Perceptive Content Email Broker Connector

Configuration Guide

Version: 3.0

HYLAND™

Documentation Notice

Table of Contents

Overview

The Perceptive Content Email Broker Connector (Connector) has two configuration points, the start parameters and the appsettings.json file. The start parameters allow you to specify the location of the app settings and crash information files. The appsettings.json file controls the remote configuration access of the service.

Start parameters

The Connector provides two optional parameters, **--config** and **--crashfile**.

The **--config** parameter allows you to specify the file path to use for your app settings file. This parameter overwrites both the default location, **./appsettings.json**, and the **ECS_PSCONTENT_BROKER_CONNECTOR_provider__source** environment variable. You may provide either a full or relative file path. To set the app settings file, enter **--config** followed by the desired file path. If the path contains spaces, enclose it with quotation marks.

For example, if your settings file is located at **C:\Program Files\Hyland\Perceptive Content Email Broker Connector\appsettings.json**, you would add the following to your start parameters:

--config "C:\Program Files\Hyland\Perceptive Content Email Broker Connector\appsettings.json"

The **--crashfile** parameter allows you to specify the file path to use for service crash files. Service crash files occur when starting the service with an invalid or missing app settings file. This setting overwrites the default location, **./pscontent.broker.connector.err**. To set the crash file, enter **--crashfile** followed by the desired file path. If the path contains spaces, enclose it with quotation marks.

For example, if your crash file is located at **C:\Program Files\Hyland\Perceptive Content Email Broker Connector\pscontent.broker.connector.err**, you would add the following start parameters:

--crashfile "C:\Program Files\Hyland\Perceptive Content Email Broker Connector\pscontent.broker.connector.err"

Windows service start parameters

If you want to use start parameters with an installed Windows service, then you must run the service controller command, **sc config**, to configure the start parameters.

To modify the service's start parameters, complete the following steps:

1. Open an elevated command prompt.

2. Run the following command:

```
sc config Perceptive.Content.Email.Broker.Connector.exe binPath=
"\"{INSTALL_DIR}\Perceptive.Content.Email.Broker.Connector.exe\" --crashfile
\"{CRASHFILE_PATH}\" --config \"{CONFIG_PATH}\""
```

Where

{INSTALL_DIR} is the location where the Connector is installed. By default, this location is **C:\Program Files\Hyland\Perceptive Content Email Broker Connector**.

{CRASHFILE_PATH} is the location where the system writes the crashfile.

{CONFIG_PATH} is the name and location of the settings.json file.

3. Restart the service.

Linux service start parameters

The Linux installer provides arguments to set the start parameters at installation time. If you want to modify the start parameters after installation, then you must modify the installed **.service** file and restart the service.

To modify services start parameters, complete the following steps:

1. Locate and open the installed **.service** file. The default service name is **PerceptiveContentEmailBrokerConnector.service** with **/etc/system/system/** as the default location. You can change the name and location during installation.

2. Locate and modify the desired **Environment** entry in the **.service** file. If the desired entry is missing, then you must add the entry yourself.

   - The **Environment="ECS_PSCONTENT_BROKER_CONNECTOR_configfile=** entry controls the **--config** start parameter.

   - The **Environment="ECS_PSCONTENT_BROKER_CONNECTOR_crashfile=** entry controls the **--crashfile** start parameter.

To use the system environment variable **ECS_PSCONTENT_BROKER_CONNECTOR_provider__source**, complete the following steps:

1. Remove the setting for the **--config** start parameter by setting the value to nothing. For example, **Environment="ECS_PSCONTENT_BROKER_CONNECTOR_configfile=**.

2. Add the system environment variable **ECS_PSCONTENT_BROKER_CONNECTOR_provider__source=/full/path/to/settings/file.json**.

3. Restart the service.

For more information on basic **systemctl** commands, refer to **Linux Service Control Commands**.

App settings

The app settings file controls how your Connector connects to the Hyland Remote Configuration Server (HRCS). The remote connections are controlled by the Remotes section in your app settings. You may also include an optional Hyland Logging section to debug issues with your remote connections. For on premise or hybrid deployments, you may also include any setting from the Remote Configuration, **but any remotes that use the same configuration keys will overwrite any settings in your app settings file**.

Remotes

The **Remotes** section contains the connection information for your HRCS connections.

The **Remote Configuration Servers** subsection is a map containing the various server configurations for the Connector. Each **<User Defined Remote Name>** entry of the **Remote Configuration Servers** map represent a unique server configuration. The **<User Defined Remote Name>** keys do not matter to the Connector, and they are used to easily track the various servers with human-readable identifiers. Typically, a Connector instance should only have a single **<User Defined Remote Name>**. For more information on Remote HRCS Connections and behavior, see Appendix B: Remote HRCS connection best practices and behavior.

For a full list of remote configuration options see Remote Configuration.

<User Defined Remote Name>

Each **<User Defined Remote Name>** is a subsection of the **Remote Configuration Servers** section and specifies the settings for each configured server. The **<User Defined Remote Name>** name is user-defined and only serves as a human-readable identifier for the server.

The following table lists the settings for the **<User Defined Remote Name>** sub-section.

Setting	Description
Configuration Reference Ids	Specifies a map of **<User Defined Reference Names>** to references IDs on the HRCS.
Host	Specifies the host IP address of the configured server.
Port	Specifies the port number of the configured server.
Route	Specifies the client route of the HRCS.
Bearer Token	Specifies the bearer token that will be used when interacting with the configured HRCS.
Reconnect Delay	Specifies how long to wait before reattempting to connect to the HRCS after a failed attempt.

ConfigurationReferenceIds <User Defined Reference Names>

The <User Defined Reference Names> keys of the **ConfigurationReferenceIds** control which configurations the Connector should retrieve from the HRCS server. The Connector supports Hyland Logging HRCS configurations identified with a **HylandLogging** prefix, and Email Broker HRCS configurations identified with an **EmailBrokerConnector** prefix. Typically, a Broker Connector instance should only have a single **EmailBrokerConnector** HRCS configuration with an optional **HylandLogging** HRCS configuration. Any entries without a **HylandLogging** or **EmailBrokerConnector** prefix are ignored by the Connector. For more information on Remote HRCS connections and behavior, see Appendix B: Remote HRCS connection best practices and behavior. For more information on best practices for logging, see Appendix C: Logging best practices.

Example

The following is an example of the **Remotes** section.

```
"Remotes": {
    "RemoteConfigurationServers": {
        "<User Defined Remote Name>": {
            "ConfigurationReferenceIds": {
                "HylandLogging": "example-hyland-logging-id",
                "EmailBrokerConnector ": "example-broker-connector-id",
                "xEmailBrokerConnector": "example-ignored-broker-connector-id"
            },
            "Host": "example-hrcs-host",
            "Port": "5001",
            "BearerToken": "example-bearer-token",
            "ReconnectDelay": "00:00:10"
        }
    }
}
```

Configuration

Editing the Connector Configuration requires an HRCS administrator to create a Hyland-Email-Broker-Connector type configuration. There are three ways to create configuration for editing.

- To start from an empty config, the HRCS administrator will create configuration by navigating to **Manage Config** > **Hyland-Email-Broker-Connector** and clicking the plus icon. After giving the config instance a description, the administrator can click the **Save and Open** button and then click the **Create Empty Config** button under **Version: HylandEmailBrokerConnectorV3**.

- To start from a pre-existing json file (appsettings.json), the HRCS administrator will navigate to **Manage Config** > **Hyland-Email-Broker-Connector** and click the plus icon. After giving the config instance a description, the administrator can click the **Save and Open** button and then click the **Upload** button under **Version: HylandEmailBrokerConnectorV3.**

- To start from an Email Agent ini file, the HRCS administrator will navigate to **Manage Config** > **Hyland-Email-Broker-Connector** and click the plus icon. After giving the config instance a description, the administrator can click the **Save and Open** button and then follow the instructions in Appendix E: Email Agent Upgrade.

Remote Configuration

The following sections contain the settings controlled by each of your HRCS connections.

Instance Options

The **Instance Options** section controls the Connector's immutable global settings.

Note You must restart the Connector before the Connector recognizes any changes within the **Instance Options** section.

The following table lists the settings for the **Instance Options** section.

Setting	Description
Instance Name	Controls the name of this instance. This name appears on all log events from this instance, and it modifies the name of the temporary files generated by this instance. If you only use one instance, then you may omit this setting. The Connector uses **HylandEmailBrokerConnector** as the default Connector name when the **Instance Name** is not specified.
Temp Directory	Controls the path to the directory used by this Connector instance to store temporary files. When omitted, this setting defaults to the temporary path defined by your operating system. On Windows, this path is **C:\Users\{Username}\AppData\Local\Temp** where **{Username}** is the name of the user running the Connector instance. On Linux, this path is **/tmp**.

