Infor Cloverleaf Integration Services Release Notes

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_release_notes_2022__en-us

Contents

About this release

This document provides information about the enhancements and changes in Infor Cloverleaf Integration Services. See the *Resolved Issues* document for the list of fixed issues that are included in this update.

To see a previous version's added features and fixes, see that version's release notes. These are accessed from the Infor Support Portal/Concierge or the Download Center.

What's New: Highlights in this release

CIS access points

Access points direct you to a specific product:

CLAPI URL

In the online help, go to **System Administration > Host Server Web Server tab**.

By default,**Enable Cloverleaf API Documentation** is cleared.

The CLAPI web page includes the CLAPI SDK document and examples. By default, it is disabled.

To enable the CLAPI web page, the host server must be running in security mode.

When the Cloverleaf host server is started with **Enable Cloverleaf API Documentation** enabled, all Cloverleaf APIs are listed in HTML through https://hostservername:15067/clapi/. This provides details about request parameters and responses for each API.

Sitedoc URL

https://server:15063/sitedoc/index.xml

In this example:

- *hostname* is your Fully Qualified Domain Name that uniquely identifies your computer. Example: medcity
- *sitename* is your domain name. Example: radio124

CL Wizard URL

In the online help, go to **Cloverleaf Wizard > Setting up the wizard**.

To set up the Wizard using the host server:

1. Install Cloverleaf Integration Services.
2. Set-up basic security.
3. Select all of the options in the **System Administration > Host Server Web Server tab**.
4. Restart the host server.
5. Open a browser and go to: https://hostservername:15067/clwizard/.

   Use the same log-in user name and password as your security install.

CIS online documentation

The Cloverleaf documentation has been removed from the Cloverleaf install package and is provided separately. This includes the Cloverleaf Portable Client.

For online help installation steps, see "Installing the CIS online help" in the Infor Cloverleaf Integration Suite Installation Guide.

Toolbar enhancements in online documentation

The toolbar for online documentation has been enhanced. Descriptive text has been added next to each icon to improve usability.

The **Print PDF** option, which was under the **Print** icon, is now represented by a **PDF** icon. Click the icon to open a PDF of the current document. You can print or download the PDF, or view it in the browser. To print a single topic, click the **Print** icon.

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: Supported platforms and configurations

This table contains links to the supported platforms and other configurations that are necessary for this release:

Section	Description
Platforms	This lists the currently supported platforms for this release.
Database software	This lists the supported databases.
Web Client software	This lists the supported client browsers.
Cloverleaf Secure Courier and Global Monitor versions	This lists the supported CSC and GM versions.
GUI and tool support	This lists the supported server-side GUIs.
Embedded technology	This lists the embedded technology.
Data Integrator support	This lists the supported DataDirect versions.
Processor support	This describes the CIS processor support.
Cloverleaf and VM	This describes the VMWare virtual machine.
Cloverleaf and Red Hat Linux	This contains information on Red Hat Linux compatibility.
Message Tracing/Warehouse supported databases	This lists the external databases that are certified for the Message Tracing and Message Warehouse features.
Protocol formats	This lists the supported protocol formats.
Healthcare formats	This lists the supported healthcare formats.
Electronic commerce formats	This lists the supported electronic commerce formats.

Platforms

The supported platforms are:

Portable/Client only

Software	CIS Version
Mac 11.x (x86 chipset)	2022.09
Windows 11	2022.09

Client/Host Server

Software	CIS Version
Windows 11 64-bit Server for demo only, not production.	2022.09
Windows 2019 64-bit	2022.09
Windows 2022 64-bit	2022.09

Host Server only

Software	CIS Version
AIX 7.2 TL5	2022.09
Linux RH 7.x certified on 7.9	2022.09
Linux RH 8.x certified on 8.5	2022.09
CentOS 7.x certified 7.9	2022.09
Amazon Linux 2	2022.09

Docker

Operating system	Server
Guest OS	Amazon Linux 2
Host OS	Supported Windows and Linux servers

TLS support

TLS 1.3 is supported in the Secure Messenger/web services adapter and host server.

TLS 1.3 also supports HS/SS RMI communication and others.

TLS 1.3 supports these cipher suites:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256
- TLS_AES_128_CCM_8_SHA256

Note: TLS1.3 does not support anonymous mode.

Python update

The Python UPoC is implemented by JPython.

Python 2 is maintained for versions 19.1.x and 6.2.x. In 20.1.x, the Python version is JEP/Python3.x.

The previous version of Python (2.x) was replaced in Jan 1, 2020 by 3.x.

For detailed information on Python3.x (JEP), see the online help at **UPoCs > Script UPoC Java Embedded Python**.

Language support

Supported languages include:

- English
- Spanish (20.1 and later)
- French (20.1 and later)
- Brazilian Portuguese (20.1 and later)
- Dutch
- German

Language support in CLWizard

To change the language:

1. Navigate to *HCIROOT*`/server/tomcat/cloverapps/clwizard/legacy/config.json`.
2. Change the language in *`selected-language-id`*.

   For example, the Dutch code is `nl-NL`.

3 Refresh your browser for the change to take the effect.

Database software

The supported database software are:

Software	Version
Oracle (customer supplied/optional)	12c Release 2 (12.2.x) 64-bit 11g
Oracle (customer supplied/optional)	19c 12c Release 2 (12.2.x) 64-bit
SQL Server (customer supplied/optional)	2016 2014 SP2
SQL Server (customer supplied/optional)	2019 2016 SP2
SQLite (embedded)	3.28.0
Raima (embedded)	9.2

Web Client software

The supported client browsers are:

- Microsoft Edge (Chromium)
- Chrome

Third-party software

Third-party software included in the release are:

- Raima Embedded Database 9.2
- Data Direct Connect Drivers 7.1.6
- Data Direct Connect Drivers 8

Cloverleaf Secure Courier and Global Monitor versions

These are the versions that have completed integration tests.

- The supported Cloverleaf Secure Courier version is 21.1.0.3. This is for message data.
- The supported Global Monitor version is 21.1.1.2. This is for monitoring data.

Other versions might work with some restrictions/exceptions. For example, Global Monitor 6.1.3 cannot be used to monitor CIS 19.1 and 20.1.

CAA-WS, Direct, ION support

Operating system families are limited to Linux and Windows on the same versions supported by CIS 2022.09.

CAA-WS and CAA-Direct support all CIS 2022.09 platforms.

These are packaged together with Cloverleaf Integration Services.

ION supports all platforms.

GUI and tool support

These server-side GUI tools are supported on all platforms:

- Certificate Manager
- ACL Manager
- Security Upgrade
- Server Administration
- Audit Log Viewer
- Site Init

Embedded technology

The included embedded technology are:

- dcmtk-3.6.6
- ICU 4.8.1.1
- JVM 8.0 (8_265) (Linux/Windows/Mac)
- JVM 1.8.0_261 (AIX only)
- Jython 2.7.2
- libCurl 7.72.0

- libssh2 1.9.0
- openSSL 1.1.1k
- Perl 5.22.0
- Raima Embedded database 9.2
- Raima server
- Cloverleaf Secure Messenger (TLS)
- SQLite 3.28.0
- SQLcipher 4.2.0

  This is an encryption extension of SQLite.
- Tcl 8.6.8
- TclCurl 7.22.0
- Tcllib 1.19
- TclX 8.4
- Host Server Apache Tomcat 9.0.64
- TOP 3.7 (AIX/Linux)
- Xalan 1.11 (XSLT)
- Xerces 3.1.4 (XML)
- zlib 1.2.8

JRE version

This JRE version information applies to Windows, Linux, and AIX installations.

