MICRO FOCUS®

IDOL Server

Software Version: 11.6.2

Release Notes

Legal notices

Warranty

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

Restricted rights legend

Confidential computer software. Except as specifically indicated, valid license from Seattle required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright notice

© Copyright 2018 EntIT Software LLC, a Micro Focus company

Trademark notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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 verify you are using the most recent edition of a document, go to https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=online help.

This site requires you to sign in with a Software Passport. You can register for a Passport through a link on the site.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your Micro Focus sales representative for details.

Support

Visit the Micro Focus Software Support Online website at https://softwaresupport.softwaregrp.com.

This website provides contact information and details about the products, services, and support that Micro Focus offers.

Micro Focus online support provides customer self-solve capabilities. It provides 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 support website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Access the Software Licenses and Downloads portal
- Download software patches
- Access product documentation
- Manage support contracts

- Look up Micro Focus support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require you to register as a Passport user and sign in. Many also require a support contract.

You can register for a Software Passport through a link on the Software Support Online site.

To find more information about access levels, go to https://softwaresupport.softwaregrp.com/web/softwaresupport/access-levels.

Contents

New in this Release

The following sections describe the enhancements for the components of IDOL Server version 11.6.2.

Content Component

New in this Release

The following enhancements were added in IDOL Content Component version 11.6.2.

- Resilience to errors has been improved when updating the XML field names file (`main/xmln.db`).

This section lists the enhancements to IDOL Server version 11.6.0.

- When `NodetableCompression` is enabled, decompressing large documents now uses less overhead memory.

- The new `DefaultOperator` parameter has been added to the `Query`, `GetQueryTagValues`, `GetContent`, and `Highlight` actions. This parameter sets the default operator to use between the terms in a query. It overrides the `DefaultQueryOperator` configuration parameter.

  > **NOTE:**
  > If you distribute actions to Content by using a DAH, you must also update DAH to 11.6 or later to use this parameter.

- You can now turn off the best term hash, by setting the new `BestTermHash` configuration parameter in the `[Server]` section. This option might increase indexing speed in cases where you are regularly adding a very large number of new terms, at the expense of increasing the disk I/O when best term information is required (such as `QuerySummary` and `Suggest`).

- The `TermGetBest` and `TermGetInfo` actions now allow you to show the unmodified query term weights, rather than the default suggestion weights, by setting the `ShowQueryWeights` parameter. This option might be useful if you want to use the term weight results as a basis to create a custom term file.

- You can now show term weight information in the `TermGetAll` action, by setting the `Weights` parameter.

- The `GetQueryTagValues` action now respects value ranges when `FieldDependenceMultiLevel` is set to **True**. Previously, the action returned values individually, rather than bracketing them into ranges. This change applies to configured `ParametricRangeType` fields, and fields with custom ranges supplied by using the `FIXED` or `FIXEDDATE` range specifiers in the action.

  > **NOTE:**
  > If you distribute actions to Content by using a DAH, you must also update DAH to 11.6 or later to use this option.

- Unstemmed processing has been improved so that Content writes out the unstemmed settings file only when required, rather than at every unstemmed flush.

- You can now configure your authorization role `SSLIdentities` to identify clients by using an email address in the certificate `subjectAltName`. You can use an optional tag for each SSL identity to specify whether it is a **dns** or **email** type identity. If there is no tag, the server treats it as **dns** type. For example:

  `SSLIdentities=email:user@example.com,dns:admin.example.com,webapp.example.com`

- When using GSS security, you can now configure the service to allow clients to authenticate to any service principal in the service's keytab, rather than requiring a single principal. You use this option by setting the `GSSServiceName` configuration parameter to an asterisk (*).

Resolved Issues

The following issues were resolved in IDOL Content Component version 11.6.2.

- Javascript could be injected into the `GetRequestLog` response by sending actions to the server.
- When using `SearchUncommittedDocuments` and when the index had more than one dynterm set, a `DRECOMPACT` operation could result in an interruption of service.
- Running a `GetStatus` action while the `DRERESIZEINDEXCACHE` index action was processing could result in an interruption of service.
- Content did not restore status files (stored in the directory configured by `[Paths] StatusPath`) from a backup when `BackupCompression` was set to **True**.
- The `DRECOMPACT` index action could cause inconsistencies in large dynterm indexes (with more than approximately 12GB of term data). Processing the affected data could subsequently cause an interruption of service.
- An interruption of service could occur when Content returned the data for a document with more than 100,000 fields at a single level.
- On an index where `RepositoryStorage` mode was turned off, the `DREVALIDATE` index action could return errors.

The following issues were resolved in IDOL Content Component version 11.6.0

- In servers that use asynchronous actions and where you have document security enabled, sending a `DREINITIAL` index action could result in an interruption of service if the number of synchronous threads plus twice the number of asynchronous threads was more than 32.
- Using an `AND`-type operator as the `DefaultQueryOperator` could result in the `SYNONYM` operator returning fewer results than expected if the `SYNONYM` contained phrases or exact stem matches.
- When `Highlight` was set to **Proximity** in a query action and the `XMLFullStructure` configuration parameter was set to **True**, highlighting could miss simple terms.
- Terms that did not satisfy the `IndexNumbers` criteria were not counted in term proximity by the `Query` action, but were counted by the `GetContent` action when doing `Boolean` highlighting. Position counting is now consistent between `Query`, `GetContent` with `Boolean` set to **True**, and the `Highlight` action with `TextParse` set to **True**. The `Highlight` action for plain text continues to count all numeric and alphanumeric terms in term proximity, regardless of the `IndexNumbers` configuration.
- If the first entry in an index field was a proper names chunk (for example, *A Smith went to town…*,

where the first term is ASMITH and has no position) then attempting proximity based highlighting on that field could result in an interruption of service.

- When using sentence breaking for a language, Content did not highlight synonym terms if they occurred at the start of a field.

- The response to the GetQueryTagValues action sometimes listed uncommon values with a count of zero (rather than 1), when Predict was set to True. When the request was sent through a DAH, the DAH response sometimes missed the count attributes for these values.

- If a custom sentence breaking library used the four sentence breaking mark syntax, wildcard searches could fail to return results.

- License related messages in the event log would appear from a different source to other messages.

Category Component

New in this Release

The following enhancements were added in IDOL Category Component version 11.6.0.

- You can now configure the background color for a generated spectrograph, by setting the SGBackgroundColor configuration parameter in the [Cluster] section.

- You can now configure your authorization role SSLIdentities to identify clients by using an email address in the certificate subjectAltName. You can use an optional tag for each SSL identity to specify whether it is a **dns** or **email** type identity. If there is no tag, the server treats it as **dns** type. For example:

  SSLIdentities=email:user@example.com,dns:admin.example.com,webapp.example.com

- When using GSS security, you can now configure the service to allow clients to authenticate to any service principal in the service's keytab, rather than requiring a single principal. You use this option by setting the GSSServiceName configuration parameter to an asterisk (*).

Resolved Issues

The following issues were resolved in IDOL Category Component version 11.6.2.

- Javascript could be injected into the GetRequestLog response by sending actions to the server.

The following issues were resolved in IDOL Category Component version 11.6.0

- License related messages in the event log would appear from a different source to other messages.

Community Component

New in this Release

The following enhancements were added in IDOL Community Component version 11.6.0.

- You can now encrypt a security configuration as a security info string by using the new `UserEncryptSecurityInfo` action.

