

Setting up Microsoft Teams in ScriptRunner

Using the ROPC workflow

Author: Michael Gall Date: 2022-08-11 Version 1.0



Table of Contents

1	1 Introduction						
2	2 Overview of the ROPC workflow						
3	Inst	Installing PowerShell modules					
4	4 Configuring the certificate		. 7				
	4.1	Creating the certificate	7				
	4.2	Exporting the certificate	8				
5	Con	figuring the service principal	10				
	5.1	Creating the service principal	10				
	5.2	Uploading the certificate	13				
6	Test	ting the connection in ScriptRunner	14				
7 Customiz		tomizing API permissions and ownership	16				
	7.1	Adjusting API permissions	16				
	7.2	Creating member users in Azure	17				
	7.3	Adding member user as owner	17				
8	Con	npleting the ScriptRunner configuration	18				
	8.1	Creating a credential	18				
	8.2	Configuring the Microsoft Teams target	18				
9	Che	cklist	20				
1	0 Pos	sible error sources	21				
	10.1	Conditional Access	21				
	10.2	Problems with the login	22				
1	1 Not	es and references	23				
	11.1	Notes	23				
11.2		References	23				



Table of Figures

Figure 1: System drawing of the ROPC workflow	5
Figure 2: Overview of the installed PowerShell modules	6
Figure 3: Output of the PowerShell console after certificate creation	7
Figure 4: Local computer certificates in LocalComputer\My	8
Figure 5: Certificate export wizard - public key only	8
Figure 6: Certificate export wizard - X.509 (.CER) format	9
Figure 7: Azure Portal login page	10
Figure 8: App registration in the Azure Portal	
Figure 9: Overview of enterprise applications in Azure AD	
Figure 10: Registering a new service principal	11
Figure 11: Overview of the new service principal	12
Figure 12: Subpage in MS_TEAMS_ROPC	
Figure 13: Security settings - certificate overview	13
Figure 14: Certificate upload in the Azure Portal	
Figure 15: New Microsoft Graph target	
Figure 16: Input form of the Microsoft Graph target	
Figure 17: Connection test output	15
Figure 18: Default permissions for Microsoft Graph	
Figure 19: API permission with admin consent	17
Figure 20: Adding the member user as an owner	
Figure 21: Microsoft Teams target in ScriptRunner	
Figure 22: Connection test output	
Figure 23: Potential restrictions through conditional access policies	21
Figure 24: Sign-in logs in the Azure Portal	21
Figure 25: Error message in ScriptRunner portal - invalid tenant ID	



1 Introduction

This document describes how to set up Microsoft Teams using ROPC workflows.

For the connection to work, the following requirements must be met:

- The ScriptRunner server is running in a <u>current version</u>*¹
- Microsoft Teams PowerShell module > = version 4.5.0 is installed
- Microsoft Graph PowerShell module >= version 1.10.0 is installed

The two modules required for Microsoft Teams and Microsoft Graph are installed in chapter 3

An account with global administrator privileges is required to set up and configure the service principal in Microsoft Azure.

The account used for the service principal is only required to be a member of the Azure tenant and must not be granted any other rights.

This document describes the individual steps:

- Preparation: Install PowerShell modules
- Create certificate for Microsoft Teams use case
- Set up service principal
- Upload certificate
- Test connection in ScriptRunner using Microsoft Graph
- Customize API permissions and ownerships
- Test connection with Microsoft Teams
- Possible errors and further resources

Note

The procedure described here was successfully implemented as part of a proof of concept on August 3rd, 2022, and reflects the current status. The document will be updated periodically to account for future changes.

Please read and work through the document **completely**. If steps are omitted, this may result in the connection setup not working.

For feedback and questions, please contact support@scriptrunner.com.

¹, tested on 2022-08-11 - current version PortalEdition R4, Build 1603



2 Overview of the ROPC workflow

This chapter contains a system drawing of the ROPC workflow.²



Figure 1: System drawing of the ROPC workflow

You will need the following data for setup:

- Azure username and password (default membership).
- Tenant ID or primary domain
- Application ID of the service principal
- Certificate thumbprint

To log in via the ROPC workflow, you need a username and password in addition to the certificate, tenant ID, and application ID.

