



OAuth2 - Office 365 & Gmail

Quick Start Guide
version 1.0

Introduction

This document describes the requirements of the connector and provides the instruction on how to setup the connector for Capturing and Sending Emails.

Other essential configuration steps that are part of the basic ScannerVision features (e.g. installation, configuring Networking Settings, templates, Users, etc) are not covered by this document.

This document will cover a generic explanation of the Application Registration Process in Azure, however, the local Azure Administrator will be able to provide accurate information for each particular implementation.

This document will not cover the full configuration of the application in Google, only the part related to Gmail. Please refer to the Google OAuth 2.0 setup manual for this.

The Email Connector has been updated to make use of OAuth 2.0. This covers incoming emails via IMAP and outgoing emails via SMTP.

Requirements

The ScannerVision Email Connector requires minimum version of ScannerVision Server V9.8.0.1385 and HPN V9.7.4.1201. Setup of the app within Azure (App Registration) can only be done by the Microsoft Azure AD Administrator.

To be able to send and receive emails, the user needs to have the correct role and rights configured in the environment. Please contact your Azure AD administrator to get more information about this requirement.

Should you have any questions, please contact our support team at support@ubunye.com for assistance.

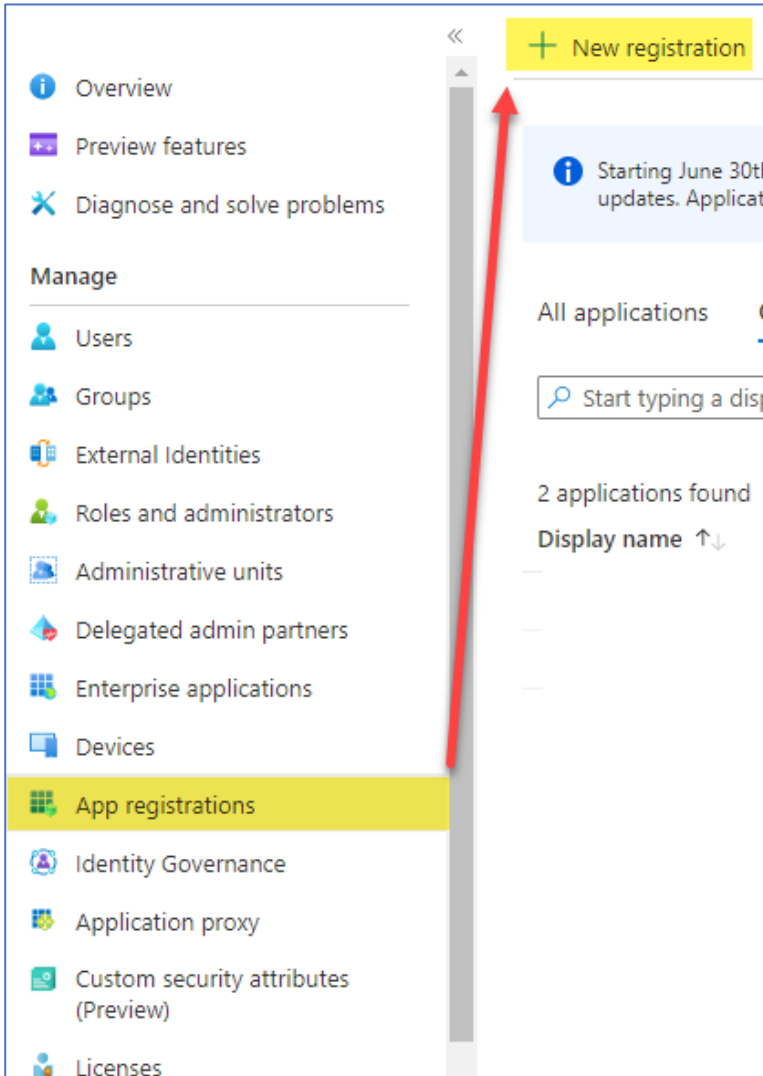
ScannerVision™

Application Registration (Azure AD)

Configuration

This section is based on a generic setup from Azure AD – Your company may have different settings. Please refer to your IT administrator for more information.

- Under **App Registration**, click **+ New Registration**.



Register an application ...

