inetum
realdolmen
Positive digital flow

Self Service Privileged Identity Management

Self Service PIM

Installation Guide

inetum.world

22/09/2021 | ©2021 Inetum | v1.0
Classification: external document

Contents

1. Preface

This document will elaborate on a number of different topics:

- Initial configuration of Self Service PIM (SSPIM) after purchase (authentication & authorization)
- Domain, Tenant and agent configuration
- Groups and privileges configuration

Other helpful assets are these YouTube videos:

- How to use Self Service PIM: https://youtu.be/NLx62UkNSeY
- How to Configure and Manage Self Service PIM: https://youtu.be/lIdM5tatpnQ
- How to Install and Configure Self Service PIM: https://youtu.be/Y29AuKZvEaI

Requirements of the SSPIM Agent:

- Outbound connectivity on port 443 to https://[yourinstance].selfservicepim.com
- Operation System of Windows Server 2012 R2 or later (Windows Server 2019 preferred)
- Latest version of .NET framework

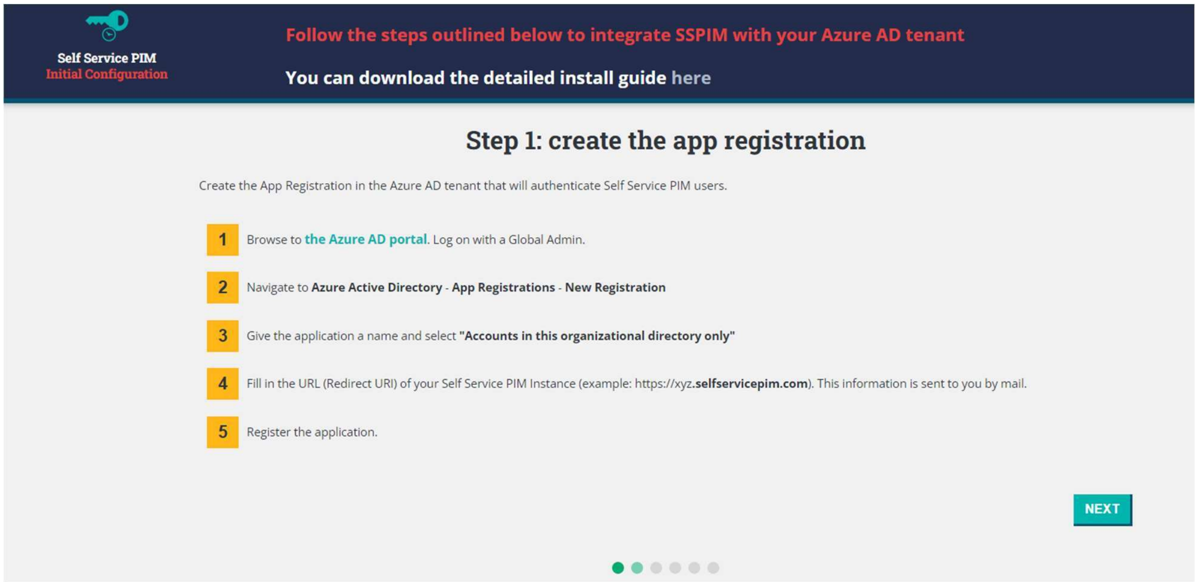
2. Initial Setup

2.1. Confirmation Email

After you subscribed to SSPIM from the Azure Marketplace, you will receive a confirmation email containing the URL of your dedicated Self Service PIM instance. This will be a URL along the lines of https://**[yourinstance].selfservicepim.com**. The email is sent to the Technical Contact that you provided during the subscription process.

2.2. Authentication and authorization

When you navigate to your Self Service PIM instance, you will be presented with a wizard-like interface that allows you to configure the authentication (OpenID Connect) and authorization part.



Follow the steps outlined below to integrate SSPIM with your Azure AD tenant

You can download the detailed install guide here

Step 1: create the app registration

Create the App Registration in the Azure AD tenant that will authenticate Self Service PIM users.

1 Browse to the Azure AD portal. Log on with a Global Admin.

2 Navigate to **Azure Active Directory** - **App Registrations** - **New Registration**

3 Give the application a name and select **"Accounts in this organizational directory only"**

4 Fill in the URL (Redirect URI) of your Self Service PIM Instance (example: https://xyz.**selfservicepim.com**). This information is sent to you by mail.

