IDOL Server

Software Version 12.9.0

Release Notes

Micro Focus

Legal notices

Copyright notice

© Copyright 2021 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for updated documentation, visit https://www.microfocus.com/support-and-services/documentation/.

Support

Visit the MySupport portal to access contact information and details about the products, services, and support that Micro Focus offers.

This portal also provides customer self-solve capabilities. It gives you a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the MySupport portal to:

- Search for knowledge documents of interest
- Access product documentation
- View software vulnerability alerts
- Enter into discussions with other software customers
- Download software patches
- Manage software licenses, downloads, and support contracts
- Submit and track service requests
- Contact customer support
- View information about all services that Support offers

Many areas of the portal require you to sign in. If you need an account, you can create one when prompted to sign in. To learn about the different access levels the portal uses, see the Access Levels descriptions.

Contents

Introduction to IDOL 12

IDOL 12 is the latest major version of IDOL, and introduced some significant new features.

- **IDOL Audio Analysis** functionality is now available in Media Server, so that you do not need to install IDOL Speech Server separately.

  > **NOTE:** As a result of this change, IDOL Speech Server is not available in IDOL 12.0.0 and later.

- **IDOL Text Index Encryption**. You can now encrypt your IDOL text data index, using AES encryption.

- **Geospatial Index**. The new IDOL text geospatial index improves the handling of geographical search. You can now index geographical regions, as well as points, and the new index supports several new FieldText operators for geographical searches.

- **Dynamic Corpus Functionality**. Web Connector has new functionality to allow you to embed IDOL analytics into the decision making during the data collection process. It can now use custom algorithms to choose whether to ingest a page based on the result of a Lua script.

- **Improved embedded Web browser**. The Web Connector has a new and improved embedded Web browser.

IDOL NiFi Ingest

In addition to the new features and improvements available in the existing IDOL components, the wider IDOL framework now includes IDOL NiFi Ingest.

IDOL NiFi Ingest is a new way to plan and configure your ingestion stream. It uses Apache NiFi to allow you to easily configure and manipulate your data ingest process, from your connectors, to KeyView and other import processes (such as media analysis and Eduction), and your IDOL index.

NiFi Ingest is intended as an alternative to the Connector Framework Server. For more information, refer to the *IDOL NiFi Ingest Help*.

New in this Release

The following sections describe the enhancements for the components of IDOL Server version 12.9.0.

Content Component

New in this Release

- The implementation of AES that IDOL uses to encrypt security info strings has been updated. This update is not backwards compatible with earlier versions. If you use AES to encrypt security info strings, you must upgrade all IDOL components that process security info (Community, Content, DAH, and Answer Server) to version 12.9, to ensure that components can successfully exchange security info.

  This change includes built-in authentication, so additional HMAC validation (by using the `HMACValidation` parameter) is no longer required or supported. The `HMACValidation` is now deprecated, and might be deleted in future.

- On-disk index encryption in the Content component has been hardened, by using a newer and more secure implementation of AES encryption.

  > **NOTE:** Micro Focus recommends that you back up your index before you upgrade the Content executable.
  >
  > The changes are backwards compatible, so that Content can still read existing encrypted indexes after you upgrade. However, you cannot then return to an older version of Content, as older versions cannot decrypt data written in the new format.
  >
  > For information about which indexes are encrypted, and how encryption is applied to existing indexes, refer to the *IDOL Server Administration Guide*. The `GetStatus` action response displays an encryption status of **partial** for indexes that contain data that was encrypted with the older AES implementation.

- Scoring of phrases inside the SYNONYM query operator has been adjusted, to prefer documents containing a higher number of occurrences of all the terms in a phrase.

- ACI servers can now communicate with a License Server instance that requires a GSSAPI authenticated connection (that is, where the License Server configuration has `RequireGSSAuth` set to **True**). To allow this communication, you must set `GSSServiceName` in the `[License]` section of the configuration file to the GSSAPI service name of the License Server. For example:

```
[License]
GSSServiceName=LICENSESERVER
```

- The third-party OpenSSL library has been updated to 1.1.1.j.

- The `Admin`, `Help`, `LoadDoc`, and `LoadImage` actions now set the HTTP response header `Content-`

`Security-Policy`, to improve security against cross-site scripting. If the `Content-Type` header is set, these actions also set the header `X-Content-Type-Options: nosniff`.

Resolved Issues

- On Windows, synchronizing the Bitfield index occasionally reported an error.

- On Windows, regenerating the Security index occasionally failed.

- The `GetStatus` action response reported `num_databases` as the number of active and deleted databases. The `num_databases` tag now reports the number of active databases.