* Name
The user-facing display name for this application (this can be changed later).
Email Authentication ✓

Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (Single tenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
 Personal Microsoft accounts only
[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
Web ✓ http://localhost ✓

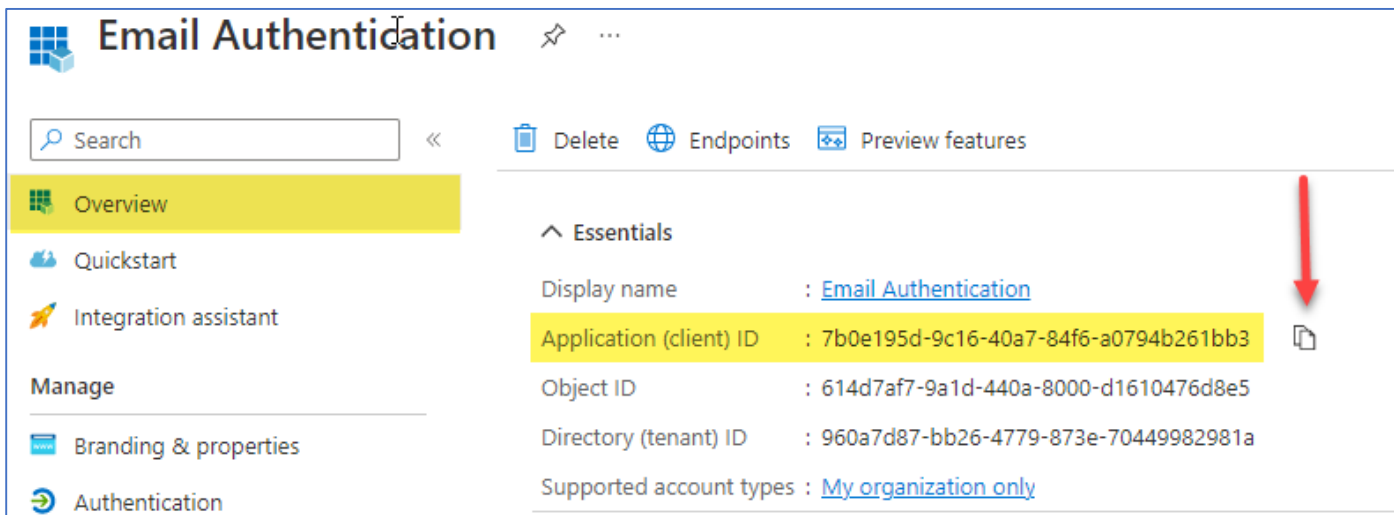
Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#) ↗

Register

- Give the application a name
- **Supported Account types** will normally be set as shown.
- **Redirect URI:**
 - Select: **WEB**
 - Enter: **http://localhost**
- Click **Register**

Note: Best Practice is to open a notepad application and cut and paste the following information ready to be input into the ScannerVision configuration screens.



Email Authentication

Search << Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Essentials

Display name : [Email Authentication](#)

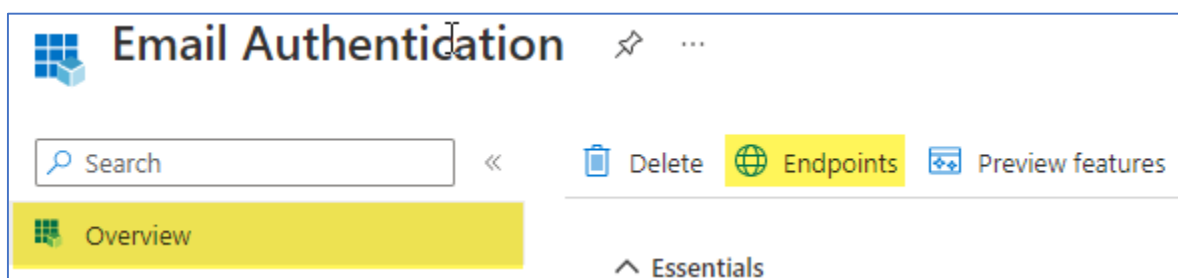
Application (client) ID : 7b0e195d-9c16-40a7-84f6-a0794b261bb3

Object ID : 614d7af7-9a1d-440a-8000-d1610476d8e5

Directory (tenant) ID : 960a7d87-bb26-4779-873e-70449982981a

Supported account types : [My organization only](#)

- Under **Overview** use the button indicated to copy the **Application (client) ID**
- **Paste into the notepad document.**
- Select **Endpoints**



