

Einrichtung des ROPC Workflows für Microsoft Teams in ScriptRunner

Schritt-für-Schritt-Anleitung

Autor: Michael Gall

Datum: 09.08.2022

Stand: Version 1.0

Inhaltsverzeichnis

1	Einleitung	4
2	Übersicht des ROPC-Workflows	5
3	PowerShell-Module installieren	6
4	Zertifikat konfigurieren	7
4.1	Zertifikat erstellen.....	7
4.2	Zertifikat exportieren.....	8
5	Service-Prinzipal konfigurieren	10
5.1	Service-Prinzipal erstellen.....	10
5.2	Zertifikat hochladen.....	13
6	Verbindung in ScriptRunner testen	14
7	API-Berechtigungen und Ownership anpassen	16
7.1	API-Berechtigungen anpassen.....	16
7.2	Mitgliedbenutzer in Azure erstellen	17
7.3	Mitgliedbenutzer als Owner hinzufügen	17
8	Abschließende Einrichtung im ScriptRunner	18
8.1	Credential anlegen	18
8.2	Microsoft Teams-Zielsystem konfigurieren.....	18
9	Checkliste	20
10	Mögliche Fehlerquellen	21
10.1	Conditional Access	21
10.2	Probleme bei der Anmeldung.....	22
11	Anmerkungen und Quellenangaben	23
11.1	Anmerkungen.....	23
11.2	Quellenangaben	23

Abbildungsverzeichnis

Abbildung 1: Systemzeichnung des ROPC-Workflows.....	5
Abbildung 2: Übersicht der installierten PowerShell-Module	6
Abbildung 3: Ausgabe der PowerShell-Konsole nach der Zertifikatserstellung.....	7
Abbildung 4: Lokale Computerzertifikate in LocalComputer\My.....	8
Abbildung 5: Export-Wizard des Zertifikats – nur öffentlicher Schlüssel	8
Abbildung 6: Export-Wizard des Zertifikats – Format X.509 (.CER)	9
Abbildung 7: Anmeldeseite im Azure Portal	10
Abbildung 8: Anmeldeseite im Azure Portal	10
Abbildung 9: Übersicht der Enterprise-Applikationen in Azure AD	11
Abbildung 10: Registrieren eines neuen Service-Prinzipals	11
Abbildung 11: Übersichtsseite des neuen Service-Prinzipals	12
Abbildung 12: Unterseite im MS_TEAMS_ROPC	13
Abbildung 13: Sicherheitseinstellungen - Zertifikatsübersicht.....	13
Abbildung 14: Zertifikats-Upload im Azure Portal.....	13
Abbildung 15: Neues Microsoft Graph-Zielsystem.....	14
Abbildung 16: Eingabemaske des Microsoft Graph-Zielsystems	14
Abbildung 17: Ausgabe des Verbindungstests	15
Abbildung 18: Standardberechtigungen für Microsoft Graph	16
Abbildung 19: Eingerichtete API-Berechtigung mit Admin Consent.....	17
Abbildung 20: Hinzufügen des Mitgliedbenutzers als Owner.....	17
Abbildung 21: Microsoft Teams-Zielsystem in ScriptRunner.....	18
Abbildung 22: Ausgabe des Verbindungstests	19
Abbildung 23: Mögliche Einschränkungen durch Conditional Access Policies	21
Abbildung 24: Sign-in Logs im Azure Portal	21
Abbildung 25: Fehlermeldung im ScriptRunner Portal – ungültige Tenant ID	22

1 Einleitung

In diesem Dokument wird die Einrichtung von Microsoft Teams mittels ROPC-Workflows beschrieben. Damit der Verbindungsaufbau funktioniert, müssen folgende Voraussetzungen erfüllt sein:

- Der ScriptRunner-Server wird in einer [aktuellen Version](#)^{*1} betrieben
- Microsoft Teams-PowerShell-Modul >= Version 4.5.0 ist installiert
- Microsoft Graph-PowerShell-Modul >= Version 1.10.0 ist installiert

Die beiden Module für Microsoft Teams und Microsoft Graph werden im Kapitel 3 installiert.

Für die Einrichtung und die Konfiguration des Service-Prinzipals in Microsoft Azure wird ein Konto mit globalen Administratorrechten benötigt. Das Konto, das für den Service-Prinzipal verwendet wird, muss lediglich Mitglied im Azure Tenant sein und sollte keine weiteren Rechte erhalten. Dieses Dokument beschreibt die einzelnen Teilschritte:

- Vorbereitung: PowerShell-Module installieren
- Zertifikat für den Microsoft Teams Use Case erstellen
- Service-Prinzipal einrichten
- Zertifikat hochladen
- Verbindung in ScriptRunner mittels Microsoft Graph testen
- API-Berechtigungen und Ownerships anpassen
- Verbindung mit Microsoft Teams testen
- Mögliche Fehlerquellen und weitere Quellen

Hinweis

Das hier beschriebene Vorgehen wurde im Rahmen eines Proof of Concepts am 3. August 2022 erfolgreich umgesetzt und entspricht dem aktuellen Stand.

Zukünftige Änderungen können abweichend sein, das Dokument wird in regelmäßigen Abständen aktualisiert werden.

Bitte lesen und arbeiten Sie das Dokument **vollständig durch**. Ausgelassene Schritte können dafür sorgen, dass der Verbindungsaufbau nicht funktioniert.

Bei Anmerkungen und Fragen wenden Sie sich bitte an support@scriptrunner.com.

¹, geprüft am 9.8.2022 – Aktuelle Version PortalEdition R4, Build 1603

2 Übersicht des ROPC-Workflows

Dieses Kapitel enthält eine Systemzeichnung des ROPC-Workflows.²

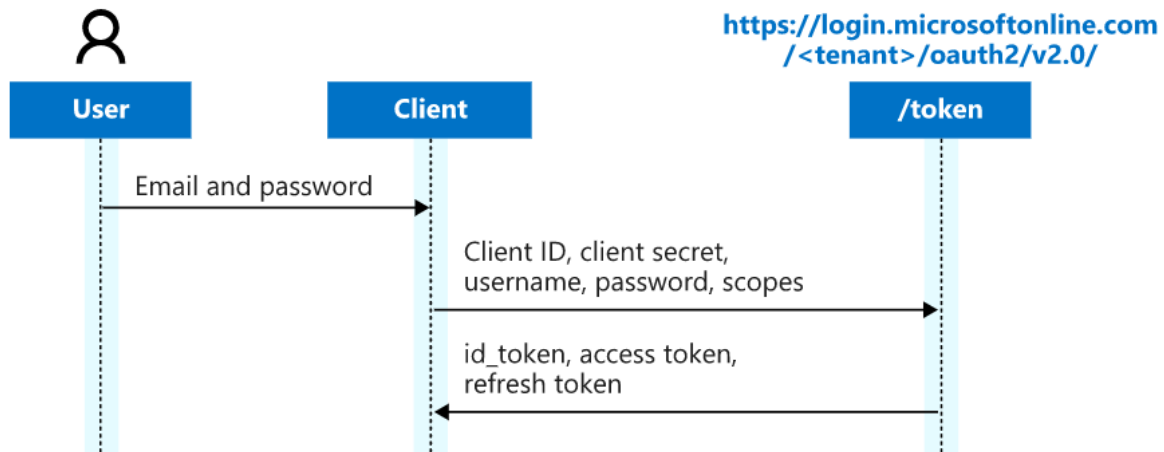


Abbildung 1: Systemzeichnung des ROPC-Workflows

Zur Einrichtung benötigen Sie die folgenden Daten:

- Name und Kennwort eines Azure-Benutzers (Standardmitgliedschaft)
- Tenant ID bzw. primäre Domain
- Application ID des Service-Prinzipals
- Zertifikats-Thumbprint

Bei der Anmeldung über den ROPC-Workflow benötigen Sie neben dem Zertifikat, der Tenant ID und der Application ID einen Benutzernamen und ein zugehöriges -kennwort.

Für die Einrichtung ist in Azure AD eine Azure AD Premium P1- oder P2-Lizenz erforderlich. Den Benutzern sollte mindestens eine Microsoft 365 E3-Lizenz zugeordnet sein. Microsoft Teams muss eingerichtet sein, ansonsten können keine API-Berechtigungen vergeben werden.

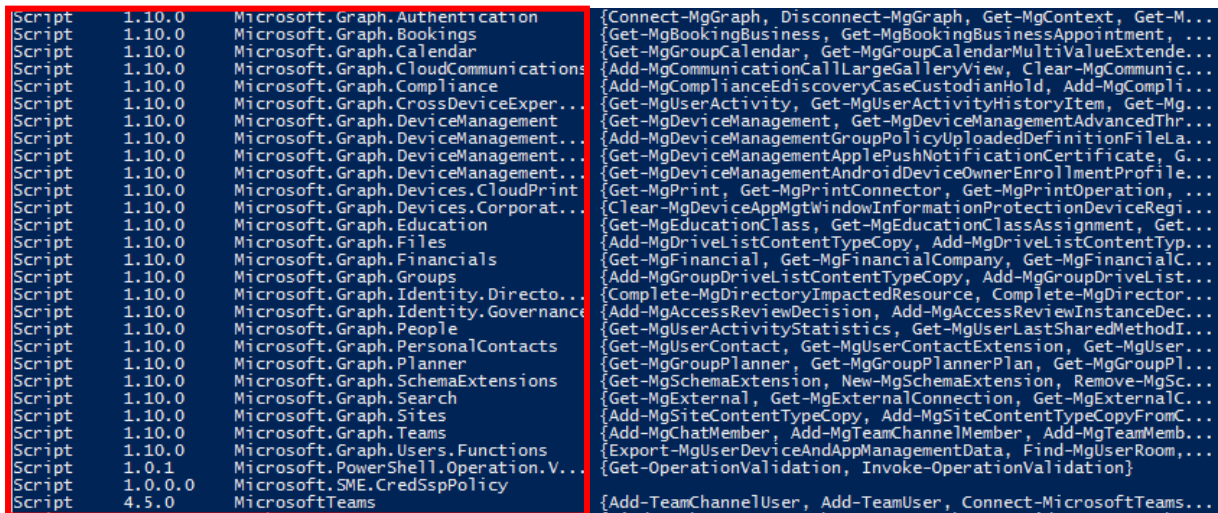
² ,geprüft 3.8.2022 – Zeichnung übernommen von: <https://docs.microsoft.com/de-de/azure/active-directory/develop/v2-oauth-ropc>

3 PowerShell-Module installieren

Bevor Sie mit der Einrichtung starten können, prüfen Sie bitte, ob die betreffenden Module für Microsoft Teams und Microsoft Graph bereits installiert sind. Führen Sie dazu den folgenden PowerShell-Befehl aus:

```
Get-Module -ListAvailable
```

Als Ausgabe erhalten Sie eine Übersicht der installierten Module. In dieser Liste sollte sowohl Microsoft Graph als auch Microsoft Teams aufgelistet sein.



```
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-MgComplianceDiscoveryCaseCustodianHold, 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... {Clear-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-MgDriveListContentTypeTyp...
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 {Add-TeamChannelUser, Add-TeamUser, Connect-MicrosoftTeams...
Script 4.5.0 MicrosoftTeams {Find-Booking, Get-Booking, Get-BookingBusiness, Get-Booki...
```

Abbildung 2: Übersicht der installierten PowerShell-Module

Fehlen die genannten PowerShell-Module, können Sie sie mit den folgenden Befehlen installieren:

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

4 Zertifikat konfigurieren

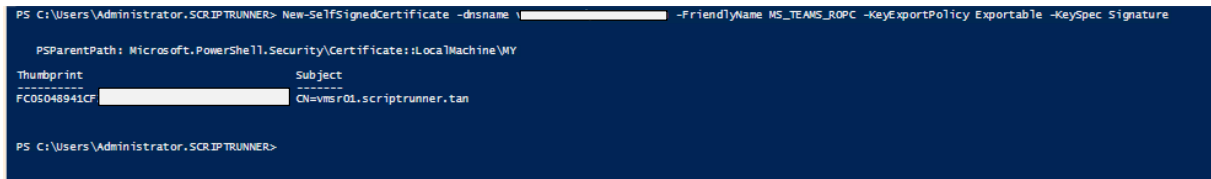
In diesem Kapitel wird die Erstellung des Zertifikats und dessen Export beschrieben.

4.1 Zertifikat erstellen

Soll für die Absicherung des Zertifikats ein selbstsigniertes Zertifikat verwendet werden, können Sie dieses mithilfe des folgenden PowerShell-Befehls erstellen:

```
New-SelfSignedCertificate -DnsName <FQDN> -FriendlyName  
MS_TEAMS_ROPC -KeyExportPolicy Exportable -KeySpec Signature
```

Nachdem das Zertifikat erstellt wurde, wird in der Konsole der jeweilige Zertifikats-Thumbprint angezeigt. Kopieren Sie sich den Zertifikats-Thumbprint, sodass Sie ihn bei der späteren Einrichtung zur Hand haben.



```
PS C:\Users\Administrator.SCRIPTRUNNER> New-SelfSignedCertificate -dnsname [redacted] -FriendlyName MS_TEAMS_ROPC -KeyExportPolicy Exportable -KeySpec Signature  
  
PSParentPath: Microsoft.PowerShell.Security\Certificate:\LocalMachine\My  
Thumbprint   Subject  
-----  
FC05048941CF [redacted] CN=[redacted].scriptrunner.tan  
  
PS C:\Users\Administrator.SCRIPTRUNNER>
```

Abbildung 3: Ausgabe der PowerShell-Konsole nach der Zertifikatserstellung

Hinweis

Achten Sie darauf, das Zertifikat mit dem Parameter **-KeySpec Signature** zu erstellen, da das Zertifikat andernfalls für den Verbindungsaufbau nicht eingesetzt werden kann.

