Hewlett Packard Enterprise

IDOL Server

Software Version: 11.5.0

Release Notes

Document Release Date: October 2017

Software Release Date: October 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

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

The following sections describe the enhancements for the components of IDOL Server version 11.5.0.

Content Component

New in this Release

- You can now select the document fields to use to generate query summaries in the query action, by using the new `SourceFields` parameter. This parameter overrides the configured `SourceType` fields.
- Improvements have been made for the `GetQueryTagValues` action when `ValueDetails` is set to **True**, and the field is an optimized numeric field (but not parametric):
  - Performance has been improved.
  - Percentiles are now populated correctly.
  - Multiple occurrences of a `NumericType` field in a document are now accounted for.
  - Standard numeric processing of the field contents is now applied (for example, a field that contains a comma-separated list of numeric values is treated as multiple numeric values, rather than a single string).
  - `NumericType` fields with a custom range applied can now use the whole value, rather than being truncated to an integer.
- When you send the `GetQueryTagValues` action with `ValueDetails` set to **True**, you can now set the new `Print` parameter to **NoResults**, to return only the `ValueDetails` response. This option significantly improves the performance for this type of action when you only want the `ValueDetails` information.
- The relevancy calculation has been improved for queries that contain hard restrictions (for example exact phrase or field restricted search).
- The `DateFormatCSVs` configuration parameter now supports the `#ISODATETIME` option, which accepts the ISO-8601 date format `YYYY-MM-DDTHH:MM:SS.FFFFZ` and some variations (such as optional times, time zones, and separators). For details, refer to the *IDOL Server Reference*.
- You can now configure GSS authentication on the ACI and service ports without using ACI encryption. In this mode, all connections to the ports must be authenticated using GSSAPI and the Negotiate HTTP authentication mechanism.

  To use GSS authentication, you must set the `GSSServiceName` parameter in the `[Server]` section to the full service name, domain, and Kerberos realm for the service. You can then set the `RequireGSSAuth` parameter in the `[Server]` section to enable GSS authentication on the ACI port, and set `RequireGSSAuth` in the `[Service]` section to enable GSS authentication on the service port.

  > **NOTE:**
  > You cannot configure `RequireGSSAuth` with the `[ACIEncryption]` configuration options. If

> you attempt to configure both, the server does not start.
>
> This method provides an authentication requirement only. HPE recommends that you use it in conjunction with TLS/SSL to encrypt the authentication data.

- All ACI server ports now support the `Expect: 100-continue` HTTP header. Previously, third-party client applications that used this header (for example, using the cURL utility with the -F option to POST form data) could experience increased latency when communicating with the ACI server.

Resolved Issues

- The `Quick` summary type could return invalid XML output when summarizing CJK documents.

  > **NOTE:**
  > Other summary modes can fall back on a `Quick` summary. This issue occurred when the text did not contain whitespace to split on. This usually applies to CJK languages, but might also apply to other languages (for example if a document contained only emoji characters).

- When the `SearchUncommittedDocuments` configuration parameter was set to `True`, the `TermGetAll` action could take a very long time to complete when the index cache was empty.
- The `KillDuplicates` `GREATER:`*`VersionField`* modifier did not work reliably in indexes that had multiple reference fields.
- The `KillDuplicates` `GREATER:`*`VersionField`* modifier did not work reliably unless the `=2` mode was used to apply `KillDuplicates` across all databases.
- The `GetQueryTagValues` action sometimes returned a `total_values` tag with the value **0** for numeric fields. It now returns the `total_values` tag for numeric fields only if there is a range specified.
- The `GetQueryTagValues` action did not return the `total_values` tag when the `FieldDependence` parameter was set. This tag now returns the number of tuples available.

  > **NOTE:**
  > The default value for `TotalValues` is now **`True`** when `FieldDependence` is **`False`**, and **`False`** when `FieldDependence` is **`True`**.

- Sending a `GetQueryTagValues`action with both `FieldDependence` and `ValueDetails` set to **`True`**, and with either no sorting or a document count-based sort, could result in the same sets of values appearing multiple times in the response.
- Sending a `GetQueryTagValues` action with `FieldDependenceMultiLevel` set to **`True`** and a document count-based sort could result in the same value appearing multiple times at the same level in the response. Each value now appears at most once at each level, sorted by their aggregated document counts.
- Using the `SOUNDEX`, `DREFUZZY`, or `SYNONYM` operators in a query with the `Synonym` parameter set to **`True`** and an Ngram-enabled language could wrongly return an error.

  > **NOTE:**
  > Synonym file expansion is now disabled inside of the `SOUNDEX`, `DREFUZZY`, and `SYNONYM` modifiers to improve the quality of query results.

- When sending a `GetContent` action with `Boolean` set to **`True`**, highlighting, and proximity operators in the links parameter, highlight tags could be incorrectly placed in fields with restricted indexing of alphanumeric terms (that is, when `IndexNumbers` is not set to **1**, or the `IndexNumbers`*N*`MaxLength` settings are used).
- The `GetQueryTagValues` action could return incorrect values for `NumericIntegerOnly` type fields with a custom range applied.
- When an authorization role defined `Actions`, `ServiceActions`, or `IndexActions`, and the authorization role `Clients` parameter contained host names, calling the `ShowPermissions` action could result in an interruption of service.

Category Component

New in this Release

- All ACI server ports now support the `Expect: 100-continue` HTTP header. Previously, third-party client applications that used this header (for example, using the cURL utility with the -F option to POST form data) could experience increased latency when communicating with the ACI server.
- You can now configure GSS authentication on the ACI and service ports without using ACI encryption. In this mode, all connections to the ports must be authenticated using GSSAPI and the Negotiate HTTP authentication mechanism.

  To use GSS authentication, you must set the `GSSServiceName` parameter in the `[Server]` section to the full service name, domain, and Kerberos realm for the service. You can then set the `RequireGSSAuth` parameter in the `[Server]` section to enable GSS authentication on the ACI port, and set `RequireGSSAuth` in the `[Service]` section to enable GSS authentication on the service port.

  > **NOTE:**
  > You cannot configure `RequireGSSAuth` with the `[ACIEncryption]` configuration options. If you attempt to configure both, the server does not start.
  >
  > This method provides an authentication requirement only. HPE recommends that you use it in conjunction with TLS/SSL to encrypt the authentication data.

Resolved Issues

- When an authorization role defined `Actions`, `ServiceActions`, or `IndexActions`, and the authorization role `Clients` parameter contained host names, calling the `ShowPermissions` action could result in an interruption of service.

Community Component

New in this Release

- The performance of the `UserReadUserListDetails` action has been improved for when thousands of users are requested.
- All ACI server ports now support the `Expect: 100-continue` HTTP header. Previously, third-party client applications that used this header (for example, using the cURL utility with the -F option to POST form data) could experience increased latency when communicating with the ACI server.
- You can now configure GSS authentication on the ACI and service ports without using ACI encryption. In this mode, all connections to the ports must be authenticated using GSSAPI and the Negotiate HTTP authentication mechanism.

  To use GSS authentication, you must set the `GSSServiceName` parameter in the `[Server]` section to the full service name, domain, and Kerberos realm for the service. You can then set the `RequireGSSAuth` parameter in the `[Server]` section to enable GSS authentication on the ACI port, and set `RequireGSSAuth` in the `[Service]` section to enable GSS authentication on the service port.

  > **NOTE:**
  > You cannot configure `RequireGSSAuth` with the `[ACIEncryption]` configuration options. If you attempt to configure both, the server does not start.
  >
  > This method provides an authentication requirement only. HPE recommends that you use it in conjunction with TLS/SSL to encrypt the authentication data.

Resolved Issues

- When a new user, agent or profile was added while a backup operation was running in another thread, Community could become unresponsive. Community now returns an error advising that the add operation cannot be run.
- When an authorization role defined `Actions`, `ServiceActions`, or `IndexActions`, and the authorization role `Clients` parameter contained host names, calling the `ShowPermissions` action could result in an interruption of service.

