Infor Cloverleaf Integration Services Installation Guide

Release 2022.09

Important Notices

The material contained in this publication (including any supplementary information) constitutes and contains confidential and proprietary information of Infor.

By gaining access to the attached, you acknowledge and agree that the material (including any modification, translation or adaptation of the material) and all copyright, trade secrets and all other right, title and interest therein, are the sole property of Infor and that you shall not gain right, title or interest in the material (including any modification, translation or adaptation of the material) by virtue of your review thereof other than the non-exclusive right to use the material solely in connection with and the furtherance of your license and use of software made available to your company from Infor pursuant to a separate agreement, the terms of which separate agreement shall govern your use of this material and all supplemental related materials ("Purpose").

In addition, by accessing the enclosed material, you acknowledge and agree that you are required to maintain such material in strict confidence and that your use of such material is limited to the Purpose described above. Although Infor has taken due care to ensure that the material included in this publication is accurate and complete, Infor cannot warrant that the information contained in this publication is complete, does not contain typographical or other errors, or will meet your specific requirements. As such, Infor does not assume and hereby disclaims all liability, consequential or otherwise, for any loss or damage to any person or entity which is caused by or relates to errors or omissions in this publication (including any supplementary information), whether such errors or omissions result from negligence, accident or any other cause.

Without limitation, U.S. export control laws and other applicable export and import laws govern your use of this material and you will neither export or re-export, directly or indirectly, this material nor any related materials or supplemental information in violation of such laws, or use such materials for any purpose prohibited by such laws.

Trademark Acknowledgements

Publication Information

Release: Infor Cloverleaf Integration Services 2022.09
Publication Date: September 29, 2022
Document code: clis_2022.09_installation_guide_2022__en-us

Contents

Contacting Infor

If you have questions about Infor products, go to Infor Concierge at https://concierge.infor.com/ and create a support incident.

The latest documentation is available from docs.infor.com or from the Infor Support Portal. To access documentation on the Infor Support Portal, select **Search > Browse Documentation**. We recommend that you check this portal periodically for updated documentation.

If you have comments about Infor documentation, contact documentation@infor.com.

Chapter 1: Obtaining and setting the license key

If you have purchased only Cloverleaf Integration Services, then you are entitled to install only that component of the Suite. Your license key enables only that component upon completion of the installation.

You can complete the Host Server installation and can run the system without your license keys. Without a license, though, there is limited access to engine processes, for example, testing tools cannot run without a license key.

Server installation must be completed before requesting a license key.

Note: A new license key is required when changing major versions.

To set the license key:

1. Log in to https://support.infor.com or https://concierge.infor.com.
2. Select **Resources > Request a Software Key**.
3. Complete the required information and submit. A notification is sent stating the key request has been received. Processing is completed within 24 hours.
4. After the license is obtained, place the `license.dat` license file into the `vers` directory of your Cloverleaf install directory at `%HCIROOT%/vers`.
5. Run `hcilictest` to check if the license is valid.

License management

The license key value is shown in the server startup log.

A new license key is required when changing major versions.

Whenever there are any changes to a license, the Host Server must be restarted to maintain consistency.

User Interface

On Windows platforms, whenever a network NIC is not available, the `hcihostid` program returns this message:

```
Unable to determine Host ID due to Network Card (NIC)
```

There is no disk ID backup method.

After the thread-limited license is in place, the engine enforces the thread limit per root level at runtime. If there are more runtime threads than what was licensed, then the extra threads that exceed the license limit are not started.

For example, 20 runtime threads have a license, but 26 threads are configured. When you attempt to start the process containing all 26 threads, the engine starts the first 20 threads. The remaining six threads are not started. This error message is listed in the log file:

```
You had 20 threads running, you are about to run more threads for this instance.
You have licensed 20 threads
You do not seem to be licensed to run more threads.
Contact your Customer Service Representative for assistance.
Exiting
```

Server interface

The engine limits the threads per installation instance as specified by the new license key. The engine validates the license against the total number of threads that are running among all sites under the instance. This validation happens only when you start a thread or process.

Performance effect

The performance effect is kept to a minimum. This effect varies depending on the number of sites and the number of threads in each site. The larger number of sites or threads, the longer time it takes to validate the thread limits.

License changes

Whenever there are any changes to a license, the Host Server must be restarted to maintain consistency.

UUID-based hostid

Supported platforms for Universally Unique IDentifier (UUID) licensing are:

- Windows:
  - VMWare
  - VirtualBox
  - Hyper-V
  - AWS

The UUID is 36 characters in length.

AWS instances begin with the prefix `EC2`. For example:

```
EC2AE145-D1DC-13B2-94ED-01234ABCDEF
```

Verifying that your platform is supported

On Linux AWS, run this command:

```
cat /sys/class/dmi/id/sys_vendor
```

Result:

```
Amazon EC2
```

Note: Linux non-AWS instances are not supported.

On Windows AWS:

1. Get the version:

   ```
   wmic csproduct get version
   ```

   Result:

   ```
   x.x.amazon
   ```

2. Get the primary owner:

   ```
   wmic computersystem get primaryowner
   ```

   Result:

   ```
   ec2
   ```

3. Get the UUID:

   ```
   wmic csproduct get uuid
   ```

   Result:

   ```
   EC2AE145-D1DC-13B2-94ED-01234ABCDEF (UUID w/ EC2 prefix)
   ```

For Windows non-AWS, to verify your platform is supported, run this command:

```
wmic computersystem get model
```

Accepted models are: "Virtual Machine", "VMware Virtual Platform", "VirtualBox".

Retrieving the UUID before installing Cloverleaf

To retrieve the UUID before `hcihostid` and Cloverleaf are installed:

On AWS instances of Windows and Linux, go to:

- https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/identify_ec2_instances.html
- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/identify_ec2_instances.html

On Windows non-AWS instances, run this command:

```
wmic csproduct get uuid
```

Note: Linux non-AWS instances are not supported.

Acquiring the hostid based on the UUID

In a supported system, `hcihostid` retrieves a 32-character `hostid` based on the UUID. This is not a UUID.

This UUID-based `hostid` does not contain the hyphen (-) characters that the UUID contains.

If the UUID cannot be found, then the `hcihostid` creates a `hostid` based on SNMP and MAC. The output is a 16-character length `hostid`.

Licensing process

After a UUID or a UUID-based `hostid` is obtained, you can generate a license using one of these in the License Generator's **hostid** field.

When the input is a UUID, in the `license.dat` file, the **hostid** field contains the 32-character UUID-based `hostid`. For example:

```
HOSTID=1cb40f2f7c9c0d44ec216398d796bc1d
```

The `license.dat` file is received by email. When you receive this file, add it to the appropriate directory:

- CIS: `HCIROOT/vers`
- CSC: `CSCROOT/vers`

Validation

You can verify the license has been installed correctly and is valid, using:

```
hcilictest “feature name”
```

The feature name is located in the `license.dat` file, prefixed by `FEATURE`.

`hcilicstatus` also displays features that are licensed and valid.

Chapter 2: Installing the CIS online help

The online help is now packaged as a separate zip file. This file must be installed after the software installation.

Note: Many browsers do not support running Javascript outside of a web server. Because of this, the online help does not function when you unzip the online help docs to a local drive in a file directory, not to a web server directory. The online help must be installed on the web server where the product is installed.

These steps explain how to host the Online Help documentation from the Host Server web server instance.

1. The online help zip file is provided separately from the software. After installing the software, go to one of these locations to download the online help documentation zip file:
   - Download Center (DLC)
   - Infor Concierge
2. Unzip `clis_vers_clfisolh_op_en-us_oxyhelp7.zip` to the `$HCIROOT/docs` folder. This is packaged as a zip file within `DOCUMENTATION.zip`.

   For example: `C:\cloverleaf\cis20.1\integrator\server\tomcat\cloverapps\documentation\HVI-CLIS_20.010000_DOCUMENTATION.zip\`
3. In a web browser, access the documentation, using URL:

   `http://hostname:port/cldocs/cloverleaf.htm`

   The port is different in each major release.

   For 20.1.x, the port is 15050. The URL for the 20.1.x documentation is: `http://hostname:15050/cldocs/cloverleaf.htm`.
4. The online help is now available for usage. Press F1 to open the help page.

   When using the Portable Client, on the **Select an Infor Cloverleaf Integration Services Server and Environment** dialog box, specify a server from which to access online help.

   For users who do not have CIS installed on their machine, they can specify the server address to access the online help.

   For users who have a remote IDE, the online help is accessed remotely. To access the local online help in remote mode, select **Open local help document** in the **Client Preferences > General** tab. This option is not necessary when using the Portable Client.

   You must also manually set the document base directory. This is in the `$HCIROOT\client\client.ini` file. For example:

```
Select an Infor Cloverleaf Integration Services Server[general]
doc_base_dir=C:\cloverleaf\cis20.1\integrator
```

Chapter 3: Cloverleaf Integration Services and VM

Cloverleaf is certified against processor chipset and operating system combinations. VMWare is not an operating system; therefore, Cloverleaf is not certified against VMWare.

VMWare is certified to work with a list of processor chipsets and operating system combinations for running within their virtual machines.

Cloverleaf works within a VMWare virtual machine as long as the processor/OS environment running within that virtual machine is on the Cloverleaf certified processor/OS list.

In a virtual environment, we recommend that hardware sizing and specifications be allocated as reserved resources. Failure to reserve the resources may result in performance issues as other virtual machines consume the resources allocated for Cloverleaf.

Note: It is a VM best practice to dynamically assign MAC address values. Cloverleaf installed on a Windows server requires a static MAC address value for licensing to work properly.

Chapter 4: Default ports used in the CIS GUI

This table lists the default ports that are used in the IDE, Host Server, and Security Server in different Cloverleaf versions.

Additional ports are also available.

Note: Best practice is to use the same install mode to install both CIS19.1 and 20.1. This avoids the duplication of ports. If necessary, then you can also change the conflicted ports after install.

Cloverleaf version	Default RMI registry port host server	Default RMI registry port security server	Tomcat default ports host server	Tomcat default ports security server
6.0	13020	13020	N/A	N/A
6.1	13021	13021	Shutdown: 15025 Catalina service: • HTTP: 15020 • AJP: 15021 • HTTPS: 15023 CatalinaRestWS service: HTTPS: 15027	N/A
6.2	13022	TLS: 14022 SSL (from CIS 6.2.2): 14023	Shutdown: 15035 Catalina service: • HTTP: 15030 • AJP: 15031 • HTTPS: 15033 CatalinaRestWS service: HTTPS: • False client authentication: 15037 • True client authentication: 15039 (from 6.2.2)	From CIS 6.2.2 Shutdown: 15135 Catalina service: • HTTP: 15130 • AJP: 15131 • HTTPS: 15133 CatalinaRestWS service: HTTPS: 15139

Cloverleaf version	Default RMI registry port host server	Default RMI registry port security server	Tomcat default ports host server	Tomcat default ports security server
19.1	13023	TLS: 14024 SSL: 14025	Shutdown: 15045 Catalina service: • HTTP: 15040 • AJP: 15041 • HTTPS: 15043 CatalinaRestWS service: HTTPS: • False client authentication: 15047 • True client authentication: 15049	Shutdown: 15145 Catalina service: • HTTP: 15140 • AJP: 15141 • HTTPS: 15143 CatalinaRestWS service: HTTPS: 15149
20.1	13024	TLS: 14026 SSL: 14027	Shutdown: 15055 Catalina service: • HTTP: 15050 • HTTPS: 15053 CatalinaRestWS service: HTTPS: • False client authentication: 15057 • True client authentication: 15059	Shutdown: 15155 Catalina service: • HTTP: 15150 • HTTPS: 15153 CatalinaRestWS service: HTTPS: 15159

Chapter 5: Using the contrib/ folder

A `contrib/` folder is included with the Cloverleaf software. This folder contains implementations and configurations contributed by the development community. These are not officially supported or tested. To use (enable) these, you must manually move the objects from `contrib/` to the correct location.

Everything under `contrib/` is unsupported and untested. Use at your own risk!

Chapter 6: Python3.8.x environment

To use Python3.8.x in Cloverleaf, you must install it on your machine.

These topics guide you in the installation of Python3.8.x on Windows and Linux.

Note: Only Python 3.8.0 is supported.

Installing Python on Linux from pre-built binary

To install Python on Linux:

1. Download linux-gnu-install and save to your local drive.
   For example: `/work/cpython3.8.0/`.
2. Untar the downloaded file to the a directory.
   Included is a directory named as the local Python. For example, `/work/cpython3.8.0/python`.
   Confirm that this includes `python/lib directory/libpython3.8.so.1.0`.
3. Add the Python path to the shell `$PATH` and `$LD_LIBRARY_PATH` by updating the shell `.rc` file.
   - For `bash`, add these lines to `~/.bashrc`:

     ```
     export PATH=/work/cpython3.8.0/python/bin:$PATH
      export LD_LIBRARY_PATH=/work/cpython3.8.0/python/lib:$LD_LIBRARY_PATH
     ```

   - For `tcsh`, add these lines to in `~/.cshrc`:

     ```
     setenv PATH /work/cpython3.8.0/python/bin:$PATH
      setenv LD_LIBRARY_PATH /work/cpython3.8.0/python/lib:$LD_LIBRARY_PATH
     ```

4. Log-in again to your system and run `python --version` in a shell to verify the installation.
   The version is returned if the installation is successful.

Installing Python on Windows from a pre-built binary

To install Python from a pre-built binary for Windows x64:

1. Download windows-msvc-shared-install and save to the local drive.
   For example, `C:\work\python3.8.0`.
2. Unzip the package locally. Included is a directory named as the local Python.
   For example, `C:\work\python3.8.0\python`.
3. In the local Python directory, add the Python path `C:\work\python3.8.0\python` to the system environment variable *"%PATH%"*.
4. Add a new system environment variable named "*PYTHONPATH*" that has the value `C:\work\python3.8.0\python\Lib; C:\work\python3.8.0\python\DLLs`.
5. Open a command window and run `python --version` in the DOS prompt. This verifies the version.

Installing Python on Linux from source code

To install Python on Linux from source code:

1. Refer to https://computingforgeeks.com/how-to-install-python-on-3-on-centos/. The `sudo yum -y update` step is unnecessary if there is no requirement to update CentOS.
2. Check if “Development Tools” is already installed. To do this, use the command `yum grouplist | grep "Development Tools"`.
3. Before running `yum install xxx`, run `yum info xxx` to check if the package has already been installed.
4. Set up `JAVA_HOME`. For example, `setenv JAVA_HOME /work/java/corretto-8.242`. Add this to `$PATH`.
5. Get the Python release using the command `wget https://www.python.org/ftp/python/3.8.0/Python-3.8.0.tgz`.
6. Extract the package by running `tar zxvf Python-3.8.0.tgz`.
7. Change the directory to the Python release path, using `cd Python-3.8/`.
8. Set up the installation by running the `configure` script: `/configure --enable-shared--enable-optimizations`.
9. Run `sudo make altinstall` to build and install Python.
10. Confirm the Python installation using `python3.8 --version” and “pip3.0 --version`.

Installing Python on Linux/Windows with Installer

To install Python on Linux, run the command `yum install python`.

Note: This might not install the most recent version of Python.

To install a specific version of Python, you can install it from the source code. To do this, see Installing Python on Linux from source code on page 20.

To install Python on Windows using the Installer:

1. Download the Python installer from https://www.python.org/downloads/ and run the installer as "administrator".
2. Change the default install path to a shorter path. For example, `C:\Python38`.
3. After the installation, ensure that paths similar to `C:\Python38` and `C:\Python38\Scripts` are added to `%PATH%`.
4. Verify the Python version. To do this, use the command `python --version`.

Chapter 7: AIX installation

Place the Installer into the `/tmp` folder creates a `/tmp/installer_temp_directory` file which conflicts with the `/tmp/installer_temp_directory` directory that the Installer attempts to create. Therefore, do not copy the Installer into the `/tmp` folder.

If there is a previously installed version of 6.X or above, then install the current version in the same directory path as the previous version.

For AIX platforms, the install path is user-defined. To find the current install directory, log-in as the hci user and specify the this command:

```
echo $CL_INSTALL_DIR
```

System file updated during installation

During installation on AIX, the `/etc/environment` system file is updated.

For all other AIX platforms, the `/etc/profile` system file is updated.

The `/etc/environment` system file is updated with these values:

```
# begin HCIenv current_version
FPATH=/opt/cloverleaf/cis current_version/integrator/kshlib
export FPATH
CL_INSTALL_DIR=/opt/cloverleaf/cis current_version
export CL_INSTALL_DIR
# end HCIenv current_version
```

`/opt/cloverleaf` is the install location.

Note: `FPATH` and `CL_INSTALL_DIR` are set according to the install location specified during installation. It is not necessary to manually set these before installation.

Multi-version

You can install and implement more than one version of the system. Previous versions that can coexist with this version are:

- 6.0
- 6.1
- 6.2
- 19.1

Host server process port numbers

- 6.0: 13020
- 6.1: 13021
- 6.2: 13022
- 19.1: 13023
- 20.1: 13024

Notes

After completing the installation, read the release notes to learn about features, known problems, and known problem workarounds.

All versions can run simultaneously on the same host machine.

If you require to verify that your machine complies with the hardware requirements, then contact Support.

This is a universal installation program for the product Suite.

- If you have purchased only the Integrator, then you are entitled to install only that component of the Suite. Your license key only enables that component of the installation.
- If you have purchased the Suite, then select the appropriate component and follow the installation instructions provided in the corresponding component installation section.
- Refer to the terms of your contract regarding your license agreement.

AIX pre-installation

Installation requirements are:

- You must have your license key to correctly run the system.
- Before installation, read and follow the pre-installation instructions for your operating system.
- If you have questions regarding any step of the installation, then contact Support.
- AIX systems without a minimum of 16-bit color depth have icons of lesser quality due to the color reduction capabilities of the X-server.
- ODBC installs require:
  - DataDirect Connect ODBC driver installation on the host server.
  - An ODBC license key.
- You must run the site promotion tools for update installs.
- If you run the system in a High Availability AIX environment, then you must update the `hci.profile`
- If the shell used by `hci`, `hcitest`, and `hcispt1` is not installed under `/bin`, then the related user cannot be successfully created. To avoid this, ensure the shell in installed under file to reflect the current version. `/bin`.
- Verify that you have the correct install procedures:
  - If this is the first time to install the system on your machine, then use the scratch install procedures for your platform.
  - If you have an installed version, then use the update install procedures for your platform.

The differences between platforms are:

- Only AIX server platforms have SNA drivers. A supported SNA stack is required for SNA interfaces.
- Math operation results are platform dependent.
- The number of file descriptors is platform dependent.
- On AIX, the `hci` and `hcitest` users use `ksh`.

Minimum space requirements

For minimum space requirements, see AIX scratch installation.

Installation password

During installation, the password that is created is **`gofish`**.

AIX installation order

Read all the steps included in the installation procedures for your platform. If you have any questions, then contact Support.

It is not necessary to shut down current versions that are running.

Follow the steps in the appropriate installation procedure, beginning with the platform-specific pre-installation instructions and proceeding to the installation options.

1. Start by becoming familiar with the information in this chapter.
2. Read AIX pre-installation.
3. Go to the topic for your specific platform and follow those instructions.

   Ensure you are logged on as root.

   For your platform, read each section carefully to ensure you have correctly set parameters, have sufficient disk space, and so on.
4. Note that a system backup must be made before continuing.
5. Un-tar the `<platform>.tar` file into a directory under `/root`.
6. Now you can begin the Host Server Install.

   For example, to install using the console mode, switch to the `IntegrationServices` folder and run the install script for console mode: `./CLInstall.sh -i console`
7. Use all defaults through the install, taking note of the Host ID.
8. Request a license key. See Obtaining and setting the license key.
9. If you do not have your license key, then the install script notifies you that you do not have a license file installed for this release. Instructions are then given to obtain your license key.
10. To run the ODBC drivers in the system, you must install the ODBC drivers.
11. Note that you can complete the Host Server installation and can run the system without your license key. Without a license, the engine does not run, and you cannot to use `hcixlttest` or `hciroutetest`.