- When index encryption was configured, a reference-based stored state created with the `StoredStateField` parameter could contain incorrect data, and would fail to match the correct documents when used as a restriction on subsequent queries.

- When `SecureTermExpansion` was turned on, a `TermExpand` action with `Expansion` set to **Phrase** could cause IDOL Content to exit unexpectedly.

- With an encrypted index, certain specific distributions of index terms could cause a small number of terms to be unsearchable, reporting an error `Unable to read term info`. These errors were reported during disk index validation.

  Spurious errors could also be reported in this state: `Unable to read term info` when querying specific, non-existent terms, and `Term list file size mismatch` when re-starting the engine.

Category Component

New in this Release

- ACI servers can now communicate with a License Server instance that requires a GSSAPI authenticated connection (that is, where the License Server configuration has `RequireGSSAuth` set to **True**). To allow this communication, you must set `GSSServiceName` in the `[License]` section of the configuration file to the GSSAPI service name of the License Server. For example:

```
[License]
GSSServiceName=LICENSESERVER
```

- The third-party OpenSSL library has been updated to 1.1.1.j.

- The `Admin`, `Help`, `LoadDoc`, and `LoadImage` actions now set the HTTP response header `Content-Security-Policy`, to improve security against cross-site scripting. If the `Content-Type` header is set, these actions also set the header `X-Content-Type-Options: nosniff`.

Resolved Issues

There were no resolved issues in Category Components version 12.9.0.

Community Component

New in this Release

- The implementation of AES that IDOL uses to encrypt security info strings has been updated. This update is not backwards compatible with earlier versions. If you use AES to encrypt security info strings, you must upgrade all IDOL components that process security info (Community, Content, DAH, and Answer Server) to version 12.9, to ensure that components can successfully exchange security info.

  This change includes built-in authentication, so additional HMAC validation (by using the `HMACValidation` parameter) is no longer required or supported. The `HMACValidation` is now deprecated, and might be deleted in future.

- Community can now communicate with an OmniGroupServer instance that requires a GSSAPI authenticated connection (that is, where the OmniGroupServer configuration has `RequireGSSAuth` set to **True**). To allow this communication, you must set `GSSServiceName` in the section of the Community configuration file for the security repository to the GSSAPI service name of the OmniGroupServer for that repository. For example:

  ```
  [MyRepository]
  GSSServiceName=OMNIGROUPSERVER
  ```

- ACI servers can now communicate with a License Server instance that requires a GSSAPI authenticated connection (that is, where the License Server configuration has `RequireGSSAuth` set to **True**). To allow this communication, you must set `GSSServiceName` in the `[License]` section of the configuration file to the GSSAPI service name of the License Server. For example:

  ```
  [License]
  GSSServiceName=LICENSESERVER
  ```

- The third-party OpenSSL library has been updated to 1.1.1.j.

- The `Admin`, `Help`, `LoadDoc`, and `LoadImage` actions now set the HTTP response header `Content-Security-Policy`, to improve security against cross-site scripting. If the `Content-Type` header is set, these actions also set the header `X-Content-Type-Options: nosniff`.

Resolved Issues

- When SSL was configured for the Data DRE, the background database list update failed, logging an error `Unable to configure a SSL connection with Data DRE`.

Connector Framework Server

CFS includes KeyView filters and can run Eduction. For new features and resolved issues related to these components, refer to the *KeyView Release Notes* and *Eduction Release Notes*.

New in this Release

- CFS can send IDOL documents to an Amazon Kinesis Data Firehose. This is a cloud service that can optionally transform the data before delivering it to one or more destinations, such as an Amazon S3 bucket.

- The IDOL indexer has a new parameter named `IdxUseXmlSafeFieldValues`. When you set this to `TRUE`, characters in document fields that are forbidden in XML are replaced with spaces. This parameter applies only when you index documents in IDX format. When you index documents in XML format, the forbidden characters are always replaced by spaces (in this case there is no change from earlier versions of CFS). The IDX writer also supports this feature, but the parameter is named `IdxWriterUseXmlSafeFieldValues`.

- ACI servers can now communicate with a License Server instance that requires a GSSAPI authenticated connection (that is, where the License Server configuration has `RequireGSSAuth` set to **True**). To allow this communication, you must set `GSSServiceName` in the `[License]` section of the configuration file to the GSSAPI service name of the License Server. For example:

```
[License]
GSSServiceName=LICENSESERVER
```

- The third-party OpenSSL library has been updated to 1.1.1.j.

- The `Admin`, `Help`, `LoadDoc`, and `LoadImage` actions now set the HTTP response header `Content-Security-Policy`, to improve security against cross-site scripting. If the `Content-Type` header is set, these actions also set the header `X-Content-Type-Options: nosniff`.