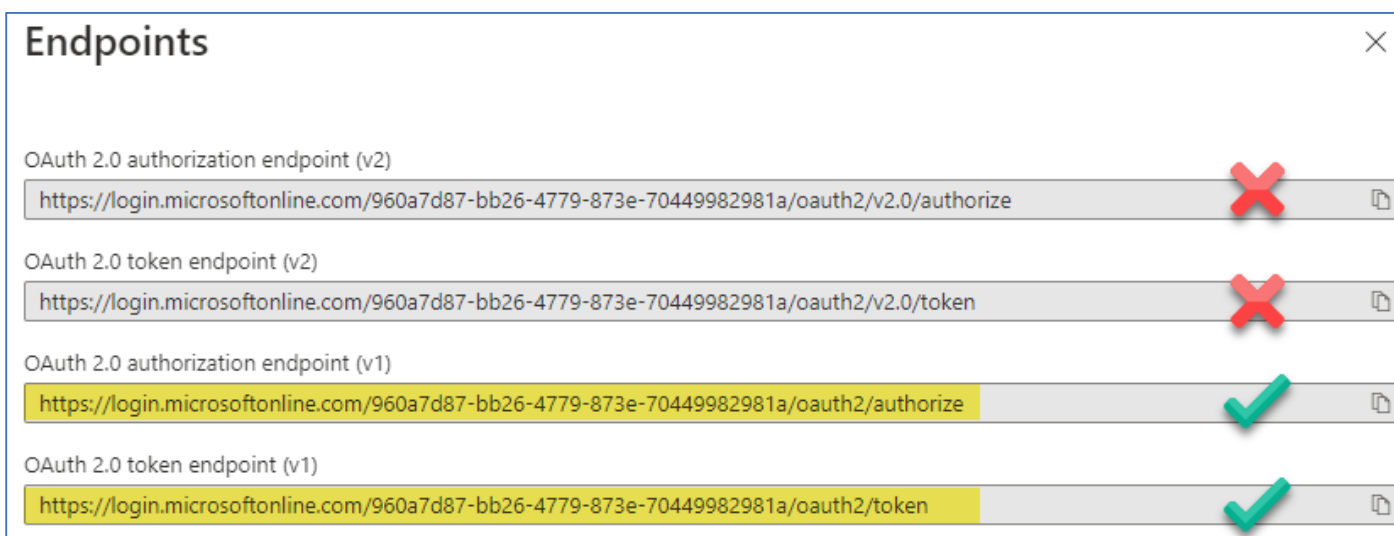
Email Authentication

Search << Delete Endpoints Preview features

Overview

Endpoints

Essentials



Endpoints

OAuth 2.0 authorization endpoint (v2)

<https://login.microsoftonline.com/960a7d87-bb26-4779-873e-70449982981a/oauth2/v2.0/authorize>

OAuth 2.0 token endpoint (v2)

<https://login.microsoftonline.com/960a7d87-bb26-4779-873e-70449982981a/oauth2/v2.0/token>