Connector Framework Server

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

New in this Release

- CFS can extract images from supported file formats, and ingest the images as separate documents. You might want to do this so that you can send the images to Media Server for analysis. To enable image extraction, set the new parameter `ExtractImages` to `TRUE`.
- The action `GetDocumentStatus` has been added. This accepts a document reference and returns the status of the document (such as awaiting import, awaiting indexing, or indexing complete).
- Media analysis has been improved. The Lua functions `analyze_media_in_document` and `analyze_media_in_file` can be passed the path of a configuration file to send to Media Server. They also accept a named parameter, `config_params`, that you can use to override parameters in the specified configuration file. CFS includes example Lua scripts (in `scripts/mediaserver`), example Media Server configurations (in `script_resources/mediaserver`) and example XSL templates (in `xslt/mediaserver`) for running media analysis.
- CFS has a new import task to detect the language of a document. You can use this to filter out documents where a language cannot be detected.
- CFS includes an example Lua script, `filterdodgyfiles.lua`, which demonstrates various ways to reject unwanted files.
- CFS can use third-party translation services to translate documents from one language to another. Language translation is available through an import task. The task library is not supplied with the standard CFS installation but can be obtained from technical support.
- The configuration parameters `MetadataAttribute` and `ChildMetadataAttribute` have been added to the `WkoopHtmlExtraction` task. You can use these with existing parameters for metadata extraction, to extract attribute values from the HTML and add the values to the document, or child document, metadata.
- The Eduction task supports a new parameter, `RequestTimeout`. This specifies the maximum amount of time to spend searching for matches in a single document. If the timeout is reached, Eduction stops processing and returns any results that were found. The default value of this parameter is 300 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.
- The IDOL Speech task supports the new parameters `MaximumSilencePercentage` and `MinimumAverageConfidencePercentage`. You can use these parameters to reject documents unless they meet certain thresholds. `MaximumSilencePercentage` specifies the maximum amount of silence to allow in the speech-to-text transcript. `MinimumAverageConfidencePercentage` specifies the minimum average confidence score, for speech-to-text to be considered successful.
- CFS supports a new control field, `AUTN_NO_INDEX`. Documents that have this field are not indexed. You might use this when you want to troubleshoot the ingestion process without indexing documents.
- All ACI server ports now support the `Expect: 100-continue` HTTP header. Previously, third-party client applications that used this header (for example, using the cURL utility with the -F option to POST form data) could experience increased latency when communicating with the ACI server.
- You can now configure GSS authentication on the ACI and service ports without using ACI encryption. In this mode, all connections to the ports must be authenticated using GSSAPI and the Negotiate HTTP authentication mechanism.

To use GSS authentication, you must set the `GSSServiceName` parameter in the `[Server]` section to the full service name, domain, and Kerberos realm for the service. You can then set the `RequireGSSAuth` parameter in the `[Server]` section to enable GSS authentication on the ACI port, and set `RequireGSSAuth` in the `[Service]` section to enable GSS authentication on the service port.

> **NOTE:**
> You cannot configure `RequireGSSAuth` with the `[ACIEncryption]` configuration options. If you attempt to configure both, the server does not start.
>
> This method provides an authentication requirement only. HPE recommends that you use it in conjunction with TLS/SSL to encrypt the authentication data.

Resolved Issues

- The `extract_text_from_binary_file` Lua function could fail with the error "Invalid UTF-8 sequence encountered while trying to encode UTF-32 character".
- When an authorization role defined `Actions`, `ServiceActions`, or `IndexActions`, and the authorization role `Clients` parameter contained host names, calling the `ShowPermissions` action could result in an interruption of service.

Controller

New in this Release

- The `GetServices` action now returns the GSSAPI service name of your services, if you have configured GSSAPI authentication. Controller retrieves the service names directly from the service configuration files.

  > **CAUTION:**
  > Controller stores the service names in local storage files, and in a configured remote Controller SQL database. Storing the service names changes the SQL schema from earlier versions of Controller and Coordinator. Controller 11.5.0 automatically updates the schema when it starts. The updated tables are not compatible with earlier versions of Controller and Coordinator.

- The Controller Lua functions and methods have the following changes:
  - New functions and classes have been added for manipulating and parsing JSON. The new functions are `parse_json`, `parse_json_array`, and `parse_json_object`. The new classes are `LuaJsonArray`, `LuaJsonObject`, and `LuaJsonValue`.
  - New general Lua functions have been added for manipulating and parsing IDOL documents. The new functions are `parse_document_idx`, `parse_document_xml`, and `parse_document_csv`.
  - You can now call the `insertJson` method 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.
  - The `LuaLogService` class and `get_log_service` function have been added. You can use these options to write log messages to a custom log file (instead of the standard ACI server log files).

  - The `get_config` function now uses the standard ACI server configuration file if you do not specify the `path` argument.
  - The general function `get_log(config, logstream)` has been deprecated. This function has been replaced with the new `get_log(log_type)` function.
- You can now configure GSS authentication on the ACI and service ports without using ACI encryption. In this mode, all connections to the ports must be authenticated using GSSAPI and the Negotiate HTTP authentication mechanism.

  To use GSS authentication, you must set the `GSSServiceName` parameter in the `[Server]` section to the full service name, domain, and Kerberos realm for the service. You can then set the `RequireGSSAuth` parameter in the `[Server]` section to enable GSS authentication on the ACI port, and set `RequireGSSAuth` in the `[Service]` section to enable GSS authentication on the service port.

  > **NOTE:**
  > You cannot configure `RequireGSSAuth` with the `[ACIEncryption]` configuration options. If you attempt to configure both, the server does not start.
  >
  > This method provides an authentication requirement only. HPE recommends that you use it in conjunction with TLS/SSL to encrypt the authentication data.

- All ACI server ports now support the `Expect: 100-continue` HTTP header. Previously, third-party client applications that used this header (for example, using the cURL utility with the -F option to POST form data) could experience increased latency when communicating with the ACI server.

The following feature was released in Controller 11.4.1.

- Controller now supports running in OEM-licensed environments. Coordinator, Controller, and all registered services must use the same OEM license key.

  > **NOTE:**
  > To use OEM licensing with Coordinator and Controller, you must update both components to version 11.4.1 or later. If you are using these components with IDOL Site Admin, you must also update the IDOL Site Admin application to version 11.4.1 or later.

Resolved Issues

- When the Controller configuration included a scheduled Lua task that referenced a nonexistent script, Controller could exit unexpectedly when trying to run the task.
- Controller reported the index port of the target server for scheduled index actions, rather than the ACI port.
- When an authorization role defined `Actions`, `ServiceActions`, or `IndexActions`, and the authorization role `Clients` parameter contained host names, calling the `ShowPermissions` action could result in an interruption of service.

Coordinator

New in this Release

- You can now configure GSS authentication on the ACI and service ports without using ACI encryption. In this mode, all connections to the ports must be authenticated using GSSAPI and the Negotiate HTTP authentication mechanism.

  To use GSS authentication, you must set the `GSSServiceName` parameter in the `[Server]` section to the full service name, domain, and Kerberos realm for the service. You can then set the `RequireGSSAuth` parameter in the `[Server]` section to enable GSS authentication on the ACI port, and set `RequireGSSAuth` in the `[Service]` section to enable GSS authentication on the service port.

  > **NOTE:**
  > You cannot configure `RequireGSSAuth` with the `[ACIEncryption]` configuration options. If you attempt to configure both, the server does not start.
  >
  > 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 `AddController` action to allow you to set the service name for the child Controller components.

  > **NOTE:**
  > If you use GSSAPI authentication, you cannot use SSDP to automatically detect Controllers. You must manually add the Controllers by host and port.

- The `GetControllers` action now returns the GSSAPI service name of your Controllers, if you have configured GSSAPI authentication.

  > **CAUTION:**
  > Coordinator stores the service names in local storage files, and in a configured remote Controller SQL database. Storing the service names changes the SQL schema from earlier versions of Controller and Coordinator. Coordinator 11.5.0 automatically updates the schema when it starts. The updated tables are not compatible with earlier versions of Coordinator and Controller.