Resolved Issues

There were no resolved issues in Connector Framework Server version 12.9.0.

Controller

New in this Release

- ACI servers can now communicate with a License Server instance that requires a GSSAPI authenticated connection (that is, where the License Server configuration has `RequireGSSAuth` set to **True**). To allow this communication, you must set `GSSServiceName` in the `[License]` section of the configuration file to the GSSAPI service name of the License Server. For example:

```
[License]
GSSServiceName=LICENSESERVER
```

- The third-party OpenSSL library has been updated to 1.1.1.j.

- The `Admin`, `Help`, `LoadDoc`, and `LoadImage` actions now set the HTTP response header `Content-Security-Policy`, to improve security against cross-site scripting. If the `Content-Type` header is set, these actions also set the header `X-Content-Type-Options: nosniff`.

Resolved Issues

There were no resolved issues in Controller version 12.9.0.

Coordinator

New in this Release

- ACI servers can now communicate with a License Server instance that requires a GSSAPI authenticated connection (that is, where the License Server configuration has `RequireGSSAuth` set to `True`). To allow this communication, you must set `GSSServiceName` in the `[License]` section of the configuration file to the GSSAPI service name of the License Server. For example:

```
[License]
GSSServiceName=LICENSESERVER
```

- The third-party OpenSSL library has been updated to 1.1.1.j.

- The `Admin`, `Help`, `LoadDoc`, and `LoadImage` actions now set the HTTP response header `Content-Security-Policy`, to improve security against cross-site scripting. If the `Content-Type` header is set, these actions also set the header `X-Content-Type-Options: nosniff`.

Resolved Issues

There were no resolved issues in Coordinator version 12.9.0.

Distributed Action Handler

New in this Release

- The implementation of AES that IDOL uses to encrypt security info strings has been updated. This update is not backwards compatible with earlier versions. If you use AES to encrypt security info strings, you must upgrade all IDOL components that process security info (Community, Content, DAH, and Answer Server) to version 12.9, to ensure that components can successfully exchange security info.

- ACI servers can now communicate with a License Server instance that requires a GSSAPI authenticated connection (that is, where the License Server configuration has `RequireGSSAuth` set to `True`). To allow this communication, you must set `GSSServiceName` in the `[License]` section of the configuration file to the GSSAPI service name of the License Server. For example:

```
[License]
GSSServiceName=LICENSESERVER
```

- The third-party OpenSSL library has been updated to 1.1.1.j.

- The `Admin`, `Help`, `LoadDoc`, and `LoadImage` actions now set the HTTP response header `Content-Security-Policy`, to improve security against cross-site scripting. If the `Content-Type` header is set, these actions also set the header `X-Content-Type-Options: nosniff`.

Resolved Issues

- The `PreserveCarriageReturn` configuration parameter was not respected properly for free XML (that is, the contents of a document tag) at all levels of a multi-level DAH setup.

- When `PreserveCarriageReturn` was set to **True**, DAH could return invalid XML for certain actions. This mainly affected mirror mode, but could also affect certain 'stateless' actions (such as `Highlight` and `DetectLanguage`) in other distribution modes.

- The `GetStatus` action response reported an incorrect number of databases when databases had been deleted in underlying Content servers. It now reports the correct figure.

- In failover mode, with Combinator VDBs configured, DAH sometimes did not use the correct primary child server at start up when it was available, and after failover could continue using a secondary child server after the primary server became available. DAH now uses the correct child server, when available, and returns to earlier child servers when available.

Distributed Index Handler

New in this Release

- ACI servers can now communicate with a License Server instance that requires a GSSAPI authenticated connection (that is, where the License Server configuration has `RequireGSSAuth` set to **True**). To allow this communication, you must set `GSSServiceName` in the `[License]` section of the configuration file to the GSSAPI service name of the License Server. For example:

```
[License]
GSSServiceName=LICENSESERVER
```

- The third-party OpenSSL library has been updated to 1.1.1.j.

- The `Admin`, `Help`, `LoadDoc`, and `LoadImage` actions now set the HTTP response header `Content-Security-Policy`, to improve security against cross-site scripting. If the `Content-Type` header is set, these actions also set the header `X-Content-Type-Options: nosniff`.

Resolved Issues

There were no resolved issues in Distributed Index Handler version 12.9.0.

File System Connector

New in this Release

- The connector can communicate with other IDOL components that have been configured to require GSSAPI authentication. To enable this, set the `GSSServiceName` parameter in the `[Ingestion]`, `[DistributedConnector]`, and `[ViewServer]` sections of the configuration file, for requests to CFS, Distributed Connector, and IDOL View Server respectively.