12 Log on as hci and restart the Host Server using `hciss -s h`. Restarting the Host Server updates the `.ini` files.

13 Validate the installation by following the steps in Validating the installation.

AIX user-defined file system

The AIX installation program does not create a file system. The *user-defined* file system is created by the user. You can also use an existing file system, as long as it has the required free space for server installation.

user-defined is meant solely as a reminder that you must specify a file system name of your own choosing.

If you create the file system, then mount it as `/cloverleaf`, as your user-defined file system, and install to this directory path.

If you use an existing file system that contains the required free space, then specify a directory named `cloverleaf` in which to install.

For example, mount a file system as `/opt` that contains the required free space to install the system. At the install path prompt during installation, specify `/opt/cloverleaf`. This directory is created by the install program.

Changing the /tmp location

InstallAnywhere is used to generate installers for the different platforms. During installation, the first step of every installer created by InstallAnywhere is to self-extract its contents to a temporary directory.

On AIX platforms, InstallAnywhere extracts to the `/tmp` directory. The self extractor checks for adequate free disk space on the volume where the `/tmp` directory is located.

If there is not enough space available in the `/tmp` directory, then the installer does not prompt to select another location; the `IATEMPDIR` environment variable can be manually set to a location with sufficient temp space.

To change the `/tmp` location:

1 If `/tmp` does not have enough disk space, then set the `IATEMPDIR` environment variable to a directory on a disk partition with enough free disk space.

2 To set the variable, use these AIX commands:

Bourne shell (sh), ksh, bash, and zsh:

```
$ IATEMPDIR=/your/free/space/directory
$ export IATEMPDIR
```

C shell (csh) and tcsh:

```
$ setenv IATEMPDIR /your/free/space/directory
```

After the install has been successfully completed or canceled, the temporary resources used by the installer are deleted. It is not recommended to set the temp directory to the same location as the install location.

XWindows emulators

XWindows emulators allow users to access AIX and Linux-based X Window applications from their Windows desktop.

MobaXterm is the only certified emulator, allowing you to access AIX and Linux-based XWindow applications from a Windows desktop. Using other emulators can cause window location issues.

Note:

- XManager is the XWindow supported by InstallAnywhere.
- XMing, although free, could have problems. The CIS installer has been enhanced to avoid using message boxes, unless an error condition requires to show the message.
- You can also use the console mode installer on AIX. If you run the installation in console mode and cancel the installation after the files are copied, then the changes are not rolled back. In this case, you must manually clean up the files by running the uninstaller.

Configuring the MobaXterm emulator

To configure the MobaXterm emulator:

1. Install the x11 package on UNIX with `root`.
2. On Linux 8.x (CentOS or RHEL), PowerTools must be enabled for the packages `xorg-x11-server-devel` and `xorg-x11-apps`.

   ```
   >dnf config-manager --enable PowerTools
   >yum -y install xorg-x11-server-Xorg xorg-x11-xauth
   xorg-x11-server-devel xorg-x11-apps xorg-x11-fonts-Type1
   ```

3. Update `/etc/ssh/sshd_config`.

   `AllowAgentForwarding` = yes

   `X11Forwarding` = yes

   `DenyUsers` = hci

4. Restart the `sshd` service.

   ```
   >systemctl restart sshd.service
   ```

5. On the client side, Launch MobaXterm with SSH.

Chapter 8: AIX scratch installation

Use this type of install on a machine that does not have a previous version of the system installed. The recommended base for this version is an AIX scratch install and any optional layered products. See the release notes for the supported versions.

See AIX installation order for the order of steps during installation. If you have any questions, then contact Support.

AIX scratch requirements

Before installing, AIX must be correctly installed on your machine. The procedures for installing AIX are in IBM's Installation manuals. Complete the appropriate Base Operating System (BOS) installation procedure and perform the Optional Software Installation procedure.

- AIXwindows client Applications
- AIXwindows Default Fonts
- AIXwindows Latin 1 Fonts
- AIXwindows Runtime Common Directories
- AIXwindows Runtime Configuration Applications
- AIXwindows Runtime Environment
- AIXwindows Runtime Libraries
- AIXwindows Runtime Shared Memory Transport
- AIXwindows Utility Applications
- AIXwindows X Consortium Fonts
- AIXwindows aixterm Application
- Base Operating System Runtime
- Base System Locale ISO Code Set–U.S. English
- System Management Interface Tool (SMIT)
- TCP/IP client Support
- TCP/IP SMIT Support
- TCP/IP Server
- Text Formatting Services Commands
- Unix to Unix Copy Program
- License Management

Note: If any required products are missing, then the install script notifies you and suggests that you quit the installation process.

Use `smit lslpp_installed` as the root user to display the products installed on your system.

The **List the Installed Software** screen is displayed. Press **Enter** to use the defaults. Then use **PgUp**, **PgDown**, and the arrow keys, described on the screen, to scroll through the list.

IBM XL C Runtime Library 13.1.3.1

The IBM XL C Runtime Library 13.1.3.1 is required to run Cloverleaf AIX runtime. For example:

```
clbuild@aix71 02>lslpp -l | grep xlC.
 xlC.adt.include 13.1.3.0 COMMITTED C Set ++ Application
 xlC.aix61.rte 13.1.3.1 COMMITTED IBM XL C++ Runtime for AIX 6.1
 xlC.cpp 9.0.0.0 COMMITTED C for AIX Preprocessor
 xlC.rte 13.1.3.1 COMMITTED IBM XL C++ Runtime for AIX
 xlC.sup.aix50.rte 9.0.0.1 COMMITTED XL C/C++ Runtime for AIX 5.2
 xlCcmp.13.1.3 13.1.3.0 COMMITTED XL C++ compiler
 xlCcmp.13.1.3.lib 13.1.3.0 COMMITTED XL C++ libraries
 xlCcmp.13.1.3.license 13.1.3.0 COMMITTED XL C++ license files
 xlCcmp.13.1.3.tools 13.1.3.0 COMMITTED XL C++ tools
```

Additional information is available at the IBM site. See http://www-01.ibm.com/support/docview.wss?uid=swg24041950.

Optional software

In addition to the required products, you can install these software products. These products are not required:

- Base System Programming Information
- Base System Standard Information
- INed Text Editor
- X-Station Manager
- X-Station Manager U.S. English Messages

Maxuproc setting

Set the maximum number of processes that are allowed per user, `maxuproc`, to a value of 2048.

System parameter settings

We recommend that some parameters in `/etc/security/limits` be increased. These are located in the `default` section and are `data`, `rss`, `stack`, and `nofiles`.

For example:

```
default:
fsize = 2097151
core = 2097151
cup = -1                    Recommended Changes:
data = 262144               x 12
rss = 65536                 x 8
stack = 65536               x 8
nofiles = 2000              = 10000
```

This results in:

```
default:
fsize = 2097151
core = 2097151
```

```
cpu = -1
data = 3145728
rss = 524288
stack = 524288
nofiles = 10000
```

- Sizes are in multiples of 512 byte blocks
- CPU time is in seconds (a value of zero or -1 implies an unlimited value)
- `fsize` is the maximum file size in blocks
- `core` is the maximum core file size in blocks
- `cpu` is the per process CPU time in seconds
- `data` is the maximum data segment size in blocks
- `rss` is the maximum real memory usage in blocks
- `stack` is the maximum stack segment size in blocks
- `nofiles` is the number of open files per process

Note: A value of zero or -1 implies that the value is "unlimited."

EXTSHM environment variable

This variable turns on the extended shared memory facility and should be unset (for example, set to OFF) for the runtime environment to run correctly.

Note: Contact Support if there is a requirement to have this flag turned on.

AIX kernel settings

There is no standard kernel setting for CIS. hciengine is initially shipped with maxdata of 1G.

If you must set or verify the kernel settings, then use `ulimit -a` to check memory/disk, and so on.

For example:

```
hci@sjcaix005 2>ulimit -a
time(seconds)              unlimited
file(blocks)               2097151
data(kbytes)               131072
stack(kbytes)              32768
memory(kbytes)             32768
coredump(blocks)           097151
nofiles(descriptors)       2000
threads(per process)       unlimited
processes(per user)        unlimited
```

For a production environment with a powerful machine, you can use the these settings:

- Memory: `ulimit -m unlimited`
- Stack: `ulimit -s unlimited`
- Data: `ulimit -d unlimited`

AIX scratch pre-installation

You must complete these steps before attempting installation on your machine:

1. Log on as the `root` user.
2. Verify your space requirements. 980 MB is required in the file system where you intend to install the system. Additional requirements for the installation are:
   - `/tmp`: 1 GB
   - `/home`: 5 MB
   - `/usr`: 5 MB
   - `/`: 1 MB
   - `/<user-defined>`: 980 MB

   The install temporarily uses the `/tmp` disk space during the install. If you do not have enough temporary disk space in `/tmp`, then see Changing the /tmp location on page 25.

   For information on the *`user-defined`* file system, see AIX user-defined file system on page 25.
3. Verify that you have enough free space by running this command and looking for the number of free kilobytes:

   `df -k /tmp/home/usr/user-defined`

   `user-defined` is the file system name created by the user.

   For example:

File system	1024-blocks	Free	% used	lused	%lused	Mounted on
/dev/hd3	81920	55860	32%	272	2%	/tmp
/dev/hd1	425984	346256	19%	1975	2%	/home
/dev/hd2	1556480	10612	100%	52166	14%	/use
/dev/lvhci	327680	165208	50%	12445	16%	/<user-defined>
/dev/hd4	16384	6008	64%	1883	23%	/

   You must convert 1024-blocks to MB (for example, 15320 is approximately 15.32 MB).

   If you have mount point conflicts or logical volume conflicts, then you must resolve them before running the install script.
4. The install script creates several new users on your system. Before running the install script, verify that there are no conflicts with existing user names or existing user IDs. User accounts are:
   - `hci`

     Main system account. This user owns most of the files that are associated with the system. It is also the account used to access the dialog box and command-line tools that make up the interface.

     Default UID: 1001
   - `hcitest`

     Similar to the `hci` account, this is used to access the system. The difference between the two is that this account accesses your test site after it is created. The `hci` account accesses your production site.

There are two sites so that you can test changes to your configuration in the test site as the production site continues to run. You can also test the system independent from your production site.

Default UID: 1002

- `hcispt1`

  This account is used by Support when supporting your system installation.

  Default UID: 1003

Note: These users are created by the install script during a new install. Do not create them manually. If the UID is used by another user, then the system assigns the UID.

Check for user name conflicts: `grep "^hci" /etc/passwd`

You should not get output from this command.

Check for user ID conflicts: `grep "^[^:]*:[^:]*:100[123]:" /etc/passwd`

You should not get output from this command.

If you have a user name conflict, then contact Support for advice on how to proceed.

5 Verify that the two groups listed below already exist on your system:

`lsgroup -f staff,security`

Note: Use no space between `staff` and `security`.

Example output:

- staff:

```
id=1
      users=aconn,daemon
```

- security:

```
  id=7
      users=root
```

For the `staff` group, all users that are listed in Step 4 are members of this group. All files that are part of the system are owned by this group.

`security` is used to set ownership on `/etc/security/passwd` as new accounts are created. The required groups should exist because they are part of the base AIX installation.

Chapter 9: AIX update installation

Use this type of install on a machine that currently has a previous version installed. If you have any questions regarding how to proceed, then contact Support.

See AIX installation order for the order of steps during installation. If you have any questions, then contact Support.

System parameter changes

The system parameters are configured by the number of threads in your sites. For a list of settings, including `EXTSHM` environment variable settings, see AIX scratch installation.

High availability environments

If you run the system in a High Availability environment, then you must update the `hci.profile` file to reflect the current version.

AIX update pre-installation

You must complete these steps before attempting to install the system on your machine:

1. Log on as the `root` user.
2. Verify that you are logged on as `root`:

   ```
   whoami
   ```

   Output: root
3. 980 MB is required in the file system where you intend to install the system for the first time. Additional requirements for the installation are:
   - `/tmp`: 1 GB
   - `/home`: 5 MB
   - `/usr`: 5 MB
   - `/`: 1 MB
   - *`.user-defined`*: 980 MB

     The install temporarily uses the `/tmp` disk space during the install. If you do not have enough temporary disk space in `/tmp`, then see Changing the /tmp location on page 25.

     For information on the *`user-defined`* file system, see AIX user-defined file system on page 25.

4 Verify that you have enough free space by running this command and looking for the number of free kilobytes:

`df -k /tmp /home/usr/ user-defined`

For example:

File system	1024-blocks	Free	% used	lused	%lused	Mounted on
/dev/hd3	81920	55860	32%	272	2%	/tmp
/dev/hd1	425984	346256	19%	1975	2%	/home
/dev/hd2	1556480	10612	100%	52166	14%	/use
/dev/lvhci	327680	165208	50%	12445	16%	/<user-de-fined>
/dev/hd4	16384	6008	64%	1883	23%	/

5 To continue the install, go to AIX Host Server Install.

You must convert 1024-blocks to MB (for example, 15320 is approximately 15.32 MB).

For more space, use `smit chjfs` to extend the file systems. Or, remove any unnecessary files in `/tmp` to make more room available.

Making backups

Note: Do not install the system without creating the system backups described in these procedures.

Obtain two or more blank tapes to create system backups.

If you have more than one volume group, then back up any partitions outside of the `rootvg` volume group. Find out how many volume groups you have with the `lsvg` command.

For each listed volume group in addition to `rootvg`, determine what file systems are located in the volume group. Then perform a backup using these steps. Start your backups using `smit savevg`. This saves the volume group to tape.

Complete the smit dialog box:

1 Specify the first directory name in the **DIRECTORY** field.
2 Specify the name of your tape device in the **DEVICE** field. A typical tape drive name is **`/dev/rmt0`**.
3 Leave defaults for all other fields.
4 Insert a blank tape into the drive.
5 Click **OK**.
6 Repeat the above steps for each directory not included in the root volume group.

Put multiple backups on the same tape with `tar` or `cpio` directly. See your System Administration manuals for details. Obtain further system administration help in the AIX manuals or contact IBM support staff for assistance.

7 Label all resulting tapes, write-protect them, and store them in a safe place. Keep all backup tapes as permanent archives.

8 Make a backup copy of your `rootvg`. Start your backup by:
   - Specifying the `smit mksysb` command as `root`.
   - Specifying your tape device's name in the **DEVICE** field. A typical tape drive name is **`/dev/rmt0`**.
   - Insert the tape into the drive and click **OK**.

9 Remove the backup tape from the drive. Label it as a "pre-system install mksysb backup," write-protect it, and store it in a safe place. Keep this backup as a permanent archive.

10 To continue the install, go to AIX/Linux Host Server installation.

Chapter 10: Linux installation

RedHat Linux ES 3.0, ES 4.0, and ES 5.0 are no longer supported. See the release notes for the supported versions.

For users that run RedHat Linux AS, AS provides added support of extended hardware. Any program that runs on RedHat Linux ES also runs on AS.

Setting system parameters

You must complete these steps before installing on your machine:

1. Log on as the `root` user.
2. Check your current kernel parameters using:

   ```
   cat /proc/sys/kernel/shmmax
   cat /proc/sys/kernel/sem
   cat /proc/sys/fs/file-max
   ```

3. Back up `/etc/sysctl.conf` and apply these settings:

   Note: There is no requirement to apply these settings if your current settings are greater than these:

   ```
   echo "kernel.shmmax=2147483648" >> /etc/sysctl.conf
   echo "kernel.sem=250 32000 100 1024" >> /etc/sysctl.conf
   ```

   Note: This is a minimum value. This value is not fixed and must be updated according to size of your CIS installation (the number of sites, processes, and threads).

   ```
   echo "fs.file-max=65536" >> /etc/sysctl.conf
   ```

4. Reboot your machine or run the `sysctl -p` command to make the parameters effective.

   Note: Scheduled downtime might be necessary with your user community before rebooting.

Best practices for Linux kernel settings

The Host Server or Tomcat can crash when a large amount of invalid remote commands are run through CLAPI or the Remote Command tool.

Set the kernel limits:

```
cat /proc/sys/kernel/shmmax
cat /proc/sys/kernel/sem
cat /proc/sys/fs/file-max
cat /proc/sys/vm/swappiness
cat /proc/sys/vm/vfs_cache_pressure

vi /etc/security/limits.conf
# Increase limits for hci
* hard core 0
hci soft nofile 62000
hci hard nofile 65000
hci soft nproc 62000
hci hard nproc 65000
vi /etc/security/limits.d/90-nproc.conf (Linux 6.x)
vi /etc/security/limits.d/20-nproc.conf (Linux 7.x)
# Default limit for number of user's processes to prevent
# accidental fork bombs.
# See rhbz #432903 for reasoning.
* soft nproc 4096
root soft nproc unlimited
hci soft nproc 4096
hci hard nproc 4096
```

Check the limits:

```
ulimit -a
```

Troubleshooting: Displaying the number of `nprocs`.

```
ps h -Led -o user | sort | uniq -c | sort -n
```

Troubleshooting: Displaying the threads per process for `hci`.

```
ps -o nlwp,pid,lwp,args -u hci | sort -n
```

Using "libncurses.so.6" on Linux 8.x and AL 2

On RHEL 8.x and Amazon Linux2 (AL2) `libncurses.so.6` is used instead of `libncurses.so.5`.

After installing CIS on RHEL 8.x or AL2, you must make a symlink from `libncurses.so.5` to `libncurses.so.6`.

To do this, run these commands:

```
>sudo ln -s /lib64/libncurses.so.6 /lib64/libncurses.so.5
 >sudo ln -s /lib64/libtinfo.so.6 /lib64/libtinfo.so.5
```

Example on AL2:

```
[hci@amazonlinux2 vers]$ hcisitectl -K

Killing hcimonitord

Killing lockmgr 'lm_cis20.1_helloworld'
 console: error while loading shared libraries: libncurses.so.5: cannot open shared object file:
```

```
 No such file or directory
 Lockmgr didn't die, trying again.

Lockmgr is running on pid 31190
 hcimonitord is NOT running

[build@amazonlinux2 lib64]$ sudo ln -s /lib64/libncurses.so.6 /lib64/libncurses.so.5
[build@amazonlinux2 lib64]$ sudo ln -s /lib64/libtinfo.so.6 /lib64/libtinfo.so.5
[build@amazonlinux2 lib64]$ su - hci
 Password:
 Last login: Mon Jan 18 14:34:27 UTC 2021 on pts/0
[hci@amazonlinux2 ~]$ setsite helloworld
[hci@amazonlinux2 ~]$ hcisitectl

Lockmgr is NOT running
 hcimonitord is NOT running
[hci@amazonlinux2 ~]$ hcisitectl -S

Starting IP lock manager

Starting hcimonitord

Lockmgr is running on pid 32835
 hcimonitord is running on pid 32841
[hci@amazonlinux2 ~]$
[hci@amazonlinux2 ~]$
[hci@amazonlinux2 ~]$ hcisitectl -K

Killing hcimonitord

Killing lockmgr 'lm_cis20.1_helloworld'

Lock Manager Console Utility
 RDM Embedded 9.2 [30-Oct-2019] http://www.raima.com/
 Copyright (c) 1992-2013 Raima, Inc.. All Rights Reserved.

Lock manager terminated.

Lockmgr is NOT running
 hcimonitord is NOT running
```

Chapter 11: Linux scratch installation

Use this type of install on a machine that does not have a previous version of the system installed. The recommended base for this version is a scratch install of Red Hat Enterprise Linux and any optional layered products.

See AIX installation order for the order of steps during installation. If you have any questions, then contact Support.

Before installing, Linux must be correctly installed on your machine. The procedures for installing Red Hat Linux are in Red Hat's Linux Installation manual.

Making Linux backups

Do not install without creating system backups.

Make a backup of your system. See the Red Hat Enterprise Linux manual for details.

Label the backup media as a "pre-system install backup," write-protect it, and store in a safe place. Keep all backups as a permanent archive.

Linux scratch pre-installation

You must complete these steps before attempting to install on your machine.

Caution: Although RHEL 8 is supported in CIS 19.1.1.0, CIS 19.1.x does not function correctly on RHEL 8 due to missing libraries. Some shared libraries that are required by CIS are not included in the install package by default. To correct this, you must yum install the `libnsl` package on RHEL 8 before CIS installation.