5 Register the application.

A. App Registration creation

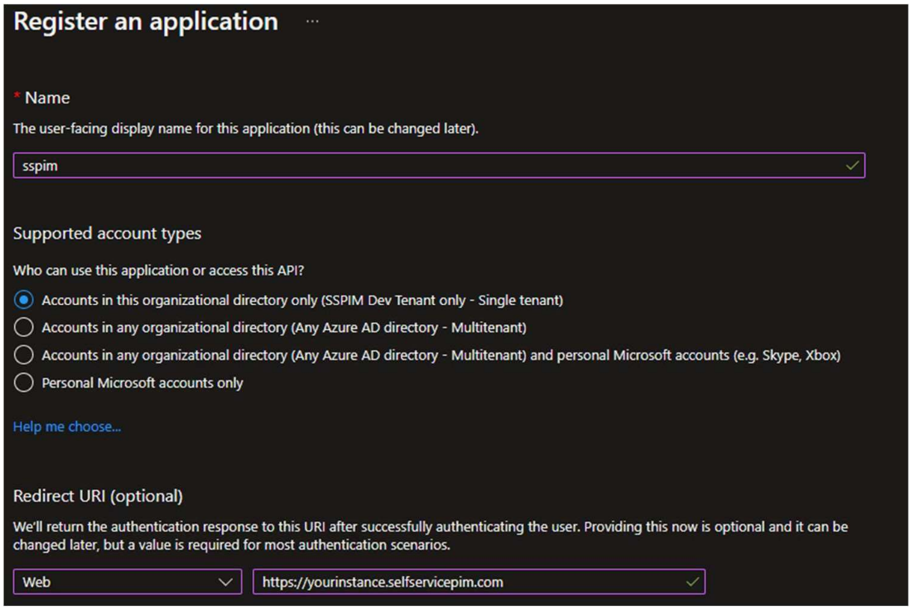
Entra ID >> App Registrations >> New registration

First step is to logon to the Entra ID portal that will function as the Identity Provider, with a Global Admin credential. There, you will need to create a new **App Registration**.

Make sure to select **Accounts in this organizational directory only**.

Provide a name for the application, confirm your naming convention.

Provide the correct Redirect URI; https://**[yourinstance].selfservicepim.com**



Register an application ···

* Name

The user-facing display name for this application (this can be changed later).

sspim ✓

Supported account types

Who can use this application or access this API?

- ● Accounts in this organizational directory only (SSPIM Dev Tenant only - Single tenant)
- ○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ○ Personal Microsoft accounts only

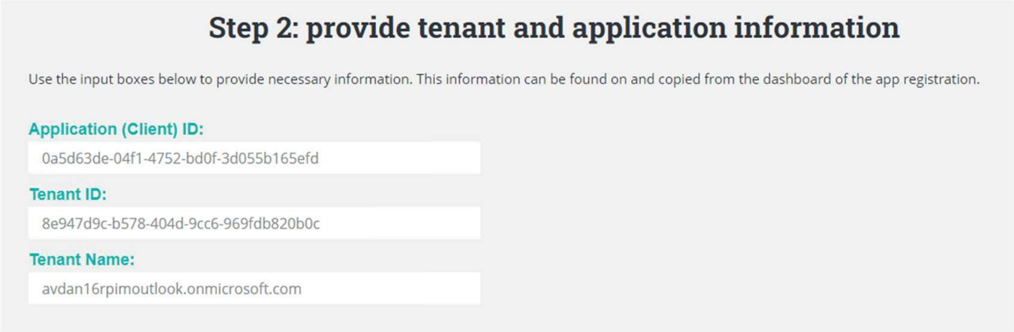
Help me choose...

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.

