glück kanja

RealmJoin – Tenant Data Access Details

Data Protection Information

Version: July 2018

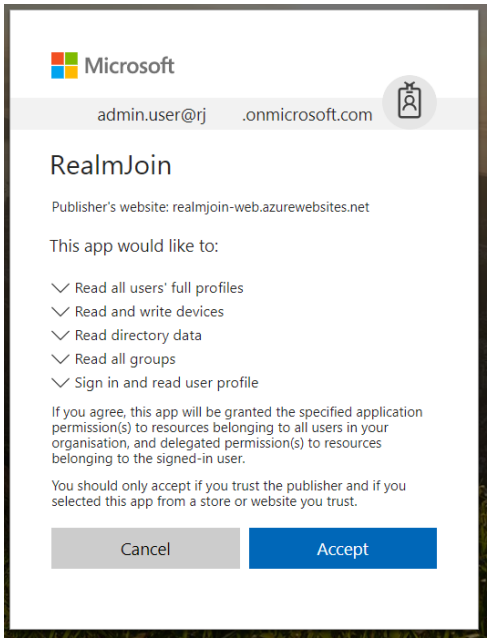
Glück & Kanja Consulting AG, Kaiserstraße 39, D-63065 Offenbach am Main, Germany
HRB 12381 Offenbach am Main, Steuer-Nr.: 035 234 46203
Vorstände: Michael Breither, Christoph Fausak, Harald Glück, Christian Kanja, Felix Storm
Aufsichtsratsvorsitzende: Lilian Glück

Table of Contents

RealmJoin backend connectivity with Microsoft Graph API

The RealmJoin backend is an Azure web application using an Azure SQL database and the available Azure services. The backend is hosted on an Azure tenant exclusively used for RealmJoin. All customer realms within this tenant are isolated from each other.

During the tenant enrollment the RealmJoin backend creates an access token with the consent of a customer tenant administrator to access certain endpoints in the Microsoft Graph API. This API is – in this case – comparable to the on premise Active Directory or LDAP access of corporate directory data. Because of the very strict permission modell of Mircrosoft Graph API the consent is only given to a limited range of endpoints shown in the following image:



Tenant Synchronization (persistent data)

By default the RealmJoin backend is synchronizing groups which are prefixed by

```
"cfg-"
"cfg -"
"app-"
"app -"
```

This default configuration may be changed by a tenant administrator but it is in the interest of Glück & Kanja and the customer to synchronize only groups and users relevant for the application deployment assignment.

Based on these prefixes the RealmJoin backend synchronizes the following data on a regular base from the connected Microsoft Graph API group endpoint:

```
Group GUID
Group Display Name
Group Description
Group Member GUIDs
```

With the given information about the members of the relevant groups the RealmJoin backend synchronizes the following data on a regular base from the connected Microsoft Graph API user endpoint:

```
User GUID
User UPN (E-Mail address)
```

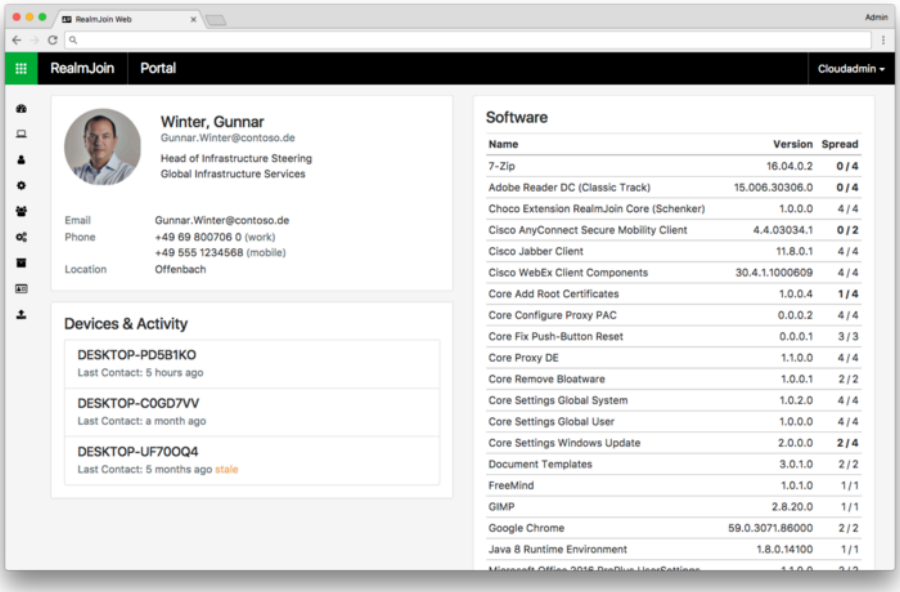
Only the above data from the customer tenant is persistet in the encrypted RealmJoin backend database system.

