Perceptive Content Email Agent

Installation and Setup Guide

Version: 1.3.x
Perceptive Content 7.x

Written by: Product Knowledge, R&D
Date: February 2023

Hyland™

Documentation Notice

Table of Contents

Email Agent

Perceptive Content Email Agent collects and manages email in the Perceptive Content system. Email Agent captures and indexes email messages. The agent can then route messages through workflow queues and forward the messages based upon settings you configure. As a server-side process, the agent delivers your emailed information, including attachments and graphics, to Perceptive Content for review and processing.

To use Email Agent, the administrator sets up one or more email accounts and configures the agent to monitor the inbox for that address. Email Agent then indexes all messages received and stores them as documents on Perceptive Content Server.

Note This document assumes you are installing Email Agent for the first time or have no earlier versions running on your computer. To update the agent or upgrade from a previous version, refer to Appendix C, Update Email Agent.

Set JAVA_HOME

Before installing the agent, you must set JAVA_HOME to the install path of Java prior to installing Email Agent. JAVA_HOME is not set automatically during installation. To set JAVA_HOME, use one of the following options.

Windows

You must add JAVA_HOME as an environment variable in the system settings for Windows. When creating the new system variable, set the variable name to “JAVA_HOME” and the variable value to the location of the installed Java directory.

You must also modify the PATH environment variable. In the PATH variable, append ;%JAVA_HOME%\bin to the variable value.

For detailed instructions on creating or changing environment variables, refer to the Java or Windows product documentation.

Linux

You must set JAVA_HOME in Linux by editing the ~./bashrc file. In the file, append the following line.

```
export JAVA_HOME=/installation/path
```

For detailed instructions on creating or changing environment variables in Linux, refer to the Java or Linux product documentation.

Install Email Agent

Use the following procedures to download, install on either Windows or Linux, and license Email Agent.

Note You must install Java on the server prior to installing Email Agent. For more information, refer to the *Email Agent Technical Specifications*.

Download the Email Agent files

To download Perceptive product installation files, complete the following steps.

1. Go to the Hyland Community site.
2. From the menu, click **Support** and then under **Software Downloads** select **Perceptive Downloads**.
3. Find and download the installer file corresponding to the version to be installed.

Note New and updated documentation and help topics are regularly published to the documentation website at docs.hyland.com.

Install Email Agent on Windows attended

Use the following procedures to install Email Agent on Windows. You can create multiple instances by running the installation from a different directory.

1. From the temporary directory where you downloaded the installation files, extract the files to a **[*drive*:]\Email.Agent**, or similar, directory.
2. Open a **Command Prompt** window as an administrator, navigate to the directory where the files were extracted, and execute the following command.

   ```
   install-windows
   ```

3. From the prompt, enter an instance name.

Install Email Agent on Linux attended

Use this procedure to install Email Agent in your Linux environment. You can create multiple instances by running the installation from a different directory.

1. From the temporary directory where you downloaded the installation files, extract the files to a [*drive*:]\Email.Agent, or similar, directory.
2. Navigate to the directory where the files were extracted and execute the following command.

   ```
   ./install-linux.sh
   ```

3. From the prompt, enter an instance name.

Install Email Agent on Windows or Linux unattended

Installing Email Agent silently is an automatic way to run an installation.

Run the unattended installation

Enter the following commands in a Command Prompt or Terminal window. Note that you can use any value, not exclusively Primary and Secondary.

- **Windows** `install-windows.bat Primary`

- **Linux** `./install-linux.sh Secondary`

Install the Email Agent license

When you purchase Email Agent, you receive a license file. Copy the license file to a temporary folder where you can access it with an ImageNow or Perceptive Content Client, depending on your version. Before authenticating the license, you must install ImageNow or Perceptive Content Server and at least one Client.

1. Copy the license file provided by your Enterprise Software representative to a temporary folder where you can access it with a Client.
2. On the **Start** menu, click **All Programs** and select one of the following options.
    1. In 6.7 environments, point to **ImageNow 6** and click **ImageNow 6**.
    2. In 7.x environments, point to **Perceptive Content** and click **Perceptive Content**.
3. In the login screen, click **License Manager**.
4. In the **License Management** dialog box, select **Upload licenses** and click **OK**.
5. Browse to the license file from its temporary directory, click **Open,** and then click **OK**.
6. In the **License Generation - Server Information** dialog box, complete the following substeps.
    1. In the **User ID and Password** boxes, type the user name and password of the owner or a manager.
    2. In the **Server Name or IP Address** box, type the Perceptive Content Server computer host name or IP address.
    3. In the **Port Number** box, type the port number of the Perceptive Content Server computer host.
    4. Click **OK**.
7. In the **License Upload** dialog box, verify the status of the license is **SUCCESS** and then click **Close**.

    Note For an explanation of why the license upload succeeded or failed, click **Details**.

Configure the Email Agent service

To configure the service, use Windows Explorer to navigate to the \etc directory in the Email Agent installation directory and open the emailAgent.ini file with a text editor. Then complete the steps in the following sections as necessary.

Important You cannot upgrade from any version of Mail Agent to Email Agent. You must manually copy any inserverMail.ini configuration settings to the emailAgent.ini file.

Configure logging

Logging helps to troubleshoot errors and login problems. The [Logging] group determines the level of logging and when to create new log files. Complete the following steps to configure logging. For more information, refer to the emailAgent.ini settings table in Appendix B.

1. In the **[Logging]** group, next to **level**, set the level of logging to output by entering one of the available options.
2. Set **policy.type** to either **time** or **size** based on your log file rollover preference.

3. If **policy.type** is set to **time**, set **policy.time.rolloverperiod** to specify the amount of time between log rollover events.

   Note Longer rollover periods may result in prohibitively large log files.

4. Optional. When **policy.type** is set to time, you can set the maximum number of log files to archive by setting **policy.time.maxhistory**.

   Note By omitting this setting, Email Agent will archive all log files.

5. If **policy.type** is set to **size**, set **policy.size.maxmbsize** to specify the maximum number of MB a log file can reach before triggering a rollover event.

6. If **policy.type** is set to **size**, set **policy.size.maxlogstokeep** to specify the maximun number of log files to archive.

7. Save the **emailAgent.ini** file.

Configure the [email0] or [email1] group

The remaining settings in the emailAgent.ini file are for the [email0] or [email1] group. To create a new [email] group (without any copied configurations), use the [email1] group, located at the bottom of the emailAgent.ini file. The [email1] group contains the same settings as the [email0] group, but does not include instructions or sample configurations.

You can rename the [email0] or [email1] group to any unique name except for existing group names in the emailAgent.ini file (such as [Remote] or [Logging]). You must duplicate the [email0] or [email1] group for each mail account you want Email Agent to monitor. In the [email0] group (or the group for the email account you want to modify), complete the following steps.

Enable or disable the monitoring of an email account

When you enable an email account, Email Agent monitors the email account and imports email from the account into Perceptive Content. To enable an email account, for the enable setting, type `TRUE`.

Set flag to create a log file for a profile

The **createprofilelog** setting determines whether to isolate specific log messages. When enabled, the logger writes all events in the profile and the primary Email Agent to a separate log file in addtion to the **email.agent.all.log** file. This isolated log name is **email.agent.[profilename].log** and its archiving behavior matches the configurations in the [Logging] group in the emailAgent.ini file. The default setting is **FALSE**.

For example, a profile named [email0] would have a profile log of email.agent.email0.log.

Set work times to monitor an email account

The work.type setting determines when Email Agent monitors the associated email account. Complete the following steps to define when Email Agent monitors the email account.

1. Locate **work.type** and type one of the following options.
   - To monitor the associated email account continuously, for **work.type**, type `ALWAYS`.

     Note When **work.type** is set to `ALWAYS`, **work.start.time** and **work.end.time** are ignored.
   - To monitor the associated email account, for **work.type**, type `SCHEDULED`.

     Note When set to `SCHEDULED`, you configure the **work.start.time** and **work.end.time** settings to define when the email account is monitored.
2. If you typed SCHEDULED, configure work.time.start and work.time.stop by specifying the following times.
   1. For **work.time.start**, type the starting number between **0000** (which represents 12:00 AM) and **2359** (11:59 PM).
   2. For **work.time.stop**, type the ending number between **0000** (which represents 12:00 AM) and **2359** (11:59 PM).
3. Save the **emailAgent.ini** file.

Set up your server to receive email

The incoming server settings configure the incoming mail server. You must define these settings so Email Agent can monitor and collect incoming emails sent to the specified email account. Modify one or more of the following settings to configure Email Agent for your system.

- **server.incoming** to specify the hostname or IP address of the incoming mail server. For example, you can supply the server name, server@domain.com, or the IP address, 168.34.151.3.
- **server.incoming.protocol** to set the type of communication protocol to the email server. Type POP3/IMAP for unencrypted connections, POP3S/IMAPS for SSL/TLS encrypted connections, GIMAP for Gmail OAuth Connections, or EWS/EWSCS/EWSROPC for Exchange Web Services connections. The EWS, POP3, POP3S, IMAP, and IMAPS protocols use Basic Auth to connect to the incoming server. Basic Auth protocols required the **server.incoming.password** field. EWS OAuth protocols require the **server.incoming.clientid** and **server.incoming.tenantid** fields. The EWSCS uses the Client-Secret OAuth access flow and requires the **server.incoming.clientsecret** field. The EWSROPC uses the Resource Owner Password Credentials (ROPC) OAuth access flow and requires the **server.incming.password** field. The GIMAP protocol uses GSuite service account authentication and requires the **server.incoming.credentialspath** field. GIMAP also uses its own SSL encryption and ignores the **server.incoming.ecryption.protocols** and **server.incoming.starttles** settings.

