



**Enhancements in System
Email Account & User Mail
Server Setting**

*Microsoft 365 Outlook
Server Type Implementation*



Table of Contents

1. Overview	3
1.1. Enhancements in System Email Account Setup.....	3
1.1.1. Microsoft 365 Outlook Settings	4
1.1.2. OAUTH 2.0 Settings for Microsoft 365 Outlook.....	4
1.2. Enhancements in User Mail Server Settings	7
1.3. User Options:	9



1. Overview

ServicePRO facilitates a new Microsoft 365 Outlook Server Type option in System email account setup and User Mail Server Settings, for use with the Office 365 / Exchange Online Mailboxes, in order to address the disabling of EWS in Exchange Online by Microsoft, starting October 1, 2026.

Microsoft 365 Outlook Server Type option works only with Office 365 / Exchange Online Mailboxes only.

1.1. Enhancements in System Email Account Setup

In the “Configure System Email Account” screen, for the Mail Server Type selection, a new option “Microsoft 365 Outlook” has been added. Please make sure to select this Mail Server Type if you are using an Office 365 / Exchange Online Mailbox for you are System Email Account.

The screenshot shows the 'Configure System Email Account' window. The 'Mail Server Type' is set to 'Microsoft 365 Outlook'. The 'Account Information' section includes fields for Profile Name (Client3), Email Address (client3@helpstar.com), Account Name (client3@helpstar.com), Authentication Kind (OAUTH 2.0), Account Password, and Domain (helpstar.com). The 'Server Information' section includes a URL (https://graph.microsoft.com/v1.0), Authentication Type (Exchange Authentication), Agent Mailbox Name, Agent Mailbox Email, and Agent Password. The 'Properties' section includes checkboxes for 'Process Emails from Users with the 'Email' option disabled in User Properties', 'End User Reply Behavior (non-requester): Do not allow', 'Find Sender using: Email then Display Name', 'Processing CC'ed User when creating a request: Create user and allow email', and 'Send a copy of all 'Request Failed' messages to:'. The 'Test Settings' section includes a 'Test Account Settings...' button. The 'Dispatch Folder' and 'Dispatch' buttons are also visible.

Configure System Email Account

Mail Server Type: ☐ POP3/SMTP ☐ Exchange Server (EWS) ☒ Microsoft 365 Outlook ☐ IMAP/SMTP

Account Setting Reply Messages Outgoing Request Updates Reopening Request Attachments Block List Ignore List

Account Information

Profile Name: Client3

Email Address: client3@helpstar.com

Account Name: client3@helpstar.com

Authentication Kind: OAUTH 2.0

Account Password:

Domain: helpstar.com

Dispatch Folder Dispatch

Server Information

Microsoft 365 Outlook Settings

URL: https://graph.microsoft.com/v1.0

Authentication Type: Exchange Authentication

Agent Mailbox Name:

Agent Mailbox Email:

Agent Password:

Properties

☐ Process Emails from Users with the 'Email' option disabled in User Properties

End User Reply Behavior (non-requester): Do not allow

Find Sender using: Email then Display Name

Processing CC'ed User when creating a request: Create user and allow email

Send a copy of all 'Request Failed' messages to:

☒ Create text log for incoming email ☒ Create text log for outgoing email

Test Settings

After filling out the information on this screen, we recommend that you test your account by clicking on the button below. (Requires network connection)

Test Account Settings...

Save Cancel



1.1.1.1. Microsoft 365 Outlook Settings

- **Exchange Authentication** - uses the credentials specified in the Account Information section to authenticate to the system. A password is required within ServicePRO but the ServicePRO Starwatch Service can be run under the default "Local System" account.
- **Agent Authentication** - uses a separate mailbox's name, email address, and password to authenticate to the system email account which can now be specified in the Microsoft 365 Outlook Settings section. Please make sure that the designated agent mailbox has proper access to the System email account mailbox.

In order to use a Shared Mailbox for system email account, Agent Authentication method should be used, by specifying one of the user mailbox credentials that has access to the shared mailbox, under the Agent Authentication section. Note: The account being used must have the application impersonation role set on itself in the Exchange Admin console so that it can send emails on behalf of another account.

1.1.2. OAUTH 2.0 Settings for Microsoft 365 Outlook

When "Microsoft 365 Outlook" server type is chosen, the only option available for "Authentication Kind" is OAUTH 2.0.

