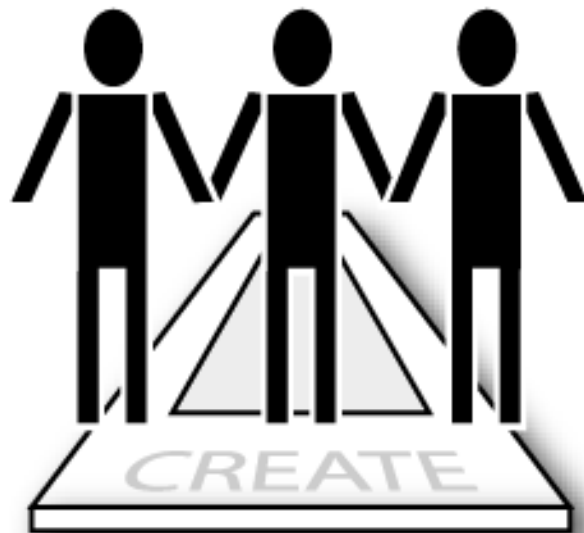


**Halden Virtual Reality Centre
HVRC CREATE**

Administration Guide

Server

HVRC CREATE Server Cybersecurity and System Deployment



**HVRC CREATE
Release 4.2.2
August 2026**

HVRC CREATE: Server Administration Guide.

This document contains information proprietary to IFE. Information contained herein may not be copied, reproduced, disclosed or used without the express written permission of IFE. This document may be copied for use internally at the licensed site only.

IFE makes no warranties with respect to the contents or use of this document, including but not limited to the implied warranties of merchantability and fitness for a particular purpose.

The information contained in this document is subject to change without notice.

Java™ is a trademark of Oracle Corp.

OpenGL® is a registered trademark of Hewlett Packard Enterprise.

Apple®, MacOS X® and macOS® are registered trademarks of Apple, Inc.

Microsoft® and Windows® are registered trademarks of Microsoft Corp.

All other trademarks used within this document are the properties of their respective trademark holders.

Comments about this document are welcome and may be sent to <create-support@ife.no>.

© Halden Virtual Reality Centre, IFE 2002-2026. All rights reserved.

Table of Contents

1	OVERVIEW	5
1.1	HVRC CREATE	5
1.2	SERVER	5
2	GETTING STARTED	6
2.1	SYSTEM REQUIREMENTS	6
2.2	INSTALLATION	6
2.2.1	Upgrading	6
2.2.2	Uninstalling and Reinstalling	6
2.3	STARTING THE SERVER	6
2.4	SUPPORT	7
2.5	USER IDENTIFICATION	8
2.6	CHANGING THE ADMINISTRATOR USER PASSWORD	8
2.7	OVERVIEW OF THE USER INTERFACE	8
3	DEPLOYMENT GUIDANCE AND RECOMMENDATIONS	9
3.1	CONNECTION TO CYBER ASSETS	9
3.2	CYBERSECURITY POLICY	9
3.3	ACCESS	9
3.3.1	Access to Cyber Assets	9
3.3.2	Access Control Policy	9
3.3.3	Notification and Revocation	9
3.4	AUTHENTICATION AND AUTHORIZATION	9
3.5	SOFTWARE AND SERVICES	10
3.6	SOFTWARE ARCHITECTURE	10
3.7	MALWARE DETECTION AND PREVENTION	10
3.8	VULNERABILITY MANAGEMENT	10
3.9	HARDWARE, FIRMWARE, SOFTWARE, AND PATCH INTEGRITY	11
3.10	PATCHING GOVERNANCE	11
3.11	SECURE DEVELOPMENT PRACTICES	11
3.12	VIRUSES, FIRMWARE, AND MALWARE	11
3.13	END OF LIFE OPERATING SYSTEMS	11
3.14	CRYPTOGRAPHIC REQUIREMENTS	11
3.15	REMOTE ACCESS	11
3.16	DATA IMPORT AND EXPORT	11
4	SERVER CONFIGURATION AND MANAGEMENT	13
4.1	CONFIGURING DATA STORAGE LOCATION	13
5	TROUBLESHOOTING	14
5.1	GENERAL PROBLEMS ACCESSING A SERVER AFTER INSTALLATION	14

