



**Hewlett Packard**  
Enterprise

# HPE IDOL Server

Software Version: 11.4.0

## Release Notes

Document Release Date: June 2017

Software Release Date: June 2017

## Legal notices

### Warranty

The only warranties for Hewlett Packard Enterprise Development LP 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. HPE 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. Valid license from HPE 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 2017 Hewlett Packard Enterprise Development LP

### 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.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

## 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 recent software updates, go to <https://downloads.autonomy.com/productDownloads.jsp>.

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

This site requires that you register for an HPE Passport and sign in. To register for an HPE Passport ID, go to <https://hpp12.passport.hpe.com/hppcf/login.do>.

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

## Support

Visit the HPE Software Support Online web site at <https://softwaresupport.hpe.com>.

This web site provides contact information and details about the products, services, and support that HPE Software offers.

HPE Software 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 web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Access product documentation
- Manage support contracts
- Look up HPE 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 that you register as an HPE Passport user and sign in. Many also require a support contract.

To register for an HPE Passport ID, go to <https://hpp12.passport.hpe.com/hppcf/login.do>.

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

To check for recent software updates, go to <https://downloads.autonomy.com/productDownloads.jsp>.

# Contents

New in this Release .....	7
Content Component .....	7
New in this Release .....	7
Resolved Issues .....	9
Category Component .....	10
New in this Release .....	10
Resolved Issues .....	10
Community Component .....	11
New in this Release .....	11
Resolved Issues .....	11
Connector Framework Server .....	12
New in this Release .....	12
Resolved Issues .....	13
Controller .....	13
New in this Release .....	13
Resolved Issues .....	14
Coordinator .....	15
New in this Release .....	15
Resolved Issues .....	16
Distributed Action Handler .....	16
New in this Release .....	16
Resolved Issues .....	17
Distributed Index Handler .....	17
New in this Release .....	17
Resolved Issues .....	19
File System Connector CFS .....	19
New in this Release .....	19
Resolved Issues .....	20
Find .....	20
New in this Release .....	20
Resolved Issues .....	22
HTTP Connector CFS (Solaris only) .....	24
New in this Release .....	24
Resolved Issues .....	25
IDOL Admin .....	25
IDOL Proxy Component .....	25
New in this Release .....	25

Resolved Issues .....	25
IDOL Site Admin .....	26
New in this Release .....	26
Resolved Issues .....	26
IDOL Speech Server .....	26
New in this Release .....	26
Resolved Issues .....	28
Knowledge Graph Component .....	28
New in this Release .....	28
Resolved Issues .....	29
License Server .....	29
New in this Release .....	29
Resolved Issues .....	30
Media Server (Windows and Linux only) .....	30
New in this Release .....	30
Resolved Issues .....	33
Query Manipulation Server Component .....	33
New in this Release .....	33
Resolved Issues .....	34
Statistics Server Component .....	35
New in this Release .....	35
Resolved Issues .....	35
View Server Component .....	35
New in this Release .....	35
Resolved Issues .....	37
Web Connector (Windows and Linux only) .....	37
New in this Release .....	37
Resolved Issues .....	38
Upgrade Information .....	39
Upgrade to IDOL 11.x .....	39
Upgrade Document Tracking .....	39
Requirements .....	40
Minimum System Requirements .....	40
Software Dependencies .....	40
Supported Operating System Platforms .....	41
Notes .....	42

Documentation .....48

# New in this Release

The following sections describe the enhancements for the components of HPE IDOL Server version 11.4.0.

## Content Component

### New in this Release

- You can now enable Content to search for documents that have not yet been flushed to disk, by setting the `SearchUncommittedDocuments` parameter to `True` in the `[Server]` section. In this case, documents are available to query from the time that an index job reaches the `Pending Commit` state.
- The `Query` action `Text` parameter now accepts the `SYNONYM` operator, which allows you to specify a list of terms to consider as synonyms. The query returns results as though these terms have `OR` operators between them, but relevance scores are calculated for all the synonym terms as if they were a single term. For example:

```
Text=SYNONYM(cat moggy kitten) NEAR sale
```

- You can now control the weight contribution that a single term in a particular field has toward the result score in a query, by using the new `MaxTermContribution` field property. This option allows you more fine control on the weighting of terms in your queries, if required.
- You can now configure Content to use GSSAPI authorization on the index port. To enable it, you must set the `GSSServiceName` parameter in the `[Server]` section to the fully qualified GSSAPI service name that the Content component must use to identify itself. You must also set `RequireGSSAuth` to `True` in the `[IndexServer]` section to enable authorization.

**NOTE:**

This method provides an authentication requirement only. HPE recommends that you use it in conjunction with TLS/SSL to encrypt the authentication data.

- The `GSSServiceName` parameter has been added to the `DREEXPORTREMOTE` index action to allow you to export documents to a server that uses GSSAPI authentication.
- The Content component now supports refreshing of `SecurityInfo` tokens. When you configure the new `SecurityTokenIdleTime` parameter in Community 11.4, Content returns refresh tokens in a `responsedata/autn:securityinfo` element in the response for actions that accept the `SecurityInfo` parameter.
- The `MinDate` and `MaxDate` query parameters now accept the following ISO-8601 date specifiers.
  - `YYYY-MM-DD`
  - `YYYY-MM-DDTHH:NN:SSZ`
  - `YYYY-MM-DDTHH:NN:SS±HHMM`

In particular, this change allows you to specify time zone information. These new formats are also available for the `BIASDATE` and `RANGE` `FieldText` operators, the `FIXEDDATE` option in the `Ranges` parameter for `GetQueryTagValues`, the `BackupForRestoreTime` action parameter, and the `ArchiveCleanupCutOffTime` and `RestoreTime` index action parameters.

- The `DateFormatCSVs` parameter `ZZZZ` option now matches a single `Z` character as UTC, and matches time zone values between `-1300` and `+1500`.
- The `GetQueryTagValues` action now provides additional information about the range of numeric data when you set `ValueDetails` to `True`. The response now includes the `<autn:valuepercentile>` tag, with values for various percentile values. By default, it returns the 10th, 25th, 50th (median), 75th, and 90th percentiles. You can optionally use the new `ValuePercentiles` parameter to specify additional options.

**NOTE:**

If you send the `GetQueryTagValues` action to a DAH, the `ValueDetails` response always includes only the default value percentiles. However, the DAH requests additional percentiles from the child servers so that it can calculate the appropriate ranges for the whole dataset.

- The `Ranges` parameter for the `GetQueryTagValues` action now accepts a `FIXEDDATE` operator, which allows you to set ranges of dates for date fields. You can specify dates in the same formats as the `MinDate` and `MaxDate` parameters. For example:

```
FIXEDDATE{.,13/03/2017,12:00:00 13/03/2017,10/03/2017,.}:autn_date
```

- You can now use multiple field names in the `FIXED` and `FIXEDDATE` operators in the `Ranges` parameter for the `GetQueryTagValues` action. Separate multiple field names after the operator with colons to apply the set of ranges to multiple fields. For example:

```
FIXEDDATE{.,13/03/2017,12:00:00 13/03/2017,10/03/2017,.}:autn_date:NUMDATE2
```

- The `GetQueryTagValues` action `ValueDetails` response now includes date attributes for values from `DateType` or `NumericDateType` fields, which contain formatted date values. When you also set `DateOffset`, the response also includes `date_with_offset` attributes.
- You can now filter the values that the `GetQueryTagValues` action returns by a string value (which can include wildcard characters), by using the new `ValueRestriction` parameter. When you set this parameter, the action returns only values for the field that match one of the specified restrictions.
- The `GetQueryTagValues` response now includes an `end_date` attribute for any date range values returned (for example, when you use the `FIXEDDATE` option in `Ranges`).

**NOTE:**

If you use Content through a DAH or QMS component, you must also upgrade those components to 11.4.0 to return the new response tag.

- The `CostEstimate` parameter has been added to the `DocumentStats` action. This parameter returns an estimate of the cost of running a query with the specified `Text`, including the minimum and maximum documents that Content might be read, and an estimate of the amount of data that might be read.
- The generic mapped security module supports Boolean operators in ACL fields such as `AUTONOMYMETADATA`. This allows connectors and custom scripts to use more complex logic to specify who is permitted to view a document. This might be necessary if the repository has a

complex security model that cannot be represented by a single ACL.

- You can now configure action authorization more flexibly. The [AuthorizationRoles] configuration section has been added. You can add subsections to create roles, which can use a combination of existing roles (equivalent to the existing AdminClients, QueryClients, and so on), or a specific set of actions. For each role, you can specify the client IPs and hosts, SSL identities, and GSS principals to use to identify users that have particular permissions to run actions.

If you want to use only SSL and GSS authorization, you can disable the client settings by setting the appropriate client configuration parameters to "". For example, AdminClients="" disables client authorization for administrative actions, and ensures that users must meet the SSL or GSS requirements.

- You can now set SSLCertificate to be a chain certificate in PEM format (consisting of the end-entity certificate, any intermediate certificates, and ending with the root CA certificate). This option allows a complete certificate to be returned to the connected peer.
- You can now set SSLCheckCertificate to False even when SSLCACertificate or SSLCACertificatePath are set. This allows the component to fill in any chain required for the SSLCertificate by using the certificates that you specify in SSLCACertificate and SSLCACertificatePath, without requiring a certificate from the connected peer.
- The GSSAPILibrary configuration parameter has been added to the [Paths] section. You can set this parameter to the path to the GSSAPI shared library or DLL that the application uses. Depending on your system configuration, HPE IDOL Server attempts to detect the appropriate library to use. However, if you use Kerberos or GSSAPI security in your setup, HPE recommends that you set an explicit value for this parameter.

## Resolved Issues

- When restarting, Content could erroneously log an error Expected at least  $N$  stemming entries, but read only  $M$  from stemming hash file.
- The GetQueryTagValues action sometimes omitted the <autn:total\_values> response tag for fields where no values were returned, even when TotalValues was set to True.
- The persistent term cache was not correctly updated with newly indexed data.
- The QuerySummary response <autn:element> tag pdocs and poccs attributes could count the occurrences of the summary element that were not exact phrase matches. For example, the counts for *cat dog* would also include occurrences of *dog cat* and *cat dogs*.
- The QuerySummary response <autn:element> tag ids attribute could contain the IDs of any documents that contained all the terms in the element, regardless of whether they appeared as a phrase.
- When sending a query that set Highlight to Proximity, highlight tags could be incorrectly placed in fields with restricted indexing of alphanumeric terms (that is when your configuration has IndexNumbers is set to a value other than 1, or includes the IndexNumbers/MaxLength settings).
- Sending the GetTagValues action with FieldName set to a metadata field could result in an ACI thread getting stuck in a busy loop.
- The response for the GetQueryTagValues action with AllowNonParametricFields set to True did not use consistent case normalization for values from parametric and non-parametric fields. Now, values for both parametric and non-parametric fields are returned as upper case unless you have configured CaseSensitiveParametricValues.