AIX

- Java version 1.8.0_331
- Java(TM) SE Runtime Environment (build 8.0.7.11 - pap3280sr7fp11-20220601_01(SR7 FP11))
- IBM J9 VM (build 2.9, JRE 1.8.0 AIX ppc-32-Bit 20220511_28614 (JIT enabled, AOT enabled)
- OpenJ9 - 844d750
- OMR - d297a72
- IBM - 7175f82)
- JCL - 20220531_01 based on Oracle jdk8u331-b09

Note: TLS 1.3 is not supported on AIX. AIX supports IBM JDK 1.8.0_261 on AIX.

Windows/Linux/MacOS

- OpenJDK version 1.8.0_342
- OpenJDK Runtime Environment Corretto-8.342.07.3 (build 1.8.0_342-b07)
- OpenJDK 64-Bit Server VM Corretto-8.342.07.3 (build 25.342-b07, mixed mode)

Data Integrator support

DataDirect 8.0 is supported for all platforms.

Earlier versions of DataDirect Connect are no longer supported.

DataDirect SequeLink is no longer supported.

Processor support

Intel x86 architecture is supported on Windows and Red Hat platforms.

With the increase in duo core, quad core, or multiple duo/quad core processors, Cloverleaf can be scaled to multiple processors. This is handled automatically in the operating system.

Beginning with version 6.2, Cloverleaf is a 64-bit application on Windows and Linux.

Most of the 64-bit operating systems support running 32-bit applications on a 64-bit operating system. For RedHat, if it is an x86_64 platform, then it can run 32-bit applications.

In some cases, a 32-bit application on a 64-bit operating system could lead to problems, as it is intended to load a 64-bit shared lib with Cloverleaf. A 32-bit binary must use 32-bit shared libraries.

Cloverleaf 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 chipset 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, it is best if recommended hardware sizing and specifications are 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 correctly.

Cloverleaf and Red Hat Linux

Cloverleaf is certified against a specific major and minor version of Red Hat Linux.

Red Hat Linux claims binary compatibility across minor releases providing the application adheres to standard Application Binary Interfaces (ABIs). Cloverleaf adheres to this standard. More detail is available on the Red Hat policy at:

https://access.redhat.com/solutions/5154

Cloverleaf works with a non-certified minor release of Red Hat Linux, provided that Red Hat maintains the binary compatibility policy. If compatibility issues in a Red Hat minor release arise due to deviations of the binary compatibility policy, then reasonable efforts are made to provide a hot fix.

CentOS conforms fully with Red Hat, Inc's redistribution policies and aims to be functionally compatible with Red Hat Enterprise Linux. CentOS mainly changes packages to remove trademarked vendor branding and artwork.

Message Tracing/Warehouse supported databases

These external databases are certified for the Message Tracing and Message Warehouse features.

CIS 19.1.0.0:

- SQL Server 2014, 2016
- Oracle 11g Release 2 11.2.x
- Oracle 12c Release 1 12.1.x 64-bit

CIS 19.1.2.0:

- SQL Server 2014, 2016
- Oracle 11g Release 2 11.2.x
- Oracle 12c Release 1 12.2.x 64-bit

CIS 20.1.0.0:

- SQL Server 2016, 2019
- Oracle 12c Release 2 12.2.x 64-bit
- Oracle 19c (64-bit)

Protocol formats

The supported protocol formats are:

- database-inbound
- database-outbound

- dicom
- dtc
- file
- fileset-ftp

  This includes ftps and sftp.
- fileset-local
- http-client

  This includes proxy server.
- java
- java/direct-retriever

  This is part of caa-ws.
- java/direct-sender

  This is part of caa-ws.
- java/ion-retriever

  This is part of caa-ws.
- java/ion-sender

  This is part of caa-ws.
- java/ws-client

  This is part of caa-ws.
- java/ws-rawclient

  This is part of caa-ws.
- java/ws-server

  This is part of caa-ws.
- link (UNIX)
- LU 3 (AIX only)
- LU 6.2 APPC (AIX only)
- *MQs (8.0) (see Note)
- pdl async

  Programmable Driver Language used for asynchronous communications.
- pdl tcpip

  Transmission Control Protocol/Internet Protocol that is implemented with PDL.
- prosper (UNIX)
- tcpip
- upoc

Note: * The IBM MQSeries (MQS) name has been changed to WebSphere MQ.

Healthcare formats

The supported healthcare formats include:

FHIR

- FHIR R4
- JSON FHIR 4.3

HL7

- 2.1
- 2.2
- 2.3
- 2.3.1
- 2.4
- 2.5
- 2.5.1
- 2.6
- 2.7
- 2.8
- 2.8.1
- 2.8.2
- 2.9

HPRIM

- 2.1
- 2.2
- 2.3
- 2.4

HPRIM XML

- 1.03a
- 1.04
- 1.05
- 1.06
- 1.07
- 2.00

NCPDP

- NCPDP Telecom 5.1
- NCPDP SCRIPT 4.2
- NCPDP SCRIPT 8.1
- NCPDP SCRIPT 10.6 (native and XML)
- NCPDP Formulary & Benefits 1.0

XML 1.0

Electronic commerce formats

The supported electronic commerce formats include:

X12

- 003020
- 003030
- 003040
- 003050
- 003060
- 003070
- 004010
- 004020
- 004030
- 004060
- 005010
- 005040
- HIPAA-004010
- HIPAA-004010A1
- HIPAA-005010A1
- X12N-4010

EDIFACT

- 94B
- 95B
- 96B
- 97B
- 01B

Chapter 2: Portable Client file permissions

Weak file permissions could exist in `C:\cloverleaf*` files and directories that are used by the Cloverleaf Client.

Incorrectly configured file permissions can result in information leakage and possible unauthorized file modifications.

To ensure security, see these topics to make improvements:

- Updating Cloverleaf permissions using Windows Internet Explorer on page 20
- Updating Cloverleaf permissions using the command line on page 21

Updating Cloverleaf permissions using Windows Internet Explorer

Note: You must have Administrator permission to complete these updates:

After you complete these steps, only the `hciuser` and `administrator` groups can access the `integrator` folder. Other users are unable to read/write files in this folder.

To update Cloverleaf permissions using Windows Internet Explorer:

1. Right-click the `integrator` folder and select “Properties”.
2. On the Properties dialog box, select the **Security** tab and click **Advanced**.
3. In the **Advanced Security Setting** dialog box, click **Change** to change the owner of the `integrator` folder.
4. In the **Select User or Group** dialog box, click **Locations** and select the local machine's host name. Click **OK**.
5. Specify “hciuser” in "Enter the object name to select" and click **Check Names**. This generates the correct user name.
6. After the name has been updated, click **OK**.
7. Return to the **Advanced Security Setting** dialog box and select both check boxes (**Replace owner on subcontainers and objects** and **Replace all child object permission entries . . .**). Click **Apply**.
8. After processing completes, select **Disable inheritance** to remove the inheritance principle from the parent folder.
9. Remove the permission for “Users” and “Authenticated Users”. To do this, click the “Users” and “Authenticated Users” lines and then click **Remove**.

10 In the "Permission entries" section, double-click the “hciuser” line and select **Full control** under "Basic permissions". Click **OK**.

After this is finished, "hciuser", "Administrators", and "SYSTEM" display "Full control".

Only the "hciuser" and "Administrator" groups can access the `integrator` folder. Other users are unable to read/write the files in this folder.

Updating Cloverleaf permissions using the command line

Use the command line to change permissions:

1 Open a command prompt as administrator.

2 Run these commands:

```
setroot
ICACLS %HCIROOT% /REMOVE:g *S-1-5-11 /t
ICACLS %HCIROOT% /REMOVE:g Users /t
ICACLS %HCIROOT% /grant hciuser:F /t
ICACLS %HCIROOT% /INHERITANCE:r /t
ICACLS %HCIROOT% /SETOWNER hciuser /T /C
```

These commands remove the permissions for the “Users” and “Authenticated Users” groups, grant full control for hciuser, set hciuser as the owner of `%HCIROOT%`, and disable inheritance.