Standardmäßig wird das Zertifikat im Store **Cert:\LocalMachine\My** angelegt.

4.2 Zertifikat exportieren

Über den Zertifikatsmanager in Microsoft Management (MMC) können Sie das gerade erstellte Zertifikat exportieren. Hier reicht es aus, den öffentlichen Schlüssel zu exportieren. Der private Schlüssel kann in Azure nicht importiert werden. Führen Sie dazu einen Rechtsklick auf das Zertifikat aus und klicken Sie auf **All Tasks > Export...**

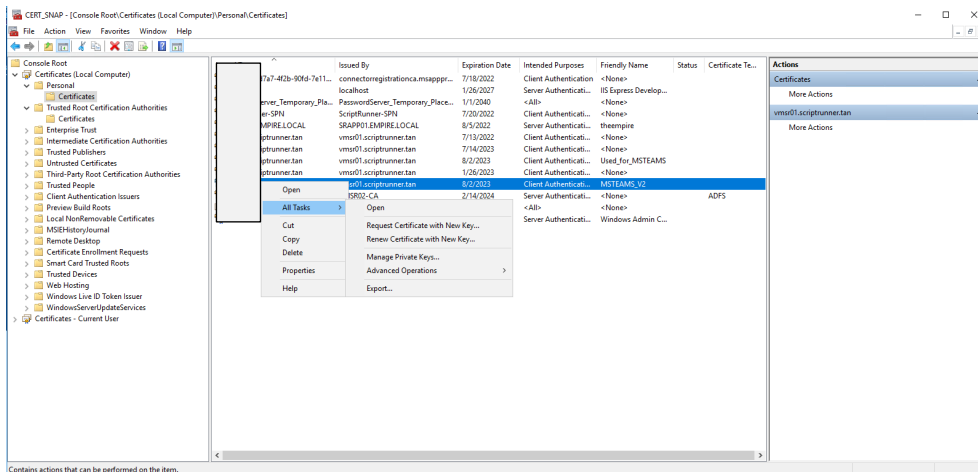


Abbildung 4: Lokale Computerzertifikate in LocalComputer\My.

Ein Wizard öffnet sich. Aktivieren Sie die Option **No, do not export the private key**.

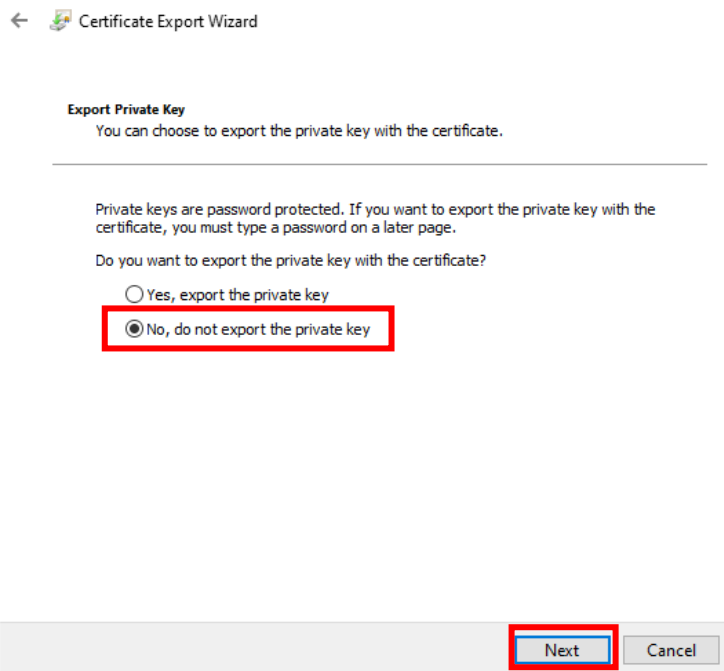



Abbildung 5: Export-Wizard des Zertifikats – nur öffentlicher Schlüssel

Exportieren Sie das Zertifikat im Format X.509 (.CER).

←  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)

Abbildung 6: Export-Wizard des Zertifikats – Format X.509 (.CER)

5 Service-Prinzipal konfigurieren

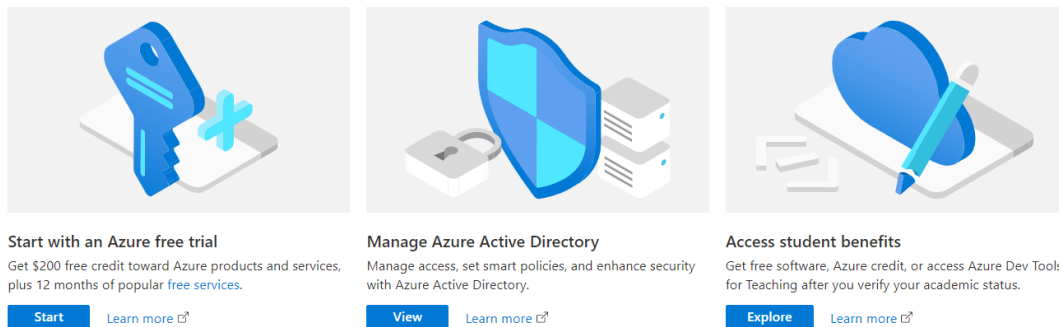
Dieses Kapitel beschreibt die Einrichtung und Konfiguration des Service-Prinzipals.

5.1 Service-Prinzipal erstellen

Die Einrichtung des Service-Prinzipals findet in Azure Active Directory statt. Melden Sie sich dazu unter **portal.azure.com** an und klicken Sie auf **Azure Active Directory**.

Welcome to Azure!

Don't have a subscription? Check out the following options.



The screenshot shows three promotional cards on the Azure Welcome page:

- Start with an Azure free trial:** Get \$200 free credit toward Azure products and services, plus 12 months of popular free services. Includes a 'Start' button and a 'Learn more' link.
- Manage Azure Active Directory:** Manage access, set smart policies, and enhance security with Azure Active Directory. Includes a 'View' button and a 'Learn more' link.
- Access student benefits:** Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status. Includes an 'Explore' button and a 'Learn more' link.

Azure services

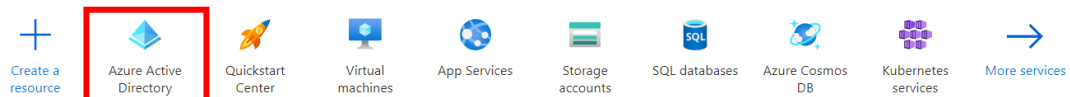


Abbildung 7: Anmeldeseite im Azure Portal

Klicken Sie auf der folgenden Übersichtsseite in der linken Navigationsleiste auf **App registrations**.

App registrations

Abbildung 8: Anmeldeseite im Azure Portal

Auf dieser Seite erhalten Sie eine Übersicht über alle Applikationen, eigene Applikationen und über gelöschte Applikationen.