Web | https://yourinstance.selfservicepim.com ✓

B. Find and Provide Client ID, Tenant ID and Tenant name



Step 2: provide tenant and application information

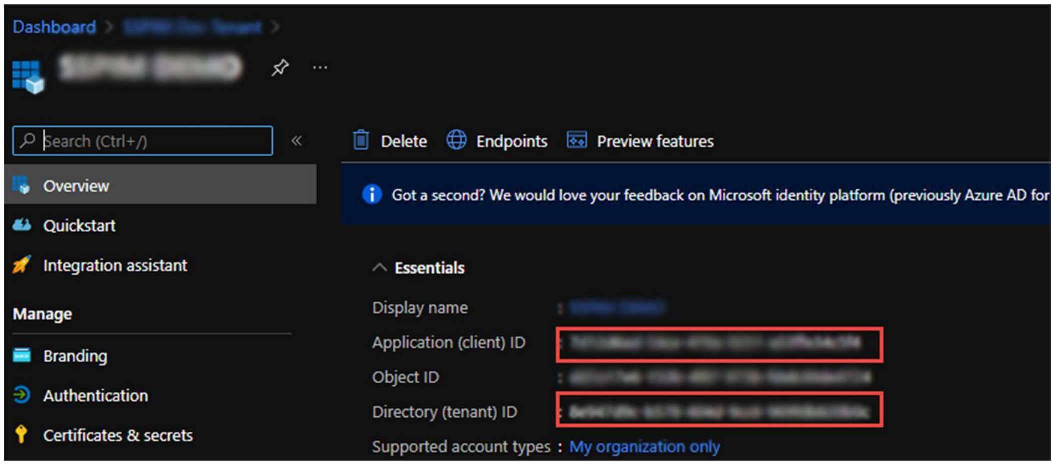
Use the input boxes below to provide necessary information. This information can be found on and copied from the dashboard of the app registration.

Application (Client) ID: 0a5d63de-04f1-4752-bd0f-3d055b165efd

Tenant ID: 8e947d9c-b578-404d-9cc6-969fdb820b0c

Tenant Name: avdan16rpimoutlook.onmicrosoft.com

You can find the ClientID and the Tenant ID on the **Overview** page of your newly created App Registration.



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for

Essentials

Display name : [redacted]

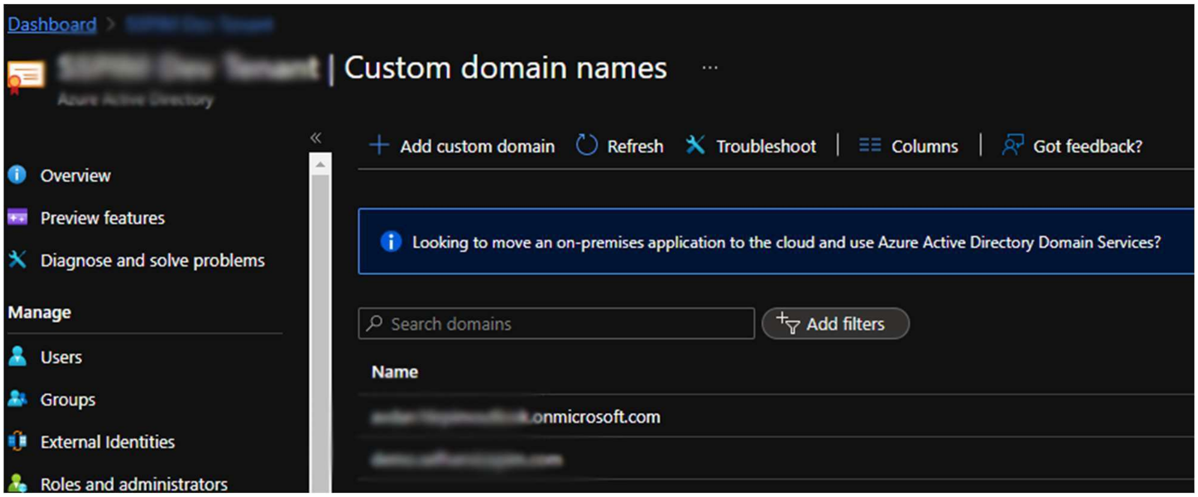
Application (client) ID : [redacted]

Object ID : [redacted]

Directory (tenant) ID : [redacted]

Supported account types : My organization only

You can find your Tenant Name (onmicrosoft) on the **Custom domain names blade** of **Azure Active Directory**.