You can also change permissions for the “Users” and “Authenticated Users” groups to “Read”, to have read access to *`%HCIROOT%`*.

The final actions depend on the user's Security policy.

Chapter 3: New features

Listed are the new features for Infor Cloverleaf Integration Services version 2022.09.

Document scheduler node in WS Client/WS Raw Client protocol thread (CISCL-7909)

`TIMEMETHOD=doTimeEvent` is located in the `ini` file for a thread.

Users can customize `TIMEMETHOD` in the **Java Driver Protocol Properties** dialog box.

The thread `ini` file content of CAA-related protocol threads, including `TIMEMETHOD`, are not displayed in the GUI since they are static.

Feature: Separate configuration from runtime (CISCL-7930)

Users running the engine are now separate from users doing configuration. For example, configuring users who can modify the allowlist from runtime.

Upgrade Tomcat to the latest version (CISCL-7944)

Host Server Apache Tomcat has been updated to version 9.0.64.

License Agreement removed from CIS installation (CISCL-7886)

A SKU product now ties directly to an existing license agreement. The product click wrap license is no longer necessary.

The License Agreement has been removed from the CIS installer. This applies to major and patch versions.

CLWizard Lookup Table retains the trailing and leading spaces in add and edit modes (CISCL-7891)

In previous versions, when a new row for a lookup table was added, the input trailing and leading spaces were automatically removed when saving the configuration. When editing an existing row, the spaces could be saved, but the leading space did not display.

The trailing and leading spaces are necessary input values in lookup tables. These are now kept in the configuration.

CLWizard Lookup Table now has a user-initiated Save button (CISCL-7892)

Auto-saving is used when a user clicks off of or changes a table cell. When this happens, the table would update before the right side of the table is edited. This can result in invalid output from the interface.

There is now a user-initiated **Save** button that avoids these instances.

User-defined command allowlist is separate from the overall allowlist (CISCL-7920) (CISCL-7901)

In the CIS design, root-level items are updated with the application update. Customer implementations are separate. When a new application version is released, customers can pull the new docker container with their existing persistent sites and begin to run.

The allowlist at the root level is a mixture of application items (hashes for CIS binaries and jars) and customer implementations (hashes for user-defined binaries and jars). Because of this, when the clean container is pulled the database is semi-persistent.

Commands that are run in the **Remote Command** tool are defined in the allowlist.

It goes through the site, master site, and root allowlist. If the command is the user-defined command, then it is located under the site or root `usercmds` folder. This is defined in the site or master site allowlist.

The user-defined allowlist is now separate from the default list.

The alert validation has also been updated.

`Monitord`, `hciengine` (JAVA driver) and `hcischeduler` load all commands or Jars/classes from these `allowlistdb` files:

- `root/conf/allowlist.db`
- `mastersite/conf/allowlist.db`
- `currentsite/conf/allowlist.db`

Delivering docker for on-premise partners (CISCL-7714)

The Cloverleaf Docker licensing section has been updated to describe the detailed steps to request a Cloverleaf license.

Host Server restart not required when allowlist digests are updated (CISCL-7727)

The allowlist is reloaded when the digests are updated. The reload restful API is also run to reload the site allowlist when it is enabled

The digest update is no longer required to restart the host server. The remote command tool now reloads the allowlist.

SSAPI: Swagger user interface cannot be accessed (CISCL-7827)

Due to incorrect certificate settings, the Swagger user interface cannot be accessed normally.

To access Swagger, create the certificate and import it into your browser. Then, you can access the SSAPI Swagger-UI page after enabling the SS API and SS API Doc.

CAA-WS GUI support for OAuth 2.0 with engine (CISCL-93)

WS client support for OAuth2 authentication has been improved to access the published web services.

OAuth 2.0 is designed to allow a website or application to access resources that are hosted by other web apps on behalf of a user.

The CAA thread functions as a back-end service and a OAuth2 client. To facilitate this, there is a new "OAuth2" type on the **Conduit Authentication** configuration panel.

These fields are available for OAuth2 Authentication settings:

- **Grant Type**
- **OAuth2 Token URL**
- **Scope**
- **Client ID**
- **Client Secret**
- **Service Account Name**
- **Service Account Password**

Additional information is located in the "CAA-WS Swagger" topic of the **Infor Cloverleaf Application Adaptor Web Services User Guide**.

Raima upgraded to version 15.2 (CISCL-7836)

Raima has been upgraded to version 15.2 for CIS 2022.09.

Access control for every resources on CLAPI level (CISCL-7377)

The APIs are access controlled by the `root/application/clapi` node. Each `subnode` of the `clapi` node represents a group of APIs.

This allows better permission control.

Ming.le admin web UI for server configuration (CISCL-7438)

The admin user can configure SAML(Ming.le) on the **Admin Web** user interface to enable SAML(Ming.le) user authentication.

Parameters and options include:

- **Enable SAML(Ming.le) user authentication**

  This enables/disables the Cloverleaf IDE SAML(Ming.le) user authentication. The default is disabled.

- **CA password**

  This is used in creating the user certificate and private key files.

  If the CA password already exists, then it is not necessary to re-enter.

There are two metadata and properties sections on the interface:

- IDP properties and metadata
- SP properties

IDP properties and metadata:

- **Entity ID**

  This IDP (Identity Provider) property corresponds to the `idp.saml.entityid` key in the IDP properties file.

  Click **Import IDP Properties** to import the Entity ID from the IDP properties file.

- **Domain name**

  This IDP (Identity Provider) property corresponds to the `idp.last.activity.domain.name` key in the IDP properties file.

  Click **Import IDP Properties** to import the domain name the from the IDP properties file.

- **Cookie name**

  This IDP (Identity Provider) property corresponds to the `idp.last.activity.cookie.name` key in the IDP properties file.

  Click **Import IDP Properties** to import the cookie name from the IDP properties file.

- **Home page URL**

  This IDP (Identity Provider) property corresponds to the `idp.mingle.homepage.url` key in the IDP properties file.

  Click **Import IDP Properties** to import the home page URL from the IDP properties file.

- **Portal URL**

  This IDP (Identity Provider) property corresponds to the `idp.mingle.portal.url` key in the IDP properties file.

  Click **Import IDP Properties** to import the portal URL from the IDP properties file.

- **Metadata**

  This is the IDP (Identity Provider) metadata file content in XML format.

  Click **Import IDP Metadata** to import the metadata from the IDP metadata file.

SP properties:

- **Entity ID**

  This is a required property of the SAML SP (Service Provider). This must be unique across the deployment region.

  Copy this from the registered Ming.le service provider.

- **SSO URL**

This is an internal URL generated by CLAPI for SAML implementation.

- **SLO URL**
  This is an internal URL generated by CLAPI for SAML implementation.

Java Driver Protocol GUI should support asynchronous mode (CISCL-7701)

When the application type is selected, method are no longer validated.

The `doStart` and `doStop` method validations have been removed. When the Class type is selected, the `RUNMETHOD` is checked. The `RUNMETHOD` is `doMsg` or `doReply`. There is a method validation when Class type is selected.

Security Server migration tool enhancement (CISCL-7310)

CIS 6.1 and 6.2 are no longer supported.

CIS 20.1 has been added to the source versions.

The destination version is updated to CIS 2022.09.

The LDAP user information, including first name, last name, distinguished name, and description, can be migrated from an earlier version.

Dynamic store procedure support in DBLookup (CISCL-7322)

A stored procedure can be dynamically called based on a value in a field. For example, if `PV1.2 == I`, then the stored procedure invokes `sp_inpatient`. If `PV1.2 == O` then `sp_outpatient` is invoked with different parameters.

Plain-text passwords are no longer returned through API endpoints (CISCL-7331)

Plain-text password information using API endpoints is no longer returned.