System

The **System** section specifies the global settings for how a worker starts and executes.

The following table lists the settings for the **System** section.

Setting	Description
Default Worker Execution Interval	Controls how often a worker should fire. If the execution interval elapses before a worker finishes processing its inbox, then the Broker allows the worker to continue without interruption and does not attempt to start the worker until after the next interval. Should match the **[-][d'.']hh':'mm':'ss['.'fffffff]** timespan format. If you omit this setting, the app uses **1** minute as the default. If the time elapses and a worker is still working, then the worker will simply continue its current task.
Worker Shutdown Timeout	Controls how long the app should wait for a worker to shut down during a configuration change or during shutdown. The value should match the **[-][d'.']hh':'mm':'ss['.'fffffff]** timespan format. If you omit this setting, the app uses **10** seconds as the default. If a worker does not shut down gracefully within the timeout, then the broker will forcibly stop the worker, regardless of its current task. This may result in partially captured messages on your S3 server.
Stagger Startup	Controls how the app starts its workers. If **Stagger Startup** is true, then each worker starts after its **Execution Interval**. If **Stagger Startup** is **false**, then the app starts all workers immediately. The default is **false**.
Debug Flags	The debug flags control behaviors for troubleshooting issues with the Broker. These settings require an attached debugger and may cause unsafe or unexpected behavior. Do not use in a production environment.

Hyland Logging

The **Hyland Logging** section controls the logging behavior for the Connector. Typically, a deployment only uses the **Routes** settings, but the Connector supports all Hyland Logging settings.

Routes

This section is a subsection of **Hyland Logging** and specifies the configuration information for each configured route.

<Name of Route>

The **<Name of Route>** section is a subsection of the **Routes** section and specifies the settings for each configured route. The **<Name of Route>** name is user-defined.

The following table lists the settings for the **<Name of Route>** section.

Setting	Description
Console	Specifies logging to the console. Leave this value empty.
File	Specifies the path and name of the log file to where the logger writes.

Splunk	Specifies the http address of the Splunk server. Omit to disable Splunk logging.
Splunk Token	Specifies the authentication token to use for the Splunk server
Exclude Profiles	Specifies which profiles are not written to this route. Profiles not listed are written to the route. The **include-profiles** setting overrides this setting. The default is **Empty List**.
Include Profiles	Specifies which profiles are written to this route. Profiles not listed are not written. The default is **Empty List**.
Minimum Level	Specifies the minimum level of logging, **Trace**, **Debug**, **Information**, **Warning**, **Error**, **Critical**, or **None**, you want the system to log.
Maximum Level	Specifies the maximum level of logging, **Trace**, **Debug**, **Information**, **Warning**, **Error**, **Critical**, or **None**, you want the system to log.
File Roll on Size	Specifies if the logger should rollover based on size. The default is **false**.
File Count Limit	Specifies the number of rollover log files to keep. Setting **File Count Limit** to **""** (empty string) specifies that the logger should keep an infinite number of log files. The default is **31**.
File Byte Limit	Specifies the maximum size a log file may reach before the logger stops writing to the file. If **File Roll on Size** is set to **false**, then the logger will not write to the file until another log rollover event occurs, or the file is deleted. The default is **1 GB**.
Output Format	Specifies the output format to use when logging. Valid values are **json**, **text**, and **minimal**. The default is **json**. Note that the minimal format does not include logging context data, so some logging information may be missing.

Content Management Servers

The **Content Management Servers** section is a set of **Content Management Server** sections used by the **Workers** configurations. Each section under **Content Management Servers** represents a unique server that is user-defined. This name is referenced by the Workers' **Worker Capture > Content Management Server** property.

<Content Management Server Name>

The **<Content Management Server Name>** is a subsection of the **Content Management Servers** section and specifies the settings for each configured server. The **<Content Management Server Name>** name is user-defined.

Integration Server

The **Integration Server** section is a subsection of the **<Content Management Server Name>** section and specifies information about Integration Server.

The following table lists the settings for the **Integration Server** section.

Setting	Description
License Type	Specifies the license type, **Standard** or **Cloud**, you want to configure.
URL	Specifies the location of the Content Server's Integration Server.
Authentication	Contains the subsection **Token Authentication** which specifies the authorization settings used to connect with Integration Server. The following lists the settings for the Token Authentication section. **Token** – Specifies the token required by the Integration Server. The settings key is **Token**.

Storage Servers

The **Storage Servers** section specifies the set of storage servers used by the Workers configurations. Each section under Storage Servers represents a unique server that is named by its section property. This name is referenced by the Workers' **Storage Server > Server** property. Each server can be an S3 Server or a Local Server. Typically, a Connector will have one storage server using the S3 protocol with connection options for each desired storage bucket. The Connector can support multiple storage servers with any valid protocol. The bucket layout does not matter to the Connector, so there is no best practice for bucket layouts. Your layout only depends on your S3 server's best practices. Multiple workers can share a bucket, or each worker can have their own bucket.

Note The Storage Servers must match your Broker Configuration.

S3 Server

The **S3 Server** section specifies the settings for the stored email data on an Amazon S3 compatible server. See Appendix D: S3 permissions for information on the required S3 permissions.

The following settings are available for the **S3 Server Storage** section.

Setting	Description
Endpoint	Specifies the IP address or DNS name of the storage server. This endpoint must include the server's port number. It must not include a http:// or https:// prefix. Use the **Enable Https** setting to control the endpoint's SSL behavior. Either the endpoint must specify a region, or the **Region** field must be configured. The HRCS plugin cannot validate this for you.
Region	Specifies the physical location of the server. By default, it is blank. If you are unsure of the location, or if you are using a local S3 server, leave it unset. Either the endpoint must specify a region, or the **Region** field must be configured. The HRCS plugin cannot validate this for you.
Enable Https	Controls the SSL settings used when communicating with the endpoint.
Connection Options	Specifies the connections options available with this server. Each connection option has a user-defined name. These options are referenced by the **Workers' Storage Server Connection Option** property. Multiple options may share their settings, and multiple workers may reference the same option. The setting is in the **Connection Options** section. **Authentication** – Specifies the authentication used by this connection option. This section contains a **Basic Authentication** sub-section that contains the settings Username and Password.

Local Server

The **Local Server** section specifies the settings for retrieving an email stored by the **Connector** on the local machine.

The following setting is available for the **Local** section.

Setting	Description
Location	Specifies the path to the local disk storage directory. Because of directory control concerns, we recommend that multiple local servers do not share their storage directory. However, if you have multiple workers that should write to the same directory, then multiple workers may reference the same local storage server. Note that workers referencing a local server do not use a **Storage Server Connection Option**.

Message Queuing Servers

The **Message Queuing Servers** section specifies the set of message queuing servers used by the **Workers** configurations. Each section under **Message Queueing Servers** represents a unique server that is named by its section property. The **Workers' RabbitMQ Message Queueing Server > MQServer Server** property references this name.

Each server's configuration must match an **MQ Server** configuration from the **Broker** configuration. Unlike **Storage Servers**, the server names do not need to match the name from the broker's **Message Queueing Servers** section, but we suggest using the same names to avoid any confusion regarding the relation between the two configuration sections.

The Connector only supports **Advanced Message Queuing Protocol (AMQP)** compatible connections.

RabbitMQ

The **RabbitMQ** section specifies the settings necessary to connect to a RabbitMQ server. All settings in this section are optional. Any omitted settings will use the default behavior as described by RabbitMQ's documentation. Note that if you wish to use RabbitMQ's default authentication, you must configure and reference a **Connection Options** set to use **No Authentication**.

The following settings are available for the **RabbitMQ** section.

Setting	Description
Host Name	Specifies the name of the host used by this RabbitMQ server.
Virtual Host	Specifies the virtual host used by this RabbitMQ server.
Port	Specifies the port number exposed by your RabbitMQ server. Type **-1** to use RabbitMQ's default port number.
Operation Timeout	Specifies the number of milliseconds past the expected operation durations the server should wait for RabbitMQ operations. This setting must be between 0 and 60000 milliseconds (1 minute), or it must be completely omitted. If the setting value is 0 or omitted, then the server only waits for the expected duration of each operation. Should match the **[-][d'.']hh':'mm':'ss['.'fffffff]** timespan format.
SSL	Specifies the SSL section contains the settings that control the SSL options for this server. For more information on the available settings, see the **SSL table** below.
Connection Options	Specifies the connections options available with this server. Each connection option has a user defined name. These options are referenced by the Workers' **Message Queueing Server Connection Option** property. Multiple options may share their settings, and multiple workers may reference the same option. For more information on the available settings, see the **Connection Options** table below.

Ssl

The **Ssl** section is a subsection of the **RabbitMQ** section and specifies the settings that control the SSL options for this server.

The following settings are available for the **Ssl** section.

