.server.loadDefaultCAFile

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

8.3.36 openSSL.server.cipherList

Specifies the supported ciphers in OpenSSL notation.

Changed in v3.0.0. Default value changed.

8.3.37 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.

8.3.38 openSSL.server.privateKeyPassphraseHandler.options.password

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

8.3.39 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.

8.3.40 openSSL.server.cacheSessions

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

8.3.41 openSSL.server.extendedVerification

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

8.3.42 openSSL.server.requireTLSv1_2

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

Added in v2.2.0. Default value changed.

8.3.43 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.

8.3.44 openSSL.fips

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

8.4 Client Settings

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

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

CHAPTER

NINE

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.

9.1 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
```

9.2 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.

9.2.1 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`.

9.2.2 Register the Windows Service

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

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

The scyld-cloud-workstation 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.bat.

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

9.2.3 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
```

9.3 Change the Config File Password

Scyld Cloud Workstation lets you optionally store a username and hashed password in the config file for authentication. The credentials specified by Server.Auth.Username and Server.Auth.ShadowPassword attributes are entirely independent from LDAP, the remote operating system, and ScyldCloudAuth.

You can change this password by calling `scyld-cloud-workstation.sh --passwd` in Linux or `scyld-cloud-workstation.exe /passwd` in Windows from a command line. This password change takes effect without a service restart.

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.

9.4 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`.

In Linux, debug and higher level log messages can be found at: `/opt/scyld-cloud-workstation/bin/scyld-cloud-workstation.log`.

In Windows, debug and higher level log messages can be found at: `C:\Program Files (x86)\Scyld Cloud Workstation\boot.log` and `C:\Program Files (x86)\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 does not display a timestamp with each log message. To add a timestamp to all of your output, open the `scyld-cloud-workstation.xml` and set `LogFormat` to: `%Y-%m-%d %H:%M:%S %q%q: %s:%u: %t`.

9.5 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.

9.6 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.

Upon 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.

9.7 User Controls

The control buttons allow you to enter fullscreen mode, submit `Ctrl-Alt-Del` to the remote OS, or sign out from Scyld Cloud Workstation session.

Key-combinations such as `Ctrl+N`, `Ctrl+W`, and `Ctrl+T` are not relayed to Scyld Cloud Workstation in most browsers. Chrome users can work around this issue by running Chrome in "app mode" by appending the `--app=<url>` flag when calling it from a command line or shortcut.

Key-combinations such as `Ctrl-Alt-Del` are intercepted by the client OS and must be sent to Scyld Cloud Workstation via control buttons.

9.8 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 OS X clipboard to the remote Linux / Windows desktop, press `Cmd+V` to synchronize the clipboards and then `Ctrl+V`.

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

9.9 Change Screen Resolution

Warning: Changing screen resolutions has one 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.

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

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).

9.10 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.

9.11 Sign Out

Windows and Linux 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.

CHAPTER

TEN

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.

10.1 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.ConcurrentClients.MaxClientCount` setting in the config file at `scyld-cloud-workstation.xml`.

10.2 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.

10.3 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.

10.4 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.

10.5 Pause Guest Video

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

10.6 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.

10.7 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.

10.8 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.

CHAPTER

ELEVEN

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.

11.1 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.

11.2 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.

11.3 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.

11.4 Further Help

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

CHAPTER

TWELVE

FREQUENTLY ASKED QUESTIONS

12.1 How many users can sign in at a time?

Scyld Cloud Workstation currently supports multiple signed in users at a time. At the time of this writing this defaults to 6. This value can be changed in the config XML file via the MaxClientCount option.

12.2 What screen resolutions are supported?

See ServerScreenResolution.

12.3 Can the sign in page connect to LDAP?

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 and set the Server.Auth.ScyldCloudAuth.URL and Server.Auth.ScyldCloudAuth.Allow.Username values.

12.4 I'm only seeing a gray rectangle.

This is either caused by caching problems, 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 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.

12.5 How do I press Ctrl+Alt+Del?

There is a shortcut button for this keyboard combination at the bottom of the Scyld Cloud Workstation video screen.

12.6 How do I press Ctrl+N, Ctrl+T, Ctrl+W, Ctrl+Tab, Ctrl+Page Up, or Ctrl+Page Down?

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.

12.7 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).

12.8 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.

12.9 Will it run on my iPad / mobile device?

Official support for mobile devices is on the roadmap as a lower priority feature. Please let us know if this should be a higher priority!

12.10 Is there audio support?

Audio support is on the roadmap as a lower priority feature. Please let us know if this should be a higher priority!

12.11 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.

12.12 What graphics cards do you support?

See *Server Hardware*.

12.13 How many NVIDIA GRID GPUs do I need?

You only need one NVIDIA GRID GPU. An NVIDIA GRID K2 card comes with two GRID GPUs, which means with the right virtualization support you could have two VMs have one GRID GPU each.

CHAPTER

THIRTEEN

INDICES AND TABLES

- genindex
- search

INDEX

O

openSSL.client.verificationMode, 34
openSSL.fips, 34
openSSL.server.cacheSessions, 34
openSSL.server.certificateFile, 33
openSSL.server.cipherList, 33
openSSL.server.extendedVerification, 34
openSSL.server.invalidCertificateHandler.name, 33
openSSL.server.loadDefaultCAFile, 33
openSSL.server.privateKeyFile, 33
openSSL.server.privateKeyPassphraseHandler.name, 33
openSSL.server.privateKeyPassphraseHandler.options.password, 33
openSSL.server.requireTLSv1_2, 34
openSSL.server.verificationMode, 33

S

Server.Auth.Enabled, 28
Server.Auth.FailAttempts, 30
Server.Auth.FailDelay, 30
Server.Auth.MinPasswordLength, 29
Server.Auth.ScyldCloudAuth.Allow, 30
Server.Auth.ScyldCloudAuth.Deny, 30
Server.Auth.ScyldCloudAuth.URL, 30
Server.Auth.Session.DefaultTimeout, 31
Server.Auth.Session.OnSignIn, 31
Server.Auth.ShadowPassword, 29
Server.Auth.Username, 28
Server.AutoLock, 27
Server.BootLogFile, 27
Server.LocalCursor, 27
Server.LogFile, 27
Server.LogFormat, 27
Server.LogLevel, 27
Server.Port, 28
Server.Secure, 28
Server.Video.MaxClientCount, 32
Server.Video.MaxFrameRate, 32
Server.Video.MinFrameRate, 32
Server.Video.StartFrameRate, 31
Server.VideoSource, 31