For the setup in Azure AD, an Azure AD Premium P1 or P2 license is required. Users should have at least a Microsoft 365 E3 license associated. Microsoft Teams must be set up, otherwise API permissions cannot be granted.

² , verified 2022-08-11 - drawing taken from: https://docs.microsoft.com/de-de/azure/active-directory/develop/v2-oauth-ropc



3 Installing PowerShell modules

Before starting the setup, verify that the relevant modules for Microsoft Teams and Microsoft Graph are already installed. To do so, run the following PowerShell command:

Get-Module -ListAvailable

You will get an overview of the installed modules as an output. This list should include both Microsoft Graph and Microsoft Teams.

Script	1.10.0	Microsoft.Graph.Authentication	{Connect-MgGraph, Disconnect-MgGraph, Get-MgContext, Get-M
Script	1.10.0	Microsoft.Graph.Bookings	{Get-MgBookingBusiness, Get-MgBookingBusinessAppointment,
Script	1.10.0	Microsoft.Graph.Calendar	{Get-MgGroupCalendar, Get-MgGroupCalendarMultiValueExtende
Script	1.10.0	Microsoft.Graph.CloudCommunications	{Add-MgCommunicationCallLargeGalleryView, Clear-MgCommunic
Script	1.10.0	Microsoft.Graph.Compliance	{Add-MgComplianceEdiscoveryCaseCustodianHold, Add-MgCompli
Script	1.10.0	Microsoft.Graph.CrossDeviceExper	{Get-MgUserActivity, Get-MgUserActivityHistoryItem, Get-Mg
Script	1.10.0	Microsoft.Graph.DeviceManagement	{Get-MgDeviceManagement, Get-MgDeviceManagementAdvancedThr
Script	1.10.0	Microsoft.Graph.DeviceManagement	{Add-MgDeviceManagementGroupPolicyUploadedDefinitionFileLa
Script	1.10.0	Microsoft.Graph.DeviceManagement	{Get-MgDeviceManagementApplePushNotificationCertificate, G
Script	1.10.0	Microsoft.Graph.DeviceManagement	{Get-MgDeviceManagementAndroidDeviceOwnerEnrollmentProfile
Script	1.10.0	Microsoft.Graph.Devices.CloudPrint	{Get-MgPrint, Get-MgPrintConnector, Get-MgPrintOperation,
Script	1.10.0	Microsoft.Graph.Devices.Corporat	{Clear-MgDeviceAppMgtWindowInformationProtectionDeviceRegi
Script	1.10.0	Microsoft.Graph.Education	{Get-MgEducationClass, Get-MgEducationClassAssignment, Get
Script	1.10.0	Microsoft.Graph.Files	{Add-MgDriveListContentTypeCopy, Add-MgDriveListContentTyp
Script	1.10.0	Microsoft.Graph.Financials	{Get-MgFinancial, Get-MgFinancialCompany, Get-MgFinancialC
Script	1.10.0	Microsoft.Graph.Groups	{Add-MgGroupDriveListContentTypeCopy, Add-MgGroupDriveList
Script	1.10.0	Microsoft.Graph.Identity.Directo	{Complete-MgDirectoryImpactedResource, Complete-MgDirector
Script	1.10.0	Microsoft.Graph.Identity.Governance	{Add-MgAccessReviewDecision, Add-MgAccessReviewInstanceDec
Script	1.10.0	Microsoft.Graph.People	{Get-MgUserActivityStatistics, Get-MgUserLastSharedMethodI
Script	1.10.0	Microsoft.Graph.PersonalContacts	{Get-MgUserContact, Get-MgUserContactExtension, Get-MgUser
Script	1.10.0	Microsoft.Graph.Planner	{Get-MgGroupPlanner, Get-MgGroupPlannerPlan, Get-MgGroupPl
Script	1.10.0	Microsoft.Graph.SchemaExtensions	{Get-MgSchemaExtension, New-MgSchemaExtension, Remove-MgSc
Script	1.10.0	Microsoft.Graph.Search	{Get-MgExternal, Get-MgExternalConnection, Get-MgExternalC
Script	1.10.0	Microsoft.Graph.Sites	{Add-MgSiteContentTypeCopy, Add-MgSiteContentTypeCopyFromC
Script	1.10.0	Microsoft.Graph.Teams	{Add-MgChatMember, Add-MgTeamChannelMember, Add-MgTeamMemb
Script	1.10.0	Microsoft.Graph.Users.Functions	{Export-MgUserDeviceAndAppManagementData, Find-MgUserRoom,
Script	1.0.1	Microsoft.PowerShell.Operation.V	{Get-OperationValidation, Invoke-OperationValidation}
Script	1.0.0.0	Microsoft.SME.CredSspPolicy	
Script	4.5.0	MicrosoftTeams	{Add-TeamChannelUser, Add-TeamUser, Connect-MicrosoftTeams