- You can now define your own user password complexity rules by using a Lua script. The new `UserLuaScript` configuration parameter allows you to set the location of a Lua script to use. This script must define a `password_complexity_check` function, which must accept the password string as an argument, and returns a Boolean value (**true** if the password is acceptable). You can use this option with the existing `PasswordStrength` parameter, in which case, Community runs the Lua script first.

- Community supports the following new Lua functions:

  - `deleteFieldByPath`, which you can call on a `LuaDocument` or `LuaField` object to delete fields or sub-fields that match a specified path.

  - `getFieldsByRegex`, which you can call on a `LuaDocument` or `LuaField` object to get fields or sub-fields where the name or path of the field or sub-field matches a regular expression.

- You can now configure your authorization role `SSLIdentities` to identify clients by using an email address in the certificate `subjectAltName`. You can use an optional tag for each SSL identity to specify whether it is a **dns** or **email** type identity. If there is no tag, the server treats it as **dns** type. For example:

  `SSLIdentities=email:user@example.com,dns:admin.example.com,webapp.example.com`

- When using GSS security, you can now configure the service to allow clients to authenticate to any service principal in the service's keytab, rather than requiring a single principal. You use this option by setting the `GSSServiceName` configuration parameter to an asterisk (*).

Resolved Issues

The following issues were resolved in IDOL Community Component version 11.6.2.

- Javascript could be injected into the `GetRequestLog` response by sending actions to the server.

The following issues were resolved in IDOL Community Component version 11.6.0

- License related messages in the event log would appear from a different source to other messages.

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

The following enhancements were added in CFS version 11.6.0.

- CFS can send files to Media Server using HTTP POST requests. This means that in some cases you no longer need to configure a shared folder. Micro Focus recommends that you continue to use a shared folder if you are analyzing large files.

- CFS supports the following Lua functions:

- ○ `deleteFieldByPath`, which you can call on a `LuaDocument` or `LuaField` object to delete fields or sub-fields that match a specified path.

- ○ `getFieldsByRegex`, which you can call on a `LuaDocument` or `LuaField` object to get fields or sub-fields where the name or path of the field or sub-field matches a regular expression.

- XML processing has been improved.

  - ○ XML schema and transforms are loaded when CFS starts. If a schema or transform is invalid, CFS writes a message to the application log and stops.

  - ○ CFS writes a message to the action log whenever an XML transform is used.

  - ○ CFS can log the reasons why an ingested XML file does not match a schema. This feature is for troubleshooting purposes only and should not be used in a production system. To enable it, set `LogValidationErrors=TRUE`.

  - ○ When an XML transformation or conversion into IDOL documents fails, CFS adds the document to the import queue so that it is processed by KeyView. The only exception to this rule is when an XML file matches a schema and is transformed successfully, but does not result in any IDOL documents. This is not considered a failure and no documents are indexed.

- CFS includes an XSL template to help you send `IngestTest` actions. To use the template, open a web browser and navigate to `http://host:7000/action=IngestTest&Template=IngestTest` (where *host* is the machine where CFS is running and `7000` is the CFS ACI port). Micro Focus does not support the XSL template, it is provided only as an example of a template that you could build.

- CFS generates an event when the import queue or the outgoing queue for indexing becomes full, becomes empty, or the size of the queue passes certain thresholds. You can handle these events with any of the existing event handlers. For example, you might run a Lua script that notifies an administrator if a queue becomes more than 80 percent full.

- When you run Eduction, you can choose the document fields to search using wildcards and regular expressions (in the value of the `SearchFields` parameter).

- The server generates events to alert you when an asynchronous action queue becomes full, becomes empty, and when the queue size passes certain thresholds. You can handle these events with any of the existing event handlers.

- You can now configure your authorization role `SSLIdentities` to identify clients by using an email address in the certificate `subjectAltName`. You can use an optional tag for each SSL identity to specify whether it is a **dns** or **email** type identity. If there is no tag, the server treats it as **dns** type. For example:

  `SSLIdentities=email:user@example.com,dns:admin.example.com,webapp.example.com`

- When using GSS security, you can now configure the service to allow clients to authenticate to any service principal in the service's keytab, rather than requiring a single principal. You use this option by setting the `GSSServiceName` configuration parameter to an asterisk (*).

Resolved Issues

The following issues were resolved in Connector Framework Server version 11.6.2.

- Javascript could be injected into the `GetRequestLog` response by sending actions to the server.

The following issues were resolved in Connector Framework Server version 11.6.0

- Language detection always reported the language of a document as "unknown".

- The `LogSysLog` logging configuration option did not output event logs.
- License related messages in the event log would appear from a different source to other messages.

Controller

New in this Release

The following enhancements were added in Controller version 11.6.0.

- Date processing has been improved for the scheduling actions:
  - For the `AddSchedule` and `EditSchedule` actions, the `ScheduleStart` and `ScheduleEnd` parameters, and the `Schedule` XML now accept a date in the ISO-8601 format `YYYY-MM-DDTHH:NN:SS.FFFFZ`.
  - All actions now return all dates in UTC.
  - You can now specify the date format that you want to use in the schedule action responses by setting the `ResponseDateFormat` parameter. This allows you to return dates in `AUTNDATE` or ISO-8601 format, or in a custom format that you define. This parameter is available for `AddSchedule`, `EditSchedule`, `GetSchedules`, `PauseSchedule`, and `ResumeSchedule`.

- The diagnostic action now copies the `controllerinfo.cfg` and `serviceinfo.cfg` files to the diagnostic package if they are available. Note that if you use a remote database to store your service and controller information, those details might not be present in the local files.

- You can now configure a timeout for scheduled actions. You can set the `ScheduleActionTimeout` parameter in the `AddSchedule` and `EditSchedule` actions to specify the number of seconds that Controller waits before timing out the action. You can also configure the default value by setting `DefaultActionTimeout` in the `[Scheduler]` configuration section.

- You can now configure timeouts for the `SendAction` action. You can set the `SendActionConnectTimeout` and `SendActionReadTimeout` configuration parameters in the `[Server]` section to specify the number of seconds to wait for connecting to the component and reading the response, respectively.

- Controller supports the new `deleteFieldByPath` Lua function, which you can call on a `LuaDocument` or `LuaField` object to delete fields or sub-fields that match a specified path.

- Controller supports the following new Lua functions:
  - `deleteFieldByPath`, which you can call on a `LuaDocument` or `LuaField` object to delete fields or sub-fields that match a specified path.
  - `getFieldsByRegex`, which you can call on a `LuaDocument` or `LuaField` object to get fields or sub-fields where the name or path of the field or sub-field matches a regular expression.

- You can now configure your authorization role `SSLIdentities` to identify clients by using an email address in the certificate `subjectAltName`. You can use an optional tag for each SSL identity to specify whether it is a **dns** or **email** type identity. If there is no tag, the server treats it as **dns** type. For example:

  ```
  SSLIdentities=email:user@example.com,dns:admin.example.com,webapp.example.com
  ```

- When using GSS security, you can now configure the service to allow clients to authenticate to any service principal in the service's keytab, rather than requiring a single principal. You use this option by setting the `GSSServiceName` configuration parameter to an asterisk (*).

Resolved Issues

The following issues were resolved in Controller version 11.6.2.

- Javascript could be injected into the `GetRequestLog` response by sending actions to the server.

The following issues were resolved in Controller version 11.6.0

- After a restart, Controller could not schedule index actions.

- License related messages in the event log would appear from a different source to other messages.

- The `LogSysLog` logging configuration option did not output event logs.

Coordinator

New in this Release

The following enhancements were added in Coordinator version 11.6.0.

