Process Director Documentation

Configuring Azure OAuth

BP LOGIX

Process Driven, Business Focused

Last Updated: 2024-02-05, 09:48

TOC

Configuring Azure for Process Director Integration

Microsoft Modern Authentication (an OAuth-based authentication system) provides much more secure access to SharePoint, SMTP email, and other Azure services from Process Director, but does require a complex setup process. To set up Modern Authentication between Azure and Process Director, you must complete the following steps.

1. Create a certificate to authenticate Process Director with Azure.
   a. Using Microsoft's certreq.exe, installed on all modern Windows OS versions.
   b. Using PowerShell, also included with all modern Windows OS versions.
2. Add Process Director as a Registered Active Directory application in the Azure Active Directory portal.
   a. Add the public key certificate to the Process Director application in Azure.
   b. Configure the appropriate Azure settings.

In this topic, we'll address each of these required steps in detail. Additional information about this topic can also be obtained from Microsoft's online documentation.

> ❗ You cannot configure any OAuth settings for SharePoint Datasources or SMTP Email in Process Director until you have created and registered an Azure Active Directory Application in Azure by completing the steps described in this topic.

Create a certificate to authenticate Process Director with Azure

Microsoft prefers the use of certificates for authentication. Each certificate includes both the public and private keys used to encrypt data. The public key (in a CER file) is used by SharePoint Online to authenticate Process Director. The private key is packaged in a password-protected PFX file and is used by Process Director to authenticate with Azure Services. There are two methods that can be used on Windows-based systems to create a proper certificate.

- Using Microsoft's certreq.exe, installed on all modern Windows OS versions.
- Using PowerShell, also included with all modern Windows OS versions.

> ❗ Keep in mind that certificates expire after a set period of time. Most organizations specify the maximum length of time certificates should be used. By default, the instructions that follow will generate certificates valid for one year. You should, therefore, generate and install new certificates well before existing certificates expire. This implies that your organization also has a mechanism in place to be reminded when expiration is approaching, to ensure that service interruptions don't occur.

Creating a Certificate with certreq.exe

This method of certificate creation might be preferred if you're less comfortable with command-line operations and don't intend to automate the generation of certificates. Microsoft's online documentation has additional information about certreq.exe.

Instructions

First, using a text editor like Notepad, copy and paste the following text into a new document:

```
[Version]
Signature = "$Windows NT$"

[Strings]
szOID_ENHANCED_KEY_USAGE = "2.5.29.37"
szOID_KEY_ENCIPHERMENT = "1.3.6.1.5.5.7.3.1"

[NewRequest]
Subject = "cn=BP Logix Process Director"
MachineKeySet = false
KeyLength = 2048
HashAlgorithm = Sha1
Exportable = true
RequestType = Cert

KeyUsage = "CERT_KEY_ENCIPHERMENT_KEY_USAGE"
; The following values can be changed to generate certificates that expire
; sooner or later depending on your organizations needs. The default is 1 year.
ValidityPeriod = "Years"
ValidityPeriodUnits = "1"

[Extensions]
%szOID_ENHANCED_KEY_USAGE% = "{text}%szOID_KEY_ENCIPHERMENT%"
```

Once you've done so, save the document as an INF file in a folder on your system, e.g., `c:\Users\Some.User\Documents\PD Certificate\CertReq.inf`.

Open the Windows Command Prompt. You can press the [WINDOWS] key, type "cmd", then select the "Command Prompt" application.

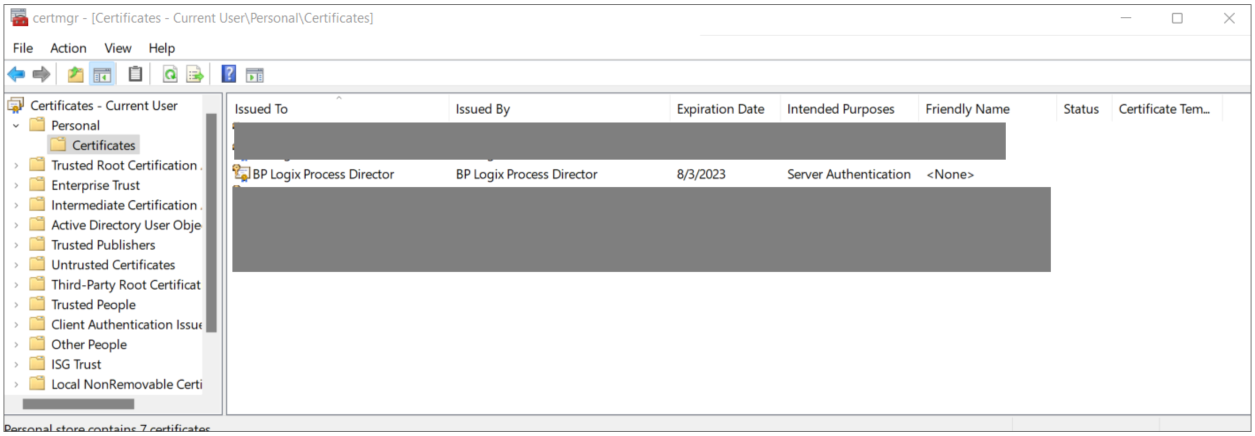
In the Command Prompt, open the directory in which you installed the INF by using the cd command, and the folder path to the INF file, then pressing the [ENTER] key. Using the example above, you'd need to type:

```
cd c:\Users\Some.User\Documents\PD Certificate\
```

Once the directory changes, type the following and press the [ENTER] key to run the certreq application.

```
certreq -new certreq.inf PublicKey.cer
```

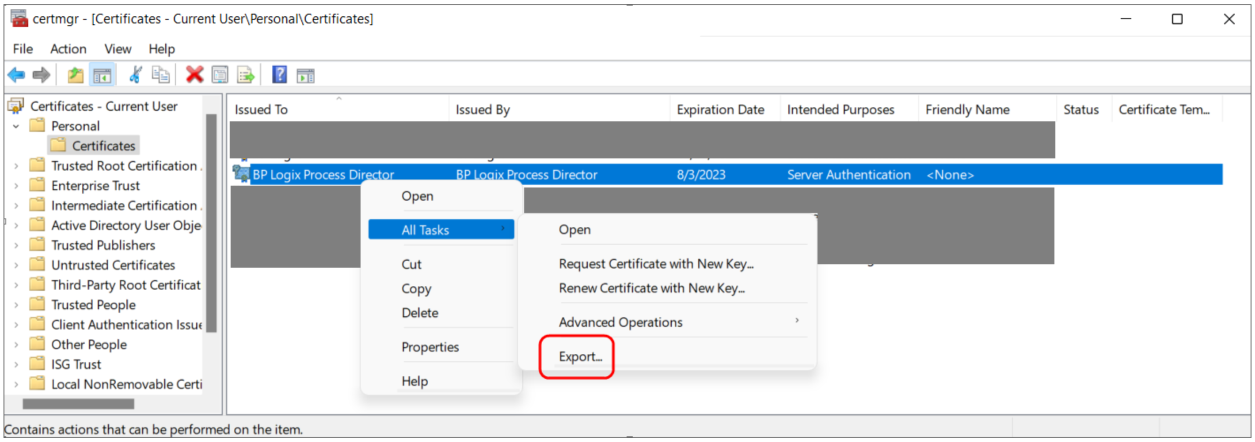
Running the certreq application will create the certificate, and add it to the Windows Certificate Manager. To continue, you'll need to open the Certificate Manager to access the new certificate. To open the Certificate Manager, you can press the [WINDOWS] key, type "certmgr", then select the "Manage computer certificates" option. When the Certificate Manager opens, you'll need to navigate to the `Personal\Certificates` folder, where you should see the certificate issued to and by BP Logix Process Director.


certmgr - [Certificates - Current User\Personal\Certificates]
File Action View Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification
Enterprise Trust
Intermediate Certification
Active Directory User Obje
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificat
Trusted People
Client Authentication Issue
Other People
ISG Trust
Local NonRemovable Certi

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
[redacted]						
BP Logix Process Director	BP Logix Process Director	8/3/2023	Server Authentication	<None>		
[redacted]						

Personal store contains 7 certificates.