- **server.incoming.port** to specify the port number (1 - 65535) of the incoming mail server. By default, POP3 servers use port 110 and IMAP servers use port 143. The default for POP3S is 995 and the default for IMAPS and GIMAP servers is 993. EWS ignores this setting.
- **server.incoming.username** to specify the user name to use when connecting to the incoming mail server.
- **server.incoming.password** to specify the password to use when connecting to the incoming mail server. This setting is required when using Basic Auth protocols or when using ROPC protocols. This setting is not allowed when using Client-Secret protocols or GIMAP.
- **server.incoming.clientid** to specify the client ID to use when connecting to the incoming mail server using OAuth 2.0. This setting is not allowed if the incoming protocol does not support EWS OAuth 2.0.
- **server.incoming.tenantid** to specify the tenant ID to use when connecting to the incoming mail server using OAuth 2.0. This setting is not allowed if the incoming protocol does not support EWS OAuth 2.0. For EWSCS and EWSROPC you may use the tenant's name or the tenant's unique ID.
- **server.incoming.clientsecret** to specify the client secret to use when connecting to the incoming mail server using OAuth 2.0. This setting is not allowed if the incoming protocol does not support EWS OAuth 2.0 or if the protocol uses ROPC OAuth 2.0.
- **server.incoming.credentialspath** to specify the path to the json GSuite service account credentials file to use when connecting to the email server using the GIMAP protocol. This setting is not allowed if the incoming protocol only supports Basic Auth or if the protocol uses EWS OAuth.
- **server.incoming.interval** to set how often in seconds (30 seconds to 2147483647 seconds) you want to poll the incoming mail server. The default interval is 60.
- **server.incoming.disconnectdelay** to set how long in seconds you want Email Agent to wait after disconnecting from the email server. The default disconnect delay is 1.
- **server.incoming.encryption.protocols** to specify a space-separated list of supported encryption protocols to negotiate when connecting to the email server. For example, **server.incoming.encryption.protocols=SSLv3 or server.incoming.encryption.protocols=SSLv3 TLSv1 TLSv1.1 TLSv1.2**. This setting is optional. The EWS, EWSCS, EWSROPC, and GIMAP protocols ignore this setting.
- **server.incoming.starttls** to enable TLS encryption using an existing unencrypted connection. This setting is not necessary if the port is already encrypted or if the email server does not support the STARTTLS command. The default value is **FALSE**. The EWS, EWSCS, EWSROPC, and GIMAP protocols ignore this setting.

  TRUE = The STARTTLS command will be issued to use TLS encryption.

  FALSE = The STARTTLS command will not be issued.
- **server.incoming.ignoresslcertificates** to ignore an expired SSL certificate and keep importing email, set to `TRUE`**.** Otherwise, you restrict email from an expired SSL certificate by specifying `FALSE`.
- **server.incoming.mailconnectiondebug** to log debug information specific to the mail server if set to `TRUE`.
- **server.incoming.logHeaders** to provide additional logging information for the incoming email headers. The default value is **false**.
- **server.incoming.logAttachments** to provide additional logging information for email message attachments.

- **server.incoming.timeout.seconds** to set how often in seconds you want to poll the server when connecting before timing out. The default is 30.

Enable automatic reply, forward, and notify

The outgoing server settings configure the outgoing mail server. You can define these settings if you want Email Agent to forward or to reply automatically to incoming emails.

Automatic reply sends a response to the sender of any email message that Email Agent processes. Automatic forward enables Email Agent to forward all the email messages it processes. The messages are forwarded to a specified address. Complete the following steps to enable automatic reply and forward.

1. Modify one or more of the following settings.
    - **server.outgoing**, type the IP address or hostname of the outgoing mail server.
    - **server.outgoing.protocol**, type GSMTP, SMTP, SMTPS, EWS, EWSCS, or EWSROPC for the connection protocol. Use SMTPS for TLS encryption. Use EWSCS for client-secret with the **server.outgoing.clientsecret** field, or EWSROPC with the **server.outgoing.password** field for EWS OAuth 2.0 server access. All EWS OAuth protocols require the **server.outgoing.clientid** and **server.outgoing.tenantid** fields. The GSMTP protocol uses GSuite service account authentication and requires the **server.outgoing.credentialspath** field. GSMTP also uses its own TLS encryption and ignores the **server.outgoing.encryption.protocols** and **server.outgoing.starttls** settings.
    - **server.outgoing.port**, type the port number (1 - 65535) of the outgoing mail server. The default is 25. EWS ignores this setting.
    - **server.outgoing.username**, type the user name to use to connect to the outgoing mail server, if required by your mail server.
    - **server.outgoing.password**, type the password to use to connect to the outgoing mail server.

      Note This setting is required if a user name is set for **server.outgoing.username,** or if the **server.outgoing.protocol** uses ROPC OAuth. This setting is not allowed when using client-secret EWS OAuth 2.0 or the GSMTP protocol.
    - **server.outgoing.clientid**, type the client ID to use when connecting to the outgoing email server using OAuth 2.0. This setting is not allowed if the outgoing protocol does not support EWS OAuth 2.0.
    - **server.outgoing.tenantid**, type the tenant ID to use when connecting to the email server using OAuth 2.0. This setting is not allowed if the outgoing protocol does not support EWS OAuth 2.0.
    - **server.outgoing.clientsecret**, type the client secret to use when connecting to the email server as a client when using OAuth 2.0. This setting is not allowed if the outgoing protocol does not support EWS OAuth 2.0 or the protocol uses the ROPC OAuth 2.0 flow.
    - **Server.outgoing.credentialspath**, type the path to the json GSuite service account credentials file to use when connecting to the email server using the GSMTP protocol. This setting is not allowed if the outgoing protocol only supports Basic Auth or if the protocol uses EWS OAuth.
    - **server.outgoing.mailconnectiondebug**, type `TRUE` to log additional debug information specific to the outgoing mail server. Type `FALSE` if not. The default is `FALSE`.
    - **server.outgoing.timeout.seconds** sets how often in seconds you want Email Agent to poll the server when connecting before timing out. The default is 30.

2. To set up automatic reply, complete the following substeps.
    1. Set **autoreply** to `TRUE` to enable automatic replies or `FALSE` to disable automatic replies. The default is `FALSE`.
    2. Set **autoreply.message** by typing the message you want to include in the reply email.
3. To set up automatic forward, complete the following substeps.
    1. Set **autoforward** to `TRUE` to enable automatic email forwarding or `FALSE` to disable automatic email forwarding. The default is `FALSE`.
    2. Set **autoforward.email** by typing the email address to which the Email Agent email messages will be forwarded.
4. To set up the notify process failure message, complete the following substeps.
    1. Set **notifyprocessfailure** to `TRUE` to enable automatic notification of errors encountered while processing email.
5. Set **notifyprocessfailure.email** to provide the destination email address for the Email Agent notifications.
6. To provide a destination email address for Email Agent replies, forwards, or error message notifications, set **reply.email** by entering the full email address. This address will appear in the **From** line of the auto reply email message.

    Important Do not configure **reply.email** to the same email account Email Agent is monitoring. If this is not followed, and the automatic reply email is undeliverable, Email Agent could enter an endless cycle of receiving and sending the same email message.

    Some mail servers, such as Gmail, do not allow the sender of an email to be set to anything other than the actual account from which it is being sent. If this is the case, the sender address will be that of the account Email Agent uses to connect to the outgoing server.

6. Save the **emailAgent.ini** file.

Move broken emails

To enable Email Agent to move email messages that fail to process from the inbox to another folder, complete the following steps.

1. In the **[email0]** group, set **movefailedmessage** to `TRUE`.

    Note This setting cannot be enabled for **pop3** and **pop3s server.incoming.protocols**.

2. If **movefailedmessage** is set to `TRUE`, set **movefailedmessage.foldername** to the name of the destination folder for failed messages.

Set the destination of captured email messages

To specify if Email Agent sends captured email directly into Perceptive Content or to a workflow process, complete the following steps.

1. For **document.destination.type**, type one of the following options.
   - `DOCUMENT` to import incoming email directly into Perceptive Content.
   - `WORKFLOW` to import email into a Perceptive Content Workflow queue.
2. If you typed `WORKFLOW` for **document.destination.type**, complete the following substeps.
   1. For **document.destination.queue**, type the name of an existing Perceptive Content Workflow queue that has the appropriate privileges.
   2. For **document.destination.queue.priority**, type `LOW`, `MEDIUM`, or `HIGH` to define the priority Email Agent uses to add email to workflow. The default is `MEDIUM`.
3. Save the **emailAgent.ini** file.

Automatically index incoming email

Email Agent can automatically index captured email with document keys up to 40 characters in length. The document keys are made up of several fields: Drawer, Document Type, Field1, Field2, Field3, Field4, and Field5.

Specify a default drawer

Specify a default drawer for Email Agent to use in the event that the drawer value you define for document.keys.drawer.type and document.keys.drawer is invalid. For document.keys.drawer.default, type the name of a predefined Perceptive Content drawer.

Automatically assign a drawer value

A Perceptive Content drawer is the highest-level document key value in the index hierarchy. Complete the following steps to assign a drawer value to captured email automatically.

1. For **document.keys.drawer.type**, type one of the following options.
   1. `LITERAL` to populate the drawer value with the name of an existing Perceptive Content drawer.
   2. `FIELD` to populate the drawer value with text from the imported email message.
   3. `FUNCTION` to populate the drawer value based on a built-in function.
2. For **document.keys.drawer**, type one of the following options based on your selection in the previous step. Your entry cannot exceed 40 characters in length.
   1. If you set **document.keys.drawer.type** to `LITERAL`, type the name of an existing Perceptive Content drawer.
   2. If you set **document.keys.drawer.type** to `FIELD`, type one of the following options that correspond to the email section: `FROM`, `TO`, `CC`, `SUBJECT`, `REPLY_TO`, or `ATTACHMENT_COUNT`.

3. If set **document.keys.drawer.type** to `FUNCTION`, use the following built-in function: **search(<field>, <searchString>, <offset>, <EOL>** or **<numberOfCharacters>)**, where you can provide the following parameters.
   - ***<field>*** to specify the part of the email to search (**FROM**, **TO**, **CC**, **SUBJECT**, **SEND_DATE**, **REPLY_TO**, **BODY**, or **ATTACHMENT_COUNT**).
   - ***<searchString>*** to specify the string to search for (case sensitive).
   - ***<offset>*** to specify the number of characters to skip after the searchString is found.
   - ***<EOL>*** to capture all characters to the end of the line.
   - ***<numberOfCharacters>*** to specify a specific number of characters to capture.

