

**amasty**



For more details see how the [SMTP Email Settings for Magento 2](#) extension works.

# Ultimate Guide for Magento 2 SMTP Email Settings

Send only reliable emails from a popular local hosting or a custom Magento 2 SMTP server. Run tests before emails dispatch to make sure that customers and partners receive all emails you send.

- Secure Magento 2 SMTP authentication and connection
- Pre-defined settings for popular email service providers
- Debug mode for email testing
- Log all sent emails and view any message in detail
- Significantly decrease email rejection

---

**ADD TO CART**

**GO TO EXTENSION PAGE**

---

Explore our internal [Knowledge Base](#) to gain even more valuable insights and uncover answers to popular questions about the configuration and features of the Magento 2 SMTP Email Settings extension.

## Extension Configuration

To configure Magento 2 SMTP server, please go to **Stores** → **Configuration** → **SMTP Email Settings**

### General Settings



## General Settings

**Enable SMTP For E-mail**  
[store view]

Yes

When disabled, the extension has no impact on Magento e-mail sending routines.

**Log Outgoing Mail**  
[store view]

Yes

Makes it possible to see the list of all e-mails ever sent through Magento, including email contents.

**Enable Debug Mode**  
[store view]

No

When enabled, all debug information is logged. Recommended not to use on production sites.

**Disable E-mail Delivery**  
[store view]

No

Set to "Yes" to not actually send e-mails. Useful when logging is enabled, for debug/development purposes.

**Enable SMTP For E-mail** - When set to 'No' this setting disables all features of the module including debug and emails log.

**Log Outgoing Mail** - Set this option to 'Yes' to log all emails sent from Magento. The feature enables you to view the list of the emails, including the contents at any time.

**Enable Debug Mode** - Debug information can help to set up emails dispatch. Please disable the debug option when emails sending works properly.

**Disable E-mail Delivery** - Set this option to 'No' to send out emails. When set to 'Yes', emails will not be sent. The system will 'pretend' that it is sending emails - the messages will still be added to the log and you will see all debug info. It's helpful for testing the system.


Get 14 additional detailed report types with the **Magento 2 reports extension**.

---

## SMTP Basic Configuration



## SMTP Configuration

<b>SMTP Provider</b> <small>[store view]</small>	<div>Gmail ▼</div>	<div>Autofill</div>
	Pre-defined SMTP providers	
<b>Server Address</b> <small>[store view]</small>	<div>smtp.gmail.com</div>	
	Either host name or IP address	
<b>Port</b> <small>[store view]</small>	<div>465</div>	
	Usually is 25, 587 or 465. Please consult with your service provider.	
<b>Authentication Method</b> <small>[store view]</small>	<div>Login/Password (Deprecated for Microsoft) ▼</div>	
<b>Login</b> <small>[store view]</small>	<div>example@gmail.com</div>	
<b>Password</b> <small>[store view]</small>	<div>.....</div>	
<b>Connection Security</b> <small>[store view]</small>	<div>SSL ▼</div>	
<b>Custom 'Reply To'</b> <small>[store view]</small>	<div>custom@test.com</div>	
	Specify the email you want to use for receiving replies. Leave it empty to receive replies to the original email address.	
<b>Send Test E-mail To</b> <small>[store view]</small>	<div>receiver@test.com</div>	
	<div> Please save the configuration before testing connection.</div>	
	<div>Test Connection</div>	

**SMTP Provider** - Choose your SMTP provider and click 'Autofill' to fill in some fields automatically. This way you can connect your Magento 2 store to Gmail SMTP. Select 'Other' if you own a server.

**Server Address** - Specify the hostname or IP address of the server.

**Port** - Define the port number.

**Authentication Method** - Set the required method:

- Authentication Not Required



- Login/Password (Deprecated for Microsoft)
  - OAUTH2 Client ID (Google)
  - OAUTH2 Service Account (Google)
  - OAUTH2 Client ID (Microsoft)
- 

## For Login/Password

**Login** - Specify your login in this field.

**Password** - Define a password for your login.

---

## For OAUTH2 Client ID (Google)

**Client Email**, **Client ID**, **Client Secret** and **Refresh Token** should be provided by Google. Read in [this section](#) how to get these credentials.

---

## For OAUTH2 Service Account (Google)

**G-Suite User Email** - provide the email of a user who has access to the service account specified in the Service Email field. This email will be used for the authentication in Google.

**Service Email** - provide the email for SMTP configuration generated by Google.

**Service Account Credentials** - upload the credentials in the json format. Check ow to get the credentials in [this section](#).

---

## For OAUTH2 Client ID (Microsoft)

**Sender Email** - specify Azure AD username that will be used as sender in the emails.

**Client Secret** - insert the generated secret token in the *Certificates&secrets* section on the Azure application.

**Application (Client) ID** - provide the value from the *Essentials* section in the created Azure application.

**Directory (Tenant) ID** - the value is also specified in the *Essentials* section in the created Azure application.

---



Explore the detailed configuration guide of the method in [this section](#).

---

**Connection Security** - Specify the protocol used for secure communication (the field can be filled automatically).

**Custom 'Reply To'** - Enter the email address where you want to receive replies. Leave it empty to receive replies to the original email address.

**Use Another Email Sender** - Choose **Yes**, if you want to replace the sender email (the option is available only when the **SMTP Provider** is defined as "Other").

When **Use Another Email Sender** is set to **Yes**, two additional fields will appear: **Sender Email** and **Sender Name**.

**Sender Email** - Define a new sender email for which the original sender email will be changed.

**Sender Name** - Specify the name of a new sender.

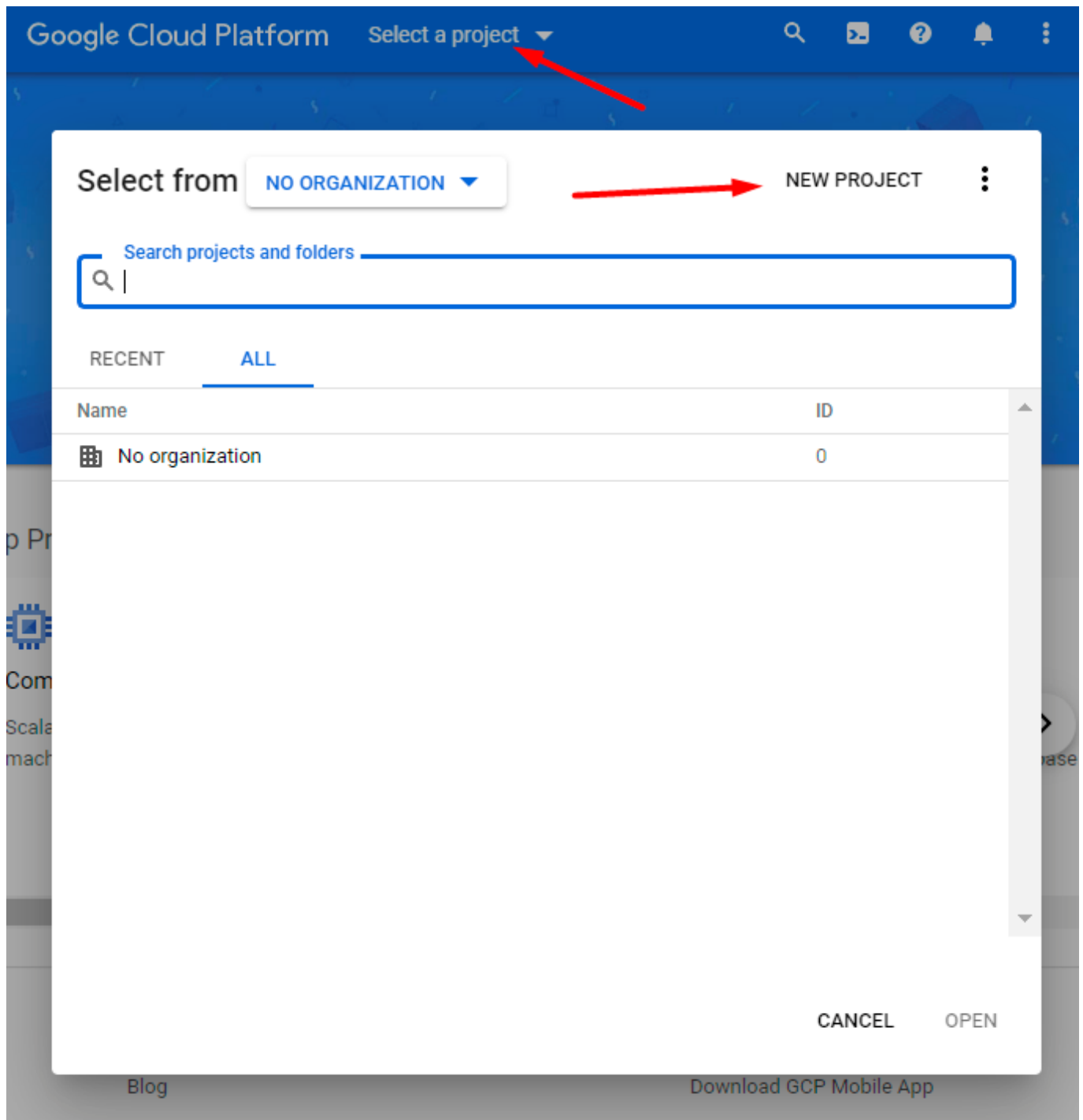
**Send Test E-mail To** - Specify an email for the test and click the 'Check Connection' button to run a test and make sure that you filled in the correct data and the setup works well. As a result, you should get the 'Connection Successful' message and receive a test email.

## OAuth 2.0 for Google Client ID

To get credentials for setting up a new authentication method OAUTH2 Client ID (Google), first of all, log in to your Google account and go [here](#).



You need to create a new project. To do this, click the **Select a project** dropdown and hit the **New Project** button.






Set project name, organization and location. Click **Create**.




 Google Cloud Platform 

## New Project


 You have 12 projects remaining in your quota. Request an increase or delete projects. [Learn more](#)  
[MANAGE QUOTAS](#)

Project name \*

SMTP 

Project ID: smtp-304613. It cannot be changed later. [EDIT](#)

Organization \*

No organization 

Select an organization to attach it to a project. This selection can't be changed later.