1. Log on as the `root` user.
2. For a newly installed CentOS system, some libraries are not installed by default. To keep Cloverleaf running correctly, you must ensure these development libraries are installed to the system:
   - glibc.x86_64
   - libstdc++.x86_64
   - krb5-libs.x86_64
   - libzip.x86_64
   - libXtst.x86_64
   - libXrender.x86_64

- libXext.x86_64
- libX11.x86_64
- libxcb.x86_64
- libXext.x86_64
- libXdmcp.x86_64
- libXi.x86_64
- freetype.x86_64
- freetype-devel.x86_64
- libpng.x86_64
- fontconfig.x86_64
- fontconfig-devel.x86_64

In CentOS, run this command:

```
sudo yum install -y glibc.x86_64 libstdc++.x86_64 krb5-libs.x86_64 libzip.x86_64 libXtst.x86_64

libXrender.x86_64 libXext.x86_64 libX11.x86_64 libxcb.x86_64 libXext.x86_64 libXdmcp.x86_64
 libXi.x86_64
freetype.x86_64 freetype-devel.x86_64 libpng.x86_64 fontconfig.x86_64 fontconfig-devel.x86_64
```

3 Verify that you have enough free space. 950 MB is required in the file system where you require to install. Additional requirements for the installation are:

- `/tmp`: 350 MB
- `/home`: 5 MB
- `/usr`: 5 MB
- `/`: 1 MB
- */user-defined*: 950 MB

  For information on the *user-defined* file system, see AIX user-defined file system on page 25.

Note: The dialog box install temporarily uses the `/tmp` disk space when performing the install. If you do not have enough temporary disk space in `/tmp`, then see Changing the /tmp location on page 25.

4 The install script creates several new users on your system. Before running the install script, verify that there are no conflicts with existing user names or existing user IDs.

User accounts are:

- `hci`

  Main system account. This user owns most of the files that are associated with the system. It is also the account used to access the dialog box and command-line tools that make up the interface.

  Default UID: 1001

- `hcitest`

  Similar to the `hci` account, this one is used to access the system. The difference between the two is that this account accesses your test site after it is created and the hci account accesses your production site. There are two sites so that you can test changes to your configuration in the test site as the production site continues to run. You can test the system independent from your production site.

  Default UID: 1002

- `hcispt1`

This account is used by Support when supporting your system installation.

Default UID: 1003

These users are created by the install script during a new install. Do not create them manually. If the UID is used by another user, then the system assigns the UID.

5 Check for user name conflicts with `grep "^hci" /etc/passwd`

You should not get output from this command. If you have a user name conflict, trhen contact Support for advice on how to proceed.

6 Check for user ID conflicts with `grep "^[^:]*:[^:]*:100[123]:" /etc/passwd`.

7 To continue the install, go to AIX/Linux Host Server installation.

For the staff group, all users that are listed in Step 3 are members of this group. All files that are part of the system are owned by this group.

If the required groups do not exist, then they should be created before installation.

Chapter 12: Linux update installation

Use this type of install on a machine that currently has a previous version installed. If you have any questions regarding how to proceed, then contact Support.

See AIX installation order for the order of steps during installation.

System parameter changes

To update your system parameters, see Linux scratch installation.

Linux update pre-installation

You must complete these steps before attempting to install on your machine.

Caution: Although RHEL 8 is supported in CIS 19.1.1.0, CIS 19.1.x does not function correctly on RHEL 8 due to missing libraries. Some shared libraries that are required by CIS are not included in the install package by default. To correct this, you must yum install the `libnsl` package on RHEL 8 before CIS installation.

1. Log on as the `root` user.
2. Verify that you are logged on as `root`:

   ```
   whoami
   ```

   Output: root
3. 950 MB is required in the file system where you intend to install the system. Additional requirements for the installation are:
   - `/tmp`: 350 MB
   - `/home`: 5 MB
   - `/usr`: 5 MB
   - `/`: 1 MB
   - *`/user-defined`*
   - : 950 MB

   For information on the *`user-defined`* file system, see AIX user-defined file system on page 25.

   The dialog box install temporarily uses the `/tmp` disk space during the install. If you do not have enough temporary disk space in `/tmp`, then see Changing the /tmp location on page 25.

4 Verify that you have enough free space by running this command and looking for the number of free kilobytes:

```
df -k /tmp /home/usr/user-defined
```

For example:

File system	1024-blocks	Free	% used	lused	%lused	Mounted on
/dev/hd3	81920	55860	32%	272	2%	/tmp
/dev/hd1	425984	346256	19%	1975	2%	/home
/dev/hd2	1556480	10612	100%	52166	14%	/use
/dev/lvhci	327680	165208	50%	12445	16%	/<user-defined>
/dev/hd4	16384	6008	64%		23%	/

You must convert 1024-blocks to MB (for example, 15320 is approximately 15.32 MB).

5 To continue the install, go to AIX/Linux Host Server installation.

Chapter 13: AIX and Linux Host Server

See AIX installation order.

The global installer provides a list of available Cloverleaf Integration Suite products for installation. You can select one or more options.

All sub-Installers can be launched singly, and not only from the global installer. These are separate installers for each available product. This makes it more convenient when installing only one product (for example, to install only the Cloverleaf Data Integrator).

Increasing the default file handle limit setting for UNIX installations

When installing the Host Server and Security Server on UNIX, the default file handle limit setting is now increased.

We recommended that you install the Host Server and Security Server on different machines to avoid overtaking the limit.

Install modes

- GUI mode: This type of installation uses the GUI.
- Console mode: This type of installation uses the command line.
- Silent mode: This type of installation does not show the GUI or messages during the process. You modify the response (properties) file before running it. There are comments for each item in the response file.

Running the AIX and Linux installer in silent mode

The response file that comes with the installation is only a sample with comments that you can use as a template. You should modify the response file according to your requirements before running the installer in silent mode.

Before launching the global installer in silent mode, ensure the response file has been modified. This file includes the global installer and selected sub-installers.

The response file is located in the same folder as the `.sh` file, and the installer's `.bin` files are located under the `InstallSupport` folder. This avoids the possibility of launching the `.bin` files by mistake. If you are launching from the global installer in silent mode, then do not change the name or location of the response files of the sub-installers.

If you are launching the sub-installer individually, then you can use a different response file name. When running the command, you must specify the response file name with the full path when using the `-f` option.

AIX and Linux global installer

To launch the global installer (under the `root` folder):

- GUI mode: `./CISSuite.sh`
- Silent mode: `./CISSuite.sh -i silent -f $FULL_FILE_PATH/cissilent.properties`
  - `$FULL_FILE_PATH` is the full path to the response file.
  - `cissilent.properties` is the response file that resides in the same location as the `.sh` file.

AIX and Linux sub-installers

To launch the sub-installer (under the `IntegrationServices` folder):

- GUI mode: `./CLInstall.sh`
- Console mode: `./CLInstall.sh -i console`
- Silent mode: `./CLInstall.sh -i silent -f $FULL_FILE_PATH/clsilent.properties`
  - `$FULL_FILE_PATH` is the full path to the response file.
  - `clsilent.properties` is the response file that resides in the same location as the `.sh` file.

Correcting the graphical installer error

Sometimes, you might get an error during installation regarding graphical installers not supported by the VM. In this case, `DISPLAY` must be set or exported when doing a remote or VM server install.

An X emulator such as MobaXterm is required to set a display back to the workstation.

1. From the command line, to locate the IP address of the workstation, use `ifconfig`.
2. Use Telnet, PuTTY, or something similar to gain access to the system server machine.
3. Log-on to the server as `hci`, then:
   a. Run `setroot`
   b. Run `export DISPLAY=xxx.xxx.xxx.xxx:0`.
      `xxx` is the IP address from Step 1.
4. Verify `DISPLAY` is set correctly using `xclock &`. This opens a clock.
5. Continue with the installation.

Installing the Host Server on AIX and Linux

This is a universal installation program for the product Suite.

- If you have purchased only the Integrator, then you can only install that component of the Suite. Your license key only enables that component of the installation.

- If you have purchased the Suite, then select the appropriate component and follow the instructions provided in the corresponding component installation section.

Refer to the terms of your contract regarding your license agreement.

1. Download the product and extract to a local folder.
2. Verify that you are logged on as the root user.

   For AIX and Linux, use `whoami`.
3. For all AIX platforms: Run the install script. To install through the Global Installer, specify `CISSuite.sh`. You can also run the individual installers without using the Global Installer.

   Note: These steps represent using the Global Installer option.
4. Click **Next**. The **License Agreement** dialog box is displayed. To continue with the installation, you must accept the agreement.
5. Click **Next**. A dialog box is displayed for you to select in which directory to install.

   You can additionally install on a file system directory path other than the default.
6. Ensure enough free space is available in the file system. Then, select or specify the directory path to use for the *`user-defined`* file system. For example, `/opt/cloverleaf`.
7. Click **Next**. The **Choose Product** dialog box is displayed.
8. Select **`Cloverleaf Integration Services`**.
9. Click **Next**. The **Documentation Option** dialog box is displayed. Select **Yes** to install the online documentation.
10. Click **Next**. The **Pre-Installation Summary** dialog box is displayed.
11. Click **Install** to begin the installation.
12. When the installation is complete, the **Site Name** dialog box is displayed.

    A site is a folder that contains all information that is required to configure a specific deployment of the system. The system must create a default site during installation. This is the template that your organization uses to create its own site.

    By default, the site name is the network name of your computer.

    Site names cannot be empty or contain spaces, uppercase letters, special characters, or be more than 19 characters in length. To change the default site name, specify another name in the **Site Name** text box.
13. Click **Next**. The **License Key** dialog box is displayed.

    For further information, see Obtaining and setting the license key.

    For existing customers, due to changes in version 6.0, you must obtain a new license key.
14. Click **Next**. An information dialog box is displayed that reminds you of the changes to the HL7 standard formats.

    To migrate sites from previous versions to the current version, refer to the Migration section of the release notes.
15. Click **Next**. The **Installation Complete** dialog box is displayed.
16. Click **Done** to finish.
17. The online help files are separately installed.

AIX and Linux Host Server post-installation

A new license key is required when changing major versions. See Obtaining and setting the license key.

Errors and warnings are written to the `integration_services_install.log` file.

Making a bootable system backup

Note: You must complete this step. The backups allow you to restore your system to a known state if a hardware or operating system problem develops later.

- Do not use any backups created except under the direction of Support. Using the backup incorrectly results in lost data. Keep this backup in a safe location.
- Do not use the tape you created before the installation. You must save them in addition to the tape you are about to create.
- Follow the procedures for your operating system to make a bootable system image backup. Label the tape as a "post-system install backup," write-protect it, and store in a safe place. Keep it as a permanent archive.
- Follow the procedures for your operating system to make backups of file systems outside of the root volume group.
- For further help with system administration, see the documentation for your operating system.
- After completing the install, view the release notes to learn about known problems and their workarounds.
- Continue to use the `hci` and `hcitest` accounts to access the system.

Installation exit codes

To know the exit code, after the installation has completed run the `echo $?` command.

The command output is a digital code.

Code	Description
0	Installer exits with warnings or without errors.
100	Platform is not supported.
101	The current user does not have administration privileges.
103	Microsoft Visual C++ 2013 redistributable package is not installed (Windows only).
104	Product already exists (Windows only).
105	Invalid path to install.
106	No product is selected.
107	Fixed port value is invalid (Only when fixed port is enabled).

Code	Description
108	Global installer is launched in console mode.
109	Invalid certificate file.
110	Incorrect certificate password.
111	Failed to generate allowlist database or security certificate.
112	Database installation error.
147	Sub-installer failed to launch from the global installer.
148	Cannot install `pdksh` (Data Integrator installer).

Installation log file

After installation, a log file is available under `$CL_INSTALL_DIR`.

If the installer aborts during installation, for example, the product already exists on the machine, then no log is generated under `$CL_INSTALL_DIR`. Instead, it is generated in this location:

- Linux: The log file is available under `/root`.
- AIX: The log file is available under `/` .

AIX installation validation

A helloworld site comes as part of the installation, so that you can validate your installation was successful, in addition to running `hciverify`. This site shows some of the basic system functionality.

To validate your installation:

1. Open the IDE.
2. Using the**Server > Change** menu option, change to the helloworld site.
3. On the IDE, start Network Monitor.
4. Start the helloworld process.
   If everything goes green, with the in thread in **`ineof`** status, then the installation was successful.

Post-installation errors

After the installation, correct any errors, or report them to Support.

Some errors can be fixed using these commands:

- `exec ksh`

- `export FPATH=/user-defined/kshlib`
- `setroot /user-defined/cis20.1/integrator`
- `hciverify`

Note: You must be logged on as `hci` to run `hciverify`.

Restarting the Host Server

You must restart the Host Server after the install to update the `.ini` files.

1. Log on as `hci`.
2. Run `hciss -s h` to start the host server.

Chapter 14: AIX and Linux site promotion

Site promotion is the process of transferring the site configuration files saved from a previous version to the appropriate locations in the current version. You must promote each site from the old version to the new.

Site names can be any combination of lower-case letters, numerical digits, and underscore (_) characters. For a default installation, the recommended length for a site name is 19 characters or less. If the location name is other than default, then the length may be limited to fewer characters. If any of your existing site names violate these rules, then you must rename the sites before promoting them.

1. Verify that you are logged on as the `hci` user by specifying `whoami`.
2. Use `setroot` to get into the system root environment.
3. Use `showroot` to verify that you are set to the system root.
4. Specify the command for your version:

   For 19.x, specify `hcirootcopy /user-defined/cis19.x/integrator`.

   For 20.1, specify: `hcirootcopy \user-defined\cis20.1\integrator`

   `hcirootcopy` finds all the site directories and prompts you to confirm your intention to copy each site.
5. Specify the letter **y** for yes.

   `hcirootcopy` copies the selected site directories.
6. When it asks to continue, specify **y**, the default, or press **Enter**.

   If there is insufficient space in the new root for all of the old sites, then the program copies as many sites as possible. It then shows a warning and skips the excess sites.
7. After `hcirootcopy` is complete, you must `setroot` and `setsite` for each site you copied, using this command at the command prompt:

```
setroot /user-defined/cis20.1/integrator
setsite sitename
```

Testing

1. Test your configuration using the release's test tools and engine processes. Do not proceed until you understand the release's bug fixes and functionality behavior in your environment.

2. If you do not already have a test site to test your system production environment, then make a copy of your production sites. Use the test copy to verify the routing and processing configuration before using the new site in production mode.
3. Use the Network Configurator to update the thread configurations for test connections to avoid any conflicts with current production sites. For example, this might involve different protocol connections.
4. Use `hcinetdiff` to identify NetConfig differences between your previous and current sites.

   For example, to compare a previous production site named `old_site` with the new configuration for `cissite`, use this command at the prompt:

   ```
   setroot /user-defined/cis20.1/integrator cissite
   hcinetdiff /hci/root6.0/old_site/NetConfig
   ```

   or

   ```
   hcinetdiff /user-defined/cis6.X/integrator/old_site/NetConfig
   ```

   In this step, you are comparing the NetConfig of the cis20.1 site called `cissite` to the NetConfig of the `root6.0` or cis6.X site.

   Examine the output from `hcinetdiff`. Use `hcinetconfig` and other configuration tools to change the site configuration. Repeat until it is ready for production use.

   When making these changes, keep the thread names identical in the old and new sites. Changing thread names may cause messages to stay in the recovery database and not complete their processing when bringing up the connections.

Making the cutover to production

Ensure to schedule a time for the production cutover and notify all users and those who manage the external connections. All users must understand that the engine processes shut down and the connections break during the actual cutover process.

Prior to production cutover from your current production sites to version 20.1, every site's hicrootcopied translates, TCL code, and routing must be tested. This ensures there are no problems before going live in the new environment.

This is a suggested procedure for going live or cutting over your current production sites to the live or production environment.

Note: This procedure is for each site. If you have more than one production site, you must `setsite` to each site and then perform these steps.

1. In the pre-20.1 production site, shut down all inbound to the server production threads to prevent messages from coming into the database. Keep all outbound from the server threads up and running so that all messages can cycle from the engine processes.
2. After five minutes, logged on as the `hci` user, run `hcidbdump -r` from the command line. Then you can see if any messages are in the recovery database.

Any listed data messages are still in the recovery database. You must wait until these messages have left the recovery database before shutting down the current production site engine processes.

3. Now that the recovery database is empty, shut down the old pre-20.1 production sites engine processes and daemons.
4. At the command prompt, clear the new site's runtime statistics:

```
setroot /user-defined/cis20.1/integrator cissite
hcimsiutil -Z
```

In this example, `cissite` is the name of the production site to be addressed.

5. You can now start up your production processes.

Chapter 15: AIX and Linux uninstallation

Uninstalling version 20.1 from a AIX computer removes all the components that have been installed on that computer. It does not remove the directory tree. It also does not it remove any files that have been added or modified after the installation, such as network configuration.

Note: Uninstall folders have "744" permission for security reasons. Only the hci user or root can perform the uninstallation.

1. Stop all system threads, the Monitor Daemon (monitorD), and the engine.
2. Exit and log off all system GUIs and any other open applications.
3. Change the directory to `$HCIROOT/uninstall_integration_services`.

   For GUI mode, run `./uninstall_integration_services`.

   For Console mode, run `./uninstall_integration_services -i console`.
4. Click **Uninstall** and follow the prompts.

   Optionally, if your computer has system security certificate files, delete the directory that contains these files. Removing this directory eliminates any potential discrepancies if you reinstall the system, and forces whoever administers system security to reissue all user certificates.
5. When the uninstallation is complete, the **Uninstall Complete** dialog box opens. Click **Done** to finish.

   The uninstaller removes the `$CL_INSTALL_DIR` environment variable from the system.

   When there are other CIS versions on your system, then the Cloverleaf commands fail. To resolve this issue, you must manually add back `$CL_INSTALL_DIR` into the environment variable.

   For example, on CIS 6.2:

   - On Linux, edit `/etc/profile` by adding:

     ```
     FPATH=/opt/cloverleaf/cis6.2/integrator/kshlib
     export FPATH
     CL_INSTALL_DIR=/opt/cloverleaf/cis6.2
     export CL_INSTALL_DIR
     ```

   - On AIX, edit `/etc/environment`, by adding:

     ```
     FPATH=/cloverleaf/cis6.2/integrator/kshlib
     CL_INSTALL_DIR=/cloverleaf/cis6.2
     ```

Chapter 16: hciuser

During installation, the Installer creates the hciuser. The password that is created/used depends on the type of installation.

In earlier versions, the hciuser profile was a standard user, not an administrator. If your machine already has an existing hciuser, then it skips creating the user during installation.

In earlier versions, the hciuser account was created on Windows with the password `G0neF1sh1ng`, instead of `gofish`.

This is valid if the account did not previously exist or was removed when uninstalling a previous version. If the account exists, then the password is unchanged.

Note: During AIX/Linux installation, the password that is created is `gofish`.

The installer checks for different return values. It prompts you for the password if hciuser is found on the target machine and the password is not one of the defaults.

If you have changed the hciuser password from the default, then the support tools cannot determine the password to create the service with the correct log-in credentials.

When the default hciuser password does not meet the password requirements for your target machine, use these steps to silently install CIS and Security Server. For example, when special characters are required.

Note: You must create hciuser exactly (not, for example, `hciuser2`) with a customized password. Otherwise, the installer cannot locate the default hciuser.

1. Create hciuser with a password that meets your environment requirements.
2. Install the CIS service with hciuser and its password, specified in Step 1.
3. Install the Security Server service with hciuser and its password, specified in Step 1.

Note: Do not remove hciuser. This is required for the CIS and Security Server service.

Modifying hciuser

When installing the CIS system or Security Server, the installer creates hciuser as a user with required rights and starts the service using this account.

If hciuser already exists as an administrator, then you can change its rights.

The hciuser profile is a standard user, not an administrator. If your machine already has an existing hciuser, then there is no effect because it skips creating the user during installation.

Some organizations have tight security rules and do not require starting the service with a user that has administrator rights. In these cases, you can change the hciuser privileges or create another user with the required rights.

This applies to the CIS system and Security Server installation.

The system must be installed using a local administrator account to create the necessary files and environment. After that, you can alter hciuser or create another user to run the system service.

