Process Director Documentation Configuring Azure OAuth



Last Updated: 2025-01-23, 16:45

ΤΟΟ

Configuring Azure for Process Director Integration	
Create a certificate to authenticate Process Director with Azure #	
Add Process Director to Azure #	12
Conclusion	13
SharePoint Data Sources	13
Configuring a SharePoint OAuth (Tenant) Datasource #	14
Configure SharePoint Online permissions #	14
Configuring the SharePoint OAuth (Site) Datasource #	
Conclusion	21
Microsoft OAuth for SMTP	21
Office365 and CDA #	24
Configuring Azure for Office365 and Collaborative Document Auth (CDA)	oring 25
Configuring SAML Access for O365 CDA	
Configuring "Full Scope" App Registration	
Configuring the "Site" Level App Registration	
Granting "Site" App Registration Permissions	
Securely Transmit Configuration to BP Logix	
Configuring Process Director	
O365 CDA Installation Settings #	48
Configuring SharePoint for External Access	

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. <u>Create a certificate</u> 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. <u>Add Process Director as a Registered Active Directory application</u> 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 <u>Microsoft's online documentation</u>.

• 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 <u>#</u>

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. <u>Microsoft's online documentation</u> 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 U	Jser\Personal\Certificates]						_		\times
File Action View Help									
🗢 🔿 🙍 📰 🗎 🗟 😽	?								
🙀 Certificates - Current User	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificat	e Tem	
 Personal Certificates 	1								
 Trusted Root Certification . Enterprise Trust 	BP Logix Process Director	BP Logix Process Director	8/3/2023	Server Authentication	<none></none>	_			
Intermediate Certification									
Active Directory Oser Obje Trusted Publishers									
Discrete Certificates Third-Party Root Certificat									
Trusted People									
Client Authentication Issue Other People									
> 🛄 ISG Trust									
Denne al stars sentaine 7 autiliantes									

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

ᡖ certmgr - [Certificates - Current l	Jser\Personal\Certificates]							-		×
File Action View Help										
🗢 🔿 🖄 📷 🤞 🗙 🛛	1 📑 🚺 🖬									
 Certificates - Current User Personal 	Issued To	Issued By		Expiration Date	Intended Purposes	Friendly Name	Status	Certific	ate Tem	
Certificates										
 Trusted Root Certification . Enterprise Trust 	BP Logix Process Directo	or BP Logix Pro	cess Director	8/3/2023	Server Authentication	<none></none>				
Intermediate Certification . Active Directory User Obje		All Tasks	Open							
Trusted Publishers		Cut	Request Certificate	with New Key						
Third-Party Root Certificat		Сору	Renew Certificate v	vith New Key						
 Trusted People Client Authentication Issue 		Delete	Advanced Operatio	ons	>					
Other People ISG Trust		Properties	Export							
Cocal NonRemovable Certi		Help								
Contains actions that can be performe	d 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.

÷	F Certificate Export Wizard
	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
	\bigcirc No., do not export the private key
	<u>N</u> ext Cancel

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

÷	F 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) 	
	Next Cancel	

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



To maintain security, you must protect the private a password	ate key to a security principal or b	oy using
 □ <u>G</u> roup or user names (recommended)		
	Add	
	<u>R</u> emove	
Password:		
<u>C</u> onfirm password:		

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	
<u>File name:</u>	
c:\Users\Some.User\Documents\PD Certificate\PrivatePublicKeys.pfx	Browse

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.

A		ps	Documents	Web	More 🔻					1154 😨		×
Best	t match											
	Wir App	dow	rs PowerS hell							<u>ک</u>		
Арр)S								Window	s PowerS	hell	
2	Wind	ows I	PowerShell ISE		;	>				Арр	ine ii	
2	Wind	ows I	PowerShell ISE	(x86)	;	>						
2	Winde	ows I	PowerShell (x8	6)	;	>	ď	Open				
Sett	tings						2	Run as Admi	nistrator			
Îŧ	Powe	She	I Developer Se	ettings	;	>	2	Run ISE as Ad	dministrator			
	Repla Wind	ce Co ows I	ommand Prom PowerShell in t	pt with he Win	+ x ;	>	<u></u>	Windows Pov	werShell ISE	(~)		
Sea	rch the	web								\smile		
Q	powe	scho	ool - See web res	sults	;	>						
م	powe	s he l	I		;	>						
Q	powe	scho	ool login		;	>						
Q	powe	s			;	>						
Q	powe	s										

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 Cer-
t:\LocalMachine\ -KeyUsage KeyEncipherment
        -KeyAlgorithm rsa -KeyLength 2048 -subject "BP Logix
```

```
Process Director"
    -DnsName "BP Logix Process Director" -Type SSLServer-
Authentication
    -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>\Priv-
atePublicKeys.pfx -Password $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 <u>Quickstart: Register an application with the Microsoft identity platform</u> for more information.
- F. Add the Redirect URI, which is the URI for your Process Director installation, e.g., https://myorg.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
- <u>Set up SMTP email access on the Properties page</u> 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 <u>SharePoint OAuth (Tenant)</u>, while a new Datasource <u>SharePoint OAuth (Site)</u>, 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 <u>SharePoint Legacy</u>.