Klicken Sie auf den Button + **New registration**, um einen neuen Service-Prinzipal anzulegen.

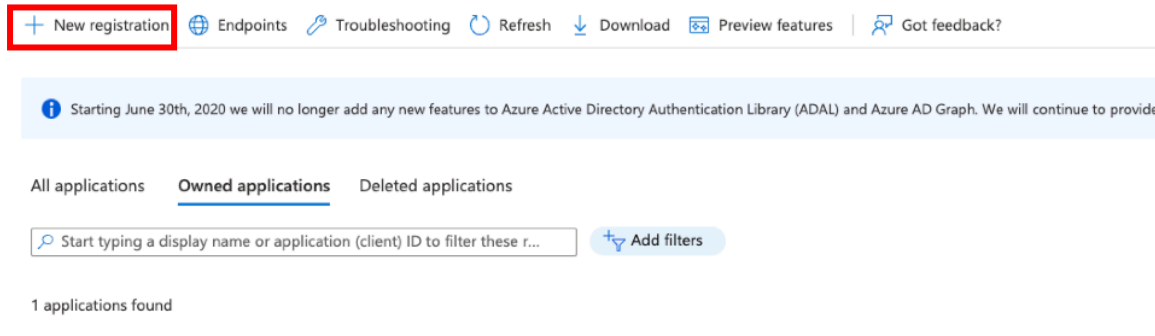


Abbildung 9: Übersicht der Enterprise-Applikationen in Azure AD

Definieren Sie einen Namen. Die übrigen Einstellungen können im Standard belassen werden.

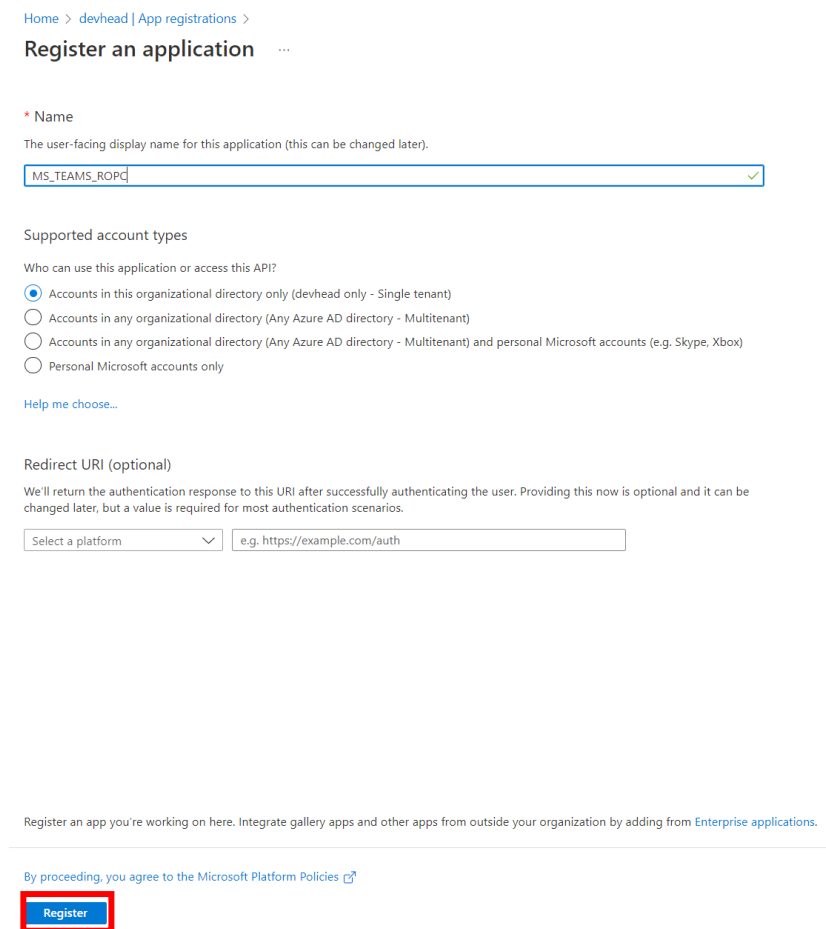




Abbildung 10: Registrieren eines neuen Service-Prinzips

Wechseln Sie nach der Erstellung in die Übersicht und lassen Sie sich die Application ID und die Tenant ID anzeigen. Diese benötigen Sie für die Einrichtung der Verbindung.

 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 : [My organization only](#)

Abbildung 11: Übersichtsseite des neuen Service-Prinzipals

5.2 Zertifikat hochladen

Nachdem der Service-Prinzipal erstellt wurde, laden Sie nun im Azure Portal Ihr erstelltes Zertifikat hoch. Klicken Sie dazu in der linken Navigationsleiste auf **Certificates & Secrets**.

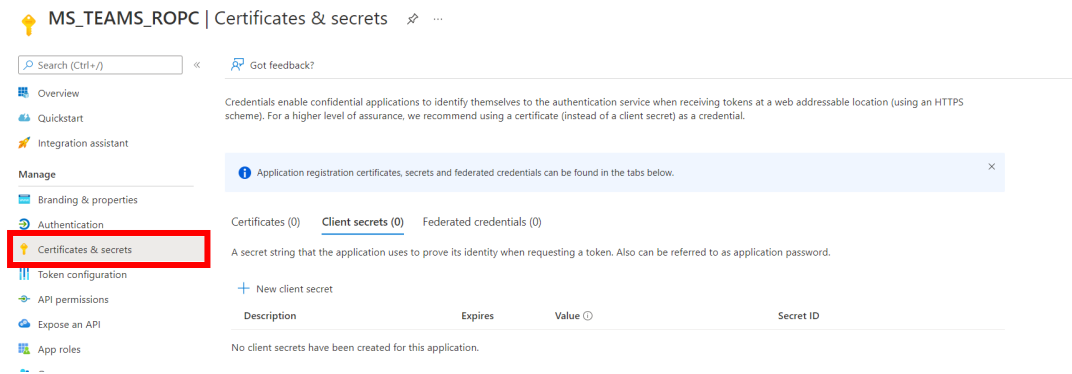


Abbildung 12: Unterseite im MS_TEAMS_ROPC

Klicken Sie im Bereich **Certificates** auf den Button **Upload Certificate**, um Ihr Zertifikat hochzuladen.

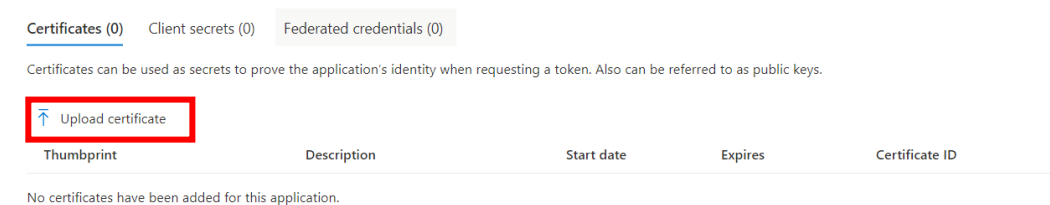


Abbildung 13: Sicherheitseinstellungen - Zertifikatsübersicht

Auf der rechten Seite öffnet sich ein Bereich zum Hochladen der Datei.