Tenant Non-Persistent Data (on demand access)

When using the RealmJoin services there are two components with access to the Microsoft Graph API to show data on demand.

The RealmJoin Administrative Portal

An assigned administrator needs to assign applications, test packages or needs to support users and devices during his daily work. To accomplish this task The RealmJoin Administrative Portal shows non-persistent data from Microsoft Graph during a valid operations session:



The data shown during theses sessions are user and device data shown in the following table (with sample data):


```
"USERS": [
        {
            "id": "6e7b768e-07e2-4810-8459-485f84f8f204",
            "deletedDateTime": null,
            "accountEnabled": true,
            "ageGroup": null,
            "businessPhones": [],
            "city": null,
            "createdDateTime": "2017-09-04T15:35:02Z",
            "companyName": null,
            "country": null,
            "department": null,
            "displayName": "Jon Doe",
            "givenName": null,
            "jobTitle": null,
            "mail": "jon.doe@M365x214355.onmicrosoft.com",
            "mobilePhone": null,
            "onPremisesDomainName": null,
            "onPremisesImmutableId": null,
            "onPremisesLastSyncDateTime": null,
            "onPremisesSecurityIdentifier": null,
            "onPremisesSamAccountName": null,
            "onPremisesSyncEnabled": null,
            "onPremisesUserPrincipalName": null,
            "officeLocation": null,
            "postalCode": null,
            "preferredDataLocation": null,
            "preferredLanguage": null,
            "isResourceAccount": null,
            "state": null,
            "streetAddress": null,
            "surname": null,
            "usageLocation": null,
            "userPrincipalName":
"jon.doe@M365x214355.onmicrosoft.com",
            "userType": "Member",
            "assignedLicenses": [],
            "assignedPlans": [],
            "deviceKeys": [],
            "onPremisesExtensionAttributes": {
                "extensionAttribute1": null,
                "extensionAttribute2": null,
                "extensionAttribute3": null,
                "extensionAttribute4": null,
                "extensionAttribute5": null,
                "extensionAttribute6": null,
                "extensionAttribute7": null,
                "extensionAttribute8": null,
                "extensionAttribute9": null,
                "extensionAttribute10": null,
                "extensionAttribute11": null,
```

```
                "extensionAttribute12": null,
                "extensionAttribute13": null,
                "extensionAttribute14": null,
                "extensionAttribute15": null
            },
            "provisionedPlans": []
        }

"DEVICES": [
        {
            "id": "00ac1bea-c1ee-4b21-9752-42dd8b153a99",
            "deletedDateTime": null,
            "accountEnabled": true,
            "complianceExpirationDateTime": null,
            "deviceId": "d259c854-d0e8-4b09-b3b6-195c6e387a85",
            "deviceMetadata": null,
            "deviceVersion": 2,
            "displayName": "DESKTOP-TVJBA62",
            "isCompliant": false,
            "isManaged": true,
            "onPremisesLastSyncDateTime": null,
            "onPremisesSyncEnabled": null,
            "operatingSystem": "Windows",
            "operatingSystemVersion": "10.0.15063.1029",
            "physicalIds": [],
            "profileType": null,
            "systemLabels": [],
            "trustType": "AzureAd"
        }
```


The RealmJoin Client

During a user session on a corporate managed device the local RealmJoin Agent is able to 'lookup' the above data for the current user only in the current user session only. This is necessary for several on demand application installation decisions, especially some of the details are available to the installations to personalize the device (profiles based on location, department, user name for office templates, etc.).