- ACI servers can now communicate with a License Server that requires a GSSAPI authenticated connection (that is, where the License Server configuration has `RequireGSSAuth` set to **True**). To allow this communication, you must set `GSSServiceName` in the `[License]` section of the configuration file to the GSSAPI service name of the License Server. For example:

  ```
  [License]
  GSSServiceName=LICENSESERVER
  ```

- The `Admin`, `Help`, `LoadDoc`, and `LoadImage` actions now set the HTTP response header `Content-Security-Policy`, to improve security against cross-site scripting. If the `Content-Type` header is set, these actions also set the header `X-Content-Type-Options: nosniff`.

Resolved Issues

- Process group variables and parameters were not respected by the **BROWSE** tab in the advanced configuration dialog of the NiFi Ingest connector.

- The connector could not connect to NetWare file systems.

Find

New in this Release

- When using a reverse proxy, you can now instruct Find to use roles and security info from Community. Previously, when using a reverse proxy to pass user information to Find over AJP, you were required to configure a fixed set of user roles, or use the default set.

  To use the Community role option, you must start Find with the command-line option `-Dfind.reverse-proxy.pre-authenticated-roles=` (as an empty value). You must also make sure your Community configuration has the `CheckEntitlement` parameter set to False (the default value).

Resolved Issues

There were no resolved issues in Find version 12.9.0.

HTTP Connector (Solaris only)

New in this Release

- The connector can communicate with other IDOL components that have been configured to require GSSAPI authentication. To enable this, set the `GSSServiceName` parameter in the `[Ingestion]`, `[DistributedConnector]`, and `[ViewServer]` sections of the configuration file, for requests to CFS, Distributed Connector, and IDOL View Server respectively.

- ACI servers can now communicate with a License Server that requires a GSSAPI authenticated connection (that is, where the License Server configuration has `RequireGSSAuth` set to **True**). To allow this communication, you must set `GSSServiceName` in the `[License]` section of the configuration file to the GSSAPI service name of the License Server. For example:

  ```
  [License]
  GSSServiceName=LICENSESERVER
  ```

- The `Admin`, `Help`, `LoadDoc`, and `LoadImage` actions now set the HTTP response header `Content-Security-Policy`, to improve security against cross-site scripting. If the `Content-Type` header is set, these actions also set the header `X-Content-Type-Options: nosniff`.

Resolved Issues

There were no resolved issues in HTTP Connector version 12.9.0.

IDOL Admin

New in this Release

There were no new features in IDOL Admin version 12.9.0.

Resolved Issues

- A cross-site scripting vulnerability has been resolved.

IDOL Proxy Component

New in this Release

- ACI servers can now communicate with a License Server instance that requires a GSSAPI authenticated connection (that is, where the License Server configuration has `RequireGSSAuth` set to **True**). To allow this communication, you must set `GSSServiceName` in the `[License]`

section of the configuration file to the GSSAPI service name of the License Server. For example:

```
[License]
GSSServiceName=LICENSESERVER
```

- The third-party OpenSSL library has been updated to 1.1.1.j.

- The `Admin`, `Help`, `LoadDoc`, and `LoadImage` actions now set the HTTP response header `Content-Security-Policy`, to improve security against cross-site scripting. If the `Content-Type` header is set, these actions also set the header `X-Content-Type-Options: nosniff`.

Resolved Issues

There were no resolved issues in IDOL Proxy Component version 12.9.0.

IDOL Site Admin

New in this Release

There were no new features in IDOL Site Admin version 12.9.0.

Resolved Issues

- A cross-site scripting vulnerability has been resolved.

Knowledge Graph Component

New in this Release

- ACI servers can now communicate with a License Server instance that requires a GSSAPI authenticated connection (that is, where the License Server configuration has `RequireGSSAuth` set to `True`). To allow this communication, you must set `GSSServiceName` in the `[License]` section of the configuration file to the GSSAPI service name of the License Server. For example:

```
[License]
GSSServiceName=LICENSESERVER
```

- The third-party OpenSSL library has been updated to 1.1.1.j.

- The `Admin`, `Help`, `LoadDoc`, and `LoadImage` actions now set the HTTP response header `Content-Security-Policy`, to improve security against cross-site scripting. If the `Content-Type` header is set, these actions also set the header `X-Content-Type-Options: nosniff`.

Resolved Issues

There were no resolved issues in Knowledge Graph version 12.9.0.

License Server

New in this Release

- The third-party OpenSSL library has been updated to 1.1.1.j.