5.1.1	Is there a web server running on the computer?.....	14
5.1.2	Does your server have a permanent IP (network) address?	14
5.1.3	Is there anti-virus software blocking or monitoring web-traffic on your computer?.....	14

1 Overview

1.1 HVRC CREATE

HVRC CREATE 4 is the fourth generation of the CREATE tool suite and builds on the technical platform and functionality established during the implementation of earlier versions of the software, as well as valuable feedback gained from usability evaluations and research work by the development team.

The CREATE control room design tools combine advanced interactive 3D technology with server-based user, project, and file management, providing an integrated package that supports and traces the various stages of a human-centred design process.

The software has been designed to support a flexible, iterative, design methodology, where a control room design is refined and tested many times before a final design is reached. This contrasts with traditional control room design methods where the design process only goes through one or two human factors review iterations, and where it is necessary to build a costly physical control room mock-up. Design iterations are tracked by the system.

When these virtual reality tools are used, it is not necessary to wait until a physical mock-up has been constructed before commencing design verification and validation against human factors guidelines, so greater emphasis can be placed on finding an optimal design solution for safe and efficient control room operation. Users with a variety of technical skills can operate the software, so control room operators, designers, human factors specialists, engineers and managers can all participate to some degree in the design process.

CREATE provides features designed to support and enhance communication between the various interest groups involved in a design project. Support for communication between the layout designers and reviewers is integrated into the system, while it is possible to extract electronic documents such as models, designs and reports for distribution to other interested parties.

The CREATE tools support the management of a reusable database of 3D objects, the interactive construction of control room layouts, and the validation of control room layouts against guidelines.

The CREATE tools are based on cross-platform Internet and Java technology and open standards such as ISO VRML, DAE/COLLADA, XML, and HTML.

1.2 Server

The CREATE Server is based on Apache web server technology. Windows, Linux and macOS operating systems are supported as server platforms. Currently installers are made available for Microsoft Windows and Apple macOS. Installing the server on a laptop is only recommended for single user CREATE Server licenses. Machines that will host the server for multiple users and will not be used as workstations do not need graphics acceleration. The server can be hosted on a virtual machine.

Machines used to host multi-user CREATE Servers on a network must have a static IP address. If you are unsure if the machine you plan to use as a server has a static IP address, please confer with your local network system administrator to ensure that your computer has the necessary credentials.

Approximately 1GB free disk space is required for the server if Microsoft Windows is used (plus space for your project files that will be created by users of the software -- at least another 100 MB of free space is recommended). On Linux and macOS computers, where Apache and Perl are pre-installed, about 100MB less space is required. The server data should be regularly backed up.

See the HVRC CREATE Overview User Guide document for additional details about the rights and roles of users, and an introduction to the installation process.

2 Getting Started

2.1 System Requirements

The minimum requirements for the HVRC CREATE Server are:

- Intel Core i5 (8th gen) x64 processor or similar
- 8GB RAM
- 64-bit Microsoft Windows 10 or Apple macOS 11
- For Microsoft Windows: 250MB free disk space for the complete tool suite.
For macOS: 1GB.
- A three-button mouse (or a two-button mouse with scroll-wheel "button")

Use the option or alt-key on your keyboard in combination with the left mouse button to simulate the middle mouse button if you do not have three mouse buttons.

2.2 Installation

Important: See System Requirements above before installing.

The installer called "CREATE Server Installer" installs and configures the server.

Double-click on the installer and follow the instructions provided by the installer. The HVRC CREATE software is ready for use when a license key file has been installed on the server.

The installer will guide you through the process of installing the software and installing a license key via a web-browser interface. This can all be done by a system administrator using the "admin" user.

To change the admin user password and to set up system users, install the CREATE Tools and use the User Tool to configure users and user permissions. See the User Tool User Guide for details.