- The Coordinator Lua functions and methods have the following changes:
  - New functions and classes have been added for manipulating and parsing JSON. The new functions are `parse_json`, `parse_json_array`, and `parse_json_object`. The new classes are `LuaJsonArray`, `LuaJsonObject`, and `LuaJsonValue`.
  - New general Lua functions have been added for manipulating and parsing IDOL documents. The new functions are `parse_document_idx`, `parse_document_xml`, and `parse_document_csv`.
  - You can now call the `insertJson` method 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.
  - The `LuaLogService` class and `get_log_service` function have been added. You can use these options to write log messages to a custom log file (instead of the standard ACI server log files).
  - The `get_config` function now uses the standard ACI server configuration file if you do not

specify the `path` argument.

- The general function `get_log(config, logstream)` has been deprecated. This function has been replaced with the new `get_log(log_type)` function.

- All ACI server ports now support the `Expect: 100-continue` HTTP header. Previously, third-party client applications that used this header (for example, using the cURL utility with the -F option to POST form data) could experience increased latency when communicating with the ACI server.

The following feature was released in Controller 11.4.1.

- Coordinator now supports running in OEM-licensed environments. Coordinator, Controller, and all registered services must use the same OEM license key.

> **NOTE:**
> To use OEM licensing with Coordinator and Controller, you must update both components to version 11.4.1 or later. If you are using these components with IDOL Site Admin, you must also update the IDOL Site Admin application to version 11.4.1 or later.

Resolved Issues

- When an authorization role defined `Actions`, `ServiceActions`, or `IndexActions`, and the authorization role `Clients` parameter contained host names, calling the `ShowPermissions` action could result in an interruption of service.

Distributed Action Handler

New in this Release

- When you send the `GetQueryTagValues` action through the DAH with `ValueDetails` set to **True**, you can now set the new `Print` parameter to **NoResults**, to return only the `ValueDetails` response. This option significantly improves the performance for this type of action when you only want the `ValueDetails` information.
- You can now configure GSS authentication on the ACI and service ports without using ACI encryption. In this mode, all connections to the ports must be authenticated using GSSAPI and the Negotiate HTTP authentication mechanism.

  To use GSS authentication, you must set the `GSSServiceName` parameter in the `[Server]` section to the full service name, domain, and Kerberos realm for the service. You can then set the `RequireGSSAuth` parameter in the `[Server]` section to enable GSS authentication on the ACI port, and set `RequireGSSAuth` in the `[Service]` section to enable GSS authentication on the service port.

  > **NOTE:**
  > You cannot configure `RequireGSSAuth` with the `[ACIEncryption]` configuration options. If you attempt to configure both, the server does not start.
  >
  > This method provides an authentication requirement only. HPE recommends that you use it in conjunction with TLS/SSL to encrypt the authentication data.

- DAH now supports GSSAPI authentication to connect to its child server ACI and service ports, without using ACI Encryption. To use this option, you must configure the `GSSServiceName` configuration parameter in the child server configuration section to the service name for the child component. You must also set the `ACIEncryption` configuration parameter to **False** in the child server configuration.

  > **NOTE:**
  > The `Krb5Service` parameter has been renamed to `GSSServiceName` for consistency with other components. Both versions of the parameter name work.
  >
  > When you set this parameter with `ACIEncryption` set to **False**, you must also set the child server host parameters to the fully qualified host name for the child server, which DAH uses to retrieve the GSSAPI realm. When you set `ACIEncryption` to **True** (the default), you use the `Krb5Realm` parameter to specify the realm.

- All ACI server ports now support the `Expect: 100-continue` HTTP header. Previously, third-party client applications that used this header (for example, using the cURL utility with the -F option to POST form data) could experience increased latency when communicating with the ACI server.

Resolved Issues

- The DAH would not return the `date_with_offset` attributes in the response to the `GetQueryTagValues` action when the `DateOffset` parameter had been used.
- The DAH would not return the `end_date` attribute in the response to a `GetQueryTagValues` action that queried only a single target child server with ranges.
- When processing a `GetQueryTagValues` action with both `FieldDependence` and `TotalValues` set to `True` the DAH could terminate unexpectedly.
- When a `GetQueryTagValues` action had both `FieldDependence` and `ValueDetails` set to `True`, the DAH did not sort by document count.
- When a `GetQueryTagValues` action had both `FieldDependenceMultiLevel` and `ValueDetails` set to `True`, DAH did not return `Count` attributes.
- When sorting the results of a `GetQueryTagValues` action by date or document count, there was no defined order for results that did not have valid dates, or that had equal document counts. DAH now uses alphabetical sorting as a tie-breaker.
- When a `GetQueryTagValues` action had `FieldDependence` set to `True`, DAH did not return date attributes `NumericDateType` or `autn_date` fields unless they were the first entry in the `FieldName` parameter. Additionally, if `FieldDependenceMultiLevel` was also set to `True`, the date attributes sometimes appeared at the wrong level in the nested response.
- When a `GetQueryTagValues` action had both `FieldDependenceMultiLevel` and `ValueDetails` set to `True`, DAH did not always return the date attribute for the `valueaverage` tag when the leaf field was `NumericDateType` or `autn_date`, and sometimes included the attribute for fields that were not `NumericDateType` or `autn_date`.
- The `GetQueryTagValues` action did not return the `total_values` tag when the `FieldDependence` parameter was set. This tag now returns the number of tuples available.
- When an authorization role defined `Actions`, `ServiceActions`, or `IndexActions`, and the authorization role `Clients` parameter contained host names, calling the `ShowPermissions` action could result in an interruption of service.

Distributed Index Handler

New in this Release

- The `DateFormatCSVs` configuration parameter now supports the `#ISODATETIME` option, which accepts the ISO-8601 date format `YYYY-MM-DDTHH:MM:SS.FFFFZ` and some variations (such as optional times, time zones, and separators). For details, refer to the *IDOL Server Reference*.
- You can now configure GSS authentication on the ACI and service ports without using ACI encryption. In this mode, all connections to the ports must be authenticated using GSSAPI and the Negotiate HTTP authentication mechanism.

  To use GSS authentication, you must set the `GSSServiceName` parameter in the `[Server]` section to the full service name, domain, and Kerberos realm for the service. You can then set the `RequireGSSAuth` parameter in the `[Server]` section to enable GSS authentication on the ACI port, and set `RequireGSSAuth` in the `[Service]` section to enable GSS authentication on the service port.

  > **NOTE:**
  > You cannot configure `RequireGSSAuth` with the `[ACIEncryption]` configuration options. If you attempt to configure both, the server does not start.
  >
  > This method provides an authentication requirement only. HPE recommends that you use it in conjunction with TLS/SSL to encrypt the authentication data.

- DIH now supports GSSAPI authentication to connect to its child server ACI and service ports, without using ACI Encryption. To use this option, set the `GSSServiceName` configuration parameter in the child server configuration sections to the GSSAPI service name for the child server.
- All ACI server ports now support the `Expect: 100-continue` HTTP header. Previously, third-party client applications that used this header (for example, using the cURL utility with the -F option to POST form data) could experience increased latency when communicating with the ACI server.

Resolved Issues

- When an authorization role defined `Actions`, `ServiceActions`, or `IndexActions`, and the authorization role `Clients` parameter contained host names, calling the `ShowPermissions` action could result in an interruption of service.

File System Connector CFS

New in this Release

- The configuration parameters `DirectoryFileModifiedBefore`, `DirectoryFileModifiedSince`, `DirectoryFileCreatedBefore`, and `DirectoryFileCreatedSince` now support relative dates. For

example, you can configure the connector to ingest documents for files that have been modified in the last 6 months.

- The `identifiers` fetch action returns the identifiers of all ancestors (up to the root of the repository) for the items that you request. The action accepts a new parameter, `ShowAncestors` (default `TRUE`), which specifies whether to show these identifiers.
- The `identifiers` fetch action returns status information for each item that represents a document - for example whether the item has been ingested or the number of times that the item has been modified. The action accepts a new parameter, `ShowDocStatus` (default `FALSE`), which specifies whether to show this information.
- The `View` action returns document metadata. To obtain the metadata set the action parameter `NoACI=FALSE`, because by default the `View` action returns the binary content of the file.
- The connector provides additional statistics about the work it has completed, for example the number and frequency of ingest-adds, ingest-updates, and ingest-deletes. You can view these statistics through the `GetStatistics` service action. The connector also includes an XSL template that you can use to transform the output of the `GetStatistics` action and visualize the statistics.
- The `LogTypeCSVs` configuration parameter supports additional options for customizing logging. You can now create a separate log file for a fetch task or fetch action.
- The connector adds the field `AUTN_MODIFICATIONS` to ingested documents. This field provides information about how many times an item has been modified.
- All ACI server ports now support the `Expect: 100-continue` HTTP header. Previously, third-party client applications that used this header (for example, using the cURL utility with the -F option to POST form data) could experience increased latency when communicating with IDOL Server.