- The `Admin`, `Help`, `LoadDoc`, and `LoadImage` actions now set the HTTP response header `Content-Security-Policy`, to improve security against cross-site scripting. If the `Content-Type` header is set, these actions also set the header `X-Content-Type-Options: nosniff`.

Resolved Issues

There were no resolved issues in License Server version 12.9.0.

Media Server (Windows and Linux only)

New in this Release

- Object class recognition supports a new type of recognizer that provides better accuracy, especially with recognizers that you have trained yourself. The new recognizer type is named `Generation4`. New pre-trained `Generation4` recognizers are available in the pre-trained models package (`ObjectClassRecognizer_Gen4_CommonObjects80.dat` and `ObjectClassRecognizer_Gen4_Surveillance.dat`).

- Media Server caches more information in memory, to reduce the number of queries sent to the database during process actions that include image classification or object class recognition. Previous versions of Media Server cached the models needed to classify images or recognize objects. Media Server 12.9 also caches associated data, such as class names and metadata.

- The performance of object class recognition has improved when the source media has a non-square aspect ratio. The improvement is most noticeable when processing on a CPU (rather than a GPU), with wider aspect ratios such as 16:9. Media Server completes processing these images and video frames in less time than before.

- Media Server generates a unique `id` for each clothing analysis result, so that you can match color clusters to the correct clothing result when you analyze multiple clothing regions. This was not possible in previous version of Media Server, because the clothing analysis results for the full body, upper body, and lower body all had the same `id`. Consequently, the `id` in a clothing analysis result no longer corresponds to a detected face or recognized person, but a new `parentID` element has been added to contain the identifier of the input record.

- Number plate recognition has been enhanced. Media Server supports some new number plate formats introduced recently in the United Arab Emirates. Accuracy has also been improved for UAE plates, particularly those from Abu Dhabi. Some additional number plate formats were added for Taiwan and accuracy has been improved for Taiwanese plates.

- Face recognition accuracy has improved. After upgrading to Media Server 12.9, re-train all of the faces in your training database by running the action `BuildAllFaces`.

- OCR accuracy has improved when `OCRMode=scene`.

- Media Server always uses the extension `.xml` for pre-XML output files, regardless of the extension you set in the `XMLOutputPath` parameter. This is helpful in cases where your post-XML is in another format and has a different file extension, such as `.idx`.

- The response of the `process` action (that you see using the `QueueInfo` action when you run the `process` action asynchronously) includes a new `<configname>` element that identifies the configuration that was used to process the media. The element can contain a path, a file name, or the value "Base64 data".

- The speech-to-text language pack for Spanish (`ESES` - 16kHz broadband) has been improved.

- ACI servers can now communicate with a License Server instance that requires a GSSAPI authenticated connection (that is, where the License Server configuration has `RequireGSSAuth` set to **True**). To allow this communication, you must set `GSSServiceName` in the `[License]` section of the configuration file to the GSSAPI service name of the License Server. For example:

```
[License]
GSSServiceName=LICENSESERVER
```

- The third-party OpenSSL library has been updated to 1.1.1.j.

- The `Admin`, `Help`, `LoadDoc`, and `LoadImage` actions now set the HTTP response header `Content-Security-Policy`, to improve security against cross-site scripting. If the `Content-Type` header is set, these actions also set the header `X-Content-Type-Options: nosniff`.

Resolved Issues

- Media Server could terminate unexpectedly when processing some PDF files.

- Object class recognition training could fail when there was a space in the name of a recognizer or the absolute path of the Media Server directory.

- Optical Character Recognition could use more threads than specified by the `NumParallel` parameter, for part of its analysis.

- Media Server could terminate unexpectedly when records contained a large number of nested elements and those records were processed by a Lua script.

- After training image classification or object class recognition, any attempt to run another action that required the GPU would result in the error "attempted to use too much GPU memory". This issue was only present in Media Server version 12.8.1 and occurs only when GPU acceleration is enabled.

- Media Server would terminate unexpectedly on startup, when run on Linux with GPU acceleration enabled.

- Media Server could stop responding when running GPU-enabled ANPR, Face Recognition, Image Classification, or Object Class Recognition on either Windows or Linux.

Query Manipulation Server Component

New in this Release

- ACI servers can now communicate with a License Server instance that requires a GSSAPI authenticated connection (that is, where the License Server configuration has `RequireGSSAuth` set to `True`). To allow this communication, you must set `GSSServiceName` in the `[License]` section of the configuration file to the GSSAPI service name of the License Server. For example:

```
[License]
GSSServiceName=LICENSESERVER
```

- The third-party OpenSSL library has been updated to 1.1.1.j.