Setting	Description
Enabled	Controls if this server should use the SSL settings during RabbitMQ connections. If **Enabled** is **false**, then the server will not use SSL to connect to the RabbitMQ server.
Certificate Path	The file path to the SSL certificate used by this server.
Certificate Passphrase	The password required to access the SSL certificate found at the **Certificate Path**. If your cert is not password protected, then you may omit this setting.

Setting	Description
Server Name	The name of the server used to generate the certificate found at the **Certificate Path**.
Acceptable Policy Errors	Specifies the flags for controlling any allowed SSL Policy errors If none of the flags are selected, then the server will not allow any certificate errors The following table lists the available flags for the Errors section. • Remote Certificate Not Available • Remote Certificate Name Mismatch • Remote Certificate Chain Errors
SSL Protocols	Specifies the flags for controlling the allowed SSL protocol versions. If none of the flags are selected, then the server will not be able to connect using SSL. The following table lists the available flags for the Protocols section. <table><tr><th>Setting</th><th>Description</th></tr><tr><td>SSL 2.0</td><td>Specifies the SSL 2.0 protocol. SSL 2.0 has been superseded by the TLS protocol and is provided for backward compatibility only.</td></tr><tr><td>SSL 3.0</td><td>Specifies the SSL 3.0 protocol. SSL 3.0 has been superseded by the TLS protocol and is provided for backward compatibility only.</td></tr><tr><td>TLS 1.0</td><td>Specifies the TLS 1.0 security protocol. The TLS protocol is defined in IETF RFC 2246.</td></tr><tr><td>TLS 1.1</td><td>Specifies the TLS 1.1 security protocol. The TLS protocol is defined in IETF RFC 4346.</td></tr><tr><td>TLS 1.2</td><td>Specifies the TLS 1.2 security protocol. The TLS protocol is defined in IETF RFC 5246.</td></tr></table>

Connection Options

The **Connection Options** section specifies the connections options available with this server. Each connection option has a user defined name. These options are referenced by the Workers' **Message Queueing Server Connection Option** property. Multiple options may share their settings, and multiple workers may reference the same option.

Setting	Description
Authentication	**Specifies t**he authentication used by this connection option. This section contains either a **NoAuth** section or a **BasicAuth** section.

The following table lists the settings for the **Authentication** section.

Setting	Description
No Auth**entication**	Represents a connection option that uses RabbitMQ's default authentication.
Basic Auth**entication**	Represents a connection option that uses basic authentication and includes the settings **Username** and **Password**.

Workers

The **Workers** section is a list of configured workers that monitor Message Queue Server queues for messages produced by **Broker** instances. Each section under **Workers** represents a unique workers that is named by its section property. These names do not need to match the names of the workers in your broker instances.

Each Worker needs a configured Message Queueing Server, Storage Server, and Content Management Server. Workers may share each server. Workers may share the **Connection Options** for **Message Queue Servers** ,**Storage Servers and Content Management Servers.**

The following settings are available in the **Workers** section:

Setting	Description
Enabled	Controls whether this instance should run this worker. If Enabled is false, then the worker will not execute.
Retry Delay	Controls how long this instance should wait before trying to restart this worker when this worker encounters a startup error. If specified, then this setting must be between one second and one hour. Should match the [-][d'.']hh':'mm':'ss['.'fffffff] timespan format. The default is the configured **System > Default Worker Execution Interval**.
Message Queuing Server	Controls the Message Queue server monitored by this worker. For more information, see Message Queueing Server.
Capture	Controls the capture behavior employed in creating a Perceptive Content document. For more information, see Capture.

Message Queuing Server

This is a subsection of the Worker configuration that controls which Message Queuing Server to monitor. Controls which **Message Queuing Server** to use for this worker's server connection. This name must match a configured **Message Queuing Server** from the **Message Queuing Servers** section. Multiple workers may share the same **Message Queuing Server** Connection

The following settings are available in the **Message Queuing Server** section.

Setting	Description

Server	Specifies which Message Queuing Server to use for this worker's server connection. This name must match a configured **MQ Server** from the Message Queuing Servers section. Multiple workers may share the same **MQ Server**.
Queue	Specifies the queue monitored by this worker. **Notes** • To protect data integrity and enforce message capture consistency, multiple workers may not share the same queue. • Queue names must also match queue names configured by the Broker service
Connection Option	Specifies the name of the Connection Option to use in the targeted MQ Server. Multiple workers may share the same MQ Server Connection Option.
Requeued Consumer Delay	Specifies when an item is requeued. The amount of time the connector stops listening for items in the message queue. This time gives other connectors an opportunity to grab the requeued message from the queue. The valid range for this field is 0 to 5 minutes, and the default is **0**.

Capture

The **Capture** section is a subsection of the **Worker** that controls what is going to be captured to a Perceptive Content document.

The following settings are available in the **Capture** section.

Setting	Description
Content Management Server	Specifies the name of the targeted Content Management Server. This name must match a configured **Content Management Server**.
Document Field Mapping	Controls how to create a document in Perceptive Content. For more information, see Document Field Mapping.
Failure Settings	Controls how to handle a message that has failed processing. For more information, see Failure Settings.
Warn Document Conflicts	Specifies whether to write a message in the log file indicating that a Perceptive Content document with the same keys already exists, and that the new pages are appended to it. The default is **true**, and configuration is not required unless you want to set it to **false**.
Workflow Settings	Controls whether to add the document to a Perceptive Content Workflow Queue. Options include **Do Not Submit** and **Submit**. The default is **Do Not Submit** and configuration is not required. For more information, see Workflow Settings.

Message Capture Mode

Th **Message Capture Mode** section is a subsection of **Capture** that controls the capture mode. Options include **Capture EML** and **Capture Message Parts**.

You must choose at least one of the following settings in the **Message Capture Mode** section.

Setting	Description	Value
Capture EML	When setting is defined the MIME data will be added to the document as an EML file.	For more information, see Empty Object Value.

Setting	Description	Value
Capture Message Parts	When the setting is defined only the parts specified will be added to the document as pages.	For more information, see Message Capture Settings.

Capture EML

This section is a subsection of the **Message Capture Mode** section.

Message Capture Settings

The **Message Capture Settings** section is a subsection of the **Message Capture Mode** section.

Settings

Setting	Description	Value
Email Settings	The **Email Settings** section contains various options for the email body, header, footer, and metadata.	
Attachment Capture Mode	Specifies the choice between splitting a multipage TIFF or not. For more information, see Single Document Mode and Multiple Document Mode.	
Attachment Settings	The **Attachment Settings** section describes how to capture standard attachments.	For more information, see Common Attachment Settings
Inline Attachment Settings	The **Inline Attachment Settings** section describes how to capture standard attachments.	For more information, see Common Attachment Settings

Email Settings

The **Email Settings** section is a subsection of the **Message Capture Settings** section.

Settings

The following settings are available in the **Email Settings** section.

Setting	Description
Prefer HTML	Specifies whether to use the html body of the email message when creating the page for the Perceptive Content document. Note When **Prefer HTML** flag is set to **true**, and the include header or footer flags are set to **true** a second page is created for the header and footer information.
Include Header	Specifies whether to include the email message header information with the message body. The header information includes the **From**, **Date Received**, **To**, **CC**, and **Subject** of the email being processed.
Include Footer	Specifies whether to include the email message footer information with the message body.
Include Metadata	Specifies whether to include the metadata associated with the email being processed.

Setting	Description
Message Body	Specifies a choice between **Exclude Message Body**, **Message Body**, and **Message Body With Null Body** to create or not create a Perceptive Content document with the email's message body. **Exclude Message Body** specifies a page will not be created for the message body. This option may display in the user interface as Exclude Message Body. **MessageBody** specifies a page will be created for the message body. This option may display in the user interface as Message Body. **Message Body With Null Body** specifies a page will be created even if the message body is empty. This option may display in the user interface as Message Body With Null Body.

Attachment Capture Mode

The **Attachment Capture Mode** section is a subsection of **Message Capture Settings** section. You can choose between storing attachments in **Single Document Mode** or **Multiple Document Mode**.

Exactly one of the following settings must be chosen in the **Attachment Capture Mode** section.

Setting	Description
Single Document Mode	Each attachment is captured as a separate page. For more information, see Single Document Mode
Multiple Document Mode	Each attachment is captured as a separate document. For more information, see Multiple Document Mode.

Workflow Settings

The **Workflow Settings** section is a subsection of **Capture** section and indicates whether to add documents to Perceptive Content workflow. You can choose between submitting or not submitting.

The following table lists the settings for the **Workflow Settings** section.

Setting	Description
Workflow	Specifies the choice between submitting or not submitting a document in Perceptive Content workflow. For more information, see Submit to Workflow and Do Not Submit to Workflow.