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 <u>Configuring Azure for Process Director Integration</u> 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:

Azure Active Directory admir	n center				Q Q	© R	
≪ I Dashboard I All services ★ FAVORITES	Dashboard > Default Directory App reg Test SharePoint OAu Search (Ctrl+/) «	istrations > Test SharePoint OAut ith API permission: ○ Refresh <i>R</i> Got feedba	th S 🖈 ····				
 Azure Active Directory Users Enterprise applications 	 Overview Quickstart Integration assistant Manage 	Configured permissions Applications are authorized to call all the permissions the application + Add a permission ✓ Grar	APIs when they a needs. Learn mo	are granted permissions by users/admins as part of the cor re about permissions and consent : for Default Directory	isent process. The list of co	nfigured permissions should incl	.lude
	Branding & properties	API / Permissions name	Туре	Description	Admin consent requ.	. Status	
	Authentication	V Microsoft Graph (2)					
	Tokon configuration	Sites.FullControLAll	Application	Have full control of all site collections	Yes	Granted for Default Dire	
	API nermissions	User.Read.All	Application	Read all users' full profiles	Yes	Granted for Default Dire	
	Expose an API	SharePoint (9)	Annellenden			Granted for Default Dire	
	Ann roles	Sites Masses All	Application	Participation of all site collections	tes	Granted for Default Dire	
	A Owners	Sites Read All	Application	Read and write items and lists in all site collections	Yes	Granted for Default Dire	
	Roles and administrators	Sites Read/Write All	Application	Read news in all site collections	Yes	Granted for Default Dire	
	0 Manifest	Sites Selected	Application	Access selected site collections	Ver	Granted for Default Dire	
	Constant - Teachlachastics	TermStore Read All	Application	Read managed metadata	Ves	Granted for Default Dire	
	A Traviblashastics	TermStore.ReadWrite.All	Application	Read and write managed metadata	Yes	Granted for Default Dire	
	Nou support request	User.Read.All	Application	Read user profiles	Yes	Granted for Default Dire	
	a new support request	User.ReadWrite.All	Application	Read and write user profiles	Yes	Granted for Default Dire	

Create the SharePoint OAuth (Tenant) Datasource <u>#</u>

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

Azure Active Directory admin c	enter	t
«	Dashboard > Default Directory App regi	strations >
🖾 Dashboard	Test SharePoint OAu	th 🖈 …
E All services		
+ FAVORITES	✓ Search (Ctrl+/) «	📋 Delete Endpoints 💀 Preview features
🔶 Azure Active Directory	Overview	Got a second? We would love your feedback on Microsoft
L Users	🗳 Quickstart	-
Enterprise applications	🚀 Integration assistant	↑ Essentials
	Manage	Display name Test SharePoint OAuth
	🚍 Branding & properties	Application (client) ID
	Authentication	
	📍 Certificates & secrets	Object ID
	Token configuration	Directory (tenant) ID
	API permissions	Supported account types
	🙆 Expose an API	My organization only

paste it into the Client ID Property of the Datasource definition.

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.

Azure Active Directory admin	center	t
~	Dashboard > Default Directory App reg	istrations >
🖾 Dashboard	Test SharePoint OAu	ıth ጵ …
E All services	••••	
★ FAVORITES	✓ Search (Ctrl+/) «	📋 Delete 🌐 Endpoints 🐱 Preview features
🔶 Azure Active Directory	R Overview	Got a second? We would love your feedback on Microsoft
🚨 Users	🗳 Quickstart	•
Enterprise applications	🚀 Integration assistant	↑ Essentials
	Manage	Display name Test SharePoint OAuth
	🚍 Branding & properties	Application (client) ID
	Authentication	
	📍 Certificates & secrets	Object ID
	Token configuration	Directory (tenant) ID
	- API permissions	Supported account types
	🙆 Expose an API	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

SharePoint Datasource
PROPERTIES
Description
Entry heid developing of this Object
Enter a bier description of this Object
Sharenoint Site UDI
Client ID
Tenant ID
Sharepoint Certificate File (*.pfx)
Browse
Contificate Descured (options)
Columeate r assivora (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

- 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/_lay-

outs/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.
- Now you need to grant permissions to newly registered app (AKA principal). Navigate to

https://mytenant-admin.sharepoint.com/_lay-

outs/15/appinv.aspx.

It's important to note the addition of "-admin" to your site's normal name.

iii Office 365	Admin		
SharePoint admin o	enter		
site collections			
infopath		Create	Cancel
user profiles	App Id	App Id:	
bcs	The app's	f727176a-64c9-4697-a713-0b Lookup	
term store	its title.	Process Director	
records management		App Domain:	
search		Example: "www.contoso.com"	
secure store		https://www.localhost.com/	
apps	A'- De	Example: "https://www.contoso.com/default.aspx"	
sharing	Permission Permission	<pre><apppermissionrequests allowapponlypolicy="true"></apppermissionrequests></pre>	Pight="FullControl" />
settings	XML		Right= Function 72
configure hybrid	The permission		
device access	the app.		
		Create	Cancel

- a. Add your Client Id as App Id.
- 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, <u>Add-in permissions in</u> <u>SharePoint</u>. Be careful using other values as it may prevent Process Director from working correctly.