Location \*

[BROWSE](#)

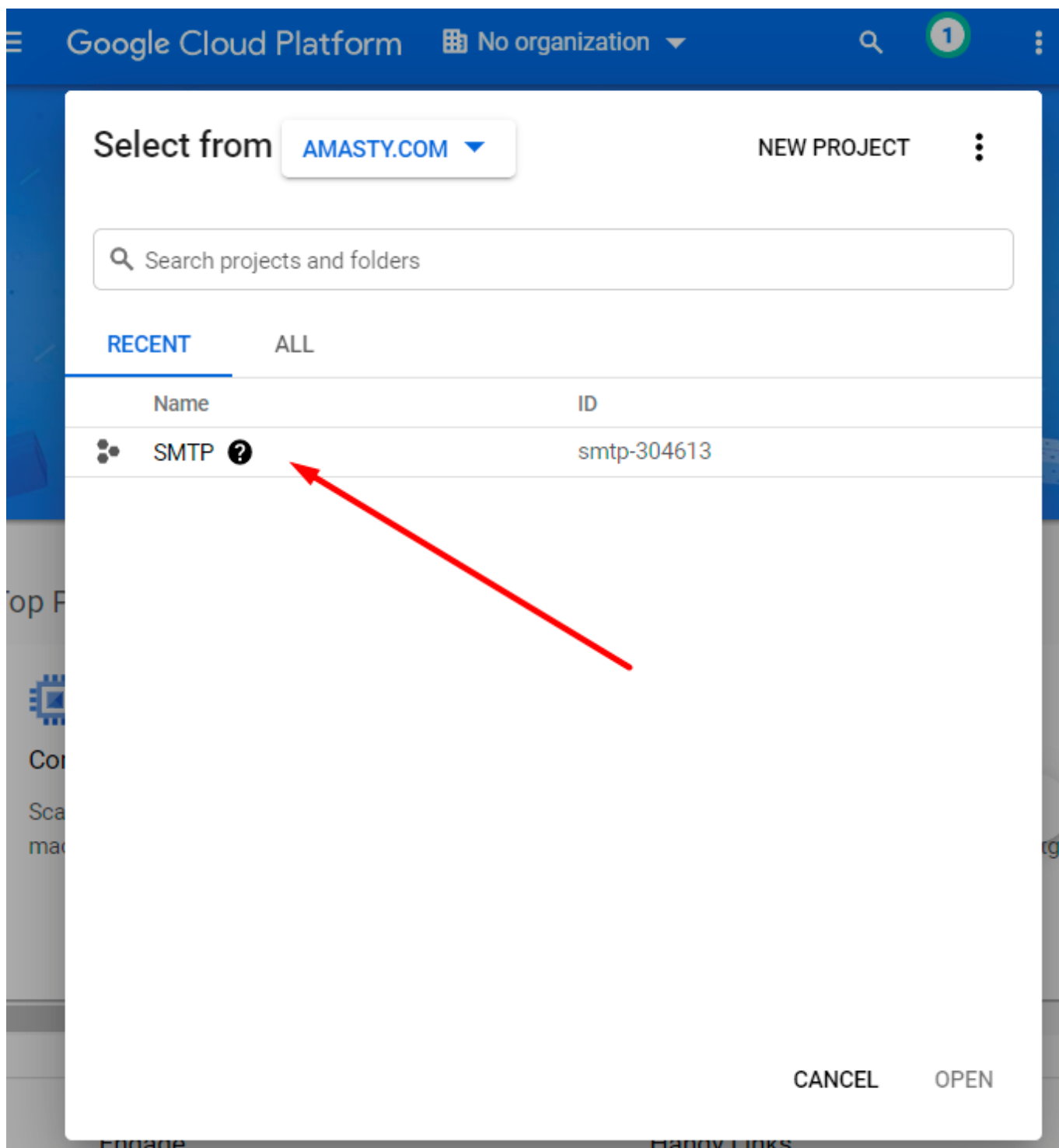
Parent organization or folder

CREATE

CANCEL

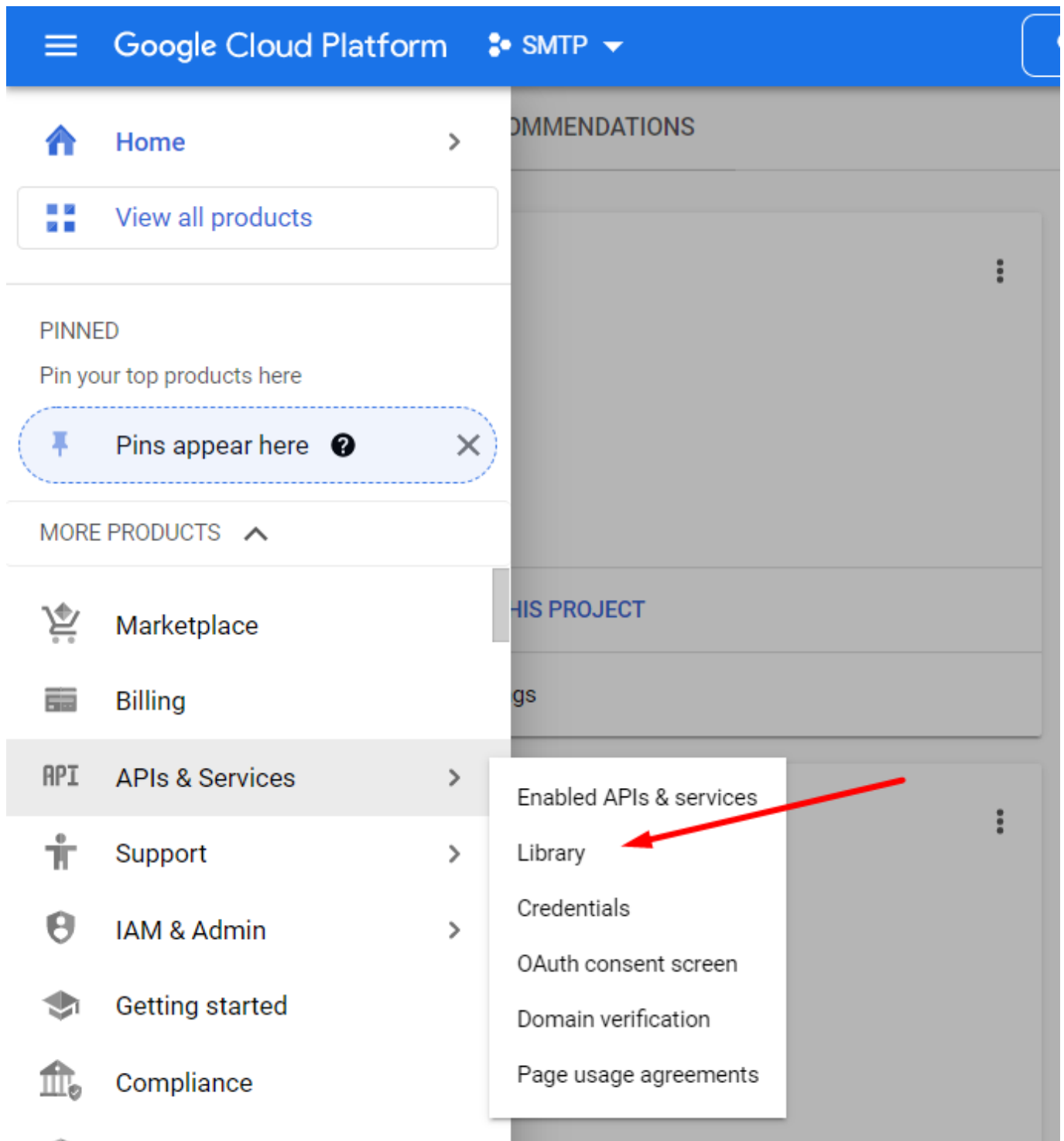
Choose a newly created project in the **Select a project** dropdown.





Navigate to **APIs & Services → Library**.





Choose **Gmail API**.






The screenshot shows the Google Cloud Platform console interface. At the top, there's a blue header with 'Google Cloud Platform' and 'SMTP' with a dropdown arrow. Below this is a search bar with the text 'Google Workspace' and a search icon. To the right of the search bar is a search input field with the placeholder text 'Search for APIs & Services'. Below the search bar, there's a 'Filter by' section with '18 results'. On the left, there's a 'CATEGORY' filter with a 'Google Workspace' tag. The main area displays a grid of API cards. A red arrow points to the 'Gmail API' card.


API Name	Provider	Description
Admin SDK API	Google	Admin SDK lets administrators of enterprise domains to view and manage resources like user,...
Apps Script API	Google	An API for managing and executing Google Apps Script projects.
G Suite Vault API	Google	Archiving and eDiscovery for G Suite.
Gmail API	Google	Flexible, RESTful access to the user's inbox
Google Drive API	Google	The Google Drive API allows clients to access resources from Google Drive
Google Sheets API	Google	The Sheets API gives you full control over the content and appearance of your spreadsheet

Hit the **Enable** button.



 Google Cloud Platform  SMTP ▼





## Gmail API



Google

Flexible, RESTful access to the user's inbox


[ENABLE](#) [TRY THIS API](#)


[OVERVIEW](#) [DOCUMENTATION](#) [SUPPORT](#)


Now you need to create credentials. Proceed to the appropriate tab.


 Google Cloud Platform  Export ▼


**API** APIs & Services


 Enabled APIs & services

 Library


 Credentials

 OAuth consent screen

 Domain verification

 Page usage agreements

← API/Service Details [DISABLE](#)



## Gmail API

The Gmail API lets you view and manage labels.

By Google Enterprise API ?

Service name

gmail.googleapis.com

Type

Public API

[METRICS](#) [QUOTAS](#) [CREDENTIALS](#)

Click **Create Credentials**.



Credentials

[+ CREATE CREDENTIALS](#)

DELETE

Create credentials to access your enabled APIs. [Learn more](#)

Remember to configure the OAuth consent screen with information about your application.

API Keys

☐

Name

Creation date

No API keys to display

OAuth 2.0 Client IDs

☐

Name

Creation date

No OAuth clients to display

Service Accounts

☐

Email

☐ export-example@export-318409.iam.gserviceaccount.com


Select the **client ID** credential type.



## Credentials

[+ CREATE CREDENTIALS](#) [DELETE](#)

Create credentials to access your project

 Remember to store your credentials securely

### API Keys

☐ Name

No API keys to display

**API key**  
Identifies your project using a simple API key to check quota and access

**OAuth client ID**  
Requests user consent so your app can access the user's data

**Service account**  
Enables server-to-server, app-level authentication using robot accounts


**Help me choose**  
Asks a few questions to help you decide which type of credential to use

## OAuth 2.0 Client IDs

Hit the **Configure Consent Screen** button.

### [←](#) Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information.

 To create an OAuth client ID, you must first set a product name on the consent screen

[CONFIGURE CONSENT SCREEN](#)

Select the **Internal** user type and click **Create**.




## OAuth consent screen

Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.

### User Type

☒ Internal  

Only available to users within your organization. You will not need to submit your app for verification.

☐ External 

Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to [verify your app](#).

[Let us know what you think](#) about our OAuth experience

Now fill in the required fields (App Name, User Support Email, Email Addresses), then Save and continue.



### Edit app registration

- 1 OAuth consent screen
- 2 Scopes
- 3 Summary

### App information

This shows in the consent screen, and helps end users know who you are and contact you

App name \*

TestSMTP

The name of the app asking for consent

User support email \*

john.thompson@amasty.com

For users to contact you with questions about their consent

App logo

BROWSE

Upload an image, not larger than 1MB on the consent screen that will help users recognize your app. Allowed image formats are JPG, PNG, and BMP. Logos should be square and 120px by 120px for the best results.

### App domain

To protect you and your users, Google only allows apps using OAuth to use Authorized Domains. The following information will be shown to your users on the consent screen.

Application home page

Provide users a link to your home page

Application privacy policy link

Provide users a link to your public privacy policy

Application terms of service link

Provide users a link to your public terms of service

### Authorized domains ?

When a domain is used on the consent screen or in an OAuth client's configuration, it must be pre-registered here. If your app needs to go through verification, please go to the [Google Search Console](#) to check if your domains are authorized. [Learn more](#) about the authorized domain limit.

+ ADD DOMAIN

### Developer contact information

Email addresses \*

john.thompson@amasty.com

These email addresses are for Google to notify you about any changes to your project.