Document Field Mapping

The **Document Field Mapping** section is a subsection of **Capture** and is required for each **Worker**. This specifies the configuration for creating a Perceptive Content document. Includes the following fields, **Drawer**, **Document Type**, **Field Keys**, and **Document Notes**.

The following table describes the **Document Field Mapping** fields.

Setting	Options	Description	Reference Object
Drawer	Literal Field Mapping Search Field Mapping	Specifies how to map data to the Perceptive Content document.	For more information, see: Literal Field Mapping Search Field Mapping

Setting	Options	Description	Reference Object
Document Type	Literal Field Mapping Search Field Mapping	Specifies how to populate the document type in a Perceptive Content document.	For more information, see Literal Field Mapping Search Field Mapping
Field Keys	Field1 Field2 Field3 Field4 Field5	Specifies which fields to map. You must select at least one.	For more information, see Literal Field Mapping Time Stamp Field Mapping For more information, see UniqueID Field Mapping Email Field Mapping Search Field Mapping
Document Notes	Exclude Include	Specifies whether to include or exclude document notes. For more information, see Include Notes and Exclude Notes.	For more information, see Literal Field Mapping Time Stamp Field Mapping UniqueID Field Mapping Email Field Mapping Email Fields Mapping Search Field Mapping

```
}
```

Failure Settings

The **Failure Settings** section specifies how the system should handle failures.

Settings

The following settings are available for the **Failure Settings** section.

Setting	Description
Max Retry	Specifies how many times to requeue a message when there is a failure capturing.
Workflow Queue Name	Specifies to which workflow queue to add the failed document.
Only Use Fallback Document Mapping	A flag that specifies how to define a Perceptive Content document when failure occurs in the process of creating the document. true specifies that a document's keys are mapped using the following mapping: • drawer: default • document Type: default • Field1: Unique Id • Field2: "capture-error" • Field3: Capture Id When set to **true** the **Queue Name** is required to be valid in Perceptive Content. If it is not valid, the system requeues the message and does not store it in Perceptive Content.

	When set to **false** the Perceptive Content document is mapped based on the mapping configuration defined. If the defined mapping cannot be used or resolved by the connector, then the fallback document mapping is used.

Reference Objects

Common Attachment Settings

The **Attachment Settings** and **Inline Attachment Settings** are children of **Message Capture Settings.**

Exactly one of the following settings must be chosen in this section.

Setting	Description	Reference Object
Exclude	Specifies that attachments are not added to the document.	For more information, see Empty Object Value.
Include	Specifies which attachments to capture and if metadata should be captured.	For more information, see Include Attachments.

Exclude Attachments

The **Exclude Attachments** section specifies that attachments are excluded from the Perceptive Content document.

The following table lists the settings for the **Exclude Attachments** section.

Setting	Description	Value
Exclude	Specifies that attachments are not added to the document.	For more information, see Empty Object Value.

Include Attachments

The **Include Attachments** section describes how to capture inline attachments.

The following table lists the settings for the **Include Attachments** section.

Setting	Options	Reference Object
Metadata	Note The following options may display differently, as shown in the parentheses, in the user interface. • **Exclude Metadata** specifies that attachment's metadata is not included. • **Include Metadata** specifies that a new page for the attachment's metadata is created. • **Include With Empty Metadata** specifies that a new page, even	

	when there is no metadata for the attachment, is created.	
Filter Type	• NoFilter • InclusiveFilter • ExclusiveFilter	For more information, see Filter Type.

Filter Type

The **Filter Type** section describes how to filter attachments. Options include **Inclusive Filter**, **Exclusive Filter**, and **No Filter**.

Inclusive Filter

The **Inclusive Filter** section specifies the attachments you want to process.

The following table lists the settings for the **Inclusive Filter** section.

Settings	Description	Reference Object
Extensions	List of file extensions indicating which file attachments to include.	For more information, see Extensions.
Include Unextended Files	Flag indicating whether to create a page when there is no extension associated with the attachment.	

Exclusive Filter

This section specifies the attachments you do not want to process.

The following table lists the settings for the **Exclusive Filter** section.

Settings	Description	Reference Object
Extensions	List of file extensions indicating which file attachments to exclude.	For more information, see Extensions.
Exclude Unextended Files	Flag indicating whether to create a page when there is no extension associated with the attachment.	

No Filter

The **No Filter** section includes all attachments without any filtering set.

The following table lists the settings for the **No Filter** section.

Setting	Description	Value
No Filter	Specifies not to filter.	For more information, see Empty Object Value.

Extensions

The **Extensions** section defines the list of file extensions.

The following tables lists the settings for the **Extensions** section.

Settings	Description	Value
Values	Specifies the file extension being added.	For more information, see Empty Object Value.

Document Notes Mapping

The **Document Notes Mapping** section specifies whether to include document notes. This field is optional.

The following table lists the settings for the **Document Notes** section.

Setting	Description	Reference Object
Document Notes	Specifies whether to include or exclude document notes. Options include **Exclude Notes** and **Include Notes**.	For more information, see Exclude Notes and Include Notes.

Exclude Notes

Specifies that document notes are excluded.

Include Notes

Specifies that document notes are included.

The following table lists the settings for the **Include Notes** section.

Setting	Description
Include	The following mappings can be used to map to **Document Notes**. • Literal Field Mapping • Search Field Mapping • Time Stamp Mapping • UniqueID Mapping • Email Field Mapping • Email Fields Mapping

Document Field Mapping

Literal Field Mapping

The following table lists the settings for the **Literal Field Mapping** section.

Setting	Description
Literal	Controls the value placed in the document field.
	Object containing the literal value.
	Value
	Places the specified value into the named document field.
	Note
	If the Value is longer than 40 characters and the document field is not notes, then the system truncates the value to 40 characters.

Search Field Mapping

The **Search Field Mapping** section uses a regex pattern to search for a value from a specified email field and places it into the named document field.

The following table lists the settings for **Search Mapping** section.

Setting	Description	Reference
Search Pattern	Specifies regular expression pattern to search for.	
Default	When the search pattern returns not found, this would be the **Default** value.	
	Default is required when this mapping is used for Drawer and **Document Type**.	
Email Field List	Specifies a list of email fields to search using the **Search Pattern**.	For more information, see Email Fields Mapping.
	The keys to this list are user defined, but we recommend using numbers to represent the order in which to search.	

Time Stamp Field Mapping

The following table lists the settings for **Time Stamp Mapping** section.

Setting	Description
Time Stamp	Controls the value placed in the document field.
	Object containing the time stamp value.
	Format
	The **Format** field supports the culturally invariant standard date and time format strings. If your format results in a value that is longer than 40 characters and the document field is not Notes, then the system truncates the value.
	If the format is not specified, then the mapper uses the standard date time format of o which is Round-trip date/time. The default format is equivalent to **yyyy'-'MM'-'dd'T'HH':'mm':'ss'.'fffffffK**.

Setting	Description
	TargetTimeZone
	The **TargetTimeZone** field supports both Windows Zone IDs and the 2019c NodaTime Zone IDs. If the target time zone is not specified, then the mapper uses the current system's time zone. If your business logic is time zone sensitive, you should explicitly specify the target time zone and use a format that includes the time zone information.

UniqueID Field Mapping

Generates an ID using System.Guid.NewGuid() and places it into the named field. This type does not require any additional fields.

The configuration includes the Empty Object Value and is automatically done by the user interface.

Email Field Mapping

The following table lists the settings for **EmailField** section.

Setting	Description	Reference
Text Field	Specifies how the mapper extracts any email fields that are not address or date related.	For more information, see Text Field Mapping.
Address Field	Specifies how the mapper extracts email address fields.	For more information, see Address Field Mapping.
Email Date	Specifies how the mapper extracts email date fields.	For more information, see, Date Field Mapping.

Text Field Mapping

The following table lists the settings for **Email Text Value** section.

Setting	Description
Text Field	The following lists the available email field options, which are not address or date related, from which to extract.
	Note The following options may display differently, as shown in the parentheses, in the user interface.
	• CaptureId (Capture ID)
	• HtmlBody (HTML Body)
	• Importance (Importance)
	• InlineAttachmentCount (Inline Attachment Count)
	• HasAttachments (Attachments)
	• HasInlineAttachments (Has Inline Attachments)
	• ServerMessageId (Server Message ID)
	• StandardAttachmentCount (Standard Attachment Count)

	• TotalAttachmentCount (Total Attachment Count)
	• TextBody (Text Body)
	• Subject (Subject)

Address Field Mapping

The following table lists the settings for **Email Address Value** section.