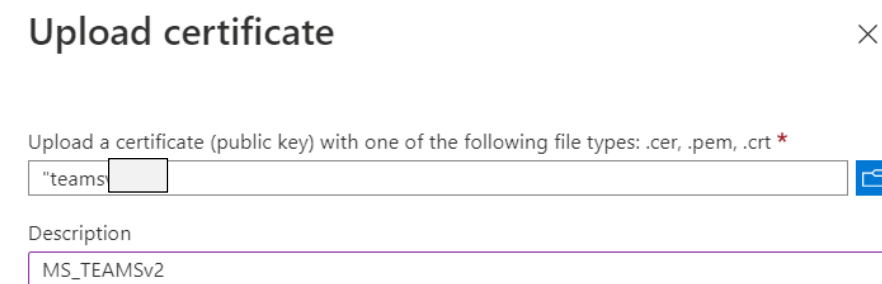


Abbildung 14: Zertifikats-Upload im Azure Portal

Wurde das Zertifikat hochgeladen, ist die Einrichtung des Service-Prinzipals für die Konfiguration mit Microsoft Graph abgeschlossen.

Wenn Sie alle Konfigurationen vorgenommen haben, können Sie in ScriptRunner via Microsoft Graph einen Verbindungstest durchführen. Prüfen Sie, ob ein Verbindungsaufbau möglich ist (siehe Kapitel 6).

6 Verbindung in ScriptRunner testen

Richten Sie in ScriptRunner nun das Zielsystem ein. Öffnen Sie das ScriptRunner Portal und wechseln Sie in den Bereich **Targets**. Klicken Sie auf **Create > Microsoft 365**. Vergeben Sie einen Namen für das Zielsystem. Wechseln Sie in den Bereich **Microsoft services** und fügen Sie den Service **Microsoft Graph** hinzu.

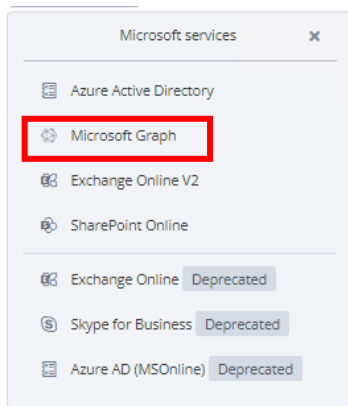


Abbildung 15: Neues Microsoft Graph-Zielsystem

Geben Sie in den Einstellungen des Service die Tenant ID, die Application ID und den Zertifikats-Thumbprint ein. Das Feld **Credential** muss freigelassen werden!

MS Graph Devhead

Save Run test Delete

CONFIGURATION

- General
- Microsoft services**
- Advanced settings

INFORMATION

- Used by

Microsoft services

Credential **Credential bitte freilassen!**

Activate service

Microsoft Graph

Sign-in method

Certificate Client secret

Tenant ID
[redacted]onmicrosoft.com

Application ID
67c04b6a-[redacted]

Certificate thumbprint
21551EF4-[redacted]

PowerShell module

Must be installed on the execution host

Deactivate service

Abbildung 16: Eingabemaske des Microsoft Graph-Zielsystems

Speichern Sie Ihre Einstellungen. Klicken Sie auf **Run test**, um einen Verbindungstest durchzuführen.

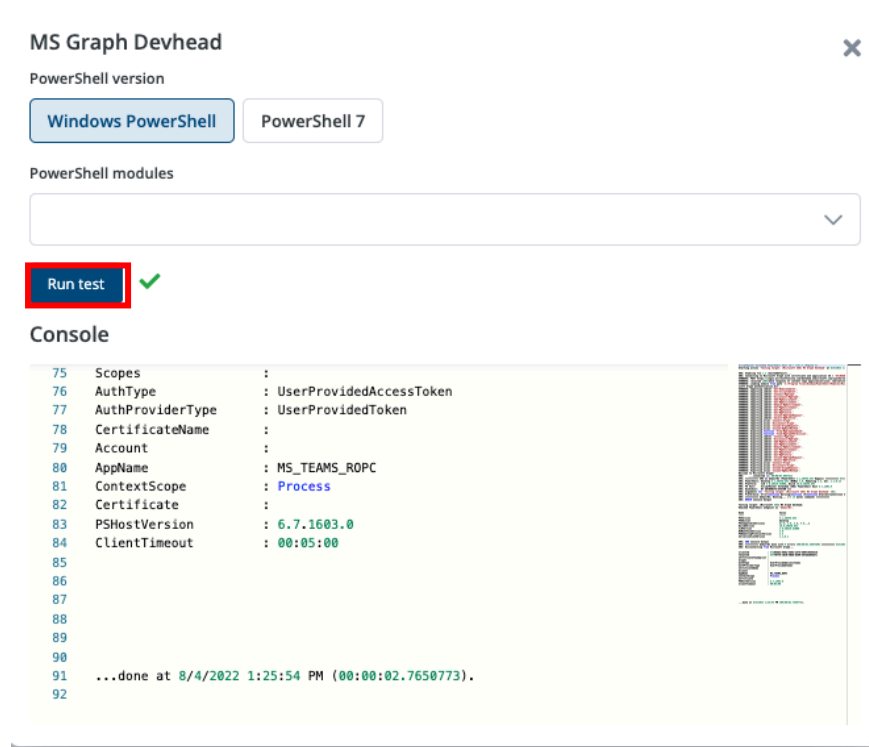


Abbildung 17: Ausgabe des Verbindungstests

War der Verbindungsaufbau erfolgreich können Sie weitere erforderliche Einstellungen vornehmen, die im kommenden Kapitel beschrieben werden.

7 API-Berechtigungen und Ownership anpassen

In diesem Kapitel werden die abschließenden Schritte beschrieben, die erforderlich sind, um eine Anmeldung im ROPC-Workflow durchzuführen.

7.1 API-Berechtigungen anpassen

Öffnen Sie die Einstellungen des registrierten Service-Prinzipals im Azure Portal. Klicken Sie in der linken Navigationsleiste auf **API Permissions**.

Standardmäßig ist hier lediglich die Berechtigung **User.Read** vorhanden:

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

Grant admin consent for devhead

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				...
User.Read	Delegated	Sign in and read user profile	No	...

To view and manage permissions and user consent, try [Enterprise applications](#).

Abbildung 18: Standardberechtigungen für Microsoft Graph

Klicken Sie auf den Button **+Add a permission**, um die folgenden Rechte als Typ **Delegated** hinzuzufügen:

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

Sind alle Berechtigungen korrekt hinterlegt, klicken Sie auf den Button **Grant admin consent for <name>**.