Dashboard > [redacted]

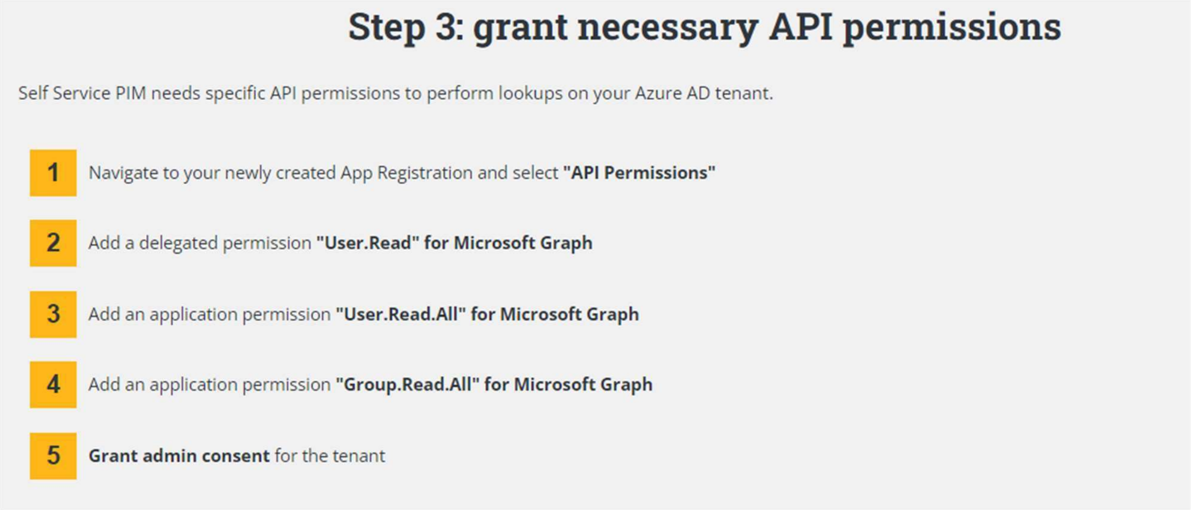
[redacted] | Custom domain names ...

[redacted]

Looking to move an on-premises application to the cloud and use Azure Active Directory Domain Services?

Name
[redacted].onmicrosoft.com
[redacted]

C. Grant API Permissions and give Admin Consent



Step 3: grant necessary API permissions

Self Service PIM needs specific API permissions to perform lookups on your Azure AD tenant.

1 Navigate to your newly created App Registration and select **"API Permissions"**

2 Add a delegated permission **"User.Read" for Microsoft Graph**

3 Add an application permission **"User.Read.All" for Microsoft Graph**

4 Add an application permission **"Group.Read.All" for Microsoft Graph**

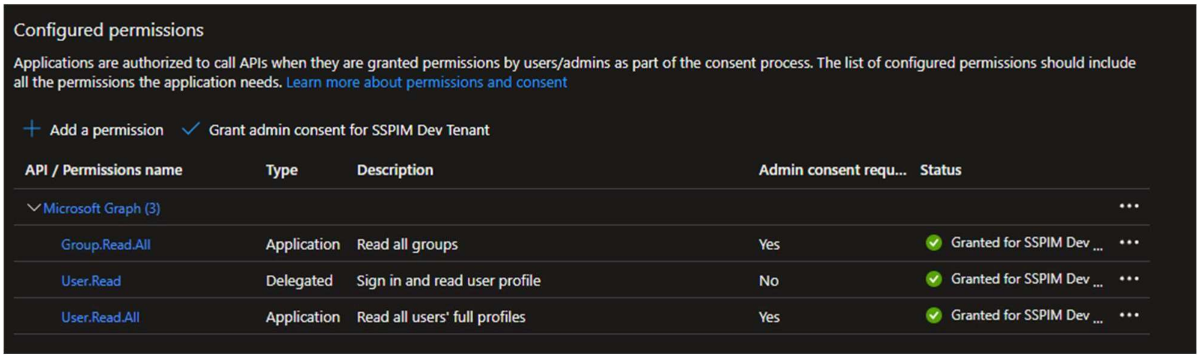
5 **Grant admin consent** for the tenant

Entra ID >> App Registrations >> Your App >> API Permissions

Self Service PIM will also use the App Registration to perform Graph API calls. Following permissions are needed:

API	Type	Permission Name
Microsoft Graph	Application	User.Read.All
Microsoft Graph	Application	Group.Read.All

Make sure to grant **Admin Consent** for the permissions that have just been selected.