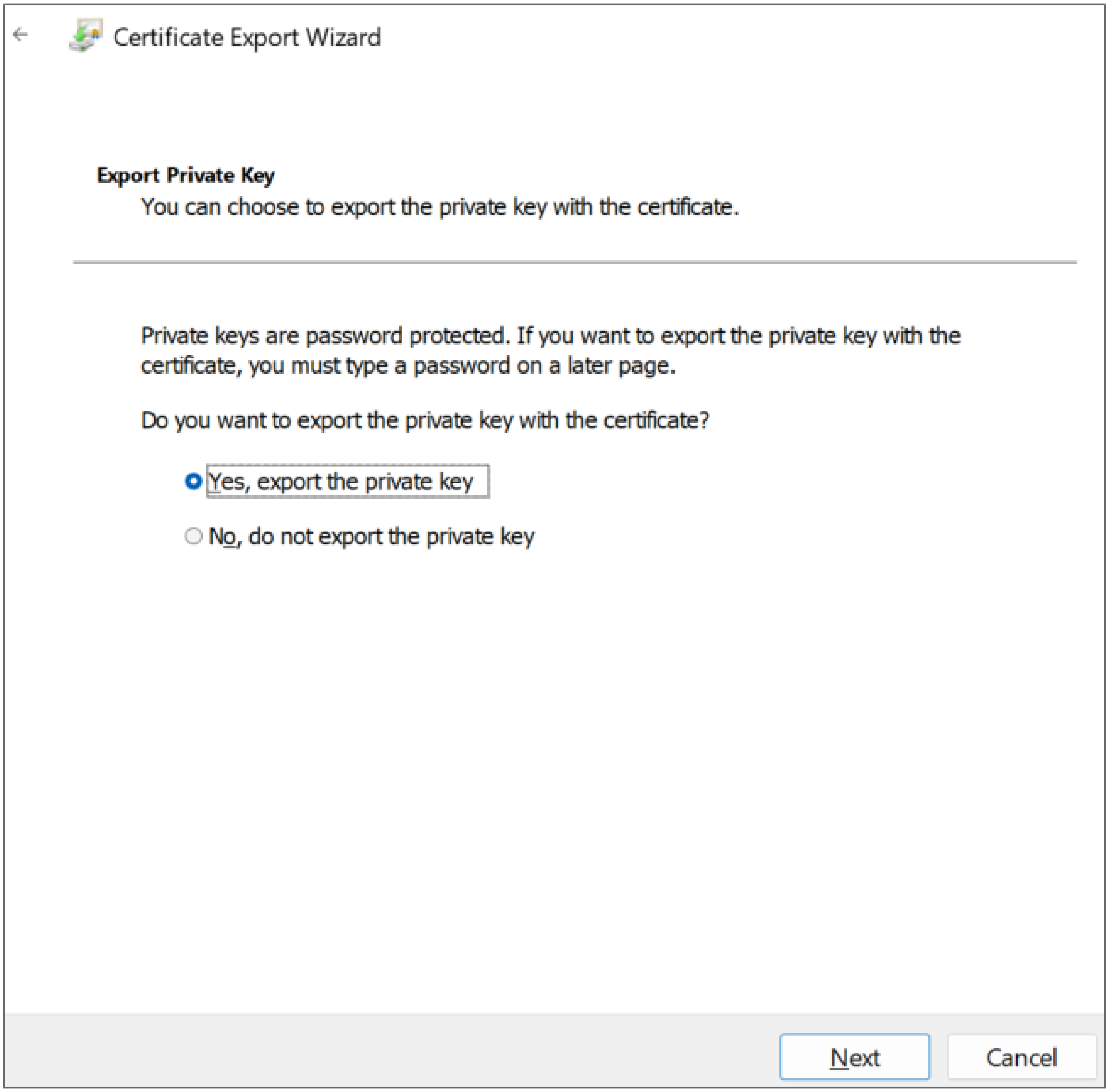
Right-click that certificate and then select All Tasks > Export.


certmgr - [Certificates - Current User\Personal\Certificates]
File Action View Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification
Enterprise Trust
Intermediate Certification
Active Directory User Obje
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificat
Trusted People
Client Authentication Issue
Other People
ISG Trust
Local NonRemovable Certi
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Renew Certificate with New Key...
Advanced Operations
Export...

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
[redacted]						
BP Logix Process Director	BP Logix Process Director	8/3/2023	Server Authentication	<None>		
[redacted]						

Contains actions that can be performed on the item.

The Certificate Export Wizard will open. On the first screen, click the Next button. On the Export Private Key screen, select Yes, export the private key, then click the Next button.



Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

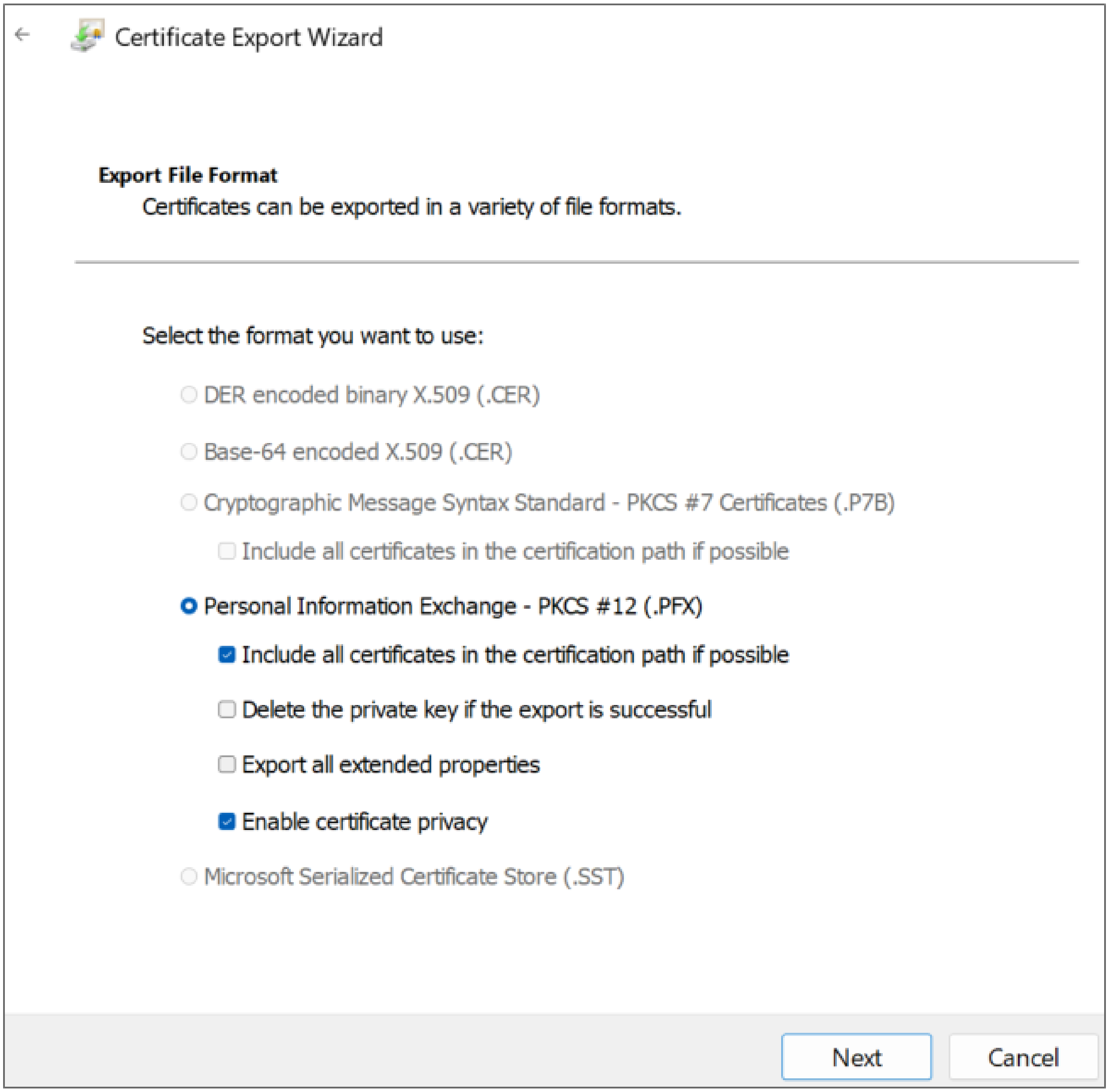
Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

On the Export File Format screen of the Wizard, Ensure that you select the following options:

- Personal Information Exchange - PKCS #12 (.PFX)
- Include all certificates in the certification path, if possible
- Enable certificate privacy