<AppPermissionRequests AllowAppOnlyPolicy="true"> <AppPermissionRequest Scope-

e="http://sharepoint/content/sitecollection" Rightt="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 the**Test 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.

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 <u>Configuring Azure for Process Director Integration</u> 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 <u>SMTP OAuth implementation</u>.

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: <u>How to set up a multifunction device or</u> <u>application to send emails using Microsoft 365 or Office 365</u>.

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*.

- 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.Ac-cessAsUser.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. **(i)** For more information on authentication permissions, please refer to the <u>Microsoft Graph Permissions Reference</u> 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 <u>Properties page</u> 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 <u>Global Variables page</u> 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*.

Office365 and CDA

For Process Director v6.1.300 and higher, CDA can optionally be used in conjunction with Microsoft Office365, rather than the OnlyOffice service. Like the use of Azure/Exchange for SMTP through Microsoft, there is additional configuration required to use O365 as the editor for documents.

First, you must set up the configuration in Azure to create the appropriate application endpoints, as described in the <u>Configuring Office365 for CDA</u> topic of the System Administrator Guide. The configuration of O365 CDA is different from the SMTP OAuth configuration, and will require additional settings.

Next, the Properties page of the Installation Settings section of the IT Admin area has <u>several properties that must be configured</u> to create the connection to both the O365 installation and the shared root folder in which document attachments will be stored. These properties also require supplying the OAuth settings for the Registered AAD Application in Azure.

Configuring Azure for Office365 and Collaborative Document Authoring (CDA)

• This topic discusses a product feature in active development, and is subject to change at any time.

For Process Director v6.1.300 and higher, Collaborative Document Authoring (CDA), can be implemented using the online version of Microsoft Office365 (O365). Setting up O365 CDA is a relatively complex process. This process will require setup within your Azure/Entra instance, and will, in most cases, also require some assistance from BP Logix. BP Logix recommends that read this guide thoroughly before executing the steps provided. Key information can be overlooked if you're not careful.

In order to provide optimal security, confining Process Director to a single SharePoint site, you'll need to create two different application registrations in Microsoft Entra. The first "Full Scope" registration is used only during initial configuration. The second "Site" registration is configured through the "Full Scope" registration and is the application registration that Process Director will utilize, once configured.

There are several steps to the process of configuration, each of which are linked to a documentation topic below, in the order in which they must be completed. In each topic, we'll specifically designate which steps you must perform as part of your Azure/Entra configuration, and which steps BP Logix must perform to complete the configuration in Process Director. Configuring O365 CDA requires that the steps, in order, that must be completed.

- 1. Configure SAML access for PD in Azure.
- 2. <u>Create and configure "Full Scope" App Registration for PD in Azure/Entra.</u>
- 3. <u>Create and configure "Site" App Registration for PD in Azure/Entra</u>.
- 4. Grant proper "Site" App Registration permission.
- 5. <u>Securely exchange "Site" App Registration and related settings with Process</u> <u>Director</u>.
- 6. <u>Configure Process Director to leverage the application registration</u>.
- 7. Configure SharePoint external sharing.

Configuring SAML Access for O365 CDA

There are several ways to register external applications for use in Azure; however, only Enterprise applications currently support SAML. Thus for this topic, we'll cover the creation of the Enterprise Application for configuring SAML with Process Director.

To begin creating the Enterprise application for SAML integration, first navigate to the Microsoft Entra ID page of your Azure portal.



From this page, use the navigation bar on the left side of the screen to navigate to the Enterprise Applications page.



From the toolbar at the top of the page, select the **New application** button.



Click the **Create your own application** button, then select the option labeled, Integrate any other application you don't find in the gallery.



Once the application has been created, you'll need to select the application type. To do so, click the Single sign-on button from the navigation bar on the left side of the page, then click the SAML button that will appear in the main portion of the screen.



On the SAML-based Sign-on page, you'll need to add the appropriate identifying URLS to configure the linkage between Process Director's SAML-related pages and Azure/Entra.