SAVE AND CONTINUE

CANCEL



Proceed to **Add or remove scopes**.

## Edit app registration

✓ OAuth consent screen — **2 Scopes** — 3 Summary

Scopes express the permissions you request users to authorize for your app and allow your project to access specific types of private user data from their Google Account. [Learn more](#)

ADD OR REMOVE SCOPES



### Your non-sensitive scopes

API ↑	Scope	User-facing description
No rows to display		

In the appeared pop-up, select all items and click **Update**.



credit to explore G

op registratio

Auth consent s

es express the

nd allow your p

their Google Ac

OR REMOVE SO

non-sensiti

↑ Sco

ows to display

our sensitive

ve scopes are s

↑ Sco

ows to display

our restricte

ted scopes are s

↑ Sco

ows to display

AND CONTINUE

✕ Update selected scopes

?

Only scopes for enabled APIs are listed below. To add a missing scope to this screen, find and enable the API in the [Google API Library](#) or use the Pasted Scopes text box below. Refresh the page to see any new APIs you enable from the Library.

Filter Filter table ?

✓	API ↑	Scope	User-facing description
✓		.../auth/userinfo.email	View your email address
✓		.../auth/userinfo.profile	See your personal info, including any personal info you've made publicly available
✓		openid	Associate you with your personal info on Google
✓	BigQuery API	.../auth/bigquery	View and manage your data in Google BigQuery
✓	BigQuery API	.../auth/cloud-platform	View and manage your data across Google Cloud Platform services
✓	BigQuery API	.../auth/bigquery .readonly	View your data in Google BigQuery
✓	BigQuery API	.../auth/cloud-platform .read-only	View your data across Google Cloud Platform services
✓	BigQuery API	.../auth/devstorage .full_control	Manage your data and permissions in Google Cloud Storage
✓	BigQuery API	.../auth/devstorage .read_only	View your data in Google Cloud Storage
✓	BigQuery API	.../auth/devstorage .read_write	Manage your data in Google Cloud Storage

Rows per page: 10 ▾ 1 – 10 of 40 < >

Manually add scopes

If the scopes you would like to add do not appear in the table above, you can enter them here. Each scope should be on a new line or separated by commas. Please provide the full scope string (beginning with "https://"). When you are finished, click "Add to table".

ADD TO TABLE

UPDATE










Save the changes.



## Edit app registration


### Your sensitive scopes

Sensitive scopes are scopes that request access to private user data.

API 	Scope	User-facing description	
BigQuery API	.../auth/bigquery	View and manage your data in Google BigQuery	
BigQuery API	.../auth/cloud-platform	View and manage your data across Google Cloud Platform services	
BigQuery API	.../auth/bigquery.readonly	View your data in Google BigQuery	
BigQuery API	.../auth/cloud-platform.read-only	View your data across Google Cloud Platform services	
BigQuery API	..../auth/devstorage.full_control	Manage your data and permissions in Google Cloud Storage	
BigQuery API	..../auth/devstorage.read_only	View your data in Google Cloud Storage	
BigQuery API	..../auth/devstorage.read_write	Manage your data in Google Cloud Storage	

### Your restricted scopes

Restricted scopes are scopes that request access to highly sensitive user data.

API 	Scope	User-facing description
No rows to display		

SAVE AND CONTINUE

 CANCEL

Go **back to the dashboard**.



## Scopes

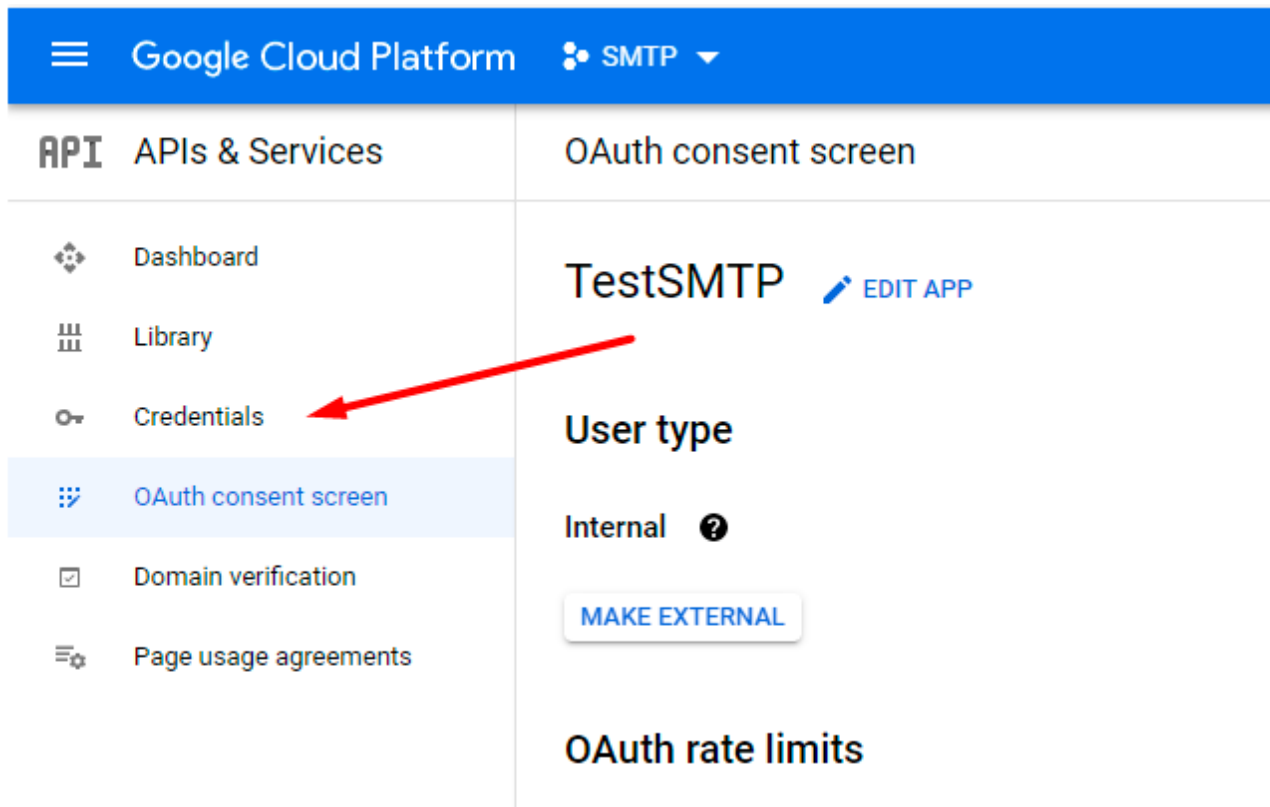
API ↑	Scope	User-facing description
	.../auth/userinfo.email	View your email address
	.../auth/userinfo.profile	See your personal info, including any personal info you've made available
	openid	Associate you with your personal info on Google
BigQuery API	.../auth/bigquery	View and manage your data in Google BigQuery
BigQuery API	.../auth/cloud-platform	View and manage your data across Google Cloud Platform services
BigQuery API	.../auth/bigquery.readonly	View your data in Google BigQuery
BigQuery API	.../auth/cloud-platform.read-only	View your data across Google Cloud Platform services
BigQuery API	.../auth/devstorage.full_control	Manage your data and permissions in Google Cloud Storage
BigQuery API	.../auth/devstorage.read_only	View your data in Google Cloud Storage
BigQuery API	.../auth/devstorage.read_write	Manage your data in Google Cloud Storage

BACK TO DASHBOARD



Return to the **Credentials** section.





Once again hit the **Create Credentials** button and choose **OAuth Client ID**.



Platform SMTP ▼ Search products and

### Credentials

[+ CREATE CREDENTIALS](#) [DELETE](#)

Create credentials to access Google services

#### API Keys

☐ Name

No API keys to display

#### OAuth 2.0 Clients

☐ Name Creation date ▼

No OAuth clients to display

#### Service Accounts

☐ Email

No service accounts to display

API key  
Identifies your project using a simple API key to check quota and access

OAuth client ID  
Requests user consent so your app can access the user's data

Service account  
Enables server-to-server, app-level authentication using robot accounts

Help me choose  
Asks a few questions to help you decide which type of credential to use

Specify **Application type**, **Name** and **Authorized redirect URLs** (for tests we used the following one: <https://developers.google.com/oauthplayground>).



## Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information.

Application type \*

Web application ▼

[Learn more](#) about OAuth client types

Name \*

Web client 1

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.



The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorized domains](#).

### Authorized JavaScript origins

For use with requests from a browser

[+ ADD URI](#)

### Authorized redirect URIs

For use with requests from a web server

URIs

<https://developers.google.com/oauthplayground>

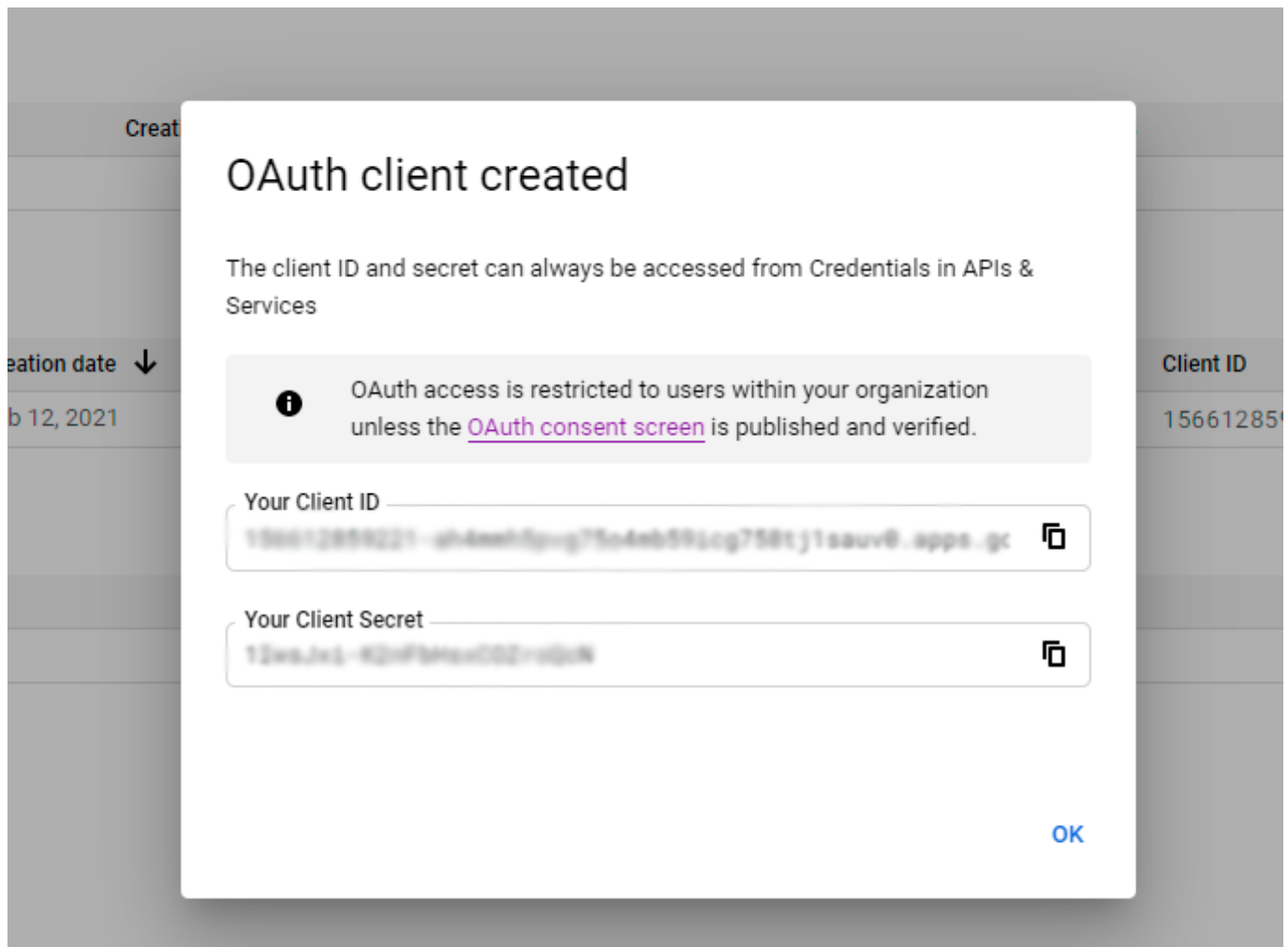
[+ ADD URI](#)