- The `GetVersion` action could incorrectly report their operating system on Microsoft Windows 10 and Microsoft Windows Server 2016 platforms.

## Category Component

### New in this Release

- You can now use additional parameters to control the creation of missing snapshots when you generate a spectrograph. When you send the `ClusterSGDataGen` action with the `FillGaps` parameter set to `True`, you can now set `DREQuery`, `Params`, `Values`, `SeedSize`, and `SeedBindLevel`, in the same way as for the `ClusterSnapshot` action.

- Category now logs additional details about the job queue for the schedule log type when `LogLevel` is set to `FULL`.

- You can now configure action authorization more flexibly. The `[AuthorizationRoles]` configuration section has been added. You can add subsections to create roles, which can use a combination of existing roles (equivalent to the existing `AdminClients`, `QueryClients`, and so on), or a specific set of actions. For each role, you can specify the client IPs and hosts, SSL identities, and GSS principals to use to identify users that have particular permissions to run actions.

If you want to use only SSL and GSS authorization, you can disable the client settings by setting the appropriate client configuration parameters to `""`. For example, `AdminClients=""` disables client authorization for administrative actions, and ensures that users must meet the SSL or GSS requirements.

- You can now set `SSLCertificate` to be a chain certificate in PEM format (consisting of the end-entity certificate, any intermediate certificates, and ending with the root CA certificate). This option allows a complete certificate to be returned to the connected peer.
- You can now set `SSLCheckCertificate` to `False` even when `SSLCACertificate` or `SSLCACertificatePath` are set. This allows the component to fill in any chain required for the `SSLCertificate` by using the certificates that you specify in `SSLCACertificate` and `SSLCACertificatePath`, without requiring a certificate from the connected peer.
- The `GSSAPILibrary` configuration parameter has been added to the `[Paths]` section. You can set this parameter to the path to the GSSAPI shared library or DLL that the application uses. Depending on your system configuration, HPE IDOL Server attempts to detect the appropriate library to use. However, if you use Kerberos or GSSAPI security in your setup, HPE recommends that you set an explicit value for this parameter.

### Resolved Issues

- The `GetVersion` action could incorrectly report their operating system on Microsoft Windows 10 and Microsoft Windows Server 2016 platforms.

## Community Component

### New in this Release

- You can now decrypt the user security strings that IDOL creates by using the `UserDecryptSecurityString` action. This action allows you to test your IDOL setup to ensure that security settings are applied correctly. This action is restricted to users with administrative permissions.
- You can now configure Community to automatically refresh `SecurityInfo` tokens. To enable token refresh, you must set the `SecurityTokenIdleTime` and `SecurityTokenRefreshInterval` configuration parameters in the `[Security]` section (or `[UserSecurity]` in a unified IDOL Server configuration file). To use refreshing tokens, you must also update the IDOL Content component, DAH component, and QMS component to version 11.4.0.
- You can now configure action authorization more flexibly. The `[AuthorizationRoles]` configuration section has been added. You can add subsections to create roles, which can use a combination of existing roles (equivalent to the existing `AdminClients`, `QueryClients`, and so on), or a specific set of actions. For each role, you can specify the client IPs and hosts, SSL identities, and GSS principals to use to identify users that have particular permissions to run actions.  
  
If you want to use only SSL and GSS authorization, you can disable the client settings by setting the appropriate client configuration parameters to `""`. For example, `AdminClients=""` disables client authorization for administrative actions, and ensures that users must meet the SSL or GSS requirements.
- You can now set `SSLCertificate` to be a chain certificate in PEM format (consisting of the end-entity certificate, any intermediate certificates, and ending with the root CA certificate). This option allows a complete certificate to be returned to the connected peer.
- You can now set `SSLCheckCertificate` to `False` even when `SSLCACertificate` or `SSLCACertificatePath` are set. This allows the component to fill in any chain required for the `SSLCertificate` by using the certificates that you specify in `SSLCACertificate` and `SSLCACertificatePath`, without requiring a certificate from the connected peer.
- The `GSSAPILibrary` configuration parameter has been added to the `[Paths]` section. You can set this parameter to the path to the GSSAPI shared library or DLL that the application uses. Depending on your system configuration, HPE IDOL Server attempts to detect the appropriate library to use. However, if you use Kerberos or GSSAPI security in your setup, HPE recommends that you set an explicit value for this parameter.

### Resolved Issues

- Community did not respect the `DeferLogin` configuration parameter.
- The `GetVersion` action could incorrectly report their operating system on Microsoft Windows 10 and Microsoft Windows Server 2016 platforms.

## 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

- Improved support for extracting information from HTML. CFS can now use an embedded browser (WKOOP) to process HTML in a similar way to the IDOL Web Connector. This has many advantages over previous methods of processing HTML. The embedded browser allows scripts to run before the page is processed, so CFS can extract content and links that are added by JavaScript. You can also remove unwanted content, divide pages into multiple documents, and extract metadata using CSS selectors rather than regular expressions. There is a new pre-import task, `wkoopHtmlExtraction`, and a new Lua function, `wkoop_html_processing`, to provide these features.

**NOTE:**

To use this feature you must also install the IDOL Web Connector, because WKOOP is not provided with CFS.

- CFS can transform XML files using an XSL stylesheet, before attempting to parse them. You might want to use this feature if you need to process XML documents that have different schema to IDOL documents. You can configure multiple transformations and CFS can determine which transformation to run by validating that the ingested XML matches a schema file.
- CFS includes the libraries that are necessary to run Lua functionality from an external process or IDE. This allows you to use an IDE to develop and test Lua scripts.
- The `ImportExtractExternal` parameter has been added. Some documents contain links to external files, for example URLs to files that are available through a web site. KeyView processes a link to an external file as a sub-file, but it cannot retrieve the external file and so returns an error. To prevent CFS creating documents for sub-files that cannot be processed, and logging errors that are returned by KeyView, set `ImportExtractExternal=False`.
- The Eduction task supports a new parameter, `MatchTimeout`. This specifies the maximum amount of time to spend searching for matches (to all chosen entities) at a specific offset. If the timeout is reached, Eduction returns the best match it has found (if any) and continues looking for matches later in the text. The default value of this parameter is 60 seconds, but in most cases the timeout is never reached. The timeout has been added to prevent Eduction running for a long time with abnormal input text.
- Eduction can now extract entities from zones (a zone is a part of a field defined by start and end patterns). The configuration parameters `EntityZoneN`, `ZoneStartN`, and `ZoneEndN` have been added.
- CFS can index documents into a MetaStore using SSL/TLS. The MetaStore indexer now supports the configuration parameter `SSLConfig`, which specifies the name of the section in the configuration file that contains the SSL settings.
- CFS supports the following Lua functions:

- `get_log_service`, and the new class `LuaLogService`. You can use these when you want to write log messages to a custom log file (instead of the standard ACI server log files).
- `parse_document_csv`, `parse_document_idx`, and `parse_document_xml`. These functions parse CSV, IDX, or XML files into documents and call a function on each document. `parse_document_idx` and `parse_document_xml` can also parse a string or file that contains a single document and return a `LuaDocument` object.
- New functions and classes for parsing and manipulating JSON. The new functions are `parse_json`, `parse_json_array`, and `parse_json_object`. The new classes are `LuaJsonArray`, `LuaJsonObject`, and `LuaJsonValue`.
- You can now configure action authorization more flexibly. The `[AuthorizationRoles]` configuration section has been added. You can add subsections to create roles, which can use a combination of existing roles (equivalent to the existing `AdminClients`, `QueryClients`, and so on), or a specific set of actions. For each role, you can specify the client IPs and hosts, SSL identities, and GSS principals to use to identify users that have particular permissions to run actions.  
  
If you want to use only SSL and GSS authorization, you can disable the client settings by setting the appropriate client configuration parameters to `""`. For example, `AdminClients=""` disables client authorization for administrative actions, and ensures that users must meet the SSL or GSS requirements.
- You can now set `SSLCertificate` to be a chain certificate in PEM format (consisting of the end-entity certificate, any intermediate certificates, and ending with the root CA certificate). This option allows a complete certificate to be returned to the connected peer.
- You can now set `SSLCheckCertificate` to `False` even when `SSLCACertificate` or `SSLCACertificatePath` are set. This allows the component to fill in any chain required for the `SSLCertificate` by using the certificates that you specify in `SSLCACertificate` and `SSLCACertificatePath`, without requiring a certificate from the connected peer.
- The `GSSAPILibrary` configuration parameter has been added to the `[Paths]` section. You can set this parameter to the path to the GSSAPI shared library or DLL that the application uses. Depending on your system configuration, HPE IDOL Server attempts to detect the appropriate library to use. However, if you use Kerberos or GSSAPI security in your setup, HPE recommends that you set an explicit value for this parameter.

## Resolved Issues

- The `GetVersion` action could incorrectly report their operating system on Microsoft Windows 10 and Microsoft Windows Server 2016 platforms.

## Controller

### New in this Release

- You can now configure Coordinator and Controller to store statistics in a shared SQL database, rather than locally on disk. You can also set up multiple coordinators to use the same database, for a simple high availability setup.

As part of this change, the Controller components now store the statistics in the database.

To configure Controller to use a SQL database, set `UseODBCDatabase` to `True` in the `[Server]` section, and set `ConnectionString` in the `[Server]` section to the connection string for the database.

**CAUTION:**

As part of this update, the statistics format has been changed. As a result, when you upgrade to Controller 11.4.0, you cannot view the older statistics.

- Supported scheduled index actions can now take additional parameters in the same way as the scheduled ACI actions.
- You can now configure action authorization more flexibly. The `[AuthorizationRoles]` configuration section has been added. You can add subsections to create roles, which can use a combination of existing roles (equivalent to the existing `AdminClients`, `QueryClients`, and so on), or a specific set of actions. For each role, you can specify the client IPs and hosts, SSL identities, and GSS principals to use to identify users that have particular permissions to run actions.  
  