■ Microsoft Azure	P Search resources, services, and docs (G	იე დილისის და და მამორი არ
Home > 1 Enterprise application PD O365 SAML Enterprise Application	Sons > Enterprise applications All applications > PD 0365 SAML SAML-based Sign-on ···· Subject extends the ···· Channel (induced mode : ■ test the conduction ····	Basic SAML Configuration × Image: Save R Got feedback2
Coverview Coverview Deployment Plan Covers Diagnose and solve problems Diagnose and solve problem	Set up Single Sign-On with SAML An SSD implementation based on federation protocols improves security, reliability, and end user implement. Choose SAML single sign-on whenever possible for existing applications that do not us more. Read the configuration guide 10 for help integrating PD 0365 SAML PubProTrials. Basic SAML Configuration Identifier (Entity ID) Respl UIE, (Assertion Consumer Service URL) Respl UIE, (Assertion Consumer Service URL) Reply UIE, (Assertion Consumer Service URL) Reply UIE, (Assertion Consumer Service URL) Respl UIE, (Identifier (Entity ID) - ○ The unique D that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra Itenant: The default identifier will be the audience of the SAML response for IDP-initiated SOL Default https:// /login_saml.aspx /login_saml.aspx?skipintegrated=18:dkpsaml=8:usertype= ○ Add identifier ○ Reply URL (Assertion Consumer Service URL) - ○ The reply URL is where the application oppects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.
Application proxy Application proxy Self-service Costom security attributes Security Permissions Token encryption Activity	Attributes & Claims givenname usergivenname surname usersumame enalididress user.uman name user.userprincipalname Unique User identifier user.userprincipalname SAML Certificates	Index Default https:// /login_samil.sspx Image: Comparison of the sign of the sign on URL (Optional) Sign on URL (Optional) Sign on URL (Optional) sign on URL (optional) Sign on URL (optional) sign on URL (optional) Sign on URL (optional) type: application. This field is unnecessary if you want to perform identity provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign on.
 Sign•in logs M Usage & insights Audit logs Provisioning logs Roccess reviews Troubleshooting + Support ▲ New support request 	Token signing certificate Status Active Thumbprint 1C 1 Expiration 12/27/207, 2:2:34 PM 1 Notification Email	Relay State (Optional) The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL with the application. Enter a relay state Logout Url (Optional) This URL is used to send the SAML logout response back to the application. https:// Vlogout.aspx Vlogout.aspx
	Set up PD 0365 SAML 5 You'll need to configure the application to link with Microsoft Entra ID. Login URL Microsoft Entra Identifier Logout URL Intps://ts.windows.net/9 Intps://login.microsoftonline.com/9e93	

First, you'll need to add the Identifier (Identity ID) URLs that specify where the SAML logins will originate in Process Director. There are three of them that must be configured, using your actual Process Director server domain in place of the <pdserver.domain> placeholder text:

- 1. https://<pdserver.domain>/login_saml.aspx
- 2. https://<pdserver.domain>/login_saml.aspx?skipintegrated=1&skipsaml=&usertype=
- 3. https://<pdserver.domain>/login_saml.aspx?skipsaml=&usertype=

You'll then need to supply the Reply URL (Assertion Consumer Service URL) property to: https://<pdserver.domain>/login_saml.aspx.

Next, set the Signon URL (Optional) property to: https://<pdserver.domain>/login_saml.aspx. Finally, set the Logout Url (Optional) property to: https://<pdserver.domain>/logout.aspx.

The remainder of the Azure default property settings can remain unchanged. Click the Save button to save your newly configured application. Keep the page open, however, as we'll want to test the configuration later.

With the application configured in Azure, you'll now need to make the appropriate changes to your Process Director installation to enable SAML sign on for Process Director. **For Cloud customers, this process will most likely be done by BP Logix personnel.** On-Premise customers, however, will have to perform this configuration in their Process Director installation. Please see the appropriate Process Director documentation for configuring <u>SAML 2.0 (Federated Identity) Support</u> in the Installation Guide. This configuration will require setting several <u>SAML Custom Variables</u> in your Custom Variables file.

Once SAML is correctly configured in Process Director, you can return to the Azure Application window. At the bottom of the configuration page, click the **Test** button. This button will verify that all your changes work by opening a pop-up browser window to perform the connection testing. It will even look up errors you may receive from Microsoft's login server and provide you help with resolving them.

Once the testing is complete, and you've corrected any SAML configuration or connection errors that may appear, your Process Director server should be fully integrated with Azure for SAML authentication.

With the configuration completed, you'll then need to determine how existing users will be added to Process Director from your SAML system. There are two common methods for adding existing users:

- 1. Direct import into Process Director via a CSV/Excel file.
- 2. Enabling Process Director to auto-create user accounts when the user first logs in via SAML.

BP Logix personnel will work with you to determine the most appropriate method for your user provisioning, both initially and on an ongoing basis. There are, as always, pros and cons with both methods, so BP Logix will work with you to determine the user provisioning method that best meets your needs.

With SAML set up properly, you can move to the next step, which is to <u>create and</u> <u>configure the "Full Scope" App Registration</u> in Azure.

Configuring "Full Scope" App Registration

When fully configured, O365 CDA will access a single, specified SharePoint site. In order to create this configuration, you'll need to provide a mechanism to isolate that site. A "Full Scope" application registration in Azure provides this isolation mechanism, which we'll use to create the site-level application later.

The official Azure/Entra proprietary term for creating the entity we're about to configure is *Application (App) Registration*, and that's the term we'll use in this documentation. Your personnel who have IT/IS specialties may refer to this Azure/Entra entity by different names. Most commonly, the generic term *Service Principal* is likely familiar, since it's a generic term that can be used for other cloud providers like AWS and Google Cloud, and is the term commonly used in Internet Security.

To create the "Full Scope" App Registration, first navigate to the Microsoft Entra ID page of your Azure installation.



From this page, use the navigation bar on the left side of the screen to navigate to the App Registrations page. From this page, click the New registration button that appears at the top of the page.