- The diagnostic action now copies the `controllerinfo.cfg` and `serviceinfo.cfg` files to the diagnostic package if they are available. Note that if you use a remote database to store your service and controller information, those details might not be present in the local files.

- You can now configure a timeout for scheduled actions. You can set the `ScheduleActionTimeout` parameter in the `AddSchedule` and `EditSchedule` actions to specify the number of seconds that Coordinator waits before timing out the action. You can also configure the default value by setting `DefaultActionTimeout` in the `[Scheduler]` configuration section, which by default uses the configured value in Controller.

- You can now configure timeouts for the `SendAction` action. You can set the `SendActionConnectTimeout` and `SendActionReadTimeout` configuration parameters in the `[Server]` section to specify the number of seconds to wait for connecting to the component and reading the response, respectively.

- You can now configure your authorization role `SSLIdentities` to identify clients by using an email address in the certificate `subjectAltName`. You can use an optional tag for each SSL identity to specify whether it is a **dns** or **email** type identity. If there is no tag, the server treats it as **dns** type. For example:

    `SSLIdentities=email:user@example.com,dns:admin.example.com,webapp.example.com`

- When using GSS security, you can now configure the service to allow clients to authenticate to any service principal in the service's keytab, rather than requiring a single principal. You use this option by setting the `GSSServiceName` configuration parameter to an asterisk (*).

Resolved Issues

The following issues were resolved in Coordinator version 11.6.2.

- Javascript could be injected into the `GetRequestLog` response by sending actions to the server.

The following issues were resolved in Coordinator version 11.6.0

- License related messages in the event log would appear from a different source to other messages.

- The `LogSysLog` logging configuration option did not output event logs.

Distributed Action Handler

New in this Release

The following enhancements were added in DAH version 11.6.0.

- DAH was updated to process the new `DefaultOperator` parameter in the `Query`, `GetQueryTagValues`, `GetContent`, and `Highlight` actions.

- DAH was updated to process value ranges in the `GetQueryTagValues` action when `FieldDependenceMultiLevel` is set to **True**.

- You can now configure your authorization role `SSLIdentities` to identify clients by using an email address in the certificate `subjectAltName`. You can use an optional tag for each SSL identity to specify whether it is a **dns** or **email** type identity. If there is no tag, the server treats it as **dns** type. For example:

  `SSLIdentities=email:user@example.com,dns:admin.example.com,webapp.example.com`

- When using GSS security, you can now configure the service to allow clients to authenticate to any service principal in the service's keytab, rather than requiring a single principal. You use this option by setting the `GSSServiceName` configuration parameter to an asterisk (*).

Resolved Issues

The following issues were resolved in Distributed Action Handler version 11.6.2.

- Javascript could be injected into the `GetRequestLog` response by sending actions to the server.

The following issues were resolved in Distributed Action Handler version 11.6.0

- DAH did not always correctly pass full `DatabaseMatch` parameters to child servers.

- DAH would incorrectly log errors when processing a `LanguageSettings` action.

- DAH did not use the configured `GSSServiceName` when obtaining outgoing credentials using the service's client keytab.

- License related messages in the event log would appear from a different source to other messages.

Distributed Index Handler

New in this Release

The following enhancements were added in DIH version 11.6.0.

- You can now configure your authorization role `SSLIdentities` to identify clients by using an email address in the certificate `subjectAltName`. You can use an optional tag for each SSL identity to specify whether it is a **dns** or **email** type identity. If there is no tag, the server treats it as **dns** type. For example:

    `SSLIdentities=email:user@example.com,dns:admin.example.com,webapp.example.com`

- When using GSS security, you can now configure the service to allow clients to authenticate to any service principal in the service's keytab, rather than requiring a single principal. You use this option by setting the `GSSServiceName` configuration parameter to an asterisk (*).

Resolved Issues

The following issues were resolved in Distributed Index Handler version 11.6.2.

- Javascript could be injected into the `GetRequestLog` response by sending actions to the server.

The following issues were resolved in Distributed Index Handler version 11.6.0

- License related messages in the event log would appear from a different source to other messages.

File System Connector CFS

New in this Release

The following new features were released in File System Connector version 11.6.0.

- If the connector synchronizes some items but the task stops or encounters an error, the next synchronize cycle starts from that point and does not process the same items again. You can configure this behavior with the new configuration parameter `SynchronizeAllowResume`.

- The connector generates events to alert you when an asynchronous action queue becomes full, becomes empty, and when the queue size passes certain thresholds. You can handle these events with any of the existing event handlers.

- The connector can assign a priority to documents retrieved by a fetch task so that when they are ingested they are processed before documents retrieved by other tasks or other connectors. To use this feature set the new configuration parameter `IngestPriority`.

- The connector supports the following Lua functions:

  - `deleteFieldByPath`, which you can call on a `LuaDocument` or `LuaField` object to delete fields or sub-fields that match a specified path.

  - `getFieldsByRegex`, which you can call on a `LuaDocument` or `LuaField` object to get fields or sub-fields where the name or path of the field or sub-field matches a regular expression.

- You can now configure your authorization role `SSLIdentities` to identify clients by using an email address in the certificate `subjectAltName`. You can use an optional tag for each SSL identity to specify whether it is a **dns** or **email** type identity. If there is no tag, the server treats it as **dns** type. For example:

  `SSLIdentities=email:user@example.com,dns:admin.example.com,webapp.example.com`

- When using GSS security, you can now configure the service to allow clients to authenticate to any service principal in the service's keytab, rather than requiring a single principal. You use this option by setting the `GSSServiceName` configuration parameter to an asterisk (*).

Resolved Issues

The following issues were resolved in File System Connector version 11.6.2.

- JavaScript could be injected into the `GetRequestLog` response by sending actions to the server.

The following issues were resolved in File System Connector version 11.6.0.

- License related messages in the event log would appear from a different source to other messages.

- The `LogSysLog` logging configuration option did not output event logs.

Find

New in this Release

The following enhancements were added in Find version 11.6.0.

- Find now uses synonym database restriction options with Query Manipulation Server (QMS). This option enables any synonym database restrictions that you include in your synonym rules. In this case, a Find query matches a synonym rule only if the query database restrictions match the restrictions in the synonym rule.

  You can turn this option off by deselecting the **Apply database match to synonyms** box on the Find configuration settings page. You can add synonym database restrictions to your synonym rules by using IDOL Data Admin version 11.6 or later.

- The dashboard Sunburst and Trending widgets have been improved. When a user clicks on the widget, Find now automatically opens the appropriate tab for the saved query, with the correct parametric fields selected by default.

- You can now specify the maximum number of results to use when you compare two saved searches, by setting the `comparisonStoreStateMaxResults` option in your `config.json` file. This option might improve the performance of comparisons for very large IDOL data sets, where you are

comparing many millions of documents. By default, the maximum number of results is not limited.

- You can now specify a set of databases to exclude from searches by default, by setting the `defaultDeselectedDatabases` option in your `config.json` file.

- You can now add CORS settings for the Video Panel widget in you dashboard configuration, by setting the `crossOrigin` property in your `widgetSettings` object. You might need this option to enable Find to export videos as an image in a PowerPoint report if you store videos on a different server to Find.

- You can now modify the order of values in the filters list, by updating the `filterOrder` array in your Find configuration file. You can also add separators to the filter list, by including a dash as an item in the array.

- When you open a shared search (for example from a dashboard), and you select **Open as Query**, Find now opens the search in the view that you were using.

- You can now configure Find to open a read-only shared search as a new query, by setting the `openSharedDashboardQueryAsNewSearch` option in the `uiCustomization` section of your `config.json`. By default, Find opens the read-only query, and you can use **Open as Query** to change the query.