If you want to use only SSL and GSS authorization, you can disable the client settings by setting the appropriate client configuration parameters to `""`. For example, `AdminClients=""` disables client authorization for administrative actions, and ensures that users must meet the SSL or GSS requirements.
- You can now set `SSLCertificate` to be a chain certificate in PEM format (consisting of the end-entity certificate, any intermediate certificates, and ending with the root CA certificate). This option allows a complete certificate to be returned to the connected peer.
- You can now set `SSLCheckCertificate` to `False` even when `SSLCACertificate` or `SSLCACertificatePath` are set. This allows the component to fill in any chain required for the `SSLCertificate` by using the certificates that you specify in `SSLCACertificate` and `SSLCACertificatePath`, without requiring a certificate from the connected peer.
- The `GSSAPILibrary` configuration parameter has been added to the `[Paths]` section. You can set this parameter to the path to the GSSAPI shared library or DLL that the application uses. Depending on your system configuration, HPE IDOL Server attempts to detect the appropriate library to use. However, if you use Kerberos or GSSAPI security in your setup, HPE recommends that you set an explicit value for this parameter.

## Resolved Issues

- Controller sometimes sent plain HTTP requests to child services configured for HTTPS.
- Controller did not retrieve statistics from child services configured for HTTPS.
- Controller sometimes failed to detect a Windows service that did not have a valid service description.
- The `GetVersion` action could incorrectly report their operating system on Microsoft Windows 10 and Microsoft Windows Server 2016 platforms.

# Coordinator

## New in this Release

- Coordinator can now store collected statistics in your SQL database backend, alongside Controller information. To use this option, set the `UseODBCDatabase` parameter to `True` in the `[StatsCollector]` section, and set the `ConnectionString` parameter in the `[Server]` section to the connection string for the database.

**NOTE:**

For consistency with other IDOL components, the `SQLConnectionString` parameter is now called `ConnectionString`. You can still use `SQLConnectionString` as the parameter name. If your configuration file contains both parameters, Coordinator uses the `SQLConnectionString` parameter.

- You can now configure Coordinator and Controller to store statistics in a shared SQL database, rather than locally on disk. You can also set up multiple coordinators to use the same database, for a simple high availability setup.

As part of this change, the Controller components now store the statistics in the database. Coordinator uses the database to store information about the Controller components, and also reads the statistics information.

To configure Coordinator to use a SQL database, set `UseODBCDatabase` to `True` in the `[StatsCollector]` section, and set `ConnectionString` in the `[Server]` section to the connection string for the database.

**CAUTION:**

As part of this update, the statistics format has been changed. As a result, when you upgrade to Coordinator 11.4.0, you cannot view the older statistics.

- The `LiveDetails` parameter has been added to the `ListMeters` action. By default, Coordinator attempts to retrieve live values for meter names from the child Controller servers. If a Controller is unavailable, Coordinator uses the cached values, and returns a warning that the values are cached. You can also set `LiveDetails` to `False` to explicitly request the locally stored cache values. In this case, Coordinator does not return a warning.
- Supported scheduled index actions can now take additional parameters in the same way as the scheduled ACI actions.
- You can now configure action authorization more flexibly. The `[AuthorizationRoles]` configuration section has been added. You can add subsections to create roles, which can use a combination of existing roles (equivalent to the existing `AdminClients`, `QueryClients`, and so on), or a specific set of actions. For each role, you can specify the client IPs and hosts, SSL identities, and GSS principals to use to identify users that have particular permissions to run actions.  
  
If you want to use only SSL and GSS authorization, you can disable the client settings by setting the appropriate client configuration parameters to `""`. For example, `AdminClients=""` disables client authorization for administrative actions, and ensures that users must meet the SSL or GSS requirements.

- You can now set `SSLCertificate` to be a chain certificate in PEM format (consisting of the end-entity certificate, any intermediate certificates, and ending with the root CA certificate). This option allows a complete certificate to be returned to the connected peer.
- You can now set `SSLCheckCertificate` to `False` even when `SSLCACertificate` or `SSLCACertificatePath` are set. This allows the component to fill in any chain required for the `SSLCertificate` by using the certificates that you specify in `SSLCACertificate` and `SSLCACertificatePath`, without requiring a certificate from the connected peer.
- The `GSSAPILibrary` configuration parameter has been added to the `[Paths]` section. You can set this parameter to the path to the GSSAPI shared library or DLL that the application uses. Depending on your system configuration, HPE IDOL Server attempts to detect the appropriate library to use. However, if you use Kerberos or GSSAPI security in your setup, HPE recommends that you set an explicit value for this parameter.

## Resolved Issues

- The `GetVersion` action could incorrectly report their operating system on Microsoft Windows 10 and Microsoft Windows Server 2016 platforms.

## Distributed Action Handler

### New in this Release

- The DAH has been updated to return the new `<autn:valuepercentiles>` tags in the response to the `GetQueryTagValues` action when `ValueDetails` is set to `True`.

**NOTE:**

When you send the `GetQueryTagValues` action to a DAH, the `ValueDetails` response always includes only the default value percentiles. DAH ignores any values you set in the new `ValuePercentiles` parameter. However, the DAH requests additional percentiles from the child servers so that it can calculate the appropriate ranges for the whole dataset.

- The DAH has been updated to process the new `CostEstimate` parameter for the `DocumentStats` action.
- The DAH has been updated to process the new `ValueRestriction` parameter for the `GetQueryTagValues` action.
- The DAH now supports refreshing of `SecurityInfo` tokens. When you configure the new `SecurityTokenIdleTime` parameter in Community 11.4, DAH returns refresh tokens in a `responsedata/autn:securityinfo` element in the response for actions that accept the `SecurityInfo` parameter.
- You can now configure action authorization more flexibly. The `[AuthorizationRoles]` configuration section has been added. You can add subsections to create roles, which can use a combination of existing roles (equivalent to the existing `AdminClients`, `QueryClients`, and so on), or a specific set of actions. For each role, you can specify the client IPs and hosts, SSL identities, and GSS principals to use to identify users that have particular permissions to run actions.

If you want to use only SSL and GSS authorization, you can disable the client settings by setting the appropriate client configuration parameters to "". For example, `AdminClients=""` disables client authorization for administrative actions, and ensures that users must meet the SSL or GSS requirements.

- You can now set `SSLCertificate` to be a chain certificate in PEM format (consisting of the end-entity certificate, any intermediate certificates, and ending with the root CA certificate). This option allows a complete certificate to be returned to the connected peer.
- You can now set `SSLCheckCertificate` to `False` even when `SSLCACertificate` or `SSLCACertificatePath` are set. This allows the component to fill in any chain required for the `SSLCertificate` by using the certificates that you specify in `SSLCACertificate` and `SSLCACertificatePath`, without requiring a certificate from the connected peer.
- The `GSSAPILibrary` configuration parameter has been added to the `[Paths]` section. You can set this parameter to the path to the GSSAPI shared library or DLL that the application uses. Depending on your system configuration, HPE IDOL Server attempts to detect the appropriate library to use. However, if you use Kerberos or GSSAPI security in your setup, HPE recommends that you set an explicit value for this parameter.

## Resolved Issues

- DAH sometimes split the `authn:field` tags in the response to a `GetQueryTagValues` action with `FieldDependenceMultiLevel` set to `True`.
- A `GetQueryTagValues` action could fail if `FieldDependenceMultiLevel` was set to `True` and a child server was unavailable.
- When merging `GetQueryTagValues` actions from child servers, DAH sometimes returned the wrong minimum values in the `ValueDetails` responses when some engines did not return any values.
- The `CombineIgnoreMissingValues` configuration parameter did not have an effect on queries sent through a DAH with the `Combine` action parameter set to `FieldCheck`.

### NOTE:

To resolve this issue, you must also update your Content components to version 11.4.0 or later.

- When requesting a JSON response from an action configured as a `DistributedCommand`, DAH could terminate unexpectedly.
- The `GetVersion` action could incorrectly report their operating system on Microsoft Windows 10 and Microsoft Windows Server 2016 platforms.

## Distributed Index Handler

### New in this Release

- You can now configure DIH to use GSSAPI authentication on the index port. To enable it, you must set the `GSSServiceName` parameter in the `[Server]` section to the fully qualified GSSAPI service

name that the Content component must use to identify itself. You must also set `RequireGSSAuth` to **True** in the `[IndexServer]` section to enable authentication.

You can also set `GSSServiceName` in the child server configuration sections (`[DIHEngineN]` or `[IDOLServerN]`) to use GSSAPI authentication to connect to the child server index ports. This option sets the service name to use for the child server.

**NOTE:**

This method provides an authentication requirement only. HPE recommends that you use it in conjunction with TLS/SSL to encrypt the authentication data.

- The `DIH EngineManagement` action now supports the `SSLConfig`, `ServiceSSLConfig`, and `GSSServiceName` parameters, to allow you to set these parameters when you add a new child server in the action.
- The `GSSServiceName` parameter has been added to the `DREEXPORTREMOTE` index action to allow you to export documents to a server that uses GSSAPI authentication.
- In `DistributeByDate` mode, you can now configure the `UnknownFieldValueAction` configuration parameter in the `[Server]` section to determine how to treat documents where the date field is missing, or does not contain a valid value in one of the configured date ranges.

The `UnknownFieldValueAction` configuration parameter has the same options as for `DistributebyFields` mode, but in `DistributeByDate` mode the default value is `Ignore`, which matches the existing behavior. For more information, refer to the *DIH Reference*.

- You can now configure action authorization more flexibly. The `[AuthorizationRoles]` configuration section has been added. You can add subsections to create roles, which can use a combination of existing roles (equivalent to the existing `AdminClients`, `QueryClients`, and so on), or a specific set of actions. For each role, you can specify the client IPs and hosts, SSL identities, and GSS principals to use to identify users that have particular permissions to run actions.

If you want to use only SSL and GSS authorization, you can disable the client settings by setting the appropriate client configuration parameters to `""`. For example, `AdminClients=""` disables client authorization for administrative actions, and ensures that users must meet the SSL or GSS requirements.

- You can now set `SSLCertificate` to be a chain certificate in PEM format (consisting of the end-entity certificate, any intermediate certificates, and ending with the root CA certificate). This option allows a complete certificate to be returned to the connected peer.
- You can now set `SSLCheckCertificate` to `False` even when `SSLCACertificate` or `SSLCACertificatePath` are set. This allows the component to fill in any chain required for the `SSLCertificate` by using the certificates that you specify in `SSLCACertificate` and `SSLCACertificatePath`, without requiring a certificate from the connected peer.
- The `GSSAPILibrary` configuration parameter has been added to the `[Paths]` section. You can set this parameter to the path to the GSSAPI shared library or DLL that the application uses. Depending on your system configuration, HPE IDOL Server attempts to detect the appropriate library to use. However, if you use Kerberos or GSSAPI security in your setup, HPE recommends that you set an explicit value for this parameter.

## Resolved Issues

- The `GetVersion` action could incorrectly report their operating system on Microsoft Windows 10 and Microsoft Windows Server 2016 platforms.