On the Register an application page, Set the Name of the new application as "Full Scope" (or a suitable name of your choosing but note we refer to it as "Full Scope" in this document). Typically, the default setting of the Supported Account Types property is "Accounts in this organizational directory only" is satisfactory and provides optimal security.

\equiv Microsoft Azure	\mathcal{P}_{-} Search resources, services, and docs
Home > Default Directory App registrations >	
Register an application	
* Name	
The user-facing display name for this application (this can be changed later).	
Full Scope	✓
Supported account types	
Who can use this application or access this API?	
 Accounts in this organizational directory only (Default Directory only - Single tenant) 	
Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)	
Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and per Xbox)	sonal Microsoft accounts (e.g. Skype,
Personal Microsoft accounts only	
Help me choose	
Redirect URI (optional)	
We'll return the authentication response to this URI after successfully authenticating the user. Provi changed later, but a value is required for most authentication scenarios.	ding this now is optional and it can be
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 o	rganization by adding from Enterprise app
By proceeding, you agree to the Microsoft Platform Policies 🖪	
Register	

You can click the **Register** button at the bottom of the page to register the new application. Once registered, you'll see the **Overview** page for the new application. Note the Application (client) ID and Directory (tenant) ID properties. These values will be needed later when we grant access to the "Site" level App Registration. They are easily copied when hovering the mouse over each value.

=	Microsoft Azure			${\cal P}$ Search resources, services, and do	cs (G+/)	Copilot		₫	© (
н									
	🖕 foobar app reg 👒 🗠								
R	Search × «	📋 Delete Endpoint	s 💀 Preview features						
	Overview								
	Quickstart	Essentials							
-	Integration assistant	Display name	: <u>foobar app reg</u>		Client credentials	: <u>Add a certificat</u>	<u>e or secret</u>		
		Application (client) ID	: 7	ie i	Redirect URIs	: Add a Redirect	URI		
^	Diagnose and solve problems		:0	58	Application ID URI				
\sim	Manage		: 9	11	Managed applicati	on in I : <u>foobar app reg</u>			
	🧮 Branding & properties	Supported account type							
	Authentication								
	📍 Certificates & secrets	Welcome to the ne	w and improved App regi	trations. Looking to learn how it's changed i	rom App registrations (Legacy)? Learn more				
	Token configuration								
	API permissions	Starting June 30th, provide feature up	2020 we will no longer ad dates. Applications will ner	d any new features to Azure Active Directory ed to be upgraded to Microsoft Authenticati	Authentication Library (ADAL) and Azure Active Director on Library (MSAL) and Microsoft Graph. <u>Learn more</u>	y Graph. We will continue to	provide tech	nical su	pport and
	Expose an API	Cat Granted Design							

Next, you'll need to click the API Permissions menu item from the left sidebar of the page to open the API Permissions page. You'll need to edit some of the default permissions for this application.

If the user.read permission is shown, you'll need to delete it.

Next, you'll need to click the Add a permission button to open its dialog box. Select Microsoft Graph, then Application Permissions. Once in the Application Permissions section, you'll need to ad the Sites.FullControl.All permission to the application.



Once you've done so, click the Add Permissions button at the bottom of the page. Once you do, you'll need to click the Grant admin consent for <Enterprise name> button to confirm the change.

Now that the permissions have been changed, you'll need to create the Client Secret property for the new application. To do so, click the Certificates & secrets navigation menu item on the left sidebar of the page. When the page open, click the New Client Secret button to create a new client secret. You'll need to provide a Name for the new item. Once you do so, click the Add button.

• Once you click the *Add* button, you are presented with the secret *once and only once*. Do not navigate away or refresh the page.



Click the Copy to clipboard icon and then paste the secret into a secure document or file. Keep the file secret, and store it in a safe and secure place, preferably one that is backed up securely. Losing this value will make it impossible to use the "Full Scope" app to create the site isolation for the O365 CDA integration.

Keep the values for the Client Secret as well as the Client ID and Tenant ID properties for the "Full Scope" App Registration on hand. We'll need them to <u>create and</u> <u>configure the "site" level App Registration</u>, which is the next step in the process.

Configuring the "Site" Level App Registration

(i) As mentioned at the end of the previous configuration step, you're going to need to refer to the Client Secret, Client ID, and Tenant ID properties of the "Full Scope" App registration. The "Site" level App registration also has the same properties, with the same property names. To avoid confusion dusring the configuration, we'll explicitly refer to these

properties as "Full Scope" or "Site" when referring to the property names, e.g., Full Scope Client ID, Site Client ID, etc.

The purpose of the "Site" level App Registration is to enable the Process Director web application server to access your enterprise's Microsoft 365 (Office Online/O365/SharePoint Online) document storage for the purposes of using it for CDA. The "Site" level application is what CDA will access to enable the use of O365 for the collaborative editing of documents.

To create the "Site" level App Registration, To create the "Full Scope" App Registration, first navigate to the Microsoft Entra ID page of your Azure installation.



From this page, use the navigation bar on the left side of the screen to navigate to the App Registrations page. From this page, click the New registration button that appears at the top of the page.