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

☑ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

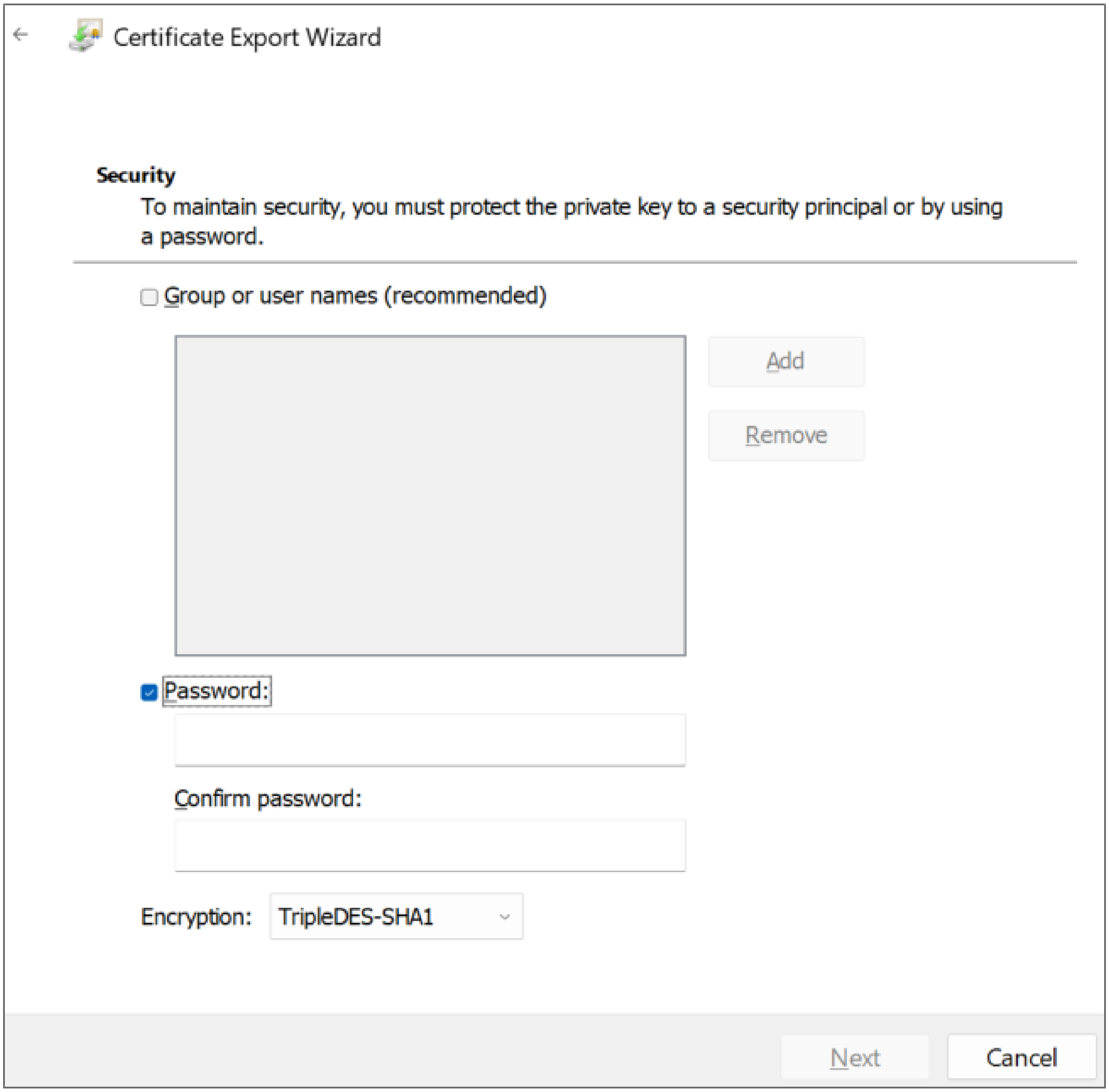
☑ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

On the Security screen, check Password as the security protocol and enter a password twice.

ⓘ Be sure to store this password securely, you'll need it in future steps.

! Be sure to use a long, sufficiently complex password in line with your organization’s cryptographic standards.



Certificate Export Wizard

Security

To maintain security, you must protect the private key to a security principal or by using a password.

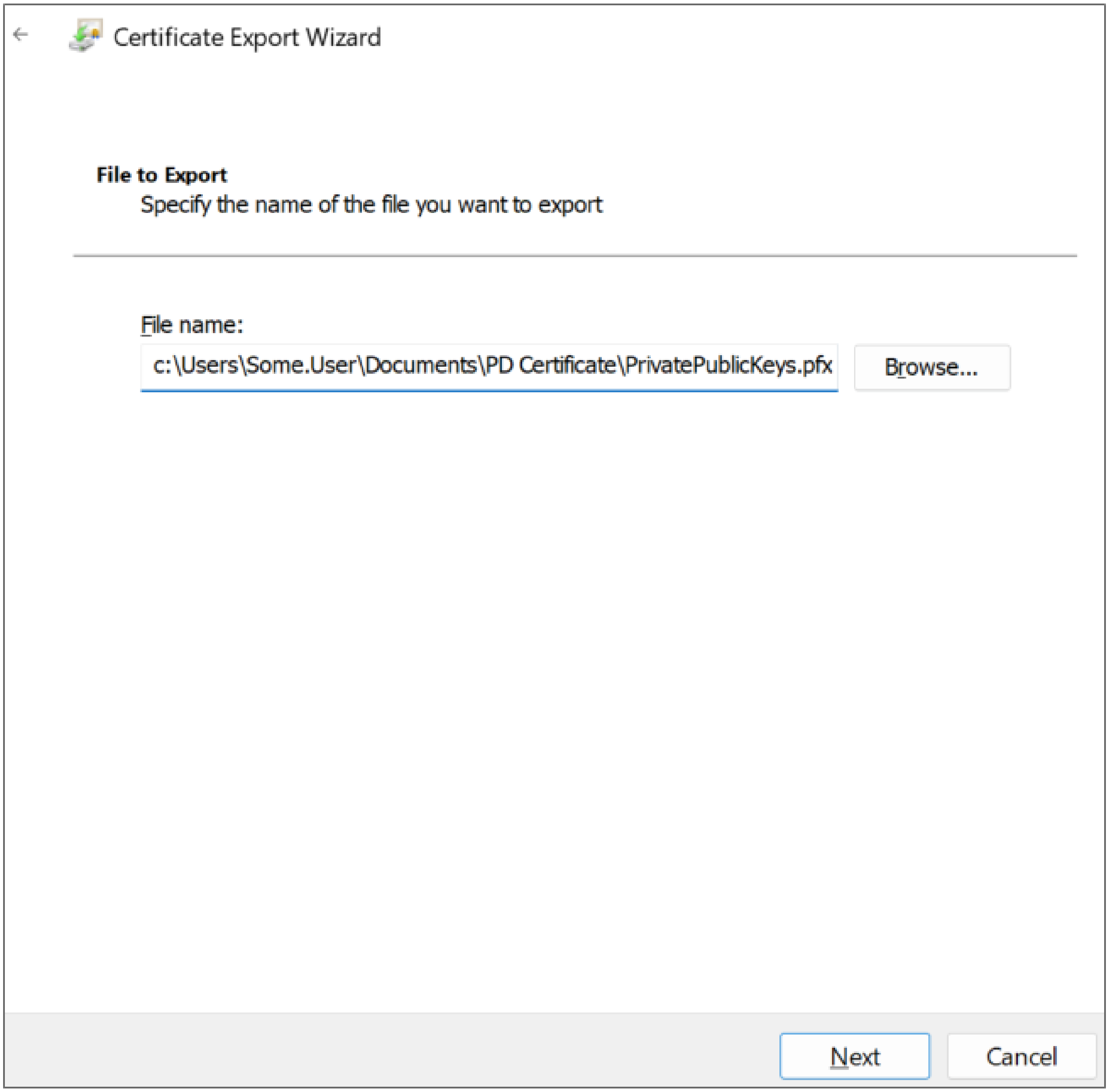
□ Group or user names (recommended)

☑ Password:

Confirm password:

Encryption: TripleDES-SHA1

On the File to Export screen, store the resulting PFX file in the same folder as you stored the CertReq.Inf and PublicKey.Cer files, then click the Next button.



File to Export

Specify the name of the file you want to export

File name: c:\Users\Some.User\Documents\PD Certificate\PrivatePublicKeys.pfx

Click the Finish button on the next Wizard screen, then OK to finish the Wizard and close it.