Figure 2: Overview of the installed PowerShell modules

Should any of the mentioned PowerShell modules be missing, install them with the following commands:

```
Install-Module -Name MicrosoftTeams -Scope AllUsers
Install-Module -Name Microsoft.Graph -Scope AllUsers
```



4 Configuring the certificate

This chapter describes how to create and export the certificate.

4.1 Creating the certificate

Create a self-signed certificate using the following PowerShell command:

```
New-SelfSignedCertificate -DnsName <FQDN> -FriendlyName
MS TEAMS ROPC -KeyExportPolicy Exportable -KeySpec Signature
```

After the certificate has been created, the console displays the certificate thumbprint. Make a copy of the certificate thumbprint for later use.



Figure 3: Output of the PowerShell console after certificate creation

Note

Be sure to create the certificate with the **-KeySpec Signature** parameter, otherwise the certificate cannot be used to establish the connection.

By default, the certificate is created in the **Cert:\LocalMachine\My** store.



4.2 Exporting the certificate

Export the certificate you just created using the Certificate Manager in the Microsoft Management Console (MMC).

Exporting the public key is sufficient since the private key cannot be imported into Azure.

Right-click the certificate and click **All Tasks** > **Export**...

	^							
certificates (Local Computer)		Issued By	Expiration Date	Intended Purposes	Friendly Name St	itus Certificate Te	Actions	
Personal	17a7-4f2b-90fd-7e11	connectorregistrationca.msapppr	7/18/2022	Client Authentication	<none></none>		Certificates	
Certificates	erver Temporary Pla	PasswordServer Temporary Place	1/1/2040	<all></all>	<none></none>		More Actions	
Trusted Root Certification Authorities	er-SPN	ScriptRunner-SPN	7/20/2022	Client Authenticati	<none></none>		vmsr01.scriptrunner.tan	
Enterprise Trust	MPIRELOCAL	SRAPP01.EMPIRE.LOCAL	8/5/2022	Server Authenticati	theempire		More Actions	
Intermediate Certification Authorities	iptrunner.tan	vmsr01.scriptrunner.tan	7/13/2022	Client Authenticati	<none></none>			
Trusted Publishers	iptrunner.tan	vmsr01.scriptrunner.tan	7/14/2023	Client Authenticati	<none></none>			
Untrusted Certificates	iptrunner.tan	vmsr01.scriptrunner.tan	8/2/2023	Client Authenticati	Used_for_MSTEAMS			
Third-Party Root Certification Authorities	ipu uniner.tan	sn)1.scriptrupper.tan	8/2/2023	Client Authenticati	MSTEAMS V2			
Client Authentication Issuers	Open	ISR02-CA	2/14/2024	Server Authenticati	<none></none>	ADFS		
Preview Build Roots	All Tasks	> Open		<all></all>	<none></none>			
Local NonRemovable Certificates MSE-historyJournal Remote Desktop Certificate Enrollment Requests Smart Card Trusted Roots	Cut	Request Certificate with New Key		Server Authenticati	Windows Admin C			
		Renew Certificate with New	ew Key					
	Delete							
		Manage Private Keys Advanced Operations						
Trusted Devices	Properties							
Web Hosting	Help	Export						
Windows Ene ID Fotoen issuer WindowsServerUpdateServices Certificates - Current User								

Figure 4: Local computer certificates in LocalComputer\My.