- The speed of loading Find document previews has been improved by retrieving only the required fields in View and Connector-based viewing modes.

- You can now use Find with an IDOL View Component configured in Universal Viewing mode.

- You can now expand document text in the results list by hovering the mouse over the document. Find shows two lines by default, and expands the text to up to 40 lines when a user hovers over it.

- You can now include the `FindAdmin` role when using pre-authenticated roles in a reverse proxy setup.

- The Find settings page now has an option to set a message of the day, which is visible at the top of the screen when users log in.

- You can now configure Find to read parametric fields from IDOL XML documents that use a non-standard document root, by setting the `idolFieldPathNormalizerXMLPrefixes` in your Find configuration file.

- You can now make a saved search publicly available to all users, by selecting the check box on the Sharing Options screen.

- You can now close dialog boxes by using the keyboard `ESC` key.

- In the Find template configuration, the `equal` helper has been updated to allow you to test equality against multiple candidates. The helper now accepts two or more arguments, and it prints the block if the first argument is referentially equal to any of the subsequent arguments.

- You can now set the `find.reverse-proxy.pre-authenticated-username` system property to a single user name to bypass authentication so that anyone using Find is automatically logged in as that user name. For example you can set `find.reverse-proxy.pre-authenticated-username=anon` and `server.reverseProxy=true` to log all users in as the user **anon**.

  In this case, you do not need to use a reverse proxy with Find, you just need to set the `server.reverseProxy=true` flag. The normal Find HTTP/HTTPS port still works.

- You can now configure entity searches in Find. In this case, when a user selects some text, Find opens an entity search dialog box and searches for the text in an IDOL Content component that you configure for entity search. You can also set up an Answer Server for entity search. For details about

how to configure the entity search components, and how to set up templates to display the entity search results, refer to the *Find Administration Guide*.

- Several new helpers have been added to the template configurations, to allow you to easily format and template numbers, dates, and strings. For more information, refer to the *Find Administration Guide*.

- Shared searches now display the name of the user who created the search, if it was not the current user.

- If a user clicks on a dashboard widget based on a saved search that is shared with them, and the owner has given them edit permissions, Find now shows the editable search directly, rather than a read-only copy.

- You can now select the fields that you want to include in the Find CSV export, by setting the new `csvExport` parameter in the `fieldsInfo` section of the `config.json` file to include or exclude a particular field. For more information, refer to the *Find Administration Guide*.

- The Find access log now uses the same logging mechanism as the other logs. The output file is now called `tomcat-access.log` rather than `access.log`. This change means that the maximum file size is now bounded (to 100MB by default). You can configure the format pattern to use by using the `server.tomcat.access.log.pattern` configuration option. To disable this log, you can set this parameter to a blank value. You can now configure the file name, rollover, maximum file size, and other details by using the `logback-spring.xml` configuration, in the same way as for other log files.

  > **NOTE:**
  > The previous `server.tomcat.accesslog.enabled` option has been replaced. If you previously set `server.tomcat.accesslog.enabled` to `false` to disable the access log, you must set the new `server.tomcat.access.log.pattern` to a blank value.

- The Sunburst visualization has been improved. The outermost layer of the visualization now expands on hover even if there is only a single layer. Also, the visualization now scales with the page height.

- The `hpe.find.home` property has been renamed to `idol.find.home`. The older version of this property is still supported, but it is deprecated. It might be removed in a future version.

- You can now use a mirror mode Distributed Action Handler (DAH) that distributes to a cluster of Community components, as an alternative to a single Community component.

- The map visualization now displays the field name when you hover over a result, rather than in the title of the result.

- You can now change the maximum number of characters in a query summary by setting the `querySummaryMaxCharacters` option in the `config.json` configuration file. The default value is 250.

Resolved Issues

- Export to CSV did not work when QMS was enabled but there were no blacklists defined.

- In Sunburst or table view, the selected parametric filter field was reset when the query text was changed. Find now resets the field only if the new query does not have any results with the selected field.

- The Trending view could show an error message after the search was changed if the IDOL backend contained data but did not have any parametric values.

- The Trending view could show an error after zooming in when the data contains only one point.
- The Trending view could permanently stay in a loading state after the selected field was changed if the new field had the same minimum and maximum date values.
- The Trending view could permanently stay in a loading state after resizing the window, when there was only a single result and the snap to now option was not selected.
- In some circumstances, when using Microsoft Internet Explorer 11, Find could return a 404 error when attempting to load fonts.
- When Find was using a reverse proxy, clicking the sharing options button to attempt to share a search could cause the page to reload.
- When Find was using a context path (for example in a reverse proxy setup), Find did not keep full screen dashboard windows active.
- When Find was using a context path (for example in a reverse proxy setup), Find could fail to retrieve the logo.
- When Find was using a context path (for example in a reverse proxy setup), the small and large logo options did not appear in the customization screen when a user was logged in as an admin.
- Find did not use customized support messages when they were set in the `errorCallSupportString` configuration option.
- Date pickers and ranges did not display the correct results when the dates came from fields configured as `NumericDateType` in IDOL.
- When using the `DRECONTENT` fallback for document viewing, search terms were not highlighted correctly.
- The Sunburst visualizer could return an error if the IDOL response was missing the value `count` attribute. Find now ignores values that do not have a count. An issue has also been resolved in IDOL Content component 11.6 to ensure that it returns this attribute.

HTTP Connector CFS (Solaris only)

New in this Release

The following new features were released in HTTP Connector version 11.6.0.

- The connector generates events to alert you when an asynchronous action queue becomes full, becomes empty, and when the queue size passes certain thresholds. You can handle these events with any of the existing event handlers.
- The connector can assign a priority to documents retrieved by a fetch task so that when they are ingested they are processed before documents retrieved by other tasks or other connectors. To use this feature set the new configuration parameter `IngestPriority`.
- The connector supports the following Lua functions:
  - `deleteFieldByPath`, which you can call on a `LuaDocument` or `LuaField` object to delete fields or sub-fields that match a specified path.
  - `getFieldsByRegex`, which you can call on a `LuaDocument` or `LuaField` object to get fields or sub-fields where the name or path of the field or sub-field matches a regular expression.

- You can now configure your authorization role `SSLIdentities` to identify clients by using an email address in the certificate `subjectAltName`. You can use an optional tag for each SSL identity to specify whether it is a **dns** or **email** type identity. If there is no tag, the server treats it as **dns** type. For example:

  `SSLIdentities=email:user@example.com,dns:admin.example.com,webapp.example.com`

- When using GSS security, you can now configure the service to allow clients to authenticate to any service principal in the service's keytab, rather than requiring a single principal. You use this option by setting the `GSSServiceName` configuration parameter to an asterisk (*).

Resolved Issues

The following issues were resolved in HTTP Connector version 11.6.2.

- JavaScript could be injected into the `GetRequestLog` response by sending actions to the server.

The following issues were resolved in HTTP Connector version 11.6.0.

- License related messages in the event log would appear from a different source to other messages.
- The `LogSysLog` logging configuration option did not output event logs.

IDOL Admin

New in this Release

There were no new enhancements in IDOL Admin version 11.6.0.

Resolved Issues

- In IE11, the loading of Font Awesome fonts could fail, resulting in errors in the error log.

IDOL Proxy Component

New in this Release

The following enhancements were added in IDOL Proxy version 11.6.0.