Setting	Description
Address Format	The following lists the available option: Note The following options may display differently, as shown in the parentheses, in the user interface. • AddressOnly (Address Only) to extract just the email address. • FriendlyName to extract email address with the user's friendly name (Friendly Name). • FriendlyNameAndAddress (Friendly Name and Address) to extract both parts of the email address. If the email address does not specify a friendly name, then the address will always appear like it was extracted using AddressOnly. Note If an email address field contains multiple addresses, then the formatted addresses are separated by the , (comma) character. If AddressFormat is not specified, then the field defaults to FriendlyName.
Email Field	The following lists the available email field options from which to extract: Note The following options may display differently, as shown in the parentheses, in the user interface. • Cc • From • ReplyTo (Reply To) • Sender • To

Date Field Mapping

The following table lists the settings for **Email Date Value** section.

Setting	Description	Reference
Time Stamp Format	Specifies the configuration for formatting a date time string.	For more information, see Time Stamp Field Mapping.
Target Time Zone	Specifies the time zone for the date time string.	For more information, see Time Stamp Field Mapping.
Email Field	DateReceived **Note** This option may display in the user	

Setting	Description	Reference
	interface as Date Received.	

Email Fields Mapping

The following table lists the settings for **Email List** section.

Setting	Description
Entire Header	For more information, see Entire Header Field Mapping.
Text Field	For more information, see Email Field Mapping.
Address Field	For more information, see Address Field Mapping.
Email Date	For more information, see Date Field Mapping.

Email Entire Header Field Mapping

Specifies whether to extract the **from**, **to**, **cc**, **subject**, **date_received**, and **reply_to** fields.

This mapping is only valid for Document Notes Mapping and Search Mapping.

The following table lists the settings for **Entire Header Value** section.

Setting	Description	Reference Object
Address Format	Options include **AddressOnly**, **FriendlyName**, and **FriendlNameAndAddress**.	
Time Stamp Format	Specifies how to format a timestamp.	For more information, see Time Stamp Field Mapping.
Target Time Zone	Specifies the time zone for the date time string.	For more information, see Time Stamp Field Mapping.
Email Field	EntireHeader **Note** This option may display in the user interface as Entire Header.	

Empty Object Value

The **Empty Object** value is the value that is applied to an empty object. This value is automatically set in the user interface by the system.

The following table lists the settings for the **Empty Object** section.

Key	Value	Description
State	Enabled	Specifies the setting or value required when using an empty object.

Attachment Mode

Single Document Mode

The **Single Document Mode** section specifies whether to create a single Perceptive Content document for all processed attachments.

The following table lists the settings for the **Single Doc Mode** section.

Setting	Description
Split Tiffs	Specifies whether a multipage TIFF should be split. Options are true or false.

Multiple Document Mode

The **Multiple Document Mode** section specifies whether to create new Perceptive Content documents for each processed attachment.

The following table lists the settings for the **Multi Document Mode** section.

Setting	Description
Split Tiffs	Specifies whether a multipage TIFF should be split. Note The following options may display differently, as shown in the parentheses, in the user interface. • No Split specifies not splitting. • Split Tiffs Into Docs specifies that for each page split from a tif create a new Perceptive Content document • Split Tiff Into Pages specifies that all the split pages from the tiff are put into the same Perceptive Content document.

Workflow

Submit

The **Submit** section specifies whether to add the document to Perceptive Content workflow.

The following table lists the settings for the **Submit To Workflow** section.

Setting	Description
Priority	Specifies the priority to use when adding items to the workflow queue. Options include, low, medium, and high. The default is medium.
Workflow Queue Name	Specifies the name of the Perceptive Content workflow queue.

Do Not Submit

The **Do Not Submit** setting specifies that the document is not added to Perceptive Content workflow.

The following table lists the settings for the **Do Not Submit** section.

Setting	Description	Value
Do Not Submit to Workflow	Specifies that the document is not added to Perceptive Content workflow.	Empty object value

Appendix A: Hyland Application Settings Utility (HASU)

This section gives a brief overview of how to use HASU, a command line utility, to register certificates to the required certificate store and write values to an existing property within a configuration file.

Register

The **register** command registers a valid x509Certificate2 into the cert store in CurrentUser:My store location for future encryption and decryption. This is required for Linux based environments.

The following table list the available actions for register.

Action	Description
-p –password	Required. Specifies the password that protects the certificate.
--filePath	Required. Specifies the full file path to the PFX certificate.
--verbose	Sets minimum **LogLevel** to **Trace**. The default is **Error**.

Example

```
./Hyland.Application.Settings.Utility register --filePath /etc/pki/tls/certs /sample-
certificate.pfx --password YourPassword –verbose
```

Write

The **write** command stores the value to an existing property within the configuration file.

The following table lists the available actions for write.

Action	Description
-p, --property	Required. Property of the config file. Nested objects should be separated by a colon ':'.
-a, --applicationRoot	Required. Specifies the path to the application root.
--file	Required. Specifies the relative file path to the JSON configuration from the application root.
-v, --value	Required. Specifies the value to protect.
-i, --inline	Required. Encrypts the value of the provided property in the provided file.
-r, --recursive	Required. Encrypt all of the values under the provided property in the provided file.
--verbose	Sets minimum **LogLevel** to **Trace**. The default is **Error**.

Action	Description
-f, --force	Forces creation of value if not present. The default if **false**.
--encrypt	Boolean flag to determine if the value should be encrypted before being stored. The default is false. If needed, you can read the encrypted settings stored in the configuration file.
-t, --thumbprint	Required for Linux. Specifies the certificate thumbprint used to hash the encryption key.

Example

```
./Hyland.Application.Settings.Utility write -a /opt/brokerConnector --file
appsettings.json -p Remotes:RemoteConfigurationServers:Remote1:BearerToken -i --
thumbprint 03D724DD2666B9D858CAB84808372BAE82F89A36 --encrypt
```

Read

The **read** command displays the property value in the console output.

The following table lists the available actions for read.

Action	Description
-p, --property	Required. Property of the config file. Nested objects should be separated by a colon ':'.
-a, --applicationRoot	Required. Specifies the path to the application root.
--file	Required. Specifies the relative file path to the JSON configuration from the application root.
--verbose	Sets minimum **LogLevel** to **Trace**. The default is **Error**.
--decrypt	Boolean flag to determine if the value should be decrypted before being retrieved. The default is **false**.

Example

```
./Hyland.Application.Settings.Utility read -a /opt/brokerconnector --file
appsettings.json -p Remotes:RemoteConfigurationServers:Remote1:BearerToken
```

Appendix B: Remote HRCS connection best practices and behavior

Behavior

The Connector adds a connection for all configuration references that start with the **HylandLogging** prefix. These configurations are added under the **Hyland Logging** section, and they must have a **Hyland.Logging** configuration type or the Connector will fail to retrieve the configurations.

The Connector adds a connection for all configuration references that start with the **EmailBrokerConnector** prefix. These configurations are added directly to the root of the configuration. They are expected to be reference instances version **HylandEmailBrokerConnectorV3** of the **Hyland-Email-Broker-Connector** configuration type.

The order of the connections and the order of the references IDs controls the order that the remote configurations are applied to the Connector, so for any conflicting settings the Connector uses the value from the last connection. Unique values are preserved from each connection.

All the **Hyland Logging** configurations are added before the **EmailBrokerConnector** configurations, so any **Hyland.Logging** settings in any **EmailBrokerConnector** configuration take precedence over the settings from any **HylandLogging** configuration.

Example

Given:

```
"Remotes": {
    "RemoteConfigurationServers": {
        "<UserDefined-Remote>": {
            "ConfigurationReferenceIds": {
                "EmailBrokerConnector-Config1": "example-connector-id-1",
                "EmailBrokerConnector-Config2": "example-connector-id-2"
            },
            "Host": "example-hrcs-host",
            "Port": "5001",
            "Route": "example-hrcs-client-route",
            "BearerToken": "example-bearer-token",
            "ReconnectDelay": "00:00:10"
        }
    }
}
```

Or given:

```
"Remotes": {
    "RemoteConfigurationServers": {
        "<UserDefined-Remote-1>": {
            "ConfigurationReferenceIds": {
                "EmailBrokerConnector ": "broker-connector-id-1"
            },
            "Host": "example-hrcs-host-1",
            "Port": "5001",
            "Route": "example-hrcs-client-route-1",
            "BearerToken": "example-bearer-token-1",
            "ReconnectDelay": "00:00:10"
        },
        "<UserDefined-Remote-2>": {
            "ConfigurationReferenceIds": {
                "EmailBrokerConnector": "broker-connector-id-2"
            },
            "Host": "example-hrcs-host-2",
            "Port": "5001",
            "Route": "example-hrcs-client-route-2",
            "BearerToken": "example-bearer-token",
            "ReconnectDelay": "00:00:10"
        }
    }
}
```

With **broker-connector-id-1** settings:

```
{
  "key1": "b1-v1",
  "key2": {
    "subkey1": "b1-v2-1",
    "subkey2": "b1-v2-2"
```

```
    },
    "key3": "b1-v3"
}
```

With **broker-id-2** settings:

```
{
    "key1": "b2-v1",
    "key2": {
        "subkey2": "b2-v2-2"
    },
    "key4": "b2-v4"
}
```

The resulting configuration would be:

```
{
    "key1": "b2-v1",
    "key2": {
        "subkey1": "b1-v2-1",
        "subkey2": "b2-v2-2"
    },
    "key3": "b1-v3",
    "key4": "b2-v4"
}
```

Best practices

The Connector allows multiple Remotes and **ConfigurationReferenceIds** to have as much flexibility as possible. However, you must be careful of the layer behavior when using more than one of each. Typically, your Broker Connector should have a single **RemoteConfigurationServers** entry with a single **EmailBrokerConnector ConfigurationReferenceIds** and a single, optional **Hyland Logging** section. Using only one configuration reference with one remote prevents unintended configuration layering behavior. See Appendix C: Logging best practices for information on when you should include a **Hyland Logging** section.