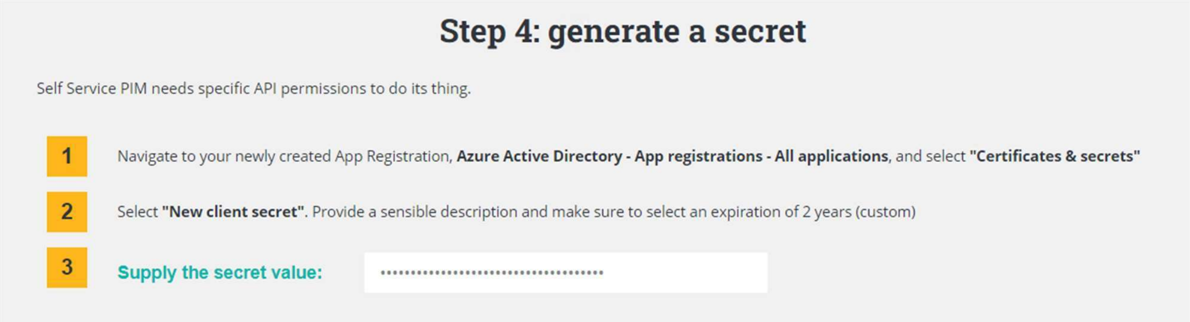


Configured permissions

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

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
Group.Read.All	Application	Read all groups	Yes	✓ Granted for SSPIM Dev ...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for SSPIM Dev ...
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for SSPIM Dev ...

D. Generate a Client Secret



Step 4: generate a secret

Self Service PIM needs specific API permissions to do its thing.

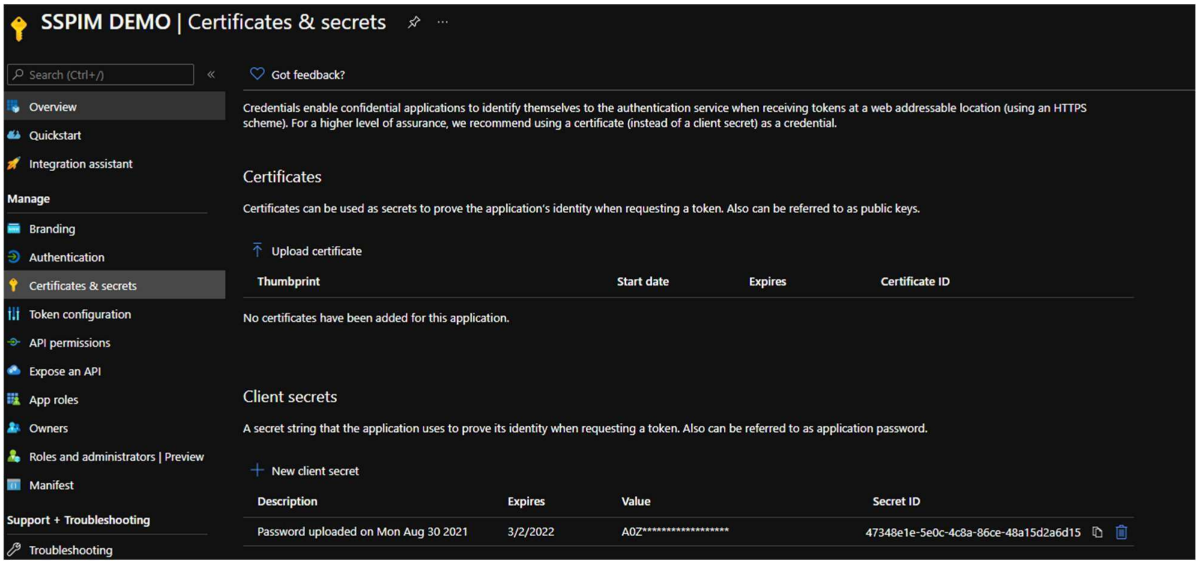
1 Navigate to your newly created App Registration, **Azure Active Directory - App registrations - All applications**, and select **"Certificates & secrets"**

2 Select **"New client secret"**. Provide a sensible description and make sure to select an expiration of 2 years (custom)

3 Supply the secret value: ••••••••••••••••••••••••••••••••••••

Entra ID >> App Registrations >> Your App >> Certificates and secrets

To perform Graph API calls, a Client Secret is needed. We can generate one in the **Certificates and Secrets** section under your newly created App Registration.



SSPIM DEMO | Certificates & secrets

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.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires	Certificate ID

No certificates have been added for this application.