This information is now masked as "******" in application responses.

This information is now retrieved using a secure shared resource, such as a password vault.

This applies to all API versions.

For the `GET /{apiVersion}/api/site/{siteName}/netconfig/{netconfigName}` API, all passwords or credentials are masked in protocol properties as "******" in the response when the password is not null or empty. This applies to all API versions.

The protocol masked password list includes:

- APPC protocol
- DICOM: SCP options, SCU options
- Fileset FTP, FTP Account, FTPS, SFTP
- PPCF Protocol
- TCPIP IB email: POP3 options, SMTP options
- TCPIP SSL

The protocols masked credentials include:

- `httpClient`
- `httpProxy`

For the `GET /{apiVersion}/api/root/preferences/{siteName}/{properties}` API, all passwords are masked as "******" in the response when the password is not null or empty. This applies to all API versions.

CLAA-WS support for SAML2 and OAUTH2 (CISCL-7369)

CLAA-WS now supports SAML2 and OAUTH2. Supported are functionality, samples, GUI, and others.

"Route replies to original source only" is now cleared by default on processes of CAA-Client protocols (CISCL-6955)

The default value of **Route replies to original source only** is now cleared.

Affected protocols are:

- java/ws-client
- java/ws-rawclient
- java/direct-sender
- java/ion-sender

All other CAA Client protocol processes retain the original default of being selected.

"Route replies to original source only" is now cleared by default on a process (CISCL-6986)

The **Route replies to original source only** is now unselected by default on process properties. When this option is selected, the reply messages are routed only to the original source thread. When it is cleared, the outbound thread reply is routed back by all reply routes to all inbound threads.

Select this when you have multiple inbound threads and only require the reply to go to the originating thread.

This is located on the GUI at **Process > Configure. . . > Properties**.

CLAPI: Restful API best practices on HTTP verbs and updated APIs (CISCL-7374)

HTTP verbs are used to operate on the collections and elements. For example, `GET`, `POST`, `PUT`, `PATCH`, and `DELETE`.

Note: The `PUT` and `DELETE` methods are not allowed in CLAPI by OWASP.

HTTP verbs are:

HTTP Verb	CRUD operation	URL /orders	URL /orders/{*ID*}
`GET`	Read	List All Orders Response Code: HTTP 200 (OK) Use pagination, sorting, and filtering.	Get details of a order identified with ID. Response Code: • HTTP 200 (OK) • 404 (not found)
`POST`	Create	Create New Order Response Code: HTTP 201 (created) Return `/orders/{ID}` in location `resp` header.	Error Response Code: HTTP 405 (method not allowed)
`PUT`	Update	Bulk Update Orders 405 (Method not allowed), unless you must update every resource in the entire resource collection.	Update existing order. Response Code: • HTTP 200 (OK) • 204 (No content); 404 (not found)
`PATCH`	Update delta	Bulk Update Orders 405 (method not allowed), unless you must modify the collection.	Update existing order. Response Code: • HTTP 200 (OK) • 204 (No content) • 404 (not found)

HTTP Verb	CRUD operation	URL /orders	URL /orders/{*ID*}
DELETE	Delete	Error Response Code: HTTP 405 (method not allowed)	Delete existing order. Response Code: • HTTP 200 (OK) • 204 (No content) • 404 (not found)

Updated APIs are:

Original API (v1.0 to v2)	Updated API (v3)
GET /api/site/{siteName}/log/alerts	GET /api/sites/{siteName}/logs?logType=alerts
GET /api/site/{siteName}/log/file reuse	GET /api/sites/{siteName}/logs?logType=xxx
GET /api/site/{siteName}/log/monitord reuse	GET /api/sites/{siteName}/logs?logType=monitord
GET /api/site/{siteName}/log/monitord/error reuse	GET /api/sites/{siteName}/logs?logType=monitordError
GET /api/site/{siteName}/log/process/{processName} reuse	GET /api/sites/{siteName}/logs?logType=process&processName=xxx
GET /api/site/{siteName}/log/process/{processName} reuse	GET /api/sites/{siteName}/logs?logType=process&processName=xxx
GET /api/site/{siteName}/log/process/{processName}/error reuse	GET /api/sites/{siteName}/logs?logType=processError&processName=xxx

"hcirootcopy" now copies file data/time stamps (CISCL-6919)

The last modified timestamp of files and directories are replicated when doing site migration using `hcirootcopy`.

If files are migrated during `hcirootcopy`, then the timestamp is updated to the current time. For example, the SMAT database, allowlist database, statistic database, and other SQLite databases.

Empty directory timestamps are kept.

IDE support for user/account management/password authentication in Ming.le (CISCL-7247)

For improved IDE security, support has been added for user/account management/password authentication in Ming.le.

When a user logs in to the IDE using AppStream, or their local workstation by remote mode, the user name and password are authenticated in Ming.le.

The user name and password are authenticated through Ming.le for both basic and advance security mode.

"GlobalVariable" support for ENV variables (CISCL-5797)

Environmental variables have been added to CIS Global Variables. By avoiding hard-coded paths in Cloverleaf, migrating versions require less manual work.

For example:

- `$HCIROOT`, `$HciRoot`, `$HciRootDir`
- `$HCISITE`, `$HciSite`
- `$HCISITEDIR`, `$HciSiteDir`
- `$HCIMASTERSITE`, `$HciMasterSite`
- `$HCIMASTERSITEDIR`, `$HciMasterSiteDir`

These variables can be nested for the value definition of other global variables. These variables are replaced by matched `ENV` values.

For example:

- `$HCIROOT=$HciRoot=$HciRootDir=/opt/cloverleaf/cis20.1/integrator`
- `$HCISITE=$HciSite=site_prod`
- `$HCISITEDIR=$HciSiteDir=/opt/cloverleaf/cis20.1/integrator/site_prod`
- `$HCIMASTERSITE=$HciMasterSite=master_site`
- `$HCIMASTERSITEDIR $HciMasterSiteDir=/opt/cloverleaf/cis20.1/integrator/master_site`
- `$$ssh_key=$HCIROOT/site_master/data/certs/test.cloverleaf.key=/opt/cloverleaf/cis20.1/integrator/site_master/data/certs/test.cloverleaf.key`

Drop-down list added that supports NCSA and SLF4J at the Jetty/engine-level access log (CISCL-5850)

The Jetty access log has been enabled with CAAWS providers.

There is now a **Log HTTP Requests** located on the **WS Server** dialog box.

This supports NCSA and SLF4J at the Jetty/engine levelI.

Available values are:

- SLF4J
- NCSA
- blank/none/empty (default)

The relevant `xml` is added to `applicationContext.xml`. If "blank/none/empty" is selected, then the logging function is removed from `applicationContext.xml`.

WS Client support to consume swagger file (CISCL-6460)

Updates have been made to CAA-WS to simplify its management and configuration.

These include:

- `cookies`
- `form`
- `dataMap`
- `payloadKey`

These updated are located in the **Infor Cloverleaf Application Adaptor Web Services User Guide** at **API > USERDATA format > Client outbound overrides**.

Update to "hciss -help" (CISCL-6585)

The help content has been updated to match the command behavior.

Earlier version help example:

```
E:\cloverleaf\cis20.1\integrator\mh_fhir>hciss -h
hciss version: 20.1.1.0P, built: Thu Mar 25 2021
hciss [-s <what>] | [-start <what>] | [-k <what>] | [-K <what>] | [-h | -help]
-s <what> or -start <what> start specified server
 what: h = host server
 s = security server
-k <what> or -kill <what> kill specified server
 what: h = host server
 s = security server
```

Updated help example:

```
E:\cloverleaf\cis20.1\integrator\mh_fhir>hciss -h
hciss version: 20.1.1.0P, built: Thu Mar 25 2021
hciss [-s <what>] | [-S <what>] | [-k <what>] | [-K <what>] | [-h | -help]
-s <what> or -S <what> start specified server
 what: h or H = host server
 s or S = security server
-k <what> or -K <what> kill specified server
 what: h or H = host server
 s or S = security server
```

No longer a forced connect to previously used instance in the IDE (CISCL-6808)

When a user has different instances and numerous sites, the IDE is forced to reconnect to the previously used instance or site.