**CREATE**

CANCEL

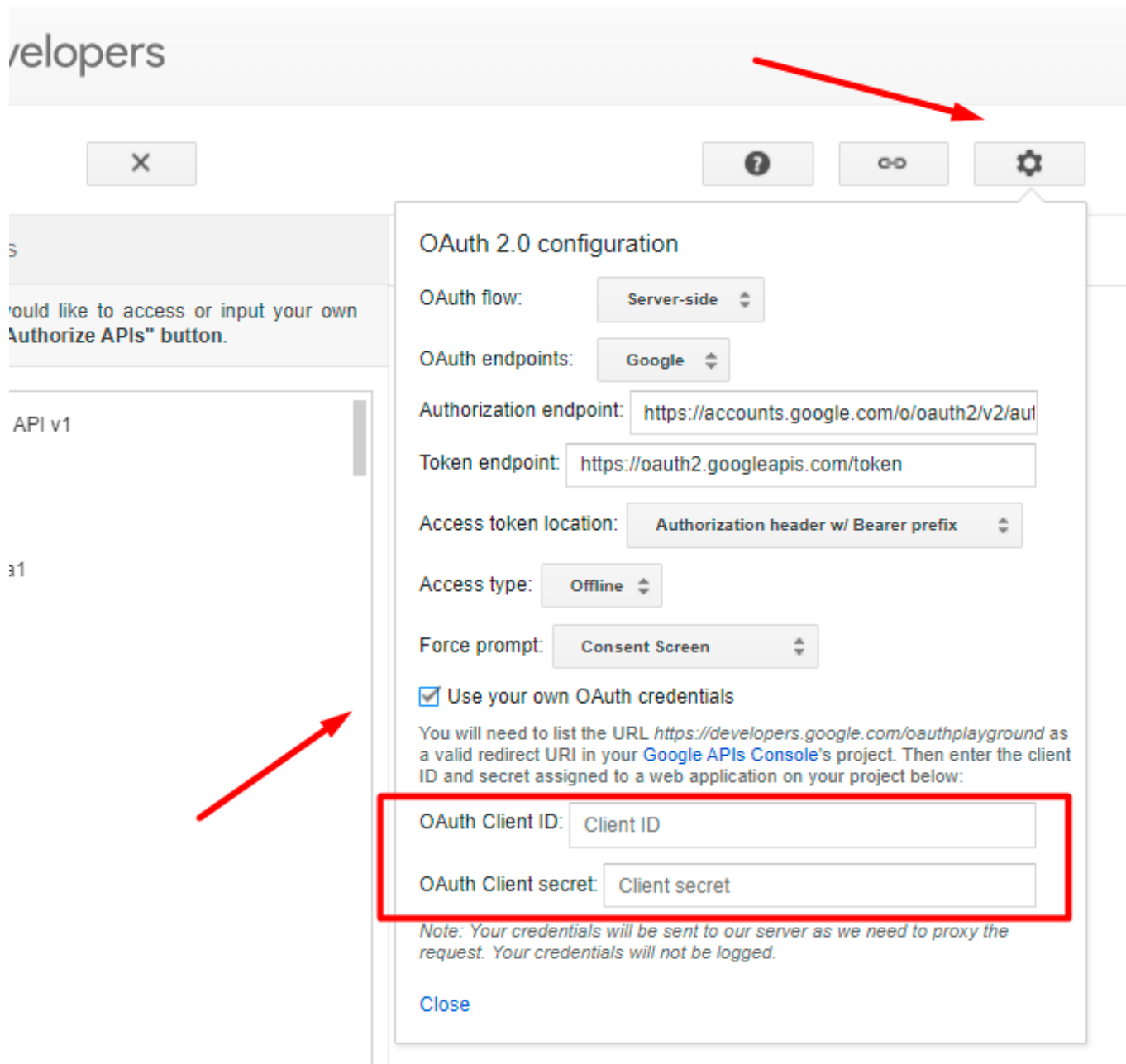
Your **Client ID** and **Client Secret** have been generated. Copy them.





Now go to the specified in the settings URL - <https://developers.google.com/oauthplayground/>. Open the settings, hit the **Use your own OAuth credentials** checkbox and paste the copied values.





In the list of methods, find the **Gmail API v1** and select <https://mail.google.com/>.





## OAuth 2.0 Playground





## ▼ Step 1 Select &amp; authorize APIs

Select the scope for the APIs you would like to access or input your own OAuth scopes below. Then click the "Authorize APIs" button.

## Request / Response

No request.

- ▶  Fitness API v1
- ▶  G Suite Vault API v1
- ▶  Genomics API v1
- ▼  Gmail API v1
  - ✓ <https://mail.google.com/>
  - <https://www.googleapis.com/auth/gmail.addons.current.action.compose>
  - <https://www.googleapis.com/auth/gmail.addons.current.message.action>
  - <https://www.googleapis.com/auth/gmail.addons.current.message.metadata>
  - <https://www.googleapis.com/auth/gmail.addons.current.message.readonly>
  - <https://www.googleapis.com/auth/gmail.compose>

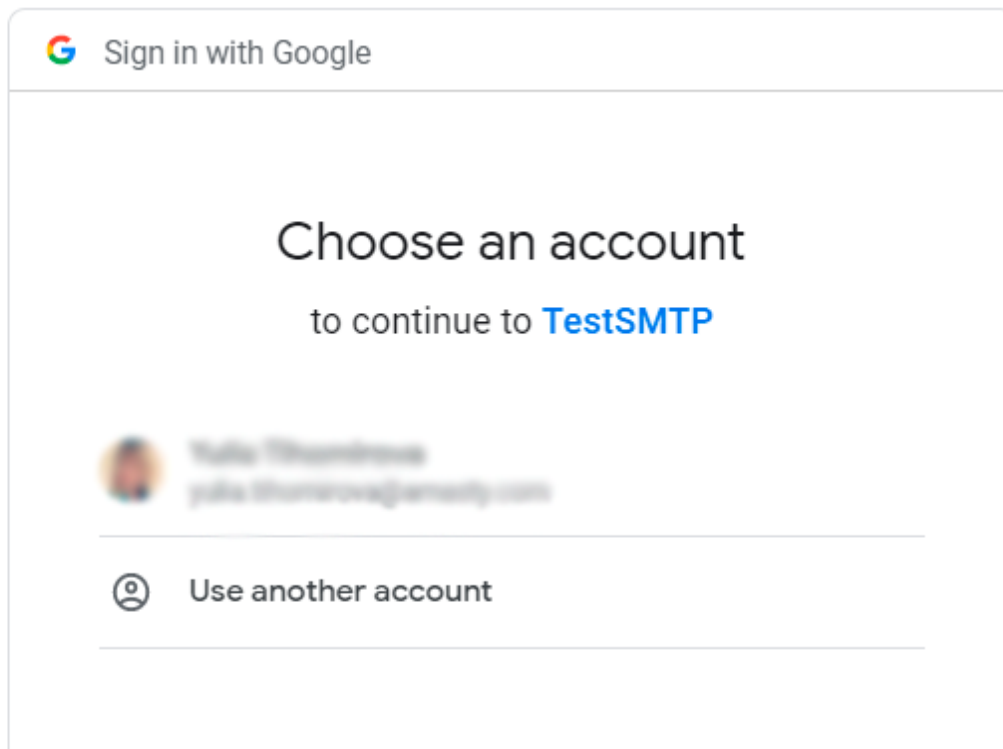
**Authorize APIs**

## ▶ Step 2 Exchange authorization code for tokens

Then click **Authorize APIs**.

Choose the required Google account and hit Allow in the next window.





On the appeared page, click the **Exchange Authorization code for tokens**.





## OAuth 2.0 Playground



### ▶ Step 1 Select & authorize APIs

### ▼ Step 2 Exchange authorization code for tokens

Once you got the Authorization Code from Step 1 click the **Exchange authorization code for tokens** button, you will get a refresh and an access token which is required to access OAuth protected resources.

Authorization code:

Exchange authorization code for tokens

Refresh token:

Access token:

Refresh access token

☐ Auto-refresh the token before it expires.

*Note: The OAuth Playground will automatically revoke refresh tokens after 24h. You can avoid this by specifying your own application OAuth credentials using the Configuration panel.*

### Request / Response

HTTP/1.1 302 Found  
Location: <https://accounts.google.com/ah4mmh5pvg75o4mb59icg758tj1sauv6>

GET /oauthplayground/?code=4/0A1ah4mmh5pvg75o4mb59icg758tj1sauv6  
Host: developers.google.com

Thus, you get the **Refresh Token**. Copy it.





## OAuth 2.0 Playground



### Step 1 Select & authorize APIs

### Step 2 Exchange authorization code for tokens

Once you got the Authorization Code from Step 1 click the **Exchange authorization code for tokens** button, you will get a refresh and an access token which is required to access OAuth protected resources.

Authorization code:

40AY0e-g4bz0Rmh80GsKsEvIah4mmh5pvg75o4mb59icg758tjlsauvI

Exchange authorization code for tokens

Refresh token:

15840e\_18A1u-EGp7HBAAGAC0B0f-L8p7HBAAGAC0B0f

Access token:

ya29.a0AfH6SI

Refresh access token

☐ Auto-refresh the token before it expires.

The access token will expire in **3553** seconds.

*Note: The OAuth Playground will automatically revoke refresh tokens after 24h. You can avoid this by specifying your own application OAuth credentials using the Configuration panel.*

### Request / Response

POST /token HTTP/1.1  
Host: oauth2.googleapis.com  
Content-length: 306  
content-type: application/x-www-form-urlencoded  
user-agent: google-oauth-playground

code=4%2F0AY0e-g4bz0Rmh80GsKsEvIah4mmh5pvg75o4mb59icg758tjlsauvI

HTTP/1.1 200 OK  
Content-length: 415  
X-xss-protection: 0  
X-content-type-options: nosniff  
Transfer-encoding: chunked  
Expires: Mon, 01 Jan 1990 00:00:00  
Vary: Origin, X-Origin, Referer  
Server: scaffolding on HTTPServer  
-content-encoding: gzip  
Pragma: no-cache  
Cache-control: no-cache, no-store  
Date: Fri, 12 Feb 2021 15:50:45  
X-frame-options: SAMEORIGIN  
Alt-svc: h3-29=":443"; ma=2592000  
Content-type: application/json;

```
{
  "access_token": "ya29.a0AfH6SI",
  "scope": "https://mail.google.com/",
  "token_type": "Bearer",
  "expires_in": 3599,
  "refresh_token": "1//04Qei_U1I"
}
```

Now you have all credentials and may configure the extension.