In the wizard, enable the No, do not export the private key option.

. .

Export Privat	e Key					
You can	choose to expo	rt the private	key with the	certificate.		
Private certifica	eys are passwo te, you must typ	ord protected.	If you want on a later p	to export thage.	e private key	with the
Do you	want to export	the private ke	y with the ce	rtificate?		
0	(es, export the	private key				
۲	No, do not expo	rt the private	key			

Figure 5: Certificate export wizard - public key only

Setting up MS Teams in ScriptRunner

Using the ROPC Workflow



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)
O Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification path if possible
O 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
O Microsoft Serialized Certificate Store (.SST)

Figure 6: Certificate export wizard - X.509 (.CER) format



5 Configuring the service principal

This chapter describes the setup and configuration of the service principal.

5.1 Creating the service principal

Setup the service principal in Azure Active Directory. Log in to **portal.azure.com** and click **Azure Active Directory**.



Figure 7: Azure Portal login page

In the left navigation bar on the overview page, click **App registrations**.

App registrations

Figure 8: App registration in the Azure Portal

This page gives you an overview of all applications, owned applications and deleted applications.

Click + New registration to create a new service principal.

Setting up MS Teams in ScriptRunner



Using the ROPC Workflow

+ New registration	🕀 Endpoints 🧷	Froubleshooting 💍 Refre	esh 🛓 Download	Mark Preview features	Sot feedback?	
Starting June 3	0th, 2020 we will no longer	add any new features to Azur	e Active Directory Aut	hentication Library (ADAL)	and Azure AD Graph. We w	ill continue to provide
All applications	Owned applications	Deleted applications				
O Start turing a d	icelau nome er eneliestie	n (client) ID to filter these r	t- Add 6	ltors		
> start typing a d	isplay name or application	in (client) ID to filter these r.		ners		
1 applications found	ł					

Figure 9: Overview of enterprise applications in Azure AD

Assign a name. For the other settings, the default can remain selected.

Home > devhead App registrations >
Register an application
* News
* Name
The user-facing display name for this application (this can be changed later).
MS_TEAMS_ROPC
Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (devhead only - Single tenant)
O Accounts in any organizational directory (Any Azure AD directory - Multitenant)
O Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
O Personal Microsoft accounts only
Help me choose
Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
Select a platform
Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies යි.

Figure 10: Registering a new service principal

Switch back to the overview and display the application ID and the tenant ID. You will need both to set up the connection.



Ţ	🗍 Delete 🌐 Endpoints	Preview features
	∧ Essentials	
	Display name	: MS TEAMS ROPC
	Application (client) ID	: 67c04b6a-886a-4b9e-
	Object ID	: 1124eac4-6a04-4e15-b3f7-
	Directory (tenant) ID	: 557f8ff5-
	Supported account types	: <u>My organization only</u>

Figure 11: Overview of the new service principal



5.2 Uploading the certificate

To upload your certificate in the Azure Portal, click **Certificates & Secrets** in the left navigation bar.

P Search (Ctrl+/)	🖉 🖉 Got feedback?
 Overview Quickstart Integration assistant 	Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.
Manage	Application registration certificates, secrets and federated credentials can be found in the tabs below. X
 Branding & properties Authentication Certificates & secrets 	Certificates (0) Client secrets (0) Federated credentials (0) A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.
Token configuration API permissions Evnose an API	+ New client secret Description Expires Value ⊙ Secret ID
App roles	No client secrets have been created for this application.

Figure 12: Subpage in MS_TEAMS_ROPC

In the Certificates section, click Upload certificate.

Certificates (0)	Client secrets (0)	Federated credentials (0)						
Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.								
↑ Upload certif	icate							
Thumbprint		Description	Start date	Expires	Certificate ID			

No certificates have been added for this application.

Figure 13: Security settings - certificate overview

An area for uploading the certificate opens on the right side.