When this happens, users must wait until the time-out before connecting to another instance or site.

This behavior has been improved.

The Cloverleaf IDE no longer automatically connects to the previously used Cloverleaf instance and site. Instead, there is an **Automatically connect to the last connected host and site when the client starts** option on the **Client Preferences** dialog box.

CAA-WS support for OAUTH2 (CISCL-100)

CAA-WS now supports OAUTH2. This includes functionality, samples, GUI, and other support for different OAUTH2 profiles.

Refactored CXF's `BearerAuthSupplier` and `CodeAuthSupplier` have been refactored with improved usage and more customizable options. These can be configured on the GUI. Access tokens are cached with the refreshable supplier.

Engine support for multi-threaded/asynchronous WS Client (CISCL-92) (CISCL-125)

Support has been added for multi-threaded and asynchronous clients.

For additional information, see the **Infor Cloverleaf Application Adaptor Web Services User Guide** at:

- **Architecture and flow > Web Client working models**

- **API > Open Java API**
- **CAAWS sample sites > Asynchronous SOAP Client**

Asynchronous settings have been added to the **Infor Cloverleaf Application Adaptor Web Services User Guide**. These are located on the **WS Raw Client > Bus > General** tab.

- **Asynchronous Message Delivery**

  This enables all message delivery options.
- **Core Pool Size**

  The core number of threads. The default is 8.
- **Maximum Pool Size**

  The maximum allowed number of threads. The default is 64.
- **Keep Alive Time**

  This is the amount of time that threads in excess of the core pool size can remain idle before being terminated.
- **Shutdown Timeout**

  The maximum time to wait for the completed execution after a shutdown request.
- **Cloverleaf No Exception Handler**

  The full class name that is used to customize the error handler.

CLAPI: Restful API best practices on Resource URLs - phase 2 (CISCL-7373)

The original APIs are accessed using the version number from v1.0 to v2. For example, `/clapi/v1.2/api`.

Updated APIs are only accessed using version number "v3". For example, `/clapi/v3/api`. The default CLAPI version is "v3".

Updated API features include:

- Updated APIs are included in group "v3 UPoC".
- The response code is updated to "201" and the location is set in the response header for the RESTful POST method to create a resource.
- API descriptions are added using "@ApiOperation(*description*)".
- A new Constants class is included for magic strings and "Use ResponseEntity" as the response body.

API standards are:

- A URL identifies a resource.

  Example: Orders, Items, or Users.
- URLs must include nouns, but not verbs.

  Example: Use "orders" instead of "createorders".
- Use plural nouns, no singular nouns.

Example: Use "orders" instead of "order".

- Limit URL resources to two.

  Example: `orders/{ID}/lines`.

Using parameters in URL versus the header:

- If the parameter changes the logic you write to handle the response, then put it in the URL, for example, paging parameters.
- If the parameter does not alter the logic for each response, then put it in the header. For example, "OAuth2 access token".
- Specify optional fields in a comma separated list.
- Allow users to indicate expected response format. For example, JSON, XML, and CSV. This is in the form of:
  - `api/v2/resource/{id}.json _e.g. https:// {ionapi-host.infor.com}`
  - `/{tenant_id}/{suite}/v1/orders.json` or `https:// {[ionapi-host.infor.com|http://ionapi-host.infor.com/]}`
  - `/{tenant_id}/{suite}/v1/orders.xml_`

Updated APIs are:

Controller	Original API ("v1.0" to "v2")	Updated API (from "v3")
JavaController	`GET /api/site/{siteName}/upoc/java/list/class`	`GET /api/sites/{siteName}/java-upocs?type=CLASS` `enum` is required. Response Body: `java-upoc` file summary list This includes the file name and level.
JavaController	`GET /api/site/{siteName}/upoc/java/list/jar`	`GET /api/sites/{siteName}/java-upocs?type=JAR` `enum` is required. Response Body: `java-upoc` file summary list. This includes the file name and level.
JavaController	`POST /api/site/{siteName}/upoc/java/upload/class`	`POST /api/sites/{siteName}/java-upocs?type=CLASS` for create `PUT /api/sites/{siteName}/java-upocs?type=class` for update
JavaController	`POST /api/site/{siteName}/upoc/java/upload/jar`	`POST /api/sites/{siteName}/java-upocs?type=JAR` for create `PUT /api/sites/{siteName}/java-upocs?type=JAR` for update
ScriptController	`GET /api/site/{siteName}/upoc/javascript/download`	`GET /api/site/{siteName}/javascript-upocs/{fileName}`
ScriptController	`GET /api/site/{siteName}/upoc/javascript/list`	`GET /api/sites/{siteName}/javascript-upocs`

Controller	Original API ("v1.0" to "v2")	Updated API (from "v3")
ScriptController	`POST /api/site/{siteName}/upoc/javascript/upload`	`POST /api/sites/{siteName}/javascript-upocs` for create `PUT /api/sites/{siteName}/javascript-upocs/{fileName}` for update
ScriptController	`GET /api/site/{siteName}/upoc/python/download`	`GET /api/site/{siteName}/python-upocs/{fileName}`
ScriptController	`GET /api/site/{siteName}/upoc/python/list`	`GET /api/sites/{siteName}/python-upocs`
ScriptController	`POST /api/site/{siteName}/upoc/python/upload`	`POST /api/sites/{siteName}/python-upocs` for create `PUT /api/sites/{siteName}/python-upocs/{fileName}` for update

“allowlist” commands now support site-level allowlist (CISCL- 7960)

All instances of “whitelist” have been updated to “allowlist”.

These updates have been made for `allowlist` commands:

- `hciwhitelist` is updated to `hciallowlist`.
- `hciupdatewhitelisthash` is updated to `hciupdateallowlisthash`.
- `-s` *`sitename`* specifies the site.

  This is available for `hciallowlist` and `hciupdateallowlisthash`.
- The `-i` argument is no longer available.
- `hciwhitelist` and `hciupdateallowlisthash` only work for a site.

CLAPI allowlist interface should support site (CISCL-7959)

In earlier versions, CLAPI only supported root-level changes. Now, site-level changes are supported.

The new API URLs are updated to include the site name parameter. The new APIs are:

- `GET /{apiVersion}/api/server-admin/{siteName}/allowlist-config`
- `POST /{apiVersion}/api/server-admin/{siteName}/allowlist-config`
- `PUT /{apiVersion}/api/server-admin/{siteName}/allowlist-config/hashes`

Server Administrator support to customize site-level allowlist (CISCL-7958)

A drop-down list has been added to the **Server Administration > Allowlist** tab for selecting a site. The allowlist of a specific site can be customized.

CIS 2022.09 default ports (CISCL-7985)

The CIS default ports have been updated for 2022.09.

Table 1: Default RMI Registry

Host Server	13025
Security Server	TLS: 14028 SSL: 14029

Table 2: Tomcat

Host Server	• SHUTDOWN: 15065 Catalina (service): • HTTP: 15060 • HTTPS: 15063 CatalinaRestWS (service): HTTPS: • False Client authentication: 15067 • True Client authentication: 15069
Security Server	SHUTDOWN: 15165 Catalina (service): • HTTP: 15160 • HTTPS: 15163 CatalinaRestWS (service): HTTPS: 15169

CLAPI: New API for Lookup Table password validation (CISCL-8008)

In previous versions, the Cloverleaf Wizard did password validation by saving the Lookup Table. This is unsuitable for saving with cached data.