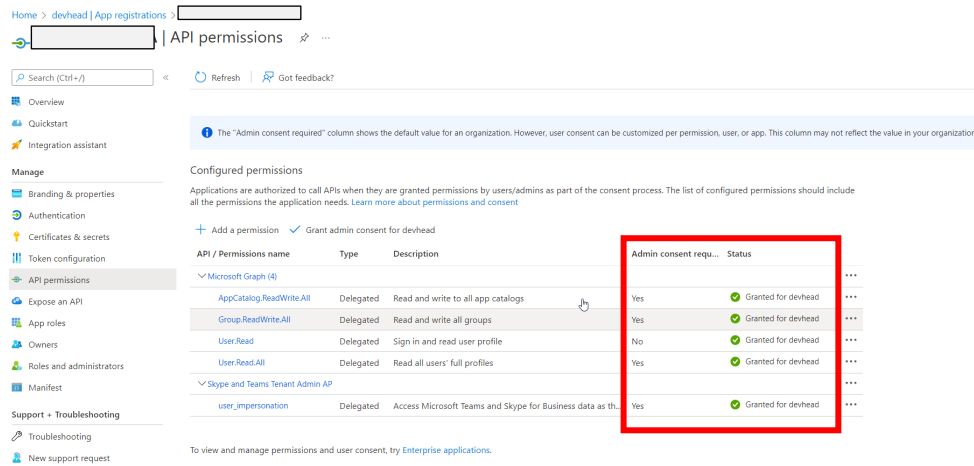


Abbildung 19: Eingerichtete API-Berechtigung mit Admin Consent

7.2 Mitgliedbenutzer in Azure erstellen

Sie benötigen weiterhin einen eigenen, separierten Owner. Verwenden Sie hierfür nicht das globale Administratorkonto, sondern ein Mitgliedskonto.

Hier ist es absolut ausreichend einen Standardbenutzer ohne weitere Rechte einzurichten.

7.3 Mitgliedbenutzer als Owner hinzufügen

Dieser Benutzer muss als Owner hinterlegt werden. Klicken Sie hierzu in der linken Navigationsleiste auf **Owners**.

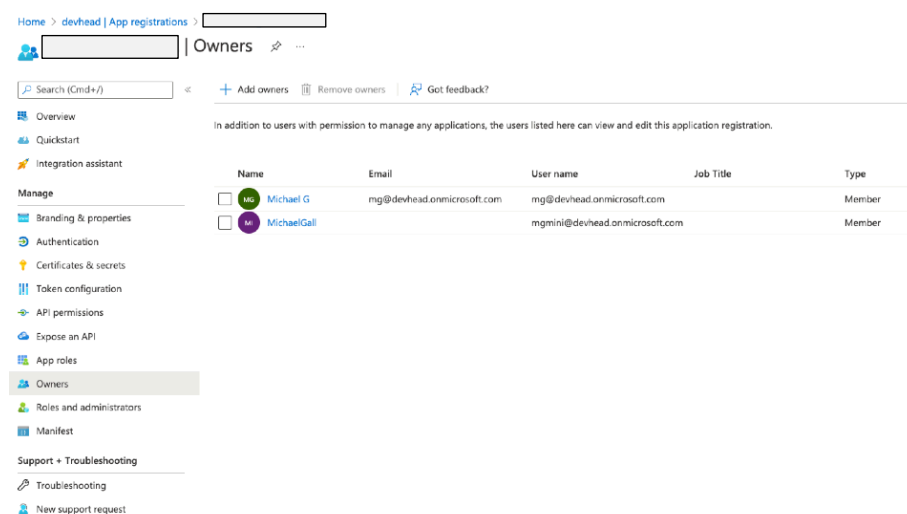


Abbildung 20: Hinzufügen des Mitgliedbenutzers als Owner

8 Abschließende Einrichtung im ScriptRunner

Hinterlegen Sie in ScriptRunner nun das Credential des Benutzerkontos und schließen Sie die Einrichtung ab.

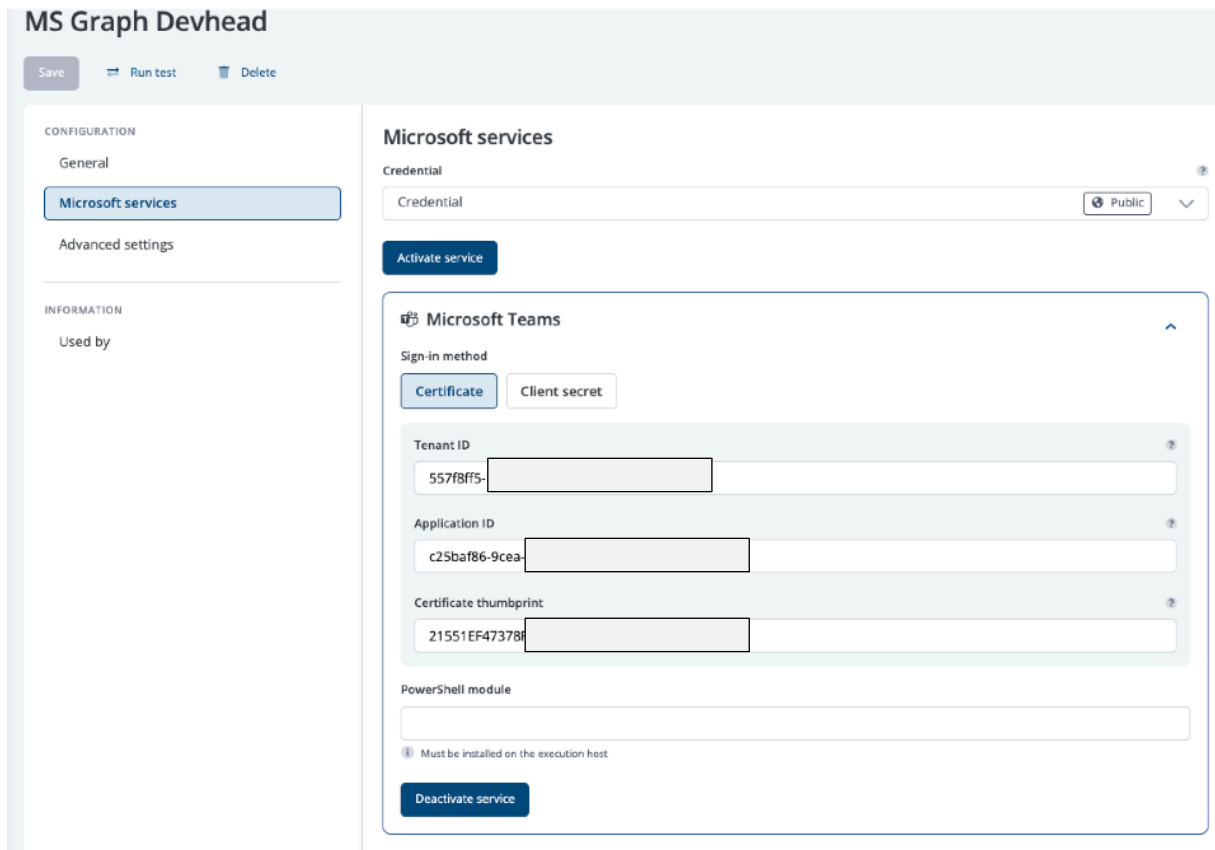
8.1 Credential anlegen

Öffnen Sie das ScriptRunner Portal und wechseln Sie in den Bereich **Credentials**. Hinterlegen Sie die Anmeldedaten des Azure-Kontos (Mitgliedskonto).