Resolved Issues

- When an authorization role defined `Actions`, `ServiceActions`, or `IndexActions`, and the authorization role `Clients` parameter contained host names, calling the `ShowPermissions` action could result in an interruption of service.

Find

New in this Release

- You can now add geographic map filters (circles or polygons) to limit results to an area or exclude results from an area. Exclusion takes priority over inclusion. You can create separate filters for each geographic field pair, which are defined in the existing `map.locationFields` option in the Find configuration file (`config.json`).
- The preview and document detail views now support hash fragments in references so that the view automatically jumps to the correct location in a document.
- The trending visualizer now uses short month names to fit more labels in.
- You can now set initial search text in a URL for users with the FindBI role. For example:

  ```
  http://localhost:8082/public/search/query/my%20initial%20query%20text
  ```

- In the dashboard configuration file, you can now add the `cssClass` property in the widget definition to define a CSS class for the widget.
- The template configuration now has a `getFieldValues` helper to print multiple field values of a field.

Resolved Issues

- The Find user interface could provide an error UUID for errors that did not appear in the log files.
- The Find session cookie used the generic name `JSESSIONID`, which could result in sessions IDs being overwritten when multiple applications were run from the same domain. the Find session cookie is now called `FINDSESSIONID`.

  > **NOTE:**
  > If you want to run multiple Find instances from the same domain, you can override the session cookie ID by adding the following argument to the Java run command:
  >
  > `-Dorg.apache.catalina.SESSION_COOKIE_NAME=MYNEWSESSIONNAME`
  >
  > This option allows you to keep the session details separate for your Find instances.

- In some cases, the Export to CSV dialogue box failed to open.
- In some cases, Find used an incorrect character encoding for exported CSV files.
- Location tagging for results did not work in the expanded document preview.
- In Trending view and the Date widgets, the text date selector sometimes overlapped the calendar icon.
- Differences between Windows and Linux line endings in SQL files could cause checksum mismatches when the same database was used by applications on multiple platforms. The SQL files now always use Linux line endings.

  > **NOTE:**
  > If you have previously built Find from source on Windows platforms, and never used the Linux version, you must perform an additional migration step before you rebuild Find from the latest version. Modify the file `com/hp/autonomy/frontend/find/idol/beanconfiguration/FlywayIdolConfigUpdateHandler.java` to add the `flyway.repair()` call before `flyway.migrate`. For example:
  >
  > ```
  > // Fix checksums
  > flyway.repair();
  > flyway.migrate();
  > ```

HTTP Connector CFS (Solaris only)

New in this Release

- The connector provides additional statistics about the work it has completed, for example the number and frequency of ingest-adds, ingest-updates, and ingest-deletes. You can view these

statistics through the GetStatistics service action. The connector also includes an XSL template that you can use to transform the output of the GetStatistics action and visualize the statistics.

- The LogTypeCSVs configuration parameter supports additional options for customizing logging. You can now create a separate log file for a fetch task or fetch action.
- All ACI server ports now support the Expect: 100-continue HTTP header. Previously, third-party client applications that used this header (for example, using the cURL utility with the -F option to POST form data) could experience increased latency when communicating with IDOL Server.

Resolved Issues

- When an authorization role defined Actions, ServiceActions, or IndexActions, and the authorization role Clients parameter contained host names, calling the ShowPermissions action could result in an interruption of service.

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

- All ACI server ports now support the Expect: 100-continue HTTP header. Previously, third-party client applications that used this header (for example, using the cURL utility with the -F option to POST form data) could experience increased latency when communicating with the ACI server.

Resolved Issues

- When an authorization role defined Actions, ServiceActions, or IndexActions, and the authorization role Clients parameter contained host names, calling the ShowPermissions action could result in an interruption of service.

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

- You can now manually delete alert messages that relate to a Controller that you deregistered from IDOL Site Admin. By default, IDOL Site admin keeps these alerts so that it can resume tracking if you re-register the Controller.
- In OEM Encryption mode, you can now configure IDOL Site Admin by using the settings page.

The following feature was added in IDOL Site Admin version 11.4.1.

- You can now use IDOL Site Admin in an OEM-licensed environment. To use this option, you must set the `-Dhp.idolsiteadmin.oemEncryptionKey` system property to the OEM encryption key string to use for communication with the IDOL Community component and Coordinator component. For more information, refer to the *IDOL Site Admin Installation Guide*.

  > **NOTE:**
  > To use OEM encryption in your IDOL Site Admin system, you must also upgrade the Controller and Coordinator components to version 11.4.1 or later.

Resolved Issues

- IDOL Site Admin sometimes returned primary key violation errors when attempting to register Controllers or services.
- The audit log (`siteadmin.log`) did not include information about user login , and did not show user names for audited actions.
- The IDOL Site Admin scheduler was not able to create or run a `DREBACKUP` index action with certain parameters.
- It was not possible to modify an existing index action schedule. To resolve this issue, you must also update the Controller component to 11.5.0 or later.
- When attempting to run a Lua script on a particular Controller component, IDOL Site Admin sometimes ran the Lua script in all Controllers.
- The IDOL Site Admin scheduler page list did not wrap long strings correctly, so that the columns stretched outside the screen size.

The following issue was resolved in IDOL Site Admin version 11.4.1.

- In some cases, IDOL Site Admin could fail to persist group changes after the application was restarted.

IDOL Speech Server

New in this Release

- New improved Neural Network technology is now used for Speech-to-text. You can use Speech Server version 11.5.0 with the new 9.0+ Language Packs to improve results accuracy. In addition,

the new technology is typically faster than older server and language pack combinations.

- Speech Server speech to text tasks now generate word confidence values by default. The `stt` module `EnableConfidence` configuration parameter now has a default value of **True**.
- Language identification and Speaker identification tasks now normalize confidence scores to a value between 0.0 and 1.0 by default. You can modify this behavior by changing the `ScoreMode` parameter in the `ivscore` or `langid` module configuration to display the raw scores instead. This parameter is also available as a parameter for the `LangId` and `IvSpkId` standard tasks.
- The Speech Server standard tasks have been simplified so that you can use the same task for audio file and stream processing, with an `InputType` parameter to specify the correct input type (**file**, **data**, or **stream**). In addition, other task sets have been simplified. For all language identification tasks, you can now use the `LangId` task, with the `LidMode` parameter set to provide segmented, cumulative, or boundary mode identification.

  As part of this change, existing tasks have been deprecated and replaced with the new equivalents.

  The following table lists the deprecated tasks, and the new task to use instead.

Old Task (Deprecated)	New Task
`WavToText`	`SpeechToText` (with `InputType=File`)
`StreamToText`	`SpeechToText` (with `InputType=Stream`)
`StreamToTextMusicFilter`	`SpeechToTextFilter`
`TelWavToText`	`SpeechToTextTelephony`
`ivSpkIdTrainWav`	`ivSpkIdTrainAudio` (with `InputType=File`)
`ivSpkIdTrainStream`	`ivSpkIdTrainAudio` (with `InputType=Stream`)
`ivSpkIdDevelWav`	`ivSpkIdDevelAudio` (with `InputType=File`)
`ivSpkIdDevelStream`	`ivSpkIdDevelAudio` (with `InputType=Stream`)
`ivSpkIdEvalWav`	`ivSpkId` (with `InputType=File`)
`ivSpkIdEvalStream`	`ivSpkId` (with `InputType=Stream`)
`ivSpkIdSetInfo`	`ivSpkIdInfo` (with `TemplateSet`)
`ivSpkIdTmpInfo`	`ivSpkIdInfo` (with `TemplateFile`)
`ivSpkIdSetEditThresh`	`ivSpkIdEditThresh` (with `TemplateSet` and `TemplateName`)
`ivSpkIdTmpEditThresh`	`ivSpkIdEditThresh` (with `TemplateFile`)
`LangIdSegLif`	Language identification on feature files is deprecated. Use `LangId`.
`LangIdCumLif`	Language identification on feature files is deprecated. Use `LangId`.
`LangIdBndLif`	Language identification on feature files is deprecated. Use `LangId`.
`LangIdSegWav`	`LangId` (with `InputType=File` and `LidMode=Segmented`)