- The `ResponseFormat` general ACI action parameter has a new option, **simplejson**. This format is similar to the `json` format, but it does not use $ nodes to represent XML nodes unless the equivalent XML node contains attributes. This response format also does not use `autn:` prefixes in node names.
- You can now configure your authorization role `SSLIdentities` to identify clients by using an email address in the certificate `subjectAltName`. You can use an optional tag for each SSL identity to

specify whether it is a **dns** or **email** type identity. If there is no tag, the server treats it as **dns** type. For example:

```
SSLIdentities=email:user@example.com,dns:admin.example.com,webapp.example.com
```

Resolved Issues

The following issues were resolved in IDOL Proxy Component version 11.6.2.

- Javascript could be injected into the `GetRequestLog` response by sending actions to the server.

The following issues were resolved in IDOL Proxy Component version 11.6.0

- License related messages in the event log would appear from a different source to other messages.

IDOL Site Admin

New in this Release

The following enhancements were added in IDOL Site Admin version 11.6.0.

- IDOL Site Admin now limits the number of calls that it sends to Coordinator to avoid building up large queues if a component is responding slowly for any reason.
- The `hp.idolsiteadmin.home` and `hp.idolsiteadmin.oemEncryptionKey` properties have been renamed to `idol.idolsiteadmin.home` and `idol.idolsiteadmin.oemEncryptionKey` respectively. The older versions of these properties are still supported, but they are deprecated. They might be removed in a future version.

Resolved Issues

- If a `GetStatusOverview` request from IDOL Site Admin to the Coordinator component timed out, IDOL Site Admin could stop updating the System Notifications list without giving any warning in the user interface of the underlying error.
- Error emails were not sent if a user was not logged in. IDOL Site Admin now checks for errors and emails notifications every five minutes.

IDOL Speech Server

New in this Release

The following enhancements were added in Speech Server version 11.6.0.

- Text normalization support has been added for Gulf Arabic (`ARGU`), Modern Standard Arabic (`ARMSA`), US Spanish (`ESUS`), Farsi (`FAIR`), and Russian (`RURU`).

- The iVector base pack has been updated to improve speaker identification accuracy.

- In speaker identification, each speaker can now have multiple iVector-based templates.

- The default value for the `balanceBias` parameter in the `ivdevel` module has been changed to 0.3.

- Date and time options have been improved for Speech Server scheduling:

  - You can now configure schedules to run on a particular date in the month, or day of the week, both in the task schedule file and in the `AddSchedule` action. The `ListSchedules` action also now returns this information.

  - In the task schedules, you can now specify special placeholder values by using the format `{PLACEHOLDER}`, rather than `${PLACEHOLDER}`. The older format is still accepted.

  - You can now place a limit on the `{ITERATION}` placeholder, to cycle through a set of output files. For example, if you set `test-{ITERATION_5}.ctm` as your output file name in a schedule, Speech Server creates five output files with the names `test-0.ctm`, `test-1.ctm`, through to `test-4.ctm`, and then resets the value to 0 on the next iteration.

- You can now save schedules that you add as actions to a schedule configuration file by using the `SaveSchedules` action. You can also load a schedule from a schedule configuration file, or from a previously saved schedule configuration, by using the `LoadSchedules` action.

- You can now enable dial tone identification when performing audio category classification. The **audiopreproc** module has a new parameter `DoToneClass`, which you can set to true, false, or auto, to always do tone classification, never do tone classification, or to do tone classification for 8kHz (telephony) audio only. This parameter is also available as an action parameter for the `AudioAnalysis` and `SpeechSilClassification` tasks.

- The logic for audio category classification has been improved, leading to more reliable results.

- You can now configure IDOL Speech Server to upsample audio when required. In general, Micro Focus does not recommend upsampling, because it can reduce audio quality. However, you can use the new `AudioUpsampling` parameter to enable upsampling in cases where the audio sample rate is lower than required by a task. In this case, IDOL Speech Server upsamples the audio and logs a warning.

- You can now configure your authorization role `SSLIdentities` to identify clients by using an email address in the certificate `subjectAltName`. You can use an optional tag for each SSL identity to specify whether it is a **dns** or **email** type identity. If there is no tag, the server treats it as **dns** type. For example:

  `SSLIdentities=email:user@example.com,dns:admin.example.com,webapp.example.com`

- When using GSS security, you can now configure the service to allow clients to authenticate to any service principal in the service's keytab, rather than requiring a single principal. You use this option by setting the `GSSServiceName` configuration parameter to an asterisk (*).

Resolved Issues

The following issues were resolved in IDOL Speech Server version 11.6.2.

- Javascript could be injected into the `GetRequestLog` response by sending actions to the server.

The following issues were resolved in IDOL Speech Server version 11.6.0

- Text normalization of Hindi text could result in an interruption of service.

- License related messages in the event log would appear from a different source to other messages.
- The `LogSysLog` logging configuration option did not output event logs.

Knowledge Graph Component

New in this Release

The following enhancements were added in Knowledge Graph version 11.6.0.

- You can now configure your authorization role `SSLIdentities` to identify clients by using an email address in the certificate `subjectAltName`. You can use an optional tag for each SSL identity to specify whether it is a **dns** or **email** type identity. If there is no tag, the server treats it as **dns** type. For example:

  `SSLIdentities=email:user@example.com,dns:admin.example.com,webapp.example.com`

- When using GSS security, you can now configure the service to allow clients to authenticate to any service principal in the service's keytab, rather than requiring a single principal. You use this option by setting the `GSSServiceName` configuration parameter to an asterisk (*).

Resolved Issues

The following issues were resolved in Knowledge Graph version 11.6.2.

- Javascript could be injected into the `GetRequestLog` response by sending actions to the server.

The following issues were resolved in Knowledge Graph version 11.6.0

- License related messages in the event log would appear from a different source to other messages.
- The `LogSysLog` logging configuration option did not output event logs.

License Server

New in this Release

The following enhancements were added in License Server version 11.6.0.

- You can now configure your authorization role `SSLIdentities` to identify clients by using an email address in the certificate `subjectAltName`. You can use an optional tag for each SSL identity to specify whether it is a **dns** or **email** type identity. If there is no tag, the server treats it as **dns** type. For example:

  `SSLIdentities=email:user@example.com,dns:admin.example.com,webapp.example.com`

- When using GSS security, you can now configure the service to allow clients to authenticate to any service principal in the service's keytab, rather than requiring a single principal. You use this option by setting the `GSSServiceName` configuration parameter to an asterisk (*).

Resolved Issues

The following issues were resolved in License Server version 11.6.2.

- Javascript could be injected into the `GetRequestLog` response by sending actions to the server.

The following issues were resolved in License Server version 11.6.0

- License related messages in the event log would appear from a different source to other messages.

Media Server (Windows and Linux only)

New in this Release

The following enhancements were added in Media Server version 11.6.0.

Media Server Core

- NVIDIA Pascal series cards (with CUDA compute capability 6.0 and 6.1) are now supported by GPU Media Server.

- The server generates events to alert you when an asynchronous action queue becomes full, becomes empty, and when the queue size passes certain thresholds. You can handle these events with any of the existing event handlers.

- You can now configure your authorization role `SSLIdentities` to identify clients by using an email address in the certificate `subjectAltName`. You can use an optional tag for each SSL identity to specify whether it is a **dns** or **email** type identity. If there is no tag, the server treats it as **dns** type. For example:

  `SSLIdentities=email:user@example.com,dns:admin.example.com,webapp.example.com`

- When using GSS security, you can now configure the service to allow clients to authenticate to any service principal in the service's keytab, rather than requiring a single principal. You use this option by setting the `GSSServiceName` configuration parameter to an asterisk (*).