BP Logix recommends that you remove the certificate installed in the Certificate Manager by right-clicking it and then selecting Delete followed by Yes to delete it in the confirmation dialog.

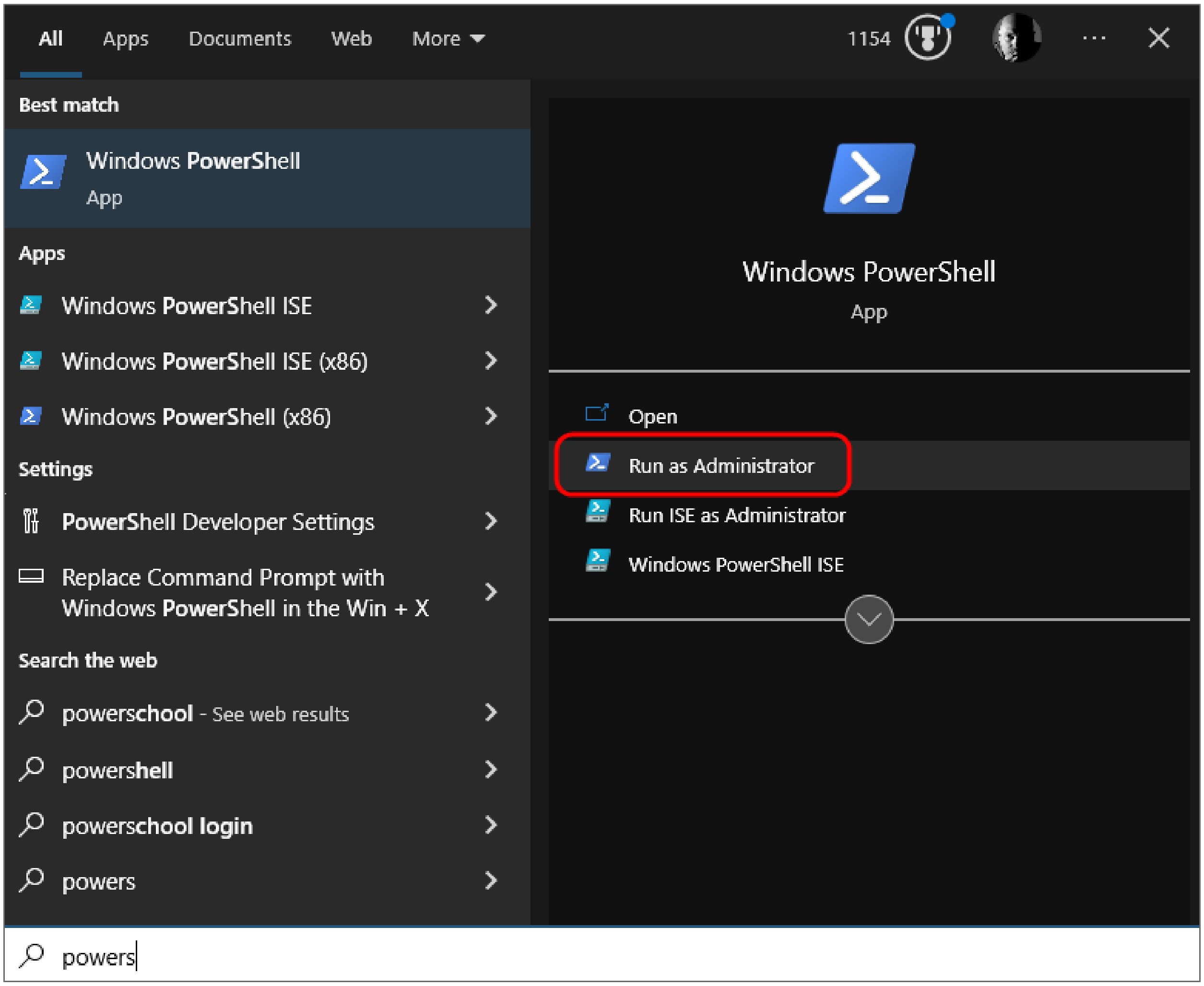
Keep both the PublicKey.cer and PrivatePublicKeys.pfx files handy for subsequent steps in this setup process. You should also archive them in a secure, backed up location as well.

Creating a Certificate with PowerShell

PowerShell is a command line application that's included with all modern versions of Windows. You can choose this method if you're comfortable with PowerShell and might want to automate certificate generation on a recurring basis.

Instructions

Open PowerShell by pressing the [WINDOWS] key, typing "PowerShell" then selecting the Run as Administrator option to open Windows PowerShell.



In PowerShell, create or navigate to the directory you'd like to use to store the certificate files. Once you're in the desired directory, run the following command:

```
$cert = New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\ -
KeyUsage KeyEncipherment
    -KeyAlgorithm rsa -KeyLength 2048 -subject "BP Logix Process Director"
    -DnsName "BP Logix Process Director" -Type SSLServerAuthentication
    -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.1")
```

Next, run these commands in PowerShell, replacing `<password>` with a password of your choosing. Ensure the passowrd is cryptographically secure, in accordance with your organization’s standards. Be sure to also store this password securely, as you'll need it in future steps.

```
$pwd = ConvertTo-SecureString -String '<password>' -Force -AsPlainText
$path = 'cert:\LocalMachine\My\' + $cert.Thumbprint
```

Finally, run these commands to create the .PFX and .CER files. Modify the `<path>` value to store the file in a location of your choosing.

```
Export-PfxCertificate -cert $path -FilePath <path>\PrivatePublicKeys.pfx -Pass-
word $pwd
Export-Certificate -cert $path -FilePath <path>\PublicKey.cer
```

Keep both the PublicKey.cer and PrivatePublicKeys.pfx files handy for subsequent steps in this setup process. You should also archive them in a secure backup location as well.

Add Process Director to Azure

To add Process Director as an application in your Azure Active Directory portal at the Tenant level, complete the steps below after signing into your Azure portal (portal.azure.com):

1. Register Process Director as an Application

A. If you have access to multiple tenants, use the Directories + subscriptions filter in the top menu to switch to the tenant in which you want to register the application.
B. Search for and select Azure Active Directory.
C. Under Manage, select App registrations > New registration.
D. Enter a display Name for your application, e.g., “Process Director”. This name can be changed later, if needed.
E. Specify who can use the application. Typically, only accounts in this organizational directory should be used. See the Microsoft documentation titled Quickstart: Register an application with the Microsoft identity platform for more information.
F. Add the Redirect URI, which is the URI for your Process Director installation, e.g., https://my-org.bplogix.net.
G. Click the Register button to register the application.

2. Add Your Public Key Certificate

To add your public key certificate to the Process Director application in Azure, complete the steps below.

A. In the Azure portal, in App registrations, select the Process Director application you created previously, e.g., “Process Director”, as in step 1D, above.
B. Select Certificates & secrets > Certificates > Upload certificate.
C. Select the PublicKey.cer file you created earlier.
D. Upload the certificate file to Azure.

Your AAD Application should now be properly registered and secured with a certificate.

Conclusion

Congratulations! Assuming that you've correctly followed the instructions above, you've now configured an Azure Integration with Process Director. To complete the integration, you'll need to perform some additional, specialized configuration in Azure, depending on whether you're trying to:

- Create a Sharepoint data source or
- Set up SMTP email access on the Properties page of the IT Admin area's Installation Settings section, using the "Office365/Microsoft OAuth" SMTP Authentication Type.

SharePoint Data Sources

With the implementation of Microsoft's move to **Modern Authentication**, using the Microsoft identity platform, logging into cloud-based versions of SharePoint is no longer possible by simply using a user name and password. Legacy installations that user older versions of SharePoint may still do so, but SharePoint has largely implemented an OAuth-based authentication scheme, with additional security provided by the use of encryption certificates.

In Process Director v5.44.1000, Modern Authentication for SharePoint was implemented using the SharePoint OAuth Datasource, which only gives access to SharePoint at the Tenant (organizational) level.

For Process Director v5.44.1103, The SharePoint OAuth Datasource was renamed to SharePoint OAuth (Tenant), while a new Datasource SharePoint OAuth (Site), was added to give access to SharePoint at the Site level, rather than at the entire tenant.

The existing SharePoint Datasource, which uses the simple username/password authentication scheme, is still available for customers who are using older versions of SharePoint. This legacy authentication method should be relevant to only a very small minority of customers, and has been renamed to SharePoint Legacy.

This update to the SharePoint Datasources will require updating the SharePoint Custom Tasks!