- The `Admin`, `Help`, `LoadDoc`, and `LoadImage` actions now set the HTTP response header `Content-Security-Policy`, to improve security against cross-site scripting. If the `Content-Type` header is set, these actions also set the header `X-Content-Type-Options: nosniff`.

Resolved Issues

There were no resolved issues in Query Manipulation Server version 12.9.0.

Statistics Server Component

New in this Release

- ACI servers can now communicate with a License Server instance that requires a GSSAPI authenticated connection (that is, where the License Server configuration has `RequireGSSAuth` set to `True`). To allow this communication, you must set `GSSServiceName` in the `[License]` section of the configuration file to the GSSAPI service name of the License Server. For example:

```
[License]
GSSServiceName=LICENSESERVER
```

- The third-party OpenSSL library has been updated to 1.1.1.j.

- The `Admin`, `Help`, `LoadDoc`, and `LoadImage` actions now set the HTTP response header `Content-Security-Policy`, to improve security against cross-site scripting. If the `Content-Type` header is set, these actions also set the header `X-Content-Type-Options: nosniff`.

Resolved Issues

There were no resolved issues in Statistics Server version 12.9.0.

View Server Component

New in this Release

- When generating constructed link URLs in documents, View now uses a root-relative default format (starting with the slash (/) character), rather than absolute (starting with `http://` or `https://` and the View component host and port). These links work in a wider range of scenarios.

  This change applies to the default value of `URLPrefix` (if `DefaultURLPrefix` is not configured), and to the default values of `AbsoluteLinkPrefix` and `AbsoluteImagePrefix` when `RedirectAbsoluteLinks` is turned on.

  If required, you can restore the previous behavior by setting the new `UseAbsoluteURLDefaults` configuration parameter to **True** in the `[Viewing]` section of your configuration file.

- ACI servers can now communicate with a License Server instance that requires a GSSAPI authenticated connection (that is, where the License Server configuration has `RequireGSSAuth` set to **True**). To allow this communication, you must set `GSSServiceName` in the `[License]` section of the configuration file to the GSSAPI service name of the License Server. For example:

  ```
  [License]
  GSSServiceName=LICENSESERVER
  ```

- The third-party OpenSSL library has been updated to 1.1.1.j.

- The `Admin`, `Help`, `LoadDoc`, and `LoadImage` actions now set the HTTP response header `Content-Security-Policy`, to improve security against cross-site scripting. If the `Content-Type` header is set, these actions also set the header `X-Content-Type-Options: nosniff`.

Resolved Issues

- View printed some logging messages to stdout.

- When opening some PDF files, View could exit unexpectedly.

- When `EmbedImages` was set to **True** in the `View` action, View sometimes displayed a black square in place of the image. `EmbedImages` now works correctly with KeyView Export functionality.

Web Connector (Windows and Linux only)

New in this Release

- The embedded web browser has been updated to Chromium version 90.0.4392.1 for all platforms, except `RHEL7FIPS` where Web Connector uses Qt Webkit 5.1.1.

- The connector can communicate with other IDOL components that have been configured to require GSSAPI authentication. To enable this, set the `GSSServiceName` parameter in the `[Ingestion]`, `[DistributedConnector]`, and `[ViewServer]` sections of the configuration file, for requests to CFS, Distributed Connector, and IDOL View Server respectively.

- ACI servers can now communicate with a License Server that requires a GSSAPI authenticated connection (that is, where the License Server configuration has `RequireGSSAuth` set to **True**). To allow this communication, you must set `GSSServiceName` in the `[License]` section of the configuration file to the GSSAPI service name of the License Server. For example:

```
[License]
GSSServiceName=LICENSESERVER
```

- The `Admin`, `Help`, `LoadDoc`, and `LoadImage` actions now set the HTTP response header `Content-Security-Policy`, to improve security against cross-site scripting. If the `Content-Type` header is set, these actions also set the header `X-Content-Type-Options: nosniff`.

Resolved Issues

- The number of errors reported in the `<documentcount>` element of a fetch action response could be incorrect because some errors were counted twice.

- Process group variables and parameters were not respected by the **BROWSE** tab in the advanced configuration dialog of the NiFi Ingest connector.

Requirements

This section describes the system requirements, supported platforms, and software dependencies for IDOL Server 12.9.0.