You may use the **prefix** behavior to store multiple references for easy configuration switching **while testing**. However, you should remove any unused references and remotes from production environments to prevent accidentally using the wrong configuration.

Example Reference Switching

The following example demonstrates a **Remotes** section with two reference IDs. You can switch between them easily by adding or removing the **x** from the reference ID names. Note that you must restart your Broker when switching for the changes to take effect.

```
"Remotes": {
    "RemoteConfigurationServers": {
        "<UserDefined-Remote>": {
            "ConfigurationReferenceIds": {
                "EmailBrokerConnector-TestEnv1": "example-test-settings-1",
                "xEmailBrokerConnector-TestEnv2": "example-test-settings-2"
            },
            "Host": "example-hrcs-host",
            "Port": "5001",
            "Route": "example-hrcs-client-route",
            "BearerToken": "example-bearer-token",
            "ReconnectDelay": "00:00:10"
        }
    }
```

```
}
```

Appendix C: Logging best practices

Typically, all logging settings should be configured in HRCS using either the **Email BrokerConnector** plugin or the **Hyland.Logging** plugin. The **Hyland Logging** section of the **Email BrokerConnector** configuration should have any instance or service specific logging settings. The **Hyland.Logging** configuration should have any logging settings that you wish to share across multiple instances or services such as a shared Splunk logging configuration.

If you do not have any cross service/instance logging settings, then you should omit **HylandLogging** from your configuration. If you have cross service/instance logging settings, then you need to be mindful of the layering behavior when configuring both **Email Broker Connector** plugin logging and **Hyland.Logging.** Generally, it is safest to only have **Email Broker Connector** plugin settings **or Hyland.Logging** plugin settings.

Additionally, the Connector supports configuring **Hyland.Logging** directly in the **appsettings.json** to facilitate debugging your **Remotes** connections. However, the **appsettings.json** logging settings should be removed once you properly establish your **Remotes** connections since the appsettins.json settings may interfere with the remote settings due to layering behavior.

Example

The following is an example of the **Hyland.Logging** section for your appsettings.json.

```
"Hyland.Logging": {
    "Routes": {
        "Console": {
            "Console": "",
            "minimum-level": "Information",
            "maximum-level": "Critical"
        },
        "All-Logs": {
            "file": "example-valid-path/file-name",
            "minimum-level": "Debug",
            "FileRollOnSize": true,
            "FileRollInterval": "day",
            "FileByteLimit": 100000000,
            "FileCountLimit": 50,
            "OutputFormat": "text"
        }
    }
}
```

Appendix D: S3 permissions

Your S3 account needs to be able to access the following S3 APIs to function.

- HeadBucket - https://docs.aws.amazon.com/AmazonS3/latest/API/API_HeadBucket.html
- ListBuckets - https://docs.aws.amazon.com/AmazonS3/latest/API/API_ListBuckets.html
- ListObjects - https://docs.aws.amazon.com/AmazonS3/latest/API/API_ListObjects.html
- CreateBucket - https://docs.aws.amazon.com/AmazonS3/latest/API/API_CreateBucket.html
- GetObject - https://docs.aws.amazon.com/AmazonS3/latest/API/API_GetObject.html

- PutObject - https://docs.aws.amazon.com/AmazonS3/latest/API/API_PutObject.html

- DeleteObject - https://docs.aws.amazon.com/AmazonS3/latest/API/API_DeleteObject.html

- HeadObject - https://docs.aws.amazon.com/AmazonS3/latest/API/API_HeadObject.html

- GetBucketLocation - https://docs.aws.amazon.com/AmazonS3/latest/API/API_GetBucketLocation.html

The permissions mechanisms vary based on your S3 server implementation, so contact your S3 administrator to properly configure permissions.

Appendix E: Email Agent upgrade

The Connector's HRCS plugin upgrades any Email Agent ini settings with an equivalent Broker Connector Hyland Remote Configuration (HRC) setting. These upgraded settings match the original behavior as close as possible, and the upgrader generates settings for new options that do not exist in the original Email Agent ini settings. This upgrade creates a worker for each Email Agent ini profile [{Profile}].

The Connector Plugin upgrades all possible Email Agent ini settings as they are written in the ini file, so validity is not guaranteed. You may need to correct your upgraded configuration before using it if the original settings were not valid.

{profile} is the section heading for a profile in the Email Agent ini file.

The Connector upgrader uses the following Email Agent ini sections and settings groups.

- [Logging] > *
  - With [{profile }] > createprofilelog
- [Remote] > integrationserver.*
- [{profile}] > document.destination.*
- [{profile}] > document.{Capture Path}
  - Where {Capture Path} is
    - keys.drawer,
    - keys.documentType,
    - keys.field[1-5]
    - notes
- [{profile}] > document.email*
- [{profile}] > document.inline*
- [{profile}] > document.attachments*
- [{profile}] > document.attachments.mode
- [{profile}] > document.tif.split

The upgrade process requires an HRCS administrator to create a Hyland-Email-Broker-Connector type configuration. During the upgrade you may encounter upload or upgrade failures, see Upload and Upgrade Failures for information on resolving these issues. To upgrade an Email Agent ini file to Email

Broker Connector configuration using a newly created Hyland-Email-Broker-Connector type configuration, perform the following steps.

1. Open your created configuration.

2. Upload a **Version: EmailAgent** configuration.

3. Upgrade to the **Version: HylandEmailBrokerConnectorV3** configuration from Source Version **EmailAgent**.

Upload and upgrade failures

While attempting to upload the Email Agent ini file or upgrading to a Broker Connector configuration, you may encounter failures. The following tables outline some common failures and how to resolve them

Upload failures

Failure	Solution
"Invalid ini key: {key}" where {key} contains ':'	Remove the ':' character from the ini section key. For example, "[Section:1]" would need to be "[Section – 1]" or something similar. The HRCS ini parser does not support ini sections containing ':'. If you encounter this error, you will likely see the error multiple times since an invalid ini section also invalidates all the properties in that section.

Upgrade failures

The following references are used by the **Upgrade Failures** table.

- {keyType} is one of the following document configuration types:
  - drawer
  - documentType
  - field[1-5]
  - notes
- **{msgPath}** is Worker: {profile} Document Settings {keyType}
- **{inputTimezonePattern}**
  - "General"
  - "RFC 822"
- **{inputPattern}** is the pattern that is being upgraded to Broker Connector configuration.
- **{brokenPattern}** is the feedback to which parts of the {inputPattern} that are unsupported or invalid.
- **{valid options}** in most failures the UI presents valid options to help fix the problem.

The following table outlines possible errors when upgrading from the Email Agent ini.

Failure	Solution

Logger has an unsupported rollover period "WEEK". Supported periods are: MINUTE, HOUR, DAY, MONTH.	Reconfigure the Agent logger to use one of the supported periods or switch to a size-based rollover. Hyland Logging does not support the WEEK rollover period. HRCS requires you to switch to a supported period or to size-based rollover prior to upgrading to avoid any unintended log rolling behavior.
{msgPath} Email message field value "ENTIRE_HEADER" is not valid. Select one of the following: {*valid options*}	Reconfigure selecting one of the {valid options} given.
{msgPath} Email message field value is required.	Reconfigure selecting one of the {valid options} given.
{msgPath} Unable to create an email field mapping from value "Serial".	Reconfigure selecting one of the {valid options} given.
{msgPath} Document Key Type "SERIAL" is not supported. Select one of the following: {valid options}.	Reconfigure selecting one of the {valid options} given.
{msgPath} Unable to convert DateTimeFormatter {inputPattern} {inputTimezonePattern } timezone pattern "brokenPattern" is not supported	The upgrader only supports "ISO 8601" time zone patterns "X" and "XXX"
{msgPath} Unable to convert DateTimeFormatter {inputPattern} Pattern character "brokenPattern" is not supported	
{msgPath} Unable to convert DateTimeFormatter {inputPattern} Pattern character "brokenPattern" is not valid.	
{msgPath} Unable to create an email field mapping from value"send_date". Unable to convert SimpleDateFormat {inputPattern} {inputTimezonePattern } timezone pattern "brokenPattern" is not supported	The upgrader only supports "ISO 8601" time zone patterns "X" and "XXX"
{msgPath} Unable to create an email field mapping from value"send_date". Unable to convert SimpleDateFormat {inputpattern} Pattern character "brokenPattern" is not supported	
{msgPath} Unable to create an email field mapping from value"send_date". Unable to convert SimpleDateFormat {inputPattern} Pattern character "brokenPattern" is not valid.	