8.2 Microsoft Teams-Zielsystem konfigurieren

Legen Sie analog zu Kapitel 6 ein Microsoft Teams-Zielsystem an und übernehmen Sie die Daten aus dem Microsoft Graph-Zielsystem.

Wählen Sie im Feld **Credential** das soeben erstellte Credential aus.



The screenshot shows the 'MS Graph Devhead' interface. On the left, there is a sidebar with 'CONFIGURATION' and 'INFORMATION' sections. Under 'CONFIGURATION', there are 'General', 'Microsoft services', and 'Advanced settings'. Under 'INFORMATION', there is 'Used by'. The main area is titled 'Microsoft services' and contains a 'Credential' dropdown menu, an 'Activate service' button, and a 'Microsoft Teams' configuration box. The 'Microsoft Teams' box has a 'Sign-in method' section with 'Certificate' and 'Client secret' options. Below this are fields for 'Tenant ID' (5578ff5-...), 'Application ID' (c25baf86-9cea-...), and 'Certificate thumbprint' (21551EF473788-...). There is also a 'PowerShell module' field and a 'Deactivate service' button at the bottom.

Abbildung 21: Microsoft Teams-Zielsystem in ScriptRunner

Speichern Sie Ihre Einstellungen. Klicken Sie auf **Run test**, um einen Verbindungstest durchzuführen.

MS Graph Devhead ✕

PowerShell version

Windows PowerShell

PowerShell 7

PowerShell modules

Run test

✓

Console

```

3838
3839
3840
3841
3842
3843
3844
3845
3846 SRX: END Console Output
3847 SRX: ***** demosr01 done with 0 errors (00:00:08.6405807) ***** 8/4/2022
3848 SRX: Disconnecting from Microsoft Teams...
3849
3850
3851
3852
3853
3854 ...done at 8/4/2022 2:08:55 PM (00:00:09.3419472).
3855
                
```

Abbildung 22: Ausgabe des Verbindungstests

9 Checkliste

Voraussetzungen prüfen

- ScriptRunner wird in aktueller Version betrieben (mindestens Portal Edition R4 Build 1603)
- Microsoft Teams-PowerShell-Modul >= Version 4.5.0 ist installiert
- Microsoft Graph-PowerShell-Modul >= Version 1.10.0 ist installiert

Zertifikat einbinden/erstellen

- Falls bereits vorhanden: Microsoft Azure einbinden
- Falls nicht vorhanden: Erstellen eines selbstsignierten Zertifikats mit **-KeySpec Signature**
- Nur den öffentlichen Schlüssel exportieren

Service-Prinzipal in Azure erstellen

- Service-Prinzipal in Azure erstellen
- Application ID, Tenant ID und Zertifikats-Thumbprint notieren
- Zertifikat hochladen

Microsoft Graph-Zielsystem erstellen

- In ScriptRunner ein Microsoft Graph-Zielsystem mit den Daten aus dem Service-Prinzipal anlegen
- Feld **Credential** muss leer bleiben
- Verbindungstest ausführen

API-Berechtigungen anpassen

- Siehe Kapitel 7.1

Eingeschränktes Azure-Konto anlegen (Tenant-Mitglied)

- Siehe Kapitel 7.2

Service-Prinzipal als Owner hinzufügen

- Siehe Kapitel 7.3

Einrichtung in ScriptRunner abschließen

- Unter **Credentials** das Mitgliedskonto anlegen
- Daten aus dem MS Graph-Zielsystem in das Microsoft Teams-Zielsystem übernehmen
- Im Feld **Credential** das Azure-Konto auswählen
- Verbindungstest durchführen

10 Mögliche Fehlerquellen

Dieses Kapitel beschreibt mögliche Fehlerquellen.

10.1 Conditional Access

Stellen Sie sicher, dass keine Regel im Conditional Access den Zugriff einschränkt.

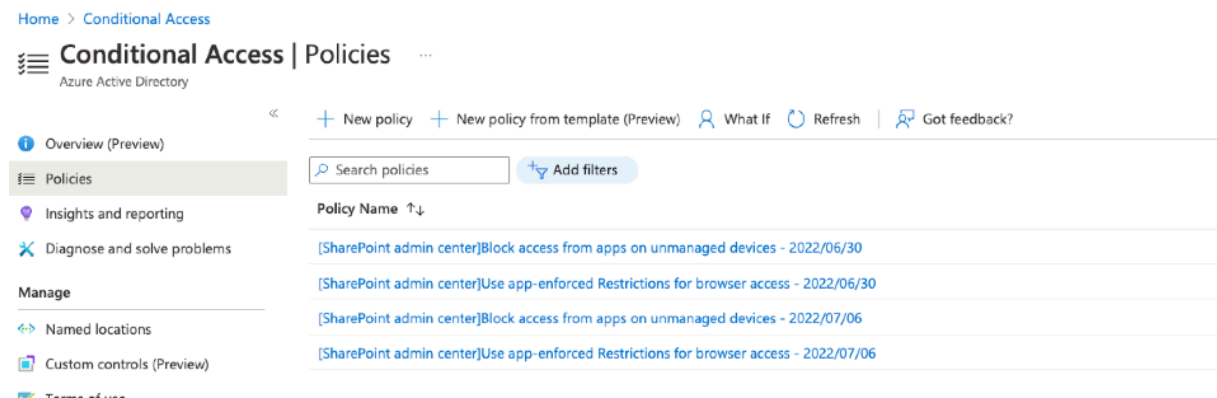


Abbildung 23: Mögliche Einschränkungen durch Conditional Access Policies

Ob eine solche Regel den Zugriff tatsächlich blockt, können Sie über **Monitoring > Sign-in logs** prüfen. Mit dem Wizard kann der betreffende Fehler nachgestellt werden.