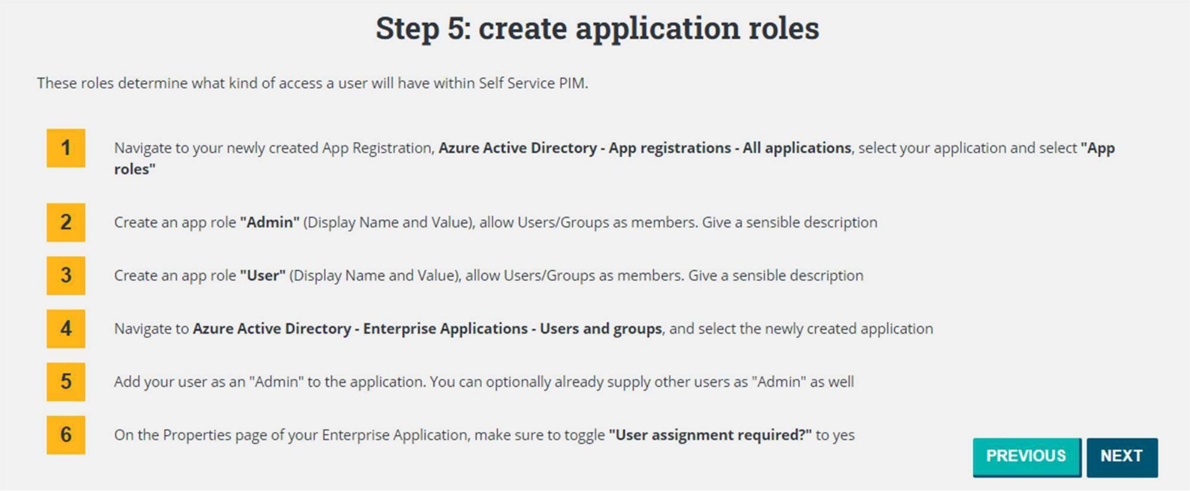
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
Password uploaded on Mon Aug 30 2021	3/2/2022	A0Z******************	47348e1e-5e0c-4c8a-86ce-48a15d2a6d15

The generated secret needs to be supplied in the Initial Setup wizard on Step 4.

E. Create and Assign Application Roles



Step 5: create application roles

These roles determine what kind of access a user will have within Self Service PIM.

1 Navigate to your newly created App Registration, **Azure Active Directory - App registrations - All applications**, select your application and select **"App roles"**

2 Create an app role **"Admin"** (Display Name and Value), allow Users/Groups as members. Give a sensible description

3 Create an app role **"User"** (Display Name and Value), allow Users/Groups as members. Give a sensible description

4 Navigate to **Azure Active Directory - Enterprise Applications - Users and groups**, and select the newly created application

5 Add your user as an "Admin" to the application. You can optionally already supply other users as "Admin" as well

6 On the Properties page of your Enterprise Application, make sure to toggle **"User assignment required?"** to yes

Create

Entra ID >> App Registrations >> Your App >> App Roles

Applications roles are needed within SSPIM to distinguish between a regular user and an SSPIM administrator. A regular user is able to logon to SSPIM and request escalations (if the user was authorized for a privilege). An SSPIM administrator can manage all aspects of SSPIM (domains, agents, groups, privileges) and perform reporting related tasks.

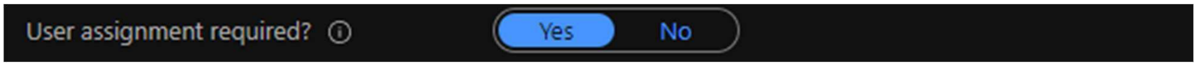
Under the **App Roles** section, you can create these app roles. Make sure that **Value** is exactly the same as stipulated below. Display Name and Description can be adjusted to your liking.

Display Name	**Description**	**Value**	**Member types**
User	Regular SSPIM user	User	Users/Groups
Admin	SSPIM administrator	Admin	Users/Groups
SuperAdmin*	A user that has access to all privileges.	SuperUser	Users/Groups

Assign

Entra ID >> Enterprise Applications >> Your App >> Properties

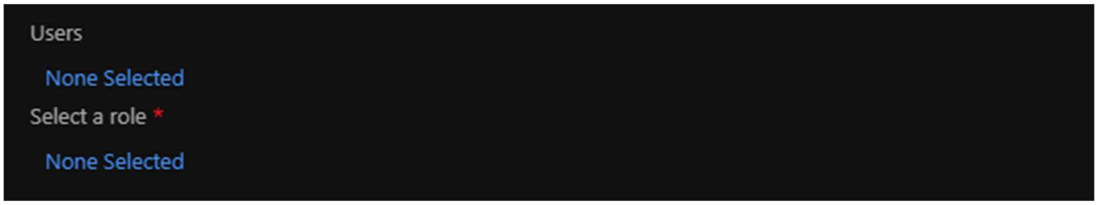
Make sure that not everybody can use the Application. You can accomplish this by altering the property **User assignment required** to **Yes.** This is of paramount importance! If this step is not completed, guest accounts for example will fail to receive the correct App Roles.