## File System Connector CFS

### New in this Release

- The `identifiers fetch` action supports a new parameter, `FilterTypes`, which accepts a comma-separated list of the types of items to return identifiers for.
- The connector supports progress reporting for the `collect`, `delete`, `insert`, `stub`, and `update fetch` actions.
- The connector supports the following Lua functions:
  - `get_log_service`, and the new class `LuaLogService`. You can use these when you want to write log messages to a custom log file (instead of the standard ACI server log files).
  - `parse_document_csv`, `parse_document_idx`, and `parse_document_xml`. These functions parse CSV, IDX, or XML files into documents and call a function on each document. `parse_document_idx` and `parse_document_xml` can also parse a string or file that contains a single document and return a `LuaDocument` object.
  - New functions and classes for parsing and manipulating JSON. The new functions are `parse_json`, `parse_json_array`, and `parse_json_object`. The new classes are `LuaJsonArray`, `LuaJsonObject`, and `LuaJsonValue`.
- You can now call the Lua method `insertJson` on `LuaField` objects as well as `LuaDocument` objects. You can also pass it one of the new `LuaJsonArray` or `LuaJsonObject` objects instead of a string.
- You can now configure action authorization more flexibly. The `[AuthorizationRoles]` configuration section has been added. You can add subsections to create roles, which can use a combination of existing roles (equivalent to the existing `AdminClients`, `QueryClients`, and so on), or a specific set of actions. For each role, you can specify the client IPs and hosts, SSL identities, and GSS principals to use to identify users that have particular permissions to run actions.

If you want to use only SSL and GSS authorization, you can disable the client settings by setting the appropriate client configuration parameters to `""`. For example, `AdminClients=""` disables client authorization for administrative actions, and ensures that users must meet the SSL or GSS requirements.
- You can now set `SSLCertificate` to be a chain certificate in PEM format (consisting of the end-entity certificate, any intermediate certificates, and ending with the root CA certificate). This option allows a complete certificate to be returned to the connected peer.
- You can now set `SSLCheckCertificate` to `False` even when `SSLCACertificate` or `SSLCACertificatePath` are set. This allows the component to fill in any chain required for the

SSLCertificate by using the certificates that you specify in SSLCACertificate and SSLCACertificatePath, without requiring a certificate from the connected peer.

- The GSSAPILibrary configuration parameter has been added to the [Paths] section. You can set this parameter to the path to the GSSAPI shared library or DLL that the application uses. Depending on your system configuration, HPE IDOL Server attempts to detect the appropriate library to use. However, if you use Kerberos or GSSAPI security in your setup, HPE recommends that you set an explicit value for this parameter.

## Resolved Issues

- The GetVersion action could incorrectly report the operating system on Microsoft Windows 10 and Microsoft Windows Server 2016.

## Find

### New in this Release

- You can now configure custom templates to use to display search results, by using the new templates.json configuration file.

**NOTE:**

As part of this change, the directAccessLink option in the config.json configuration file has been removed. To set up Find to open the original document in a new tab, you must now configure a custom template.

- You can now configure dashboards to be accessible only to users with a particular role, by setting the roles property in the dashboard configuration.
- You can now share saved searches with other users. Each saved search has a **Sharing Options** button to allow you to share the search with other users, and to give other users different permissions for your saved search. You can optionally give other users permission to edit your saved search.

The Search page now includes a **Shared by others** drop down list to show you shared saved searches (for example, searches used in dashboards).

- The API to reload the Find dashboard configuration has been updated so that you can reload all customization configuration, such as applications. The new API endpoint is:

```
/api/admin/customization/config/reload
```

**NOTE:**

The /api/admin/dashboards/reload endpoint is no longer available.

- You can now upload a custom logo to the Find user interface. The new Customizations settings page allows you to upload logos for the splash screen (visible to users who do not belong to the **FindBI** role), and the small logo that appears in the navigation bar.

The following features were added in Find version 11.3.1.

- Find now has configurable dashboards for users with the `FindBI` role, to allow you to set up easy ways for your business information users to monitor and review data. You configure your dashboards to display a set of widgets. Each widget shows a visualization (such as a topic map or sunburst), search results, or some static or video content.

The configured dashboards are listed in the Find sidebar, and you can also access them by URL. You can display the dashboards in full screen mode, and export them to a presentation file.

- The new **Trending** visualizer has been added to the Find search user interface. This visualizer displays a chart of document rate against time, for the values in a particular field, to show how particular topics have changed in popularity over time. The document rate is the number of documents added in the specified time unit (second, minute, hour, day, or year). The appropriate time unit is chosen according to the document rates in your data.

You can select the field to display. Each field value is displayed in a different color on the chart.

- Find now has a configurable option for adding links to additional applications to the Find navigation sidebar. You can configure applications by using the `applications.json` configuration file, which specifies a list of application URLs to link to.
- The configuration for setting a friendly display name for a parametric field or value has been improved. You now configure the display name and value mappings in the `fieldsInfo` section of the configuration file. These settings now also apply to fields in the document preview tabs. #

**NOTE:**

As part of this change, the `parametricDisplayValues` configuration section has been removed. You must update your configuration to use the new option. For more information, refer to the *HPE Find Administration Guide*.

- You can now configure fields to show and hide in document previews, by using the `fieldsInfo` section of the configuration file. For more information, refer to *HPE Find Administration Guide*.
- Find can now display location information from multiple field pairs in the map visualizer. Markers for locations belonging to different fields are differentiated by color. By default, locations are displayed for all field pairs, and you can deselect pairs in the user interface to show results only for particular fields.
- Find now preserves the current results view (topic map, list, sunburst, and so on) between login sessions, if you were previously routed to a visualizer in a saved search tab.

**NOTE:**

New searches still route to the first visualizer that you configure in the `resultViewOrder` configuration option.

- Find now stores the ID of a saved search in the URL, so that you can refer to it more easily.
- The Find application load time has been improved by optimizing the parametric value loading.
- Find now loads only the top five parametric values to display in the UI sidebar, which optimizes the loading time.
- The performance for loading parametric values has been improved. Find now estimates the number of documents for each value when there are a large number of results.
- The performance for loading parametric field names has been improved. Find now uses fewer actions to the IDOL backend to retrieve this information.
- Find now displays loading spinners and error messages separately for filter fields and field values.

- Find now displays the friendly names of fields in the metadata tab for a document.
- Document viewing has been improved. If a document does not have the required reference field or connector group and identifier, Find now renders the title and document content from the Content index in the document previews. In this case, it uses the `autn:title` and `DRECONTENT` fields to populate the title and content, respectively.
- You can now configure the location that Find uses to store the application log files, by setting the `logging.path` property in the Java run command.
- Find now generates an `access.log` file to log all HTTP requests.
- Find now generates an `idol-access.log` file to log all actions that it sends to an IDOL component ACI or service port. This log includes information about the component, action, and the status codes or errors that returned. It also logs timing information for performance monitoring. The log is enabled by default, but you can turn off IDOL action logging by modifying the `idol.log.enabled` property in the Java run command. You can also turn off the timing information by setting the `idol.log.timing.enabled` property in the Java run command.
- The handling of XML fields in the data indexes has been improved. Find now supports nested XML fields. However, the XML hierarchy must be nested within `DOCUMENTS/DOCUMENT` tags.
- Find now shows the transcript for a video (if it exists) in the basic preview panel when you select a result in the results list, as well as the full preview page.
- Find now generates numeric and date visualizations for fields that are configured in IDOL as `NumericType` and `NumericDateType`. Previously the visualizations required the fields to be `ParametricType`.
- Find now uses IDOL prediction for queries. Prediction means that when there are a large number of results, IDOL estimates the total number, rather than counting every result, which can improve the query performance. You can modify the threshold at which prediction applies in your IDOL Content component configuration. For more information, refer to the *IDOL Server Reference*.
- The Find interactive installer now works with .NET Framework versions up to v4.
- The performance of Topic Map generation has been improved. Find now no longer animates the loading process.
- The version of Spring Boot was upgraded. As a result, Find no longer logs a warning message at startup.
- Find now sends the `UserRead` action with the `DeferLogin` parameter. This option allows you to use an IDOL Community component that uses a third-party repository (such as LDAP) to authenticate users.
- You can now configure a list of default roles that Find assigns to a new user, by setting the `find.defaultRoles` property in the Java run command. You can use this option to assign default roles to new users when you have an IDOL Community component that uses a third-party repository to authenticate users.

## Resolved Issues

- The Sunburst visualizer sometimes appeared blank when a query did not return any results and the user switched between views.
- When loading the Trending tab, Find could make additional unnecessary calls to the IDOL components.

- Users were unnecessarily added to the database multiple times.

**CAUTION:**

This change involves an upgrade and migration of your existing data. HPE strongly recommends that you back up the data folder in your home directory before you run the installer.

When you run the Find 11.4.0 installer in an existing installation, the installer migrates your data automatically.

- Snapshot queries could show up-to-date query results, rather than results from the time that the snapshot was saved.

The following issues were resolved in HPE Find version 11.3.1.

- In the CSV file produced by Export to CSV, headers were repeated every 1000 results.
- The snapshot details screen used the original field names for parametric filters, rather than the custom display names.
- In BI mode, Find could perform auto-correction on search terms when the concepts were changed.
- When Find auto-corrected a search term, it sometimes displayed a **No more results found** message, as well as the auto-correction information and results for the auto-corrected terms.
- The field selectors in Table and Sunburst views contained fields in a different order to the parametric field list. Find now always uses the order of the parametric filters for the field selection views (including order specified by configuration).
- Related concepts could fail to load after a user followed a URL that was redirected.
- It was possible to change a concept to an empty string and save it.
- The Find standard field configuration did not match the latest IDOL connector standard field names. The Find configuration now matches both the new and old IDOL standard fields. For example, AU\_REPOSITORY\_METADATA\_URL\_FILE\_STRING and REPOSITORY\_METADATA\_URL\_FILE\_STRING are both supported.
- When polling for new saved search results, time zone offsets were not handled correctly.
- In some cases, Find included an incorrect estimated document age in results lists.
- When an IDOL component was unavailable or configured incorrectly, saving the Find Settings page resulted in a *Server returned error* message. The error messages are now more specific.
- When running the initial Find configuration, it was possible to save the settings with incomplete information for the Community component, such that Find did not retrieve user login information from Community and users could not log in to the new installation. Find now requires that you test the connection to the Community component before you can save the configuration.
- The document preview pane was not sized correctly when using Microsoft Windows 10 with the Microsoft Edge browser.
- Selecting the calendar option on the Autn Date filter time bar selected the whole time bar.
- When the search terms for a saved search were changed, Find could use the previous search terms to compare results for two saved searches (in the **Compare** view).