LangIdCumWav	LangId (with InputType=File and LidMode=Cumulative)
LangIdBndWav	LangId (with InputType=File and LidMode=Boundary)
LangIdSegStream	LangId (with InputType=Stream and LidMode=Segmented)
LangIdCumStream	LangId (with InputType=Stream and LidMode=Cumulative)
LangIdBndStream	LangId (with InputType=Stream and LidMode=Boundary)
afpAddTrackWav	afpAddTrack (with InputType=File and afpMode=standard)
afpAddTrackStream	afpAddTrack (with InputType=Stream and afpMode=standard)
afpMatchWav	afpMatch (with InputType=File and afpMode=standard)
afpMatchStream	afpMatch (with InputType=Stream and afpMode=standard)
afptAddTrackWav	afpAddTrack (with InputType=File and afpMode=robust)
afptAddTrackStream	afpAddTrack (with InputType=File and afpMode=robust)
afptMatchWav	afpMatch (with InputType=File and afpMode=robust)
afptMatchStream	afpMatch (with InputType=Stream and afpMode=robust)
afptRemoveTrack	afpRemoveTrack (with afpMode=robust)
afptDatabaseInfo	afpDatabaseInfo (with afpMode=robust)
wavPhraseSearch	PhraseSearch
wavToFmd	createFmd

- The new audio module has been added, which allows you to process audio files, binary data, or streams in the same module. This module replaces the wav and stream modules, which are now deprecated.

  This module accepts the same parameters as the old wav module, and also a new InputType parameter, which defines what type of input to process.

  The following tasks use the new module. As such, you can use these tasks for audio files or streams.

afpMatch	createFmd	phraseSearch
afpAddTrack	dialToneIdentification	SNRCalculation
audioAnalysis	ivSpkId	speechSilClassification
audioSecurity	ivSpkIdFeature	speechToText
clippingDetection	ivSpkIdTrainAudio	speechToTextFilter
clusterSpeech	ivSpkIdDevelAudio	speechToTextTelephony

clusterSpeechTel	langId	
clusterSpeechToTextTel	langIdFeature	

In addition, these tasks now also accept the StartTime and EndTime parameter to choose a point to start and end in an audio file or stream.

- The new SpeechToTextTelephony task now applies music and noise filtering to the transcript, in addition to dial-tone and DTMF detection.
- The fptdb resource has been deprecated. You can now use the fpdb resource for template audio fingerprinting, as well as standard.
- The SegmentWav task has been deprecated. You can use the ClusterSpeech task to perform a similar operation.
- Acoustic modeling is now deprecated, in favor of the newer Deep Neural Network (DNN) approaches. The following tasks have been deprecated:
  - WavToPlh
  - AmTrain
  - AmTrainFinal
  - DataObfuscation

  The following related modules are also deprecated:
  - amadapatadddata
  - amadaptend

  In addition, the TrainedAm task parameter and TrainedAmDir configuration parameter are now deprecated.
- The lbout module has been deprecated. Information about language boundaries is provided in the output from the lidout module. Speech Server language identification boundary mode no longer produces a separate boundary output file.
- The audio fingerprinting tasks have a new OutputNonResults parameter to allow you to output periodic non-results options in periods where no matches are detected. This option provides feedback on the progress of the matching process.
- You can now force Speech Server to unload a language pack immediately by setting the new Force parameter to **True** in the UnloadLanguage action.
- A new base language identification pack and classifier set has been added for broadband language identification, taking advantage of new neural network technology.

  > **NOTE:**
  > If you use user-trained language classifiers, HPE recommends that you retrain your classifiers with the new base pack. If you do not retrain the classifiers, performance might be adversely affected.

- You can now configure GSS authentication on the ACI and service ports without using ACI encryption. In this mode, all connections to the ports must be authenticated using GSSAPI and the Negotiate HTTP authentication mechanism.

  To use GSS authentication, you must set the GSSServiceName parameter in the [Server] section to the full service name, domain, and Kerberos realm for the service. You can then set the

RequireGSSAuth parameter in the [Server] section to enable GSS authentication on the ACI port, and set RequireGSSAuth in the [Service] section to enable GSS authentication on the service port.

> **NOTE:**
> You cannot configure RequireGSSAuth with the [ACIEncryption] configuration options. If you attempt to configure both, the server does not start.
>
> This method provides an authentication requirement only. HPE recommends that you use it in conjunction with TLS/SSL to encrypt the authentication data.

- All ACI server ports now support the Expect: 100-continue HTTP header. Previously, third-party client applications that used this header (for example, using the cURL utility with the -F option to POST form data) could experience increased latency when communicating with the ACI server.

Resolved Issues

- In some cases, it was not possible to retrieve results from Speaker ID and Language ID tasks by using the GetResults action when the returned labels (speaker or language names) contained spaces.

  > **NOTE:**
  > Speech Server now writes any labels that contain spaces into the CTM results file using the   HTML identifier to replace the space. The space is restored when you use GetResults to view the results.

- The task progress time that was reported by GetStatus (in the ProcessingEnd value) could occasionally regress.
- Speech Server could send warnings when using an audio fingerprinting database that had previously had tracks removed.
- Speech Server could sometimes exit unexpectedly while running DTMF or dial tone identification.
- The TaskHelp action could log spurious errors.
- When an authorization role defined Actions, ServiceActions, or IndexActions, and the authorization role Clients parameter contained host names, calling the ShowPermissions action could result in an interruption of service.

Knowledge Graph Component

New in this Release

- All ACI server ports now support the Expect: 100-continue HTTP header. Previously, third-party client applications that used this header (for example, using the cURL utility with the -F option to POST form data) could experience increased latency when communicating with the ACI server.
- You can now configure GSS authentication on the ACI and service ports without using ACI encryption. In this mode, all connections to the ports must be authenticated using GSSAPI and the Negotiate HTTP authentication mechanism.

To use GSS authentication, you must set the `GSSServiceName` parameter in the `[Server]` section to the full service name, domain, and Kerberos realm for the service. You can then set the `RequireGSSAuth` parameter in the `[Server]` section to enable GSS authentication on the ACI port, and set `RequireGSSAuth` in the `[Service]` section to enable GSS authentication on the service port.

> **NOTE:**
> You cannot configure `RequireGSSAuth` with the `[ACIEncryption]` configuration options. If you attempt to configure both, the server does not start.
>
> This method provides an authentication requirement only. HPE recommends that you use it in conjunction with TLS/SSL to encrypt the authentication data.

Resolved Issues

- When an authorization role defined `Actions`, `ServiceActions`, or `IndexActions`, and the authorization role `Clients` parameter contained host names, calling the `ShowPermissions` action could result in an interruption of service.

License Server

New in this Release

- All ACI server ports now support the `Expect: 100-continue` HTTP header. Previously, third-party client applications that used this header (for example, using the cURL utility with the -F option to POST form data) could experience increased latency when communicating with the ACI server.
- You can now configure GSS authentication on the ACI and service ports without using ACI encryption. In this mode, all connections to the ports must be authenticated using GSSAPI and the Negotiate HTTP authentication mechanism.

  To use GSS authentication, you must set the `GSSServiceName` parameter in the `[Server]` section to the full service name, domain, and Kerberos realm for the service. You can then set the `RequireGSSAuth` parameter in the `[Server]` section to enable GSS authentication on the ACI port, and set `RequireGSSAuth` in the `[Service]` section to enable GSS authentication on the service port.

  > **NOTE:**
  > You cannot configure `RequireGSSAuth` with the `[ACIEncryption]` configuration options. If you attempt to configure both, the server does not start.
  >
  > This method provides an authentication requirement only. HPE recommends that you use it in conjunction with TLS/SSL to encrypt the authentication data.