Upload certificate	Х
Upload a certificate (public key) with one of the following file types: .cer, .pem, .crt *	В
Description	
MS_TEAMSv2	

Figure 14: Certificate upload in the Azure Portal

Once the certificate has been uploaded, the setup of the service principal for configuration with Microsoft Graph is complete.

When you have made all configurations, perform a connection test in ScriptRunner via Microsoft Graph. Test whether it is possible to establish a connection (see chapter 6).



6 Testing the connection in ScriptRunner

Next, set up the target system in ScriptRunner. Open the ScriptRunner Portal and go to **Configuration** > **Targets**. Click **Create** > **Microsoft 365** and assign a display name to the target. In the **Microsoft services** section, add the **Microsoft Graph** service.



Figure 15: New Microsoft Graph target

Enter the **Tenant ID**, the **Application ID**, and the **Certificate thumbprint** in the service settings. The **Credential** field must be left blank!

General	Microsoft services Credential field empty	1
Microsoft services		
Advanced settings	Activate service	
FORMATION Used by	Microsoft Graph Sign-in method Certificate Client secret	,
	devhead.onmicrosoft.com	,
	67c04b6a-886a-4b9e-a4f5-680f18545318	
	Certificate thumbprint 21551EF47378F53UC4C2CC83710018D45D681A60	
	PowerShell module	

Figure 16: Input form of the Microsoft Graph target



Save your settings. Click **Run test** to perform a connection test.

MS G	raph Devhead		×
Win	dows PowerShell	PowerShell 7	
PowerS	hell modules		
			~
Run t	test 🗸		
75 76 77 80 81 82 83 84 85 86 87 88 89 90 91 92	Scopes AuthType AuthProviderType CertificateName Account AppName ContextScope Certificate PSHostVersion ClientTimeout	: UserProvidedAccessToken :UserProvidedToken : :MS_TEAMS_ROPC :Process : : 6.7.1603.0 :00:05:00	

Figure 17: Connection test output

Once the connection has been successfully established, API permissions and ownership can be set up.



7 Customizing API permissions and ownership

This chapter describes the final steps required to perform a login in the ROPC workflow.

7.1 Adjusting API permissions

Open the settings of the registered service principal in the Azure Portal. In the left navigation bar, click **API Permissions**.

By default, only the User.Read permission is provided here:

Configured permissions		
Applications are authorized to call APIs when all the permissions the application needs. Lea	hey are granted permissions by users/admins as part of the con- n more about permissions and consent	onsent process. The list of configured permissions should include
$+$ Add a permission \checkmark Grant admin co	sent for devhead	
API / Permissions name Type	Description	Admin consent requ Status
✓Microsoft Graph (1)		
	d Circle and and an Ch	N

To view and manage permissions and user consent, try Enterprise applications.

Figure 18: Default permissions for Microsoft Graph

Click +Add a permission to add the following permissions as Delegated type:

- Microsoft Graph
 - App.Catalog.ReadWrite.All
 - Group.ReadWrite.All
 - o User.Read
 - User.Read.All
- Skype and Teams Tenant Admin AP
 - o user_impersonation

Once all permissions are set correctly, click Grant admin consent for <name>.

Setting up MS Teams in ScriptRunner

Using the ROPC Workflow



Home > devhead App registrations >							
	Pl permissions 🔌						
Search (Ctrl+/) «	🕐 Refresh 🕴 🔗 Got feedbac	đ					
Soverview							
🖴 Quickstart 💉 Integration assistant	The "Admin consent required"	column shows t	he default value for an organization. However,	user consent can be	customized per permission,	user, or app. This column may r	ot reflect the value in your organization
Manage	Configured permissions						
 Branding & properties Authentication Certificates & secrets 	Applications are authorized to call A all the permissions the application of + Add a permission ✓ Grant	Pls when they reeds. Learn m	are granted permissions by users/admins a ore about permissions and consent t for devhead	s part of the conse	nt process. The list of con	igured permissions should in	clude
III Token configuration	API / Permissions name	Туре	Description		Admin consent requ	Status	
 API permissions 	Microsoft Graph (4)						
Expose an API	AppCatalog.ReadWrite.All	Delegated	Read and write to all app catalogs	H	Yes	Granted for devhead	•••
H App roles	Group.ReadWrite.All	Delegated	Read and write all groups	0	Yes	Granted for devhead	•••
A Owners	User.Read	Delegated	Sign in and read user profile		No	Granted for devhead	
& Roles and administrators	User.Read.All	Delegated	Read all users' full profiles		Yes	Granted for devhead	
Manifest	✓ Skype and Teams Tenant Admin A	P					
Support + Troubleshooting	user_impersonation	Delegated	Access Microsoft Teams and Skype for B	usiness data as th	Yes	Granted for devhead	
Troubleshooting New support request	To view and manage permissions ar	ıd user consen	t, try Enterprise applications.	ļ			•