Choose the **OAUTH2 Client ID (Google)** authorization method and fill in the data you got.



## SMTP Configuration

<b>SMTP Provider</b> <small>[store view]</small>	Gmail ▼	Autofill
Pre-defined SMTP providers		
<b>Server Address</b> <small>[store view]</small>	smtp.gmail.com	
Either host name or IP address		
<b>Port</b> <small>[store view]</small>	465	
Usually is 25, 587 or 465. Please consult with your service provider.		
<b>Authentication Method</b> <small>[store view]</small>	OAUTH2 Client ID (Google) ▼	
<b>Client Email</b> <small>[global]</small>	example@mail.com	
Client Email who granted access to google app.		
<b>Client ID</b> <small>[global]</small>	123456789012-abcdefghijklmnopqrstuvwxyz1234567890.apps	
<b>Client Secret</b> <small>[global]</small>	.....	
<b>Refresh Token</b> <small>[global]</small>	.....	
<b>Connection Security</b> <small>[store view]</small>	SSL ▼	
<b>Send Test E-mail To</b> <small>[store view]</small>	receiver@test.com	
Save and Check Connection		

Save and test the connection.

## OAuth 2.0 for Google Service Account

Service accounts only works for G-Suite users, it doesn't work for personal Gmail accounts. It means that any Google user can create a service account, but the G-Suite administrator has to authorize it in G-Suite Admin Console to access the user mailbox.

To get the credentials, go to [Google Developers Console](#).

Create a new project as described for the [client ID configuration](#).

If ready, open this project and proceed to **Credentials → Manage service accounts**.



Google Cloud Platform My Project 94077

APIs & Services Credentials + CREATE CREDENTIALS DELETE

Dashboard

Library

Credentials

OAuth consent screen

Domain verification

Page usage agreements

Create credentials to access your enabled APIs. [Learn more](#)

Remember to configure the OAuth consent screen with information about your application.

CONFIGURE CONSENT SCREEN

### API Keys

<input type="checkbox"/>	Name	Creation date ↓	Restrictions	Key
No API keys to display				

### OAuth 2.0 Client IDs

<input type="checkbox"/>	Name	Creation date ↓	Type	Client ID
No OAuth clients to display				

### Service Accounts

[Manage service accounts](#)

<input type="checkbox"/>	Email	Name ↑
No service accounts to display		

Hit the **Create Service Account** button.



My Project 94077

1

Service accounts

+ CREATE SERVICE ACCOUNT

SHOW INFO PANEL

Service accounts for project "My Project 94077"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. [Learn more about service accounts.](#)

Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. [Learn more about service account organization policies.](#)

Filter

Filter table

<input type="checkbox"/>	Email	Status	Name ↑	Description	Key ID	Actions
No rows to display						

Provide **Service account name** and **Service account ID**. Click **Create and continue**.



## Create service account

### 1 Service account details

Service account name

my-service

Display name for this service account

Service account ID \*

my-service



Email address: my-service@export-318409.iam.gserviceaccount.com



Service account description

Describe what this service account will do

CREATE AND CONTINUE



### 2 Grant this service account access to project (optional)

### 3 Grant users access to this service account (optional)

DONE

CANCEL

Select a role - **Owner**.

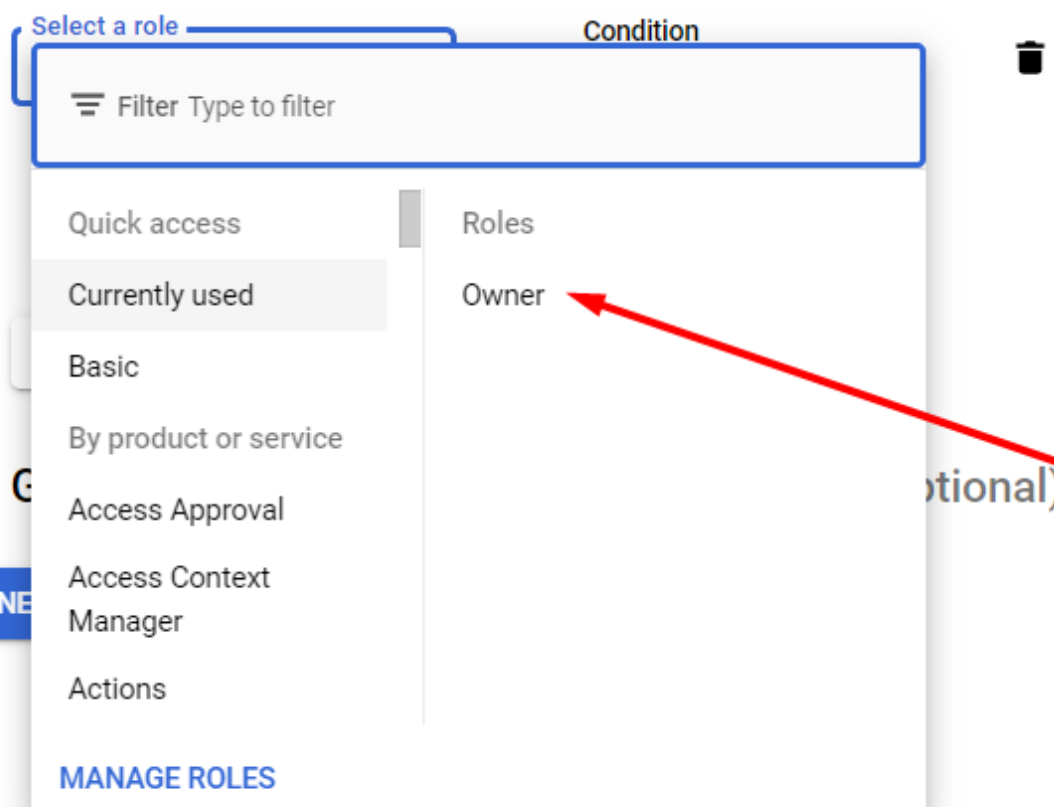


## Create service account

### ✓ Service account details

### 2 Grant this service account access to project (optional)


Grant this service account access to Export so that it has permission to complete specific actions on the resources in your project. [Learn more](#)





Then you can click **Done** without the changes.


Now the account is created. Navigate to **Service Accounts** and open the newly created account.





IAM & Admin


IAM


Identity & Organization


Policy Troubleshooter


Policy Analyzer


Organization Policies


Service Accounts


Workload Identity Federat...

Labels

Tags

Settings

Privacy & Security


Identity-Aware Proxy

Service accounts





Service accounts for project "Export"

A service account represents a Google Cloud service identity, s  
Compute Engine VMs, App Engine apps, or systems running ou  
[about service accounts](#).

Organization policies can be used to secure service accounts a  
features, such as automatic IAM Grants, key creation/upload, o  
accounts entirely. [Learn more about service account organizati](#)

Filter

Enter property name or value

<input type="checkbox"/>	Email	Status
<input type="checkbox"/>	 export-example@export-318409.iam.gserviceaccount.com	
<input type="checkbox"/>	 my-service@export-318409.iam.gserviceaccount.com	

Proceed to the **Keys** section.

amasty



[←](#) my-service

DETAILS

PERMISSIONS

KEYS

METRICS

LOGS

## Service account details

Name

my-service

SAVE

Description

SAVE

Email

my-service@export-318409.iam.gserviceaccount.com

Click **Add Key → Create new key**.

[←](#) my-service

DETAILS

PERMISSIONS

KEYS

METRICS

LOGS

## Keys

⚠

Service account keys could pose a security risk if compromised. We recommend you avoid authenticate service accounts on Google Cloud [here](#).

Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using [organization policies](#).  
[Learn more about setting organization policies for service accounts](#)

ADD KEY ▾

Create new key

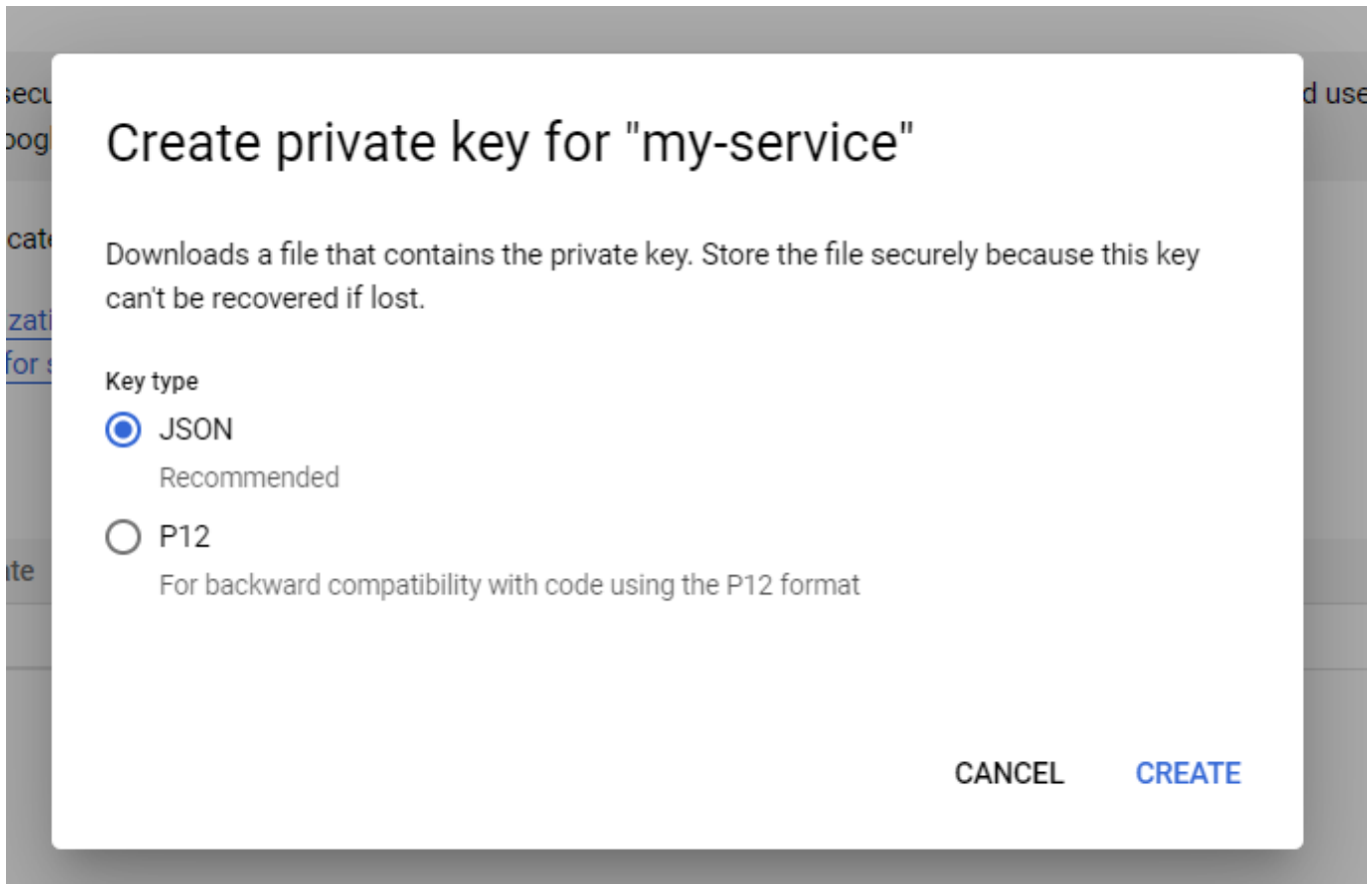
Upload existing key

Key creation date

Key expiration date

Choose **JSON** type.