## HTTP Connector CFS (Solaris only)

### New in this Release

- The connector supports the following Lua functions:
  - `get_log_service`, and the new class `LuaLogService`. You can use these when you want to write log messages to a custom log file (instead of the standard ACI server log files).
  - `parse_document_csv`, `parse_document_idx`, and `parse_document_xml`. These functions parse CSV, IDX, or XML files into documents and call a function on each document. `parse_document_idx` and `parse_document_xml` can also parse a string or file that contains a single document and return a `LuaDocument` object.
  - New functions and classes for parsing and manipulating JSON. The new functions are `parse_json`, `parse_json_array`, and `parse_json_object`. The new classes are `LuaJsonArray`, `LuaJsonObject`, and `LuaJsonValue`.
- You can now call the Lua method `insertJson` on `LuaField` objects as well as `LuaDocument` objects. You can also pass it one of the new `LuaJsonArray` or `LuaJsonObject` objects instead of a string.
- You can now configure action authorization more flexibly. The `[AuthorizationRoles]` configuration section has been added. You can add subsections to create roles, which can use a combination of existing roles (equivalent to the existing `AdminClients`, `QueryClients`, and so on), or a specific set of actions. For each role, you can specify the client IPs and hosts, SSL identities, and GSS principals to use to identify users that have particular permissions to run actions.  
  
If you want to use only SSL and GSS authorization, you can disable the client settings by setting the appropriate client configuration parameters to `""`. For example, `AdminClients=""` disables client authorization for administrative actions, and ensures that users must meet the SSL or GSS requirements.
- You can now set `SSLCertificate` to be a chain certificate in PEM format (consisting of the end-entity certificate, any intermediate certificates, and ending with the root CA certificate). This option allows a complete certificate to be returned to the connected peer.
- You can now set `SSLCheckCertificate` to `False` even when `SSLCACertificate` or `SSLCACertificatePath` are set. This allows the component to fill in any chain required for the `SSLCertificate` by using the certificates that you specify in `SSLCACertificate` and `SSLCACertificatePath`, without requiring a certificate from the connected peer.
- The `GSSAPILibrary` configuration parameter has been added to the `[Paths]` section. You can set this parameter to the path to the GSSAPI shared library or DLL that the application uses. Depending on your system configuration, HPE IDOL Server attempts to detect the appropriate library to use. However, if you use Kerberos or GSSAPI security in your setup, HPE recommends that you set an explicit value for this parameter.

## Resolved Issues

- The `GetVersion` action could incorrectly report the operating system on Microsoft Windows 10 and Microsoft Windows Server 2016.

## IDOL Admin

IDOL Admin was updated in line with other IDOL components. There were no new features or resolved issues.

## IDOL Proxy Component

### New in this Release

- You can now configure action authorization more flexibly. The `[AuthorizationRoles]` configuration section has been added. You can add subsections to create roles, which can use a combination of existing roles (equivalent to the existing `AdminClients`, `QueryClients`, and so on), or a specific set of actions. For each role, you can specify the client IPs and hosts, SSL identities, and GSS principals to use to identify users that have particular permissions to run actions.

If you want to use only SSL and GSS authorization, you can disable the client settings by setting the appropriate client configuration parameters to `""`. For example, `AdminClients=""` disables client authorization for administrative actions, and ensures that users must meet the SSL or GSS requirements.

- You can now set `SSLCertificate` to be a chain certificate in PEM format (consisting of the end-entity certificate, any intermediate certificates, and ending with the root CA certificate). This option allows a complete certificate to be returned to the connected peer.
- You can now set `SSLCheckCertificate` to `False` even when `SSLCACertificate` or `SSLCACertificatePath` are set. This allows the component to fill in any chain required for the `SSLCertificate` by using the certificates that you specify in `SSLCACertificate` and `SSLCACertificatePath`, without requiring a certificate from the connected peer.
- The `GSSAPILibrary` configuration parameter has been added to the `[Paths]` section. You can set this parameter to the path to the GSSAPI shared library or DLL that the application uses. Depending on your system configuration, HPE IDOL Server attempts to detect the appropriate library to use. However, if you use Kerberos or GSSAPI security in your setup, HPE recommends that you set an explicit value for this parameter.

## Resolved Issues

- The `GetVersion` action could incorrectly report their operating system on Microsoft Windows 10 and Microsoft Windows Server 2016 platforms.

## IDOL Site Admin

IDOL Site Admin was updated in line with other IDOL components. There were no new features or resolved issues.

### New in this Release

There were no new features in IDOL Site Admin version 11.4.0

### Resolved Issues

There were no resolved issues in IDOL Site Admin version 11.4.0.

## IDOL Speech Server

### New in this Release

- Open set language identification has been added, to allow for unknown languages in the data. In this case, if the confidence that a section of audio matches a particular language is lower than the threshold, Speech Server returns that the language is **unknown**.

This change also includes the following changes:

- The language identification classifier packs have been updated to support open set mode.
  - Single language classifier identification is now supported. You can use this option with open set classification if you want to confirm whether a segment of audio contains a particular language, and do not need to know what other languages it might contain.
  - Score thresholds for language classifiers are now automatically estimated during the optimization process.
  - The optimization log output has been improved and extended.
  - Language ID scores are now given as raw values, rather than normalized between zero and one. The raw scores are compared directly to the score thresholds.
- You can now use your IDOL Content component data index as a source of text when you build language models. To use this, you can configure the host and port of the Content component in the `lmbuild` module, and the `LanguageModelBuild` standard task. The following table describes the new configuration parameters that you can specify for the `lmbuild` module. For more detail, refer to the *IDOL Speech Server Reference*.

ContentHost

ContentPort

ContentDatabase

ContentTextTag

- You can now optionally produce diagnostic information for language model building by using the `DiagLevel` and `DiagFile` parameters in the `lmbuild` module, and the `LanguageModelBuild` standard task.
- You can now add a build label to a custom language model to make it easier to track language models. The `BuildLabel` parameter has been added to the `lmbuild` module, and the `LanguageModelBuild` standard task.
- The new `BuildLabel` parameter has been added to the `ListCustomLM` action. You can use this parameter to filter the response to a particular language model build label. You can also use the new `LatestOnly` parameter to filter to the latest version of the language model.
- The `GetStatus` action now returns additional information about loaded language models. The new `<lm>` sections provide details about the name, file name, weight, and build label, and specifies whether it is a custom language model.
- The an `ID` parameter has been added to the `UnloadLanguage` action, to allow you to unload a language resource by its ID. You can retrieve the ID from the `GetStatus` action response.
- You can now run scheduled tasks in Speech Server. For example, you might want to use a regular `LanguageModelBuild` task to update the language model with new data.

You can set up schedules by configuring the `[Schedule]` section in the Speech Server configuration file. You can also use the new `ScheduleTask` action to set up a new schedule. The new `ListSchedules` and `UnscheduleTask` actions allow you to list and cancel schedules, respectively.

For more information, see the *IDOL Speech Server Reference* and *IDOL Speech Server Administration Guide*.

- You can now set the maximum length of a segment of speech or non-speech in a speaker identification task, by using the new `MaxSpeech` and `MaxNonSpeech` parameters in the `speakerid` module, or in the `IvSpkIdEvalStream` and `IvSpkIdEvalWav` standard tasks.  
Shorter maximum segment sizes can reduce the latency of result generation, because Speech Server must wait for the speech segment to finish before it runs speaker segmentation and identification. However, reducing the maximum size by too much can affect the accuracy of results.
- The `StartTime` and `EndTime` parameters have been added to the `LangIDBndWav`, `LangIDCumWav`, `LangIDFeature`, and `LangIDSegWav` standard tasks, to allow you to specify the start and end time of the section that you want to process in the audio file.
- You can now configure action authorization more flexibly. The `[AuthorizationRoles]` configuration section has been added. You can add subsections to create roles, which can use a combination of existing roles (equivalent to the existing `AdminClients`, `QueryClients`, and so on), or a specific set of actions. For each role, you can specify the client IPs and hosts, SSL identities, and GSS principals to use to identify users that have particular permissions to run actions.  
If you want to use only SSL and GSS authorization, you can disable the client settings by setting the appropriate client configuration parameters to `""`. For example, `AdminClients=""` disables client authorization for administrative actions, and ensures that users must meet the SSL or GSS requirements.
- You can now set `SSLCertificate` to be a chain certificate in PEM format (consisting of the end-entity certificate, any intermediate certificates, and ending with the root CA certificate). This option allows a complete certificate to be returned to the connected peer.

- You can now set `SSLCheckCertificate` to `False` even when `SSLCACertificate` or `SSLCACertificatePath` are set. This allows the component to fill in any chain required for the `SSLCertificate` by using the certificates that you specify in `SSLCACertificate` and `SSLCACertificatePath`, without requiring a certificate from the connected peer.
- The `GSSAPILibrary` configuration parameter has been added to the `[Paths]` section. You can set this parameter to the path to the GSSAPI shared library or DLL that the application uses. Depending on your system configuration, HPE IDOL Server attempts to detect the appropriate library to use. However, if you use Kerberos or GSSAPI security in your setup, HPE recommends that you set an explicit value for this parameter.

## Resolved Issues

- The duration of `NonSpeech` segments in `Speaker ID` was often reported as shorter than actually computed.
- Incorrect parsing of temporary files could occasionally lead to a loss of service while language models were building.
- Running the `LanguageModelBuild` task with an invalid output language model name (invalid file extension) could result in an interruption of service.
- A `ListManager` error could sometimes prevent `Speech Server` from starting.
- Setting the speaker template threshold by using the `ivSpkIDTmpEditThresh` task could result in an interruption of service.
- When running language identification in boundary mode, the task progress times given in `GetStatus` did not update correctly when there was no change in language detected.
- The `GetVersion` action could incorrectly report their operating system on Microsoft Windows 10 and Microsoft Windows Server 2016 platforms.

## Knowledge Graph Component

### New in this Release

- You can now configure action authorization more flexibly. The `[AuthorizationRoles]` configuration section has been added. You can add subsections to create roles, which can use a combination of existing roles (equivalent to the existing `AdminClients`, `QueryClients`, and so on), or a specific set of actions. For each role, you can specify the client IPs and hosts, SSL identities, and GSS principals to use to identify users that have particular permissions to run actions.  
If you want to use only SSL and GSS authorization, you can disable the client settings by setting the appropriate client configuration parameters to `""`. For example, `AdminClients=""` disables client authorization for administrative actions, and ensures that users must meet the SSL or GSS requirements.
- You can now set `SSLCertificate` to be a chain certificate in PEM format (consisting of the end-entity certificate, any intermediate certificates, and ending with the root CA certificate). This option allows a complete certificate to be returned to the connected peer.