Minimum System Requirements

The following are minimum system requirements for IDOL Server 12.9.0 on any supported operating system platform:

- a dedicated SCSI disk
- 4 GB RAM
- 100 GB disk space
- a minimum of 2 dedicated CPU - Intel Xeon or AMD Opteron or above

To run IDOL Server version 12.9.0, or its components, on UNIX platforms, the server must have the following minimum versions of libraries:

- GLIBC_2.3.2
- GLIBCXX_3.4.21
- GCC_4.8.0

> **NOTE:** The IDOL Server installer and component stand-alone zip packages provide these libraries in the `libgcc_s` and `libstdc++` shared libraries.
>
> If you start components from the command line (rather than using the init script), you might need to set the `LD_LIBRARY_PATH` to include the *InstallDir*/common and *InstallDir*/common/runtimes directories, to ensure that the component can access the installed shared libraries.
>
> You can also copy the shared libraries to the component working directory.

To run IDOL Server version 12.9.0 on the Microsoft Windows operating system, you might need to install Microsoft Visual C++ Redistributable packages. The IDOL Server installer includes the required redistributable files for Microsoft Visual C++ 2019, 2017, and 2013. You can also update your packages by using the latest version at: http://support.microsoft.com/kb/2019667.

Software Dependencies

Some IDOL Server components depend on specific third-party or other Micro Focus IDOL software. The following table details the IDOL Server software and feature dependencies.

Component	Dependencies

Find	Java Runtime Rnvironment (JRE) 8 or 11
IDOL Data Admin	Java Runtime Environment (JRE) 8 or 11
IDOL NiFi Ingest	Java Runtime Environment (JRE) 8
IDOL Site Admin	Java Runtime Environment (JRE) 8 or 11
MMAP	Java Runtime Environment (JRE) 8 or 11
Browsers	- Mozilla Firefox (latest version) - Chrome (latest version)

Supported Operating System Platforms

IDOL Server 12.9.0 is supported on the following platforms.

Windows (x86-64)

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012

Linux (x86-64)

The minimum supported versions of particular distributions are:

- Red Hat Enterprise Linux (RHEL) 6
- CentOS 6
- SuSE Linux Enterprise Server (SLES) 12
- Ubuntu 14.04
- Debian 8

Solaris (x86-64 and SPARC 64)

- Solaris 11
- Solaris 10

Some components, for example IDOL Media Server and IDOL Web Connector, are not available on Solaris.

Notes

- As a result of changes made to support TLS version 1.3:

  ○ Certificates that use outdated signature algorithms such as `md5WithRSAEncryption` must be replaced with certificates that use a more secure algorithm, such as `sha256WithRSAEncryption`.

  ○ RC4 ciphers are no longer supported.

- If you are running IDOL server on the Solaris operating system, ensure you specify an installation path that is less than 30 characters. This prevents an issue with the stop script.

- The autpassword command-line tool has been updated to provide hardened AES encryption for passwords. Micro Focus strongly recommends that you reencrypt all passwords in configuration files by using the updated tool.

  The older AES encryption format and basic encryption methods are now deprecated. Passwords that you have encrypted with older versions continue to work, but the server logs a warning. Support for these older encryption methods will be removed in future.

- The provided default configuration files for many IDOL components now define the following sections from a common configuration file, `idol.common.cfg`: `[License]`, `[AdminRole]`, `[QueryRole]`, `[IndexRole]`, `[Logging]`, `[ApplicationLogStream]`, `[QueryLogStream]`, and `[IndexLogStream]`.

Content

- The default Agentstore configuration files now include an `AlwaysMatchType` field with `PropertyFieldCSVS=*/ALWAYSMATCH`.

- The provided default configuration files now define the following sections from a common configuration file, `idol.common.cfg`: `[License]`, `[AdminRole]`, `[QueryRole]`, `[IndexRole]`, `[Logging]`, `[ApplicationLogStream]`, `[QueryLogStream]`, and `[IndexLogStream]`.

- **Deprecated Features**

  The following features are deprecated and might be removed in a future release.

Category	Deprecated Feature	Deprecated Since
Configuration	The `HMACValidation` configuration parameter. In version 12.9.0, the AES implementation for encrypting security info strings was updated to include built-in authentication, so additional HMAC validation is no longer required or supported.	12.9.0

Configuration	The `NGramOrientalOnly` configuration parameter. You must now use the equivalent `NGramSentenceBrokenScriptOnly` parameter instead.	12.7.0

Community

- The provided default configuration files now define the following sections from a common configuration file, `idol.common.cfg`: `[License]`, `[AdminRole]`, `[QueryRole]`, `[IndexRole]`, `[Logging]`, `[ApplicationLogStream]`, `[QueryLogStream]`, and `[IndexLogStream]`.

- **Deprecated Features**

  The following features are deprecated and might be removed in a future release.

Category	Deprecated Feature	Deprecated Since
Configuration	The `HMACValidation` configuration parameter. In version 12.9.0, the AES implementation for encrypting security info strings was updated to include built-in authentication, so additional HMAC validation is no longer required or supported.	12.9.0

Eduction

Deprecated Features

The following features have been deprecated.