Resolved Issues

- When an authorization role defined `Actions`, `ServiceActions`, or `IndexActions`, and the authorization role `Clients` parameter contained host names, calling the `ShowPermissions` action could result in an interruption of service.

Media Server (Windows and Linux only)

New in this Release

Media Server Core

- GPU acceleration is now available for GeForce GTX graphics cards with CUDA compute capability 3.0 to 5.2.
- Media Server supports a new method of chaining (sending records to another Media Server for further processing). With the new method, called *feedback chaining*, the downstream Media Server returns the results of analysis to the upstream Media Server and output tasks occur on the upstream server. The downstream Media Server performs analysis on records independently, which has implications for licensing and the number of requests that can be handled simultaneously. For more information about the differences between one-way chaining and feedback chaining, refer to the *Media Server Administration Guide*. To support this new feature, Media Server has a new analysis engine (`Type=RemoteAnalysis`).
- Media Server supports OEM licensing.
- Media Server has been validated in cloud environments such as Amazon Web Services, Microsoft Azure, and Google Cloud.
- The action `ValidateProcessConfig` has been added. This validates a task configuration without starting processing.
- Media Server has a new action, `GetExampleRecord`, which returns an example record for a specified output track of a specified analysis engine.
- Media Server provides a new Lua function, `log(message)`, so that you can write log messages from Lua scripts. The messages are written to a new log type (`LogTypeCSVs=Lua`).
- The configuration parameter `CompressionQuality`, for the image encoder and image format transformation engines, is now supported for images in PDF format. You can specify a quality level from 0 to 100, or "lossless".
- In the Lua representation of a record you can access data by type. For example, `record.FaceRecognitionResult.identity.identifier` can be simplified to `record.IdentityData.identifier`, in the same way as for macros.
- All ACI server ports now support the `Expect: 100-continue` HTTP header. Previously, third-party client applications that used this header (for example, using the cURL utility with the -F option to POST form data) could experience increased latency when communicating with the ACI server.
- You can now configure GSS authentication on the ACI and service ports without using ACI encryption. In this mode, all connections to the ports must be authenticated using GSSAPI and the Negotiate HTTP authentication mechanism.

  To use GSS authentication, you must set the `GSSServiceName` parameter in the `[Server]` section to the full service name, domain, and Kerberos realm for the service. You can then set the `RequireGSSAuth` parameter in the `[Server]` section to enable GSS authentication on the ACI port, and set `RequireGSSAuth` in the `[Service]` section to enable GSS authentication on the service port.

> **NOTE:**
> You cannot configure `RequireGSSAuth` with the `[ACIEncryption]` configuration options. If you attempt to configure both, the server does not start.
>
> This method provides an authentication requirement only. HPE recommends that you use it in conjunction with TLS/SSL to encrypt the authentication data.

Ingest

- The image ingest engine extracts significantly more metadata from TIFF files.
- Media Server (on Windows platforms only) can ingest video from Genetec Security Center. This feature is provided by a new ingest engine (`Type=GenetecIngest`).
- Media Server supports a new action, `DescribeMedia`, which returns information about a media file or stream, estimates the ability of Media Server to ingest it, and recommends which ingest engine to use.
- 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`).
- Media Server includes a new ingest engine (`Type=Wittwin`) to ingest video from Wittwin and read Wittwin timestamps.

Analysis

- Face recognition has been improved, for example Media Server now has greater tolerance for uneven illumination and rotated faces. As a result of these improvements, you must retrain Media Server to recognize faces by running the action `BuildAllFaces`.
- The accuracy of optical character recognition (OCR) has been improved for poor-quality images of scanned documents.
- OCR can process multiple pages of a multi-page image or document at the same time. Providing that your server has sufficient CPU cores, this feature can decrease the amount of time required to perform OCR. To specify the number of pages to process concurrently, use the configuration parameter `NumParallel`.
- Object recognition supports a new algorithm for detecting 2-D objects (`Geometry=AFF2`). HPE recommends that you use this mode when the objects are expected to be small compared to the distance from the camera (so the objects take up a small part of the image, or the camera has a long focal length).
- Number plate recognition accepts a new parameter, `LocationWithPriorities`. You can set this instead of `Location`, in cases where you want to specify priorities for each location. For example, `LocationWithPriorities=fr:1.0,de:0.1,be:0.05` recognizes French, German, and Belgian number plates, but instructs Media Server that German number plates are ten times less likely to be seen than French plates, and Belgian number plates are twenty times less likely to be seen than French plates.
- Image comparison supports 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.
- Scene analysis can generate alarms based on the path an object has taken through the scene. You can define one or more tripwires that an object must cross in order to cause an alarm.
- Number plate recognition can read personalized number plates for New Zealand (`Location=NZ-PP`).

Encoding

- Media Server can encode and stream video in MJPEG format. This feature is provided by a new encoding engine (`Type=MJPEG`).
- The image encoder can create multi-page TIFF and PDF files by appending images to an output file instead of overwriting it. To do this, set the new configuration parameter `Append` to `TRUE`.

Event Stream Processing

- ESP tasks can accept the same track for two inputs. In previous versions of Media Server, this resulted in an error. Using the same track for two inputs can be useful in some cases, such as with the `AndNot` engine, to filter the records in a track based on properties of other records in the same track. For example, you can exclude records if there is a record with greater confidence within a specified time interval.

Output

- Media Server includes a new output engine (`Type=GenetecOutput`), to send events to a Genetec Security Center.
- Media Server includes a new output engine (`Type=Lua`), which produces a Lua representation of each record and writes the representations to disk. This engine is intended to help you write and troubleshoot Lua scripts.

User Interfaces

- The scene analysis training utility can display the position of regions of interest when you review alarms or existing alarm classifications.
- When reviewing alarms in the scene analysis training utility, you can choose to sort the alarms by object size or by the time the alarms occurred.
- The scene analysis training utility no longer requires a category to have false alarms in its region of interest for the category to be optimized.
- Previous versions of scene analysis could filter alarms by time of day but you can now choose to apply the time filters only on weekdays or weekends.
- When reviewing alarms in the scene analysis training utility, you can choose to always show the alarm details.
- In the scene analysis training utility, you can now review alarms that you have classified and modify the classifications.
- In the scene analysis training utility, you can change the shape of a region of interest without having to draw a new region.
- When you optimize a category in the scene analysis training utility, you can choose whether to use the Min Time in Scene and Min Time in ROI alarm filters for reducing the number of false and missed alarms (in some cases you might have set these filters and might not want to change the values).

Resolved Issues

This section lists the resolved issues in Media Server version 11.5.0.

- The scene analysis training utility did not permit some valid values to be entered for the maximum object size in the category details.
- An issue with the OpenBLAS library could cause Media Server to terminate unexpectedly when using convolutional neural networks.

  To run tasks that use convolutional neural networks on a machine that has a processor from the AMD Bulldozer series, download the latest version of `libopenblas_AMD_Bulldozer.dll` from the Big Data Download Center, and rename it such that it replaces the file `libopenblas.dll` that is included in the Media Server installation.

The following issues were resolved in Media Server version 11.4.1:

- Media Server did not provide any warning when scene analysis was configured to read traffic lights but the positions of the lights were not defined. The task would start but no alarms would ever be generated.
- In scene analysis, user-generated alarms that were classified as false alarms were lost and could not be used to optimize the configuration.
- The scene analysis training utility did not correctly track modifications to a configuration. In some cases there was no prompt to save the configuration after changes had been made.
- When an authorization role defined `Actions`, `ServiceActions`, or `IndexActions`, and the authorization role `Clients` parameter contained host names, calling the `ShowPermissions` action could result in an interruption of service.