Set the Name property of the new registration to "Site" (or a suitable name of your choosing but we'll refer to it as "Site" in this document), to distinguish it from the "Full Scope" registration you created previously. Typically, the default setting of the Supported Account Types property is "Accounts in this organizational directory only" is satisfactory and provides optimal security.

	\mathcal{P} Search resources, services, and doc
Home > Default Directory App registrations >	
Register an application	
* Name	
The user-facing display name for this application (this can be changed later).	
Site	~
Supported account types	
Who can use this application or access this API?	
Accounts in this organizational directory only (Default Directory only - Single tenant)	
Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)	
Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and per Xbox)	sonal Microsoft accounts (e.g. Skype,
Personal Microsoft accounts only	
Help me choose	
Redirect URI (optional)	
We'll return the authentication response to this URI after successfully authenticating the user. Provi changed later, but a value is required for most authentication scenarios.	ding this now is optional and it can be
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 o	rganization by adding from Enterprise ap
By proceeding, you agree to the Microsoft Platform Policies 🗗	
Register	

You can click the **Register** button at the bottom of the page to register the application. Once registered, you'll see the **Overview** page for it. Note the Application (client) ID and Directory (tenant) ID properties. These values are easily copied when hovering the mouse over each value.

As mentioned in the note at the top of the page, these are same property names that are used in the "Full Site" App Registration, so we'll refer to them as Site Client ID and Site Tenant ID for the remainder of this document. Similarly, we'll refer to the Full Scope Client ID and Full Scope Tenant ID for the same properties used by the "Full Scope" App Registration.

\equiv Microsoft Azure			$^{ m (c)}$ Search resources, services, and do	cs (G+/)	Copilot	Σ	P 🕸	6
ң foobar app reg 🔗								
	📋 Delete 🕀 Endpoint	s 🐱 Preview features						
😽 Overview	A Frankisla							
📣 Quickstart	Essentials							
💅 Integration assistant	Display name	: roobar app reg	0	Client credentials	: <u>Add a certr</u>	roct LIPI		
🗙 Diagnose and solve problems	Object ID	:0	58	Application ID UR	: Add an Ap	plication ID URI		
∨ Manage	Directory (tenant) ID	: 9	11	Managed applicat	ion in I : foobar app			
🧮 Branding & properties	Supported account type							
Ə Authentication								
📍 Certificates & secrets	Welcome to the ne	w and improved App regis	trations. Looking to learn how it's changed f	rom App registrations (Legacy)? Learn more				
Token configuration								
API permissions	Starting June 30th, provide feature up	2020 we will no longer add dates. Applications will nee	I any new features to Azure Active Directory d to be upgraded to Microsoft Authentication	Authentication Library (ADAL) and Azure Active Directo on Library (MSAL) and Microsoft Graph. <u>Learn more</u>	ry Graph. We will continu	ie to provide techr	ical suppor	t and
📤 Expose an API	Cat Bratad Dara							

Next, you'll need to click the API Permissions menu item from the left sidebar of the page to open the API Permissions page. You'll need to edit some of the default permissions for this application.

If the user.read permission is shown, you'll need to delete it.

Next, you'll need to click the Add a permission button to open its dialog box. Select Microsoft Graph, then Application Permissions. Once in the Application Permissions section, you'll need to add the Sites.Selected permission to the application.

			0	4 Copilot	E 🖉 🏾 0	greg.vogel@techsuppor
Home > Default Directory App registrat			Request API permissio	ns		
-3- Site API permission	s 🖈 …					
Search × «	🕐 Refresh 🖗 Got feedback?		All APIs Microsoft Graph https://graph.microsoft.com/ Docs			
💐 Overview	4 You are editing permission(s) to your application,	users will have to consent even if they've already	What type of permissions does your ap	plication require?		
📣 Quickstart			Delegated permissions		Application permissions	
🛒 Integration assistant			Your application needs to access the API as	the signed-in user.	Your application runs as a signed in user	background service or daemon without a
X Diagnose and solve problems	Granting tenant-wide consent may revoke permised	ssions that have already been granted tenant-wide				
∨ Manage			Select permissions			
Branding & properties	The "Admin consent required" column shows the default value for an organization. However, user c will be used losses are as a second		₽ Sites.Selected			
Authentication			Permission			Admin consent required
📍 Certificates & secrets	Configured permissions					
Token configuration	Applications are authorized to call APIs when they are	e granted permissions by users/admins as par	✓ Sites (1)			
API permissions	all the permissions the application needs. Learn more		Sites.Selected			Yes
📤 Expose an API	+ Add a permission 🗸 Grant admin consent f		Access selected site collections			
🧱 App roles	API / Permissions name Type	Description				
🎎 Owners	No permissions added					
🚴 Roles and administrators						
Manifest	To view and manage consented permissions for indi	vidual apps, as well as your tenant's consent se				
Support + Troubleshooting						
🙎 New support request			Add permissions Discard			

Once you've done so, click the Add Permissions button at the bottom of the page. Once you do, you'll need to click the Grant admin consent for <Enterprise name> button to confirm the change.

Now that the permissions have been changed, you'll need to create the Client Secret property for the new application. To do so, click the Certificates & secrets navigation menu item on the left sidebar of the page. When the page open, click the New Client Secret button to create a new client secret. You'll need to provide a Name for the new item.