2.2.1 Upgrading

To upgrade a server to the latest version, download and run the "CREATE Server Updater". Note that it does not upgrade any data on the server.

On Microsoft Windows, the installer includes the server run-time environment in the installer. This is not the case on macOS or Linux where the server uses standard system components on those platforms. Using the updater will upgrade the CREATE platform functionality to the latest version. but not the run-time environment components. On Windows, it is therefore necessary to uninstall and reinstall the software using the "CREATE Server Installer" to force updating of the server components (Apache and Perl) and ensure that the latest security fixes in the server components are installed.

2.2.2 Uninstalling and Reinstalling

The server installation includes an uninstaller. Note that if you uninstall the software then only the software is removed. The uninstaller will not delete any data or configuration files.

Consequently, uninstalling the server software and then reinstalling it using the full "CREATE Server Installer" will restore server functionality and reenale access to the data via the server.

2.3 Starting the Server

The Server starts automatically when installed and when the server computer is restarted.

On Windows, the ApacheMonitor tool (link provided in the Start-menu) can be used to stop, start, or restart the server.

On macOS and Linux, the command-line tool `apachectl` can be used to stop, start, or restart the server process. As super-user or a user with administrator privileges, execute the command `apachectl stop`, `apachectl start`, or `apachectl restart` to control the server.

2.4 Support

Please send questions, bug reports, or requests for new features to: create-support@ife.no

When submitting bug reports, please include the following information:

- A description of the result and how it differed from what you expected
- The conditions or circumstances under which the problem occurred
- Any other information that could be useful to isolate the problem, including the version of CREATE you are using, the version of the operating system of your computer, and the type of graphics card you are using for issues with the CREATE Tools. An overview of useful technical information is displayed in the User Tool's About dialog, located in the Help menu, and can be copied into an email or saved to disk in a text file.