3. Save the **emailAgent.ini** file.

Specify a default document type

Specify a default document type up to 40 characters in length for Email Agent to use in the event that the document type value you define for document.keys.documentType.type and document.keys.documentType is invalid. For document.keys.documentType.default, type the name of a predefined Perceptive Content document type.

Automatically assign a document type

Like a drawer, a document type is another document key that categorizes a document. For example, when Email Agent captures an email, you can assign the document type of Invoice to the email and its attachments.

1. For **document.keys.documentType.type**, type one of the following options.
   1. `LITERAL` to populate the document type value with the name of an existing Perceptive Content document type.
   2. `FIELD` to populate the document type value with text from the imported email message.
   3. `FUNCTION` to populate the document type value based on a built-in function.
2. For **document.keys.documentType**, type one of the following options based on your selection in the previous step. Document type values cannot exceed 40 characters in length.
   1. If you set **document.keys.documentType.type** to `LITERAL`, type any existing Perceptive Content document type name to populate the document type.
   2. If you set **document.keys.documentType.type** to `FIELD`, type one of the following options that correspond to the email section: `FROM`, `TO`, `CC`, `SUBJECT`, `REPLY_TO`, or `ATTACHMENT_COUNT`.

3. If you set **document.keys.documentType.type** to `FUNCTION`, use the following built-in function: **search(<field>, <searchString>, <offset>, <EOL>** or **<numberOfCharacters>),** where you can provide the following parameters.
   - **<*field*>** to specify the part of the email to search (**FROM**, **TO**, **CC**, **SUBJECT**, **SEND_DATE**, **REPLY_TO**, **BODY**, or **ATTACHMENT_COUNT**).
   - **<*searchString*>** to specify the string to search for (case sensitive).
   - **<*offset*>** to specify the number of characters to skip after the searchString is found.
   - **<*EOL*>** to capture all characters to the end of the line.
   - **<*numberOfCharacters*>** to specify a specific number of characters to capture.

3. Save the **emailAgent.ini** file.

Automatically assign Field1, Field2, Field3, Field4, and Field5

This section outlines steps to configure Email Agent to assign the Field1, Field2, Field3, Field4, and Field5 document keys automatically to captured email. The number of these keys you configure Email Agent to assign to your captured email depends on your business process.

1. For **document.keys.<*key*>.type** (where **<*key*>** can be **Field1**, **Field2**, **Field3**, **Field4**, or **Field5**), type one of the following options.
   - `LITERAL` to assign a literal key value.
   - `FIELD` to populate the key value with text from the imported email message.
   - `UNIQUEID` to populate the key value with a unique ID generated by Perceptive Content.
   - `TIMESTAMP` to populate the key value with the current timestamp.
   - `UNDEFINED` to ignore the key value.
   - `SERIAL` to populate the key value based on the serial settings.
   - `FUNCTION` to populate the key value based on a built-in function.
2. If you set **document.keys.<key>.type** to `LITERAL`, `FIELD`, or `FUNCTION`, configure **document.keys.<key>** to one of the following options.
   - If you set **document.keys.<key>.type** to `LITERAL`, type any valid name. This literal string populates the key.
   - If you set **document.keys.<key>.type** to `FIELD`, type one of the following options to define which part of the email message populates the key value.
     - `FROM`, `TO`, `CC`, `SUBJECT`, `SEND_DATE`, `REPLY_TO`, or `BODY` to populate the key with the specified portion of the email.
     - `ATTACHMENT_COUNT` to populate the key value with the number of attachments.
   - If you set **document.keys.<*key*>.type** to `FUNCTION`, define the following built-in function to populate the key value: **search(<*field*>, <*searchString*>, <*offset*>, <*EOL*>, or <*numberOfCharacters*>)**. You can supply the following parameters for the function.
     - **<*field*>** to specify the part of the email to search (**FROM, TO, CC, SUBJECT, SEND_DATE, REPLY_TO, BODY,** or **ATTACHMENT_COUNT**).
     - **<*searchString*>** to specify the string to search for (case sensitive).

- **<*offset*>** to specify the number of characters to skip after the searchString is found.
- **<*EOL*>** to capture all characters to the end of the line.
- **<*numberOfCharacters*>** to specify a specific number of characters to capture.

3. If you set **document.keys.<key>.type** to `SERIAL`, complete the following substeps.
    1. For **document.keys.<*key*>.type.serial.format**, use the following options to define the format of the serial data value Email Agent uses to populate the associated key.
        - **#** to not display zero values. All other values are considered constants. For example, if you type **##,###** and Email Agent receives the value 1984, the agent formats the key value as 1,984.
        - **0** to display zero values. All other values are considered constants. For example, if you type **#,###.00** and Email Agent receives the value 982.1, the agent formats the key value as 982.10.
    2. For **document.keys.<*key*>.type.serial.start**, configure the starting serial value by entering a positive integer. Email Agent automatically updates the value as it processes email. For example, if you assign the start value of 10, the agent sets the setting to 31 after it processes 20 emails.
4. If you set **document.keys.<key>.type** to `TIMESTAMP` or `FIELD` with **document.keys.<keys>** set to `SEND_DATE`, type a date and time pattern string for **document.keys.<key>.dateformat**. The default format is **EEE MMM d HH:mm:ss zzz yyyy** (for example, Thu Jan 15 09:20:27 GMT-06:00 2004). For additional date and time formats, refer to Appendix A, Specify date and time formats for automatic indexing.
5. Save the **emailAgent.ini** file.

Automatically assign Notes

You can optionally configure Email Agent to automatically assign additional metadata called notes to captured email. The value you define as a note appears in the Notes field within the document properties pane for the Perceptive Content document.

Note The ability to assign document notes requires Perceptive Integration Server 7.1.3 or higher.

1. For **document.notes.type**, type one of the following options.
    - `LITERAL` to assign a literal value to the Notes field.
    - `FIELD` to populate the Notes field with text from the imported email message.
    - `UNIQUEID` to populate the Notes field with a Unique ID generated by Perceptive Content.
    - `TIMESTAMP` to populate the Notes field with the current timestamp.
    - `UNDEFINED` to ignore the notes settings.
    - `SERIAL` to populate the Notes field based on the serial settings.
    - `FUNCTION` to populate the Notes field based on a built-in function.

2. If you set **document.notes.type** to `LITERAL`, `FIELD`, or `FUNCTION`, configure **document.notes** to one of the following options.
   - If you set **document.notes.type** to `LITERAL`, enter any literal string to populate the Notes field.
   - If you set **document.notes.type** to `FIELD`, type any number of the following options to define which part of the email message populates the Notes field. Use a pipe (|) to separate multiple options. The system ignores empty options.
     - `FROM`, `TO`, `CC`, `SUBJECT`, `SEND_DATE`, `REPLY_TO`, or `BODY` to populate the Notes field with the specified portion of the email.
     - `ATTACHMENT_COUNT` to populate the Notes field with the number of attachments in the email.
     - `ENTIRE_HEADER` to populate the Notes field with the entire email header. This option is equivalent to setting your document.notes field to `FROM` | `TO` | `CC` | `SUBJECT` | `SEND_DATE` | `REPLY_TO`. Each item in the output is delimited by a pipe (|). Sub items are delimited by a comma (,). The output does not add spaces next to the delimiters.
   - If you set **document.notes.type** to `FUNCTION`, define the following built-in function to populate the Notes field: search(<field>, <searchString>, <offset>, <EOL> | <numberOfCharacters>). You can supply the following parameters for the function.
     - ***<field>*** to specify the part of the email to search (`FROM`, `TO`, `CC`, `SUBJECT`, `SEND_DATE`, `REPLY_TO`, `BODY`, or `ATTACHMENT_COUNT`). This parameter does not support multiple options using a pipe (|).
     - ***<searchString>*** to specify the string to search for (case sensitive).
     - ***<offset>*** to specify the number of characters to skip after the searchString is found.
     - ***<EOL>*** to capture all characters to the end of the line.
     - ***<numberOfCharacters>*** to specify a specific number of characters to capture.
3. If you set **document.notes.type** to `SERIAL`, complete the following substeps.
   1. For **document.notes.type.serial.format**, use the following options to define the format of the serial data value Email Agent uses to populate the Notes field.
      - **#** to not display zero values. All other values are considered constants. For example, if you type **##,###** and Email Agent receives the value 1984, Email Agent formats the value as 1,984.
      - **0** to display zero values. All other values are considered constants. For example, if you type **#,###.00** and Email Agent receives the value 982.1, Email Agent formats the value as 982.10.
   2. For **document.notes.type.serial.start**, configure the starting serial value by entering a positive integer. Email Agent automatically updates the value as it processes email. For example, if you assign the start value of 10, Email Agent sets the setting to 31 after it processes 20 emails.
4. If you set **document.notes.type** to `TIMESTAMP` **or** `FIELD` with **document.notes** set to `SEND_DATE`, type a date and time pattern string for **document.notes.dateformat**. The default format is **EEE MMM d HH:mm:ss zzz yyyy** (for example, Thu Jan 15 09:20:27 GMT-06:00 2004). For additional options, refer to Appendix A, Specify date and time formats for automatic indexing.
5. Save the **inserverMail.ini** file.

Import attachments, but not the email message

You can choose to import an email message and its attachment(s) or capture only the email attachment(s). By default, Email Agent captures both the email message and any associated attachments. If you only want to capture email attachments, set the **document.email** setting to `FALSE`.

Note Attachments will only be captured if **document.attachments** is set to `TRUE`.

Enable email headers, footers, graphics, and attachments

When capturing an email, you can include the email header or footer information with the imported body text. An email footer appends the attachment file names to the bottom of the email body text. You can also enable or disable the automatic importing of inline graphics, which are graphics included within the body of an email message. For example, a graphical business card or background pattern in the body of an email message is an inline graphic. It is also possible to import an HTML body rather than the text-only body, if HTML is present in the email.

You can configure Email Agent not to capture email attachments. It is also possible to accept attachments while denying only certain file types. This feature protects against potential virus and security threats that may be in an attachment.