Category	Deprecated Feature	Deprecated Since
Configuration	`[PostProcessingTasks]` configuration section. Use the `PostProcessingTaskN` and `PostProcessThreshold` parameters in the `[Eduction]` section.	12.5

Media Server

- Media Server 12.9 generates a unique `id` for each clothing analysis result, so that you can match color clusters to the correct clothing result when you analyze multiple clothing regions. Consequently, the `id` in a clothing analysis result no longer corresponds to a detected face or recognized person, but a new `parentID` element has been added to contain the identifier of the input record.

- Face recognition accuracy has improved. After upgrading to Media Server 12.9, re-train all of the faces in your training database by running the action `BuildAllFaces`.

- The XML output engine has a new parameter, named `OutputPath`, for setting the path of the output files. The parameter `XMLOutputPath` is now optional, and specifies the path of pre-XML output for debugging purposes. This means that `XMLOutputPath` now has the same purpose for all output engines. Micro Focus recommends that you update your XML output task configurations by adding the parameter `OutputPath`.

- The default value of the OCR configuration parameter `WordRejectThreshold` has been changed from `1` to `0`.

Deprecated Features

The following features are deprecated and might be removed in a future release.

Category	Deprecated Feature	Deprecated Since
Session configuration	The `RestrictToInputRegion` configuration parameter has been deprecated. Micro Focus recommends setting `Region=Input` instead.	12.7.0
Session configuration	To simplify configuration, units can be specified in the same parameter as the corresponding value. As a result the following configuration parameters have been deprecated: • `BorderUnit` (Crop transformation) • `CharHeightUnit` (Number plate recognition, text detection) • `PathUnit` (Path alerts) • `RegionUnit` • `SizeUnit` (Face detection, object recognition, persistent change detection) • `TripwireUnit` (Tripwire alerts) Micro Focus recommends that you update your session configurations. For example, if you have a configuration that sets the `Region` parameter, add units alongside the parameter value. If the parameters listed above are removed in a future version of Media Server, values without units will become invalid.	12.7.0
Databases	The `ODBCDriverManager` parameter (in the `[Database]` section of the Media Server configuration file, and for output engines that use ODBC). You no longer need to set this parameter.	12.6.0

Actions	The `GetLatestRecord` action. The new actions `KeepLatestRecords` and `GetLatestRecords` provide more control over what to store and retrieve.	12.5.0
Event Stream Processing	The `MinTimeInterval` and `MaxTimeInterval` parameters for the `And`, `AndThen`, `AndAny`, `AndThenAny`, `AndNot`, `AndNotThen`, and `Combine` engines. Micro Focus recommends using the new configuration parameter `TimestampCondition` instead.	12.3.0
Server / Service	The `AdminClients`, `QueryClients`, `ServiceControlClients`, and `ServiceStatusClients` configuration parameters. Micro Focus recommends that you use authorization roles instead.	11.5.0
Rolling buffer	The action parameter `name`, available on the actions `AddStream`, `EditStream`, `GetStreamInfo`, `PreAllocateStorage`, and `RemoveStream`. Micro Focus recommends that you use the parameter `stream`, instead. The action parameters `OldName` and `NewName`, on the action `RenameStream`. Micro Focus recommends that you use the parameters `Stream` and `NewStream` instead.	11.4.0

Removed Features

The following deprecated features have been removed.

- All deprecated fields have been removed from the output of Audio Matching and Speaker ID.

Documentation

The following documentation was updated for IDOL Server version 12.9.0.

- *IDOL Expert*

- *IDOL Getting Started Guide*

- *IDOL Server Reference* (online help)

- *IDOL Server Administration Guide*

- *IDOL Document Security Administration Guide*

- *Distributed Action Handler Reference* (online help)

- *Distributed Action Handler Administration Guide*

- *Distributed Index Handler Reference* (online help)

- *Distributed Index Handler Administration Guide*

- *License Server Reference* (online help)

- *License Server Administration Guide*

- *Connector Framework Server Reference* (online help)

- *Connector Framework Server Administration Guide*

- *File System Connector Help*

- *HTTP Connector Help*

- *Web Connector Help*

- *QMS Reference* (online help)

- *QMS Administration Guide*

- *Media Server Reference* (online help)

- *Media Server Administration Guide*

- *Controller Reference*

- *Coordinator Reference*

- *Knowledge Graph Reference* (online help)

- *Knowledge Graph Administration Guide*

- *Find Administration Guide*

- *IDOL Site Admin Installation Guide*

- *IDOL Site Admin User Guide*