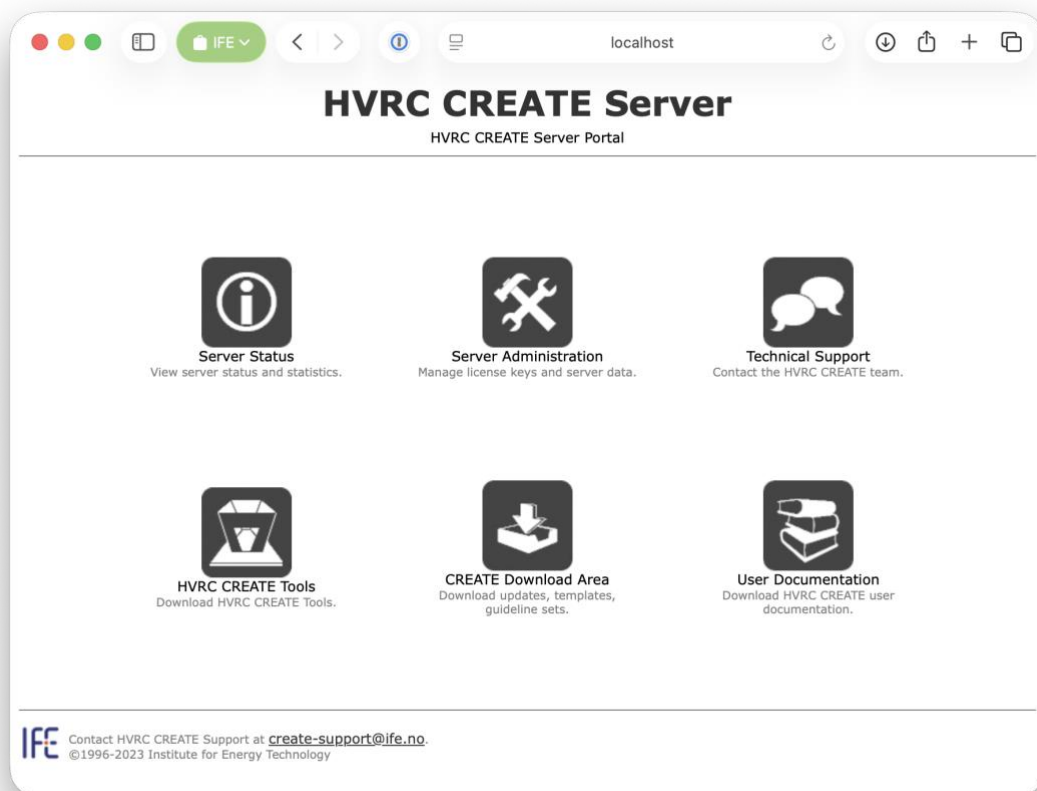
2.5 User Identification

If you are the system administrator, then you can use the login name “admin”. The administrator’s password is initially set to “admin”. You should change this password as soon as possible using the User Tool. Only users with CREATE server administration rights are permitted to use the User Tool. These can be assigned using the User Tool to delegate user management for a CREATE Server to a specific CREATE user, if desirable.

2.6 Changing the Administrator User Password

See “Setting a user password” (section 3.5) in the User Tool User Guide for information on changing the password for the “admin” user.

2.7 Overview of the User Interface



The CREATE Server Dashboard Interface

The Server dashboard can be accessed by entering the address of the server in a web browser. It mostly provides access to statistics and user documentation but also an interface for managing server license keys and certificates. It also provides convenient shortcuts for accessing the download pages for the latest versions of the software and supporting data packages.

To access the Server Administration interface through the dashboard, you must enter the login name “admin” and the associated password when prompted after clicking on the Server Administration icon.

3 Deployment Guidance and Recommendations

This chapter provides an overview of the cybersecurity-related deployment aspects of the HVRC CREATE system. Its purpose is to answer typical questions and to offer insights and recommendations regarding the practical deployment of the system in a controlled environment.

3.1 Connection to Cyber Assets

HVRC CREATE is a self-contained teamwork server designed primarily for use by in-house design teams. It is not intended to be connected to external critical digital assets (CDAs) and provides only basic support for remote management. It uses standard Apache webserver with Perl technology as a platform. All data is by default stored locally on the server PC where the Apache web server and CREATE Server configuration are installed, however the system and project data can be manually re-configured to use a file location on a remote server. There are no specific cloud or offsite services prescribed, and all data management and backup responsibilities rest with the organization operating the server. The CREATE Server functions as a gateway for users with CREATE Server user accounts, serving data via the client applications (CREATE Tools). Direct file access is therefore limited to those authorized by the organization at the operating/file system level. The CREATE Tools depend entirely on data stored on the Server to operate.

3.2 Cybersecurity Policy

HVRC CREATE is developed and maintained according to ISO-certified secure development practices. This includes code review, formal testing, and static code analysis to identify vulnerabilities. The software is not released with known security vulnerabilities found during testing until they have been addressed. The system is not designed to meet all requirements of cloud-based or enterprise-wide cybersecurity frameworks, as it is intended for a much more limited and specialized scope, which may include use on a computer or network without Internet access.

3.3 Access

3.3.1 Access to Cyber Assets

HVRC CREATE does not access or connect to any assets beyond its own server installation. All access is managed by the organization's administrators.

3.3.2 Access Control Policy

User accounts and roles for the CREATE system are managed using the CREATE User Tool and Project Management Tool. The default configuration for the CREATE Server uses authentication provided by the Server only. Single sign-on is not enabled out of the box. Thus, all user management is normally local to the web based CREATE Server. Only users with CREATE-specific user accounts and assigned roles can access project data via the CREATE Server software.

3.3.3 Notification and Revocation

User account creation and revocation for the CREATE Server is normally managed by a system administrator using the CREATE User Tool.