Query Manipulation Server Component

New in this Release

- You can now configure QMS to use GSS authentication to communicate with its child components. The `GSSServiceName` parameter has been added to the `[Community]`, `[IDOL]` and `[PromotionAgentstore]` configuration sections. Set these parameters to the GSSAPI service name of the child component. You must also set the associated `Host` parameter to the fully qualified domain name for the child component server, which QMS uses to retrieve the realm. QMS then uses GSSAPI authentication to connect to those child services.
- Lua scripts that you call in QMS can now use IDOL standard Lua methods and functions. These functions are available in Request Cooker and Type Ahead Lua scripts. For more information about the method and functions available, see the *QMS Reference*.
- The `TypeAhead` action has the new **Answerbank** mode, which retrieves suggestion values from an Answer Server Answer Bank system. This option allows you to use reference questions from the Answer Bank as query suggestions, directing users towards existing answers. To use this option, you must configure the `[AnswerServer]` configuration section, with the Host and Port of your Answer Server. You must also set the `AnswerBankSystem` parameter in your `[TypeAhead]` configuration section to the name of the Answer Bank system that you want to use.
- The URL-decoding function in the `autn_aci.lua` script (provided with QMS) now changes plus (+) characters into spaces.
- All ACI server ports now support the `Expect: 100-continue` HTTP header. Previously, third-party client applications that used this header (for example, using the cURL utility with the -F option to

POST form data) could experience increased latency when communicating with the ACI server.

- You can now configure GSS authentication on the ACI and service ports without using ACI encryption. In this mode, all connections to the ports must be authenticated using GSSAPI and the Negotiate HTTP authentication mechanism.

  To use GSS authentication, you must set the `GSSServiceName` parameter in the `[Server]` section to the full service name, domain, and Kerberos realm for the service. You can then set the `RequireGSSAuth` parameter in the `[Server]` section to enable GSS authentication on the ACI port, and set `RequireGSSAuth` in the `[Service]` section to enable GSS authentication on the service port.

  > **NOTE:**
  > You cannot configure `RequireGSSAuth` with the `[ACIEncryption]` configuration options. If you attempt to configure both, the server does not start.
  >
  > This method provides an authentication requirement only. HPE recommends that you use it in conjunction with TLS/SSL to encrypt the authentication data.

Resolved Issues

- QMS did not return responsive unindexed promotion documents in a promotions query if the other responsive static and dynamic promotions did not retrieve any documents from the Content data index.
- When an authorization role defined `Actions`, `ServiceActions`, or `IndexActions`, and the authorization role `Clients` parameter contained host names, calling the `ShowPermissions` action could result in an interruption of service.

Statistics Server Component

New in this Release

- All ACI server ports now support the `Expect: 100-continue` HTTP header. Previously, third-party client applications that used this header (for example, using the cURL utility with the -F option to POST form data) could experience increased latency when communicating with the ACI server.
- You can now configure GSS authentication on the ACI and service ports without using ACI encryption. In this mode, all connections to the ports must be authenticated using GSSAPI and the Negotiate HTTP authentication mechanism.

  To use GSS authentication, you must set the `GSSServiceName` parameter in the `[Server]` section to the full service name, domain, and Kerberos realm for the service. You can then set the `RequireGSSAuth` parameter in the `[Server]` section to enable GSS authentication on the ACI port, and set `RequireGSSAuth` in the `[Service]` section to enable GSS authentication on the service port.

  > **NOTE:**
  > You cannot configure `RequireGSSAuth` with the `[ACIEncryption]` configuration options. If you attempt to configure both, the server does not start.

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

Resolved Issues

- When an authorization role defined `Actions`, `ServiceActions`, or `IndexActions`, and the authorization role `Clients` parameter contained host names, calling the `ShowPermissions` action could result in an interruption of service.

View Server Component

New in this Release

- All ACI server ports now support the `Expect: 100-continue` HTTP header. Previously, third-party client applications that used this header (for example, using the cURL utility with the -F option to POST form data) could experience increased latency when communicating with the ACI server.
- You can now configure GSS authentication on the ACI and service ports without using ACI encryption. In this mode, all connections to the ports must be authenticated using GSSAPI and the Negotiate HTTP authentication mechanism.

  To use GSS authentication, you must set the `GSSServiceName` parameter in the `[Server]` section to the full service name, domain, and Kerberos realm for the service. You can then set the `RequireGSSAuth` parameter in the `[Server]` section to enable GSS authentication on the ACI port, and set `RequireGSSAuth` in the `[Service]` section to enable GSS authentication on the service port.

  > **NOTE:**
  > You cannot configure `RequireGSSAuth` with the `[ACIEncryption]` configuration options. If you attempt to configure both, the server does not start.
  >
  > This method provides an authentication requirement only. HPE recommends that you use it in conjunction with TLS/SSL to encrypt the authentication data.

Resolved Issues

- View Server could return an invalid JSON response when asked to view a large document and to return as JSON.
- View server did not correctly handle security strings in universal viewing mode when making calls to a Distributed Connector.
- When an authorization role defined `Actions`, `ServiceActions`, or `IndexActions`, and the authorization role `Clients` parameter contained host names, calling the `ShowPermissions` action could result in an interruption of service.

Web Connector (Windows and Linux only)

New in this Release

- The connector can ingest information by retrieving a list of URLs from a text file. You might want to specify a list of pages when you have an external process generating the URLs. To configure this, use the new configuration parameter `SitemapFile`.
- The connector supports login forms where submitting the form results in an AJAX request rather than a page load.
- The configuration parameter `DeleteOnServerError` has been added. This specifies whether to delete pages from IDOL when the web server returns an HTTP 500 (internal server error) response code. The default value is `false`.
- The configuration parameters `MetadataAttribute` and `ChildMetadataAttribute` have been added. You can use these with existing parameters for metadata extraction, to extract attribute values from the HTML and add the values to the document, or child document, metadata.
- The connector handles `<meta http-equiv="refresh"...>` instructions contained with the `<head>` section of a page. The connector proceeds as if it has received an HTTP response redirecting it to another URL.
- The connector can rank pages by importance, based on their depth, the number links from other pages, and the amount of time since they were last modified. The connector adds the rank to a document field named `AUTN_RANK`. To rank pages, set the new configuration parameter `RankPages` to `TRUE`.
- If the connector synchronizes some items but the task stops or encounters an error, the next synchronize cycle starts from that point and does not process the same items again. You can configure this behavior with the new configuration parameter `SynchronizeAllowResume`.
- The connector provides additional statistics about the work it has completed, for example the number and frequency of ingest-adds, ingest-updates, and ingest-deletes. You can view these statistics through the `GetStatistics` service action. The connector also includes an XSL template that you can use to transform the output of the `GetStatistics` action and visualize the statistics.
- The `LogTypeCSVs` configuration parameter supports additional options for customizing logging. You can now create a separate log file for a fetch task or fetch action.
- The connector adds the field `AUTN_MODIFICATIONS` to ingested documents. This field provides information about how many times an item has been modified.
- All ACI server ports now support the `Expect: 100-continue` HTTP header. Previously, third-party client applications that used this header (for example, using the cURL utility with the -F option to POST form data) could experience increased latency when communicating with IDOL Server.

Resolved Issues

- When an authorization role defined `Actions`, `ServiceActions`, or `IndexActions`, and the authorization role `Clients` parameter contained host names, calling the `ShowPermissions` action could result in an interruption of service.

Upgrade Information

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

Upgrade to IDOL 11.x

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

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

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

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

Upgrade Document Tracking

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

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

Requirements

This section describes the system requirements, supported platforms, and software dependencies for IDOL Server 11.5.0.

Minimum System Requirements

The following are minimum system requirements for IDOL Server 11.5.0 on any supported operating system platform:

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

To run IDOL Server version 11.5.0, 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 IDOL Server installer and component stand-alone zip packages provide these libraries in the `libgcc_s` and `libstdc++` shared libraries.
>
> If you start components from the command line (rather than using the init script), you might need to set the `LD_LIBRARY_PATH` to include the *`InstallDir`*`/common` and *`InstallDir`*`/common/runtimes` directories, to ensure that the component can access the installed shared libraries.
>
> You can also copy the shared libraries to the component working directory.

To run IDOL Server version 11.5.0 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	• Internet Explorer 11 • Mozilla Firefox (latest version) • Chrome (latest version)

Supported Operating System Platforms

The following operating system platforms are available for IDOL Server 11.5.0.

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

The documented platforms are the recommended and most fully tested platforms for 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.
- The following configuration parameters for setting server action authorization by client IP address have been deprecated:
  - `[Server] AdminClients`
  - `[Server] IndexClients`
  - `[Server] QueryClients` or `UserClients`
  - `[Service] ServiceControlClients`
  - `[Service] ServiceStatusClients`

  You can now use the `[AuthorizationRoles]` configuration section to set up authorization for your servers more flexibly. These configuration parameters are still available for existing implementations, but they might be incompatible with new functionality. The parameters might be deleted in future.