Figure 19: API permission with admin consent

7.2 Creating member users in Azure

You still need a separate owner. Do not use the global administrator account, but instead a member account.

It is entirely sufficient to set up a standard user without any additional rights.

7.3 Adding member user as owner

This user must be added as an owner. In the left navigation bar, click **Owners**.

Home > devhead App registrations >					
<u>*</u>	Owners 🖈 …				
🔎 Search (Cmd+/)	+ Add owners II Remove	owners 🛛 🛱 Got feedback?			
 Overview Quickstart 	In addition to users with permiss	ion to manage any applications, the us	ers listed here can view and edit this ap	plication registration.	
🚀 Integration assistant	Name	Email	User name	Job Title	Туре
Manage	MG Michael G	mg@devhead.onmicrosoft.com	mg@devhead.onmicrosoft.com		Member
🚟 Branding & properties	MichaelGall		mgmini@devhead.onmicrosoft.com		Member
Authentication					
Certificates & secrets					
Token configuration					
API permissions					
🛆 Expose an API					
1 App roles					
24 Owners					
& Roles and administrators					
Manifest					
Support + Troubleshooting					
<i>D</i> Troubleshooting					
New support request					

Figure 20: Adding the member user as an owner



8 Completing the ScriptRunner configuration

Store the credential of the user account in ScriptRunner and complete the configuration.

8.1 Creating a credential

Open the ScriptRunner Portal. In the **Credentials** section, enter the credential of the Azure account (member account).

8.2 Configuring the Microsoft Teams target

Create a Microsoft Teams target in the same way as explained in chapter 6 and copy the data from the Microsoft Graph target.

In the **Credential** field, select the credential you just created.

CONFIGURATION	Microsoft services	
Microsoft services	Credential	
Advanced settings	Activate service	
NFORMATION Used by	Sign-in method Certificate Client secret	^
	Tenant ID 557f8ff5-	2
	Application ID c25baf86-9cea	8
	Certificate thumbprint 21551EF47378	2
	PowerShell module	
	• Must be lest slind as the even time best	

Figure 21: Microsoft Teams target in ScriptRunner



Save your settings. Click Run test to perform a connection test.

MS Graph Devhead PowerShell version	×
Windows PowerShell PowerShell 7	
PowerShell modules	
	~
Run test 🗸	
Console	
<pre>3838 3839 3840 3841 3841 3842 3843 3844 3845 3846 SRX: END Console Output 3847 SRX: ************************************</pre>	The second
3855	B MURbary,

Figure 22: Connection test output



9 Checklist

Checking requirements

- The ScriptRunner server is running in a <u>current version</u>* (at least Portal Edition R4 Build 1603)
- Microsoft Teams PowerShell module >= version 4.5.0 is installed
- Microsoft Graph PowerShell module >= version 1.10.0 is installed

Embedding/creating a certificate

- If available: Embed in Microsoft Azure
- If not yet available: Create a self-signed certificate with -KeySpec Signature
- Export the public key only

Creating a service principal in Azure

- Create a service principal in Azure
- Save application ID, tenant ID and certificate thumbprint
- Upload certificate

Creating a Microsoft Graph target system

- Create a Microsoft Graph target system in ScriptRunner using the data from the service principal
- **Credential** field must remain empty
- Run connection test

Customizing API permissions

• See chapter 7.1

Creating restricted Azure account (tenant member)

• See chapter Fehler! Verweisquelle konnte nicht gefunden werden.