If hciuser already exists as an administrator, then you can change its rights through these steps:

1. Remove hciuser from the administrator group.
2. If the `Performance_Monitor_Users` group exists on the current machine, then add `hciuser` to it. Otherwise, grant `READ` permission to hciuser on `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib` key.
3. Grant these rights to hciuser:
   - Log on as a service
   - Change the system time
   - Increase scheduling priority
   - Load and unload device drivers
   - Modify firmware environment values
   - Profile single process
   - Profile system performance
   - Restore files and directories
   - Take ownership of files or other objects

   You can grant modify permissions to at least the `exec` directory and subdirectories for each site. To avoid having to do this for each site, you can grant modify permissions from `C:\cloverleaf\cis20.1` on down.
4. These registry keys are granted `FULL` permission:
   - `HKEY_CLASSES_ROOT\.htc`
   - `HKEY_CLASSES_ROOT\.pl`
   - `HKEY_CLASSES_ROOT\hcitcl\Shell\Open\Command`
   - `HKEY_CLASSES_ROOT\Perl\Shell\Open\Command`
   - `HKEY_LOCAL_MACHINE\SOFTWARE`
   - `HKEY_LOCAL_MACHINE\SOFTWARE\Perl`

     Note: This key might not be present on your system.
5. Permission to start/stop the Cloverleaf service is granted after creating the service with the `subinacl.exe` command from Microsoft:

   ```
   subinacl /SERVICE "Infor Cloverleaf(R) Integration Services 201"
   /GRANT=hciuser
   ```

Creating a new user

1. Stop the service.

2 Go to **Control Panel > Administrator Tools > Services**.

Double-click **`Infor Cloverleaf(R) Integration Services 201`** and click the **Log On** tab.

3 Select **This account** and specify the name and password of the new user.

4 Delete the hciuser account.

5 Grant the new user these rights:

- Log-on as a service
- Change the system time
- Increase scheduling priority
- Load and unload device drivers
- Modify firmware environment values
- Profile single process
- Profile system performance
- Restore files and directories
- Take ownership of files or other objects

6 Add the new user to the Performance_Monitor_Users group.

7 Grant modify permissions to at least the `exec` directory and subdirectories for each site. To avoid having to do this for each site, you can grant modify permissions from `C:\cloverleaf\cis20.1` on down.

8 Restart the service.

Chapter 17: Specifying an alternate hciuser on Windows

You can create an alternate user that can log in to the Windows service. This alternate hciuser should have all Cloverleaf file system permissions assigned to it.

All resources that are assigned to hciuser go to the specified user.

Note: This only works when the user already exists before installing CIS.

For example, an alternate hciuser can set the user upon installation. This alternate hciuser is also the user that runs the engine and contacts your web services. By doing this, no other application can use your web services and your support staff does not require to set up multiple users.

Example:

The hciservice201 interface is:

```
hciservice [install [user [passwd]]|uninstall|adduser [user [passwd]|deluser [user]]
```

The `hciservice install paswd` is not supported in CIS. Instead, `hciservice install user passwd` is used.

Usage example

This example creates a default service:

1. Create a default service user and install the service.

   Then, uninstall the service and delete the default user.

```
C:\>call hciservice201 adduser
AddHciUser returned: 0 -- Creating user succeeded
C:\>call hciservice191 install
C:\>call hciservice191 uninstall
C:\>call hciservice191 deluser
DelHciUser returned: 0 -- Deleting user succeeded
```

2. Create the specific (alternate) service user with the default password, and do a cleanup.

```
C:\>call hciservice201 adduser testhci2
testhci2: AddHciUser returned: 0 -- Creating user succeeded
C:\>call hciservice191 install testhci2
C:\>call hciservice191 uninstall
C:\>call hciservice191 deluser testhci2
testhci2: DelHciUser returned: 0 -- Deleting user succeeded
```

3 Create the specific (alternate) service user and password, and do a cleanup.
Note: If the user is created with a specified password, then the password must be provided when `hciservice` is installed by that specified user.

```
C:\>call hciservice191 adduser testhci2 GoneInging0x$
testhci2: AddHciUser returned: 0 -- Creating user succeeded
C:\>call hciservice191 install testhci2 GoneInging0x$
C:\>call hciservice191 uninstall
C:\>call hciservice191 deluser testhci2
testhci2: DelHciUser returned: 0 -- Deleting user succeeded
```

Users other than hciuser

If a user other than hciuser is created and is the user of hciservice, then `%HCIROOT%` must be re-granted with access permission to the new user.

This applies to any new user other than hciuser, which is created by the Cloverleaf installer.

Previously, this step was taken by the Cloverleaf installer. The installer cannot be updated, so this line must be added to the command line operation.

In this example, `%HCIROOT%` (`c:\cis20.1\integrator`) is granted access permission to user "testhci".

```
>> icacls c:\cis20.1\integrator  /grant testhci:f /t /c /q
Successfully processed 33054 files; Failed processing 0 files
```

Domain user as log-on user of Cloverleaf windows service

Because domain\user should be created elsewhere, install the Cloverleaf windows service with that domain\user and user password, which is required:

```
C:\>hciservice201 install domain\user userpassword
```

To uninstall the Cloverleaf windows service, it is the same as before:

```
C:\>hciservice201 uninstall
```

If domain\user has not been granted access permission to `%HCIROOT%`, use the steps in Users other than hciuser to grant the permission.

```
C:\>icacls c:\cis20.1\integrator /grant:r "domain\user":f /t /c /q
Successfully processed 33054 files; Failed processing 0 files
```

Troubleshooting by using the “net helpmsg” cmd

Use the `net helpmsg` command to troubleshoot the installation. For example:

```
C:\>hciservice201 adduser testit2now passwdshort
NetUserAdd failed: 2245
testit2now: AddHciUser returned: 3 -- Failed to add user
C:\>net helpmsg 2245
The password does not meet the password policy requirements. Check the minimum password length,

password complexity and password history requirements.
```

Chapter 18: Windows pre-installation

These differences exist between platforms:

- Math operation results are platform dependent.
- The number of file descriptors is platform dependent.

If you install the Host Server and Client or the Client only on an unsupported platform, then it may not work. To ensure correct functioning, install only on a supported platform.

The system can include various combinations of Windows and AIX computers. For example, Clients running on Windows computers can access a Host Server running on a AIX computer. If you plan to include any AIX computers in your system, then you can obtain installation instructions for the appropriate platform from Support.

You can install more Clients at any time.

Universal installation

This is a universal installation program for the product Suite.

- If you have purchased only the Integrator, then you can only install that component of the Suite. Your license key only enables that component of the installation.
- If you have purchased the Suite, then select the appropriate component and follow the installation instructions provided in the corresponding component installation section.

Refer to the terms of your contract regarding your license agreement.

InstallAnywhere space requirements

InstallAnywhere is used to generate installers for the various platforms. During installation, the first step of every installer created by InstallAnywhere is to self-extract its contents to a temporary directory.

On Windows, InstallAnywhere extracts to the Windows `temp` directory. This is the directory specified by the TEMP environment variable. The self extractor checks for free disk space 3x the size of the installer on the volume where the temp directory is located.

If enough free space is not available, then the installer prompts for an alternate location for extraction.

Note: It is not recommended to set the `temp` directory to the same location as the install location.

After the install has been successfully completed or canceled, the temporary resources used by the installer are deleted.

You must run the site promotion tools for update installs.

Microsoft Visual C++ Redistributable Package for Visual Studio 2013

For installations on Windows, the Visual C++ Redistributable Package for Visual Studio 2013 (x64) is required before installation.

This package installs the required runtime components of Visual C++ libraries. This is required for both client and server installs if the necessary files are not detected on the target machine. The system is built on Visual Studio 2013. All binaries depend on the Visual C++ 2013 Redistributable Package.

You must install the package before installation can be completed.

This package is available at: https://www.microsoft.com/en-us/download/details.aspx?id=40784

This link is valid as of the release date. If this link does not work, then it might have been updated. In this case, contact Support for the latest address.

Windows Client requirements

We recommend that the platform where you install the Client meets these specifications:

- - The computer system must have at least 128MB of RAM (256 MB recommended) and at least 500MB of disk space.
  - The computer system must have a Pentium III processor or better with 333MHz or better processor speed.
  - The computer system must have 16MB (32MB recommended) video memory.
  - Check the Release Notes for the current list of supported Client platforms.

Uninstalling the Client does not remove existing sites or other files that have been changed or added after the previous system installation. You can promote old sites into the latest version of the system by following the instructions in Windows site promotion.

If you install the Client on an unsupported platform, then it might not work. To ensure correct functioning, install only on a supported platform.

You cannot run any Client until the Host Server is installed and running on a connected machine.

Windows Host Server and Client requirements

Installing the Host Server automatically installs the Client on the same computer. The Client provides a user interface to the Host Server.

- The platform where you install the Host Server must meet these specifications:
  - The computer system must have at least 512MB of RAM (1024 MB recommended) and at least 4 GB of available storage.
  - Check the Release Notes for the current list of supported Host Server and Client platforms.
  - The Client and Host Server should run on a dedicated Windows machine. That is, no Windows applications other than those in the system family should be installed on the same machine.
- You cannot run any Client until the Host Server is installed and running on a connected machine.
- Your system must have at least one Host Server and one Client. If there is only one Client, then it must run on the same machine as the Host Server.

Installation order

Verify that you have the correct option for installation: Host server and client, or client only.

Follow the steps in the appropriate installation procedure, beginning with the platform-specific pre-installation instructions and proceeding to the installation options.

When installing multiple clients, you could install several clients on several computers, and then install the client and Host Server on yet another computer. Or you could install the client and Host Server on one computer, and then install several clients on other computers. Or, you could install some clients, install the client and Host Server, and then add more clients.

Chapter 19: Windows installation

The system can include various combinations of Windows and AIX computers. For example, clients running on Windows computers can access a Host Server running on a AIX computer.

After completing the installation, read the release notes to learn about features, known problems, and known problem workarounds.

For Windows users, select **`Read Release Notes Now`** from the installation.

Install modes

Several modes are available for installation:

- GUI mode uses the Cloverleaf user interface.
- Console mode uses the command line.
- Silent mode does not show the GUI or messages during the process. You modify the response (properties) file before running it. There are comments for each item in the response file. See Running the installer in silent mode.

Windows sub-installers

All sub-Installers can be launched singly, and not only from the Global Installer. These are separate installers for each available product. This makes it more convenient when installing only one product (for example, to install only the Cloverleaf Security Server).

To launch the Installer (under the `IntegrationServices` folder):

- GUI mode: `CLInstall.bat`
- Console mode: `CLInstall.bat -i console`
- Silent mode: `CLInstall.bat -i silent -f %FULL_FILE_PATH%\clsilent.properties`
  - `%FULL_FILE_PATH%` is the full path to the response file.
  - `clsilent.properties` is the response file that resides in the same location as the `.bat` file.

Running the installer in silent mode

The response file that comes with the installation package is only a sample with comments that you can use as a template. You should modify the response file according to your requirements before running the installer in silent mode.

Before launching the Global Installer in silent mode, ensure the response file for the Global Installer and sub-installers have been modified.

The response file is located in the same folder as the `.bat` file. The installer's `.exe` files are located under the `InstallSupport` folder. This avoids the possibility of launching the `.exe` files by mistake. Do not change the name or location of the response files of the sub-installers if you are launching from the Global Installer in silent mode.

If you are launching the sub-installer individually, then you can use another response file name. When running the command, you must specify the response file name with the full path when using the `-f` option.

Windows multi-version

Users have the ability to install and implement more than one version of the system.

Previous versions that can coexist with version 20.1 are:

- 6.0
- 6.1
- 6.2
- 19.1

For Windows, the install script shuts down the system service during install and uninstall. Users must start the Windows service again after an uninstall.

A backup copy of `\cloverleaf\cis20.1\integrator\bin` and the `\cloverleaf\cis20.1\integrator\startup` directory is created during installation for the old version to preserve these files.

Multiple instances of Cloverleaf of the same version

Multiple instances of the same Cloverleaf version can be installed on the same machine.

For example, with multiple instances, use your Cloverleaf test server as a candidate for failover in the event that your primary production server stops.

You can also rename a Service name, giving the potential for multiple installations. Along with the new service name, you can uniquely identify the appropriate environment variables settings for each specific service.

During installation, there is a prompt to specify the instance name. By doing this, you can install multiple instances of the same version with another product name and service name.

All versions can run simultaneously on the same host machine.

If a revision is to be run in addition to 20.1, then do not remove these folders:

- `\hci\client`
- `\hci\server`
- `\hci\security`

These directories are removed only when the revision is removed.

Previous versions are not uninstalled

Because multiple roots can exist on Windows servers, the installer does not uninstall previous versions.

To uninstall previous versions, you must uninstall with the previous version's uninstaller.

If the uninstall removes files required by the system, then they can be restored from the backup copies made during the install.

If hciuser has to be added again to the machine, then run the command `hciservice adduser`.

Windows new installation prerequisite

If you have uninstalled the previous CIS Windows installation, then you must restart your machine before installing the new CIS version.

If the previous version is uninstalled, and the new version is installed under the same directory as the previous installation without first restarting the system, then numerous `jar` files will be missing from `clgui\lib`, `clgui\java`, and the `uninstall` folder.

You must restart your machine after CIS uninstallation before starting a new installation.

Creating a different user

1. Create a new user.
2. Stop the service.
3. Go to **Control Panel > Administrator Tools > Services**.
4. Select **`Infor Cloverleaf(R) Integration Services 201`** and click the **Log On** tab.
5. Specify the name of the new user under **This account** and then specify the **Password** .
6. Delete the hciuser account.
7. Grant these rights to the new user:

- Log in as a service
- Change the system time
- Increase scheduling priority
- Load and unload device drivers
- Modify firmware environment values
- Profile single process
- Profile system performance
- Restore files and directories
- Take ownership of files or other objects

8 Add the new user to the `Performance_Monitor_Users` group, if it is on the current machine. Otherwise, grant the read permission to the new user on key `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib`.

9 Grant modify permissions to at least the `exec` directory and sub-directories for each site. To avoid having to do this for each site, you can grant modify permissions from `C:\cloverleaf\cis20.1` on down.

10 Grant FULL permission to the new user on these registry keys:

- `HKEY_CLASSES_ROOT\.htc`
- `HKEY_CLASSES_ROOT\.pl`
- `HKEY_CLASSES_ROOT\hcitcl\Shell\Open\Command`
- `HKEY_CLASSES_ROOT\Perl\Shell\Open\Command`
- `HKEY_LOCAL_MACHINE\SOFTWARE`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Perl`, if it exists

11 Grant permission to start/stop the Cloverleaf service for the new user with the `subinacl.exe` command from Microsoft:

```
subinacl /SERVICE "Infor Cloverleaf(R) Integration Services 201" /GRANT=USER NAME
```

12 Restart the service.

Host server process port numbers

The Host Server process port numbers are:

- 20.1: 13024
- 19.1: 13023
- 6.2: 13022
- 6.1: 13021
- 6.0: 13020
- 5.8: 13019
- 5.7 MB: 13018
- 5.7: 13017
- 5.6 MB: 13016
- 5.6: 13015

- 5.5: 13013
- 5.4: 13012

Chapter 20: Windows update installation

Migrating to the current version is a two-step process, involving installation of the current version and site promotion.

The update installation procedures are identical to the procedures for installing the system on a computer that does not have a previous version installed. See:

- Windows Client installation
- Windows Host Server and Client installation

Note: These procedures are for replacing an earlier version with the current version on Windows machines. To replace one point release with another on Windows machines, see the Release Notes that accompany the new point release. To update the system on another platform, see the appropriate section.

- Check the Release Notes for the current list of supported Host Server and Client platforms.
- Before you replace an earlier version of the system, you should consider the recommended operating systems for installing the current version on Windows machines. Check the Release Notes for the current list of supported Host Server and Client platforms.
- The installation procedures for installing the system on a Windows computer are identical, regardless if the computer previously had an earlier version of the system.
- The system automates the process of moving files from an earlier version's directories into their new locations. This can be in other branches of the directory tree because of the reorganization that was necessitated by changes and additions to system features and GUIs.
- Check with Support to verify that the new version of the system that you plan to install is the latest version.
- Ensure to read the appropriate sections detailing pre- and post-installation procedures, and the installation procedures themselves.
- The Security Server can be on the same machine as Cloverleaf.
- Files that have not been changed after installation are removed after uninstalling the system. It leaves the directory tree intact, along with the contents of any file that has been changed or added. There is no requirement to recreate such files or save extra backups for reuse.

Chapter 21: Windows Host Server and Client installation

1. Copy *installer_temp_directory* to a local folder.
2. Log on as **admin** on the local domain.
3. For installation options, see Windows installation overview. After selecting an option, click the `bat` file to begin.

   The installation process is Java-based, and requires a JVM to run. When the install first begins, the program verifies whether JVM is installed on the target machine. If the required version is not installed, then the program copies the required JVM version to a temporary location so that the installation can proceed.

   After the JRE is verified, the installation program checks whether the user has admin privileges.

   - If not, the program displays then an error message and exits.
   - If admin privileges are present, then the install program continues.
4. Click **Next**. The **License Agreement** dialog box is displayed. To continue with the installation, you must accept the agreement.
5. Click **Next**. The **Install Location** dialog box is displayed.
6. Select the drive and directory. The default destination folder is `C:\cloverleaf`.

   You can also specify a directory path. If the path does not exist, then the installation prompts if you require to create the directory. If a location is selected where you do not have write permission, then the installation displays an error message. The directory name must not contain spaces.
7. Click **Next**. The **Choose Product** dialog box is displayed.
8. Select **Cloverleaf(R) Integration Services** and click **Next**. The **Setup Type/Documentation Option** dialog box is displayed.
9. Select **Host server and Client**. Then select whether to install the online documentation.
10. Click **Next**. The **Pre-Installation Summary** dialog box is displayed.
11. Click **Install** to begin the installation.
12. When the files are extracted, the **Default Site Name** dialog box is displayed.

    A site is a folder that contains required information to configure a specific deployment. A default site is created during installation to provide the template that your organization can use to create its own site.

    By default, the site name is the network name of your computer. Site names cannot be empty or contain spaces, uppercase letters, special characters, or be more than 19 characters in length.

    To change the default site name, specify another name in the **Site Name** text box.
13. Click **Next**. If `hciuser` already exists on the target machine, then the installer prompts you for the password. It does not matter if the password has been changed or you are still using the default password.
14. Click **Next**. The **License Key** dialog box is displayed.

    A new license key is required when changing major versions.

See Obtaining and setting the license key.

15 Click **Next**. An information dialog box is displayed reminding you of the changes to the HL7 standard formats.

16 Click **Next**. The**Installation Complete** dialog box is displayed.

17 Click **Done** to display the next dialog box, which reminds you to restart the system to complete the installation.

18 Select **Yes** or **No** and then click **Done**. You cannot run the system until you restart your computer or restart Windows.

19 After completing the installation, read the release notes to learn about features, known problems, and known problem workarounds. Select **Read Release Notes Now** from the installation.

20 The online help files are separately installed.

Chapter 22: Windows Client installation

1. Copy *installer_temp_directory* to a local folder.
2. Log on as `admin` on the local domain.
3. For installation options, see Windows installation overview. After selecting an option, click the `bat` file to begin.

   The installation process is Java-based, and requires a JVM to run. When the install first begins, the program verifies whether JVM is installed on the target machine. If the required version is not installed, then the program copies the required JVM version to a temporary location so that the installation can proceed.

   After the JRE is verified, the installation program checks whether the user has admin privileges.

   - If not, then the program displays an error message and exits.
   - If admin privileges are present, then the install program continues.
4. Click **Next**. The **License Agreement** dialog box is displayed. To continue with the installation, you must accept the agreement.
5. Click **Next**. This opens the **Install Location** dialog box.
6. Select the drive and directory. The default destination folder is `C:\cloverleaf`.

   You can also specify a directory path. If the path does not exist, then the installation prompts if you require to create the directory. If a location is selected where you do not have write permission, then the installation displays an error message.