The Lookup Table password is now validated by the API before users can do password-related operations.

New "PKCS12" key type in Network Configurator (CISCL-5698)

The "PKCS12" key type option has been added to the **Truststore section > Type** drop-down list on the **Network Configurator**.

This options is available at these locations:

- **WS Client/WS Raw Client > Conduit > TLS > Truststore > Truststore Type**
- **WS Server > Engine > TLS secured > Truststore Type**
- **WS Server > SoapProvider > Policy Properties > X509 Certificate Handling Properties > Truststore Type**

Global variables support for "Validate Keystore/Truststore" and "Test" button of CAA-WS thread (CISCL-5167)

For CAA-WS threads, global variable support has been added for **Validate Keystore/Truststore** and **Test**.

Usage example:

1. Create a TLS Secured thread and specify the key/trust store global variables and passwords.
2. Click **Validate Keystore/Truststore**. This locates and validates the correct key/trust store.

The **Test** button also supports the global variables.

CLAPI now partitions the site list based on security server permissions (CISCL-280)

The CLAPI sites list is now verified for READ permission on the ACL site node. If a user does not have permission on that site, then CLAPI does not return this site to the user.

Only sites that have `READ` permission in these APIs are returned:

- `/api/root/sitenames`
- `/api/root/site`

CLWizard Confirmation dialog box updated when leaving Translation page without saving (CISCL-5526)

In CLWizard, a **Leave this page?** confirmation dialog box opens when you attempt to leave the **Translation** page without saving updates.

```
Changes you made are not saved. Click "OK" to leave, or "Cancel" to remain.
```

If **OK** is clicked without saving, then updates are not retained when **Leave** is clicked.

Click **Cancel** to remain on the page.

To save updates, you must click **Save** before leaving the page.

SSL engine output configuration now available in IDE (CISCL-5629)

The "ssl" module has been added to the **Engine Output Entry** dialog box. Available sub-modules are:

- "init"
- "open"
- "read"
- "write"
- "close"

The "ssl" module is located in the engine output file after specifying the "ssl" engine output configuration.

Scheduler Status Monitor (CISCL-6051)

You can now handle the status change of `hischeduler` and notify Global Monitor about the change.

To enable this feature, the web socket client user and message format have been added for `hischeduler` and the related handler.

Auto creation of JKS for HTTPS-based web service client adapters (CISCL-133)

With this enhancement, you can generate of a keystore/truststore without having to use command-line tools. This is configured using CAA-WS.

Keystore generation

A **Generate Keystore** button is located on the **Engine** panel and **Conduit TLS** panel. Clicking this button opens the **Generate Keystore** dialog box.

On this dialog box, you can generate/regenerate a keystore with a self-signed certificate. To do this, specify the common name, validity period, and other required fields.

Truststore generation

A **Generate Truststore** button is located on the **Conduit TLS** panel. Clicking this button opens the **Generate Truststore** dialog box.

Note: You cannot generate truststores on the server side **Engine** panel.

Generate the truststore by importing certs from the server to which you intend to connect.

To do this, specify the host and port in "host:port" format. Other required fields pertaining to the truststore must also be specified.

Need a TCL interface to reload GV (CISCL-7390)

A new `gvreload` Tcl interface is available.

`gvreload` reloads the global variable (GV) configuration when the configuration changes.

`GVConfig` records the modification time of `globalVariables.ini` when loading the GV configurations. The Cloverleaf engine compares the current and recorded modification times. When these times are different, this indicates the `config` file has been modified.

If the GV `config` file in the current or primary site is updated, then `gvreload` reloads the GV configuration and returns "1". Otherwise, "0" is returned.

When there is an error, `gvreload` returns an error similar to "`Error: gvreload error: ini file is empty`".

"hcirootcopy" should also copy file date/time stamps (CISCL-6919)

In previous versions, the `hcirootcopy` command did not copy the file date/time stamp.

Many users, though, have cleanup scripts that run on files based on the timestamp.

The `hcirootcopy` command has been enhanced to replicate the timestamp of files and directories.

Files and directories are now copied with the last modified timestamp.

If files are migrated during `hcirootcopy`, then the timestamp is updated to the current time. This includes the SMAT, allowlist, statistic, and other sqlite databases.

Only empty directory timestamps are preserved.

Unable to add Global Variable into BOX with remote connection to UNIX server from Windows client (CISCL-8133)

Global Variables cannot be added to a BOX when the remote connection to the UNIX server is from a Windows client.

Instead, a `No available data in Global Variants` message opens in Windows.

This happens only from a Windows client connection to a Windows server. This is not an issue on a Linux server.

This issue no longer happens.

New NetConfig host/thread validation options (CISCL-7996)

Two options have been added to the **Site Preferences** dialog box.

These options are located on a new **NetConfig** tab of the **Options menu > Site Preferences** dialog box:

- **Verify whether the host is reachable in thread**
  This disables/enables host reachable validation for a thread.
- **Verify whether the thread is reachable in destination thread**
  This disables/enables thread reachable validation for a destination thread.

By default, these options are selected. Disabling these options omits network validation. This decreases the time required in operations such as saving Network Configurator or creating a BOX. You must restart the GUI when these options are cleared.

MID second value (hub) should be a unique site ID number (CISCL-3807)

A new "`-t`" option is available for the `hciengine`, `hcienginerun`, and `hcienginerestart` commands. Use `-t` to specify the tenant ID.

The tenant ID can be specified by one of these methods:

- Using "`-t`" with `hciengine`, `hcienginerun` and `hcienginerestart`.
  or
- Using the *HCITENANT* system environment variable.

Features include:

- The maximum string length of tenant ID is 256.
- If the tenant ID is valid, then it is displayed by `eoPrintfMsg()`.
- `msgHostId` has been updated to `msgHostName` in the output of `eoPrintfMsg()`.
- The value of *MSG.HOSTID* is updated to be the host name in the Fileset outbound name template.
- The return value of the `msgmetaget $mh MSGHOSTID` TCL script is updated to the host name.
- You can retrieve the tenant ID using the `msgmetaget $mh MSGTENANTID` TCL script.
- The tenant ID is read-only.

Raw consumer Swagger: Unit test (CISCL-8182)

Description

CAA UI Swagger support almost to be done. we need to provide the Unit test case for this feature.

Attachments

"hciguisiteinit" and "hciauditlog" tool now support the Ming.le user log in (CISCL-8129)

With the resolution of IDE support for user/account management/password authentication in Ming.le (CISCL-7247) on page 31, `hciaccess` can log in as a Ming.le user, but other client GUI tools cannot log in.

For example, `hciguisiteinit` and `hciauditlog`..

This enhancement has been added.

Individual configure file available for merging Docker configuration items (CISCL-7918)

Some configuration files that are mapped to volume have been updated.

In CCH and on-premise Docker, there is a new individual configuration file. This file merges the specified configuration items instead of overwriting the existed ones, which remain unchanged.

CLAPI now provides detailed error messages when called from Swagger (Phase I) (CISCL-6320)

It can be difficult to know what the required fields are for an API run and what the valid field values are.

Swagger lists all of the fields as "`optional`", but this does not apply to all instances.

For example, the value type only states "`string`". However, specific values are required, such as "`file`" or "`engine`" for "`resend_type`". There is no method for users to know what the valid values are, other than looking at the code to determine the valid values.