1. To include email header information with the imported body text, set **document.emailheader** to `TRUE`. Otherwise, set it to `FALSE`. The default is `TRUE`.
2. To append attachment file names to the email body, set **document.emailfooter** to `TRUE`. Otherwise, set it to `FALSE`. The default is `TRUE`.
3. To convert messages to HTML, when possible, set **document.emailPreferHTML** to `TRUE`. Otherwise, set it to `FALSE`.
4. To enable automatic importing of inline graphics as separate pages to the imported document, set **document.inline** to `TRUE`. Otherwise, set it to `FALSE`.

   Note Inline graphics are not included when Email Agent counts attachments as defined for **attachment_count**.
5. To enable or disable capturing email attachments, complete the following substeps.
   1. Set **document.attachments** to `TRUE` to enable importing of attachments or `FALSE` to disable importing.
   2. For **document.attachments.exclude**, list any attachment file types (separated by commas) that you want Email Agent to exclude during the automatic import of email attachments. Because of virus risks, we recommend that you exclude the following file types: **BAT**, **EXE**, **COM**, **PIF**, **CMD**, **JS**, **VBS**, **ZIP**, **DLL**, and **SIT**.
6. Save the **emailAgent.ini** file.

Index an email message, attachment, and inline graphic

You can specify if Perceptive Content indexes an email message and its associated attachment(s) and inline graphic(s) as one Perceptive Content document or multiple Perceptive Content documents. To index them as separate documents, you must assign at least one unique document key, such as a UNIQUEID, or serial value as discussed in the **Automatically assign Field1, Field2, Field3, Field4, and Field5** section. Without a unique document key, Perceptive Content stores the email message, attachment(s), and inline graphic(s) as a single document regardless of this setting. Perform one of the following actions.

- To index an email message and its associated attachment(s) and inline graphic(s) as one document, set **document.attachments.mode** to **single_document**.
- To index an email message and its associated attachment(s) and inline graphic(s) as multiple documents, set **document.attachments.mode** to **multi_document**.

Divide a multi-page TIFF document

To specify if a multi-page TIFF image remains intact or is separated into multiple Perceptive Content pages or documents, complete the following steps.

1. If you want Email Agent to divide a multi-page TIFF into separate TIFF images, set **document.tiff.split** to `TRUE`.

   If you set **document.tiff.split** to `TRUE`, and you want Perceptive Content to store the divided TIFF images as one Perceptive Content document, set **document.tiff.keepslittiffsinsamedocument** to `TRUE`.

   If you set **document.tiff.split** to `TRUE`, and you want Perceptive Content to store each page of the TIFF image as a separate Perceptive Content document, set **document.tiff.keepslittiffsinsamedocument** to `FALSE`.
2. If you want Email Agent to maintain a multi-page TIFF as one image, set **document.tiff.split** to `FALSE`.
3. Save the **emailAgent.ini** file.

Monitor additional email accounts

After configuring one email account with Email Agent, you can quickly add additional accounts that have the same settings. For each email account you want to monitor, you must create a separate **[email]** group in the **emailAgent.ini** file.

1. Locate the default **[email0]** or **[email1]** header (or the group you want to copy).
2. Copy and paste the entire **[<*email*>]** group at the bottom of the **emailAgent.ini** file.
3. Rename the heading of the newly pasted group. You must choose a unique name.
4. Using the steps provided in this document, configure the new group to monitor the email account you specify.
5. Save the **emailAgent.ini** file.

Configure agent token authentication

Configure Email Agent to use token based agent authentication by completing the following steps.

1. On the Perceptive Content Server machine, generate an authentication token for Email Agent by running the following command.

   ```
   intool --cmd create-authentication-token --lictype Mail Agent --file EmailAgent.txt
   ```

2. On the Email Agent machine, navigate to the **etc** directory in the Email Agent installation directory.
3. Using a text editor, open the **emailAgent.ini** file.
4. In the **[Remote]** section, set the **integrationserver.authentication.token** setting to the contents of the **EmailAgent.txt**, as shown in the following example.

   ```
   integrationserver.authentication.token=[authentication token]
   ```

5. Save and close the **emailAgent.ini** file.

Configure Integration Server for token-based agent authentication

After you configure agent token authentication, you must also configure Integration Server to support token-based authentication for agent connections. For more information on importing a token signing certificate and configuring Integration Server, refer to the Perceptive Integration Server on Tomcat Installation Guide 7.8 or Perceptive Integration Server on WebSphere Installation Guide 7.8.

Complete set up of the Email Agent Service

To start the Email Agent service using Windows Computer Management, complete the following steps.

1. On your Windows Desktop, right-click the **My Computer** shortcut and then click **Manage**.
2. In the **Computer Management** dialog box, click **Services and Applications**.
3. Click **Services**.
4. In the right pane, select the service titled **Perceptive Content Email Agent (INSTANCE_NAME)** and click **Start** in the upper left-hand corner of the right pane.

Consider virus risks

Email Agent assumes incoming emails are scanned for viruses using the appropriate virus software running on the host mail server. In addition, you can exclude certain attachment types that are known to carry viruses. We suggest that you exclude some extensions, for example BAT, EXE, COM, PIF, CMD, JS, VBS, ZIP, DLL, and SIT. You can exclude extensions by setting **document.attachments.exclude** in the **emailAgent.ini** file. For more information, refer to the **Enable email headers, footers, graphics, and attachments** section in this document.

Establish trust between Integration Server and Email Agent

To establish trust between Integration Server and Email Agent, when Integration Server is set up for SSL/TLS, you must import the Integration Server certificate into the Email Agent truststore. To import the certificate, complete the following steps.

1. Open a command window and navigate to the bin directory of your JRE installation.
2. Enter the following command.

```
keytool -import -v -trustcacerts -alias integrationserver -file [path to
integrationserver.cer] -keystore ${JAVA_HOME}/jre/lib/security/cacerts
```

Appendix A: Specify date and time formats for automatic indexing

You can specify date and time formats for Email Agent to use when the agent automatically indexes email. You specify the format in the **document.keys.<*key*>.dateformat** (where <*key*> can be Field1, Field2, Field3, Field4, or Field5) and **document.notes.dateformat** settings in the **emailAgent.ini** file. The date and time formats are specified by date and time pattern strings represented by case-sensitive letters. For additional information, refer to the **Date and time format guidelines** section and following tables.

Date and time format guidelines

As you select a date and time format for your designated document key, keep in mind that key values cannot exceed 40 characters. Also, pattern letters are usually repeated because their number determines the exact presentation. Additional date and time formatting guidelines are as follows.

- **Text:** For formatting, if the number of pattern letters is 4 or more, the full form is used; otherwise a short or abbreviated form is used if available.
- **Number:** For formatting, the number of pattern letters is the minimum number of digits, and shorter numbers are zero-padded to this amount.
- **Year:** For formatting, if the number of pattern letters is 2, the year is truncated to 2 digits; otherwise the full form is used.
- **Month:** If the number of pattern letters is 3 or more, the month is interpreted as text; if less than three, the month is represented in number format.
- **General Time Zone:** Time zones are interpreted as text if they have names. For time zones representing a GMT offset value, use the following syntax :
  - **GMTOffsetTimeZone:** GMT Sign Hours : Minutes
  - **Sign:** one of: [+ | -]
  - **Hours:** one of [Digit | Digit Digit]
  - **Minutes:** Digit Digit
  - **Digit:** one of: [0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9]
- **RFC 822 Time Zone:** For formatting, the RFC 822 4-digit time zone format is used:
  - **RFC822TimeZone:** Sign TwoDigitHours Minutes

TwoDigitHours: Digit Digit Table 1: Date and Time Syntax

Character	Date or Time Component
G	Era designator
y	Year
M	Month in year
w	Week in year
W	Week in month
D	Day in year
d	Day in month
F	Day of week in month
E	Day in week
a	AM/PM marker
H	Hour in day (0-23)
k	Hour in day (1-24)
K	Hour in AM/PM (1-11)
h	Hour in AM/PM (1-12)
m	Minute in hour
s	Second in minute
S	Millisecond
z	General time zone
Z	RFC 822 time zone

Table 2: Date and Time Format Examples

Example Variable	Result
yyyy.MM.dd G 'at' HH:mm:ss z	2001.07.04 AD at 12:08:56 PDT
EEE, MMM d, 'yy	Wed, Jul 4, '01
h:mm a	12:08 PM
hh 'o''clock' a, zzzz	12 o'clock PM, Pacific Daylight Time
K:mm a, z	0:08 PM, PDT
yyyyy.MMMMM.dd GGG hh:mm aaa	02001.July.04 AD 12:08 PM
EEE, d MMM yyyy HH:mm:ss Z	Wed, 4 Jul 2001 12:08:56 -0700
yyMMddHHmmssZ	010704120856-0700

Appendix B: emailAgent.ini

The following table provides definitions and setting options for the emailAgent.ini configuration file. This table displays the INI settings under group headings in brackets, for example, [Remote], in the order the groups appear in the INI file. Each setting offers two or more options, which the table defines below along with a description of each setting and its options. Unless otherwise noted, the default setting is blank.

Group	Setting	Options	Description
Remote	integrationserver.base.url	Any valid IP address or hostname	Specifies the IP address or hostname of Perceptive Content Integration Server. For example: http://123.12.123.10:8080/integrationserver
	integrationserver.authentication.token	Any valid token	Specifies the authentication token to use for authentication with Integration Server.
	imap.fetchsize	Any positive integer	The amount of bytes to fetch at once when downloading attachments on the imap protocol. The default is 16. The minimum setting is 16 kilobytes (KB). **Note** Setting this number too high may cause out-of-memory errors. Example 1: imap.fetchsize = 256 Example 2: imap.fetchsize = 2000 (~2 megabytes) Example 3: imap.fetchsize = 200000 (~2 gigabytes)
Logging	level	error warn info debug	Specifies the logging level associated with Email Agent. error = Log only error messages. warn = Log only error and warning messages. info = Log error, warning, and info messages. debug = Log error, warning, info, and debug messages. The default is **error**. **Note** Log files are stored in the **\log** directory in the Email Agent installation directory.
	policy.type	time size	Specifies the type of policy used to roll over log files. time = The log file will roll over based on the period of time indicated by its policy.time.rolloverperiod setting. This policy will archive the newest number of logs equal to the policy.time.maxhistory setting, or it will archive all logs if the policy.time.maxhistory is omitted. The log archive pattern is determined by the precision of the policy.time.rolloverperiod setting. size = The log file will roll over based on its size in MB indicated by the policy.size.maxmbsize setting. This policy will archive the newest number of logs equal to the policy.size.maxlogstokeep setting. The log archive pattern is "log.name".%i.zip, where lower '%i' values represent newer logs.