- You can now set `SSLCheckCertificate` to `False` even when `SSLCACertificate` or `SSLCACertificatePath` are set. This allows the component to fill in any chain required for the `SSLCertificate` by using the certificates that you specify in `SSLCACertificate` and `SSLCACertificatePath`, without requiring a certificate from the connected peer.
- The `GSSAPILibrary` configuration parameter has been added to the `[Paths]` section. You can set this parameter to the path to the GSSAPI shared library or DLL that the application uses. Depending on your system configuration, HPE IDOL Server attempts to detect the appropriate library to use. However, if you use Kerberos or GSSAPI security in your setup, HPE recommends that you set an explicit value for this parameter.

## Resolved Issues

- The `GetVersion` action could incorrectly report their operating system on Microsoft Windows 10 and Microsoft Windows Server 2016 platforms.

## License Server

### New in this Release

- License Server now supports licenses bound to a cloud virtual machine instance, by using a UUID rather than an IP or MAC address.

To obtain the required instance UUID value, refer to the available documentation for your cloud provider.

**NOTE:**

On Linux, to use a UUID-bound license, License Server must be able to access the system DMI/SMBIOS information. This usually requires root access. In this case, configure License Server to run with `setuid root`. License Server releases the extra privileges as soon as it verifies that the license key is valid for use on that server, and continues to run as the user that started the process.

- You can now configure action authorization more flexibly. The `[AuthorizationRoles]` configuration section has been added. You can add subsections to create roles, which can use a combination of existing roles (equivalent to the existing `AdminClients`, `QueryClients`, and so on), or a specific set of actions. For each role, you can specify the client IPs and hosts, SSL identities, and GSS principals to use to identify users that have particular permissions to run actions.  
If you want to use only SSL and GSS authorization, you can disable the client settings by setting the appropriate client configuration parameters to `""`. For example, `AdminClients=""` disables client authorization for administrative actions, and ensures that users must meet the SSL or GSS requirements.
- You can now set `SSLCertificate` to be a chain certificate in PEM format (consisting of the end-entity certificate, any intermediate certificates, and ending with the root CA certificate). This option allows a complete certificate to be returned to the connected peer.
- You can now set `SSLCheckCertificate` to `False` even when `SSLCACertificate` or

`SSLCertificatePath` are set. This allows the component to fill in any chain required for the `SSLCertificate` by using the certificates that you specify in `SSLCertificate` and `SSLCertificatePath`, without requiring a certificate from the connected peer.

- The `GSSAPILibrary` configuration parameter has been added to the `[Paths]` section. You can set this parameter to the path to the GSSAPI shared library or DLL that the application uses. Depending on your system configuration, HPE IDOL Server attempts to detect the appropriate library to use. However, if you use Kerberos or GSSAPI security in your setup, HPE recommends that you set an explicit value for this parameter.

## Resolved Issues

- The `GetVersion` action could incorrectly report their operating system on Microsoft Windows 10 and Microsoft Windows Server 2016 platforms.

## Media Server (Windows and Linux only)

### New in this Release

#### Media Server Core

- Media Server can send records to another Media Server for further processing. This feature (chaining) can help you to make most efficient use of your hardware. For example, you might have several Media Servers running face detection on video streamed from cameras. These Media Servers can send detected faces to a single Media Server that runs face recognition. This Media Server might have a more powerful CPU, be equipped with a graphics card, or have access to a larger face recognition database. Media Server has a new ingest engine (`Type=Receive`) to receive records, and a new output engine (`Type=Post`) to send records to another Media Server.
- GPU acceleration is now available on Windows in addition to Linux. HPE Media Server can use a graphics card (GPU) to significantly increase the speed of some tasks, including face recognition, image classification, object detection, and vehicle make recognition.
- GPU Media Server uses cuDNN to provide an average 50% improvement in performance, when you set `GPUNumParallel > 8`.
- Media Server can load OCR languages and number plate formats on startup, rather than when an analysis task begins. Pre-loading this information can increase throughput when you run many process actions that complete quickly, for example if you are processing batches of images or many individual frames that you have extracted from a video. To specify what to load, set the new configuration parameters `OCRLanguages` and `NumberPlateLocation`, in the `[PersistentData]` section of the configuration file.
- Additional macros have been added to provide properties of the media source. This means that you can output analysis results or encoded media to a file that has a similar file name to the media source. Additional date and time macros have been added.
- The action `ListEngines` has been added. This returns a list of the ingest, analysis, encoding, transform, ESP, and output engines that are included in your HPE Media Server license.

- You can now configure action authorization more flexibly. The [AuthorizationRoles] configuration section has been added. You can add subsections to create roles, which can use a combination of existing roles (equivalent to the existing AdminClients, QueryClients, and so on), or a specific set of actions. For each role, you can specify the client IPs and hosts, SSL identities, and GSS principals to use to identify users that have particular permissions to run actions.

If you want to use only SSL and GSS authorization, you can disable the client settings by setting the appropriate client configuration parameters to "". For example, AdminClients="" disables client authorization for administrative actions, and ensures that users must meet the SSL or GSS requirements.

- You can now set SSLCertificate to be a chain certificate in PEM format (consisting of the end-entity certificate, any intermediate certificates, and ending with the root CA certificate). This option allows a complete certificate to be returned to the connected peer.
- You can now set SSLCheckCertificate to False even when SSLCACertificate or SSLCACertificatePath are set. This allows the component to fill in any chain required for the SSLCertificate by using the certificates that you specify in SSLCACertificate and SSLCACertificatePath, without requiring a certificate from the connected peer.
- The GSSAPILibrary configuration parameter has been added to the [Paths] section. You can set this parameter to the path to the GSSAPI shared library or DLL that the application uses. Depending on your system configuration, HPE IDOL Server attempts to detect the appropriate library to use. However, if you use Kerberos or GSSAPI security in your setup, HPE recommends that you set an explicit value for this parameter.

## Ingest

- The MaxNumParallel parameter has been added to the LibAV ingest engine. This limits the number of threads used for decoding the source media.
- Media Server can ingest Mobotix MxPEG video (but not the audio) from a file or stream. This feature is provided by a new ingest engine (Type=MxPEG).

## Analysis

- Media Server includes a new analysis engine (Type=TextDetection) for identifying regions of images and video frames that contain text.
- OCR accuracy has improved for color images of scanned documents (when processed with OCRMode=document), for text that appears in a general scene (OCRMode=scene), and for scrolling text, such as the text in news tickers.
- Speaker identification supports iVector models, which are available in Speech Server 11.3 and later.
- Language identification supports boundary mode. In this mode, language identification seeks to determine when the language changes, and returns results for the time between these boundaries.
- The speech-to-text analysis engine can periodically poll IDOL Speech Server to determine whether a custom language model has been updated. If the language model has been updated it can restart the task (on the Speech Server) so that the updated language model is used for subsequent transcription of speech to text. This feature is most useful when you are processing a long or continuous video stream, such as a television news broadcast.
- Scene analysis algorithms have been improved and now provide better object-background separation, shadow removal, and track history.

- Scene analysis supports the configuration parameter `NumParallel`. This specifies the maximum number of CPU threads to use for scene analysis.
- The actions `MoveFace`, `MoveObject`, `MoveVehicleModel`, and `MoveImageComparisonReference` have been added. These actions move faces, objects, vehicle models, and image comparison references between databases.
- The `GetFaceImage`, `GetObjectImage`, `GetVehicleModelImage`, `GetClassImage`, and `GetImageComparisonReferenceImage` actions can return images in a specific format and at a custom size. If you are developing a front-end application you might use this feature to obtain thumbnail images instead of the original training images.
- Barcode analysis, face detection, object detection, object recognition, and OCR support the configuration parameter `RestrictToInputRegion`, so that you can analyze a region of the input image or video frame that was identified by another analysis task.
- Face recognition and object recognition can recognize faces or objects against a subset of the trained faces or objects, across one or more databases, that are identified by a metadata field with a specific value. To constrain recognition in this way, use the new configuration parameter `Metadata`.
- Clothing analysis can accept records that are produced by object detection, when the object detection task is configured to detect people with the pre-trained person detector. This allows you to locate the clothing of people who are facing away from the camera.
- The action `ListDatabases` has been added. This returns a list of the databases, classifiers, and detectors that exist in the Media Server training database.
- The action `ListNumberPlateLocations` has been added. This provides a list of supported locations for number plate recognition, with ISO-3166 codes that you can use to set the `Location` configuration parameter.
- Number plate recognition supports the following locations:
  - Georgia (`Location=GE`).
  - Pakistan (`Location=PK`).

To use number plate recognition in an unsupported location, you can set `Location=NOF` (to recognize number plates without matching detected characters to number plate formats). If you can provide sufficient training data, HPE might be able to add new locations for number plate recognition. To request new locations, contact HPE support.

- A new pre-trained object detector for detecting and counting people has been released and is available from the Big Data Download Center. The new detector, `ObjectDetector_HeadAndShoulder.dat`, differs from the existing detector because it has been trained to detect only the head and shoulder region. This is useful when the media does not include the full body or you want to detect people in a crowded area.
- The vehicle make and model recognition engine now attempts to identify the vehicle make using additional search regions if the first is not successful.

### Event Stream Processing

- The Combine ESP task can combine records from multiple tracks with records from the `Input0` input track.

### Transformation

- Media Server includes a new transformation engine (`Type=Rotate`) to rotate images. If you ingest images that are not upright, you can rotate them before analysis. You can also rotate images based

on the result of analysis, for example if OCR detects text that is upside down you can rotate the image so that the text is in the correct orientation before the image is encoded.

## Output

- The Labels configuration parameter supports all system, session, and source macros.

## User Interfaces

- User interface enhancements in the Scene Analysis training utility.
- The initial scene analysis configuration is less likely to filter out alarms, providing more data for you to use to optimize the configuration.

## Resolved Issues

- Number plate recognition accepted the location code SL for Slovenia. The correct ISO-3166 code for Slovenia is SI.
- In the scene analysis training utility, the velocity indicators in the training preview were not displayed correctly when the orientation characteristic was disabled.
- The GetVersion action could incorrectly report their operating system on Microsoft Windows 10 and Microsoft Windows Server 2016 platforms.

# Query Manipulation Server Component

## New in this Release

- QMS has been updated to return refreshed SecurityInfo tokens from the Content component. When you configure the new SecurityTokenIdleTime parameter in Community 11.4, QMS returns the refresh tokens from Content in a respondedata/autn:securityinfo element in the response for actions that accept the SecurityInfo parameter.
- In QMS synonym rules, you can now use the \$QUERYTEXT\$ template string in your CONCEPT fields to use the original query text in the synonym string. You can use this option with more flexible rules, such as rules that contain wildcard values, to incorporate the query text in the final query string. For example, if you have a synonym rule that matches Matt\*, and a user searches for Matthew or Matty, you can include their exact text in the query string, without enumerating every possible wildcard expansion in the rule.
- The SYNONYMREPLACE field has been added to synonym rules. If you add this field to a rule, it overrides the SynonymReplace action parameter for queries that match the rule. Set this field to TRUE to always replace the whole query text with the contents of the synonym CONCEPT field. For example, you can use this option in combination with the new \$QUERYTEXT\$ template string to avoid repeating the query. You can also set this field to FALSE if you never want to replace the query text.