Ingest

- Media Server can ingest JPEG 2000 image files.
- Media Server can ingest WebP image files.

Analysis

- Media Server provides a way to obtain partial analysis results before an event finishes. Analysis engines can produce new output tracks, `SegmentedResult` and `SegmentedResultWithSource`. These are similar to the existing `Result` and `ResultWithSource` tracks, except that the maximum duration of a record is limited to the value of the new parameter `SegmentDuration`. When a record reaches the maximum duration, Media Server outputs the record and begins a new one with the same ID. This means that for every record in the `Result` track that exceeds the maximum duration, there will be two or more records in the `SegmentedResult` track.

Segmented results are useful when you need to obtain information about an event before it finishes. For example, if a stolen vehicle remains in view of a camera for several minutes, you do not want to wait until the vehicle has left the scene before raising an alert. You could use the `Data` track to obtain output as soon as each video frame has been analyzed, but the `SegmentedResult` track provides a balance between accuracy and latency, because Media Server can track events and analyze multiple frames before providing a result.

Segmented results are supported by the following analysis operations:

- Barcode recognition
- Face detection
- Face recognition
- Face demographics
- Face state (expression)
- Number plate recognition
- Object recognition
- Vehicle make and model recognition

- With some analysis engines, records in the `Data` track become more accurate as an event progresses, because Media Server takes into account the results obtained from analyzing previous frames. The record timestamps still relate to a single video frame. This change applies to face detection, object recognition, number plate recognition, and vehicle make/model recognition. As before, `Result` records provide optimum accuracy because Media Server can combine the data obtained from analyzing individual frames, from the beginning of the event to the end.

- A new pre-trained object detector (`ObjectDetector_CommonObjects.dat`) is available for download. This detects common objects and includes the following classes: person, bird, cat, cow, dog, horse, sheep, aeroplane, bicycle, boat, bus, car, motorbike, train, bottle, chair, dining table, potted plant, sofa, tv/monitor.

- Media Server includes a new analysis engine (`Type=AudioCategorize`) for segmenting and classifying audio into categories such as "speech", "music", "noise", and "silence". You can use audio categorization to inspect an audio file and decide whether to perform further processing. For example, when audio categorization reports that a file contains mostly speech, you might decide to run language identification and speech-to-text.

- Speech-to-text is easier to configure, because you can now set a single parameter, `SpeedBias`, to balance accuracy and speed.

- Face recognition, demographics, and expression analysis are more accurate, because they analyze multiple video frames to produce a single result. Providing you have sufficient computational resources, you can benefit from this improvement by setting the input for your face recognition, demographics, or expression task to the `DataWithSource` track that is generated by face detection. The `Result` track generated by these engines is more consistent with other analysis engines because it now contains a single record for each person, rather than a record for each frame received from face detection. The engines now generate `Data` and `DataWithSource` tracks to provide the results for individual frames.

- Object detection is more accurate because it analyzes multiple video frames to produce a single result. The `Data` and `DataWithSource` tracks have been added to provide the results for individual frames and the `Result` track now contains a single record for each detected object. This change also improves the speed of object detection when a small sample interval is used. No configuration changes are required to benefit from these improvements.

- Image hashes can be stored in the Media Server database, so that you can use image hash analysis to detect duplicate images without needing to query an IDOL Content component.

- Number plate recognition generates records that are more consistent with other analysis engines. Records are generated only when a number plate is read successfully, and records that relate to the same vehicle all have the same UUID.

- The number plate formats for the United Arab Emirates - Umm al-Quwain (AE-UQ), and United Arab Emirates - Dubai (AE-DU) have been updated so that Media Server recognizes additional plate formats.

- Number plate recognition produces fewer false positives when using `Location=NZ-PP` or `Location=NOF`.

- Number plate recognition produces fewer false positives when processing video files or streams with duplicate frames.

- Scene analysis has new alarm filters. You can prevent an alarm occurring if an object crosses a tripwire in the wrong direction, accelerates or decelerates between tripwires, or spends too much or too little time between tripwires. You can allow or reject alarms based on the proportion of the region of interest that is considered active. You can prevent an alarm occurring when an object has been continually present in a region of interest for longer than a specified time duration.

User Interfaces

- The graphical user interface, available through `action=gui`, has been improved. You can now move identities between databases, and move images between identities.

- The scene analysis training utility reads user preferences for some options from a configuration file, `TUPreferences.cfg`.

- When optimizing a category in the scene analysis training utility, you can enable or disable characteristics such as size and orientation. The training utility shows the effect on the number of false and missed alarms. This feature can help you decide whether a different combination of characteristics is more effective in filtering alarms.

- The scene analysis training utility saves additional information with each classified alarm, so that an object's time in a region of interest can be calculated more accurately if the region of interest is moved before the category is optimized.

- The scene analysis training utility always displays the position of tripwires for the current category.

Resolved Issues

The following issues were resolved in Media Server version 11.6.2.

- Javascript could be injected into the `GetRequestLog` response by sending actions to the server.

The following issues were resolved in Media Server version 11.6.0

- The file `libopenblas_AMD_Bulldozer.dll` was not released with Media Server 11.5.0 but is now available. To run tasks that use convolutional neural networks on a machine that has a processor from the AMD Bulldozer series, download the latest version of `libopenblas_AMD_Bulldozer.dll`, and rename it such that it replaces the file `libopenblas.dll` that is included in the Media Server installation.

- KeyView could terminate Media Server unexpectedly.

- Media Server could incorrectly replace special characters in the destination URL for an HTTP POST output task.

- The MPEG encoder did not segment encoded video files when the `ImageInput` parameter specified a track other than the default.

- After being restarted, Media Server did not resume `process` actions that were started with `persist=true`.

- The value of the configuration parameter `[Modules]Enable` was incorrectly expected to be lower-case.

- Number plate recognition could incorrectly reject some number plates for not matching a valid format, but only in locations where some number plate formats include sub-reads, logos, or color patches.

- With the image encoder, the values produced by the macro `%segment.sequence%` incorrectly started at 0, instead of 1.

- The `LogSysLog` logging configuration option did not output event logs.

- License related messages in the event log would appear from a different source to other messages.

- Scene analysis did not output records for an event when the source media was a file and the event occurred immediately before the end of the file.

- Scene analysis could identify too many objects in a scene, after using the default background method for some time.

- The scene analysis training utility could terminate unexpectedly after a category was added or removed from a configuration, or when alarms were reviewed.

- The scene analysis training utility would optimize alarm filter thresholds when insufficient alarms had been classified as true alarms.

- The scene analysis training utility did not save changes to alarm classifications when existing classifications were modified.

- The scene analysis training utility could set the minimum and maximum object size incorrectly.

- In the scene analysis training utility, object tracking could appear to turn on and off when live video was viewed.

- In the scene analysis training utility, reloading the open configuration failed to discard unsaved changes.

- The scene analysis training utility failed to send some settings (background type, background update, and active area threshold or deviation threshold) to Media Server when sending a training configuration.

- Alarms generated manually, through the scene analysis training utility, could have incorrect values for some alarm filter values.

Query Manipulation Server Component

New in this Release

The following enhancements were added in QMS version 11.6.0.

- You can now use a Lua script to modify a query request after QMS has processed any rules and expanded the query accordingly. You configure the new Lua script by setting the `Script` parameter in the `[ExpandedRequestCooker]` configuration section to the path to the script.

  The Lua script must define a function called `cook_expanded_request` that accepts three arguments. The first argument is the original request that QMS received (string). The second argument is the request following QMS manipulations (string). The final argument is the references of rules that were triggered by the original request (table of strings).