Group	Setting	Options	Description
	policy.time.rolloverperiod	minute hour day week month	Specifies the amount of time between log rollover events. minute = The log will roll over every minute. hour = The log will roll over every hour. day = The log will roll over every day. week = The log will roll over every week. month = The log will roll over every month. Archive patterns minute = [log file name].%d{yyyy-MM-dd_HH-mm}.zip hour = [log file name].%d{yyyy-MM-dd_HH}.zip day = [log file name].%d{yyyy-MM-dd}.zip week = [log file name].%d{yyyy-MM-ww}.zip month = [log file name].%d{yyyy-MM}.zip **Note** Larger rollover periods may result in prohibitively large log files. **Note** This setting is required when policy.type is set to time.
	policy.time.maxhistory	integer	Optional. Specifies the maximum number of log files archived when policy.type is set to time. **Note** By omitting this setting, Email Agent will archive all log files.
	policy.size.maxmbsize	integer	Specifies the maximum number of MB a log file can reach before triggering a rollover event. **Note** This setting is required when policy.type is set to size.
	policy.size.maxlogstokeep	integer	Specifies the maximun number of log files archived when policy.type is set to size. **Note** This setting is required when policy.type is set to size and has a maximum value of 20.
	enabled	TRUE FALSE	Specifies whether the email account is enabled or disabled. TRUE = Monitor the associated email account. FALSE = Do not monitor the associated email account. When disabled, Email Agent ignores all settings under the email<n> group. The default is TRUE.

Group	Setting	Options	Description
Email<n>	createprofilelog	TRUE FALSE	Enable or disable this profiles isolated log. When enabled, the logger writes all events in this profile and the main email agent a separate log file in addtion to the “email.agent.all.log". This isolated log's name is "email.agent.(profilename).log", and its archiving behavior matches the configurations from the [Logging] settings. The default setting is false. Ex: for profile [email0], the profile's log is "email.agent.email0.log".
	work.type	ALWAYS SCHEDULED	Specifies whether Email Agent monitors the associated email account constantly or on a scheduled basis. ALWAYS = Provide continuous monitoring and ignore work.time.start and work.time.stop settings. SCHEDULED = Monitor the associated email account between the times specified by work.time.start and work.time.end settings. The default is ALWAYS.
	work.time. start	4-digit time in 24-hour format	Specifies the time Email Agent begins to monitor the email account in 24-hour format. For example, 0800 is 8:00 AM, 2000 is 8:00 PM. The default is 0000. **Note** Email Agent ignores this setting if work.type = ALWAYS.
	work.time. stop	4-digit time in 24-hour format	Specifies the time Email Agent ceases to monitor the email account in 24-hour format. For example, 0800 is 8:00 AM, 2000 is 8:00 PM. The default is 2359. **Note** Email Agent ignores this setting if work.type = ALWAYS.
	server. <incoming, outgoing>	Any valid IP address or hostname	Specifies the hostname or IP address of the incoming or outgoing email server that Email Agent monitors. For example, a server name, server@domain.com, or the IP address, 168.34.151.3.

Group	Setting	Options	Description
	server. incoming. protocol	POP3 POP3S GIMAP IMAP IMAPS EWS EWSCS EWSROPC	Specifies the connection protocol Email Agent uses when connecting to the mail server. The default is POP3. The ews, pop3, pop3s, imap, and imaps protocols use Basic auth to connect to the incoming server. Basic Auth protocols require the **server.incoming.password** field. The ewscs setting is used for Exchange Servers with the client-secret EWS Oauth 2.0 grant flow. The ewsropc setting is used for Exchange Servers with the Resource Owner Password Credentials (ROPC) EWS Oauth 2.0 grant flow. EWS OAuth protocols require the **server.incoming.clientid** and **server.incoming.tenantid** fields. The gimap protocol uses GSuite service account authentication and requires the **server.incoming.credentialspath** field. Gimap also uses its own SSL encryption and ignores the **server.incoming.encryption.protocols** and **server.incoming.starttls** settings
	server. outgoing. protocol	GSMTP SMTP SMTPS EWS EWSCS EWSROPC	Specifies the connection protocol Email Agent uses when connecting to the mail server. Use SMTPS for TLS encryption. The default is SMTP The ews, smpt, and smtps protocols use Basic auth to connect to the incoming server. Basic Auth protocols require the **server.outgoing.password** field. The ewscs setting is used for Exchange Servers with the client-secret EWS Oauth 2.0 grant flow. The ewsropc setting is used for Exchange Servers with the Resource Owner Password Credentials (ROPC) EWS Oauth 2.0 grant flow. EWS OAuth protocols require the **server.outgoing.clientid** and **server.outgoing.tenantid** fields. The gsmtp protocol uses GSuite service account authentication and requires the **server.outgoing.credentialspath** field. Gsmtp also uses its own TLS encryption and ignores the **server.outgoing.encryption.protocols** and **server.outgoing.starttls settings**.
	server. <incoming, outgoing>. port	Any valid port number	Specifies the incoming or outgoing mail server's port number. **Note** By default, GIMAP servers use port 993, GSMTP servers use port 587, POP3 servers use port 110 and SMTP servers use port 25.
	server. <incoming, outgoing>. username	User name	Specifies the user name that Email Agent uses to connect to the incoming or outgoing mail server.

Group	Setting	Options	Description
	server. <incoming, outgoing>. password	Password	Specifies the password Email Agent uses to connect to the incoming or outgoing mail server. This setting is required when using basic auth with any email server, or when using ROPC OAuth. This setting is not allowed when using client-secret EWS OAuth or when using GIMAP or GSMTP. **Note** Passwords are encrypted and the unencrypted password is overwritten in the INI.
	server. <incoming, outgoing>. clientid	Application's client ID in the server's environment	The client ID to use when connecting to the email server using OAuth 2.0. This setting is not allowed if this server's protocol does not support EWS OAuth 2.0.
	server. <incoming, outgoing>. tenantid	The user's tenant name or ID	The tenant ID to use when connecting to the email server using OAuth 2.0. This setting is not allowed if this server's protocol does not support EWS OAuth 2.0.
	server. <incoming, outgoing>. clientsecret	The application's client secret in ther server's environment	The client secret to use when connecting to the email server as a client when using OAuth 2.0. This setting is not allowed if this server's protocol does not support EWS OAuth 2.0 or the server is using the ROPC OAuth 2.0 flow. **Note** client secrets are encrypted and the unecrypted secret is overwritten in the INI.
	Server. <incoming, outgoing>, credentialspath	The path to a json GSuite service account credentials file	The path to the json GSuite service account credentials file to use when connecting to the email server using the GIMAP or GSMTP protocols. This setting is not allowed if the protocol only supports basic auth or if the protocol uses EWS OAuth.
	server. incoming. interval	Any positive integer	Specifies the frequency in seconds Email Agent polls the incoming mail server for new email messages. The default is 60.
	server. incoming. disconnectdelay	Any positive integer	Specifies the number of seconds Email Agent waits after disconnecting from the email server. The default is 1. **Note** Do not modify this setting unless an "EOF on socket error" message occurs in the Email Agent log file. If such an error occurs, increase the number of seconds in this setting.
	server. <incoming, outgoing>. encryption. protocols	SSLv3 TLSv1 TLSv1.2	Specifies the list of supported protocols with which to negotiate when connecting to the incoming mail server. Each item in the list is separated by a space. This setting is ignored when using GIMAP or GSMTP. The default is SSLv3

Group	Setting	Options	Description
	server. <incoming, outgoing>. starttls	TRUE FALSE	Specifies that Email Agent will enable TLS encryption using an existing unencrypted connection with the mail server. This flag is not necessary if the port is already using TLS. TRUE = TLS encryption will be utilized with the mail server. STARTTLS must also be enabled on the mail server. FALSE = TLS encryption will not be utilized with the mail server. This setting is ignored when using GIMAP or GSMTP. The default is FALSE
	server.incoming. ignore. certificates	TRUE FALSE	Specifies whether to ignore certificate validity. This is useful if the mail server is internal and there is not a concern about the validity of certificates. TRUE = Ignore certificates, and import email regardless of the validity of the certificate. FALSE = Import only email with valid certificates. The default is FALSE. **Note** When using EWS protocol, a self-signed certificate's expiration date is always verified.
	server. <incoming, outgoing>. mailconnection debug	TRUE FALSE	Specifies whether Email Agent provides additional debugging information specific to the incoming or outgoing mail server connection. TRUE = Log additional debug information. FALSE = Do not log additional debug information. The default is FALSE.
	server.incoming.log Headers	TRUE FALSE	Provides additional logging information for email message headers. The default setting is FALSE.
	server.incoming.log Attachments	TRUE FALSE	Provides additional logging information for email message attachments. The default setting is FALSE.
	server. <incoming, outgoing>. timeout. seconds	Any positive integer	Specifies the number of seconds before Email Agent stops attempting to connect to the incoming or outgoing mail server. The default is 30.

Group	Setting	Options	Description
	autoreply	TRUE FALSE	Specifies whether Email Agent automatically replies to incoming email senders. TRUE = Reply to email senders. FALSE = Ignore the autoreply.message setting and do not reply to senders. The default is FALSE.
	autoreply. message	Any text string	Specifies the auto reply message Email Agent sends when autoreply is set to TRUE.
	autoforward	TRUE FALSE	Specifies whether Email Agent automatically forwards incoming email. TRUE = Forward email. FALSE = Ignore the autoforward.email setting and do not forward email. The default is FALSE.
	autoforward. email	Valid email address	Specifies the receiving email address of forwarded email when autoforward is set to TRUE.
	notifyprocessfailure	TRUE FALSE	Sends a notification email to a configured user indicating that an error occurred while capturing data from an email message. The default is FALSE.
	notifyprocessfailure. email	STRING	Specifies the destination email address for the notification email. **Note** This setting is required when notifyprocessfailure is set to TRUE.
	movefailedmessage	TRUE FALSE	Specifies whether to move emails that failed to process into a specified folder within the server.incoming user's inbox. TRUE = Failed messages will be moved to the inbox folder designated in the movefailedmessage.foldername setting. FALSE = Failed messages will not be moved. The default setting is FALSE. **Note** This setting cannot be enabled for pop3 and pop3s server.incoming.protocols.