Additionally you'll need to specify when this App Registration will expire, using the Expires property. This property consists of a dropdown control from which you can select how long the Site Client Secret will remain active.

• It's important to take note of the expiration time chosen. The expiration MUST be communicated to BP Logix. Also, you must provide a new Site Client Secret to BP Logix, on an ongoing basis, before the each one expires, to avoid interruptions in service.

Add a client secret		×
Description	PD secret	
Expires	Recommended: 180 days (6 months)	~
Add Cancel		

Once you've set the Name and Expires properties, click the Add button to create the new Site Client Secret.



Just as you did previously with the Full Scope Client Secret, click the Copy to clipboard icon and then paste the Site Client Secret into a secure document or file. Keep the file secret, and store it in a safe and secure place, preferably one that is backed up securely. • You must provide BP Logix with the values for the Site Client Secret, Site Client ID and Site Tenant ID properties. In addition, you'll need to provide BP Logix with the SharePoint site URL that will be used to access your enterprise's SharePoint environment. Keep in mind that these values are sensitive information, so you'll need to provide them to BP Logix via a secure method.

The initial configuration of the "Site" level App Registration is complete. Now you'll need to move to the next step, <u>granting the correct "Site" App Registration per-</u><u>missions</u>.

Granting "Site" App Registration Permissions

BP Logix will provide you with a set of Powershell scripts for applying the appropriate permissions to your "Site" level App Registration. These scripts have no additional external dependency; however, prior to running them, you should run the following PowerShell cmdlet:

Set-ExecutionPolicy -ExecutionPolicy Bypass

Once executed, it should ensure that the scripts provided by BP Logix won't be blocked from running.

Once you've done so, locate the folder into which you extracted the PowerShell scripts provided to you by BP Logix. Start PowerShell in that folder location.

First you must obtain a bearer token from the "Full Scope" App Registration you configured earlier. To obtain the bearer toke, run the PowerShell command below. For each parameter in the command, use the "Full Scope" value you obtained earlier (Full Scope Tenant ID, Full Scope Client ID, and Full Scope Client Secret).

```
.\get-access-token.ps1 -tenantId <Full Scope Tenant ID> -cli-
entId <Full Scope Client ID> -clientSecret <Full Scope Client
Secret>
```

You'll need to replace the text in angled brackets with the actual values from your "Full Scope" App Registration, e.g.:

```
.\get-access-token.ps1 -tenantId deadbeef-deed-feed-f00d-
0123456789ab -clientId 87654321-deed-feed-f00d-0123456789ab -
clientSecret dI8AQ~EKNqYwcXf0CJ_lFBJvR6xnDW0ZDM4Qbao7
```

Once you've run the script successfully, you'll have a file named "bearer.txt" in the current folder. The script will also output the bearer token to the console, though it will be truncated, due to its length.

Next you'll need to obtain the Site ID for the SharePoint site you wish to use with Process Director. Process Director uses a specific path within the site to avoid conflicts with other files, documents, and folders that may be in use.

Using a browser of your choice, login and access the SharePoint site you wish to use.

In that same browser, without logging out of SharePoint/Entra, navigate to:

```
https://<tenant- name>.sharepoint.com/sites/<site- name>/_ api/s-
ite/id
```

Once that page loads, it will display some XML values, as shown below.



In the example above, the redacted value that's outlined in blue (starts with "80" and ends with "f8") is the Site ID. Copy this value and save it.

Now that we have the correct bearer token, and SharePoint Site ID, you'll need to use them, along with the Site Client ID, the file location of the bearer.txt file that contains the bearer token, and the Site Name for the "Site" level App Registration, to run the following PowerShell command.

```
.\grant-site-selected.ps1 -siteID <SharePoint Site ID> -bear-
erTokenFile .\bearer.txt -clientID <Site Client ID> -appName
"Site"
```

Again, you'll need to replace the values in angled brackets above with the appropriate values from your systems. Upon successful completion of the script, you should see the appropriate output in the console, and there should be no red error text.



The console messages should indicate that the appropriate roles/permissions were granted to the specified "Site" App Registration.

With this complete, you can now <u>securely transmit the configuration information</u> <u>BP Logix needs</u> to configure your system (or, in the case of on-premise platform customers, configure your system).

Securely Transmit Configuration to BP Logix

(i) The secure online information exchange services mentioned in this topic are suggestions. BP Logix is happy to use other secure services you've vetted and wish to use. Avoid sending any this information in this topic to BP Logix via email or other insecure methods to prevent unnecessarily exposing this sensitive data.

Using a secure online information exchange mechanism (e.g. FireCloud, Kiteworks, ShareFile, onetimescret.com, Privnote - Send notes that will self-destruct after being read , etc.), send BP Logix the following information:

- Site Tenant ID
- Site Client ID
- Site Client Secret
- Site Client Secret Expiration Date (what month/day/year will the secret expire?)
- SharePoint site URL, e.g.: https://<tenant-name>.sharepoint.com/sites/<site-name>
- (Optional) SharePoint site folder path: If there's a specific location within the site where you'd like to store the Process Director data, provide that path here.