3.4 Authentication and Authorization

Authentication is managed using CREATE-specific user and user-role policies, the Apache web server software, and the underlying operating system (typically Windows). Passwords are stored encrypted; users can change their own passwords. Password complexity is enforced by the CREATE tools, however any change frequency policies are not enforced. Account management is the responsibility of the organization's administrators and can be delegated to a specific CREATE user other than the "admin" user, if desired. HTTPS is by default enabled in the Apache server configuration, with self-signed certificates to ensure encrypted communication between the CREATE Tools and CREATE Server software. Except in the case of a single-user standalone installation, the server must be installed on a computer/server with a fixed IP address. This is usually a local network address, which can be accessed via offsite/remote users via a VPN connection, if necessary. Please contact the CREATE

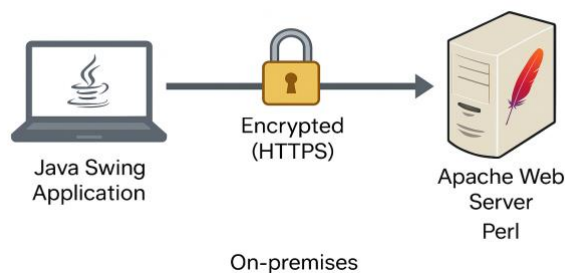
Support staff for information and guidance if you need to install your own certificates for a unique Internet IP address.

3.5 Software and Services

HVRC CREATE is delivered as a suite of tools that build on open-source platform technologies: Apache & Perl for the Server, OpenJDK Java platform for the Tools. Only necessary software components are included; unused ports and services can be disabled at the Apache configuration level. During installation of the CREATE Server, alternative network ports to the standard HTTP/Web ports are proposed if those ports are found to be already in use on the host system. Optionally, network ports can be reconfigured by a system administrator by modifying configuration files. The system does not include unnecessary utilities, compilers or protocols. Organizations are responsible for backing up the data directory. Updates are released as needed, with major releases annually and additional updates for security issues. The Java platform is installed for use by the CREATE Tools only and not as a system component.

The CREATE Tools interface to the Server and depend on it for accessing data. The Tools do not store project data locally as all data management, including revision/version management is handled by the Server. However, some tools can export information for sharing with other systems and software, such as exporting 3D models created using the software, and exporting reports.

3.6 Software Architecture



Clients: Java-based (Swing desktop app with 3D extensions on OpenJDK Platform). OpenJDK embedded into fat app, not system level install.

Server: Apache HTTP Server hosting Perl (CGI/PSGI)

Connection: HTTPS with self-signed certificates (TLS)

Deployment: On-premises only

Security posture: All communication encrypted end-to-end

The HVRC CREATE software architecture is based on a client-server model and is normally secured with self-signed TLS certificates. The system is intended for internal deployment on an isolated network server, accessible solely through a tightly controlled internal network (such as a private LAN or VLAN), and not exposed to the public internet. This approach confines all communication to known, trusted internal IP addresses, thereby reducing the risk of man-in-the-middle attacks. HVRC CREATE operates independently of any external internet connection for TLS operations, as certificate creation, configuration, and renewal are managed locally using OpenSSL. This eliminates reliance on external services and minimising the system's attack surface.

In this configuration, OpenSSL serves as the cryptographic library for TLS, utilising RSA for key exchange and server authentication. This setup ensures that all data exchanged between clients and the server is encrypted (for example, with AES) and protected by robust RSA-based signatures, making sure that only authorised clients and the server can access or modify the information.

3.7 Malware Detection and Prevention

The server should be protected by the organization's anti-virus/malware solutions. The Apache server can be monitored and audited as for any standard web server. This includes Access and Error logging.

3.8 Vulnerability Management

New releases of the CREATE software update the bundled runtime platforms with the latest security patches. Any significant security issues in Java or Apache may trigger the distribution of new installers. Registered technical contacts are notified by the CREATE Support staff of updates, but patching is not automatic. Users of the CREATE Tools receive a notification about updates when starting a tool after

an update has been made available, if the tool is used on a computer with internet access. Installing an updated version of the tools requires administrator privileges.

3.9 Hardware, Firmware, Software, and Patch Integrity

All software is delivered for local installation, using installers downloaded from a download page on the Internet. Organizations are responsible for installation, backup, and patching of the underlying OS and hardware. Updates are not delivered and installed automatically. However, the CREATE Support staff can provide guidance on automation possibilities, and on special requirements (e.g., HTTPS setup with organization certificates as opposed to self-signed).