Upgraded – [Logging]

The **Hyland Logging** upgrade creates new routes that best match the Email Agent's original **[Logging]** section. If your agent has logging disabled, then the upgrade will not create any routes. The only way to disable **Hyland Logging** is to remove all Routes. If your agent has logging enabled, then the upgrade creates a Route named **EmailAgentRoute** to handle the global logging. Additionally, the upgrade creates a route for each Email Agent profile, **[{profile}]**, with **createprofilelog=true** to maintain the Email Agent's original logging behavior. The profile Routes are clones of the global **EmailAgentRoute** with the original **{profile}** as their name and **Included Profiles** to only include the **{profile}**. If your deployment intends to

only use Splunk for logging, you must delete these routes to prevent the Connector from writing log files. All logging settings may be configured to meet your deployment requirements. These initial settings emulate the Email Agent's original behavior.

The upgrade process configures some common settings along with additional settings based on if the Email Agent's **[Logging] > policy.type** field was **size** or **time**.

Common logger upgrade

HRC Path: Hyland Logging > Routes > {Route}

[Logging] > Ini Setting	HRC Setting	Notes
level	Minimum Level	Note that if the Agent's **[Logging] > level** is off, then the upgrader will not create any routes.
	File	Based on the Agent's log file name convention. • If the route is the global **EmailAgentRoute**, then the value is email.agent.all.log. • If the route is a **{Profile}** route, then the value is **email.agent.{Route}.log**.
	Maximum Level	The upgrader sets **critical** to match the Agent's Logging behavior
	Output Format	The upgrader sets **json** to support machine readable logs.
	Include Profiles	• If the route is the global **EmailAgentRoute**, then the value is empty. • If the route is a **{Profile}** route, then the value is **{Profile}**.

[Logging] > policy.type - size upgrades

HRC Path: Hyland Logging > Routes > {Route}

[Logging] > Ini Setting	HRC Setting	Notes
policy.size.maxlogstokeep	File Count Limit	
policy.size.maxmbsize	File Byte Limit	The Agent uses a megabyte size while Hyland Logging uses a byte size, so the upgraded value will be 1,000,000 times the Agent's value.
	File Roll on Size	The upgrader sets **true** to enable size rolling.

[Logging] > policy.type - time upgrades

HRC Path: Hyland Logging > Routes > {Route}

[Logging] > Ini Setting	HRC Setting	Notes
policy.time.maxhistory	File Count Limit	
policy.time.rolloverperiod	File Roll Interval	Note the upgrade will fail if **[Logging] > policy.time.rolloverperiod** is **week**. Hyland logging

		does not support week rollover periods, so you must change your rollover period prior to upgrading.

Content Management Servers

The upgrade process creates a section under Content Management Servers named **Integration Server 1**. This section defines how to connect to Perceptive Content Integration Server.

[Remote] > integrationserver *

The following properties will be used when upgrading from the Email Agent ini.

- integrationserver.base.url

- integrationserver.authentication.token

- integrationserver.cloud.licensing

Content Management Server

HRC Path: Content Management Server > Integration Server 1

[Remote] > Ini Setting	HRC Setting	Notes
integrationserver.base.url	URL	
integrationserver.authentication.token	Authentication > Token	
integrationserver.cloud.licensing	License	If there is no value in this property, then the default is Standard

Generated - Storage Servers

The **Storage Servers** do not have an equivalent ini setting, so the upgrade process generates a single storage server named **Storage Server 1** with the **S3** option, and it generates a single **Connection Option** named **Storage Option 1** for **Storage Server 1**. The upgraded Workers are automatically configured to use this server and option. Also, the Hyland Email Broker uses the same storage server name during its upgrade process. You may rename this server and option at any time, but you must also update any workers and any settings in the Hyland Email Broker that reference the original values.

You must manually configure the generated server, **Storage Servers > Storage Server 1 > S3**, and the generated Connection Option, **Storage Servers > Storage Server 1 > S3 > Connection Options > Storage Option 1**, to match your **S3** server and account before you can use the Connector. If your deployment uses a **Local** server, then you must reconfigure **Storage Servers > Storage Server 1** to use the **Local** option and configure a **Location** (file system location) on the **Local** server.

Generated - Message Queueing Servers

The **Message Queueing Servers** do not have an equivalent ini setting, so the upgrade process generates a single MQ server named **MQ Server 1** with a single Connection Option named **MQ Option 1**. The upgraded Workers are automatically configured to use this server and option. Also, the Hyland Email Broker uses the same MQ server name during its upgrade process. You may rename this server and option at any time, but you must also update any workers and any settings in the Hyland Email Broker that reference the original values.

You must manually configure the generated server, **Message Queueing Servers > MQ Server 1**, and the generated Connection Option, **Message Queueing Servers > MQ Server 1 > Connection Options > MQ Option 1**, to match your AMQP Server and account before you can use the Connector.

Workers

The **Workers** upgrade creates a Broker Connector Worker for each Email Agent Profile.

Worker Naming

These Workers use the same name as the Email Agent profiles.

Message Queueing Server

The Message Queueing Server upgrade configures the Worker to target the generated Message Queueing Server and Connection Option, and configures a queue name. This Queue Name is derived from the Agent's Profile name using the format of **EmailBroker_{profile}** where **{profile}** is the name of the upgraded Agent Profile. To maintain the Agent's original behavior, this queue name matches the queue name generated by the Hyland Email Broker Worker upgrade. You may change this queue name at any time, but if you wish to maintain the original behavior, you must also update the Broker's configuration. Alternatively, this queue may be shared across multiple Broker Connector workers to allow the Broker Connector workers to share the Broker workers.

HRC Path: Workers > {profile} > Message Queueing Server

HRC Setting	Value	Notes
Server	MQ Server 1	References the generated placeholder configuration Message Queueing Servers > MQ Server 1
Connection Option	MQ Option 1	References the generated placeholder configuration Message Queueing Servers > MQ Server 1 > Connection Options > MQ Option 1
Queue	EmailBroker_{profile}	Where {profile} is the name of the upgraded Agent Profile.

Capture

Failure Settings

The **Workers > {profile} > Capture > Failure Settings** section is not filled out based on any Email Agent ini setting. However, a **Workflow Queue Name** is required and is given a default value of **Default-EmailBroker-Error-Queue**. This value should be changed to a valid workflow queue.

[{Profile}] > document.destination

The following properties are used by the upgrader to populate the **Workers > {profile} > Capture > Workflow Settings** section.

- document.destination.type
- document.destination.queue
- document.destination.queue.priority

The property **document.destination.type** is used by the upgrade to determine whether to create a **Submit** section.

HRC Path: Workers > {profile} > Capture > Workflow Settings

[{profile}] document.destination.type	HRC Setting
Document	Do Not Submit
Workflow	Submit

HRC Path: Workers > {profile} > Capture > Workflow Settings > Submit > Submit to Workflow

[{profile}] Ini Settings	HRC Setting	Notes
document.destination.queue	Workflow Queue Name	
document.destination.queue.priority	Priority	If this property is not filled out the default priority will be set to Medium.

[{Profile}] > document.{Capture Path}

{Capture Path} has the following list of valid mapping types in the Email Agent Ini file.

- keys.drawer
- keys.documentType
- keys.field[1-5]
- notes

The following properties are used by the upgrader to populate the Workers > {profile} > Capture > Document Field Mapping,

- [{profile}] > document.{Capture Path}.default
  - This property is only valid for drawer and documentType
- [{profile}] > document.{Capture Path}.type
- [{profile}] > document.{Capture Path}
- [{profile}] > document.{Capture Path}.addressformat
- [{profile}]> document.{Capture Path}.dateformat
  - This property is not valid for drawer and documentType

{Base Ini Path} is defined in the table below. This is the base path of the ini setting that will be going through the upgrade.

{Base HRC Path} is defined in the table below. This is the base path/navigation for HRC client based on the property {Base Ini Path}.