After this, you will automatically get a JSON file with the keys downloaded. Now go back to the admin panel and fill in the following information:

**G-Suite User Email** - insert the email of the account on which the service account was created.

**Service Email** - paste the email from the service account.

You can find this email here:

## Service account details

Name	my-service	SAVE
Description		SAVE
Email	my-service@export-318409.iam.gserviceaccount.com	
Unique ID		

**Service Account Credentials** - upload the JSON file with the keys.



## SMTP Configuration

<b>SMTP Provider</b> <small>[store view]</small>	<input type="text" value="Gmail"/> ▼	<input type="button" value="Autofill"/>
Pre-defined SMTP providers		
<b>Server Address</b> <small>[store view]</small>	<input type="text" value="smtp.gmail.com"/>	
Either host name or IP address		
<b>Port</b> <small>[store view]</small>	<input type="text" value="465"/>	
Usually is 25, 587 or 465. Please consult with your service provider.		
<b>Authentication Method</b> <small>[store view]</small>	<input type="text" value="OAUTH2 Service Account (Google)"/> ▼	
<b>G-Suite User Email</b> <small>[global]</small>	<input type="text" value="example@gmail.com"/>	
<b>Service Email</b> <small>[global]</small>	<input type="text" value="my-service@export-318409.iam.gservice"/>	
Delegated email address to google service account.		
<b>Service Account Credentials</b> <small>[global]</small>	<input type="button" value="Choose File"/> export-3184...36c06f5.json	
<b>Connection Security</b> <small>[store view]</small>	<input type="text" value="SSL"/> ▼	

Done! Test the connection to make sure everything is correct.

### How to replace an email sender?

Changing of email sender will help you to avoid email overflowing: the Magento store email addresses you usually use won't be shown to customers - they will see another sender email instead.

**Note!** The option, that allows you to change the email sender, is available only if you have your own SMTP server.

Complete two easy steps to replace the sender's email:

Step 1. Specify the value **Other** in the field **SMTP Provider**.



## SMTP Configuration

**SMTP Provider**[\[store view\]](#)

- Other -



Autofill

Pre-defined SMTP providers

**Server Address**[\[store view\]](#)

smtp.yourdomain.com

Either host name or IP address

Step 2. Set the option **Use another Email Sender** to **Yes**, then specify the **Sender Email** and the **Sender Name** fields. You can use either an existing email or a fake one.

**Port**[\[store view\]](#)

465

Usually is 25, 587 or 465. Please consult with your service provider.

**Authentication Method**[\[store view\]](#)

Login/Password

**Login**[\[store view\]](#)

example@yourdomain.com

**Password**[\[store view\]](#)

\*\*\*\*\*

**Connection Security**[\[store view\]](#)

SSL

**Use Another Email Sender**[\[store view\]](#)

Yes



Be careful! Use Sender with the same domain from where you send mail. Otherwise, your mail server can get into the ban because of spam.

**Sender Email**[\[store view\]](#)

example-2@yourdomain.com

**Sender Name**[\[store view\]](#)

Ben Curtis

**Send Test E-mail To**[\[store view\]](#)**Save and Check  
Connection**

Make sure, you use the same domain, from which you send the mails. If the domains will differ, your mail will be considered as spam and your mail server will get into the ban.



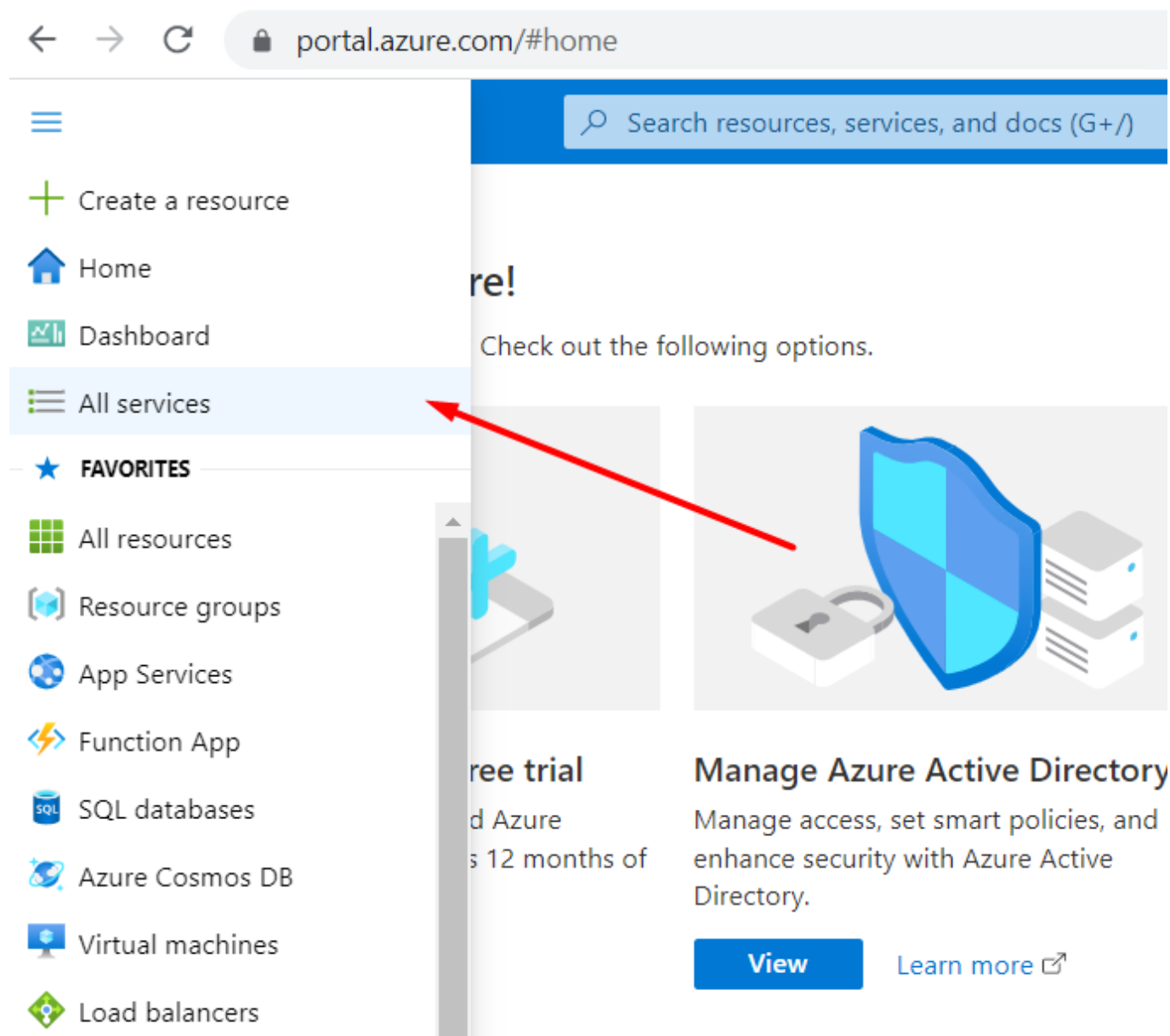
## OAUTH2 Client ID (Microsoft)

To enable Microsoft two-factor authentication, you need to create and configure an Azure App and fill in the appropriate fields in the module.

You can find Microsoft documentation [here](#).

### Azure App Configuration

To create an app, go to the [Azure home page](#) and select **All Services**.



Then proceed to the **Azure Active Directory**.



## All services

All

Favorites

Recents

**Categories**

General

Compute

Networking

Storage

Web

Mobile

Containers

Databases

Analytics

Filter services

Azure Active Directory

Virtual machines

Resource groups

App

SQL databases

Cost Management

Virtual networks

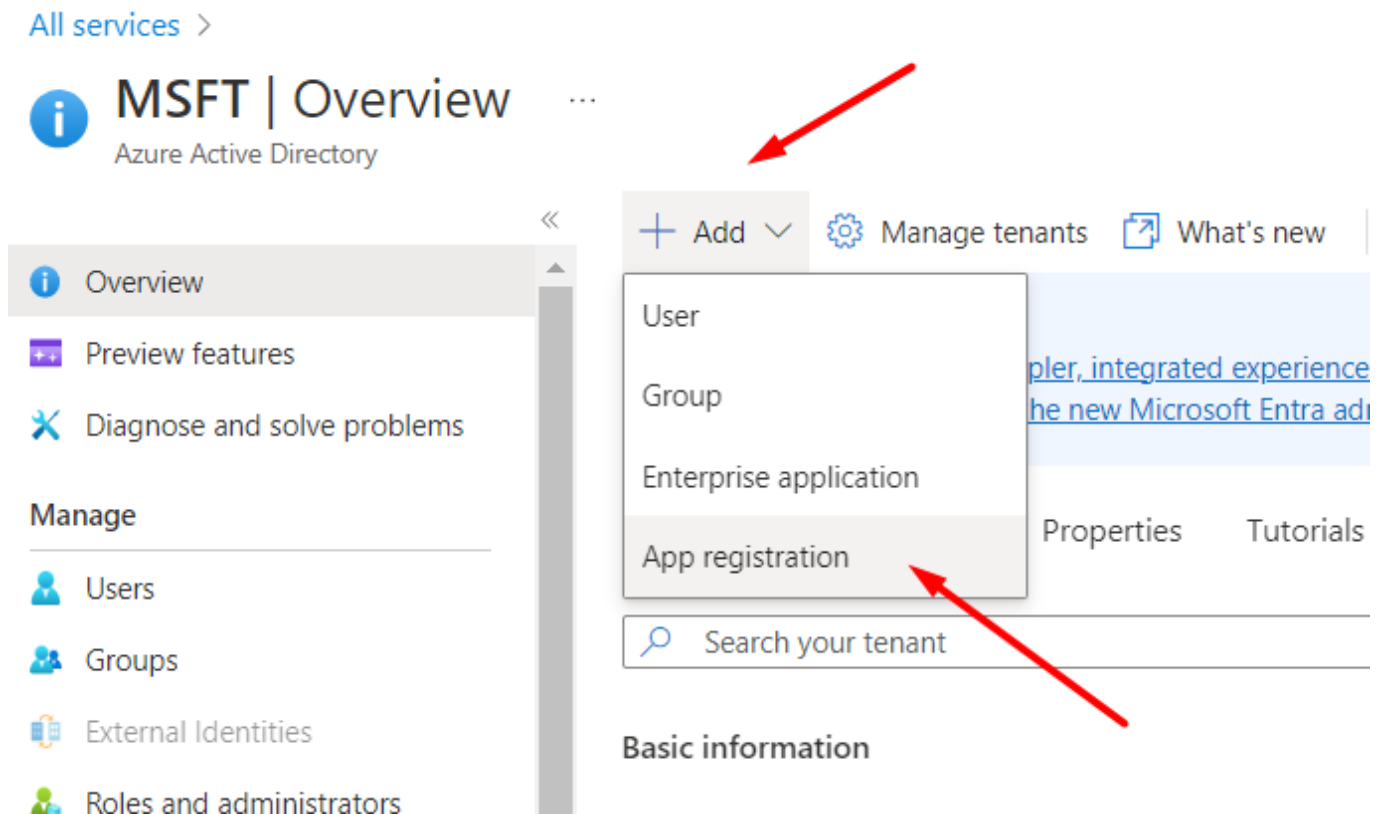
**General (18)**

All resources

Recent

Click the **Add** dropdown and choose the **App registration** option.