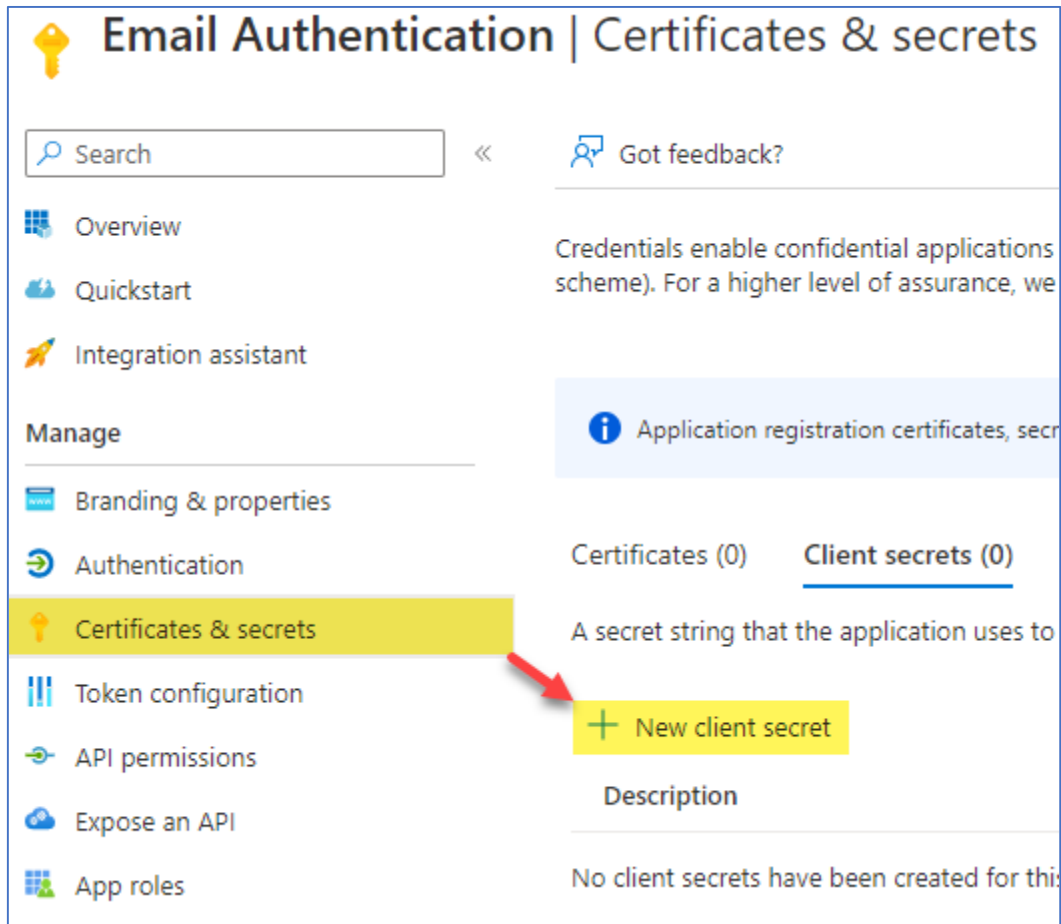
OAuth 2.0 authorization endpoint (v1)

<https://login.microsoftonline.com/960a7d87-bb26-4779-873e-70449982981a/oauth2/authorize>

OAuth 2.0 token endpoint (v1)

<https://login.microsoftonline.com/960a7d87-bb26-4779-873e-70449982981a/oauth2/token>

- Use the **Copy** button to copy **OAuth 2.0 authorization endpoint (v1)** – **Paste into the notepad document.**
- Use the **Copy** button to copy **OAuth 2.0 token endpoint (v1)** – **Paste into the notepad document.**



- Under **Certificates and Secrets**
 - Select + **New Client Secret**

- Provide a **Description**
- **Choose** an **expiry** duration
- Click **Add**

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
Email Secret Key	3/29/2023	XZd8Q~xRbvpB7I02MuAbanTxG7L66Mx...	5dada0df-ee39-4c15-9989-06375aa3e5b5

- Use the button indicated to copy the value *NOT* the ID
- Do NOT navigate away from this screen until you have copied the value as you will have to create a new secret code if you return later.
- **Paste into the notepad document:**

Email OAuth 2 | API permissions

Search Refresh Got feedback?

Overview Quickstart Integration assistant

Manage Branding & properties Authentication Certificates & secrets Token configuration **API permissions** Expose an API

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
IMAP.AccessAsUser.All	Delegated	Read and write access to mailboxes via IMAP.	No	Granted for
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for
SMTP.Send	Delegated	Send emails from mailboxes using SMTP AUTH.	No	Granted for

- Under **API permissions**, add the following permissions
 - IMAP.AccessAsUser.All
 - offline_access
 - SMTP.Send

Notes: - These options are found under **Microsoft Graph** and are **Delegated Permissions**

- Granting **Admin Consent** (optional) saves users from having to confirm permissions to get the token.

The configuration is complete. If you created a notepad document in the order described above, you should have a document ready with the settings to paste into the ScannerVision set up screens. It should look similar to this:

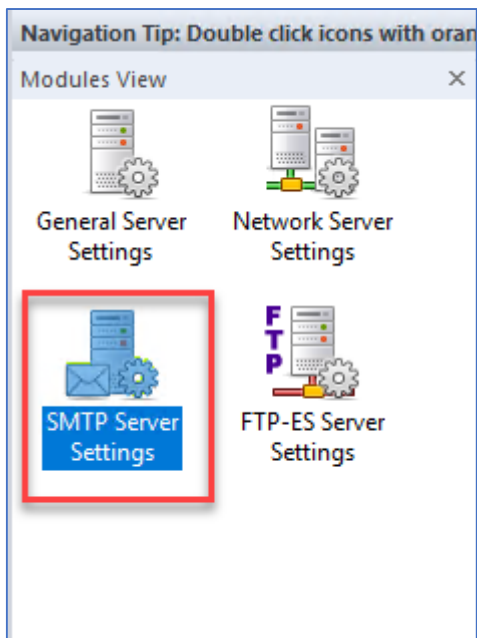
```
7b0e195d-9c16-40a7-84f6-a0794b261bb3
https://login.microsoftonline.com/960a7d87-bb26-4779-873e-70449982981a/oauth2/authorize
https://login.microsoftonline.com/960a7d87-bb26-4779-873e-70449982981a/oauth2/token
Xmc8Q~tf6pCmPYVhYNraCeb2XsU6ctUS1Jqz3cMq
```

The top item should be the - **Application (client) ID**

The last Item should be the – **Secret Key**

ScannerVision™

Outgoing (SMTP) Email Configuration



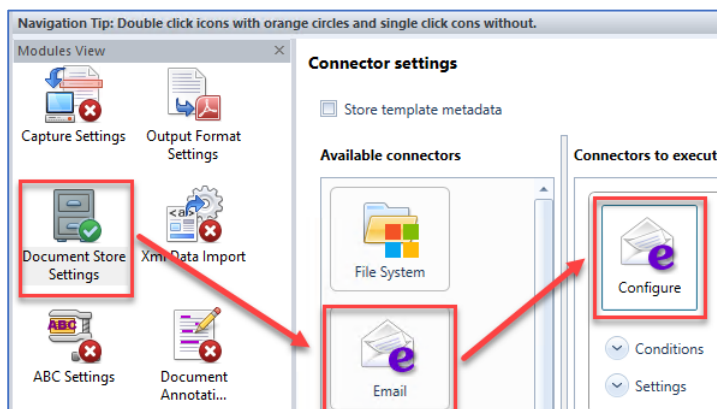
Configuration

An SMTP server can be configured in two areas:

- As the main SMTP Server.
- Per Template.

The settings are the same for each area.

- If configured as the main SMTP Server, all system related emails and notifications will be sent using this setting
- When configuring a template, you can select to use the main SMTP Server or enter new setting for a different server.



ScannerVision™

Outgoing (SMTP) Email Configuration

Email Connector Setup

Email SMTP Server

Use same settings as configured in main SMTP Server Settings

SMTP Server

SMTP Port

SSL/TLS

Encryption TLS 1.3 otherwise TLS 1.2

Authentication

Use OAuth

Configuration

These settings applicable in most cases.

***Please check with the Azure Administrator to confirm these settings where possible before configuration.**

If you have already configured the main SMTP server, you can select to use these settings or configure a new connection.

SMTP Server: The hostname of the server you will use – in most cases *SMTP.office365.com* is sufficient.

Port: Normally this will be set to **587**

SSL/TLS: Set to 'Start TLS'

Encryption: Auto

Authentication: Auto Detect

Select '**Use OAuth**'

ScannerVision™

Outgoing (SMTP) Email Configuration

User Name	<input type="text"/>
Authorization Endpoint	<input type="text"/>
Token Endpoint	<input type="text"/>
Client ID	<input type="text"/>
Client Secret	<input type="text"/>
Resource	<input type="text" value="https://outlook.office365.com"/>
Scope	<input type="text"/>
URL Suffix	<input type="text"/>
Redirect URI	<input type="text" value="http://localhost:56680"/>
<input type="button" value="Authorize"/>	
Test Email Address	<input type="text"/>
Timeout (ms)	<input type="text" value="20,000"/>
<input type="checkbox"/> Disable chunking	
<input type="button" value="Test Settings"/>	

Configuration

The highlighted settings are applicable in most cases.

User Name: Usually the email address.

The following items are entered from the Application Registration in Azure.

If you have created a notepad document from the Azure settings use these here.

Authorisation Endpoint

Token Endpoint

Client ID

Client Secret

Resource: This is usually:

<https://outlook.office365.com>

Scope: This is not normally required and can be left blank.

URL Suffix: This is not normally required and can be left blank.