{Capture Path}	Base Ini Path	Base HRC Path
keys.drawer	[{profile}] > document.keys.drawer	Workers > {profile} > Capture > Document Field Mapping > Drawer
keys.documentType	[{profile}] > document.keys.documentType	Workers > {profile} > Capture > Document Field Mapping > Document Type

| keys.field[1-5] | [{profile}] > document.keys.field[1-5] | Workers > {profile} > Capture > Document Field Mapping > Field Keys > Field[1-5] |
| notes | [{profile}] > document.notes | Workers > {profile} > Capture > Document Field Mapping > Document Notes |

The following table describes the mapping relationship between the Ini Settings and the HRC Section that will be created.

{Capture Path}.type	Ini Setting	HRC Setting
Literal	[{profile}] > document.keys.drawer [{profile}] > document.keys.documentType [{profile}] > document.keys.field[1-5] [{profile}] > document.notes	{Base HRC Path} > Literal
Field	[{profile}] > document.keys.drawer [{profile}] > document.keys.documentType	{Base HRC Path} > Search
Field	[{profile}] > document.keys.field[1-5] [{profile}] > document.notes	{Base HRC Path} > Email Field
Function	[{profile}] > document.keys.drawer [{profile}] > document.keys.documentType [{profile}] > document.keys.field[1-5] [{profile}] > document.notes	{Base HRC Path} > Search
UniqueId	[{profile}] > document.keys.field[1-5] [{profile}] > document.notes	{Base HRC Path} > Unique ID
Timestamp	[{profile}] > document.keys.field[1-5] [{profile}] > document.notes	{Base HRC Path} > Time Stamp
Undefined	[{profile}] > document.keys.field[1-5] [{profile}] > document.notes	Skipped
Serial	Not Supported	Not Supported

Literal

HRC Path: {Base HRC Path}

Ini Setting	HRC Setting
{Base Ini Path}	Literal

Time Stamp

{Base HRC Path} > Time Stamp > Time Stamp

Ini Settings	HRC Setting
{Base Ini Path}.dateformat	Time Stamp Format
This value is not provided by the Email Agent Ini and UTC will be used as the default	Target Time Zone

Email Field

When {Base Ini Path} is drawer or documentType then the field is converted into a search pattern. See Function Based On Field for further details.

Email Fields can be mapped to one of the following three tables based on the value from {Base Ini Path}.

{Base Ini Path} Values	{Base HRC Path}
Subject Attachment_count Body	{Base HRC Path} > Email Field > Text Field
From To Reply_to cc	{Base HRC Path} > Email Field > Address Field
Send_date	{Base HRC Path} > Email Field > Email Date
Entire_header (only applies to notes)	{Base HRC Path} > Email Fields > 0 > Entire Header

Text Field

Table: {Base HRC Path} > Email Field > Text Field

Ini Settings	HRC Setting
{Base Ini Path}	Email Text Field

Address Field

Table: {Base HRC Path} > Email Field > Address Field

Ini Settings	HRC Setting
{Base Ini Path}.addressformat	Address Format
{Base Ini Path}	Email Field

Email Date

Table: {Base HRC Path} > Email Field > Email Date

Ini Settings	HRC Setting
{Base Ini Path}.dateformat	Email Date Field > Time Stamp Format
Note: this is not in the Ini but defaults to UTC	Email Date Field > Target Time Zone
Note: Send_Date is translated to Date Received and is the only option for date	Date Received

Function

{Base HRC Path} > Search

Ini Settings	HRC Setting	Notes

{Base Ini Path}	Search Pattern	The value will be converted to a regex pattern
{Base Ini Path}.default	Default	When Search pattern fails to return use this value
{Base Ini Path}	Email Field Values	Any email field used in the search function will be converted to an Email Field

Function Based On Field

{Base HRC Path} > Search

Ini Settings	HRC Setting	Notes
{Base Ini Path}.type=field		Drawer and document Type handle field differently than Fields 1-5 and Document Notes.
	Search Pattern	The upgrade will create the pattern of .*
{Base Ini Path}.default	Default	When Search pattern fails to return use this value
{Base Ini Path}	Email Field Values	Will be converted to an Email Field

[{Profile}] > document.email

The following properties are used by the upgrader to populate the Workers > {profile} > Capture > Message Capture Mode > Capture Message Parts > Email Settings

- document.email
- document.emailcreatepagefornullbody
- document.emailheader
- document.emailfooter
- document.emailPreferHTML

Include Email Message Body

The following properties will be used when upgrading from the Email Agent Ini to the Connector Message Capture Mode Section of the configuration

- document.email
- document.emailcreatepagefornullbody

HRC Path: Workers > {profile} > Capture > Message Capture Mode > Capture Message Parts > Email Settings > Message Body

[{profile}] document.email	[{profile}] document. emailcreatepagefornullbody	HRC Setting
false	true or false	Exclude Message Body
true	false	Message Body
true	true	Message Body With Null Body

Include Email Message Header

The following property will be used when upgrading from the Email Agent Ini to the Connector Message Capture Mode Section of the configuration

- document.emailheader

HRC Path: Workers > {profile} > Capture > Message Capture Mode > Capture Message Parts > Email Settings > Include Header

[{profile}] document.emailheader	HRC Setting
false	not checked
true	checked

Include Email Message Footer

The following property will be used when upgrading from the Email Agent Ini to the Connector Message Capture Mode Section of the configuration.

- document.emailfooter

HRC Path: Workers > {profile} > Capture > Message Capture Mode > Capture Message Parts > Email Settings > Include Footer

[{profile}] document.emailfooter	HRC Setting
false	not checked
true	checked

Include Email Prefer HTML

The following property will be used when upgrading from the Email Agent Ini to the Connector Message Capture Mode Section of the configuration.

- document.emailPreferHTML

HRC Path: Workers > {profile} > Capture > Message Capture Mode > Capture Message Parts > Email Settings > Prefer HTML

[{profile}] document.emailPreferHTML	HRC Setting
false	not checked

true	checked

[{Profile}] > document.inline*

The following properties are used when determining to Include Inline Attachments.

- [{profile}] document.attachments
- [{profile}] document.inline
- [{profile}] document.inline.attachments.include

Include Inline Attachments

HRC Path: Workers > {profile} > Capture > Message Capture Mode > Capture Message Parts > Inline Attachment Settings

[{profile}] document.attachments	[{profile}] document.inline	HRC Setting
false	true or false	Exclude
true	true	Include

Attachments to Include

HRC Path: Workers >{profile} > Capture > Message Capture Mode > Capture Message Parts > Inline Attachment Settings

[{profile}] document.attachments	[{profile}] document.inline	[{profile}] document.inline.attachments.include	HRC Setting
false	false or true	Any List	Exclude
true	true	Empty List	Include > Filter Type > No Filter
true	true	List of file extensions	Include > Filter Type > Inclusive > Included Extensions

[{Profile}] > document.attachments*

The following properties are used when determining to Include Attachments

- [{profile}] document.attachments
- [{profile}] document.attachments.exclude

Include Attachments

The property [{profile}] document.attachments is used by the upgrade to determine whether or not to create an Include Section

HRC Path: Workers > {profile} > Capture > Message Capture Mode > Capture Message Parts > Attachment Settings

[{profile}] document.attachments	HRC Setting
false	Exclude
true	Include

Attachments to Exclude

HRC Path: Workers > {profile} > Capture > Message Capture Mode > Capture Message Parts > Attachment Settings

[{profile}] document.attachments	[{profile}] document.attachments.exclude	HRC Setting
False	Any list	Exclude
True	Empty List	Include > Filter Type > No Filter
True	Non Empty List of file extensions	Include > Filter Type > Exclusive > Excluded Extensions

[{Profile}] > document.attachments.mode

- document.attachments.mode

Attachment Capture Mode

HRC Path: Workers > {profile} > Capture > Message Capture Mode > Capture Message Parts > Attachment Capture Mode

[{profile}] document.attachments.mode	HRC Setting
single_document	Single Document
multi_document	Multi Document

[{Profile}] > document.tif.split

The following properties will be used when upgrading from the Email Agent Ini to the Connector Message Capture Mode Section of the configuration.

- document.attachments.mode
- document.tiff.split
- document.tiff.keepsplittiffsinsamedocument

Split Tiffs Single Document Mode

HRC Path: Workers >{profile} > Capture > Message Capture Mode > Capture Message Parts > Attachment Capture Mode > Single Document

[{profile}] document.attachments.mode	[{profile}] document.tiff.split	HRC Setting
single_document	false	Split TIFFs

		The box is not checked
single_document	true	Split TIFFs The box is checked

Split Tiffs Multi Document Mode

HRC Path: Workers >{profile} > Capture > Message Capture Mode > Capture Message Parts > Attachment Capture Mode > Multi Document

[{profile}] document.attachments.mode	[{profile}] document.tiff.split	[{profile}] document.keepsplittiffsinsame document	HRC Setting (Split TIFFs Behaviour)
multi_document	false	true or false	No Split
multi_document	true	false	Split TIFF Into Docs
multi_document	true	true	Split TIFF Into Pages