Configuring a SharePoint OAuth (Tenant) Datasource

Modern Authentication provides much more secure access to SharePoint, but does require a more complex setup process. To set up Modern Authentication between SharePoint and Process Director, you must first create and register an Azure Active Directory (AAD) application. The System Administrator's Guide has instructions for creating the AAD application in the Configuring Azure for Process Director Integration topic.

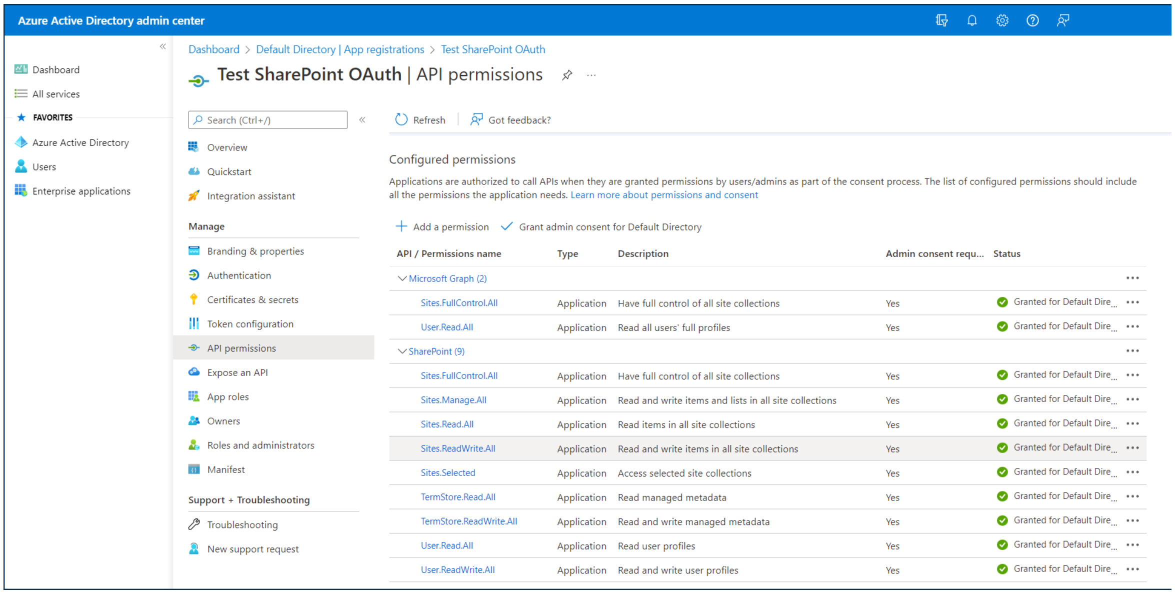
Once you've created the AAD Application, you can begin the process for configuring SharePoint Online.

Configure SharePoint Online permissions

To configure the AAD application to use SharePoint with Process Director, you'll need to perform the following configuration steps:

1. If you have access to multiple tenants, use the Directories + subscriptions filter in the top menu to switch to the tenant in which you want to register the application.
2. Search for and select Azure Active Directory.
3. Under Manage, select App registrations, then select your Process Director application In this example, we'll use “Test SharePoint OAuth” as the AAD Application name, though, of course, the name you use may vary.

4. Click API permissions.
5. Click Add a permission and add all permissions displayed below to the SharePoint section of the API Permissions area:



Test SharePoint OAuth | API permissions

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

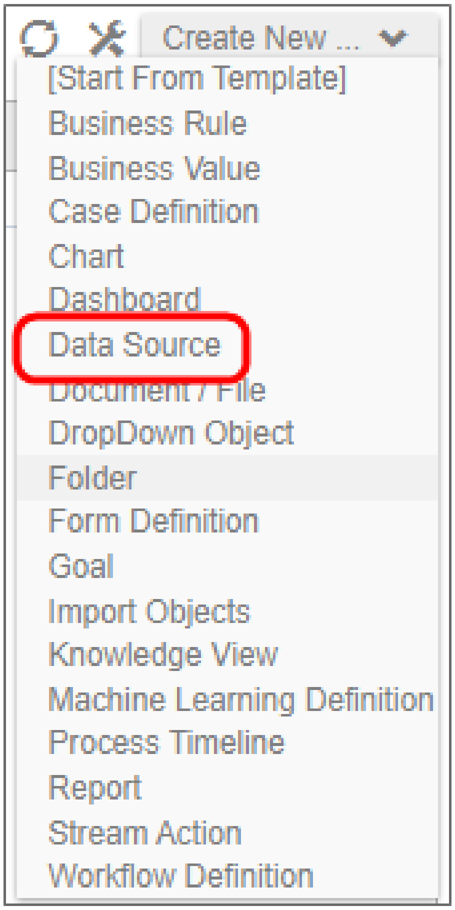
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (2)				
Sites.FullControl.All	Application	Have full control of all site collections	Yes	✓ Granted for Default Dire...
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for Default Dire...
SharePoint (9)				
Sites.FullControl.All	Application	Have full control of all site collections	Yes	✓ Granted for Default Dire...
Sites.Manage.All	Application	Read and write items and lists in all site collections	Yes	✓ Granted for Default Dire...
Sites.Read.All	Application	Read items in all site collections	Yes	✓ Granted for Default Dire...
Sites.ReadWrite.All	Application	Read and write items in all site collections	Yes	✓ Granted for Default Dire...
Sites.Selected	Application	Access selected site collections	Yes	✓ Granted for Default Dire...
TermStore.Read.All	Application	Read managed metadata	Yes	✓ Granted for Default Dire...
TermStore.ReadWrite.All	Application	Read and write managed metadata	Yes	✓ Granted for Default Dire...
User.Read.All	Application	Read user profiles	Yes	✓ Granted for Default Dire...
User.ReadWrite.All	Application	Read and write user profiles	Yes	✓ Granted for Default Dire...

Create the SharePoint OAuth (Tenant) Datasource

Now that the application has been fully registered in Azure, and the appropriate SharePoint API permissions have been set, you can create the SharePoint OAuth Datasource in Process Director. Be sure to keep the Azure window open, however, as you'll need to transfer some information from Azure to configure the SharePoint OAuth Datasource. Ensure you've opened the Azure Active Directory admin center window to the Overview tab of the App registrations page of your Process Director integration app. In this example, we'll use the "Test SharePoint OAuth" application we used in the steps above.

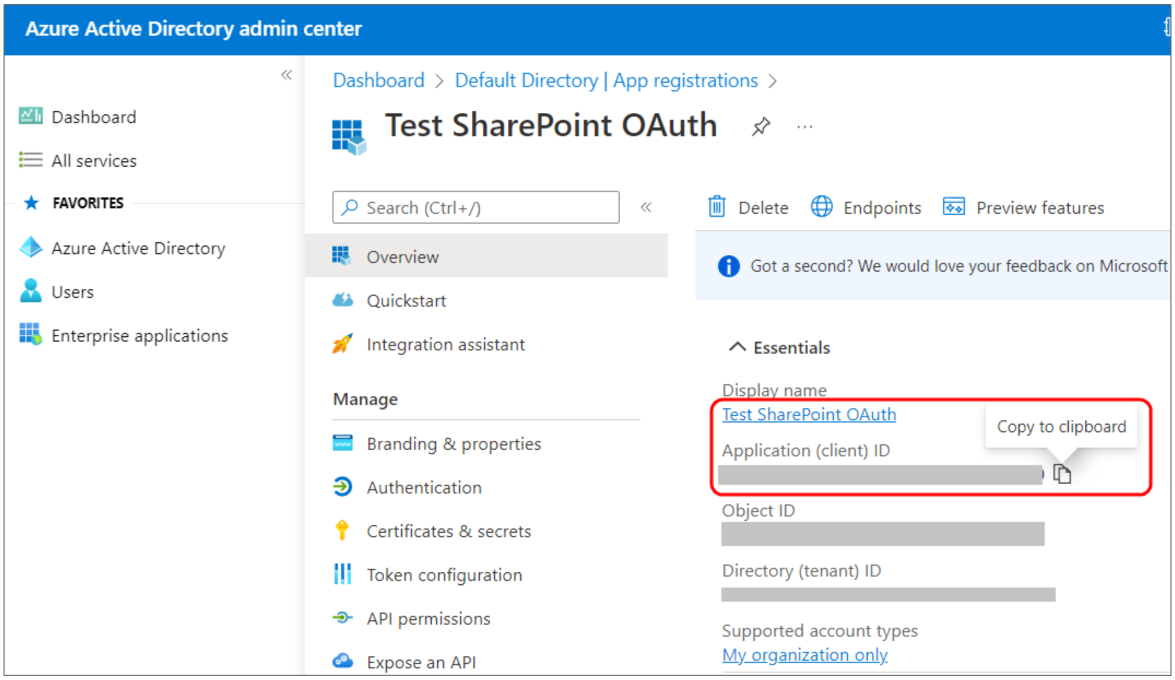
Instructions

1. Navigate to the Process Director folder in which you want to store the new Datasource, then select Data Source from the Create New menu.