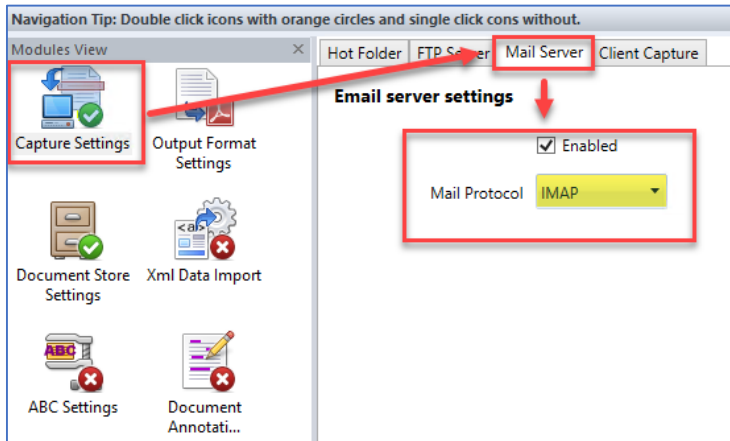
Redirect URI: This will be localhost, sometimes followed by a port number. There should be no need to change this setting.

Authorize: Clicking the Authorize button will open a web page where you can login to your Office365 account and follow the prompts to retrieve an access token.

Disable Chunking: This setting only appears on the Email Connector and is used in cases where emails are slow sending through Exchange – this should normally be unchecked.

ScannerVision™

Capture (IMAP) Email Configuration



Configuration

Incoming emails are captured using the Mail Server in the Capture Settings Menu.

Note:

- OAuth is only available when IMAP is selected.
-

ScannerVision™

Capture (IMAP) Email Configuration

Email server settings

Enabled

Mail Protocol

Mail Server Address

Mail Server Port Default 993

Connection Security

Encryption TLS 1.3 otherwise TLS 1.2

Server Authentication

Use OAuth

Configuration

These settings are applicable in most cases. Please consult your local IT administrator about your local settings.

Mail Protocol: MUST be set to IMAP

Mail Server Address: The hostname of the server you will use – in most cases, *Outlook.office365.com* is sufficient

Mail Server Port: Normally this will be set to port **993**

Connection Security: Set to 'SSL/TLS'

Encryption: Auto

Server Authentication:
Clear Authentication

Select '**Use OAuth**'

To configure these settings, please refer to the '**Outgoing SMTP Configuration**' on page 10

Email Address

Authorization Endpoint

Token Endpoint

Client ID

Client Secret

Resource

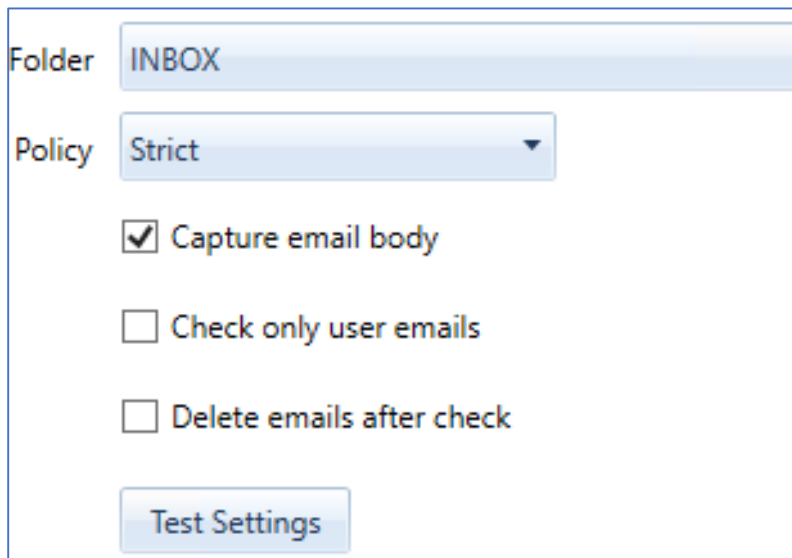
Scope

URL Suffix

Redirect URI

ScannerVision™

Capture (IMAP) Email Configuration



Folder: INBOX

Policy: Strict

Capture email body

Check only user emails

Delete emails after check

Test Settings

Configuration

These settings are General email settings.

For detailed explanation of these options, please refer to the main ScannerVision Manual or use the Help menu in the ScannerVision Server interface.