For example, a `smatdb` message is resent from Swagger:

```
{
"messageType": "Data",
"modifiedmessages": [
{
"contentBase64String": "TVNIfF5+XCZ8U0VORF9ITDd8fFJFQ1ZfSEw3fHwyMDA3MDIyMzE1NTR8fEFEVF5BMDR8MDAwM
DAwMzQ3f
FB8Mi41LjF8fHx8QUx8QUx8fApFVk58QTA0fDIwMTMxMTI4MTQ1NzA5fHx8fApQSUR8MXxQYXRpZW50SURfMzMzM3xQYXR
pZW50SUQxX
l5eXlV+UGF0aWVudElEMzMzM15eXl5OUEl8dGVzdHVuaV5eXl5VSUR8Sk9ORVMxXldJTExJQU0xXkFeSX5KT05FUz
JeV0lMTElBTTJeQ
l5JSV5eXk1+Sk9ORVMzXldJTExJQU0zXkNeSUlJXl5eTH5KT05FUzdeV0lMTElBTURFTU83XkReSVZeXl5EfE1vdGhlck1haWRl
bk5hb
WV8MTkzMzAzMjJ8RnxeXl5eXl5NXnw2fDEyMDAgTiBFTE0gU1RSRUVUXnRlc3RpbmdhZGR
eR1JFRU5TQk9ST15OQ14yNzQwMS0xMDIwXj
ExXkheXjIzfjEyMDAgTiBFTE0gU1RSRUVUMl5eR1JFRU5TQk9STzMyXk5DXjI3NDAxLTEwMjFeMTJeUF5eMjR+MTIwM
CBOIEVMTSBTVFJ
FRVQzM15eR1JFRU5TQk9STzMzXk5DXjI3NDAxLTEwMjJeMTNeU0heXjI1fHwoNTU1KTQ0NC0yMjIyXlBSTl5QSH4oN
```

```
TU1KTQ0NC0yMjIz
Xk9STl5QSH4oMjU0KTIyNTU4ODk5XlBSTl5DUH41NTU1NV5QUk5eRlh+ODg4ODheUFJOXkJQfigwMjUzKTIzODAzOD
BeT1JOfl5ORVRe
SW50ZXJuZXReYWFAYWEuY29tfCg1NTUpNDU1LTIyMzVeV1BOXlBIXnRlc3RAZ21haWwuY29tfDE0fE18NHwxMjM1NXxBRFR
TU04yMjIyf
Hx8NHwxMXx8fHx8fHxOfHx8"
}
],
"priority": 1,
"processName": "ADT_IN",
"resend_type": "resend_db",
"srcThreadName": "ADT_IN_TCP",
"threadContext": "pre-TPS"
}
```

The response is always:

```
{
"code": "UnspecifiedError",
"message": null,
"fieldErrors": null
}
```

In many instances, there is no indication of which fields are incorrect or missing.

Many hours of trial and error are spent looking at the code to finally arrive at a correct invocation:

```
{
 "files": [
 "/cloverleaf/cis20.1/integrator/hl7_tester/exec/processes/hl7/hl7_in_files.smatdb"
 ],
 "passwords": {
 "/cloverleaf/cis20.1/integrator/hl7_tester/exec/processes/hl7/hl7_in_files.smatdb": ""
 },
 "resend_type": "engine",
 "format": "newline",
 "srcThreadName": "hl7_in",
 "threadContext": "ib_pre_tps",
 "filename": "output.out",
 "messageType": "data",
 "processName": "hl7",
 "destThread": "hl7_dishchare_out",
 "priority": 5120,
 "criteria": [
 {
 "type": "plain",
 "itemName": "MID",
 "operator": "==",
 "val1": "0.0.1476"
 }
 ]
 }
```

To improve performance, an enhancement has been added where CLAPI provides detailed error messages when called from Swagger.

`string` has been changed to `enum` for all necessary parameters and classes that are used for the request body.

`enum` is provided for API string values in:

- `GET /{apiVersion}/api/site/{siteName}/smatdb/autocomplete`

  For the `messageFormat` parameter, additional values on the drop-down list include: "hl7", "hprim", and "hl7+hprim".

- `POST /{apiVersion}/api/site/{siteName}/smatdb/search`

For **Request body Schema > CloverSearchMessageContext > criteria > CloverSearchCriteria > operator**, additional schema `operator` values are now available.

PostgreSQL is now supported by the Database Schema GUI (CISCL-6225)

On the **Site Preferences > Database Configurations** tab, the. **Large Object Type** option list now includes "PostgreSQL".

The `largeobjecttype` property must be `oracle`, `sqlserver`, `sqlite`, or `postgresql`.

The default value for uncertified databases is `oracle`.

This option is only useful if it is another database, not Oracle, SQLServer, SQLite, or PostgreSQL. If the database is one of these, then the option is not available, and is not required. Other databases are configurable.

New APIs for adding, modifying, and deleting a single allowlist entry (CISCL-7647)

There are new APIs for adding, modifying, and deleting a single allowlist entry:

- `POST /{apiVersion}/api/server-admin/{siteName}/allowlist-config/entries`
- `PUT /{apiVersion}/api/server-admin/{siteName}/allowlist-config/entries/{entryId}`
- `DELETE /{apiVersion}/api/server-admin/{siteName}/allowlist-config/entries/{entryId}`

“Conduit Name” tooltip and description improvement (CISCL-7398)

The **Conduit Name** tooltip has been updated.

Update the description of Create Conduit-Basic Setting

The expression matches the client. This is one of:

- URL pattern.
  Example: `\http://somehost:port/url*\`
- Only web clients (raw clients).
  Example: `\*WebClient.http-conduit\`

- Specific SOAP port name.
  Example: `\{urn:ihe:iti:xds-b:2007}DocumentRegistry_Port_Soap12.http-conduit\`
- All clients.
  Example: `\*.http-conduit\`

On the **Create Conduit - Basic Settings** page, an **HTTP Conduit** name field is used to match against the various clients that might exist in your configuration file. For example:

- `*.http-conduit`
  This matches all clients.
- `{http://example.com/}HelloWorldServicePort.http-conduit`
  This matches against a SOAP client using that port. Copy the name from the port you want to configure.
- `*WebClient.http-conduit`
  This matches all Raw clients.
- `http://someserver:8080/some/path*`
  This matches all clients that use this URL or some subset of that path.

Values specified can be updated at any time.

For additional information, see the ///// UserGuideUpdate.docx topic ///// in the **Infor Cloverleaf Application Adaptor Web Services User Guide**.

TLS-related options do not display when creating clients and address is an HTTP URL (CISCL-7397)

The default value of **TLS Secured** depends on the URL Consumer type:

- By default, this is cleared and disabled when the Consumer address is an HTTP URL.
- By default, this is enabled and selected when the address is an HTTPS URL.

TLS Secured is disabled and the **Conduit TLS** page is not shown when the address field value begins with "`http`".

For details, see **CAA-WS IDE properties GUI > Creating a sample client > Creating a new conduit**.

For additional information, see the ///// UserGuideUpdate.docx topic ///// in the **Infor Cloverleaf Application Adaptor Web Services User Guide**.

CAA-WS server oauth2 support acts as resource server in OAuth2 engine (CISCL-7975)

Additional samples are now available in the CAAWS samples site. The `oauth2_sample` BOX contains the OAuth2 setup.

`oauthClient` and `oauthResource` are a client-server pair. The client asks for a client credentials grant type access token. The server protects its resource by forwarding the token for validation.

`oauthCodeResource` protects its resource after the authorization code grant type. Users are forwarded to the Google portal for authorization, where a code is given for accessing the resource.

Support for separating the log file location for each Portable Client user (CISCL-6645)

In *%HCIROOT%*`/client/client.ini` a new `log_directory` key has been added under the `logs` section. This is for specifying the log path of a client.

If the property is not set, then the default is *%HCIROOT%*`/client/logs`.

MonitorD respects alert SMTP configuration from master site (CISCL-5618)

The master site's Alert Email Action configurations are respected when there are no settings in the current site.

CLAPI: Lookup Table supports exporting a Lookup Table as a “csv” file (CISCL-7914)

The `/{`*apiVersion*`}/api/sites/{`*siteName*`}/lookup-tables/{`*tableName*`}/entries.csv` API is for exporting Lookup Table entries as a `csv` file.