- ServicePRO and StarWatch Service will access the mailbox using the OAuth 2.0 authentication method, by utilizing the Application ID, Tenant ID and Client Secret (Only for Government Clients, GCC Client Endpoint URL as well) that is entered in the OAUTH 2.0 settings dialog that opens when ellipsis button beside "Authentication Kind" field is selected.

1.1.2.1. OAuth 2.0 Microsoft 365 Outlook Authentication - Prerequisites

In order to enable the OAuth 2.0 Microsoft 365 Outlook Authentication kind, the following the prerequisites must be met.

1.1.2.1.1. Register ServicePRO Application in Azure

To use OAuth, ServicePRO application must have an application ID issued by Microsoft Entra ID [Previously called, Azure Active Directory].

You must register an application in the Azure Portal (Microsoft Entra ID) <https://portal.azure.com/> before filling in the OAUTH 2.0 Settings in the System Email Account Setup and User Mail Server Setting.

Step 1: App Registration

1. Navigate to Microsoft Entra ID and select App Registrations.
2. Click on New Registration.
3. Provide the required details.

Note: Set the Redirect URI according to your environment (e.g., <https://example.com/auth/azure-login>).



Register an application ...



* Name

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

ServicePRO Graph API Application



Supported account types

Choose the account types that can use this application or access this API

Single tenant only - Help Desk Technology



[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.

Single-page application (SPA)



http://localhost:4200/auth/azure-login



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

Step 2: Authentication Settings

1. Navigate to the Authentication Option.
2. Locate the token issuance settings.
3. Enable both the Access tokens and ID tokens options

Search

Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Welcome to the new and improved experience for authentication. [To switch to the old experience, please click here.](#)

Redirect URI configuration

Supported accounts

Settings

Web and SPA settings

The following settings are only applicable when building a web or SPA application.

Implicit grant and hybrid flows

The implicit grant allows an application to request a token directly from the authorization endpoint. It is only recommended for browser-based single-page applications (SPAs).

☒ Access tokens (used for implicit flows)

☒ ID tokens (used for implicit and hybrid flows)

Front-channel logout URL

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

Allow public client flows [Learn more](#)

☐ Disabled

App instance property lock [Learn more](#)

Configure the application instance modification lock.

Configure

Step 3: Client Secret Creation



1. Navigate to Certificates & secrets.
2. Click on New client secret and generate the key.
3. Copy the secret value immediately, as it will be hidden later.

Search

Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

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
Used in development	9/30/2027	Gix*****	b533f1b2-281d-40e0-92...

Step 4: API Permissions

1. Navigate to API permissions.
2. Add the below required Microsoft Graph permissions for Application type providing Admin Consent.
Calendar.ReadWrite, Contacts.ReadWrite, Directory.Read.All, Group.Read.All, Mail.ReadWrite, Mail.Send, User.ReadAll

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 Help Desk Technology

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (7)				
Calendars.ReadWrite	Application	Read and write calendars in all mailboxes	Yes	✓ Granted for Help Desk T... ***
Contacts.ReadWrite	Application	Read and write contacts in all mailboxes	Yes	✓ Granted for Help Desk T... ***
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for Help Desk T... ***
Group.Read.All	Application	Read all groups	Yes	✓ Granted for Help Desk T... ***
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	✓ Granted for Help Desk T... ***
Mail.Send	Application	Send mail as any user	Yes	✓ Granted for Help Desk T... ***
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for Help Desk T... ***



1.1.2.2. Updating OAUTH 2.0 Settings for Microsoft 365 Outlook

In the System Email Account Setup, when Microsoft 365 Outlook server type is selected, please make sure to click on the ellipsis button next to the Authentication Kind field. Update the keys in the UI for the Application ID, Tenant ID and Client Secret that were captured after completing the above step (i.e. Register ServicePRO Application in Azure)

OAUTH 2.0 Settings

Application Id :

Tenant Id :

Client Secret : Gix8

GCC Client Endpoint URL :