3.10 Patching Governance

Updates to the CREATE Tools and Server are provided as needed. Major releases, with new functionality, typically occur annually, with one or two minor releases during a year with refinements; security updates are released as required. Organizations are responsible for timely installation of patches and updates.

3.11 Secure Development Practices

IFE, the organization responsible for the development of HVRC CREATE, is ISO certified (9001:2015/14001:2015). Code review, static analysis, and formal testing are performed for each release. Known vulnerabilities are addressed before release; the software is not released with unresolved security issues. IFE and the development team follow 27001 principles and processes.

3.12 Viruses, Firmware, and Malware

HVRC CREATE does not knowingly include malicious code and is checked for viruses before distribution.

SHA256 Hashes are provided on the CREATE software download page and can be used to check the integrity of installers downloaded. Organizations are responsible for anti-virus protection on the CREATE Server computer and in particular on the computers on which the CREAE Tools are used. Any issues detected in software included in the distributed software should be reported to CREATE Support immediately.

3.13 End of Life Operating Systems

HVRC CREATE is supported on current versions of Windows. Organizations are recommended to avoid installing on end-of-life operating systems.

3.14 Cryptographic Requirements

HTTPS is by default enabled in the CREATE Server Apache configuration, with self- certificates generated and provided by the CREATE Support staff when license keys are generated for new installations of the Server. Passwords are stored encrypted; auto-login credentials are protected by Windows account security if a CREATE Tools user enables auto-login.

3.15 Remote Access

HVRC CREATE is not intended or recommended for remote access or public cloud operation from a cybersecurity perspective, although that is technically possible. Access is normally via an organization's internal network. Offsite access is possible via an organization-level VPN for remote users.

3.16 Data Import and Export

Data import and export supported by the Server through the CREATE Tools includes:

- *Guideline Sets* – Import and export supported (via Guideline Tool). Individual guidelines in a set are in HTML format.

- *3D Models* – Import and export supported for 3D models (via the Model Bank Tool). Internal storage is in ISO VRML97 format; however models can be imported into the Model Bank database in other formats, including ISO COLLADA/DAE, LWO, OBJ, PLY, and GLTF.
- *Layouts* – Import and export supported for layout data. Layout data can be exported as a complete package for import into another project or a project on another CREATE Server but can also be exported as a 3D scene in ISO VRML97 or COLLADA/DAE format.
- *Reports* – Reports can be exported from the system in HTML format, and (for layout review reports) raw XML. Reports are produced using the project tools and include Layout Inventory, Layout Review, Layout History. A template system (using XSLT/CSS) can be used to format Layout Review reports, enabling the end-user to select between multiple formatting styles.
- *2D Images* – 2D images of the 3D view can be exported in JPEG or PNG format from any of the tools with 3D views. Images can also be added to a Review Report via the Verification Tool in JPEG format. 2D image files can also be imported (JPEG or PNG) to create 2D surface objects via the Model Bank Tool or directly in the Layout Tool.

An important principle guiding the development of HVRC CREATE is that open ISO or web-standard file formats should be used to the greatest extent possible in order to ensure the long-term storage and interoperability of data produced and stored in the system. 3D data is primarily stored in ISO VRML97 and COLLADA formats, which can easily be converted to other formats due to the open nature of the file format specifications.

4 Server Configuration and Management

4.1 Configuring Data Storage Location

By default, the CREATE Server stores all data in the “data” directory relative to the installed location of the CREATE Server. For example, on Windows this is typically in “C:\Program Files\CREATE\data”. To facilitate more convenient data backup routines, including storing the data in a location that is in the cloud (e.g. Microsoft OneDrive) or on a network file server, it can be convenient to direct the CREATE Server to store data in an alternative location.

Important: The description below is for CREATE Server installation deployed on Microsoft Windows however the process is very similar for macOS and Linux, where the command-line tool `apachectl` should be used instead of `ApacheMonitor`. Also, on Unix-like systems, you should edit the file `create.conf` (typically in “/etc/apache2/other”) instead of `http.conf`.