2. In the Create New Data Source screen, enter an Name for the Datasource, then click the OK button to create the Datasource and open its configuration screen.
3. On the Properties tab of the Datasource definition, change the DataSource Type to "SharePoint OAuth (Tenant)".
4. Set the SharePoint Site URL to the URL your SharePoint Online server.
5. To set the Client ID property, go to the Azure window, and using the "Copy to Clipboard" icon, copy the value in the Application (client) ID property, then paste it into the Client ID Property of the

Datasource definition.



Display name: Test SharePoint OAuth

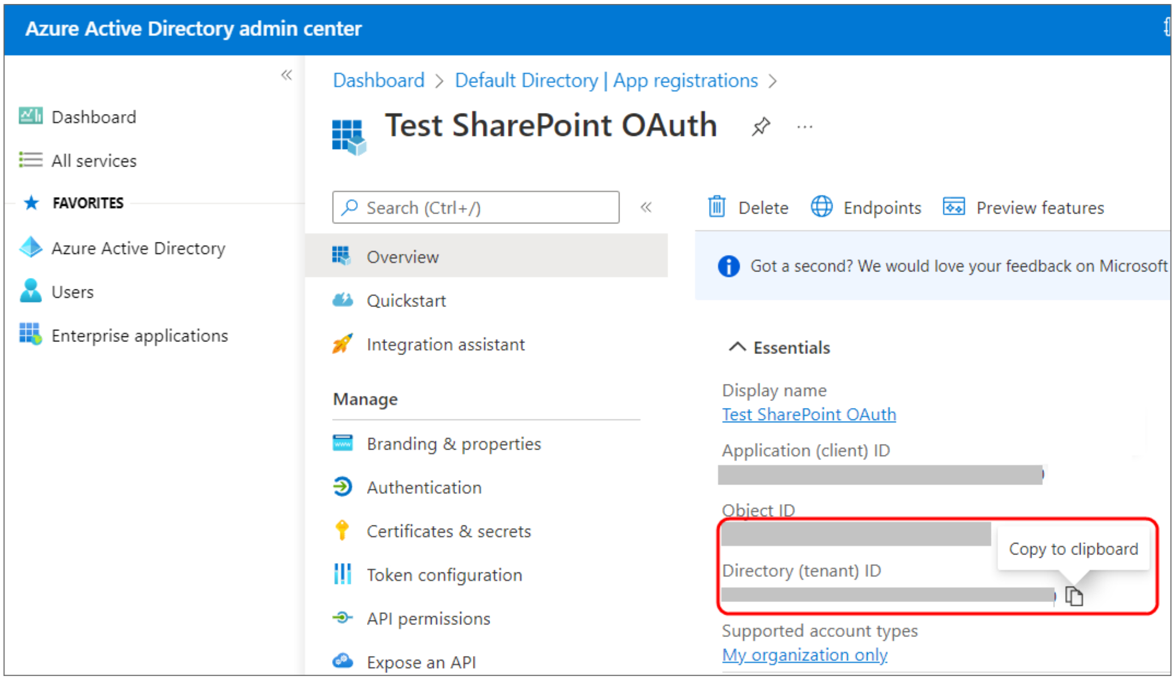
Application (client) ID: [redacted]

Object ID: [redacted]

Directory (tenant) ID: [redacted]

Supported account types: My organization only

6. Similarly, you'll need to copy the value of the Directory (tenant) ID property in Azure to the Tenant ID property of the Datasource definition.



Display name: Test SharePoint OAuth

Application (client) ID: [redacted]

Object ID: [redacted]

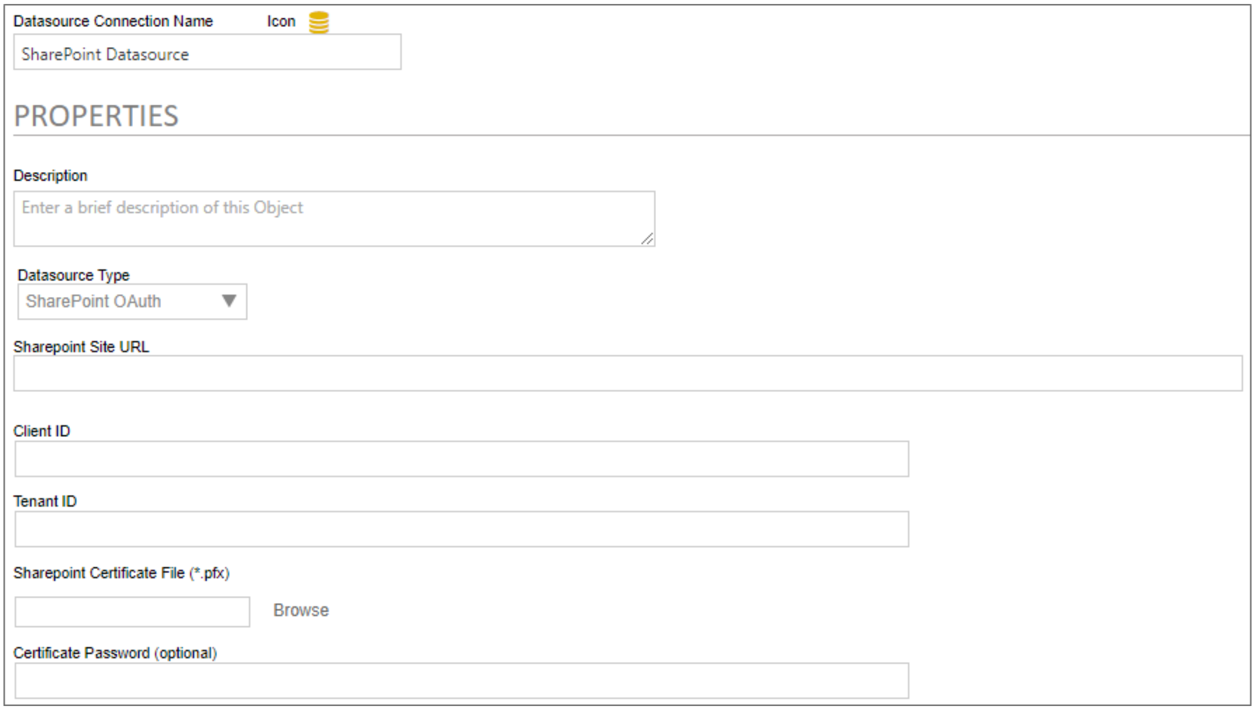
Directory (tenant) ID: [redacted]

Supported account types: My organization only

7. To set the certificate to use for this Datasource, click the Browse button for the SharePoint Certificate File property, then locate and select the PrivatePublicKeys.pfx file you created earlier (either with certreq.exe or PowerShell).
8. Enter the certificate Password that you created for the PrivatePublicKeys.pfx file.

9. Click the OK button to save your changes, then update the Datasource definition by selecting Update from the OK dropdown menu at the upper right corner of the page.
10. Click the Test Connection button to ensure that the Datasource can connect properly to SharePoint.

SharePoint OAuth (Tenant) Datasource Properties



Datasource Connection Name
SharePoint Datasource

Icon

PROPERTIES

Description
Enter a brief description of this Object

Datasource Type
SharePoint OAuth

Sharepoint Site URL

Client ID

Tenant ID

Sharepoint Certificate File (*.pfx)

Browse

Certificate Password (optional)

In addition to the standard Description property, setting the Datasource Type property to *SharePoint OAuth* enables configuration of the connection properties listed below.

SharePoint Site URL

The fully-qualified URL that connects to the SharePoint installation.

Client ID

The value of the Application (client) ID property contained in the App Registration screen in Azure.

Tenant ID

The value of the Directory (tenant) ID property contained in the App Registration screen in Azure.

SharePoint Certificate File

A Content Picker than enables you to browse to and upload the certificate (.PFX) file to Azure.