### NOTE:

When you set SYNONYMREPLACE to TRUE, you do not have to set the KEYWORDS field.

- QMS has been updated to process the new `ValueRestriction` parameter for the `GetQueryTagValues` action.
- QMS now supports the `OutputEncoding` parameter on actions that retrieve documents from your data index. To use this option, you must configure language files in the QMS configuration file, by setting the `LanguageDirectory` parameter to the location of the language files in the `[LanguageTypes]` section. For example:

```
[LanguageTypes]  
LanguageDirectory=./langfiles
```

You can retrieve the language files from an IDOL Content component installation.

- You can now configure action authorization more flexibly. The `[AuthorizationRoles]` configuration section has been added. You can add subsections to create roles, which can use a combination of existing roles (equivalent to the existing `AdminClients`, `QueryClients`, and so on), or a specific set of actions. For each role, you can specify the client IPs and hosts, SSL identities, and GSS principals to use to identify users that have particular permissions to run actions.

If you want to use only SSL and GSS authorization, you can disable the client settings by setting the appropriate client configuration parameters to `""`. For example, `AdminClients=""` disables client authorization for administrative actions, and ensures that users must meet the SSL or GSS requirements.

- You can now set `SSLCertificate` to be a chain certificate in PEM format (consisting of the end-entity certificate, any intermediate certificates, and ending with the root CA certificate). This option allows a complete certificate to be returned to the connected peer.
- You can now set `SSLCheckCertificate` to `False` even when `SSLCACertificate` or `SSLCACertificatePath` are set. This allows the component to fill in any chain required for the `SSLCertificate` by using the certificates that you specify in `SSLCACertificate` and `SSLCACertificatePath`, without requiring a certificate from the connected peer.
- The `GSSAPILibrary` configuration parameter has been added to the `[Paths]` section. You can set this parameter to the path to the GSSAPI shared library or DLL that the application uses. Depending on your system configuration, HPE IDOL Server attempts to detect the appropriate library to use. However, if you use Kerberos or GSSAPI security in your setup, HPE recommends that you set an explicit value for this parameter.

## Resolved Issues

- QMS sometimes split the `authn:field` tags in the response to a `GetQueryTagValues` action with `FieldDependenceMultiLevel` set to `True`.
- QMS did not respect the `-configfile` command line argument when starting.
- The `GetVersion` action could incorrectly report their operating system on Microsoft Windows 10 and Microsoft Windows Server 2016 platforms.

## Statistics Server Component

### New in this Release

- You can now configure action authorization more flexibly. The [AuthorizationRoles] configuration section has been added. You can add subsections to create roles, which can use a combination of existing roles (equivalent to the existing AdminClients, QueryClients, and so on), or a specific set of actions. For each role, you can specify the client IPs and hosts, SSL identities, and GSS principals to use to identify users that have particular permissions to run actions.

If you want to use only SSL and GSS authorization, you can disable the client settings by setting the appropriate client configuration parameters to "". For example, AdminClients="" disables client authorization for administrative actions, and ensures that users must meet the SSL or GSS requirements.

- You can now set SSLCertificate to be a chain certificate in PEM format (consisting of the end-entity certificate, any intermediate certificates, and ending with the root CA certificate). This option allows a complete certificate to be returned to the connected peer.
- You can now set SSLCheckCertificate to False even when SSLCACertificate or SSLCACertificatePath are set. This allows the component to fill in any chain required for the SSLCertificate by using the certificates that you specify in SSLCACertificate and SSLCACertificatePath, without requiring a certificate from the connected peer.
- The GSSAPILibrary configuration parameter has been added to the [Paths] section. You can set this parameter to the path to the GSSAPI shared library or DLL that the application uses. Depending on your system configuration, HPE IDOL Server attempts to detect the appropriate library to use. However, if you use Kerberos or GSSAPI security in your setup, HPE recommends that you set an explicit value for this parameter.

### Resolved Issues

- The GetVersion action could incorrectly report their operating system on Microsoft Windows 10 and Microsoft Windows Server 2016 platforms.

## View Server Component

### New in this Release

- You can now configure View directly to use the Distributed Connector to retrieve documents from your source repositories. The DistributedConnectorHost and DistributedConnectorPort parameters have been added to the [Viewing] section, to specify the host and port of your Distributed Connector. These new options simplify the setup for retrieving content from your original repositories for viewing in a front end application.

- You can now configure universal viewing, which is an additional View configuration that allows the View Component to work out how to retrieve your original documents. It allows you to retrieve documents from various sources to view, without requiring you to use complex logic in your front end components to work out how to send the View request.

**NOTE:**

Universal viewing requires more internal communication between your IDOL components, which might affect performance.

When you enable universal viewing, you configure the location of your document store (a Content component or DAH) and a set of reference fields that specify how to retrieve the original documents (by using Distributed Connector, a Web URL, or from the file system). For example:

```
[UniversalViewing]
Enabled=True
DocumentStoreHost=localhost
DocumentStorePort=9900
DistributedConnectorReferenceField=AUTN_IDENTIFIER
WebURLReferenceField=DREREFERENCE
FileSystemReferenceField=ORIGINAL_LOCATION
```

For more information, refer to the *IDOL Server Administration Guide* and the *IDOL Server Reference*.

- You can now configure action authorization more flexibly. The [AuthorizationRoles] configuration section has been added. You can add subsections to create roles, which can use a combination of existing roles (equivalent to the existing AdminClients, QueryClients, and so on), or a specific set of actions. For each role, you can specify the client IPs and hosts, SSL identities, and GSS principals to use to identify users that have particular permissions to run actions.  
If you want to use only SSL and GSS authorization, you can disable the client settings by setting the appropriate client configuration parameters to "". For example, AdminClients="" disables client authorization for administrative actions, and ensures that users must meet the SSL or GSS requirements.
- You can now set SSLCertificate to be a chain certificate in PEM format (consisting of the end-entity certificate, any intermediate certificates, and ending with the root CA certificate). This option allows a complete certificate to be returned to the connected peer.
- You can now set SSLCheckCertificate to False even when SSLCACertificate or SSLCACertificatePath are set. This allows the component to fill in any chain required for the SSLCertificate by using the certificates that you specify in SSLCACertificate and SSLCACertificatePath, without requiring a certificate from the connected peer.
- The GSSAPILibrary configuration parameter has been added to the [Paths] section. You can set this parameter to the path to the GSSAPI shared library or DLL that the application uses. Depending on your system configuration, HPE IDOL Server attempts to detect the appropriate library to use. However, if you use Kerberos or GSSAPI security in your setup, HPE recommends that you set an explicit value for this parameter.

## Resolved Issues

- In some cases, View Server did not correctly unescape certain HTML entities when `StripScript` was set to **True**.
- When the size of a generated HTML file was larger than the platform-specific "long" type, the View action ACI response did not have a content element.
- The `GetVersion` action could incorrectly report their operating system on Microsoft Windows 10 and Microsoft Windows Server 2016 platforms.

## Web Connector (Windows and Linux only)

### New in this Release

- The connector supports XHTML pages.
- The connector can extract text from web pages, add the text to the `DRECONTENT` document field, and ingest metadata-only documents. Using the connector to extract text, rather than sending HTML files to CFS (KeyView), can result in better text extraction because the connector processes HTML pages using the HTML Document Object Model (DOM). To configure the connector to extract text, set the new configuration parameter `IngestAsPlainText` to `TRUE`.
- The connector can process metadata fields, extracted from a HTML page using the parameters `MetadataSelector` and `MetadataFieldName`, so that they contain only plain text. To do this, set the new configuration parameter `MetadataSelectorExtractPlainText` to `TRUE`.
- The connector now applies XSL transformations to XML documents where a relevant XSL stylesheet (`<?xml-stylesheet ... type="text/xsl" ... ?>`) is provided.
- The new configuration parameter `FailOnScriptTimeout` has been added, so that you can configure whether the connector considers having to terminate a script as an error.
- The new configuration parameters `MaxLinkChanges` and `MaxLinkChangePercentage` have been added. These specify the maximum number or proportion of the links on a page that can no longer appear, compared to the last time the page was synchronized, for the connector to delete unreachable pages that it has seen before. You can use these parameters to prevent the connector sending ingest-deletes when pages fail to load correctly (for example because a script fails to complete).
- JavaScript processing is faster and detection of script inactivity has been improved.
- The `identifiers` fetch action supports a new parameter, `FilterTypes`, which accepts a comma-separated list of the types of items to return identifiers for.
- The connector supports progress reporting for the `collect` fetch action.
- The connector supports the following Lua functions:
  - `get_log_service`, and the new class `LuaLogService`. You can use these when you want to write log messages to a custom log file (instead of the standard ACI server log files).
  - `parse_document_csv`, `parse_document_idx`, and `parse_document_xml`. These functions parse CSV, IDX, or XML files into documents and call a function on each document. `parse_document_`

`idx` and `parse_document_xml` can also parse a string or file that contains a single document and return a `LuaDocument` object.

- New functions and classes for parsing and manipulating JSON. The new functions are `parse_json`, `parse_json_array`, and `parse_json_object`. The new classes are `LuaJsonArray`, `LuaJsonObject`, and `LuaJsonValue`.
- You can now call the Lua method `insertJson` on `LuaField` objects as well as `LuaDocument` objects. You can also pass it one of the new `LuaJsonArray` or `LuaJsonObject` objects instead of a string.
- You can now configure action authorization more flexibly. The `[AuthorizationRoles]` configuration section has been added. You can add subsections to create roles, which can use a combination of existing roles (equivalent to the existing `AdminClients`, `QueryClients`, and so on), or a specific set of actions. For each role, you can specify the client IPs and hosts, SSL identities, and GSS principals to use to identify users that have particular permissions to run actions.

If you want to use only SSL and GSS authorization, you can disable the client settings by setting the appropriate client configuration parameters to `""`. For example, `AdminClients=""` disables client authorization for administrative actions, and ensures that users must meet the SSL or GSS requirements.