Group	Setting	Options	Description
	movefailedmessage.foldername	STRING	Specifies the name of the folder within the inbox to move emails that failed to process. For example, the following configuration will move email messages that failed to process to an inbox folder named EmailAgentFailures. movefailedmessage.foldername=EmailAgentFailures **Note** This setting is required when movefailedmessage is set to TRUE.
	replyemail	Valid email address	Specifies the email address to use as the sending email address when replying to or forwarding email messages. **Note** This setting is required if autoforward or autoreply is set to TRUE. The email address specified must be different from the addresses specified in other settings within the email<n> group. Otherwise, an endless loop of undeliverable email is sent to the email address Email Agent monitors.
	document.destination.type	DOCUMENT WORKFLOW	Specifies how Email Agent imports the email and associated attachments into Perceptive Content. DOCUMENT = Import email and attachments directly into Perceptive Content and ignore document.destination.queue WORKFLOW = Import email and attachments directly into a workflow queue defined in document.destination.queue. The default is DOCUMENT.
	document.destination.queue	Workflow queue	Specifies the workflow queue into which Email Agent imports email and attachments. **Note** This setting is required if document.destination.type is set to WORKFLOW.
	document.destination.queue.priority	LOW MEDIUM HIGH	Specifies the priority Email Agent assigns to items it adds to the Workflow queue. The default is MEDIUM.
	document.keys.drawer.default	Drawer name	Specifies the default drawer Email Agent uses if document.keys.drawer.type is neither empty nor set to LITERAL and the specified drawer value is missing or invalid. The default drawer specified must exist in Perceptive Content. The default is DEFAULT.

Group	Setting	Options	Description
	document.keys.drawer.type	LITERAL FIELD FUNCTION	Specifies how Email Agent determines the drawer value for an email. LITERAL = Populate the drawer name with the value in document.keys.drawer. FIELD = Populate the drawer name based on text from the email, as defined in document.keys.drawer. FUNCTION = Populate the drawer name by defining the function in document.keys.drawer.
	document.keys.drawer	Multiple, see description	Specifies the value used for drawer keys. The options for this setting depend on the type specified in document.keys.drawer.type. **Note** The drawer key is limited to 40 characters. If document.keys.drawer.type is set to: LITERAL Specify a text string for Email Agent to use as the drawer key. FIELD Specify one of the following sections of the email for Email Agent to use as the drawer key: FROM = Populate the drawer key with the email's From field. TO = Populate the drawer key with the email's To field. CC = Populate the drawer key with the email's CC field. SUBJECT = Populate the drawer key with the email's Subject field. REPLY_TO = Populate the drawer key with the email's Reply To field. ATTACHMENT_COUNT = Populate the drawer key with the number of attachments included in the email. FUNCTION Specify the function in the following format: search(field, searchString, offset, [EOL OR numberOfCharacters]), where: field = from, to, cc, subject, send_date, reply_to, body, or attachment_count; searchString = the string to search for; offset = the number of characters to skip after the searchString; EOL = capture all characters to the end of the line; numberOfCharacters = a specific number of characters to capture.

Group	Setting	Options	Description
	document.keys.drawer.addressformat	address = email address only, friendly = email friendly name from the address, both = friendly + *<address>*	Specfies how Email Agent configures the email address format if document.keys.drawer.type=field and document.keys.drawer=CC, TO, or From The default is ADDRESS. **Note** The document type is limited to 40 characters.
	document.keys.documentType.default	Any existing document key	Specifies the default document type if document.keys.documentType.type is neither empty nor set to LITERAL. The default is DEFAULT. **Note** The document type specified must be an existing document type in Perceptive Content.
	document.keys.documentType.type	LITERAL FIELD FUNCTION	Specifies how Email Agent determines the document type associated with an email. LITERAL = Populate the document type with the value specified in document.keys.documentType. FIELD = Populate the document type with text from the email, as specified in document.keys.documentType. FUNCTION = Populate the document type through the function specified in document.keys.documentType.

Group	Setting	Options	Description
	document.keys.documentType	Multiple, see description	Specifies values for the document type. The options for this setting depend on the type specified in document.keys.documentType.type. **Note** The document type is limited to 40 characters. If document.keys.documentType.type is set to: LITERAL Specify a text string for Email Agent to use as the document type. FIELD Specify one of the following sections of the email for Email Agent to use as the document type: FROM = Populate the document type with the email's From field. TO = Populate the document type with the email's To field. CC = Populate the document type with the email's CC field. SUBJECT = Populate the document type with the email's Subject field. REPLY_TO = Populate the document type with the email's Reply To field. ATTACHMENT_COUNT = Populate the document type with the number of attachments included in the email. FUNCTION Specify the function in the following format: search(field, searchString, offset, [EOL OR numberOfCharacters]), where: field = from, to, cc, subject, send_date, reply_to, body, or attachment_count; searchString = the string to search for; offset = the number of characters to skip after the searchString; EOL = capture all characters to the end of the line; numberOfCharacters = a specific number of characters to capture.

Group	Setting	Options	Description
	document.keys.documentType.addressformat	address = email address only, friendly = email friendly name from the address, both = friendly + *<address>*	Specifies how Email Agent configures the email address format if document.keys.documentType.type=field and document.keys.documentType=CC, TO, or From. The default is ADDRESS. **Note** The document type is limited to 40 characters.
	document.keys.field1.type document.keys.field2.type document.keys.field3.type document.keys.field4.type document.keys.field5.type.	LITERAL FIELD UNIQUEID TIMESTAMP UNDEFINED SERIAL FUNCTION	Specifies how Email Agent determines document key values used for fields 1, 2, 3, 4, or 5, depending on the specific setting used. LITERAL = Populate the document key with the string specified in document.keys.[field<1,2,3,4,5>]. FIELD = Populate the document key with text from the email. UNIQUEID = Populate the document key with a unique ID. TIMESTAMP = Populate the document key with the current timestamp based on the user-defined document.keys.[field<1,2,3,4,5>].dateformat. UNDEFINED = Ignore the document key. SERIAL = Populate the document key based on the serial settings in document.keys.[field<1,2,3,4,5>].type.serial.format and document.keys.[field<1,2,3,4,5>].type.serial.start. FUNCTION = Populate the document through the function specified in document.keys.[field<1,2,3,4,5>].

Group	Setting	Options	Description
	document.keys.field1 document.keys.field2 document.keys.field3 document.keys.field4 document.keys.field5	Multiple, see description	Specifies values for the document key. The value options for this setting depend on the option specified in document.keys.[field<1,2,3,4,5>].type. **Note** The document key is limited to 40 characters. If document.keys. [field<1,2,3,4,5>].type is set to: LITERAL Specify a text string for Email Agent to use as the document key. FIELD Specify one of the following sections of the email for Email Agent to use as the document key: FROM, TO, CC, SUBJECT, REPLY_TO, BODY SEND_DATE = Populate the document key with the date the email was sent. ATTACHMENT_COUNT = Populate the document key with the number of attachments included in the email. UNIQUEID, TIMESTAMP, UNDEFINED Ignore this setting. SERIAL Ignore this setting but require document.keys.[field<1,2,3,4,5>].type.serial.format and document.keys.[field<1,2,3,4,5>].type.serial.start FUNCTION Specify the function in the following format: search(field, searchString, offset, [EOL OR numberOfCharacters]), where: field = from, to, cc, subject, send_date, reply_to, body, or attachment_count; searchString = Specify the string to search for; offset = Specify the number of characters to skip after the searchString; EOL = Capture all characters to the end of the line; numberOfCharacters = Specify the number of characters to capture.

Group	Setting	Options	Description
	document. keys. [field<1,2,3,4,5>]. type.serial.format	Multiple, see description	Specifies the format of the serial data value Email Agent uses to populate the associated key. This setting is required if document.keys.[field<1,2,3,4,5>].type is set to SERIAL. # = zeros are omitted. 0 = zeros are displayed. All other values are considered constants. Examples: document.keys.[field<1,2,3,4,5>].type.serial.format = #,### If the value=1984; then key=1,984 document.keys. [field<1,2,3,4,5>].type.serial.format = 000.00 If the value=30.5; then key=030.50 document.keys. [field<1,2,3,4,5>].type.serial.format = #,###.00 If the value=982.1; then key=982.10

Group	Setting	Options	Description
	document.keys.[field<1,2,3,4,5>].type.serial.start	Any positive integer	Specifies the starting serial value. This setting is required if document.keys.[field<1,2,3,4,5>].type is set to SERIAL. **Note** Email Agent automatically updates the document.keys.[field<1,2,3,4,5>].type.serial.start setting as it processes email messages. Thus if the start value is originally set to 10, Email Agent sets the setting to 31 after 20 email have been processed.
	document.keys.field[1-5].addressformat	address = email address only, friendly = email friendly name from the address, both = friendly + *<address>*	Specfies how Email Agent configures the email address format if document.keys.field[1-5].type=field and document.keys.field[1-5]=CC, TO, or From
	document.keys.[field<1,2,3,4,5>].dateformat	Multiple, see description	Specifies the dateformat setting to use if document.keys.[field<1,2,3,4,5>].type is set to TIMESTAMP or document.keys[field<1,2,3,4,5>].type is set to FIELD with document.keys[field<1,2,3,4,5,>] set to SEND_DATE. The default is EEE MMM d HH:mm:ss zzz yyyy For example: Thu Jan 15 09:20:27 GMT-06:00 2004 Date and time formats are specified by date and time pattern strings represented by the case-sensitive letters in Appendix A, “Specify date and time formats for automatic indexing.” Surround text using single quotes (') to avoid interpretation. Characters not defined in the table in Appendix A are not interpreted. Repeated pattern letters define the display format based on the pattern types. Refer to the **emailAgent.ini** file for more information.