Next, specify the application name and choose access options for the application API. In this step, leave the **Redirect URI** parameter unchanged (it will be configured later) and click **Register**.



[All services](#) > [MSFT | Overview](#) >

Register an application

...

×

\* Name

The user-facing display name for this application (this can be changed later).

Amasty SMTP

✓

Supported account types

Who can use this application or access this API?

- ☐ Accounts in this organizational directory only (MSFT 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.

Select a platform

▼

e.g. https://example.com/auth



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

After the registration, you'll get to the application home page. Here you can find the **Application (client) ID** and **Directory (tenant) ID** required for the SMTP configuration.



 Delete  Endpoints  Preview features

### ^ Essentials


Display name : [Amasty SMTP](#)


Application (client) ID : 904d5d73-4d8a-48b1-a033-28bd496175aa 

Object ID : 5843c695-a030-407a-b7d8-55aed8d01145

Directory (tenant) ID : a79d1176-589e-4c78-b57b-a072a05a2472 

Supported account types : [Multiple organizations](#)

 Welcome to the new and improved App registrations. Looking to learn how it's changed from App reg

 Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and

Next, you need to generate a **Client Secret** key. Navigate to the **Certificates & Secrets** section and click **New client secret**.




[All services](#) > [Amasty SMTP](#)




## Amasty SMTP | Certificates &amp; secrets 🔑 ...

Search

&lt;&lt;



 Got feedback?

 Overview Quickstart Integration assistant

Credentials enable confidential applications to identify the client when receiving tokens at a web addressable location (using HTTPS). For assurance, we recommend using a certificate (instead of a self-signed certificate).

## Manage


 Branding & properties

➔ Authentication


## Certificates & secrets

- Token configuration

API permissions

 [Expose an API](#)

 App roles

 Owners

 Roles and administrators

**i** Application registration certificates, secrets and federat tabs below.

Certificates (0)

Client secrets (0)

Federated cr

A secret string that the application uses to prove its identity can be referred to as application password.

- + New client secret

### Description

Expires

Value (

No client secrets have been created for this application.

Enter the description for internal usage and choose the expiration date (or leave it unchanged). Hit the **Add** button.



secrets

k?

confidential applic  
on (using an HTTPS  
tial.

registration certificat

Client secrets

at the application u

secret

have been created

## Add a client secret

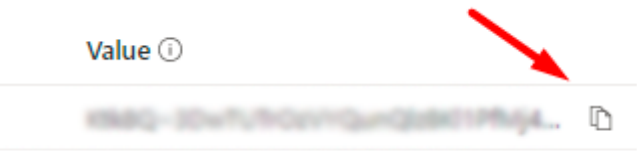
DescriptionSMTP

ExpiresRecommended: 6 months

AddCancel

Be sure to copy the **Value** of the Secret Key, because after reloading the page it disappears and it becomes impossible to get the value. This key is obligatory for the SMTP settings.





The next step is to set up API access. Go to **API permissions** → **Add a permission**.

All services > Amasty SMTP

Amasty SMTP | API permissions

Search

Refresh | Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

**API permissions**

Expose an API

App roles

Owners

Roles and administrators

Starting November 9th, 2020 end users will no longer

The "Admin consent required" column shows the default will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted all the permissions the application needs. [Learn more about permissions](#)

+ Add a permission

Grant admin consent for Microsoft Graph

API / Permissions name	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read basic profile info for the signed-in user.

Choose **Microsoft Graph**.



## permissions



Refresh



Got feedback?



Starting November 9th, 2020 end user



The "Admin consent required" column value in your organization, or in organ

## Configured permissions

Applications are authorized to call APIs with all the permissions the application needs.



Add a permission



Grant admin

API / Permissions name

Type

▼ Microsoft Graph (1)

User.Read

Delegated

## Request API permissions

Select an API

Microsoft APIs

APIs my organization uses

M

Commonly used Microsoft APIs



## Microsoft Graph

Take advantage of the tremendous amount of data available in the Microsoft Graph. Access Azure AD, Excel, Intune, Outlook/OneDrive, and more with a single endpoint.



## Azure Rights Management Services

Allow validated users to read and write protected content



Az

Programr  
functiona  
the Azure



## Flow Service

Embed flow templates and manage flows



Int

Programr

Then click the **Delegated permissions** option.




newly registered i


However, user c

# Request API permissions

[← All APIs](#)



Microsoft Graph

<https://graph.microsoft.com/> [Docs](#) 

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application pe

Your applicatio

signed-in user.

Here you can see the list of permissions. Please, choose the following ones:

openid  
offline\_access  
SMTP.Send  
User.Read

Permission	Admin
▼ OpenId permissions (2)	
<input type="checkbox"/> email ⓘ View users' email address	No
<input checked="" type="checkbox"/> offline_access ⓘ Maintain access to data you have given it access to	No
<input checked="" type="checkbox"/> openid ⓘ Sign users in	No
<input type="checkbox"/> profile ⓘ View users' basic profile	No



SMTP (1)		
<input checked="" type="checkbox"/>	SMTP.Send ⓘ Send emails from mailboxes using SMTP AUTH.	No
User (1)		
<input type="checkbox"/>	User.Export.All ⓘ Export user's data	Yes
<input type="checkbox"/>	User.Invite.All ⓘ Invite guest users to the organization	Yes
<input type="checkbox"/>	User.ManageIdentities.All ⓘ Manage user identities	Yes
<input checked="" type="checkbox"/>	User.Read ⓘ Sign in and read user profile	No
<input type="checkbox"/>	User.Read.All ⓘ Read all users' full profiles	Yes
<input type="checkbox"/>	User.ReadBasic.All ⓘ Read all users' basic profiles	No
<input type="checkbox"/>	User.ReadWrite ⓘ Read and write access to user profile	No
<input type="checkbox"/>	User.ReadWrite.All ⓘ Read and write all users' full profiles	Yes

Click **Add permissions** and check the correctness.



### Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent screen. Granting permissions is a one-time action, and you must grant all the permissions the application needs. [Learn more about permissions and consent](#)

+

Add a permission

✓

Grant admin consent for MSFT

API / Permissions name	Type	Description
▼ Microsoft Graph (4)		
offline_access	Delegated	Maintain access to data you have given it access to
openid	Delegated	Sign users in
SMTP.Send	Delegated	Send emails from mailboxes using SMTP AUTH.
User.Read	Delegated	Sign in and read user profile

Now we can set up the “Redirect URI” for our Magento website, where the replies from Microsoft will be sent. Go to **Authentication → Add a platform**:



[All services](#) > [Amasty SMTP](#)



## Amasty SMTP | Authentication



Got feedback?



Overview



Quickstart



Integration assistant

### Manage



Branding & properties



Authentication



Certificates & secrets



Token configuration



API permissions



Expose an API



App roles

### Platform configurations

Depending on the platform or device this application i  
redirect URLs, specific authentication settings, or fields spe



Add a platform

### Supported account types

Who can use this application or access this API?



Accounts in this organizational directory only (MSFT



Accounts in any organizational directory (Any Azure

[Help me decide...](#)

Choose **Web**.



## Authentication

Got feedback?

### Platform configuration

Depending on the platform, you may need to specify redirect URLs, specific authentication methods, and other platform-specific settings.

+ Add a platform

### Supported account types

Who can use this application?


☐ Accounts in this organization

☒ Accounts in any organization

[Help me decide...](#)


## Configure platforms

### Web applications



#### Web


Build, host, and deploy a web server application. .NET, Java, Python



#### Single-page app


Configure browser client and progressive web app. Javascript.

### Mobile and desktop applications



#### iOS / macOS

Objective-C, Swift, Xamarin



#### Android

Java, Kotlin, Xamarin

Next, specify the **Redirect URL** in the following format:

```
https://*your_magento_url*/amasty_smtp/oauth/callback
```



# Configure Web

[← All platforms](#)[Quickstart](#)[Docs](#)

## \* Redirect URLs

The URLs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. [Learn more about Redirect URLs and their restrictions](#)



## Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

## Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens](#).

Select the tokens you would like to be issued by the authorization endpoint:

- ☐ Access tokens (used for implicit flows)
- ☐ ID tokens (used for implicit and hybrid flows)

[Configure](#)[Cancel](#)

Click **Configure**. If you need to specify several Redirect URLs for one application, you can add one more URL:



## Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required, such as redirect URIs, specific authentication settings, or fields specific to the platform.

[+ Add a platform](#)

### ^ Web

#### Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successful login. The URIs in the request to the login server should match one listed here. Also referred to as reply URLs.

`https://your_magento_url/amasty_smtp/oauth/callback`

[Add URI](#)



## Extension Configuration

Insert the **Client Secret** you've copied (the Value field from the **Certificates & Secrets** tab).

Paste the values of the **Application (Client) ID** and **Directory (Tenant) ID** from the **Overview** tab.



Authentication Method

[store view]

OAUTH2 Client ID (Microsoft)

Sender Email

[global]

example@sf4m2.onmicrosoft.com

Azure AD username that will be used as sender in the emails.

Client Secret

[global]

.....

The generated secret token in the Certificates&secrets section on the Azure application.

Application (Client) ID

[global]

906d5d73-488a-40b1-ae55-28b4d9e178aa

Value from the Essentials section in the created Azure application.

Directory (Tenant) ID

[global]

a79d1576-5d4e-4c78-b51b-a072a09e3472

Value from the Essentials section in the created Azure application.

Connection Security

[store view]

SSL

Send Test E-mail To

[store view]

recipient@test.com

Please save the configuration before testing connection.

Test Connection

## Sender Email Update

Please, note that you need to change **Sender Email** in the general configuration as well.

Navigate to **Stores → Configuration → General → Store Email Addresses**. Update the address in the **Sender Email** field in all the tabs.



### General Contact



Sender Name

[store view]

Owner

☒ Use system value

Sender Email

[store view]

example@sf4m2.onmicrosoft.com

☐ Use system value

### Sales Representative



Sender Name

[store view]

Sales

☒ Use system value

Sender Email

[store view]

example@sf4m2.onmicrosoft.com

☐ Use system value

### Customer Support



Sender Name

[store view]

CustomerSupport

☒ Use system value

Sender Email

[store view]

example@sf4m2.onmicrosoft.com

☐ Use system value

## Automatic Log Clearing

Old log records can be removed after a certain period (in days). If you set the auto clean to 0, the option won't be applied.



## Automatic Log Clearing

Clear Sent Emails Log After

[global]

5

Automatically remove old log records after specified number of days. If set to 0, will not auto clean.

