

Knowledgebase > Lasernet > Lasernet General Information > Configure Microsoft Azure to Support Lasernet Access to Azure Storage Through App-Registration-Based Authentication

Configure Microsoft Azure to Support Lasernet Access to Azure Storage Through App-Registration-Based Authentication

Sunil Panchal - 2025-01-14 - Comments (0) - Lasernet General Information

Lasernet 10.10 and later support access to Azure Storage through app-registration-based authentication. In these Lasernet versions, Lasernet Cloud printing configuration and Lasernet modules for Azure Storage input and output provide an **Application Registration** authentication option. This option is configured with **Client ID** and **Client Secret** to enable Lasernet to authenticate with Microsoft Entra ID as an application and access Azure Storage.

The implementation of this access consists of three elements which must each be appropriately configured:

- **Microsoft Entra ID:** An app registration that represents Lasernet must be granted appropriate API permissions.
- Azure Storage container: The enterprise app (corresponding to that app registration) must be assigned appropriate app roles on the Azure Storage container that you want Lasernet to connect to.
- Lasernet: The Azure Storage modules in a Lasernet configuration, or the configuration of Lasernet Cloud printing, or both, use a client ID and client secret to authenticate with Microsoft Entra ID.

The information below describes the configuration process.

Warning

This authentication method is not applicable to Azure Storage containers that are managed by Microsoft Dynamics 365 Finance and Operations.

Intended Audience

This information is intended for experienced Microsoft Azure administrators, who will understand how to complete tasks such as configuring role assignments on a storage container. So, this article contains only the supporting information that an administrator needs, such as which roles to assign.

The final stage of the process is to configure Lasernet. This task is completed by a Lasernet administrator and is described in the <u>Lasernet Azure Guide</u> and <u>Lasernet Printer Service</u> <u>Guide</u>. Consequently, this page describes only the information that the Microsoft Azure administrator must pass to the Lasernet administrator to enable them to configure Lasernet.

Configuration Process

To appropriately configure Microsoft Azure, follow this process.

1. Create an app registration to represent Lasernet.

2. Grant the app registration an appropriate set of API permissions.

3. <u>Generate a client secret for the app registration</u>.

4. <u>Assign the enterprise application (that corresponds to the app registration) a set of appropriate roles on the storage account.</u>

5. <u>Supply the necessary information to the Lasernet administrator so that they can</u> configure Lasernet.

Each task in this process is described in more detail below.

Create an App Registration

In Microsoft Entra ID, create an app registration to represent Lasernet.

Note

Microsoft Entra ID might already contain app registrations for Lasernet that serve other purposes. Consider whether to create a new additional app registration or modify an existing one.

This article assumes that you created a new app registration for Lasernet, for the purpose of enabling it to access Azure Storage.

Grant the App Registration Appropriate API Permissions On the app registration's **API permissions** page, grant it the following permissions:

- Azure Storage
 - o user_impersonation
- Microsoft Graph
 - FileStorageContainer.Selected
 - User.Read

	🕐 Refresh 🖗 Got feedback?						
 Overview Quickstart 	Some actions may be disabled due	to your permis	sions. To request access, contact the application	n owner(s) or your administrator. View application	owners or admin	istrators.	
🚀 Integration assistant 🔀 Diagnose and solve problems	▲ Granting tenant-wide consent may i	revoke permissic	ons that have already been granted tenant-wide for	that application. Permissions that users have already	granted on their ov	vn behalf aren't aff	
Manage Branding & properties Authentication	The "Admin consent required" colur app will be used. <u>Learn more</u>	nn shows the de	sfault value for an organization. However, user cons	ent can be customized per permission, user, or app. T	his column may no	t reflect the value i	
Certificates & secrets	Configured permissions						
 Token configuration API 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						
Expose an API App roles	 + Add a permission	iin consent for Type	Formpipe (Test) Description	Admin consent required	Status		
🚨 Owners	✓ Azure Storage (1)						
🛃 Roles and administrators	user_impersonation	Delegated	Access Azure Storage	No	🔮 Granted f	•••	
0 Manifest	V Microsoft Graph (2)						
✓ Support + Troubleshooting	FileStorageContainer.Selected	Application	Access selected file storage containers	Yes	🤡 Granted f	•••	
New support request	User.Read	Delegated	Sign in and read user profile	No	🥑 Granted f	•••	
	To view and manage consented permissi	ons for individ	ual apps, as well as your tenant's consent settir	gs, try Enterprise applications.			

Generate a Client Secret for the App Registration

- 1. On the **Certificates and secrets** page, generate a client secret for the app.
- 2. Note the new client secret (before the Azure Portal obscures it).

	🖗 Got feedback?					
🐺 Overview	Some actions may be disabled due to your permissions. To request access, contact the application owner(s) or your administrator. View application owners or administrators.					
😃 Quickstart						
🚀 Integration assistant						
🗙 Diagnose and solve problems	Credentials enable contidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.					
∨ Manage						
🗮 Branding & properties	Application registration certificates secrets and federated credentials can be found in the tabs below.					
Authentication	• Abbitration Legistration recultation reactions and accounting rate of the matrix and account in the 1005 DELOT.					
📍 Certificates & secrets	Certificates (0) Client secrets (1) Federated creder	tials (0)				
Token configuration						
API permissions	A secrer string that the application uses to prove its identity when requesting a token. Also Can be referred to as application password.					
🙆 Expose an API	+ New client secret					
App roles	Description	Expires Value 🛈	Secret ID			
A Owners		11/15/2026 rVk**************	3577a886-8fcd-4f 🗈 📋			
and administrators &						
🔟 Manifest						
\checkmark Support + Troubleshooting						
New support request						

Assign the Lasernet Enterprise Application the Necessary Roles on the Storage Account 1. In the Azure Portal, navigate to the storage account that Lasernet will connect to.

2. On the **Access Control (IAM)** page, use the **Role assignment**s tab to grant the enterprise app (that corresponds to the new app registration) the necessary roles on the storage account. Grant the enterprise app the following roles:

- Storage Blob Data Contributor
- Storage Blob Data Reader
- Storage Queue Data Contributor
- Storage Queue Data Reader

ula.makowska@ipwonutesconmicro							
✓ Storage Blob Data Contributor (3)							
	Арр	Storage Blob Data Contributor ①	This resource	None			
✓ Storage Blob Data Reader (2)							
	Арр	Storage Blob Data Reader ①	This resource	None			
✓ Storage Queue Data Contributor (5)							
	Арр	Storage Queue Data Contributor ①	This resource	None			
✓ Storage Queue Data Reader (2)							
	App	Storage Queue Data Reader 🕕	This resource	None			
V Tag Contributor (10)							

Supply Configuration Information to the Lasernet Administrator

After you have completed this process, supply information from the following Microsoft Azure areas to the Lasernet administrator so that they can configure Lasernet:

- App registration
 - Application (client) ID
 - Client secret Value
- Tenant
 - Tenant domain
- Storage account
 - Storage account Name
 - Container Name

To use this information to configure Lasernet, the Lasernet administrator can follow the instructions provided in the following guides:

- Lasernet Azure Guide
- Lasernet Printer Service Guide