Group	Setting	Options	Description
	document.notes.type	LITERAL FIELD UNIQUEID TIMESTAMP UNDEFINED SERIAL FUNCTION	Specifies the method that Email Agent uses to determine document notes. This setting is used in the document.notes setting. LITERAL = Populate the notes with a text string. FIELD = Populate the notes with text from a specific location in the imported email message. UNIQUEID = Populate the notes with a unique ID. TIMESTAMP = Populate the notes with the current timestamp. UNDEFINED = Ignore the notes settings. SERIAL = Populate the notes with a serial number. FUNCTION = Populate the notes by using the defined function. **Note** The document notes settings require Perceptive Integration Server 7.1.3 or higher.

Group	Setting	Options	Description
	document.notes	LITERAL FIELD UNIQUEID TIMESTAMP UNDEFINED SERIAL FUNCTION	Specifies values for the document notes. Available options depend on the setting in document.notes.type. If document.notes.type is set to: LITERAL Specify a text string for Email Agent to use as the notes. FIELD Specify any number of the following sections of the email for Email Agent to use as the notes with multiple sections separated by a pipe (|): FROM, TO, CC, SUBJECT, SEND_DATE, REPLY_TO, BODY ATTACHMENT_COUNT uses the number of attachments included in the email. ENTIRE_HEADER uses each item in the email header, separated by |. Subheaders are separated by a comma. UNIQUEID, TIMESTAMP, UNDEFINED This setting is ignored SERIAL Email Agent ignores this setting but requires document.notes.type.serial.format and document.notes.type.serial.start. FUNCTION Specify the function in the following format: search(field, searchString, offset, [EOL OR numberOfCharacters]), where: field = from, to, cc, subject, send_date, reply_to, body, or attachment_count; searchString = the string to search for; offset = the number of characters to skip after the searchString; EOL = Capture all characters to the end of the line; numberOfCharacters = Specify the number of characters to capture.
	document.notes.addressformat	Valid email address, user-defined friendly name, or both	Specfies how Email Agent configures the email address format if document.notes.type=field and document.notes=CC, TO, or From

Group	Setting	Options	Description
	document.notes.type.serial.format	Multiple, see description	Specifies the format of the serial data value Email Agent uses to populate the associated notes. This setting is required if document.notes.type is set to SERIAL. # = zeros are omitted. 0 = zeros are displayed. All other values are considered constants. Examples: document.notes.type.serial.format= #,### If the value=1984; then key=1,984 document.notes.type.serial.format=000.00 If the value=30.5; then key=030.50 document.notes.field3.type.serial.format= #,###.00 If the value=982.1; then key=982.10
	document.notes.type.serial.start	Any positive integer	Specifies the starting serial value. This setting is required if document.notes.type is set to SERIAL. **Note** Email Agent automatically updates the document.notes.type.serial.start setting as it processes email messages. For example, if the start value is originally set to 10, Email Agent sets the setting to 31 after 20 emails are processed.
	document.notes.dateformat	Multiple, see description	Specifies the dateformat setting to use if document.notes.type is set to TIMESTAMP or document.notes.type is set to FIELD with document.notes set to SEND_DATE. The default is EEE MMM d HH:mm:ss zzz yyyy For example: Thu Jan 15 09:20:27 GMT-06:00 2004 Date and time formats are specified by date and time pattern strings represented by the case-sensitive letters in Appendix A, “Specify date and time formats for automatic indexing.” Text can be quoted using single quotes (') to avoid interpretation. Characters not defined in Appendix A are not interpreted. Repeated pattern letters define the display format based on the pattern types.

Group	Setting	Options	Description
	document.email	TRUE FALSE	Specifies whether Email Agent imports email messages into the Perceptive Content Server. TRUE = Import email messages and attachments. FALSE = Import email attachments but not email messages. **Note** This is a required setting. The default is TRUE.
	document. emailheader	TRUE FALSE	Specifies whether Email Agent includes email header information with the imported email body text. TRUE = Include email header information with the imported body text. FALSE = Do not include email header information with the imported body text. **Note** This is a required setting if document.email is set to TRUE. The default is TRUE.
	document. emailfooter	TRUE FALSE	Specifies whether Email Agent includes attachment file names at the end of the email body text. TRUE = Include attachment file names. FALSE = Do not include attachment file names. **Note** This is a required setting if document.email is set to TRUE. The default is TRUE.
	document. emailPrefer HTML	TRUE FALSE	Specifies whether Email Agent retains embedded links as HTML for documents imported using Email Agent. The default is FALSE.
	document. inline	TRUE FALSE	Specifies whether Email Agent imports inline graphics as separate pages. Inline graphics are included within the body of an email message, such as a company logo. TRUE = Import inline graphics as a separate page. FALSE = Do not import inline graphics as a separate page. The default is TRUE.

Group	Setting	Options	Description
	document.inline.attachments.include	Any file extensions	Optional. Specifies the list of file extensions to include when importing inline attachments. If the property is not set, then all file extensions are included. Notes The documents.attachments setting must be set to TRUE to use this property. Inline attachments are not included if it is on the documents.attachments.exclude list, even if it is on this list. Email Agent does not include inline graphics with attachment_count.
	document.attachments	TRUE FALSE	Specifies whether Email Agent imports email attachments. TRUE = Import attachments. FALSE = Do not import attachments and ignore document.attachments.exclude. The default is TRUE.
	document.attachments.exclude	Any file extensions	When document.attachments is set to TRUE, this option specifies which file extensions Email Agent excludes during automatic importing of email attachments. For security reasons, consider excluding the following file types: bat, exe, com, pdf, cmd, js, vbs, zip, dll, sit.
	document.attachments.mode	SINGLE_DOCUMENT MULTI_DOCUMENT	Specifies whether Email Agent stores an email and its associated attachments and inline graphics as a single Perceptive Content document or separate Perceptive Content documents. SINGLE_DOCUMENT = Store the email message and any attachments as a single Perceptive Content document. MULTI_DOCUMENT = Store the email message and any attachments as separate documents. Notes about the MUTLI_DOCUMENT option: At least one document key must be unique (such as a UNIQUEID or SERIAL value); otherwise the email and any attachments are stored as a single Perceptive Content document. If a workflow queue has been assigned, each document is sent to the specified workflow queue. The default is SINGLE DOCUMENT.

Group	Setting	Options	Description
	document.tiff.split	TRUE FALSE	Specifies whether Email Agent splits multi-page TIFF images into individual images. TRUE = Split multi-page TIFF images into individual TIFF images. FALSE = Do not split multi-page TIFF images. The default is FALSE.
	document.tiff. keepsplittiffs insamedocument	TRUE FALSE	Specifies whether Email Agent stores split TIFF documents in the same Perceptive Content document. **Note** This setting is required if document.attachments.mode is set to MULTI_DOCUMENT and document.tiff.split is set to TRUE. TRUE = Store each of the pages from a multi-page TIFF file as individual pages in a single Perceptive Content document. FALSE = Store each page of a TIFF image as a separate Perceptive Content document. The default is TRUE.
	rfc822.extension	Any file extension	Messages with the content type of MESSAGE/RFC822 will be saved using this extension when an extension is not provided by the sender. For example, rfc822.extension=eml The default extension is .eml.
	inline.disposition. mime.types	Any mime type	Specifies the mime types to include as inline attachments when the email message does not provide the disposition header. Any excluded mime types are handled as regular attachments. For example, image/png and image/jpeg.
	email.address.extra ction.mode	Ignore Strict Strip_Invalid_ Characters	Specifies how Email Agent imports email addresses that do not conform to the RFC 5322 address specification Ignore = Addresses import as they are received from the email. Strict = The email with non-standard email addresses are skipped. This is the default behavior for IMAP and POP3 protocols. Strip_Invalid_Characters = The email is not skipped. Extra quotes and trailing periods are stripped from the email address. **Note** EWS protocol does not support strict address mode and defaults to Ignore.

Appendix C: Update Email Agent

When you update Email Agent, run the same steps as if you are installing a new version.

Updating Email Agent

When updating Email Agent you must change a setting in the **[email]** group in the **emailAgent.ini** file for each custom email account you are monitoring.

- Change **server.incoming.ignoresslcertificates** to **server.incoming.ignore.certificates**

Enable Transport Layer Security

To enable Transport Layer Security (TLS) you must make changes in the **emailAgent.ini** file. For all email accounts Email Agent monitors, which includes the default accounts **[email0]** and **[email1]** as well as each custom email account, you must change the following value:

- For the setting **server.incoming.protocol**, change the value **imap** or **pop3** to **imaps** or **pop3s**

During the update, new settings are automatically added to the default accounts **[email0]** and **[email1]**, but for each custom email account Email Agent monitors, you must add the following settings.

Group	Setting	Options	Description
Email<n>	server. outgoing. protocol	SMTP SMTPS	Specifies the connection protocol used when connecting to the mail server. Use SMTPS for TLS encryption. The default is SMTP
	server. <incoming, outgoing>. encryption. protocols	SSLv3 TLSv1 TLSv1.1 TLSv1.2	Specifies the list of supported protocols with which to negotiate when connecting to the incoming mail server. Each item in the list is separated by a space. The default is SSLv3
	server. <incoming, outgoing>. starttls	TRUE FALSE	Specifies that Email Agent will enable TLS encryption using an existing unencrypted connection with the mail server. This flag is not necessary if the port is already using TLS. TRUE = TLS encryption will be utilized with the mail server. STARTTLS must also be enabled on the mail server. FALSE = TLS encryption will not be utilized with the mail server. The default is FALSE

Note If you had previously renamed **[email0]** and **[email1]**, those accounts are added back to the **emailAgent.ini** file with the new settings.

Appendix D: Non-interactive Gmail OAuth setup

After June 15, 2020, Google will limit the ability for less secure apps (LSAs) to access G Suite account data. LSAs are non-Google apps that can access your Google account with only a username and a password.