Monitoring

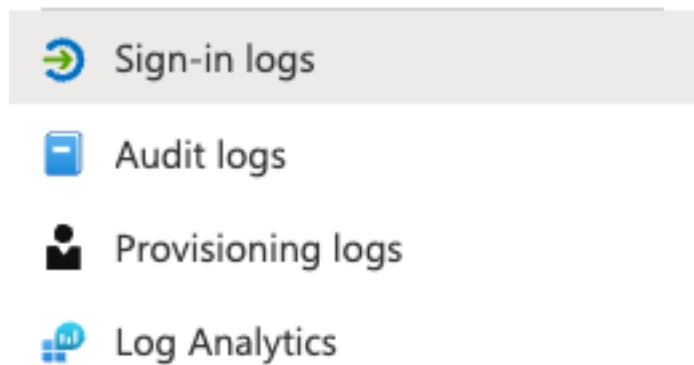


Abbildung 24: Sign-in Logs im Azure Portal

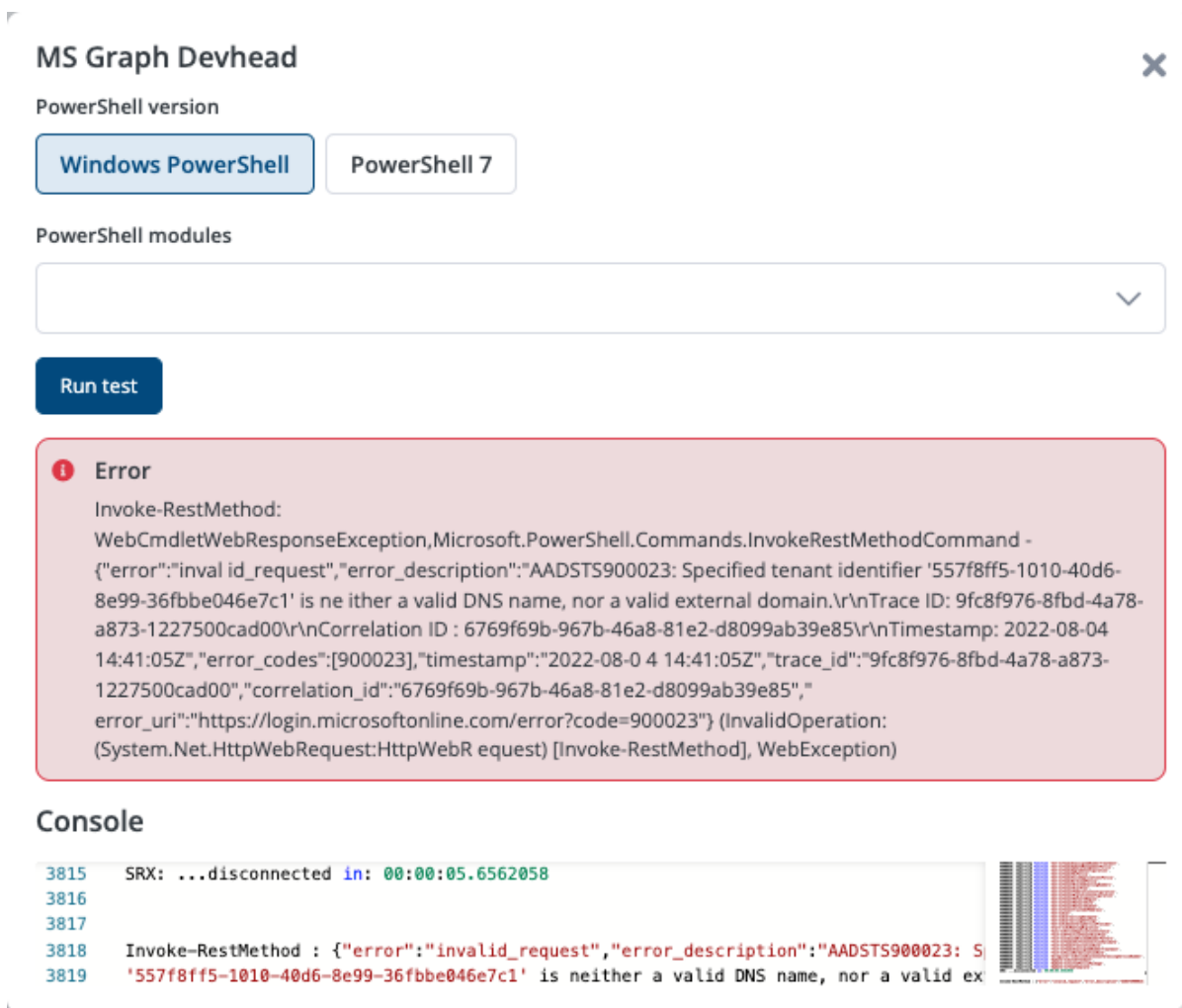
10.2 Probleme bei der Anmeldung

Verwenden Sie den Verbindungstest in der Zielsystemkonfiguration, um Probleme mit dem Zertifikat zu beheben. In aller Regel weisen die Fehlermeldungen auf das Problem hin.

Häufige Fehlerursachen sind:

- Die betreffenden PowerShell-Module fehlen
- Der Zertifikats-Thumbprint ist nicht korrekt
- Die Tenant ID oder Application ID ist nicht korrekt

Die Fehlermeldung wird im oberen Bereich angezeigt.



MS Graph Devhead ✕

PowerShell version

Windows PowerShell PowerShell 7

PowerShell modules

Run test

Error

Invoke-RestMethod:
WebCmdletWebResponseException, Microsoft.PowerShell.Commands.InvokeRestMethodCommand -
{\"error\": \"invalid_request\", \"error_description\": \"AADSTS900023: Specified tenant identifier '557f8ff5-1010-40d6-8e99-36fbbe046e7c1' is neither a valid DNS name, nor a valid external domain. Trace ID: 9fc8f976-8fbd-4a78-a873-1227500cad00 Correlation ID: 6769f69b-967b-46a8-81e2-d8099ab39e85 Timestamp: 2022-08-04 14:41:05Z, error_codes: [900023], timestamp: \"2022-08-04 14:41:05Z\", trace_id: \"9fc8f976-8fbd-4a78-a873-1227500cad00\", correlation_id: \"6769f69b-967b-46a8-81e2-d8099ab39e85\", error_uri: \"https://login.microsoftonline.com/error?code=900023\"} (InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-RestMethod], WebException)

Console

```
3815 SRX: ...disconnected in: 00:00:05.6562058
3816
3817
3818 Invoke-RestMethod : {\"error\": \"invalid_request\", \"error_description\": \"AADSTS900023: S
3819 '557f8ff5-1010-40d6-8e99-36fbbe046e7c1' is neither a valid DNS name, nor a valid ex
```

Abbildung 25: Fehlermeldung im ScriptRunner Portal – ungültige Tenant ID

11 Anmerkungen und Quellenangaben

11.1 Anmerkungen

In dieser Anleitung wurden die folgenden Microsoft Azure-Benutzer verwendet:

- mg@devhead.onmicrosoft.com -> Tenant / Globaler Administrator
- mgmini@devhead.onmicrosoft.com -> Einfaches Benutzerkonto im Tenant

Informationen zum Tenant, Tenant ID, Application ID und Zertifikats-Thumbprints wurden unkenntlich gemacht.

11.2 Quellenangaben

Microsoft Teams – ROPC-Anmeldung:

<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/teams-ps/teams/Connect-MicrosoftTeams.md>