Connector Framework Server

- To reflect changes in IDOL Speech Server, the following configuration parameters have been deprecated:
  - `LangIdCumStreamParameterSection` - use the new parameter `LangIdParameterSection` instead
  - `LangIdCumWavParameterSection` - use the new parameter `LangIdParameterSection` instead.
  - `StreamToTextParameterSection` - use the new parameter `SpeechToTextParameterSection` instead.
  - `StreamToTextTaskType` - use the new parameter `SpeechToTextTaskType` instead.
  - `WavToTextParameterSection` - use the new parameter `SpeechToTextParameterSection` instead.
  - `WavToTextTaskType` - use the new parameter `SpeechToTextTaskType` instead.

  In the `idol_speech` Lua function the named parameters `langIdCumStreamParameters`, `langIdCumWavParameters`, `streamToTextParameters`, and `wavToTextParameters` have been deprecated. Use the new named parameters `langIdParameters` and `speechToTextParameters` instead.

  > **IMPORTANT:**
  > The deprecated parameters are still available but only work with Speech Server 11.4 and earlier. If you upgrade your IDOL Speech Server, you must also update your CFS task configurations and Lua scripts. The deprecated parameters might be deleted in future.

File System Connector

- The following configuration parameters, for action authorization by client IP address, have been deprecated:
  - `[Server] AdminClients`
  - `[Server] QueryClients`
  - `[Service] ServiceControlClients`
  - `[Service] ServiceStatusClients`

  You can now use the `[AuthorizationRoles]` configuration section to set up authorization for your servers more flexibly. These configuration parameters are still available for existing implementations, but they might be incompatible with new functionality. The parameters might be deleted in future.

HTTP Connector

- The following configuration parameters, for action authorization by client IP address, have been deprecated:
  - `[Server] AdminClients`
  - `[Server] QueryClients`
  - `[Service] ServiceControlClients`
  - `[Service] ServiceStatusClients`

  You can now use the `[AuthorizationRoles]` configuration section to set up authorization for your servers more flexibly. These configuration parameters are still available for existing implementations, but they might be incompatible with new functionality. The parameters might be deleted in future.

Media Server

Licensing Changes

- GPU acceleration is now permitted with surveillance licenses.
- The licensing requirements for chaining (sending records to another Media Server for further processing) have changed. The downstream server now requires one visual channel for each session that is started by an upstream Media Server, regardless of the analysis engines used.
- The licensing model for surveillance channels has changed. Face detection and face recognition require a single surveillance channel to recognize up to 250 faces, but each additional 250 faces requires an additional surveillance channel. For example, to run face detection and face recognition with a database of 600 faces now requires three surveillance channels. A new configuration parameter, `MaxFaces`, has been added to the face recognition engine. If you want to recognize more than 250 faces using a surveillance license you must set this parameter to the number of faces in

your face database. Visual licenses are unaffected and the number of faces that you can recognize with a visual channel is unlimited.

API and Configuration Changes

- Ingestion, analysis, encoding, transformation, event stream processing, and output tasks can no longer be configured in the Media Server configuration file (`mediaserver.cfg`). The task configuration must be passed to the `process` action when you begin processing. This means that when you send a `process` action to Media Server you must set one of the action parameters `Config`, `ConfigName`, or `ConfigPath`.
- As a result of improvements to face recognition, you must retrain Media Server to recognize faces by running the action `BuildAllFaces`.
- Tracks produced by ingest engines now follow similar naming conventions to the tracks produced by other engines. The first image track is named *`TaskName`*`.Image_1`, where *`TaskName`* is the name of the ingest task. The first audio track is named *`TaskName`*`.Audio_`*`lang`*`_1`, or *`TaskName`*`.Audio__1` if the language is not available. You can use the aliases `Default_Image` or `Image_1` to refer to the first image track, and the alias `Default_Audio` to refer to the first audio track.

  > **IMPORTANT:**
  > You must update any configuration that uses track names such as `Image_2`,`Audio__2`,`Image_3`,`Audio__3`, and so on.

- The output of face recognition, objection recognition, and vehicle model identification no longer includes the `imagelabel` element, which identified the training image that best matched the recognized face, object, or vehicle.
- Media Server does not output results if there is an error communicating with the Speech Server for audio matching, language identification, speech-to-text, or speaker identification. Previous versions of Media Server created records that contained an error message, but you should use the parameter `MaxConsecutiveTries` to fail the session when the Speech Server is unavailable.
- The LibAv ingest engine no longer accepts streams from Wittwin. HPE recommends that you use the new Wittwin ingest engine instead.

User Interface Changes

- The live video display in the scene analysis training utility shows regions of interest for the current category, rather than for all categories.

Deprecated Features

Category	Deprecated Feature	Deprecated Since
Server / Service	The `AdminClients`, `QueryClients`, `ServiceControlClients`, and `ServiceStatusClients` configuration parameters. HPE recommends that you use authorization roles instead.	11.5.0
Number plate recognition	The `BlackAndWhiteCamera` configuration parameter. Media Server 11.5.0 automatically detects whether the source video is black-and-white, so you no longer	11.5.0

	need to set this parameter.	
Speech analysis	The `ErrorMessage` configuration parameter, for the audio matching, language identification, speaker identification, and speech-to-text analysis tasks. You can use the parameter `MaxConsecutiveTries` to fail the session when the Speech Server is unavailable.	11.5.0
Image classification	The `Bayesian` and `Maxvote` classifier types. HPE recommends that you use Convolutional Neural Network (`CNN`) classifiers instead.	11.4.0
Ingest - LibAV	The `IngestTime` configuration parameter. HPE recommends that you use the new configuration parameter `IngestDateTime` instead. The new parameter accepts values in a greater number of formats.	11.4.0
Number plate recognition	The `ANPRFormatsDirectory` and `ANPRWeightsDirectory` configuration parameters. You can set the path for all static data folders by setting the configuration parameter `[Paths] StaticDataDirectory`.	11.4.0
Number plate recognition	The `OutputAllIntResults` and `PlateSizeUnit` configuration parameters. HPE recommends using the new parameters `OutputAlternativeResults` and `CharHeightUnit`, respectively.	11.4.0
OCR	The `ImageBinarizeMethod` configuration parameter.	11.4.0
Speaker identification	`GMM` models. HPE recommends that you use Speaker Identification with `iVector` models instead.	11.4.0
Language identification	The configuration parameter `CumulativeMode`. HPE recommends that you use the parameter `Mode` instead.	11.4.0
Rolling buffer	The action parameter `name`, available on the actions `AddStream`, `EditStream`, `GetStreamInfo`, `PreAllocateStorage`, and `RemoveStream`. HPE recommends that you use the new parameter `stream`, instead.	11.4.0
Rolling buffer	The action parameters `OldName` and `NewName`, on the action `RenameStream`. HPE recommends that you use the new parameters `Stream` and `NewStream` instead.	11.4.0
Face detection	The `DetectEyes` configuration parameter.	11.3.0

Removed features

The following deprecated features have been removed:

- The configuration parameter `FrameRateMax`, from the image encoder.

Web Connector

- The configuration parameters `MinPageAge` and `MaxPageAge` have been deprecated, because the parameters `MinPageDate` and `MaxPageDate` now support relative dates.
- The following configuration parameters, for action authorization by client IP address, have been deprecated:
  - `[Server] AdminClients`
  - `[Server] QueryClients`
  - `[Service] ServiceControlClients`
  - `[Service] ServiceStatusClients`

  You can now use the `[AuthorizationRoles]` configuration section to set up authorization for your servers more flexibly. These configuration parameters are still available for existing implementations, but they might be incompatible with new functionality. The parameters might be deleted in future.

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 11.5.0 using the IDOL 11.5.0 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 for the following tasks has been removed. These standard tasks were removed from the Speech Server configuration file in a previous version. You can now add punctuation in the relevant speech to text tasks by using the Punctuation parameter.
  - StreamToTextMusicFilterPunct
  - StreamToTextPunct
  - TelWavToTextPunct
  - WavToTextPunct

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*