  The function must return a table that contains the parameters of the final request to run (that is, the same return type as the pre-manipulation cooker function).

- QMS supports the following new Lua functions and methods:

  ○ `deleteFieldByPath` function, which you can call on a `LuaDocument` or `LuaField` object to delete fields or sub-fields that match a specified path.

  ○ `getFieldsByRegex`, which you can call on a `LuaDocument` or `LuaField` object to get fields or sub-fields where the name or path of the field or sub-field matches a regular expression.

- You can now configure your authorization role `SSLIdentities` to identify clients by using an email address in the certificate `subjectAltName`. You can use an optional tag for each SSL identity to specify whether it is a **dns** or **email** type identity. If there is no tag, the server treats it as **dns** type. For example:

  `SSLIdentities=email:user@example.com,dns:admin.example.com,webapp.example.com`

- When using GSS security, you can now configure the service to allow clients to authenticate to any service principal in the service's keytab, rather than requiring a single principal. You use this option by setting the `GSSServiceName` configuration parameter to an asterisk (*).

Resolved Issues

The following issues were resolved in Query Manipulation Server version 11.6.2.

- Javascript could be injected into the `GetRequestLog` response by sending actions to the server.

The following issues were resolved in Query Manipulation Server version 11.6.0

- License related messages in the event log would appear from a different source to other messages.

Statistics Server Component

New in this Release

The following enhancements were added in Statistics Server version 11.6.0.

- You can now configure your authorization role `SSLIdentities` to identify clients by using an email address in the certificate `subjectAltName`. You can use an optional tag for each SSL identity to specify whether it is a **dns** or **email** type identity. If there is no tag, the server treats it as **dns** type. For example:

  `SSLIdentities=email:user@example.com,dns:admin.example.com,webapp.example.com`

- When using GSS security, you can now configure the service to allow clients to authenticate to any service principal in the service's keytab, rather than requiring a single principal. You use this option by setting the `GSSServiceName` configuration parameter to an asterisk (*).

Resolved Issues

The following issues were resolved in Statistics Server version 11.6.2.

- Javascript could be injected into the `GetRequestLog` response by sending actions to the server.

The following issues were resolved in Statistics Server version 11.6.0

- License related messages in the event log would appear from a different source to other messages.

View Server Component

New in this Release

The following enhancements were added in View Server version 11.6.0.

- You can now highlight proximity expressions in the `View` action, by setting the new `Highlight` parameter to **Proximity**. By default, View highlights the terms that you specify in the `Links` parameter. The new **Proximity** highlighting option highlights the whole span that contains the terms in a particular expression.

- You can now configure your authorization role `SSLIdentities` to identify clients by using an email address in the certificate `subjectAltName`. You can use an optional tag for each SSL identity to specify whether it is a **dns** or **email** type identity. If there is no tag, the server treats it as **dns** type. For example:

  `SSLIdentities=email:user@example.com,dns:admin.example.com,webapp.example.com`

- When using GSS security, you can now configure the service to allow clients to authenticate to any service principal in the service's keytab, rather than requiring a single principal. You use this option by setting the `GSSServiceName` configuration parameter to an asterisk (*).

Resolved Issues

The following issues were resolved in IDOL View Component version 11.6.2.

- Javascript could be injected into the `GetRequestLog` response by sending actions to the server.

The following issues were resolved in IDOL View Component version 11.6.0

- License related messages in the event log would appear from a different source to other messages.

Web Connector (Windows and Linux only)

New in this Release

The following new features were released in Web Connector version 11.6.0.

- The `synchronize` action supports a new optional parameter, `identifiers`. The `identifiers` parameter accepts a comma-separated list of document identifiers that specifies the documents to synchronize.

- The `identifiers` fetch action can report information from the datastore, instead of querying the repository. Viewing information from the datastore is useful if you want to know which items the connector has seen instead of browsing the items that exist in the repository. To view information from the datastore, set the configuration parameter `IdentifiersFromDatastore=TRUE`.

- The connector includes an XSL template to convert the results from the `identifiers` fetch action into a tree view. The template is named `FetchIdentifiersTreeview.tmpl`. Micro Focus does not support the template, it is provided only as an example of a template that you could build.

- The connector can process pages in priority order, so that pages which have changed more frequently or more recently are synchronized first. This can help keep the IDOL index up-to-date, particularly with long synchronize cycles, because items that are more likely to have changed are processed first. To synchronize pages in priority order (as much as possible), set the new configuration parameter `EnablePrioritizedSync`.

- The connector responds to `stop` (`action=QueueInfo&QueueAction=stop`) and `stopfetch` (`action=StopFetch`) requests more promptly.

- The size of the data store (that holds information related to a fetch task) has been reduced in some cases.

- The connector generates events to alert you when an asynchronous action queue becomes full, becomes empty, and when the queue size passes certain thresholds. You can handle these events with any of the existing event handlers.

- The connector can assign a priority to documents retrieved by a fetch task so that when they are ingested they are processed before documents retrieved by other tasks or other connectors. To use this feature set the new configuration parameter `IngestPriority`.

- The connector supports the following Lua functions:
  - `deleteFieldByPath`, which you can call on a `LuaDocument` or `LuaField` object to delete fields or sub-fields that match a specified path.
  - `getFieldsByRegex`, which you can call on a `LuaDocument` or `LuaField` object to get fields or sub-fields where the name or path of the field or sub-field matches a regular expression.

- You can now configure your authorization role `SSLIdentities` to identify clients by using an email address in the certificate `subjectAltName`. You can use an optional tag for each SSL identity to specify whether it is a **dns** or **email** type identity. If there is no tag, the server treats it as **dns** type. For example:

  `SSLIdentities=email:user@example.com,dns:admin.example.com,webapp.example.com`

- When using GSS security, you can now configure the service to allow clients to authenticate to any service principal in the service's keytab, rather than requiring a single principal. You use this option by setting the `GSSServiceName` configuration parameter to an asterisk (*).

Resolved Issues

The following issues were resolved in Web Connector version 11.6.2.

- JavaScript could be injected into the `GetRequestLog` response by sending actions to the server.

The following issues were resolved in Web Connector version 11.6.0.

- When a page changed depth relative to the start URL, the `DEPTH` metadata field was not updated until the next time the page content changed.

- When handling `<meta http-equiv="refresh"...>` instructions contained with the `<head>` section of a page, the connector only followed the redirection when the characters "url" were lower case.

- License related messages in the event log would appear from a different source to other messages.

- The `LogSysLog` logging configuration option did not output event logs.

Upgrade Information

This section describes how to upgrade IDOL Server and its components.

Upgrade to IDOL 11.x

The simplest way to upgrade is to index data into a fresh installation of IDOL 11.0, whilst also activating any further functionality that is appropriate for your use case. However, IDOL 11.0 is also fully compatible with existing installations and indexes, so you do not need to reindex, as long as you include certain configuration settings before you run the IDOL 11.0 executable.

You must add the following configuration setting for the Content component, unless a different value is already present. If you create a new IDOL index, you can ignore this step.

```
[Server]
ParametricMaxPairsPerDocument=104858
```

If you want to upgrade to IDOL 11.x from IDOL 7.x, there are some additional configuration updates. For more information, refer to the *IDOL 11 Upgrade Technical Note*.

Upgrade Document Tracking

In IDOL 10.9, the database schema for Document Tracking was updated. For information about upgrading your document tracking database backend from IDOL 10.8 or earlier to IDOL 10.9 or later, refer to the *Document Tracking 10.9 Upgrade Technical Note*.