How to move the CREATE Server Data directory to an alternative location

1. Stop the Apache web server.
If the Apache Monitor is running in your Windows system toolbar, then use it to stop the server. If not, then start `ApacheMonitor.exe` in “C:\Program Files\CREATE\apache\bin” (you will probably need to run it as a Windows Administrator user)
2. Copy the whole data directory from “C:\Program Files\CREATE\data” to the preferred location. Don’t delete the original just in case something goes wrong!
3. Start a text editor running as Administrator (Notepad on Windows is sufficient)
4. Copy the file path for the new location of data (e.g. “D:\CREATE\data”)
5. Open the file `C:\Program Files\CREATE\apache\conf\httpd.conf` in your text editor
6. Scroll to the end of the file and look for the first block of text with `@@ CREATE` as a comment. You should see that it defines an alias for the data directory that states the original location as “C:/Program Files/CREATE/data/”
7. Paste the new file path as a replacement for the original location and then replace the ‘\’ characters with ‘/’ and add a ‘/’ to the end so that the format looks the same as the original (which can still be seen on the next line in the file)
8. Copy the adjusted file location for data from the `Alias` line to replace the same text on the following line (`Directory`)
9. Save the file
10. Open the file
`C:\Program Files\CREATE\scripts\conf\create_config.pl`
in a text editor
11. Locate the line that starts with `$CREATEHOME` and then paste the same file path here to replace the one listed as `$CREATESEVER/data`
12. Remove the final ‘/’ from the path that you pasted in step 11
13. Save the file
14. Use Apache Monitor to (re)start the server

Everything should look and work exactly as before but using the new directory location. To be certain that the new directory is in use, try renaming the original by inserting an ‘_’ before its name. If you are sure that everything is OK, then the original can then be deleted although we would recommend archiving a copy first just to be safe.

5 Troubleshooting

5.1 General Problems Accessing a Server after Installation

In most cases, installing a server is straightforward, involving running the server installer, requesting a license key for the server information provided by the installer, and installing the key received. See the installation procedure described in the Quick Start document for details on installing and configuring a HVRC CREATE Server.

The known potential pitfalls to watch out for are explained in the installation procedure. Other common questions are answered in the FAQ included with the system documentation.

5.1.1 Is there a web server running on the computer?

The following is aimed at Windows users. Users of macOS should contact CREATE Support for assistance as CREATE extends the existing web service on macOS rather than installing a new server.

You won't be able to access the CREATE Server if another web server is running on the computer on the same network port. The CREATE Server Installer will suggest using an alternative network support during installation if it detects that the usual port is already in use. If you try to access your computer's server address (as reported by the CREATE Server installer) in a web browser and you see a welcome page other than the one for the CREATE Server, then you are in this situation and will need to adjust the configuration of one the servers to avoid conflict.

5.1.2 Does your server have a permanent IP (network) address?

The CREATE Server has been designed to support collaborative teamwork. The server can be installed *either* as a standalone server (only accessible on the computer on which it is installed) *or* as a shared network server. If the network address of a shared server changes, then the license key will be invalidated as it is locked to the server address provided when the license key was generated.

If the computer on which you intend to install a CREATE server does not have a fixed network address, then you will need to permanently allocate an address to the server computer. If you have already installed the server and been allocated a license key then you may need to reassign the IP-address associated with the key to that computer on a permanent basis.

5.1.3 Is there anti-virus software blocking or monitoring web-traffic on your computer?

Some anti-virus software blocks or filters web traffic, so the anti-virus program settings may need to be adjusted to take into account that you are running a Web server on your computer or trying to access a web server through a tool other than a web browser.

While most anti-virus software will warn you that blocking or filtering is taking place, this is not always the case and the result can be unpredictable behaviour, if some communication between HVRC CREATE Tools (such as logging in) works while other communication (updating the databases on the server) fails.

Adjusting the anti-virus, network monitoring or firewall software settings to whitelist your CREATE Servers will normally resolve this issue.