To do this, the Lookup Table must be a `tbl` type and be comma delimited in the `csv` file.

Raw consumer swagger: CAA GUI for General panel (CISCL-7934)

With CAAWS swagger support, you can get the target serviceAPI definition in real-time to assist in Consumer configuration.

On the **CAA WS-RawClient Creating Wizard** dialog box, a new **Configure Raw Consumer From Swagger File** page has been added after the **Conduit Configuration** page.

On this page, you can load the swagger JSON file to view the API paths and corresponding request method (HTTP verb) with parameters.

The wizard can generate an individual Raw Consumer for each selected HTTP verb node.

On the panel:

- **Cookies**, **Form Data**, and **Body** have been added after **Headers** for the displayed parameters.
- The **Headers**, **Cookies**, and **Form Data** tabs have **Name**, **Value**, and **Add**/**Remove**.
- **Body** is a text area.

Additional information is located in the "CAA-WS Swagger" topic of the **Infor Cloverleaf Application Adaptor Web Services User Guide**.

Need a way to set alternate default alert file(s) (CISCL-3678)

A new **Default Alert configuration Monitor Daemon uses:** text field has been added to configure the default alert file that Monitor Daemon automatically uses when starting. Only one file can be configured. The default file is `default.alrt`.

In the `siteInfo` file, `defaultalertconf=xxx` is added after saving the configuration.

This is located in the online help at **Cloverleaf Integration Services IDE > Site preferences > Alert configuration options**.

CLAPI: Lookup Table supports import a csv file into an existing lookup table (CISCL-7913)

A new `PATCH /v3/api/sites/{siteName}/lookup-tables/{tableName}` API has been added to support importing a `cvs` file into an existing lookup table.

`PATCH` is suitable for delta update and the resource in this API is `lookup-tables`.

By default, rows are overwritten if the left or right value conflicts.

New API for creating certs for users with temporary passwords (CISCL-8000)

A new API is available on the server for creating user cert/private key files. The password for the Mingle user password is temporarily generated with an algorithm.

The user certificate is created on the host server.

IDP and SP metadata CLAPIs enhanced for SAML(Ming.le) configuration (CISCL-8032)

CLAPI enhancements have been made for the admin web UI SAML(Ming.le) configuration.

These new APIs have been added:

- `(GET) idp/metadata`

  This returns the existing IDP properties and metadata.
- `(PUT) sp/metadata`

  This updates SP metadata. (`samlspEntityId`).

These APIs have been updated:

- `(POST) idp/metadata`

  A new `clapiOnly` parameter decides whether to apply IDP metadata in **CLWizard**.
- `(GET) sp/metadata`

  A new `newEntityId` parameter decides whether to return the existing Entity ID or generate a random Entity ID.

NetConfig validation options on the IDE (CISCL-7996)

Two options have been added to **Options > Site Preferences > Netconfig**. These options disable/enable host-reachable validation in a thread and thread-reachable validation in the destination thread.

These options decrease the validation time. This applies to operations such as saving NetConfig or creating a BOX.

When these options are disabled (required to restart GUIs), network validation is skipped.

- **Verify whether the host is reachable in thread** disables/enables host-reachable validation for a thread.
- **Verify whether the thread is reachable in destination thread** disables/enables thread reachable validation for a destination thread.

New CLAPI API for Lookup Table password validation (CISCL-8008)

There is a new `GET /{apiVersion}/api/sites/{siteName}/lookup-tables/{tableName}` API. The password has been relocated to the request header to avoid any security issues. The `GET` method is used in place of the `POST` method.

There is also a new `forcepwdcheck` query parameter.

When this is “true”, the password is verified. A 400 return status code is returned if the password is invalid.

When this is “false”, the encrypted data is masked if the password is invalid.

The original POST `/{apiVersion}/api/site/{siteName}/lookuptable/{tableName}/get` API is valid from version 1.0 to version 2. The new API is valid from version 3.

“allowlist” database migration now based on site level for Docker (CISCL-8163)

The allowlist is now separated into root and site levels. Each site has an allowlist database.

The allowlist database migration on docker is also based on the site level.

Temporary files under “temp” directory for message resending are now encrypted (CISCL- 7927)

The SMAT database resent temporary database files are now encrypted.

Note: This applies only to temporary file encryption for SMAT database message resending to the engine.

JSON support for “@” in the node name (CISCL-7904)

The third-party library `wjelement` as JSON validator and parser now supports "@" in the node name.

Also supported in the node name are:

- Letter
- Digit
- Whitespace

- Underscore
- Colon
- Minus sign

Documenting Installer Exit Code (CISCL-7847)

The list of installer exit codes is located in the **Infor Cloverleaf Integration Services Installation Guide** at **AIX and Linux Host Server > AIX and Linux Host Server post-installation > Installation exit codes**.

Windows Powershell support for Cloverleaf (CISCL-7672)

PowerShell is now supported on Windows Cloverleaf Integration Services.

Note: `hcicmd` will not function when " " (quotes) surround the command. For example, `pstop`,`pstart`, and others.

Certify Windows 11 for CIS Host Server demo (CISCL-7503)

Windows 11 is now certified as the CIS host server demo platform.

Test option now available outside the Web Services wizard (CISCL-6842)

A test option is now available for modifications/changes after the initial creation. For example, an updated certificate.

A message resend when message length is "0" removes OBMSGID (CISCL-6837)

A user has an outbound CAA-WS RawClient interface that performs GETs with a zero message length body/message text.

If await-replies is set and the timeout is triggered, then CIS resends. After this, the OBMSGID is removed and the message is lost.

However, it should queue and get resent, or do the function in timeout handling.

This was due to the message length being “0”. A message resend when the message length is “0” removes OBMSGID.

This function has been improved. “0”-length message handling is now configurable.

DBP/DBL should support PostgreSQL database (CISCL-6224)

The database protocol is now certified for PosgreSQL. A driver is provided.

The database protocol and database lookup are supported.

"hcischeduler" performance improvement while loading allowlist with many sites (CISCL-8194)

All `hcischeduler` job actions are now validated before being run.

Actions must be added to the current or primary site `allowlist` database first. Otherwise, the actions do not run.

The action validation order is that the current site `allowlist` comes before the primary site. When the current site and primary site both have a same named script/command in the `allowlist`, the script/command is first run from the current site.

In the primary site, `hcischeduler` only loads one primary site `allowlist` database. The database loading order is that the primary site that is defined in `siteInfo` is loaded before the primary site that defined in `rootInfo`.

You can change the primary site while `hcischeduler` is running. `hcischeduler` reloads the new primary site allowlist database when it is updated.

Need a way to set alternate default alert file (CISCL-3699)

Users can now select which alert configuration files the monitor daemons will use automatically when starting.

For example, you can add a **Default Alert Files** option in the **Site Options > Alert Configuration**.

This is available through the daemon panel or manually.

DB protocol needs to support pni file JVM Setting override (CISCL-321)

The database protocol loads JVM settings from `NetConfig`. Support has been added to load this setting from a `pni` file. The `NetConfig` JVM section is no longer available.

When there is `pni` file under site directory, the database protocol uses the JVM settings from the `pni` file. If there is no `pni` file, then the database protocol uses the default values to start the JVM.

MonitorD now run all available alerts in mastersite and site alert files (CISCL-135

Alerts now function like tables and `tcl` files. All alerts in the mastersite load first, then the alerts in the site are loaded.

If a site alert has the same name as a mastersite alert, then the site alert replaces the mastersite version.

Error message should be clear when IO exception occurs in LocalGlobalFileManager (CISCL-7632)

An error message is given when an IO exception occurs in the `LocalGlobalFileManager` constructor.

```
"rootDir is not a valid directory. Error returned: " + ex.getMessage()
```

For clarity, the error message has been updated.

```
The parameter of Global File Manager should be a directory.
```