Save Cancel

OAuth 2.0 Settings for Microsoft 365 Outlook - System Email Account

- Application Id: From the registered application in Azure (pre-requisites section)
- Tenant Id: From the registered application in Azure (pre-requisites section)
- Client Secret: From the registered application in Azure (pre-requisites section)
- GCC Client Endpoint URL: this is only for government azure client, check with the client if they are using GCC in Azure and ask to provide the URL, usually for US it is <https://login.microsoftonline.us> but it also requires to make changes in the URL in Microsoft 365 Outlook Settings in ServicePRO (instead of <https://graph.microsoft.com/v1.0> , it should be <https://graph.microsoft.us/v1.0>)

1.2. Enhancements in User Mail Server Settings

In the “User Email Accounts – Mail Server Settings” screen, for the Mail Server Type selection, a new option “Microsoft 365 Outlook” has been added. Please make sure to select this Mail Server Type if you are using Office 365 / Exchange Online Mailboxes for the users in your organization.

Configure User Email Settings

Mail Server Settings

Configured Server(s)

Server Name: LiveGraphClient

Server Type: ☐ POP3 ☐ EWS ☐ IMAP ☒ Microsoft 365 Outlook

URL:

Authentication Kind: ...

Domain:

LiveGraphClient



When " Microsoft 365 Outlook " server type is selected, a new field "EWS Authentication Kind" shows up.

When "Microsoft 365 Outlook" server type is chosen, the only option available for "Authentication Kind" is OAUTH 2.0. ServicePRO accesses the user's mailboxes using the OAuth 2.0 authentication method, by utilizing the Application ID, Tenant ID and Client Secret (Only for Government Clients, GCC Client Endpoint URL as well) that is entered in the OAUTH 2.0 settings dialog that opens when ellipsis button beside "Authentication Kind" field is selected.

A screenshot of the "OAUTH 2.0 Settings" dialog box. The dialog has a blue header bar with the title "OAUTH 2.0 Settings" and a close button (X) on the right. Below the header, there are four input fields: "Application Id" (yellow), "Tenant Id" (yellow), "Client Secret" (yellow, with "Gix8" visible), and "GCC Client Endpoint URL" (white). At the bottom, there are two buttons: "Save" and "Cancel".

OAuth 2.0 Settings for Microsoft 365 Outlook – User Mail Server Settings

In order to enable the OAuth 2.0 Authentication kind for Microsoft 365 Outlook, the pre-requisites detailed in the following section must be met - [1.1.2.1. OAuth 2.0 Microsoft 365 Outlook Authentication – Prerequisites](#). Please make sure to click on the ellipsis button next to the field and enter the Application ID, Tenant ID and Client Secret that were captured after completing the pre-requisites step (i.e. Register ServicePRO Application in Azure)

- Application Id: From the registered application in Azure (pre-requisites section)
- Tenant Id: From the registered application in Azure (pre-requisites section)
- Client Secret: From the registered application in Azure (pre-requisites section)
- GCC Client Endpoint URL: this is only for government azure client, check with the client if they are using GCC in Azure and ask to provide the URL, usually for US it is <https://login.microsoftonline.us> but it also requires to make changes in the URL in Microsoft 365 Outlook Settings in ServicePRO (instead of <https://graph.microsoft.com/v1.0> , it should be <https://graph.microsoft.us/v1.0>)

Note: When using Microsoft 365 Outlook server type for User Email Settings, users cannot change the mailbox in the email inbox (this behavior mirrors EWS OAUTH 2.0 with Integrated Security).

Note: When using EWS with OAUTH 2.0 for User Email Settings, users cannot change the mailbox in the email inbox.



1.3. User Options:

 **Email Setup** Save Cancel Help Info

General

Defaults

Colors

Security

Communication

Email

Text Messaging

Calendar

Editing and Printing

Refresh Timer Settings

My Email Account

NOTE:
ServicePRO is configured to use Microsoft 365 Outlook.
It uses following email address:

bpatel@helpstar.com

Please use Setup -> User Email Settings option to change this email address,
otherwise please contact your ServicePRO Administrator to change this email address

Send Email

Default 'Send Email' Account:

Signature: ☒ Plain Text ☐ HTML

Email Inbox

Note: When using Microsoft 365 Outlook server type for User Email Settings, users cannot change the settings under **User Options -> Email -> My Email Account** section.

Note: When using EWS with OAUTH 2.0 for User Email Settings, users cannot change the settings under **User Options -> Email -> My Email Account** section.