Adding service principal as owner

• See chapter Fehler! Verweisquelle konnte nicht gefunden werden.

Finishing ScriptRunner configuration

- Create a member account under **Credentials**
- Transfer data from the MS Graph target to the MS Teams target
- In the **Credential** field, select the Azure account
- Perform connection test



10 Possible error sources

This chapter describes possible error sources and their solutions.

10.1 Conditional Access

Make sure that there are no rules in **Conditional Access** that restrict access.

Home > Conditional Access	
E Conditional Access	Policies
×	+ New policy + New policy from template (Preview) 🛛 What If 🕐 Refresh 🕴 🞘 Got feedback?
 Overview (Preview) 	
f≡ Policies	
Insights and reporting	Policy Name 1
🔀 Diagnose and solve problems	[SharePoint admin center]Block access from apps on unmanaged devices - 2022/06/30
Manage	[SharePoint admin center]Use app-enforced Restrictions for browser access - 2022/06/30
Named locations	[SharePoint admin center]Block access from apps on unmanaged devices - 2022/07/06
Custom controls (Preview)	[SharePoint admin center]Use app-enforced Restrictions for browser access - 2022/07/06
Trans of use	

Figure 23: Potential restrictions through conditional access policies

You can check whether such a rule actually blocks access using **Monitoring** > **Sign-in logs**. Use the wizard to recreate the error in question.

Monitoring



Figure 24: Sign-in logs in the Azure Portal



10.2 Problems with the login

Use the connection test in the target configuration to troubleshoot certificate problems. In all cases, the error messages indicate the problem. Common error sources are:

- The relevant PowerShell modules are missing
- The certificate thumbprint is not correct
- The tenant ID or application ID is incorrect

The error message is displayed in the upper area.

MS G	raph Devhead
PowerS	shell version
Win	dows PowerShell PowerShell 7
PowerS	shell modules
	\sim
Dun	tost
KUN	
E III V (*	rror hvoke-RestMethod: VebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeRestMethodCommand - "error":"inval id_request","error_description":"AADSTS900023: Specified tenant identifier '557f8ff5-1010-40d6- ie99-36fbbe046e7c1' is ne ither a valid DNS name, nor a valid external domain.\r\nTrace ID: 9fc8f976-8fbd-4a78- 1873-1227500cad00\r\nCorrelation ID : 6769f69b-967b-46a8-81e2-d8099ab39e85\r\nTimestamp: 2022-08-04 4:41:05Z","error_codes":[900023],"timestamp":"2022-08-0 4 14:41:05Z","trace_id":"9fc8f976-8fbd-4a78-a873- 227500cad00","correlation_id":"6769f69b-967b-46a8-81e2-d8099ab39e85"," error_uri":"https://login.microsoftonline.com/error?code=900023"} (InvalidOperation: System.Net.HttpWebRequest:HttpWebR equest) [Invoke-RestMethod], WebException)
Cons	ole
3815 3816 3817	SRX:disconnected in: 00:00:05.6562058
3818 3819	Invoke-RestMethod : {"error":"invalid_request","error_description":"AADSTS900023: S '557f8ff5-1010-40d6-8e99-36fbbe046e7c1' is neither a valid DNS name, nor a valid ex

h.,

Figure 25: Error message in ScriptRunner portal - invalid tenant ID



11 Notes and references

11.1 Notes

The following Microsoft Azure users were used in this tutorial:

- <u>mg@devhead.onmicrosoft.com</u> -> Tenant / global administrator
- <u>mgmini@devhead.onmicrosoft.com</u> -> Simple user account in the tenant

Tenant information, tenant ID, application ID, and certificate thumbprints have been blurred.

11.2 References

Microsoft Teams - ROPC Login:

https://docs.microsoft.com/de-de/azure/active-directory/develop/v2-oauth-ropc

Github Office_Docs:

https://github.com/MicrosoftDocs/office-docs-powershell/blob/main/teams/teamsps/teams/Connect-MicrosoftTeams.md