Clear Debug Log After

[global]

30

Automatically remove old log records after specified number of days. If set to 0, will not auto clean.

## Blacklist Emails

### Blacklist Emails

Enable Blacklist

[global]

Yes

▼

**Enable Blacklist** - Set to **Yes** to block emails from being sent to blacklisted email addresses.

The blacklisted email addresses are stored on the Blacklist grid. To find this grid, navigate to **Reports** → **SMTP Email Settings** → **Blacklist**.



Blacklist

admin

Add Email

Filters

Default View

Columns

Actions


2 records found

20 per page

1 of 1

	ID	Email	Action
<input type="checkbox"/>	2	johndoe@domain.com	<a href="#">Edit</a>
<input type="checkbox"/>	1	test@gmail.vom	<a href="#">Edit</a>

Please note that with enabled blacklist functionality, invalid email addresses (e.g. test@gmail.vom) will be automatically blacklisted and recorded on the **Blacklist** grid. Also, it is possible to add email addresses to this grid manually if needed. If the email address is in blacklist, a notification will inform you when attempting to send an email to it.

 Error sending e-mail: email test@gmail.vom is in blacklist.

## Sent Emails Log

To see the list of sent emails please go to **Reports** → **SMTP Email Settings section** → **SMTP Sent Emails Log**.



## Sent Emails Log

 demouser ▾

Clear Sent Emails Log

Search by keyword



Filters



Default View ▾



Columns ▾

3 records found

20



per page



1

of 1



Date	Subject	Recipient Email	Status	Action
Dec 5, 2019 8:02:05 AM	Your Main Website Store order confirmation	roni_cost@example.com	Pending	Select ▴
Dec 5, 2019 8:02:29 AM	Your Main Website Store order confirmation	roni_cost@example.com	Pending	View
Dec 5, 2019 8:04:17 AM	Your Main Website Store order confirmation	roni_cost@example.com	Pending	Resend
				Select ▾

In the log, you can see the email subject, the date it was sent, the recipient's email address, and the email status. Click 'Select' in the Action column and choose 'View' to see the email content or 'Resend' to resend the email.

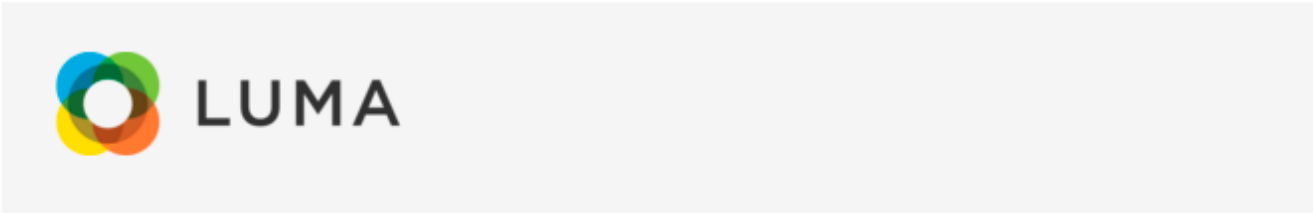
Please note that to use the **resend functionality**, you need to install the **amasty/module-smtp-email-reply-to-setting** package.

## View Sent Emails

After clicking '**View**' on the **Sent Emails** grid you can see the content of the selected email.



December 21, 2015  
Your Main Website Store order confirmation  
test@example.com



Dear Customer,

Thank you for your order from Main Website Store. Once your package ships we will send you a tracking number. You can check the status of your order by [logging into your account](#).

If you have questions about your order, you can email us at [support@example.com](mailto:support@example.com).

Your Order #0000000003

Placed on December 15, 2015 at 4:15:51 AM CST

Billing Info

John Doe  
Sacramento California 23rd str  
United States

Shipping Info

John Doe  
Sacramento California 23rd str  
United States

Debug Log

To see the extension debug log please go to **Reports** → **SMTP Email Settings section** → **SMTP Debug Log**.



# SMTP Debug Log



admin ▾

[Clear Debug Log](#)

Date	↑	Message
Dec 24, 2015 8:19:24 AM		Test e-mail was sent successfully!
Dec 24, 2015 8:19:24 AM		E-mail sent successfully at amsmtp/transport::sendMessage().
Dec 24, 2015 8:19:21 AM		Ready to send e-mail at amsmtp/transport::sendMessage()
Dec 21, 2015 3:47:44 AM		Test e-mail was sent successfully!
Dec 21, 2015 3:47:44 AM		E-mail sent successfully at amsmtp/transport::sendMessage().
Dec 21, 2015 3:47:42 AM		Ready to send e-mail at amsmtp/transport::sendMessage()
Dec 21, 2015 3:47:44 AM		E-mail sent successfully at amsmtp/transport::sendMessage().
Dec 21, 2015 3:47:42 AM		Ready to send e-mail at amsmtp/transport::sendMessage()

At this page you can find out if emails are sent and what errors if any, occur. This data will help you to configure the module. It's recommended to **disable the Debug Mode** once you've successfully setup the module and run the necessary tests.

## What is SPF Record and How to Configure it

Please be aware that it is not mandatory to setup SPF record, however doing so you will increase the chance of email delivery.

**Sender Policy Framework (SPF)** is an email validation system created to prevent email spam on the Internet by detecting email spoofing (creation of emails with forged sender addresses).

**SPF technology consists of two parts** - SPF-record in DNS (Domain Name System) zone of your domain; - email server component of the message recipient or the component of its spam combating system; SPF record is configured by email sender. It contains information about the servers that are allowed to send emails from your domain name.

Although SPF record is optional, today due to the spam issue most email servers may refuse to accept your email without this record or mark it as suspicious or unwanted.



## How to set SPF record for your own SMTP server

If you use your own email server to send emails for your domain (below we use the example.com domain for demonstration) that has IPv4 address xxxx, the SPF record will look like this:

```
example.com. IN TXT "v=spf1 a mx ip4:x.x.x.x ~all"
```

```
example.com. IN SPF "v=spf1 a mx ip4:x.x.x.x ~all"
```

If your server has more than one IPv4 address, you can list them like that: "v=spf1 a mx ip4:x.x.x.x ip4:y.y.y.y ip4:z.z.z.z -all".

If you use IPv6 addresses, the record will be: "ip6:xx:yy::zz", where "xx:yy::zz" is the IPv6 of your email server. In this example, the SPF record allows sending emails for the example.com domain from the IP address specified in the «A» record of the **example.com** domain (a), mail-exchangers of the example.com domain (mx) and from IP address x.x.x.x (ip4:x.x.x.x). The recipient's server will make the decision whether to mark as spam emails from other senders (~ all).

To restrict sending emails from senders not listed in the SPF record, you can use the **"-all"** option instead of **"~all"**. However, in case there are any inaccuracies in your settings you risk to restrict receiving of your mail.

Therefore, use this option only if you are sure that all your settings are correct.

---

## How to set SPF record for Google Apps

If you use **Google Apps** service to send emails for your domain, the SPF record settings will be slightly different.

The addresses of the email servers that are used by Google Apps can vary and consequently you'll have to enable **Google Apps SPF** configuration.

In case you use **Google Apps** to receive emails, but send emails using your **own SMTP** server you need to specify it in the SPF record:

```
example.com. IN TXT "v=spf1 a mx ip4:x.x.x.x include:_spf.google.com ~all"
```

```
example.com. IN SPF "v=spf1 a mx ip4:x.x.x.x include:_spf.google.com ~all"
```

If you use **Google Apps Service** both for sending and receiving emails, the SPF record will be the following:

```
example.com. IN TXT "v=spf1 include:_spf.google.com ~all"
```

```
example.com. IN SPF "v=spf1 include:_spf.google.com ~all"
```

---



To get more details about **SPF settings** for Google Apps, click [here](#).

## Cron Tasks List

Magento 2 SMTP Email Settings extension is preintegrated with Cron Tasks List to provide store owners with an opportunity to track and manage all cron tasks running in the website background.

To view all scheduled and executed cron tasks, go to **System → Cron Tasks List**

Run all cron tasks and generate their schedule by clicking the ‘Run Cron’ button. Also you can delete separate tasks in bulk, apply filtering and sorting options when it is needed.

Cron Tasks List

Run Cron

Last Cron Activity: 20 seconds ago

Filters

Default View

Columns

Actions

652 records found

20 per page

1 of 33

	ID	Job Code	Status	Created At	Scheduled At	Executed At	Finished At
<input type="checkbox"/>	1038	sales_grid_order_shipment	SUCCESS	Mar 18, 2019 5:47:11 AM	Mar 18, 2019 5:47:00 AM	Mar 18, 2019 5:47:20 AM	Mar 18, 2019 5:47:20 AM
<input type="checkbox"/>	1058	sales_grid_creditmemo_async	SUCCESS	Mar 18, 2019 5:47:11 AM	Mar 18, 2019 5:47:00 AM	Mar 18, 2019 5:47:20 AM	Mar 18, 2019 5:47:20 AM
<input type="checkbox"/>	1078	sales_send_order_emails	SUCCESS	Mar 18, 2019 5:47:11 AM	Mar 18, 2019 5:47:00 AM	Mar 18, 2019 5:47:20 AM	Mar 18, 2019 5:47:20 AM
<input type="checkbox"/>	1098	sales_order_invoice_emails	SUCCESS	Mar 18, 2019 5:47:11 AM	Mar 18, 2019 5:47:00 AM	Mar 18, 2019 5:47:20 AM	Mar 18, 2019 5:47:20 AM
<input type="checkbox"/>	1118	sales_send_order_shipment	SUCCESS	Mar 18, 2019 5:47:11 AM	Mar 18, 2019 5:47:00 AM	Mar 18, 2019 5:47:20 AM	Mar 18, 2019 5:47:20 AM
<input type="checkbox"/>	1196	indexer_reindex_all_invalid	SUCCESS	Mar 18, 2019 5:47:13 AM	Mar 18, 2019 5:47:00 AM	Mar 18, 2019 5:47:21 AM	Mar 18, 2019 5:47:21 AM
<input type="checkbox"/>	1200	indexer_update_all_views	MISSED	Mar 18, 2019 5:47:13 AM	Mar 18, 2019 5:47:00 AM	Mar 18, 2019 5:47:21 AM	Mar 18, 2019 5:47:21 AM
<input type="checkbox"/>	1018	sales_grid_order_invoice_async	SUCCESS	Mar 18, 2019 5:47:11 AM	Mar 18, 2019 5:47:00 AM	Mar 18, 2019 5:47:20 AM	Mar 18, 2019 5:47:20 AM
<input type="checkbox"/>	1024	sales_grid_order_invoice_async	PENDING	Mar 18, 2019 5:47:11 AM	Mar 18, 2019 5:53:00 AM		
<input type="checkbox"/>	1025	sales_grid_order_invoice_async	PENDING	Mar 18, 2019 5:47:11 AM	Mar 18, 2019 5:54:00 AM		

ADD TO CART

GO TO EXTENSION PAGE

Find out how to install the SMTP Email Settings extension via [Composer](#).



From:

<https://amasty.com/docs/> - **Amasty Extensions FAQ**

Permanent link:

[https://amasty.com/docs/doku.php?id=magento\\_2:smtp-email-settings](https://amasty.com/docs/doku.php?id=magento_2:smtp-email-settings)



Last update: **2024/11/15 10:38**