Once BP Logix receives this information, we can perform the next step in the process, Configuring your Process Director installation.

Configuring Process Director

Whether you're a Cloud customer of the Process Director platform, or a customer who has purchased a Use Case application, such as PubPro, Approvia, MIRador, etc., BP Logix will configure your Process Director and/or application installation with the values you've securely supplied to us.

If you're an On-Premise customer of Process Director, you'll need to provide the values for configuring O365 CDA on the Properties page of the IT Admin area's Installation Settings section. BP Logix has no access to the installation settings for

On-Premise customers. Please refer to the <u>documentation for the O365 CDA prop</u>-<u>erty settings</u> of **Properties** page.

You can now move to the final step of the configuration process, <u>Configuring</u> SharePoint External Access.

O365 CDA Installation Settings

For Process Director v6.1.300 and higher, the product supports the use of Office365 for CDA. All prior versions can use only the third-party document editing service provided by OnlyOffice. The implementation of O365 for CDA requires several properties be configured on the Installation Settings > Properties page.

SharePoint CDA Site URL

The URL of the SharePoint/O365 site that hosts the office installation.

SharePoint CDA Root Folder

The root folder in which the documents will be stored for access via CDA.

SharePoint CDA Tenant ID

- a. The ID of the Tenant in which the registered application resides in Azure/Entra. Creation of an application 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.

Like SMTP, This is an OAuth property to enable authentication with Microsoft.

SharePoint CDA Client ID

- a. The ID of the Application in SharePoint.
- b. This value is displayed as the Application (client) ID property on the Overview page of your application.

SharePoint CDA Client Secret

The client secret or application password the administrator created to use with the application.

SharePoint CDA Advanced options (optional)

A comma-separated list of options to pass to your O365 system.

Configuring SharePoint for External Access

Once you've configured Azure/Entra, and transmitted the appropriate information to BP Logix, you may need to make some changes to your SharePoint installation to enable its access for CDA, as a final step in this process. For some customers, this won't be necessary, since every user who accesses the documents for CDA will be valid, authenticated users of your Azure/Entra tenant. In many cases, however, you'll need to provide access to the documents for review or editing by users outside of your organization. In that case, you'll need to provide those external users with access to your SharePoint installation, to enable them to participate.

To do so, you'll first need to go to <u>admin.microsoft.com</u> to access your **Microsoft 365 Admin Center**. Once the admin center main page opens, you'll need to click the Show All menu item that appears in the sidebar on the left side of the page. Clicking this item will expand the sidebar to show additional menu items.



When the new menu items appear, you'll need to scroll down to the Admin Centers section, and select the SharePoint menu item.

Admin centers							
0	Security						
0	Compliance						
Þ	Microsoft Intune						
٥	Identity						
6 8	Exchange						
₿	SharePoint 🔗						

Clicking the SharePoint menu item will open a new browser tab to display the **SharePoint Admin Center**. On the left sidebar of the page, you'll need to click the **Sites** menu to expand it, then select the **Active Sites** menu item.



Clicking Active Sites will display the Active Sites page, listing all of your currently active SharePoint sites. Find the Web site in the list of sites, and click on it to select and expand it. When you do so, an informational pane for the selected site will appear on the right side of the page.

	SharePoint admin center					
≡ & □	Home Sites Active sites Deleted sites	^	Active sites Use this page to sort and filter sites and Learn more about managing sites + Create 🖉 Edit 🔗 Membership	change site settings. 호 욺 Hub ~ 월 Sharing 🥫	All Company Public group Email & View site i Delete General Activity Membership Settings	
٢	Containers	\sim	Site name \uparrow \checkmark	URL \sim		
<u></u>	Policies	\sim	#General	/sites/General	Email Privacy	
ې ۱	Settings	~	 All Company 	/sites/AllCompany.1738090.fto:	Let people outside the organization email this team Priv Send copies of team emails and events to team	ate

In the informational pane, a series of tabs will be displayed, just below the header information and logo. You'll need to click the Settings tab to display its contents.

AC All Company Public group Email S View site Delete General Activity Membership Settings							
Email Privacy Let people outside the organization email this team Private Send copies of team emails and events to team members' inboxes Public Don't show team email address in Outlook							
External file sharing (i) Sensitivity label (i)							
Anyone							
New and existing guests							
Existing guests Only people in your organization							

In the Settings tab, select either *Anyone* or *New and existing guests* from the External file sharing property options. You must choose one of these options to enable external sharing to users from outside of your organization. There are different security implications for each item. *New and existing guests* is a more secure option that verifies external users by sending a one-time password (OTP) to their email address. While more secure, some organizations may find this too

cumbersome for their use-case. The Anyone selection enables access to documents without the additional OTP verification. Irrespective of which option you choose, it will require specially crafted URLs to access individual documents. You'll need to refer to Microsoft's SharePoint documentation for more information about that.

Once you've set the desired External file sharing property option, you can click the Save button to save it. Once saved, the appropriate external users will be able to access the documents they need to access when participating in the edit-ing/collaboration process.

This step, combined with the changes made you to your Process Director installation, should fully enable O365 for use with the product's CDA feature.

This page intentionally left blank.