- You can now set `SSLCertificate` to be a chain certificate in PEM format (consisting of the end-entity certificate, any intermediate certificates, and ending with the root CA certificate). This option allows a complete certificate to be returned to the connected peer.
- You can now set `SSLCheckCertificate` to `False` even when `SSLCACertificate` or `SSLCACertificatePath` are set. This allows the component to fill in any chain required for the `SSLCertificate` by using the certificates that you specify in `SSLCACertificate` and `SSLCACertificatePath`, without requiring a certificate from the connected peer.
- The `GSSAPILibrary` configuration parameter has been added to the `[Paths]` section. You can set this parameter to the path to the GSSAPI shared library or DLL that the application uses. Depending on your system configuration, HPE IDOL Server attempts to detect the appropriate library to use. However, if you use Kerberos or GSSAPI security in your setup, HPE recommends that you set an explicit value for this parameter.

## Resolved Issues

- The `GetVersion` action could incorrectly report the operating system on Microsoft Windows 10 and Microsoft Windows Server 2016.

# 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 HPE IDOL Server 11.4.0.

## Minimum System Requirements

The following are minimum system requirements for HPE IDOL Server 11.4.0 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 HPE IDOL Server version 11.4.0, 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 HPE 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 HPE IDOL Server version 11.4.0 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 HPE IDOL software. The following table details the IDOL Server software and feature dependencies.

Component	Dependencies
Java	Windows, Solaris, Linux: JRE 8 or later
Browsers	<ul style="list-style-type: none"><li>• Internet Explorer 11</li><li>• Mozilla Firefox (latest version)</li><li>• Chrome (latest version)</li></ul>

## Supported Operating System Platforms

The following operating system platforms are available for HPE IDOL Server 11.4.0.

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

The documented platforms are the recommended and most fully tested platforms for HPE 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

- The Lua function `get_log(config, logstream)` has been deprecated. HPE recommends that you use the new function `get_log(log_type)` instead.
- The Lua function `string_uint_less` has been removed.

## File System Connector

- The Lua function `get_log(config, logstream)` has been deprecated. HPE recommends that you use the new function `get_log(log_type)` instead.
- The Lua function `string_uint_less` has been removed.

## Find

- The Find 11.4.0 installation involves an upgrade and migration of your existing data.

### CAUTION:

HPE strongly recommends that you back up the data folder in your home directory before you run the installer.

When you run the Find 11.4.0 installer in an existing installation, the installer migrates your data automatically.

- The `directAccessLink` configuration option in the `config.json` configuration file has been removed. You can now use templates and the `templates.json` configuration file to create templates to open results in a new tab.
- To use Find 11.3.1 or later, you must also upgrade the IDOL Content component to 11.3.1 or later, as well as the Distributed Action Handler and Query Manipulation Server, if you are using them.
- The *Find Installation Guide* has been discontinued. Information about how to install and set up Find is now included in the *Find Administration Guide*.

## HTTP Connector

- The Lua function `get_log(config, logstream)` has been deprecated. HPE recommends that you use the new function `get_log(log_type)` instead.

- The Lua function `string_uint_less` has been removed.

## Media Server

### Licensing Changes

- The licensing model for surveillance channels has changed. If you are using surveillance channels you must now allocate one surveillance channel for each analysis task such as face detection, number plate recognition, scene analysis, or text detection. If you are running actions that include more than one of these tasks you might need to obtain a new license and increase the value of the `SurveillanceChannels` parameter in your Media Server configuration file.
- Ingest, Encoding, Transformation, Event Processing, and Output tasks now require a video management channel license. These tasks are included in visual channels and surveillance channels, but if you are running actions that do not contain any tasks that are covered by either a surveillance or visual license, then you will need a video management channel to run these operations.

### New Database Schema

- The Media Server database schema has changed. If you are using an internal database, the schema upgrade is performed automatically when you start the new version of Media Server. If you are using an external PostgreSQL or MySQL database you must run an upgrade script, which is included in the Media Server 11.4.0 installation. For more information about upgrading the database schema, refer to the *Media Server Administration Guide*.

### API and Configuration Changes

- The response to the `GetStatus` action no longer includes information about the engines that are included in your HPE Media Server license. To retrieve this information use the new action `ListEngines`.
- The `process` action does not start if a non-existent track is used as the input for an output task. Previous versions of Media Server ignored the missing input and began processing anyway.
- The `Location` configuration parameter, for number plate recognition, now accepts a comma-separated list of values. If you specify a single location, number plate recognition now recognizes number plates for that location only and does not include neighboring locations.
- Action and configuration parameters that specify time durations now accept time-duration values. For example, you can set `GPUBatchingDuration=1s` or `SampleInterval=125ms`. Setting a number without any units specifies the value in the same units as earlier versions of Media Server, but this functionality is deprecated and HPE recommends that you specify the relevant units. This change affects the following parameters:

Actions	Action parameters
Rolling buffer actions	Duration GetPlaylist action: Offset, SegmentLength
Tasks	Configuration parameters

Ingest	StreamTimeout LibAv: MaximumDuration, OpenSourceTimeout Milestone: StartTimeout
Analysis	GPUBatchingDuration SampleInterval Keyframe analysis: ForceAfter, QuietPeriod New segmentation: MaxNoTopicDuration, MaxShortStoryDuration, MaxStoryDuration Number plate recognition: RepeatDelay Scene analysis: TimeBetweenAlarms Text segmentation: MaximumDuration
Encoding	MPEG encoder: SegmentDuration
ESP	MaxTimeInterval MinTimeInterval
Output	OutputInterval

- The following changes have been made to NumberPlateResult and NumberPlateResultAndImage records:
  - The binarizethreshold and platecenter elements have been deprecated.
  - The possible values for the platetype element now have initial capitals ("Regular" or "Square").
  - The minscore element has been removed.
  - The horiztransscore and verttransscore elements have been removed and replaced by a single element, sensitivitiy score.
- The following features have been deprecated:
  - The Bayesian and Maxvote classifier types, for image classification. HPE recommends that you use Convolutional Neural Network (CNN) classifiers instead. The default classifier type has been changed to CNN, so if you have classifiers where the classifierType training option has not been set, they will be retrained as CNN classifiers the next time you build them.
  - The configuration parameter IngestTime, for the LibAv ingest engine. HPE recommends that you use the new configuration parameter IngestDateTime instead. The new parameter accepts values in a greater number of formats.
  - The configuration parameters ANPRFormatsDirectory and ANPRWeightsDirectory. You can set the path for all static data folders by setting the configuration parameter StaticDataDirectory.
  - The configuration parameters OutputAllIntResults and PlateSizeUnit, for number plate recognition, have been deprecated. HPE recommends using the new parameters OutputAlternativeResults and CharHeightUnit, respectively.
  - The configuration parameter ImageBinarizeMethod, for OCR.
  - Speaker Identification with GMM models has been deprecated in IDOL Speech Server 11.4. As a result, the option to use Speaker Identification with GMM models has also been deprecated in IDOL Media Server. HPE recommends that you use Speaker Identification with iVector models

instead. As a result of this change, the default type of language model has changed from GMM to iVector. Unless you update your Speech Server language models, you might need to modify your Media Server speaker identification task by adding the parameter `ModelType=GMM`.

- The configuration parameter `CumulativeMode`, for language identification. HPE recommends that you use the parameter `Mode` instead.
- The action parameter `name`, available on the actions `AddStream`, `EditStream`, `GetStreamInfo`, `PreAllocateStorage`, and `RemoveStream`. HPE recommends that you use the new parameter `stream`, instead.
- The action parameters `OldName` and `NewName`, on the action `RenameStream`. HPE recommends that you use the new parameters `Stream` and `NewStream` instead.
- The following features have been removed:
  - The Color Cluster (Region) analysis engine. To perform analysis on a region, you can use the `ColorCluster` analysis engine with the configuration parameter `RestrictToInputRegion=TRUE`.
  - The Broadcast Monitoring output engine.
  - The ODBCdepreciated output engine.
  - The configuration parameter `FrameRate`, which was available for some analysis tasks. HPE recommends that you use the parameter `SampleInterval` instead.
  - The configuration parameters `KeyAtLeastSec` and `KeyAtMostSec`, from the keyframe analysis engine. You can use the parameters `ForceAfter` and `QuietPeriod` instead.
  - The configuration parameter `Perspective`, from the object recognition analysis engine.
  - The configuration parameters `Crop`, `CropBorder`, and `CropBorderUnit`, from the image encoder. HPE recommends using the `Crop` transformation engine to crop images.
  - The option `FaceAnalyze`, from the `Enable` configuration parameter.
  - The configuration parameters `FormatsFile` and `WeightsFiles`, from the number plate recognition analysis engine.
  - The configuration parameter `AstPath`, from the speaker identification analysis engine. You can use the parameter `TemplateSet` instead.
  - The deprecated elements `identifier` and `confidence` have been removed from image classification results. This information is still available in the `classification` element.
  - The "Reset Background" options, in the scene analysis training utility, because improvements in the scene analysis algorithms make scene analysis more tolerant to lighting changes.

## Web Connector

- The Lua function `get_log(config, logstream)` has been deprecated. HPE recommends that you use the new function `get_log(log_type)` instead.
- The Lua function `string_uint_less` has been removed.

## 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 11.4.0 using the IDOL 11.4.0 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.
- The following standard tasks have been deprecated:
  - SpkIdDevel
  - SpkIdDevelFinal
  - SpkIdDevelStream
  - SpkIdDevelWav
  - SpkIdEvalStream
  - SpkIdEvalWav
  - SpkIdFeature
  - SpkIdSetAdd
  - SpkIdSetDelete
  - SpkIdSetEditThresh
  - SpkIdSetInfo
  - SpkIdTmpEditThresh
  - SpkIdTmpInfo
  - SpkIdTrain
  - SpkIdTrainStream
  - SpkIdTrainWav

Use the equivalent iVector tasks instead (for example IvSpkIdDevel). These tasks are still available for existing implementations, but they might be incompatible with new functionality. The tasks might be deleted in future.

- The following standard tasks were deprecated in earlier versions of Speech Server. The documentation for these tasks has now been removed:
  - SidPackage
  - SidTrain
  - SidTrainFinal
  - StreamSidOptimize
  - StreamSidTrain

- StreamSpeakerId
- WavSidOptimize
- WavSidTrain
- WavSpeakerId

In addition, the documentation for the following associated modules, which were also deprecated, has been removed:

- sidfeature
- sidtrain
- sidoptimizer
- sidpackager
- The following action parameters were deprecated in earlier versions of Speech Server. The documentation for these parameters has now been removed:
  - ClassPrefix
  - Norm
- The following configuration parameters were deprecated in earlier versions of Speech Server. The documentation for these parameters has now been removed:
  - [sidout] module FullInfo
  - [Paths] TasksConfig
  - [Server] CustomLMDir
  - [Server] NestedStatus
  - [Server] TempDir
  - [Server] TrainedAmDir

# 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*