   Note: The directory name must not contain spaces.
7. Click **Next**. The **Choose Product** dialog box is displayed.
8. Select **`Cloverleaf Integration Services`** and click **Next**. The **Setup Type/Documentation Option** dialog box is displayed.
9. Select **`Client Only`** (default). Then select whether to install the online documentation. The default is **Yes**.
10. Click **Next**. The **Pre-Installation Summary** dialog box is displayed.
11. Click **Install** to begin the installation. When the files are extracted, an information dialog box opens reminding you of the changes to the HL7 standard formats.

    To migrate previous version sites to the current version, refer to the "Migration" section of the Release Notes for details.
12. Click **Next**. The **Installation Complete** dialog box is displayed.
13. Click **Next**. This completes the Client installation.

    Note: You cannot run the system until you restart your computer or restart Windows.
14. After completing the installation, read the release notes to learn about features, known problems, and known problem workarounds. Select **Read Release Notes Now** from the installation.
15. The online help files are separately installed.

Chapter 23: Windows uninstallation

Uninstalling the system from a Windows computer removes all the system components that have been installed on that computer. It does not remove the system's directory tree, nor does it remove any files that have been added or modified after the installation. For example, network configuration files or translation configuration files.

Pre-uninstallation:

- Stop all system threads, the Monitor Daemon, and the system engine. If necessary, then use the Windows Task Manager.
- Exit and log off all system GUIs.
- Exit any other open applications.

To uninstall:

1. Click **Start > All Programs > Infor Cloverleaf Integration Suite > Remove Infor Cloverleaf Integration Services** . The **Uninstall** dialog box is displayed.

   This can also be accomplished from the Start menu by clicking **Settings > Control Panel** to open the Control Panel.
2. Double-click the **Add/Remove Programs** icon to open the **Add/Remove Programs** dialog box.
3. In the list of programs, click the system program.
4. Click **Add/Remove**. This opens the Uninstall dialog box.
5. Click **Uninstall** and follow the prompts.
6. Optionally, if your computer has system security certificate files, delete the directory that contains these files. Removing this directory eliminates any potential discrepancies if you reinstall the system and forces whoever administers system security to reissue all user certificates.
7. When the uninstallation is complete, the **Uninstall Complete** dialog box is displayed.
8. Click **Done**.

   The uninstaller removes the `%CL_INSTALL_DIR%` environment variable from the system.

   However, if you have other CIS versions on your system, the Cloverleaf commands fail. To resolve this issue, you must manually add back `%CL_INSTALL_DIR%` into the environment variable.

   For example, on CIS 6.2:

   a. Open **Control Panel > System** and click **Advanced system settings**.
   b. Click **Environment Variables...**.
   c. Add system variables `%CL_INSTALL_DIR%` using the value `C:\cloverleaf\cis6.2`.

Chapter 24: Manually removing the Windows installation

In some instances, the Windows installation could fail during the install. If this happens, then any attempts to re-install result in an error message stating "`You cannot re-install the product, as it is already installed`".

In this instance, you must manually remove the Windows installation using these steps:

1. Click **Start > Run regedit**.
2. Specify `regedit` and click **OK**. This opens the Registry Editor.
3. Locate the registry key: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Infor\CIS20.1\Infor Cloverleaf(R) Integration Services 20.1`.
4. Delete the key.
5. In your file system, remove all installed folders, including the uninstall.
6. Restart your machine.
7. Re-install the product.

Chapter 25: Uninstalling a major release

When uninstalling a major release on Windows, `%CL_INSTALL_DIR%` is removed if its value is the path of the current release.

If this is not removed, then `setroot` does not function on other CIS versions that are installed on the same Windows machine.

For example:

Both CIS 20.1.x and CIS 19.1 are installed on the same Windows machine.

If `CL_INSTALL_DIR` is `C:\cloverleaf\cis20.1`, then the CIS 20.1 uninstaller remove `CL_INSTALL_DIR`.

This causes the CIS 19.1 `setroot` to be unusable.

The workaround is to manually add `CL_INSTALL_DIR`.

At the end of uninstallation, a note reminds users that this is required for older releases to continue working after the uninstallation is completed.

In addition, you must also reset the environment variable.

Resetting the env variable

Linux:

Add these lines to the `/etc/profile` file:

```
FPATH=/opt/cloverleaf/cis6.2/integrator/kshlib
export FPATH
CL_INSTALL_DIR=/opt/cloverleaf/cis6.2
export CL_INSTALL_DIR
```

AIX:

Add these lines to the `/etc/environment` file:

```
FPATH=/cloverleaf/cis6.2/integrator/kshlib
CL_INSTALL_DIR=/cloverleaf/cis6.2
```

Windows:

1. Open the **Environment Variables** dialog box.
2. Click **Edit** in the System Variables section.
3. Add the `CL_INSTALL_DIR` variable with the value "C:\cloverleaf\cis6.2".

Chapter 26: Migrating from Windows to Linux during upgrade

These steps illustrate migrating from Windows CIS 6.2 to Linux CIS 20.1.

1. Install CIS 20.1.

   Install on a Windows and a Linux machine. It is unnecessary to create the site.

2. Prepare the site on Windows CIS 6.2.

   Copy the site into the root directory and restart the host.

3. Migrate the site from CIS 6.2 to CIS 20.1.

   On the Windows machine running CIS 20.1:

   a. Copy the site to a temporary location that mimics a Cloverleaf root directory. For example, `\temp\cloverleaf\cis20.1\integrator\`.

   b. Run `hcirootcopy` to migrate the site to the CIS 20.1 environment.

4. Create a BOX for the site on Windows CIS 20.1.

   a. In CIS, go to the `netconfig` site.

   b. Select the threads to include in your BOX. If needed, **Ctrl+click** to select multiple threads. Verify all threads are selected.

   c. Right-click any of the selected threads, and select **Create BOX**.

   d. Designate a name and select a location. This is the location on the server. By default, BOX configurations are stored at `HCIROOT/box`.

   e. Click **Next** to change the default selections.

   - In **Referenced Threads**, select the **Include all referenced threads automatically**.
   - In **Master Site or Root Resources**, select the **Include non-current site resources**.
   - In **Thread Route Deployment**, clear **Only keep the routes which destination thread in Box**.
   - In **Modify Resources**, include any required scripts or Tcl procs.

   f. Click **Next**.

   g. Modify any thread configuration properties in **Configure BOX Configuration Files**. For example, TCP/IP addresses, ports, and so on. This can be also done later in the NetConfig.

   h. Click **Finish** and then **OK** on the last screen.

5. Transfer the BOX to CIS 20.1 on Linux. After the BOX is created on the Windows machine, transfer the BOX to the new host server. To do this:

   a. Expand the Configuration section and select **BOX Manager**.

   b. If the new host server is on the same network, then click the arrow on the right side of the screen. This splits the screen, enabling a remote connection to the new host on which to transfer the BOX.

c Click **Select Remote Host** and provide the address/IP of the new host server.

d After it displays, copy/paste or drag the BOX to the new host.

e If the host server cannot be reached or the transfer fails, right-click the BOX and select **Export**. This retrieves the file that was downloaded to the machine on which the GUI is running.

f Select a method for placing the file on the new host server.

6 Deploy the BOX to CIS 20.1 on Linux. After the BOX is transferred to CIS 20.1 on the Linux machine, deploy the BOX to the new host server. To do this:

a Deploy the BOX on the new host server.

b On the host server, navigate to BOX Manager. If the site has not been created, then right-click the BOX and select **Create Site**.

c Name the site and click **Next**.

d This opens a summary of what is to be deployed to the new site. Click **Next**.

e Additional modifications to thread configuration properties are made at this time. Skip this if there are no modifications. Click **Finish**.

The site is then created and everything is deployed to it. If the site already exists, right-click the BOX and select **Deploy**.

The next screen displays any conflicts. Resolve any conflicts and click **Next** when done.

Any modifications to thread configuration properties are made at this time. Skip this if there are no modifications. Click **Finish**.

The site is then created and everything is deployed to it.

After the site is on the Linux machine, see Resolving migration issues on page 75 for assistance in resolving issues.

Resolving migration issues

To resolve any issues after migration:

1 Create the missing directory and correct the path for the thread in NetConfig when you get an error such as `*** is not a directory.`

Example error:

```
[nci :nci :ERR /0: cbord_cmd:--/--/---- --:--:--] flowsheet_recv Protocol Fileset/local-tps:
IB directory
'/cloverleaf/cis20.1/integrator/cgh_test/exec/processes/cgh_test/c:/cloverleaf/cis20.1/integrator/
cgh_test/exec/processes/recv_from_cerner/eicu_flowsheet_pickup' is not a directory.
```

For this error, create the directory (`recv_from_cerner/eicu_flowsheet_pickup`) and correct the path in Netconfig `process_cgh_test`.

NOT SURE WHAT DROPS FILES INTO THIS PICKUP DIRECTORY, BUT IT SHOULD LIVE OUTSIDE THE EXEC FOLDER. ANYTIME YOU MOVE TO A NEW MACHINE OR MAKE A BASE UPGRADE, THE EXEC FOLDER WILL NOT BE COPIED OVER, IT IS RECREATED LOSING ANYTHING STORED IN IT

2 Compile the file when you get the error `***.pdl: Failed to malloc(****) for driver.`

Example error:

```
[pdl :PDL :ERR /0: cbord_send:04/12/2021 19:21:07] mlp_tcp.pdl: Failed to malloc(140698833649830)
for driver
```

For this error, navigate to the `pdls` folder and compile the file using this command:`hcipdc mlp_tcp.pdl`

3 Copy outputs folder from original directory or zip with original permissions/attributes.

Example: For these errors, copy the outputs folder from the original `cgh_test` directory or zip. Retain the original permissions and attributes.

```
[pd :wrte:ERR /0: 3m_chartfact:04/12/2021 18:42:11] Error 13 while opening FS Test file for
../../../output/chartfact_out SMAT
[pd :open:ERR /0: 3m_chartfact:04/12/2021 18:42:11] Unable to open sqlite db
../../../output/chartfact_out
[pd :open:ERR /0: 3m_chartfact:04/12/2021 18:42:11] Internal Init failed for SMAT
../../../output/chartfact_out
[pd :open:ERR /0: 3m_chartfact:04/12/2021 18:42:11] Initializing secondary for
../../../output/chartfact_out when not present
[pd :wrte:ERR /0: 3m_chartfact:04/12/2021 18:42:11] Error 13 while opening FS Test file for
../../../output/chartfact_out SMAT
[pd :open:ERR /0: 3m_chartfact:04/12/2021 18:42:11] Unable to open sqlite db
../../../output/chartfact_out
[pd :open:ERR /0: 3m_chartfact:04/12/2021 18:42:11] Internal Init failed for SMAT
../../../output/chartfact_out
[pd :open:ERR /0: 3m_chartfact:04/12/2021 18:42:11] Init on secondary failed for SMAT
../../../output/chartfact_out
[pd :open:ERR /0: 3m_chartfact:04/12/2021 18:42:11] Error in saving outbound SMAT messages in
'../../../output/chartfact_out'
```

4 Copy the missing tables when you get the error `Unable to load TBL ***`.

Example error:

```
[msg :Tbl :ERR /0:results_mu_recv:04/13/2021 12:28:12] Unable to load TBL 'lab_reflex_orders.tbl'
[sms :sms :ERR /0:results_mu_recv:04/13/2021 12:28:12] Tcl error:
[sms :sms :ERR /0:results_mu_recv:--/--/---- --:--:--] \tmsgId\t= message0
[sms :sms :ERR /0:results_mu_recv:--/--/---- --:--:--] \tproc\t= 'table_filter'
[sms :sms :ERR /0:results_mu_recv:--/--/---- --:--:--] \targs\t= '{TABLENAME
lab_reflex_orders.tbl}
[sms :sms :ERR /0:results_mu_recv:--/--/---- --:--:--] {LOCATION OBR_4}'
[sms :sms :ERR /0:results_mu_recv:--/--/---- --:--:--] \tresult\t= 'unable to load table
'lab_reflex_orders.tbl''
[sms :sms :ERR /0:results_mu_recv:--/--/---- --:--:--] \terrorInfo: '
[sms :sms :ERR /0:results_mu_recv:--/--/---- --:--:--] unable to load table
'lab_reflex_orders.tbl'
[sms :sms :ERR /0:results_mu_recv:--/--/---- --:--:--] while executing
[sms :sms :ERR /0:results_mu_recv:--/--/---- --:--:--] "tbllookup $tablename $flddata"
[sms :sms :ERR /0:results_mu_recv:--/--/---- --:--:--] (procedure "table_filter" line 31)
[sms :sms :ERR /0:results_mu_recv:--/--/---- --:--:--] invoked from within
[sms :sms :ERR /0:results_mu_recv:--/--/---- --:--:--] "table_filter {MSGID message0} {CONTEXT
 sms_ib_data} {ARGS {{TABLENAME lab_reflex_orders.tbl}
[sms :sms :ERR /0:results_mu_recv:--/--/---- --:--:--] {LOCATION OBR_4}}} {MODE run} {VERSION
3.0}"'
```

For these errors, copy over the missing tables or copy/replace the entire `Tables` folder from the original `cgh_test` directory or zip. Keep the original permissions and attributes.

5 Convert the Windows/Mac files to Linux. This includes the output, tables, and `xlate` directories.

Infor uses DOS2 UNIX and endlines. Both skip binary files.

```
- endlines check -rv Xlate (provides report of files)
- endlines lf -vr Xlate (changes endlines in file to lf, ie crlf to lf)
- dos2unix -o *.* (changes endlines in file to lf, ie crlf to lf)
```

6 Delete the unavailable external procedure when receiving the error `IB reply TPS: external proc '****' not available`.

Example :For these errors, open NetConfig, select the thread `process_send_to_pyxis` and delete `pyxis_rde_ack` from the **TPS Inbound Reply** on the **Outbound** tab.

```
[nci :nci :ERR /0: cbord_cmd:--/--/---- --:--:--] pyxis_rde_send IB reply TPS: external proc
'pyxis_rde_ack' not available
[nci :nci :ERR /0: cbord_cmd:--/--/---- --:--:--] pyxis_mfn_out IB reply TPS: external proc
'pyxis_rde_ack' not available
[nci :nci :ERR /0: cbord_cmd:--/--/---- --:--:--] pyxis_ord_send IB reply TPS: external proc
'pyxis_rde_ack' not available
```

Chapter 27: Post-installation

A new license key is required when changing major versions. See Obtaining and setting the license key.

When the installation is run in silent mode from the command line, the control returns but the process is still running in the background. To determine if the installation has completed or not, check if the installation has finished running.

No message or prompt is shown if the installer aborts. In this case, you must check the log file to see the error.

Virus scan

If your computer has a virus scanner that runs in real time, then ensure that the scanner is not set to scan all files. These files should be excluded from scanning:

- `.jar` Java archive files
- `.class` files, if your virus scanner can identify these

The reason for this is that virus scanners treat all Java files as applets, and therefore as potential security threats. The system's `.jar` and `.class` files are data files, and pose no threat whatsoever. If your virus scanner is set to scan all files, then it examines every `.jar` file for viruses, which slows dialog box processing dramatically.

Validating the installation

A helloworld site comes as part of the installation, so that you can validate your installation was successful, in addition to running `hciverify`. This site shows some of the basic system functionality.

To validate your installation:

1. Open the IDE.
2. Using the**Server > Change** menu option, change to the helloworld site.
3. On the IDE, start Network Monitor.
4. Start the helloworld process. If everything goes green with the in thread in **`ineof`** status, then the installation was successful.

Setting the engine license

After installing the Client and Host Server with no security, you must set the license that enables your organization to run the system engine.

Perform these procedures to set the license that enables your organization to run the system engine:

1. From the Start menu, click **Programs > Accessories > Command Prompt** . This opens the **Command Prompt** dialog box.
2. Ensure that the command prompt shows the drive where you installed version 20.1.
3. Specify `setroot \cloverleaf\cis20.1\integrator\`*`root-directory sitename`*.
   - *`root-directory`* is the subdirectory for the system root.
   - *`sitename`* is the name you assigned to the default site that you created.

   For example: `setroot \cloverleaf\cis20.1\integrator testSite`.
4. After the license is obtained, place the `license.dat` license file into the `vers` directory of your Cloverleaf install directory at `%HCIROOT%\vers`.
5. Run `hcilictest` or `hcilicstatus` to verify if the license is valid.

Installation and errors log files

After installation, a log file is available under `%HCIROOT%`.

If the installer aborts during installation, for example, the product already exists on the machine, then no log is generated under `%HCIROOT%`. Instead, it is generated on the Desktop.

Errors and warnings are written to `integration_services_install.log`.

Security certificate files

Basic security users must obtain a public certificate file, a private key file, and a system user ID and password from your security administrator.

The two files must be placed in the `\client\certs` subdirectory of the directory where you installed the Client. You must use the system user ID and password to log in.

Global Monitor

If you are using Global Monitor, and it does not recognize the new installation, then you can add the new Cloverleaf version to Global Monitor.

This is accomplished on the **Preferences > Host Versions** page.

Chapter 28: Windows site promotion

Site promotion transfers the site configuration files from a previous version to the appropriate locations in the system directory tree. You must promote each site from the old version to the new.

Site names can be any combination of up to 19 lower-case letters, numerical digits, and underscore (_) characters. If any of your existing site names violate these rules, then you must rename the sites before promoting them.

Related to this process is database conversion. The conversion utility converts messages from a Raima database to a Sqlite database. See Database conversion.

1. Access the **Command Prompt** dialog box by selecting **Start > Run** to open the **Run** dialog box.
2. Specify **cmd** and click **OK**.
3. At the command prompt, set the `root` and `site` by running:

   ```
   setroot C:\cloverleaf\cis20.1\integrator
   ```

   Note: This example path may be different depending on specific choices made during the install process.
4. Use `showroot` to verify that you are set to the version 20.1 root. For example:

   ```
   showroot
   ```

   Output: `root is C:\cloverleaf\cis20.1\integrator`
5. Specify this command:

   ```
   hcirootcopy \cloverleaf\cis20.1\integrator
   ```

   The `hcirootcopy` program finds all the site directories and prompts you to confirm your intention to copy each site.
6. Specify **y** for yes.
7. When it asks if you require to continue, specify **y** or press **Enter**.

   If there is insufficient space in the new root for the old sites, then the program copies as many sites as possible. It then shows a warning and skips the excess sites.
8. After `hcirootcopy` is complete, you must `setroot` and `setsite` for each site you copied by specifying this command at the prompt:

   ```
   setroot C:\cloverleaf\cis20.1\integrator
   setsite sitename
   ```

   sitename is the name of the site where you run `hcixltconvert`.

Post site promotion

Test your configuration using the release's test tools and system engine processes. Do not proceed until you understand the release's bug fixes and functionality behavior in your environment.

If you do not already have a test site to test your production environment, then make a copy of your production sites. Then you can test the routing and processing configuration before using the new site in production mode.

Use the Network Configurator to update the thread configurations for test connections to avoid any conflicts with current production sites. For example, this might involve other protocol connections.

You can use `hcinetdiff` to identify Netconfig differences between your previous and current sites.

For example, to compare a previous production site named `qdxsite` with the new 20.1 configuration for `cissite`, specify `setroot \cloverleaf\cis20.1\integrator cissite` at the command prompt.

Then, specify one of these:

- `hcinetdiff \hci\root3.8.1P\qdxsite\NetConfig`
- `hcinetdiff \quovadx\qdx5.X\integrator\qdxsite\NetConfig`

In this example, you are comparing the NetConfig of the cis20.1 site called `cissite` to the NetConfig of the root3.8.1P or `qdx5.X` site. This is for versions up to 5.7.

Examine the output from `hcinetdiff`. Use `hcinetconfig` and other configuration tools to change the system's site configuration. Repeat until it is ready for production use.

When making these changes, keep the thread names identical in the old and new sites. Changing thread names may cause messages to stay in the recovery database and not complete their processing when bringing up the connections.

Making the cutover to production

Schedule a time for the production cutover and notify all users and those who manage the external connections. Ensure that all users understand that the engine processes shut down and the connections break during the actual cutover process.

To ensure there are no problems, before production cutover from your current production sites to version 20.1, you must test:

- Every site's hicrootcopied translates
- Tcl code
- Routing

This is the suggested procedure for going live, or cutting over your current production sites to the version 20.1 live or production environment.

Note: This procedure is for each site If you have more than one production site, you must `setsite` to each site and then perform these steps.