Certificate Password

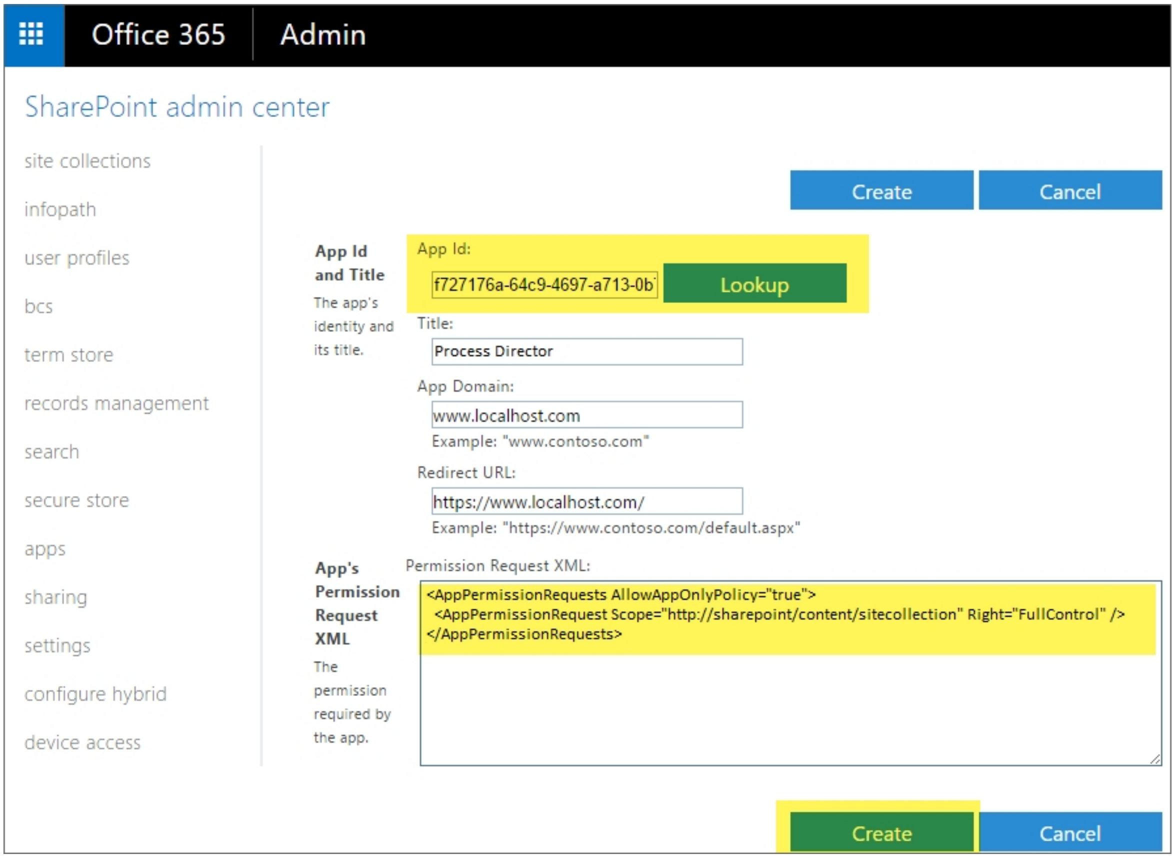
The password that you configured for the certificate (.PFX) file when you created it.

Configuring the SharePoint OAuth (Site) Datasource

Configuring the SharePoint OAuth (Site) Datasource is far less complex than configuring the tenant-level Datasource, and requires no certificate to be created or uploaded to Azure. To add Process Director as an application in your Azure Active Directory portal at the Site level, complete the steps below after signing into your Azure portal (portal.azure.com):

1. Configure SharePoint Site Permissions

1. Navigate to the site you want to configure access for in your tenant. This is typically of the form `https://mytenant.sharepoint.com`, replacing “mytenant” with the appropriate name.
2. Adjust the URL to `https://mytenant.sharepoint.com/_layouts/15/appregnew.aspx`.
   a. Click the buttons to generate both a Client Id as well as a Client Secret.
   b. Select the Client Id value, copy the text and store the value somewhere safe to be used in later steps in this guide.
   c. Select the Client Secret value, copy the text and store the value somewhere safe to be used in later steps in this guide.
3. Now you need to grant permissions to newly registered app (AKA principal). Navigate to `https://mytenant-admin.sharepoint.com/_layouts/15/appinv.aspx`. It’s important to note the addition of “-admin” to your site's normal name.



App Id and Title

The app's identity and its title.

App Id: f727176a-64c9-4697-a713-0b

Title: Process Director

App Domain: www.localhost.com

Example: "www.contoso.com"

Redirect URL: https://www.localhost.com/

Example: "https://www.contoso.com/default.aspx"

App's Permission Request XML

The permission required by the app.

Permission Request XML:

```
<AppPermissionRequests AllowAppOnlyPolicy="true">
  <AppPermissionRequest Scope="http://sharepoint/content/sitecollection" Right="FullControl" />
</AppPermissionRequests>
```

   a. Add your Client Id as App Id.
   b. Add the XML as shown, reproduced here to aid in copy and paste. Note, there are other, more restrictive options that can be considered listed in Table 1 at Microsoft's documentation topic, [Add-in permissions in SharePoint](). Be careful using other values as it may prevent Process Director from working correctly.
```
<AppPermissionRequests AllowAppOnlyPolicy="true">
     <AppPermissionRequest Scope-
e="http://sharepoint/content/sitecollection" Right="FullControl" />
</AppPermissionRequests>
```
   c. Set the Title to “Process Director”.
   d. Set App Domain to the fully qualified domain name of you Process Director deployment.
   e. Set the Redirect URL to the URL of your Process Director deployment.
4. Click Create.
5. Click Trust It in the follow-up prompt.

2. Configure the Datasource

1. In a Process Director Content List folder, select Data Source from the Create New menu.
2. Supply a Name and click OK to open the new Datasource definition.
3. Set the Datasource Type drop-down to "SharePoint OAuth (Site)".
4. Add the SharePoint Site URL for your SharePoint Online installation.
5. Add the Client ID (AKA Application Id) and Client Secret from SharePoint that you set aside in the steps for **Configure SharePoint Site Permissions** above.
6. Click OK then select the Update item from the OK menu at the top right corner of the page to save the configuration.
7. Click theTest Connection button to test your connection to the SharePoint site.

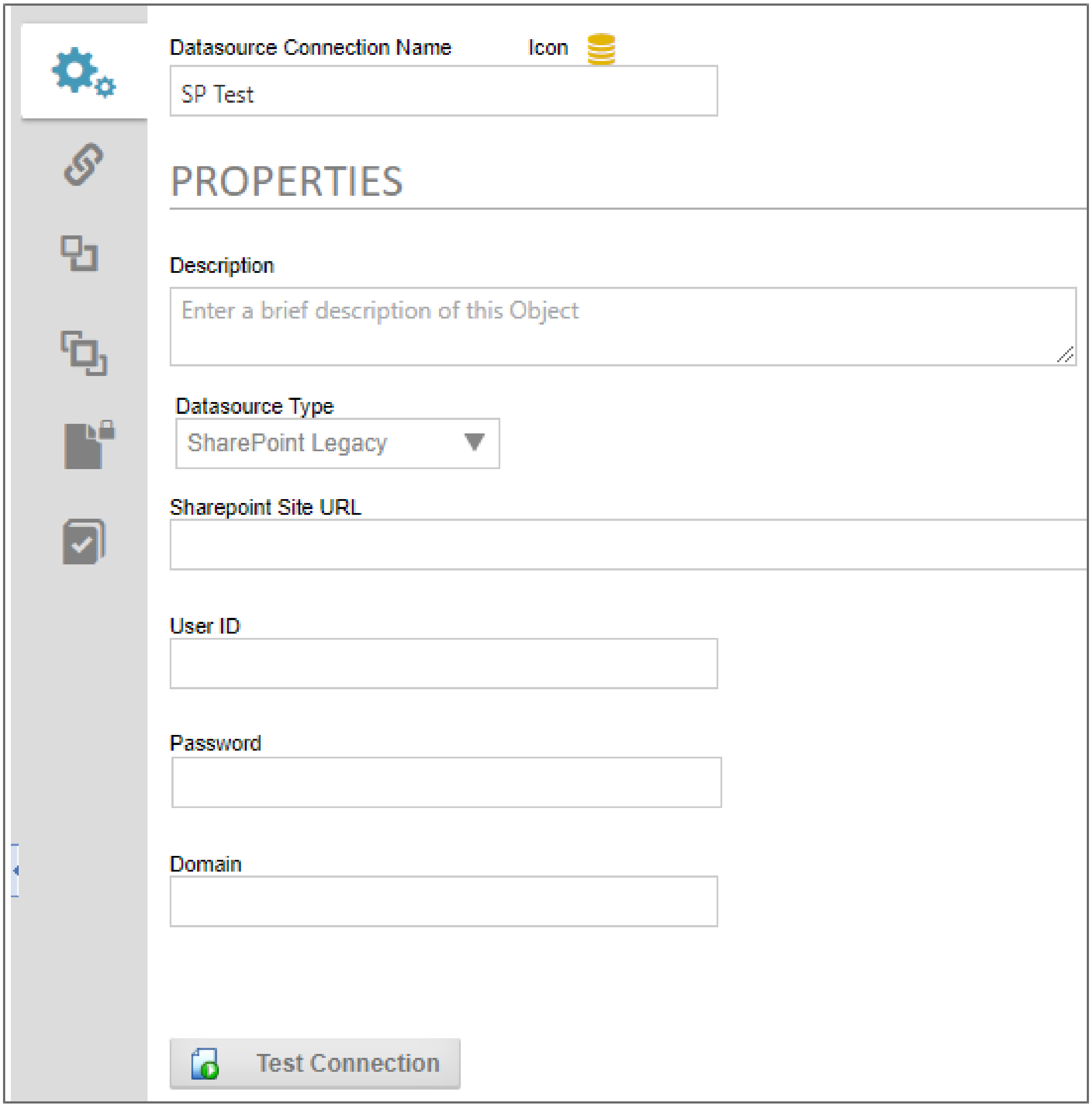
A successful test means that your Datasource is correctly configured and is connecting to the SharePoint site correctly.