Note:

- Best practice is to ensure the 'Delete Emails after check' is NOT selected until you are sure the settings are correct.
-


ScannerVision™

Gmail (IMAP) Email Capture Configuration

Setup a new application or extend the existing Google Drive application by adding the Gmail API.



Gmail API

Google Enterprise API 

The Gmail API lets you view and manage Gmail mailbox data like threads, messages, and labels.

Configuration

These settings are applicable in most cases.

Mail Protocol: MUST be set to IMAP

Mail Server Address: The hostname of the server you will use – for Gmail *imap.gmail.com* is required.

Mail Server Port: Normally this will be set to port **993**

Connection Security: Set to 'SSL/TLS'

Encryption: Auto

Server Authentication:
Clear Authentication

Select '**Use OAuth**'

Email server settings

Enabled

Mail Protocol:

Mail Server Address:

Mail Server Port: Default: 993

Connection Security:

Encryption: TLS 1.3 otherwise TLS 1.2

Server Authentication:

Use OAuth

ScannerVision™

Gmail (IMAP) Email Capture Configuration

Email Address	<input type="text"/>
Authorization Endpoint	<input type="text"/>
Token Endpoint	<input type="text"/>
Client ID	<input type="text"/>
Client Secret	<input type="text"/>
Resource	<input type="text"/>
Scope	<input type="text" value="https://mail.google.com"/>
URL Suffix	<input type="text" value="prompt=consent&access_type=offline"/>
Redirect URI	<input type="text" value="http://localhost:50332"/>
	<input type="button" value="Authorize"/>

Configuration

These settings are required for Gmail setup.

User Name: The Gmail email address.

The following items are entered from the Project created in Google Drive.

Authorisation Endpoint

Token Endpoint

Client ID

Client Secret

Resource: This is not needed for Gmail and can be left blank.

Scope: This needs to be
https://mail.google.com

URL Suffix: This needs to be
prompt=consent&access_type=offline

Redirect URI: This will be localhost, followed by a port number. There should be no need to change this setting. This URI will need to be added to the OAuth 2.0 Client IDs for the Web application under Authorized redirect URIs in Google.

Authorize: Clicking the Authorize button will open a web page where you can login to your Gmail account and follow the prompts to retrieve an access token.

ScannerVision™

Gmail (SMTP) Outgoing Email Configuration

Configuration

These settings are applicable in most cases. This setup can be done on the main SMTP Server Settings or on individual Email Connectors.

SMTP Server: The hostname of the server you will use – in most cases *smtp.gmail.com* is sufficient.

Port: Normally this will be set to **587**

SSL/TLS: Set to 'Start TLS'

Encryption: Auto

Authentication: Auto Detect

Select '**Use OAuth**'

To configure these settings, refer to **Gmail (IMAP) Email Capture Configuration on page 15.**

The screenshot shows the 'Email Connector Setup' window with the 'SMTP Server' tab selected. A checkbox 'Use same settings as configured in main SMTP Server Settings' is checked. The configuration fields are: SMTP Server (smtp.gmail.com), SMTP Port (587), SSL/TLS (Start TLS), Encryption (Auto), Authentication (Auto Detect), and a checked 'Use OAuth' checkbox.

The screenshot shows an OAuth configuration form with the following fields: Email Address, Authorization Endpoint, Token Endpoint, Client ID, Client Secret, Resource, Scope (https://mail.google.com), URL Suffix (prompt=consent&access_type=offline), and Redirect URI (http://localhost:50332). An 'Authorize' button is at the bottom.

NB: Once a user has been logged into their email account, the user will remain logged in on the browser. This will automatically authorize the user on any additional email capture/connector setups. The user will need to open a separate page and explicitly log out of their account before the next email account should be allowed to login and authorize their account in the same browser session. We recommend the browser settings must be changed to clear cookies and other site data, and the browser must be completely closed between logins of different email accounts.



**Ubunye
Gibraltar**

Suite 4, 2nd Floor
The West Wing,
Montarik House,
3 Bedlam Court,
GIBRALTAR
GX11 1AA

**Ubunye
South Africa**

Block D, Stoneridge
Office Park, 8
Greenstone Place
Greenstone, 1609
SOUTH AFRICA

**Ubunye
Asia**

Unit 29-10,
Q Sentral, 2A,
Jalan Sentral 2,
50470 KL Sentral,
Kuala Lumpur,
Malaysia