1. In the pre-20.1 production site, shut down all inbound production threads to the system server to prevent messages from coming into the database. Keep all outbound threads from the system server up and running so that all messages can cycle from the engine processes.
2. Log on as the `hci` user and run `hcidbdump -r` from the command line to see if any messages are still in the recovery database.

   Any listed data messages are still in the recovery database. You must wait until these messages have left the recovery database before shutting down the current production site's engine processes.
3. Now that the recovery database is empty, shut down the old pre-20.1 production sites engine processes and daemons.
4. At the command prompt, clear the new site’s runtime statistics by running:

   ```
   setroot \cloverleaf\cis20.1\integrator cissite
   hcimsiutil -Z
   ```

   In this example, `cissite` is the name of the production site to be addressed.
5. You can now start up your production processes.

Chapter 29: Portable Client

Included with the CIS build files is the Portable Client. This contains all client files in a `PortableIDE.exe` file. This file is much smaller than the client/server install.

This is installed similar to Cloverleaf:

1. Unzip the file to a folder. This contains the `PortableIDE.exe` file and an `integrator` folder.
2. Double-click `PortableIDE.exe` to launch the IDE.

Features of the portable Client:

- No installation is required.
- Pre-patched builds are provided for customers.
- Distributable to other desktops on the customer side.
- Clients with other patch levels can be run on the same machine. This is important for administrating remote servers that have other patch levels.

Portable Mac OS client documentation

Note: The Mac OS client is in beta.

When unzipping the `.zip` file on the MAC, you should use the finder, not the command line.

To access the online help documentation on the client, it must be installed on the server.

When the online help documentation is installed on the Cloverleaf remote server, the Portable Mac OS client launches the documentation in a web browser. If the client is connected to a remote server that does not have documentation installed, then a web browser session is launched. The page, though, is an error message.

Chapter 30: Cloverleaf SELinux module

The SELinux module provides an example of applying Cloverleaf security rules within an SELinux enforced system. It defines a maximum set of security policies to access the Linux system resources. It also defines ACL rules to access directories and files inside `HCIROOT`, ensuring the Cloverleaf functionality works.

This is provided in Linux's `HCIROOT/contrib` directory. It does not imply any security level after deploying the policy. You can customize the security rules that are based on this basic policy to meet your specific requirements in the process of Cloverleaf production implementation.

The SELinux policy package is developed based on the SELinux reference policy framework with policy version 30 under Centos 7 platform. The default policy supported in the RHEL/Centos platform is called the "targeted policy." The SELinux policy package can be built as a loadable policy module that can be loaded, working with the RHEL/Centos SELinux targeted policy.

For details about SELinux reference policy framework and loadable policy module, go to:

https://selinuxproject.org/page/NB_PolicyType#Types_of_SELinux_Policy

The RHEL/CentOS SELinux targeted policy document is available at:

https://www.centos.org/docs/5/html/Deployment_Guide-en-US/sec-sel-policy-targeted-oview.html

These SELinux files are installed in `HCIROOT/contrib/selinux`:

- `cloverleaf.te`

  SELinux type enforcement file that defines the enforcement policy rules for the SELinux subjects accessing the SELinux objects.

- `cloverleaf.fc`

  SELinux security context file that defines the default labeling rule for files and directories inside `HCIROOT`.

- `cloverleaf.if`

  SELinux interface file that defines the SELinux interface for other modules to use SELinux functionality in the reference policy framework.

Deploying Cloverleaf SELinux

To deploy the SELinux module in a targeted Linux system:

1 Log in as the root user. Then, use `yum` to install the SELinux packages:

```
yum install setools setools-console
yum install selinux-policy.noarch selinux-policy-devel.noarch
yum install policycoreutils-python-utils
```

2 As root user, edit `/etc/selinux/config`, changing the SELINUX configuration to `enforcing`.

```
SELINUX=enforcing
```

3 Restart the system. Use `sestatus` to confirm the SELinux current mode is `enforcing`.

```
sestatus
SELinux status: enabled
Current mode: enforcing
```

4 Go to *`HCIROOT`*`/contrib/selinux` and build the Cloverleaf loadable policy module using these Cloverleaf policy source files from the directory: `cloverleaf.te`, `cloverleaf.fc`, `cloverleaf.if`.

First, replace the *`HCIROOT`* stubs in `cloverleaf.fc` with the real path of the Cloverleaf installation. For example, if Cloverleaf is installed in `/opt/cloverleaf/cis6.2/integrator`, the command is similar to:

```
sed -e "s#HCIROOT#/opt/cloverleaf/cis6.2/integrator#g" < cloverleaf.fc > tmp
mv tmp cloverleaf.fc
```

5 Then, run this command to build the policy:

```
make -f /usr/share/selinux/devel/Makefile
```

When it succeeds, a `cloverleaf.pp` policy package is created. Insert this into the running SELinux policy to load the SELinux module.

6 Run `semodule -i` to insert the Cloverleaf module into the current running policy:

```
semodule -i cloverleaf.pp
```

7 Run `semodule -l` to check if the Cloverleaf module is inserted and the policy version is correct:

```
semodule -l |grep cloverleaf
  cloverleaf 1.0
```

8 Run the SELinux `semnage` management tool to add the SELinux `cloverleaf_u` user for Cloverleaf with the default SELinux `cloverleaf_r` role. `cloverleaf_r` is added by the SELinux module.

```
semanage user -a -R "cloverleaf_r" cloverleaf_u
```

9 Run `semanage -l` to verify the SELinux `cloverleaf_u` user was successfully added.

10 Change the SELinux `cloverleaf_u` user's default log-in context. To do this, edit `/etc/selinux/targeted/contexts/default_type` by adding this line to the end of the file:

```
cloverleaf_r:cloverleaf_t
```

This indicates that when the SELinux `cloverleaf_u` user with `cloverleaf_r` role logs-in on the system, the log-in shell gets the default SELinux type user with the`cloverleaf_t`.

There is also an alternative way to specify the various user contexts through another log-in context. This can override the definition in the `default_type` file.

For example, a `/etc/selinux/targeted/contexts/users/cloverleaf_u` file is created with this content:

```
system_r:local_login_t:s0      cloverleaf_r:cloverleaf_t:s0
system_r:remote_login_t:s0      cloverleaf_r:cloverleaf_t:s0
system_r:sshd_t:s0      cloverleaf_r:cloverleaf_t:s0
system_r:crond_t:s0      cloverleaf_r:cloverleaf_t:s0
system_r:xdm_t:s0      cloverleaf_r:cloverleaf_t:s0
user_r:user_su_t:s0      cloverleaf_r:cloverleaf_t:s0
user_r:user_sudo_t:s0      cloverleaf_r:cloverleaf_t:s0
system_r:initrc_su_t:s0      cloverleaf_r:cloverleaf_t:s0
```

11 `hci`/`hcitest`/`hcispt1`):

```
semanage login -a -s cloverleaf_u hci
```

Run this command to check the result:

```
semanage login -l
```

12 Run `restorecon` with the `-R` option to fix the default file context in *`HCIROOT`*. For example, if the Cloverleaf installation is in `/opt/cloverleaf/cis6.2/integrator`, then specify the command as:

```
restorecon -R /opt/cloverleaf/cis6.2/integrator
```

13 Log in to the system with the Cloverleaf Linux system user (for example, `hci`).

14 Run `id -Z` to verify that the user shell got the correct SELinux security context. For example:

```
id -Z
cloverleaf_u:cloverleaf_r:cloverleaf_t:s0
```

15 Now you can start from the `setroot` command and use Cloverleaf with SELinux enforced.

Troubleshooting Cloverleaf SELinux

You should monitor the `/var/log/audit/audit.log` log file.

SELinux denial and the associated system invocation information are logged to `/var/log/audit/audit.log`.

The `audit2allow` utility generates the SELinux policy's "allow" rules that are based on the AVC denial log:

```
grep cloverleaf audit.log | audit2allow -M cloverleaf_new
```

This generates a new `cloverleaf_new.te` enforcement file for the new policy rules and `cloverleaf_new.pp`. This can be loaded as an SELinux loadable module.

For example, a typical AVC denial log line could be:

```
type=AVC msg=audit(1523613065.537:791126): avc: denied { read write } for pid=29174 comm="lmclear"

path="/dev/pts/4" dev="devpts" ino=7 scontext=cloverleaf_u:cloverleaf_r:cloverleaf_dbtool_t:s0
tcontext=cloverleaf_u:object_r:user _devpts_t:s0 tclass=chr_file
```

This indicates the `lmclear` command with the runtime SELinux type `cloverleaf_dbtool_t` does not have read/write access to the SELinux object type `user_devpts_t`. This results in an "allow" rule in the generated enforcement file:

```
allow cloverleaf_dbtool_t user_devpts_t:chr_file { read write };
```

This can be added to `cloverleaf.te` or compiled to a new SELinux module and inserted into the system.

If these comments are before the rules, then you must run `restorecon` to fix the labeling of the corresponding SELinux objects. This is accomplished instead of adding the new policy rules to the system:

```
#!!!! The file … is mislabeled on your system.
#!!!! Fix with $ restorecon -R -v …
```

Chapter 31: User Account Control

Note: If hciuser already exists and the password is **gofish** (previous version's default password), then the installation uses hciuser with **gofish**.

Cloverleaf Integration Services can be installed with User Account Control (UAC) enabled on Windows:

- If the current user is hciuser, then CIS works well on Windows.
- If the current user is not hciuser, then the `setroot` command does not work. In this case, you must launch the command line using **Run as Administrator**.

For users with a large number of hciengines running in the background (for example, 120), increase the heap size using the registry entry:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems\Windows
```

This registry value is similar to this, all on one line:

```
%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,3072,512 Windows=On SubSystemType=Windows
ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3
ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off
MaxRequestThreads=16
```

Update the entry by changing:

- **3072** to **4096**
- **512** to **2048**

After making the change, restart your machine.

Chapter 32: Application adaptors

CAA-Direct is licensed together with CAA-WS as one extension. Both licenses are delivered together.

The `CAA_User_Guide.pdf` is included in the online help package.

Chapter 33: Secure practice

Based on security considerations, you should refer to these tasks to harden your system to run the Cloverleaf service.

Note: API Documentation (Swagger) should only be enabled for development and disabled for production.

Security mode enabled

To restrict the Cloverleaf IDE to only privileged users/operators, you must enable at least basic security mode using the Security Server.

This table show the online help locations for the applicable tasks:

Task	Online help location
For a basic understanding of security	**Cloverleaf Security**
To do access control for Cloverleaf users/operators and to enable Advanced Security mode with audit logging	**Cloverleaf Security > Upgrading and Downgrading security** and **Advanced security**
Password management	**Cloverleaf Security > Upgrading and Downgrading security > Security passwords**
Certificate management	**Certificate Manager**

Additional areas to secure include:

- Plug-in/Add-on management: You should scan any plug-in or add-on which is not officially shipped with Cloverleaf, using security testing toolsets. For example, IBM Appscan.

  Note: This applies to Java Driver and Java/Tcl/Python/JavaScript scripting.
- Monitoring: Monitoring and log analysis tools applied in the Cloverleaf runtime environment should be deployed.

  This ensures that no bad actors have modified files on the system.
- Protocol context:
  - Upload file should be restricted to administrators.
  - External connections should use TLS.
- It is best practice to deploy file system monitoring and remote logging for modified files to mitigate security risk.

Chapter 34: Database conversion

The `hcidbconvert` conversion utility converts messages from a Raima database to a Sqlite database.

Command usage is:

```
hcidbconvert [-p path] [-v] [-e]
```

- `-p` *`path`* is the file path where the exported Raima database files are located.
  If this option is not specified, then the `exec/databases` folder of the current site is used.
- `-v` is verbose mode.
- `-e` converts messages from error database.

Conversion steps for the error database

1. `setsite` to the site from which data is to be converted.
   Run command: `setsite $srcSiteName`
2. Export data from database `elog` to an ASCII text file.
   Run command: `dbexp elog`
   Files `elogctxmsg.txt`, `elogmsg.txt` and `elogmsg2000.txt` are generated under the current directory.
3. `setsite` to the site to which the data is to be converted. Run command: `setsite $destSiteName`
4. Copy the exported Raima ASCII text files to the `exec/databases` folder of the destination site.
5. Run `hcidbconvert` to convert error database data. Run command: `hcidbconvert -e`

Chapter 35: Data Integrator

Data Integrator supports ODBC (Open Database Connectivity), which is an API (Application Programming Interface). ODBC uses SQL (Structured Query Language) to provide a standard method of accessing data in various types of DBMS (Database Management Systems).

ODBC uses one set of code to manipulate multiple databases using a single, industry-standard API. A standard interface insulates the application from changes in the underlying network and DBMS versions.

Note: When using Message Archiving, AIX platforms require Data Integrator.

Third-party ODBC middleware

The third-party middleware converts the ODBC calls that are run in the application to a language understood by a particular DBMS. Network communications are handled by the ODBC middleware, by DBMS networking software, or by a combination of the two.

The ODBC middleware used in Data Integrator is supplied by DataDirect Technologies.

The Data Integrator ODBC functionality is a snap-on module available separately. This functionality consists of:

- Third-party ODBC middleware
- The ODBC Tcl extensions
- The cl-*feature* license key

The ODBC API has these components:

- Application (Data Integrator)

  This calls ODBC functions by Tcl callouts. It submits SQL statements and retrieves results.
- Driver Manager

  This loads the appropriate driver for the requested DBMS. The Driver Manager is the interface between the Data Integrator Tcl interpreter and the ODBC driver.
- Driver

  This processes ODBC function calls, submits SQL requests to a specific DBMS, and returns results. If necessary, then it translates the request into the form of SQL supported by the DBMS.
- Data source

This contains the data to be accessed, plus the operating system and network necessary to access it. This is also referred to as the DBMS.

Using the ODBC API

When the ODBC SDK has a C API, a set of Tcl extensions is provided for access to the ODBC interface from the system. A knowledge of Tcl code is required to use Data Integrator ODBC.

The Tcl extensions may change slightly between versions of the ODBC API.

Consult your database administrator to coordinate access and changes to data in the database. If necessary, then use Tcl extensions to write procedures that manipulate data.

Data Integrator ODBC components

Data Integrator ODBC includes:

- A dynamically loadable ODBC Tcl extension package.
- DataDirect Technologies DataDirect Connect.
- DataDirect Technologies documentation for the DataDirect middleware.
- License keys for the Tcl extension and DataDirect Technologies middleware.

ODBC Tcl extension

A major step in decoupling the ODBC functionality from the system was to turn the ODBC Tcl extension into a dynamically-loadable stubbed Tcl extension. `Mpexpr` and `ExtExpFilter` are the two dynamically-loadable Tcl extensions supplied with the system. To use these packages, issue a `package require xxxxx` command, where `xxxxx` is replaced by `Mpexpr` and `extexpfilter`, respectively. This dynamically loads the package code, if it has not already been loaded. Then, the commands in the package are used as if they were always available.

The same holds true for the odbc package, going one step further. As of Tcl 8.1, the capability was introduced to allow dynamically-loadable extensions to be loaded into Tcl interpreters of versions. These versions can be different than the version of which the Tcl extension was created. This was implemented by inserting stub libraries for core Tcl/Tk calls which handle any version-specific changes in these calls.

A Tcl extension that is built against Tcl 8.1 can run in a Tcl 8.4 interpreter. This enables decoupling of the ODBC extensions from the system.

One of the benefits of the decoupling is that the ODBC Tcl extensions are built with the appropriate version of the header files.

The ODBC Tcl extension is a dynamically-loadable stubbed extension. A necessary part of this step is the elimination of the SQLBindParameter, SQLBindCol, SQLGetData, SQLParamData, and SQLPutData features. These allowed system Msg and Dat objects to be bound to information sent to or retrieved from the DBMS.

As of Tcl 8.0, the ability of storing binary data in Tcl variables was added. The system Tcl extensions `msgset` and `msgget` previously moved data as null-terminated strings. They now move data as binary strings, along with all instances in the ODBC Tcl extension. The ODBC Tcl extension instances moves data back and forth from the Tcl extension layer to the Tcl layer. These changes ensure that binary data can be moved back and forth between system messages and databases.

cl-feature license key

All ODBC processing within the system is performed through the ODBC Tcl extension. The use of the ODBC Tcl extension is controlled through the ODBC license key in the system license file. If the `odbc` Tcl command is invoked without a valid `cl-aom-odbc-tcl` key, then it fails.

In addition, there is an ODBC license key which licenses the use of any DataDirect Technologies middleware product. This key is checked at the time a database connection is attempted using a DataDirect Technologies ODBC driver. Only users with licensed snap-on functionality receive the `cl-aom-odbc-mw` key.

Connect

Connect is a client-based solution.

On the client side, the machine on which the system is installed, there is an ODBC driver manager and a single database-independent ODBC driver.

The system architecture contains a separate ODBC driver for each database platform. Some of these drivers require installation of database vendor software on the client (system) machine. Other drivers, called built-in wire drivers, are designed to handle the network communication directly and require no database vendor client software. Neither type of driver requires any additional software on the server machine.

Connect and the ODBC Tcl extensions support version 3.5 of the ODBC API. Backward compatibility is maintained for ODBC 2.0 functions.

The Connect architecture contains a separate ODBC driver for each database platform. Some of these drivers require installation of database vendor software on the client machine. Other drivers, for example, built-in wire, are designed to handle the network communication directly. These require no database vendor client software. Neither type of driver requires any additional software on the server machine.

ODBC installation

The ODBC installation must take place before applying any CIS patch.

If ODBC is added after a CIS patch is installed, then the patches must be uninstalled and reinstalled.

Data Integrator installation

This is a universal installation program for the product Suite.

- If you have purchased only the Integrator, then you can install only that component of the Suite. Your license key enables only that component of the installation.
- If you have purchased the Suite, then select the appropriate component and follow the installation instructions provided in the corresponding component installation section.

Note: For CIS users who require ODBC, the ODBC installation must take place before applying any CIS patch. If ODBC is added after a CIS patch is installed, then the patches must be uninstalled and reinstalled.

Refer to the terms of your contract regarding your license agreement.

After installation, obtain the Data Integrator ODBC license keys, such as other required keys. You must provide your system server name and host ID. A new license key is required when changing major versions. See Obtaining and setting the license key on page 10

To configure data sources, view generic DataDirect Technologies documentation at:

https://www.progress.com/odbc/resources/documentation

These steps are required to install and set up Data Integrator ODBC:

1. Install the system.
2. Add the ODBC keys to the license file.
3. If you are installing DataDirect Connect and are not using a built-in wire ODBC driver, then you must install the database vendor's client software on the system machine. Contact Support for information on the database vendor's software requirements.
4. Install Data Integrator.
5. Configure your ODBC middleware and data sources.

Data Integrator installer types, modes, and space requirements

This table lists the installer types:

Type	Description
Global installer	This provides a list of available Cloverleaf Integration Suite products for installation. You can select one or more options.

Type	Description
Sub-installers	These can be launched singly, and not only from the Global Installer. These are separate installers for each available product. This makes it more convenient when installing only one product. For example, installing only the Cloverleaf Data Integrator.

This table lists the install modes:

Mode	Description
GUI	This uses the GUI.
Console	This uses the command line.
Silent	This does not show the GUI or messages during the process. You modify the response (properties) file before running it. There are comments for each item in the response file. See Running the installer in silent mode.

This table lists the minimum disk space requirements:

Platform	Requirements
Linux	`/tmp`: 45 MB `/integrator`: 103 MB
AIX	`/tmp`: 45 MB `/integrator`: 120 MB

Ensuring all Connect drivers are on driver list

To ensure that all drivers that are installed by Connect are shown on the driver list of the ODBC Data Source Administrator:

1. Install Connect.
2. From the **Control panel > Data Sources (ODBC) > Properties**, change the target to `%SystemRoot%\syswow64\odbcad32.exe`.

Data Integrator install location

If you have already installed version 6.x or later (up to 5.7), then install version 20.1 in the same directory path as the previous 6.x version.

For AIX platforms, the install path is user-defined. To find the current 6.x install directory, log in as the `hci` user and specify `echo $CL_INSTALL_DIR`.

Note: For versions earlier than 6.2, you must use `$QUOVADX_INSTALL_DIR`.

This gives output similar to `/quovadx/cis5.7`.

Installation steps

1. Verify you are logged on as the `root` user:
   AIX/Linux/Windows: `whoami`
2. Run the install script. To install the system through the Global Installer, specify `./CISSuite.sh`.
   You can also run the individual installers, without using the Global Installer.
   See Data Integrator installation on page 96.
3. Click **Next**. The **License Agreement** dialog box is displayed. To continue with the installation, you must accept the agreement.
4. Click **Next**. A dialog box is displayed for you to select the directory in which to install Data Integrator.
   Note: You can additionally install on a directory other than the default.
5. Click **Next**. The **Choose Product** dialog box is displayed. Select **`Cloverleaf Data Integrator`**.
6. Click **Next**. A dialog box is displayed for your to select the root path for the ODBC drivers. You can install on a directory other than the default.
   Note: Data Integrator cannot be used unless it is installed under `$HCIROOT`.
7. Select or specify the directory path that you would prefer to use for the *`user-defined`* file system. For example, `/cloverleaf/cis20.1/integrator`.
8. Click **Next**. The **Pre-Installation Summary** dialog box is displayed.
9. Click **Install** to begin the installation.
10. After installation is completed, the **Installation Complete** dialog box is displayed. Click **Done** to finish.

Running the installer in silent mode

The response file that comes with the Installer is only a sample with comments that you can use as a template. You should modify the response file according to your requirements before running the installer in silent mode.

Before launching the Global Installer in silent mode, ensure these have been modified:

- Response file for the Global Installer
- Sub-installers for those products that are selected in the Global Installer

The response file is located in the same folder as the `.sh` file. The installer's `.bin` files are located under the `InstallSupport` folder. This avoids the possibility of launching the `.bin` files by mistake.

Do not change the name or location of the response files of the sub-installers if you are launching from the Global Installer in silent mode.

If you are launching the sub-installer individually, then you can use another response file name. When running the command, you only are required to specify the response file name with the full path when using the `-f` option.

Sub-installer

The Data Integrator sub-installer can be launched singly, and not only from the Global Installer. This makes it more convenient when installing only the Data Integrator.

To launch the Data Integrator Installer (under the `DataIntegrator` folder):

- GUI mode: `./ODBCInstall.sh`
- Console mode: `./ODBCInstall.sh -i console`
- Silent mode: `./ODBCInstall.sh -i silent -f $FULL_FILE_PATH/disilent.properties`
  - `$FULL_FILE_PATH` is the full path to the response file.
  - `disilent.properties` is the response file that resides in the same location as the `.sh` file.

Global installer

To launch the Global Installer (under the `root` folder):

- GUI mode: `./CISSuite.sh`
- Silent mode: `./CISSuite.sh -i silent -f $FULL_FILE_PATH/cissilent.properties`
  - `$FULL_FILE_PATH` is the full path to the response file.
  - `cissilent.properties` is the response file that resides in the same location as the `.sh` file.

Chapter 36: Security Server

Security Server (advanced) is a complex feature that includes these components:

- One or more host servers with Advanced Security can process requests submitted by Clients. Before acting on a request, Host Server communicates with Security Server to verify the permissions of the person who is logged onto the requesting Client.
- One, and only one, Host Server with Advanced Security runs the security management tools that an administrator uses to manage user certificates and permissions. The administrator can manage these centrally from one server.

Additional notes to remember are:

- All Clients must have certificate files that authenticate their users.
- The Security Server can be on the same machine as Cloverleaf.
- Using Advanced Security requires the installation of the Security Server. You must complete the credentials licensing process before installing or upgrading to Advanced Security.
- The AIX installation program does not create a file system. The *user-defined* file system is created by the user. You can also use an existing file system, as long as it has the required free space for server installation.

  See AIX user-defined file system on page 25.
- Record the unique customer name and password that are given to you by Infor.
- Ensure that the customer certificate files are located in a directory on the computer where you plan to install Security Server. The installation program asks for the location of these certificate files, so ensure you know their location. Contact your security administrator for the necessary certificate files.
- The Microsoft Visual C++ Redistributable Packages for Visual Studio 2013 is required before installing on Windows 10. This package installs the required runtime components of Visual C++ libraries. This is required for both Client and server installs if the necessary files are not detected on the target machine. You must install the package before installation can be completed.

  This package is available at:

  http://www.microsoft.com/downloads/details.aspx?familyid=a5c84275-3b97-4ab7-a40d-3802b2af5fc2&displaylang=en

  This link is valid as of the release date. If this link does not work, then it might have been updated. In this case, contact Support for the latest address.
- InstallAnywhere is used to generate installers for the various platforms. During installation, the first step of every installer created by InstallAnywhere is to self-extract its contents to a temporary directory. See Changing the /tmp location on page 25.

Security Server components

Security Server is a complex feature that includes three major components:

- Using Advanced Security requires the installation of the Security Server.
- One or more host servers with Advanced Security processes requests that are submitted by Clients. Before acting on a request, the Host Server communicates with Security Server. This verifies the permissions of the person who is logged on to the requesting Client.
- One, and only one, Host Server with Advanced Security runs the security management tools that an administrator uses to manage user certificates and permissions. The administrator manages these centrally from one server.

All Clients must have certificate files that authenticate their users.

CIS and Security Server installation

The Security Server can be on the same machine as Cloverleaf.

1. Install Cloverleaf without security.
2. Run `hcihostid` for the license key. Record the license key for your files.
3. Run Certificate Manager and go through the certificate request procedure.
4. With the license key and the certificate request:
   a. For the Host Server license, you must go through the **Infor Support Portal > Resources > Request a software key > Key Request**. Follow the prompts to submit the request. There is a 48 hour turn around.
   b. After the license is obtained, place the `license.dat` license file into the `vers` directory of your Cloverleaf install directory at `%HCIROOT%/vers`.
   c. For the certificates, you must go through the Infor Support Portal and create a case to have the certificate files generated for you. Ensure to provide the name in which the certs are required to be generated.
5. Install the Security Server. This requires the location of the CA certificates. Contact your security administrator.

   For specific AIX installation steps, see Security Server AIX and Linux installation.

   For specific Windows installation steps, see Security Server Windows installation.
6. Run `hcihostid` for the license key. Record the license key for your files.
7. Request a license. See step 4.
8. Configure the Host Server for Advanced Security.

   This requires:

   - Running Security Server
   - Customer CA certificates
   - Decision on which Host Server has the security management tools

The customer CA certificate password that you received from your administrator, along with the administrator certificate password entered during Advanced Security installation. These must be stored in a safe place.

9 Open the ACL Role Manager and log in as administrator. This is located at: **Start > All Programs > Infor Cloverleaf Integration Suite > ACL Role Manager**

At this point, you can:

- Create new system roles
- Assign permissions to users and /or roles

See Advanced security administration.

Chapter 37: Security Server migration

The Security Server Migration Wizard guides you in migrating data from Security Server:

- Version 6.1 to 19.1 and above
- Version 6.2 to 19.1 and above

Before beginning the migration, you must shut down Security Server 6.1/6.2 and 19.1/20.1. The wizard removes all data in Security Server 6.1/6.2 before migration. This cannot be rolled back.

Predefined ACLs and users are migrated.

Note: Only the Security Server database is migrated. User certificates and key files that are on the Host Server are not migrated.

You can also migrate using the `hcissmigration` command. This is located at `%HCIROOT/clgui/bin`.

Migrating an older CA to the current version

Starting in CIS 20.1, the root CA that is shipped with Cloverleaf is now updated to a product-based name.

Users who have a CA from an earlier version must follow this process to migrate their CA for use with 20.1 security server or host server, without re-issuing all of their user certificates.

To synchronize the issuer of an older customer CA `CUSTOMER-cert.der` to a new root CA `Cloverleaf-cert.der` :

1. Send a request ticket to the Support team to update the old customer CA, for example, `CUSTOMER-cert.der`.
2. Back up the old `hie-cert.der` and `CUSTOMER-cert.der` located under `server/certs` on the old host server.
3. Downgrade the old host server to "none" security mode after receiving the new `CUSTOMER-cert.der` and `Cloverleaf-cert.der`.
4. Copy `Cloverleaf-cert.der` and the new `CUSTOMER-cert.der` to `server/certs`.
5. Delete `server/certs/keystore_clserver.jks` and `server/certs/ truststore_clserver.jks`.
6. Upgrade the old host server to "advanced" security mode.

Chapter 38: Security Server pre-installation

Before beginning an Advanced Security installation, you must have already performed a no security Host Server installation.

Note: Using Advanced Security requires the installation of the Security Server. You must complete the credentials licensing process before installing or upgrading to Advanced Security.

To complete the Advanced Security installation, you must have:

- The downloadable product zip file.
- The unique customer name and password that were assigned to your system by Infor.
- The necessary certificate files. Ensure that the customer certificate files are located in a directory on the computer where you plan to install Security Server. The installation program asks for the location of these certificate files, so ensure you know their location.

  To obtain these files, you must go through the Infor Support Portal or Concierge and create a case to have the certificate files generated for you. You must provide the name in which the certs are required to be generated. A security upgrade can be completed only if these two files have been copied to your computer.
- The server name and location of the directory where you copied the certificate files. This information is required during installation.
- For installations on Windows, the Visual C++ Redistributable Package for Visual Studio 2013 (x64) is required before installation.

  This package installs the required runtime components of Visual C++ libraries. This is required for both Client and server installs if the necessary files are not detected on the target machine. The system is built on Visual Studio 2013, which makes all binaries depend on the Visual C++ 2013 Redistributable Package.

  You must install the package before installation can be completed.

  This package is available at: https://www.microsoft.com/en-us/download/details.aspx?id=40784

  This link is valid as of the release date. If this link does not work, then it might have been updated. In this case, contact Support for the latest address.

hciuser and new user accounts

During installation, the Installer creates the hciuser account. The password that is created/used depends on the type of installation.

Information on hciuser is found at:

- hciuser on page 53
- Modifying hciuser on page 53

For information on creating a new user account, see Creating a new user on page 54.

Security Server installation resources

These resources are necessary for a successful installation:

- Security Server parameters:
  - Security Server host name
  - Host ID
  - Security Server certificate. See:

    Security Server AIX and Linux installation

    Security Server Windows installation on page 107
  - Customer CA certificate
- Host Server parameters:
  - Host ID
  - Customer CA certificate
  - Host server certificate
  - User certificate

Installing or updating Cloverleaf

If there is no previous system installation, then the installation creates hciuser and uses the password `G0neF1sh1ng`.

When updating a Cloverleaf instrallation, if hciuser already exists and the previous version's default password is `gofish`, the installation uses hciuser with the password `gofish`.

Passwords for Advanced Security

During Advanced Security installation, you are prompted for several passwords that are required to link Advanced Security with your system. You are also prompted to authorize access to the Host Server and to the security management tools.

All necessary passwords are created by your security administrator. These passwords and other items, such as port numbers, hostnames/numbers, and location of certificates, must be safely recorded for future reference and kept in a secure location.

Having the administrator issue passwords instead of Infor ensures that the private key and passwords are never exposed. Request and certificate files, when transmitted, only contain public information.

Only your organization has access to any private information and passwords.

Obtain the password that is used to authorize access to certificate files that are maintained by the Security Server. This is obtained from the person responsible for system security in your organization.

Note: The customer certificates are the only ones created by Infor and are the only ones required for installation. All other certificates are created at installation time.

Before Advanced Security upgrade

Ensure you remember the server name and location of the directory where you copied the certificate files. This information is required during installation.

The necessary user IDs and passwords are:

- The customer name and password that are assigned to your site by Infor.
- The Host Server password that is assigned by your organization. This authorizes access to the certificate files that are maintained by the Host Server.
- The administrator certificate password. This is any password you require to use to authorize access to the administrator certificate.

See your security administrator for the necessary certificate files.

Chapter 39: Security Server Windows installation

Security Server enables your system to take advantage of advanced security. This provides the ability to specify which system functions can be performed by individual users.

There can be multiple host servers, each running on another computer system and each connected to its own set of clients. There can be only one security server. Every Host Server that uses Advanced Security must be connected to the same Security Server.

Note: A Host Server running on Windows can be connected to a Security Server running on AIX.

This is a universal installation program for the product Suite.

- If you have purchased only the Integrator, then you can install only that component of the Suite. Your license key only enables that component of the installation.
- If you have purchased the Suite, then select the appropriate component and follow the installation instructions provided in the corresponding component installation section.

Windows sub-installers

The Security Server sub-installer can be launched singly, separate from the Global Installer. This makes it more convenient when installing only the Security Server.

To launch the sub-installer (under the `SecurityServer` folder):

- GUI mode: `SSInstall.bat`
- Console mode: `SSInstall.bat -i console`
- Silent mode: `SSInstall.bat -i silent -f %FULL_FILE_PATH%\sssilent.properties`

  `%FULL_FILE_PATH%` is the full path to the response file and `sssilent.properties` is the response file that resides in the same location as the `.bat` file.

Running the Windows Security Server installer in silent mode

The response file that comes with the Installer is only a sample with comments that you can use as a template. You should modify the response file according to your requirements before running the installer in silent mode.

Before launching the Global Installer in silent mode, ensure these have been modified:

- Response file for the Global Installer
- Sub-installers for products that are selected in the Global Installer

The response file is located in the same folder as the `.bat` file. The installer's `.exe` files are located under the `InstallSupport` folder. This avoids the possibility of launching the `.exe` files by mistake. Do not change the name or location of the response files of the sub-installers if you are launching from the Global Installer in silent mode.

If you are launching the sub-installer individually, then you can use another response file name. When running the command, you must specify the response file name with the full path when using the `-f` option.

Windows installation steps

1. Download the product and un-zip to a local folder.
2. Log-on as **`admin`** on the local domain.
3. After selecting an installation option, GUI, console, or silent, click the `.bat` file to begin.
4. Click **Next**. The **License Agreement** dialog box is displayed. You must accept the terms of the License Acknowledgment to continue with installation.
5. Select **I accept** and click **Next**.
6. Click **Next** to select the installation location.
7. Select the drive and directory. The default destination folder is `C:\cloverleaf`.

   You can also specify a directory path. If the path does not exist, then the installation asks if you require to create the directory. If a location is selected where you do not have write permission, then the installation displays an error message.
8. Click **Next**. A dialog box is displayed for product selection. It is not recommended to install the same version of the system and Security Server on the same machine.
9. Select **Security Server** and click **Next**.
10. The next dialog box asks if you have your Customer CA certificate. Contact your CA (Certificate Authority) or security administrator if you do not have a Customer CA certificate.
11. Click **Next**. The next dialog box is for installing the online documentation. The default is **Yes**.
12. Click **Next**. The **Pre-Installation Summary** dialog box is displayed.
13. Click **Install**. This file extraction process begins.

    Note: After starting the installation process, do not minimize the Installer. When re-installing Security Server under the same directory, Security Server has already been uninstalled under this directory. The

Database Already Exists dialog box is displayed. If you minimize the Installer window when the progress bar is running, then the Installer hangs before the**Database Already Exists** dialog box is displayed.

The reason is that any dialog box is displayed if the Installer window is minimized. The Installer hangs because it is waiting for input.

If you do minimize the Install window and the process hangs, then press **Enter** or use **Alt** + **O** to get past the dialog box.

14 If an existing database is detected, then a message is displayed asking you to refresh the database.

If you are re-installing Security Server without cleaning up the install folder, then there are remaining database files that were not removed during uninstallation. These files were created after installation. The installer prompts you for confirmation to refresh the database.

- If you select **Yes**, then the database files are overwritten with a new database, which means the existing data is removed.
- If you select **No**, then the installer skips creating the database and the existing data remains. If there are any schema changes between versions, then the old database might not work.

15 The next dialog box asks you to specify the location where the certificate files have been placed. You can accept the default location or select **Choose** to specify another location.

Specify the **Customer Name** and **Password**.

16 Click **Next**. The **Security Server Certificate Password** dialog box is displayed.

For **Password**, specify the password that authorizes access to certificate files that are maintained by the Security Server. This password is obtained from the person who is responsible for system security in your organization.

17 Click **Next**. The installer checks for other return values. You are prompted for the password if `hciuser` is found on the target machine and the password is not one of the defaults. If the `hciuser` password has been changed from the default, then the support tools cannot determine the password. This creates the service with the correct log-in credentials.

If the installer finds an existing `hciuser`, then the **Enter Password** dialog box is displayed for you to specify the changed `hciuser` password.

18 Click **Next**. The**License Key** dialog box is displayed.

For further information on how to obtain the license key, see Obtaining and setting the license key. You must have a separate license for the Advanced Security feature on each Host Server in your system.

19 Click **Next**. An information dialog box is displayed to remind you to refer to the release notes.

20 Click **Next**. The **Installation Complete** dialog box is displayed.

If any errors happened during installation, then refer to the installation log at:`\cloverleaf\cis20.1\integrator\security_server_install.log`

21 You must restart your computer before you can use Security Server. Select **Yes** and then click **Done** to restart.

22 The online help files are separately installed.

Chapter 40: Security Server AIX and Linux installation

Security Server enables your system to take advantage of advanced security. This provides the ability to specify which system functions can be performed by individual users.

The system can have multiple host servers, each connected to any number of clients. There can be only one Security Server.

A Host Server running on Windows can be connected to a Security Server running on a supported AIX platform.

InstallAnywhere reminds you to obtain a license key for Host Server. It also supplies the machine's host ID that is necessary to obtain the required license key.

Record the host ID for use when you request a Security Server license key.

Universal installation

This is a universal installation program for the product Suite.

- If you have purchased only the Integrator, then you are entitled to install only that component of the Suite. Your license key only enables that component of the installation.
- If you have purchased the Suite, then select the appropriate component and follow the installation instructions provided in the corresponding component installation section.

Refer to the terms of your contract regarding your license agreement.

AIX and Linux sub-installers

The Security Server sub-installer can be launched singly, separate from the Global Installer. This makes it more convenient when installing only the Security Server.

To launch the sub-installer (under the `SecurityServer` folder):

- GUI mode: `./SSInstall.sh`
- Console mode: `./SSInstall.sh -i console`
- Silent mode: `./SSInstall.sh -i silent -f $FULL_FILE_PATH/sssilent.properties`

  Where `$FULL_FILE_PATH` is the full path to the response file and `sssilent.properties` is the response file that resides in the same location as the `.sh` file.

AIX and Linux Security Server installer silent mode

The response file that comes with the Installer is only a sample with comments that you can use as a template. You should modify the response file according to your requirements before running the installer in silent mode.

Before launching the global Installer in silent mode, ensure the response file has been modified for:

- Global Installer
- Sub-installers for those products that are selected in the Global Installer

The response file is located in the same folder as the `.sh` file. The installer's `.bin` files are located under the `InstallSupport` folder. This avoids the possibility of launching the `.bin` files by mistake. You should not change the name or location of the sub-installers response files if you are launching from the Global Installer in silent mode.

If you are launching the sub-installer individually, then you can use another response file name. When running the command, you must specify the response file name with the full path when using the `-f` option.

The install script then prompts you to verify the user ID and password. Press **Enter** to accept the default answer **`y`** (yes).

Installing Security Server on AIX and Linux

InstallAnywhere reminds you to obtain a license key for Host Server, and supplies the machine's host ID that you use to obtain the key. Record the host ID for use when you request the Security Server license key.

1. Verify that you are logged on as the `root` user.
   For AIX and Linux, use `whoami`.
2. To install the Security Server through the Global Installer, specify `./CISSuite.sh`.
3. Click **Next**. The **License Agreement** dialog box is displayed. You must accept the terms of the License Acknowledgment to continue with installation.
4. Select **`I accept`** and click **Next**.
5. Click **Next**. A dialog box is displayed for you to select the installation location. You can additionally install on a file system directory path other than the default
6. Select or specify the directory path that you prefer to use for the user-defined file system. Ensure there is enough free space in the file system.
7. Click **Next**. A dialog box is displayed for product selection. It is not recommended to install the same version of the system and Security Server on the same machine.
8. Select **Security Server** and click **Next**.
9. Specify if you have your Customer CA certificate. Contact your CA (Certificate Authority) or security administrator if you do not have a Customer CA certificate.
10. Click **Next**. The next dialog box is for installing the online documentation. The default is **Yes**.
11. Click **Next**. The **Pre-Installation Summary** dialog box is displayed.

12 Click **Install** to begin the file extraction process. After starting the installation process, do not minimize the Installer.

When re-installing Security Server under the same directory, the **Database Already Exists** dialog box opens. If you minimize the Installer window as the progress bar is running, then the Installer hangs before the **Database Already Exists** dialog box opens.

The reason is that any dialog box is invisible if the installer dialog box is minimized. The installer hangs because it is waiting for input.

If you do minimize the Install window and the process hangs, then press **Enter** or use **Alt+O** to get past the dialog box.

13 If an existing database is detected, then after the files are extracted a message dialog box opens asking if you require to refresh the database.

If you are re-installing Security Server without cleaning up the install folder, then database files are left over which were not removed during uninstallation. These files were created after installation. In this case, the installer prompts you for confirmation to refresh the database.

- If you select **Yes**, then the database files are overwritten with a new database. This removes the existing data.
- If you select **No**, then the installer skips creating the database and the existing data remains. If there are any schema changes between versions, then the old database might not work.

14 Click **Yes** or **No**.

15 Specify the location where the certificate files are located. You can accept the default location or select **Choose** to specify another location.

16 Specify the **Customer Name** and **Password**.

17 Click **Next**. The **Security Server Certificate Password** dialog box is displayed.

For **Password**, specify the password that is used to authorize access to certificate files that are maintained by Security Server. This password is obtained from the person responsible for system security in your organization.

18 Click **Next**. The **License Key** dialog box is displayed.

For further information on how to obtain the license key, see Obtaining and setting the license key. You must have a separate license for the Advanced Security feature on each Host Server in your system.

19 Click **Next**. An information dialog reminds you to refer to the release notes.

20 Click **Next**. The **Installation Complete** dialog box is displayed.

If any errors happened during installation, then refer to the installation log at: `/cloverleaf/cis20.1/integrator/security_server_install.log`.

21 Click **Done** to finish.

22 Record the host ID for when you request a Security Server license key.

23 Exit the script utility. To quit the installation script utility, use the `exit` command. This shows the notice:

```
Script , file is /tmp/typescript
```

Note: `/tmp/typescript` is the log file that was created during installation. This is a record of everything you entered and everything that is shown by the install script.

If you do not have your license key, then the install tells you that you do not have a license file installed for this release. It then gives you instructions to obtain your license key.

The install updates your configuration files and asks you if you would prefer to run `hciverify`. If you select **yes**, then you get `hciverify` output.

24 The online help files are separately installed.

Chapter 41: Security Server post-installation

After installing Security Server, before Security Server and Host Server can be run, your organization must have the correct license keys. These can be obtained from your Account Manager.

After the license is obtained, place the `license.dat` license file into the `vers` directory of your Cloverleaf install directory at `%HCIROOT%/vers`.

A new license key is also required when changing major versions. See Obtaining and setting the license key.

Errors and warnings log file location

Errors and warnings are written to `security_server_install.log`.

After the installation, you must correct any errors, or report them to Support.

Some errors can be fixed using these commands (you must be logged on as `hci` to run `hciverify`):

```
exec ksh
export FPATH=/integrator/kshlib
setroot /root <version>/integrator/ (where <version> is the complete version number)
hciverify
```

Making a bootable Security Server system backup

Note: You must complete this step! Using a backup, you can to restore your system to a known state if it crashes because of a hardware or operating system problem. Do not use any backup created except under the direction of Support. Using a backup incorrectly can result in lost data.

Keep this backup in a safe location.

Use clean tape/media for the backup you are about to create.

- Follow the procedures for your operating system to make a bootable system image backup. Label the tape as a "post-Security Server install backup," write-protect it, and store in a safe place. Keep it as a permanent archive.
- Follow the procedures for your operating system to make backups of file systems outside of the root volume group.

For further help with system administration, see the documentation for your AIX system or consult with your system administrator.

Virus scans

If your computer has a virus scanner that runs in real time, then you must also ensure that it is not set to scan all files. These files should be excluded from scanning:

- `jar` (Java archive) files
- `class` files

  This depends on if your virus scanner can identify these.

Virus scanners treat all Java files as applets, and therefore as potential security threats. The system `.jar` and `.class` files are data files. These pose no threat whatsoever, but if your virus scanner is set to scan all files, it examines every `.jar` file for viruses. This could appreciably slow down dialog box processing.

Restarting the Security Server and starting Advanced Security

You must restart the Security Server after the install to update the `.ini` files.

Log-on as `hci` and specify `hciss -s s` to start the Host Server.

Starting up Advanced Security

Start Advanced Security in this order:

1. Start Security Server.
2. Start Host Server.
3. Start the Client GUIs.

Default site definition

When a Host Server is installed, a default site should be created and registered.

If no such default site was correctly registered during Host Server installation, then you must create one the first time you log-on. To do this:

1. Run `/cis20.1/integrator/clgui/bin/hciguisiteinit`.
2. Log on to the **Site Init** dialog box with the administrator certificate.

3 Create a new system site.
4 Exit the **Site Init** dialog box.

Using the Site Init dialog box

When you are running Advanced Security and add a site on the **Site Init** dialog box, the information for the new site is persisted into Security Server. This is located under the current host ACL entry.

If `acl_shared_host=` is set in `server.ini` on the Host Server, then a message is sent when you initialize a new site on the **Site Init** dialog box.

Click **OK** to continue to initialize the site or click **Cancel** to cancel the creation.

Note: For High Availability environments, we recommended that you create a new site on the primary server instead of the backup server.

Chapter 42: Advanced security administration

After Advanced Security has been installed on a system, the security administrator can begin using it to authenticate users. It can also specify the system functionality authorized to each user.

Advanced security administration can only be performed at the computer that runs the Host Server where the system security management tools have been installed.

1. From the `/clgui/bin` subdirectory of the system root directory, run `hcicertmgr`, using the administrator certificate to log in to Certificate Manager.
2. Issue new user certificates. Certificate Manager generates the certificate files in the `/cis20.1/integrator/server/certs` directory.

   Note: The certificate files for each user must be manually copied to the `/client/certs` directory of that user's computer. This is the computer that runs the client that uses the certificate.
3. From the `/clgui/bin` subdirectory of the system root directory, run `hciaclrolemgr`, using the administrator certificate to log in to ACL/Role Manager.

   The **ACL/Role Manager** dialog box should list the system users whose certificates you issued in Step 2.
4. At this point, you can:
   - Create new system roles and identify their members, users, and other roles, on the **Roles** tab.
   - Expand the tree of system functionality nodes on the **ACL** tab, and assign permissions to users and roles. Usually, the most efficient approach is to assign permissions to roles, and then add users to those roles. You can later grant or deny specific permissions on an exception basis, and add or remove users as required.

   It is usually best to define permissions for both roles and users at the highest-level node first, because they are inherited from the top down. Then you can tailor the permissions for lower-level nodes as required. For example, permissions that are granted to the administrator at the root node are automatically applied to all nodes that belong to that root. Those same permissions can also be explicitly denied at any member node.
5. After certificates have been issued, disseminated, and permissions have been assigned, end users can log in to the system and perform the appropriate tasks.

Default accounts

Note: This feature is only available in Advanced Security.

Default users, roles, and ACLs are imported from a user-supplied template through a command-line interface on the Security Server. This template contains user names, passwords, and roles with access control lists for each.

Use `hci_ACL.xsd` to do basic validation.

Issue `hciaclimport` on Security Server to store predefined ACLs into the database.

The server interface is command-line only.

Users, roles, and ACLs are defined in a template file. This file is located at `$HCIROOT/templates/hci_ACL_template.xml`.

Although the Host Server is upgrading to advanced mode, matching ACLs are applied to the resources that are associated with that Host Server.

Predefined ACLs only take effect for future upgrades. They do not change the permissions of existing resources. You must downgrade and then upgrade the Host Server to apply new predefined ACLs to current resources.

Use `hcigencerts` to generate certificates on the Host Server.

Installation items

The Host Server is installed with these items:

- Command: `hcigencerts`
- Template file: `$HCIROOT/templates/hci_ACL_template.xml and $HCIROOT /templates/hci_ACL.xsd`

The Security Server is installed with these items:

- Command: `hciaclimport`
- Template file: `$HCIROOT/templates/hci_ACL_template.xml and $HCIROOT /templates/hci_ACL.xsd`
- Mapping file: `$HCIROOT/security/aclmapping.xml`

Security Server default account

Note: This feature is only available in Advanced Security.

This feature provides a way to configure other levels of access rights, where you can:

- Define users, roles and ACLs in a template file (located in `$HCIROOT/templates/hci_ACL_template.xml` of installation path).
- Use `hci_ACL.xsd` to do basic validation.
- Issue `hciaclimport` on Security Server to store predefined ACLs into the database.

When a CIS instance's Host Server is upgrading to advanced mode and matched ACLs are found, they are applied on resources that are associated with that instance's host server.

Note: Predefined ACLs only take effect for future upgrades, and do not change the permissions of existing resources.

If a Host Server has already been upgraded, then you can still apply new/updated templates.

You can then use `hcigencerts` to generate certificates on the Host Server.

Default roles

This table lists the permissions for the default roles. These are located in `hci_ACL_template.xml`.

Username	Role	Permissions	Description
ZooKeeper	Cloverleaf administrator	Root level application Root level config Site level application Site level command Site level hcicmd Site level config	Full permissions including, but not limited to: • Security audit • Security configuration • Command allow list administration • User management
LionTamer	Cloverleaf security Admin-lite	Root level application Root level config Site level application Site level command Site level hcicmd Site level config	Cloverleaf developer with user admin. For example,creating and editing users without the CA password.
AnimalFeeder	Cloverleaf developer	Root level config Site level application Site level command Site level hcicmd Site level config	Cloverleaf interface developer. All IDE permissions.
Food	Cloverleaf operator	NetMonitor	Limited account for traditional operations personnel. Start/stop processes and threads.

Templates for these users are installed with cloverleaf. To add these users to the Security Server, you must:

1. Review the template to ensure the permissions are correct.
2. Specify the unique user IDs and passwords for the desired user accounts into the template file.
3. Import the template file before upgrading the Security Server's security level.
4. Perform the security upgrade.

The template file is located at `$HCIROOT/templates/hci_ACL_template.xml` and `$HCIROOT/templates/hci_ACL.xsd`.

Defining users, roles, and ACLs

1. Define users, roles, and ACLs in the template file. This is located in `templates/hci_ACL_template.xml` of the installation path.
2. Optionally, you can run `hciaclimport -b databasePath` to back up the database.
3. Run `hciaclimport -f <filePath> -p password [-b databasePath] [-r]` to import the predefined users, roles, and ACLs which are defined in the template file. Use the `-b` option to simultaneously back up the database.
4. Create the sites. Ensure that all sites are ready before upgrading, since only predefined ACLs are being applied to real resources during the upgrade.
5. Run `hcisecupgrade` to upgrade the Host Server to Advanced Security.
6. Run `hcigencerts` to generate certs. You can do this step at any time, even when you have not gone through the previous steps.
7. After you have modified the `templates/hci_ACL_template.xml` file:
   a. Run `hciaclimport` to update it.
   b. Downgrade the Host Server to no security.
   c. Run `hcisecupgrade` again. At this point, the updated ACLs are shown.

Configuration steps

1. A template file is provided to predefine users, roles, and their permissions. The command implements the predefined data.
2. Create users and roles. Using the command, the predefined permissions are stored in the database.
3. Generate the certificate.
4. If matching predefined permissions are found when upgrading security, then they are created on the matched ACL tree node.
5. Use the command to manage permissions, so you can update roles and permissions.

hcisecupgrade usage

Note: This command only supports an upgrade on the Host Server from none to advanced mode.

```
hcisecupgrade -cacertpath path -caname name
-capass password -hostpass password -adminpass password
-sshostname host [-ssport port] [-l log]
```

- `-cacertpath path` is the CA public certificate location.
- `-caname name` is the CA certificate name.
- `-capass password` is the CA password.
- `-hostpass password` is the password of Host Server.

- `-adminpass password`is the password of default user administrator.
- `-sshostname host` is the host name of Security Server.
- `-ssport port` is the port of Security Server.
- `-l log` is the log file path.

Using the hcigencerts template argument

To generate certificates that use a default password, country, state, and so on, you can create a template.

To create a file using a template:

1. The template is located at `templates\aclimport\hci_ACL_template.xml`. Open the file and go to the `user` section. This is all that is required to fill in. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<security>
<user name="customer1"/>
<user name="test1"/>
<user name="guest"/>
<user name="field"/>
</security>
```

2. This step is optional. Add the default certificate information using **Certificate Manager > Options > Edit Default Certificate Info**.
3. Generate the certificate using `hcigencerts`.

hci_ACL_template.xml file

The template file is located at `$HCIROOT/templates/hci_ACL_template.xml and` and `$HCIROOT/templates/hci_ACL.xsd`.

`hci_ACL_template.xml` contains user, role, and ACL parts. There is an `xsd` file which gives names of tools and can be used for validation, supporting these rights:

- Full/partial access to everything, specified sites, or master site.
- Partial access to some configuration tools in specified sites.
- Open/save/new/delete control of some configuration tools such as Alert Configurator, Script Editor, Lookup Table Configurator, Translation Configurator, and Network Configurator.
- Start, stop, resend, hold and release threads in Network Monitor.
- Open, resend, edit, and search messages in SMAT and SMAT database.
- ACL Role Manager
- BOX import and deploy

`aclmapping.xml` reflects the ACLs to resource. It is used at the time of security upgrade or when running of the command. Rights on resources of matched predefined ACLs are granted.

The `hci_ACL_template.xml` template file includes these objects:

Name	Data Type	Description
`name`	String	Required property.
`roles`	String	This can be more than one role, separated by commas.
`remark`	String	Description of this user.

This table lists the ACL (Access Control List) objects:

Name	Data Type	Description
`hosts`	String	Host name. If not specified, then this is all hosts.
`versions`	String	Version of Cloverleaf. If not specified, then this is for all versions.
`sites`	String	Site names. If not specified, then this is all sites.
`masterSiteOnly`	Boolean	Default is false. If true, then `Site` must not be specified.

This table lists the action objects:

Name	Data Type	Description
`tool`	String	This is the tool name in the GUI, and is case-insensitive. `all` indicates full access to everything. For example, "Netmonitor."
`actions`	String	Actions are separated by commas. This relates to buttons and actions in the tool. For example, `open` opens a tool, `start` starts a thread, and `stop` stops a thread. The default value is `all`.
`rights`	String	`P`: grant `N`: deny The default value is `P`.
`deleted`	Boolean	Deletes actions. When actions with the same `refACL` and tool name are found, they are deleted. The default value is `false`.
`refACL`	String	Name of the references ACL.

This table lists the permissions:

Name	Data Type	Description
`resource-id`	Integer	Resource ID in `aclmapping.xml`. This represents an individual resource.
`type`	String	Permission type: • `i`: insert • `d`: delete • `r`: read • `w`: write • `e`: run (execute) You can define multiple types in one property using a separator.
`rights`	String	`P`: grant `N`: deny The default value is `P`.
`deleted`	Boolean	Delete actions. When actions with the same `refACL` and tool name are found, they are deleted. The default value is `false`.
`refACL`	String	Name of referenced ACL

hciaclimport usage

Issuing this command is the only method of applying defined configurations. Users and roles are created at this time. Predefined permissions are stored into the database.

```
hciaclimport [-f filePath -p password [-b <databasePath] [-r] ] | [-t] | [-a tool] | [-h | -help]
```

You can also use:

```
hciaclimport -b databasePath [-r]
```

- `-f filePath` is the path of the predefined xml file.
- `-p password` is the password of CA certificate.
- `-b databasePath` is the path of the database backup.
- `-r` connects to Security Server. When this command is used during installation and Security Server is not running, this option should not be used. If Security Server has already been successfully installed and is running, then you can use `-r` to define the pre-ACLs.

- `-t` lists all supported tools.
- `-a tool` lists all supported actions of the tool.
- `-h` or `-help` prints this help message.

This command creates/updates predefined users and roles, and creates/updates/deletes predefined ACLs. Log messages are appended to the log file at `$HCIROOT/security/logs`.

This does not clear the database, but only adds/overwrites to the database. Targeted deletion of rights is permissible.

Users and roles can only be deleted in ACL Role Manager. This tool can only be used on Security Server.

1. Run `hciaclimport` to import predefined users, roles, and ACLs.
2. Create your sites.
3. Upgrade the Host Server to advanced mode.
4. After you modify a predefined user, role, or ACL:
   a. Run `hciaclimport` to update it.
   b. Downgrade the Host Server to basic or none mode.
   c. Upgrade to advanced mode again. At this point, you can see the new update ACLs.
5. Run `hcigencerts` to generate certs. This step can be taken at any time, even if you have not finished the preceding steps.

XML file

`hci_ACL_template.xml` contains user, role, and ACL parts. There is an `xsd` file which gives names of tools and can be used for validation, supporting these rights:

- Full/partial access to everything, specified sites, or main site.
- Partial access to some configuration tools in specified sites.
- Open/save/new/delete control of some configuration tools such as Alert Configurator, Script Editor, Lookup Table Configurator, Translation Configurator, and Network Configurator.
- Start, stop, resend, hold and release threads in Network Monitor.
- Open, resend, edit, and search messages in SMAT and SMAT database.
- ACL Role Manager
- BOX import and deploy

Command line

Issuing the command is the only method of applying defined configurations. Users and roles are created at this time. Predefined permissions are stored into the database.

Available commands:

```
hciaclimport [-f filePath -p password [-b databasePath]
[-r] ] | [-t] | [-a tool] | [-h | -help]
```

or

```
hciaclimport -b databasePath [-r]
```

- `-f filePath` is the path of the predefined xml file.
- `-p password` is the password of CA certificate.
- `-b databasePath` is the path of the database backup.
- `-r` connects to Security Server. When this command is used during installation and Security Server is not running, this option should not be used. If Security Server has already been successfully installed and is running, then you can use `-r` to define the pre-ACLs.
- `-t` lists all supported tools.
- `-a tool` lists all supported actions of the tool.
- `-h` or `-help` prints this help message.

This command creates/updates predefined users and roles, and creates/updates/deletes predefined ACLs. Log messages are appended to the log file stored at `$HCIROOT/security/logs`.

Note: This does not clear the database, but only adds/overwrites to the database. Targeted deletion of rights is permissible.

Users and roles can only be deleted in ACL Role Manager. This tool can only be used on Security Server.

hcigencerts

This command generates certificates on the Host Server.

```
hcigencerts -cacertpath certpath -capubcert pubkeyname -caprivkey prikeyname
-capass capassword  -pass certpassword -template filepath [-hciroot hcirootpath]
[-l logfile] [-h|-help]
```

- `-cacertpath certpath` is the path of the CA certificate.
- `-capubcert pubkeyname` is the file name of the CA public key.
- `-caprivkey prikeyname` is the file name of the CA private key.
- `-capass capassword` is the password of the CA certificate.
- `-pass certpassword` is the default password of the new user certificates.
- `-template filepath` is the path of the predefined xml file.
- `-hciroot hcirootpath` is the path of HCI root.
- `-l logfile` is the file name of the log.
- `-h` or `-help` prints this help message.

User certificates are issued by the CA certificate with the default password.

Backing up the database

1. Stop the Security Server.
2. Use the command `hciaclimport -b databasePath`.
3. Start the Security Server.

Recovering the database

1. Stop the Security Server.
2. Overwrite the current database at `$HCIROOT/security/data` using the backup database.
3. Restart the Security Server.

Chapter 43: Manually removing the Security Server

In some instances, the Security Server installation could fail during the install. If this happens, and attempts to re-install result in an error message stating `You cannot re-install Security Server, as it is already installed`, then it can be manually removed with these steps.

1. Click **Start > Run** regedit
2. Specify **`regedit`** and click **OK**. The **Registry Editor** is displayed.
3. Locate the registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\INFOR\CIS20.1\Infor Cloverleaf Security Server 20.1`.
4. Delete the key.
5. In your file system, remove all Security Server folders, including the uninstall.
6. Restart your machine.
7. Re-install Security Server.

Index

Special Characters

A

C

D

E

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

Y