Conclusion

Congratulations! Assuming that you've correctly followed the instructions above, you've now configured both SharePoint Online and Process Director. You can now use this Datasource and the SharePoint Custom Tasks in Process Director to integrate your SharePoint sites and data with Process Director.

Sharepoint Legacy Datasource

For connections to pre-OAuth versions of SharePoint, the SharePoint Legacy datasource type enables you to create a datasource connection to the SharePoint server.



Datasource Connection Name: SP Test

Icon

PROPERTIES

Description: Enter a brief description of this Object

Datasource Type: SharePoint Legacy

Sharepoint Site URL:

User ID:

Password:

Domain:

There are four properties to configure to create this datasource.

The Sharepoint Site URL property enables you to enter the fully qualified URL of the Sharepoint server to which you wish to connect.

The User ID must be the user ID for a valid SharePoint User, while the Password property will be the password for the specified user. The Domain property is the SharePoint domain that contains the specified user.

Once you've configured the datasource, you can click the Test Connection button and a message banner will appear, notifying you whether the connection was successful.

Other Datasource Types

To see more information about different Datasource Types and their configuration, please refer top the following topics:

- Common Datasources
- Excel Datasources
- File Datasources
- Social Datasources

Microsoft OAuth for SMTP

To configure integration between Azure and Process Director, you'll first need to create and register an Azure Active Directory (AAD) Application, if you do not have one. Please see the Configuring Azure for Process Director Integration topic for instructions on how to create and register an AAD Application.

Once the AAD Application has been registered, you'll need to perform some additional configuration to the AAD Application's settings in Azure.

First, in the Authentication area, you'll need to set the Allow public client flows property to: `Yes (On)`

Unfortunately, there are many factors that might impact the remaining AAD Application settings you'll need to use. Since that is so, you may wish to reference Microsoft's explanation of SMTP OAuth implementation.

Depending on your Azure installation, as well as your organization's policies, there are different configuration settings that you might need to implement, in order to enable your AAD application to enable Process Director to use OAuth to send mail messages. **BP Logix cannot, therefore, definitively describe what settings might be required to make your Azure installation accept OAuth authentication, as we have no knowledge of, or access to, your Azure configuration.**

> ! **We strongly recommend that you refer to the Microsoft documentation topic on this subject: How to set up a multifunction device or application to send emails using Microsoft 365 or Office 365.**

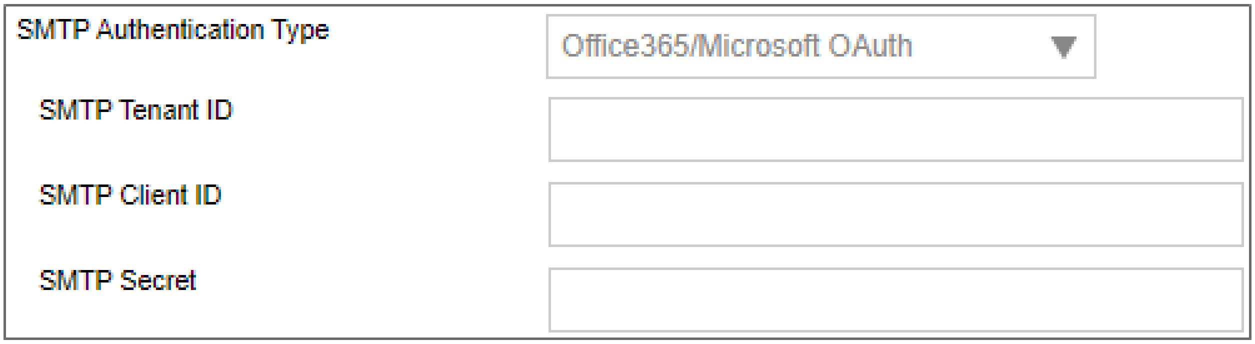
We can provide some common configuration suggestions that have worked for our customers in the past, though ***we cannot guarantee that these settings will work with your specific Azure configuration***.

1. If it's available for your Azure installation, in the Office 365 Exchange Online section of the API Permissions area, you can set the permissions `SMTP.AccessAsUser.All`. This setting is not available for all installations. This setting seems to have been deprecated for recent installations of Azure, in lieu of #2, below.
2. In the Office 365 Exchange Online area, enable the `SMTP.SendAsApp` property. You may also need to enable `IMAP.SendAsUser.All` to true.
3. In the Microsoft Graph section of the API Permissions area, you can enable the following permissions: `Microsoft.Graph Delegated SMTP.Send` and `Delegated User.Read`.
4. For more comprehensive email access, you can set `Microsoft.Graph Delegated IMAP.AccessAsUser.All`.

If no combination of the settings above work for you, you may need to contact your Microsoft Azure technical support representative to assist you with configuring the correct AAD App permissions for your installation.

For more information on authentication permissions, please refer to the Microsoft Graph Permissions Reference from Microsoft. Please be aware that BP Logix has an extremely limited ability to assist you with troubleshooting your Azure installation or settings.

Once configured, you'll need to get the following properties from the AAD Application's settings to transfer to the corresponding OAuth settings for the "Office365/Microsoft OAuth" SMTP Authentication Type, which is found on the Properties page of the Installation Settings section of the IT Admin area.:



SMTP Authentication Type	Office365/Microsoft OAuth ▼
SMTP Tenant ID	
SMTP Client ID	
SMTP Secret	

1. SMTP Tenant ID
   a. The ID of the Azure Tenant in which the AAD Registered App resides (Creation of an AAD Registered App requires the existence of a Tenant)
   b. The Tenant ID is displayed as the Directory (tenant) ID property on the Overview page of your AAD Application in Azure, but this value will also be displayed following `login.microsoft.com/...` in the Endpoint URLs that the App references
2. SMTP Client ID
   a. The ID of the AAD Registered App
   b. This value is displayed as the Application (client) ID property on the Overview page of your AAD Application.
3. SMTP Secret
   a. The client secret or application password the administrator created to use with the AAD Registered App.
4. UserID/Password
   a. Some installations may require that you provide a valid UserID and Password to connect to an email account on your system for sending mail messages, as part of the authentication.

Some Azure configurations may also be configured to require a specific email address be used to send ***all*** mails as the "From" email address. In that case, you will *at least* need to go to the Global Variables page and set the Workflow From Email Address property to the email address you've specified in Azure. You may also wish to set that email address for the Registered Email property on this page (Properties), as a backup to the Global Variables setting.

❗ Be advised that, with this configuration, ALL email addresses sent from the system MUST use the specified email address as the From address. This means that any custom email addresses you configure elsewhere, such as the "From Email" property of a Email Data control in an email template, *will not send email messages.*