The database schema for Document Tracking was updated for IDOL 10.3. For information about upgrading your document tracking database backend from IDOL 10.2 or earlier, refer to the *Document Tracking 10.3 Upgrade Technical Note*.

Requirements

This section describes the system requirements, supported platforms, and software dependencies for IDOL Server 11.6.2.

Minimum System Requirements

The following are minimum system requirements for IDOL Server 11.6.2 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 11.6.2, or its components, on UNIX platforms, the server must have the following minimum versions of libraries:

- GLIBC_2.3.2
- GLIBCXX_3.4.20
- 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 11.6.2 on the Microsoft Windows operating system, you might need to update the Microsoft Visual C++ Redistributable packages. The IDOL Server installer includes the required redistributable files for Microsoft Visual C++ 2005, 2010, 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
Java	Windows, Solaris, Linux: JRE 8 or later
Browsers	- Internet Explorer 11 - Mozilla Firefox (latest version) - Chrome (latest version)

Supported Operating System Platforms

The following operating system platforms are available for IDOL Server 11.6.2.

- Windows x86 64
- Linux x86 64
- Solaris x86 64
- Solaris SPARC 64

The documented platforms are the recommended and most fully tested platforms for IDOL Server. The following sections provide more information about the most fully tested versions of these platforms.

Windows

- Windows Server 2012 x86 64
- Windows 7 SP1 x86 64
- Windows Server 2008 R2 x86 64
- Windows Server 2008 SP2 x86 64

Linux

For Linux, the following lists the minimum recommended versions of particular distributions:

- Red Hat Enterprise Linux (RHEL) 6
- CentOS 6
- SuSE Linux Enterprise Server (SLES) 10
- Ubuntu 14.04
- Debian 7

Solaris

- Solaris 10
- Solaris 11

Notes

- 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.

Connector Framework Server

- With CFS 11.6.0, XML schemas and transforms are parsed when CFS starts. If a schema or transform is invalid, CFS does not start but logs the message `Error constructing Connector Framework Server: Failed to construct Xml Transform Configuration in section '<SectionName>'` ...

Media Server

GPU Requirements

- To use a GPU to accelerate Media Server processing tasks, you must place the GPU in TCC mode. (Windows only. This does not apply to Linux because TCC mode is used by default for headless Linux systems).
- GeForce GTX graphics cards are supported only with headless Linux operating systems.

Licensing Changes

- The licensing model for face recognition with visual channels has changed. Face detection and face recognition require a single visual channel to recognize up to 250,000 faces, but each additional 250,000 faces requires an additional visual channel. For example, to run face detection and face recognition with a database of 700,000 faces now requires three visual channels. You can no longer set the configuration parameter `MaxFaces` to `Unlimited`, and must now specify a number.

Deprecated Features

Category	Deprecated Feature	Deprecated Since
Speech-to-text	The `Mode`, `ModeValue`, and `UseFrameDuplication` configuration parameters. You can replace all of these parameters with the new parameter `SpeedBias`.	11.6.0
Number plate recognition	The `RepeatDelay` configuration parameter. Number plate recognition now produces a single result record for each appearance of a vehicle. The `resultstatus`, `integrationstatus`, and `finaldata` fields in number plate records. Number	11.6.0

	plate recognition now generates records only when a number plate is read successfully. Records that relate to the same vehicle all have the same UUID.	
Server / Service	The `AdminClients`, `QueryClients`, `ServiceControlClients`, and `ServiceStatusClients` configuration parameters. Micro Focus recommends that you use authorization roles instead.	11.5.0
Number plate recognition	The `BlackAndWhiteCamera` configuration parameter. Media Server 11.5.0 automatically detects whether the source video is black-and-white, so you no longer need to set this parameter.	11.5.0
Speech analysis	The `ErrorMessage` configuration parameter, for the audio matching, language identification, speaker identification, and speech-to-text analysis tasks. You can use the parameter `MaxConsecutiveTries` to fail the session when the Speech Server is unavailable.	11.5.0
Image classification	The `Bayesian` and `Maxvote` classifier types. Micro Focus recommends that you use Convolutional Neural Network (`CNN`) classifiers instead.	11.4.0
Ingest - LibAV	The `IngestTime` configuration parameter. Micro Focus recommends that you use the new configuration parameter `IngestDateTime` instead. The new parameter accepts values in a greater number of formats.	11.4.0
Number plate recognition	The `ANPRFormatsDirectory` and `ANPRWeightsDirectory` configuration parameters. You can set the path for all static data folders by setting the configuration parameter `[Paths] StaticDataDirectory`.	11.4.0
Number plate recognition	The `OutputAllIntResults` and `PlateSizeUnit` configuration parameters. Micro Focus recommends using the new parameters `OutputAlternativeResults` and `CharHeightUnit`, respectively.	11.4.0
OCR	The `ImageBinarizeMethod` configuration parameter.	11.4.0
Speaker identification	`GMM` models. Micro Focus recommends that you use Speaker Identification with `iVector` models instead.	11.4.0
Language identification	The configuration parameter `CumulativeMode`. Micro Focus recommends that you use the parameter `Mode` instead.	11.4.0

Rolling buffer	The action parameter `name`, available on the actions `AddStream`, `EditStream`, `GetStreamInfo`, `PreAllocateStorage`, and `RemoveStream`. Micro Focus recommends that you use the new parameter `stream`, instead.	11.4.0
Rolling buffer	The action parameters `OldName` and `NewName`, on the action `RenameStream`. Micro Focus recommends that you use the new parameters `Stream` and `NewStream` instead.	11.4.0
Face detection	The `DetectEyes` configuration parameter.	11.3.0

Removed features

The following features have been removed:

- The `Integration` and `MaxRead` parameters, from number plate recognition. Integration is still performed but no longer needs to be configured. If you want to obtain a result before a vehicle leaves the scene you can use the new `SegmentedResult` output track.

IDOL Speech Server

- Installation on Linux requires the following software:
  - GLIBC_2.3.2
  - GLIBCXX_3.4.20
  - GCC_4.8.0
- If you install IDOL Speech Server 11.6.2 using the IDOL 11.6.2 installer program, you must ensure that you have a Speech Server license key in addition to the standard IDOL Server license key. The IDOL Server license key does not contain licensing information for Speech Server, and Speech Server cannot run using it.
- The Solaris operating system does not support the audio fingerprinting feature in Speech Server.
- On Linux platforms, you must include the configured `FFmpegDirectory` in the `LD_LIBRARY_PATH` environment variable. The default start script sets this environment variable when you start the server. However, if you change the directory or if you do not use the standard script, you must update the environment variable manually.

Documentation

The following documentation was updated for this release.

- *IDOL Expert*
- *IDOL Getting Started Guide*
- *IDOL Server Reference* (online help)
- *IDOL Server Administration Guide*
- *IDOL Document Security Administration Guide*

  In earlier versions of IDOL this document was named the *Intellectual Asset Protection System (IAS) 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 (CFS) Reference* (online help)
- *File System Connector (CFS) Administration Guide*
- *HTTP Connector (CFS) Reference* (online help)
- *HTTP Connector (CFS) Administration Guide*
- *Web Connector Reference* (online help)
- *Web Connector Administration Guide*
- *QMS Reference* (online help)
- *QMS Administration Guide*
- *Media Server Reference* (online help)
- *Media Server Administration Guide*
- *IDOL Speech Server Reference* (online help)
- *IDOL Speech Server Administration Guide*
- *Controller Reference*
- *Coordinator Reference*
- *Knowledge Graph Reference* (online help)
- *Knowledge Graph Technical Note*