After February 15, 2021 Google will turn off access to LSAs for all G Suite accounts (G Suite Updates). The IMAP mail protocol with BasicAuth falls under the LSA category, so our email services need a noninteractive way to perform OAuth IMAP operations.

This section covers the steps required to setup a G Suite to handle noninteractive OAuth for the Suite's managed Gmail accounts using service accounts and G Suite application whitelisting.

Overview

The following is an overview of the steps you need to complete.

1. Create a project
2. Enable the Gmail API for the project
3. Configure the project's OAuth consent screen
4. Create and configure a service account
5. Whitelist the service account's OAuth client

Create a project

Complete the following steps to create a project.

1. Go to **Google Cloud Platform (GCP) Console**.
2. If you have not used GCP Console before, in the **Google Cloud Platform** window, complete the following substeps.
    1. From the **Country** list, select the appropriate country.
    2. Under **Terms of Service**, select **I agree to the Google Cloud Platform Terms of Service, and the terms of service of any applicable services and APIs**.
    3. Click **Agree and Continue**.
    4. On the **Dashboard**, click **Create Project**.
3. If you have used GCP Console before, complete the following substeps.
    1. From the **Project** list, click the **Down** button.
    2. In the **Select a project** window, click **New Project**.
4. In the **New Project** window, complete the following substeps.
    1. In the **Project name** box, enter a unique name for your new project. Note that the Project ID cannot be changed after you create this project.
    2. In the **Location** box, select the appropriate location.
    3. Click **Create**.

Enable the Gmail API for the project

Complete the following steps to enable the Gmail API for the project.

1. Go to **Google Cloud Platform (GCP) Console**.
2. From the **Project** list, click the **Down** button and select the appropriate project.
3. Click the **Navigation** menu, select **APIs & Services** and then click **Library**.
4. In the **Search for APIs & Services** box, type **Gmail**.
5. From the results list, click **Gmail API**.
6. Click **Enable**.

Configure the project's OAuth consent screen

Complete the following steps to configure the project's OAuth consent screen.

1. Go to **Google Cloud Platform (GCP) Console**.
2. From the **Project** list, click the **Down** button and select the appropriate project.
3. Click the **Navigation** menu, select **APIs & Services** and then click **OAuth consent screen**.
4. If your project is new and does not have a configured consent screen, select **Internal** under **User Type** and then click **Create**.
5. If your project already has a configured consent screen, complete the following substeps.
    1. Under **User Type**, verify the user type is set to **Internal**.

       Note You must set the user type to internal to allow access to the sensitive Gmail auth scopes. If you cannot change an existing project's user type, then you must create a new project.
    2. Click **Edit App**.
6. In the **Application Name** box, enter a valid name for the application.
7. Under **Scopes for Google APIs**, click **Add scope**.
8. In the **Add scope** window, select **Gmal API** `https://mail.google.com` and click **Add**.

   Notes

   The Email Agent and Email Broker require full access through the `https://mail.google.com` scope for full read, write, send and delete permissions. However, other applications may be able to use the other, more granular Gmail API scopes to match their application requirements.

   You can configure any other settings in the **Add scope** window, but they are not required for the Email Agent and Email Broker services.
9. Click **Save**.

Create and configure a service account

Complete the following steps to create and configure a service account.

1. Go to **Google Cloud Platform (GCP) Console**.
2. From the **Project** list, click the **Down** button and select the appropriate project.
3. Click the **Navigation** menu, select **IAM & Admin** and then click **Service accounts**.

4. Click **Create Service Account**.
5. In the **Create service account** window, complete the following substeps.
    1. In the **Service account name** box, enter a name for the service account.
    2. Optional. In the **Service account description** box, enter a description for the service account.
    3. Click **Create**.
6. In the **Service account permissions (optional)** window, from the **Role** list, select **Project** and then click **Owner** and then click **Continue**.
7. In the **Grant users access to this service account (optional)** window, click **Create Key**.
8. In the **Create key (optional)** window, select **JSON** and then click **Create**. The system saves the private key to your computer. Keep this file for later use.

    Notes

    This file is the credentials file used by Email Agent and Email Broker.

    These credentials only exist in this file. If you delete or lose this file, you must remove the associated key from your service account and generate a new JSON credentials file.

    You can rename the credentials file for clarity since the file's name is not relevant to the authentication process.
9. In the **Private key saved to your computer** window, click **Close**.
10. In the **Grant users access to this service account (optional)** window, click **Done**.
11. In the **Service accounts for project <your project>** window, select the email that relates to the service account you just created and then from the **Actions** list, click **Edit**.
12. In the **Service account details** window, expand **Show Domain-Wide Delegation** and then select **Enable G Suite Doman-wide Delegation**.
13. Click **Save**.
14. In the **Service accounts for project <your project>** window, click **View Client ID**.
15. In the **Client ID for service account** window, locate and copy the **Client ID**. This ID is necessary to whitelist this servie account's OAuth client.

    Note If the **domain-wide delegation** setting is not displayed, you need to click the **Show Domain-wide Delegation** setting again.

Whitelist the service account's OAuth client

Complete the following steps to whitelist the service account's OAuth client.

1. Go to the **Google Admin Console**.
2. Click **Security**.
3. Under **Security**, click **Advanced settings** and then click **Manage API client setting**s.
4. In the **Manage API client access** window, in the **Client Name** box, enter the **Client ID** that you saved during the *Create and configure a service account* section.

    Note You must use the **Client ID** in this field, do not enter a new name.
5. In the **One or More API Scopes** box, enter the `https://mail.google.com/` scope.

6. Click **Authorize**.
7. After you whitelist the service account's OAuth client, you must configure the following settings in the emailAgent.ini configuration file.
   - Set **server.incoming.protocol** to **GIMAP** or **server.outgoing.protocol** to **GSMTP**.
   - Set **server.incoming.username** and **server.outgoing.username** to the user name that Email Agent uses to connect to the incoming and outgoing mail server.
   - Set **server.incoming.credentialspath** and **server.outgoing.credentialspath** to the json CSuite service account credentials file to use when connecting to the email server using the GIMAP or GSMTP protocols.

Appendix E: Non-interactive Office and Online Exchange OAuth setup

This section covers the steps required to setup an Azure Active Directory to handle noninteractive OAuth for the Office 365 and Online Exchange APIs.

You can use the **Exchange Web Services Resource Owner Password Credentials (EWSROPC)** or the **Exchange Web Service Client Secret** protocols to authenticate the Email Agent. The **EWSROPC** uses the users password for authentication and **EWSCS** uses an application's client secret for authentication.

Overview

The following is an overview of the steps you need to complete.

- Register an application

  Note You can use an existing application provided that has the correct API permissions configured in the following step.
- Configure API permissions
- Create a Client Secret

  Note EWSROPC does not need to generate a client secret since it uses the resource owners password instead of authenticating as the application.

Register an application

Complete the following steps to register an application.

1. Navigate to Microsoft Azure Active Directory.
2. Copy the **Tenant ID**. This is the value you will use when you configure the **server.incoming.tenantid** and **server.outgoing.tenantid** settings in the emailAgent.ini configuration file.
3. In the left pane under **Manage** click **App registrations.**
4. Click **New registration**.
5. In the **Name** box, enter the user-facing display name for your new application.
6. Under **Supported account types**, select **Accounts in this organizational directory only**.
7. Click **Register**.

Important Make note of the **Client ID**. This is the ID you will use when you configure the **server.incoming.clientid** and **server.outgoing.clientid** settings in the emailAgent.ini configuration file.

Configure API permissions

Complete the following steps to configure API permissions.

1. Navigate to Microsoft Azure Active Directory.
2. In the left pane, under **Manage**, click **App registrations.**
3. Under **All applications**, select the appropriate application. This is either the application you just regisitered or an existing application that you want to modify.
4. On the application page, in the left pane, click **Authentication.**
5. Under **Advanced settings** and **Allow public client flows**, select **Yes** to **Enable the following mobile and desktop flow**.
6. Click **Save.**
7. In the left pane, click **API permissions.**
8. Click **Add a permission**.
9. On the **Request API permissions** page, click the **APIs my organization uses** tab.
10. In the list, locate and select **Office 365 Exchange Online**.
11. To select the permissions for your desired authentication types, complete the following substeps.

    Note You can add both permissions if you want to support both authentication types in the same application

    1. For EWSCS auth, click **Application permissions** and then under **Other Permissions**, select **full_access_as_app**.

       Note When the **server.incoming.protocol** or **server.outgoing.prototcol** settings are set to **EWSCS**, you must create a client secret. For more information, refer to the Create a client secret topic.

    2. For EWSROPC auth, click **Delegated permissions,** expand **EWS** and then select **EWS.AccessAsUser.All**.

       Note When the **server.incoming.protocol** or **server.outgoing.prototcol** settings are set to **EWSROPC**, you must configure the **server.incoming.username**, **server.incoming.password**, **server.outgoing.username** and **server.outgoing.password** settings in the emailAgent.ini configuration file.
12. Click **Add permissions**.
13. Click **Grant admin consent for <DIRECTORY_NAME>** to accept the permissions.

Create a client secret

Complete the following steps to create a client secret.

1. Navigate to Microsoft Azure Active Directory.
2. In the left pane, under **Manage**, click **App registrations.**
3. Under **All applications**, select the appropriate application.

Note This is either the application you just regisitered or an existing application that you want to modify.

4. In the left pane, click **Certificates & secrets**.
5. Under **Client secrets**, click **New client secret**.
6. In the **Add a client secret** dialog box, complete the following substeps.
    1. In the **Description** box, enter a description for the new secret.
    2. Under **Expires**, select when you want the certificate to expire.

       Note If the secret expires, the Email Agent will not be able to authenticate until you generate a new secret.
    3. Click **Add**.
7. Under **Client secrets**, locate the secret you just created.
8. Copy the string from the **Value** column of your secret's row. This is the value you will use when you configure the **server.incoming.clientsecret** and **server.outgoing.clientsecret** settings in the emailAgent.ini configuration file.

Important This is the only opportunity to copy the client secret's value. Once you navigate away from this page, you can no longer access the value. If you lose the client secret's value, you must delete that secret and generate a new one.