User assignment required? [✓ Yes] No

Entra ID >> Enterprise Applications >> Your App >> Users and groups

Add your user account (and optionally others) as an admin to the application. Make sure to select the Admin Role. You can immediately grant the User role to the people that will use SSPIM to request privileges (guest accounts can also be used here).



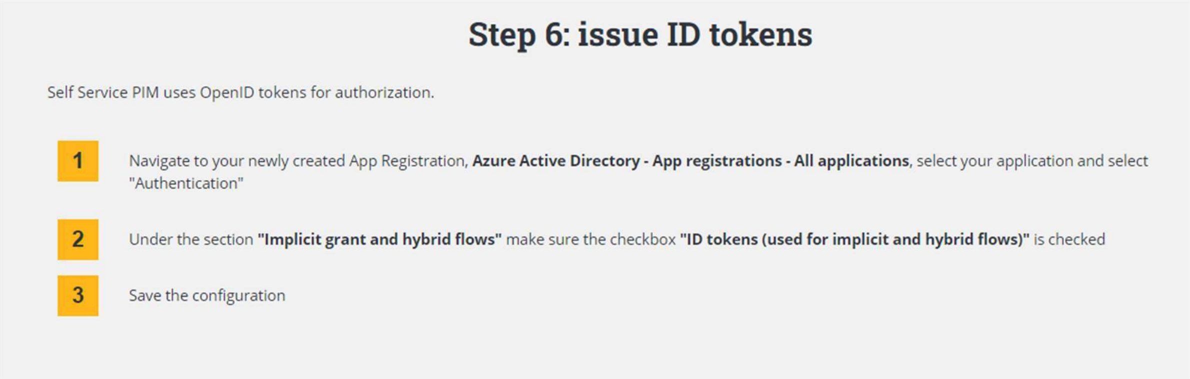
Users

None Selected

Select a role *

None Selected

F. Configure issuance of ID Tokens



Step 6: issue ID tokens

Self Service PIM uses OpenID tokens for authorization.

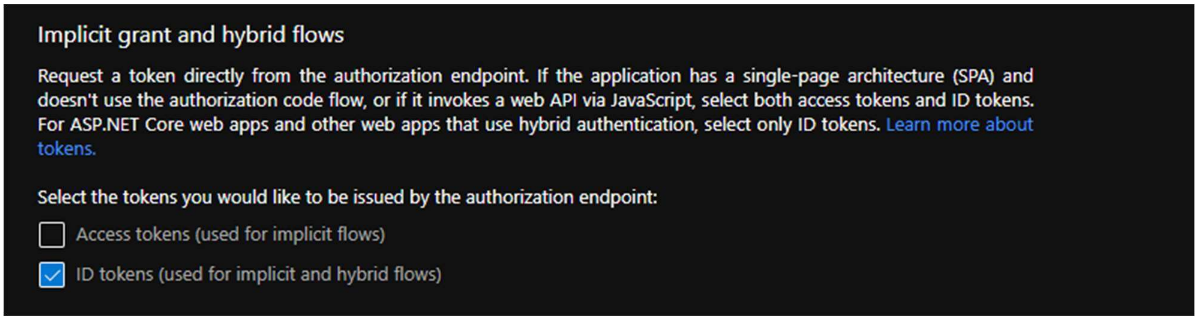
1 Navigate to your newly created App Registration, **Azure Active Directory - App registrations - All applications**, select your application and select "Authentication"

2 Under the section **"Implicit grant and hybrid flows"** make sure the checkbox **"ID tokens (used for implicit and hybrid flows)"** is checked

3 Save the configuration

Entra ID >> App Registrations >> Your App >> Authentication >> Implicit grant and hybrid flows

SSPIM uses ID tokens to perform authorization.



Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more about tokens.

Select the tokens you would like to be issued by the authorization endpoint:

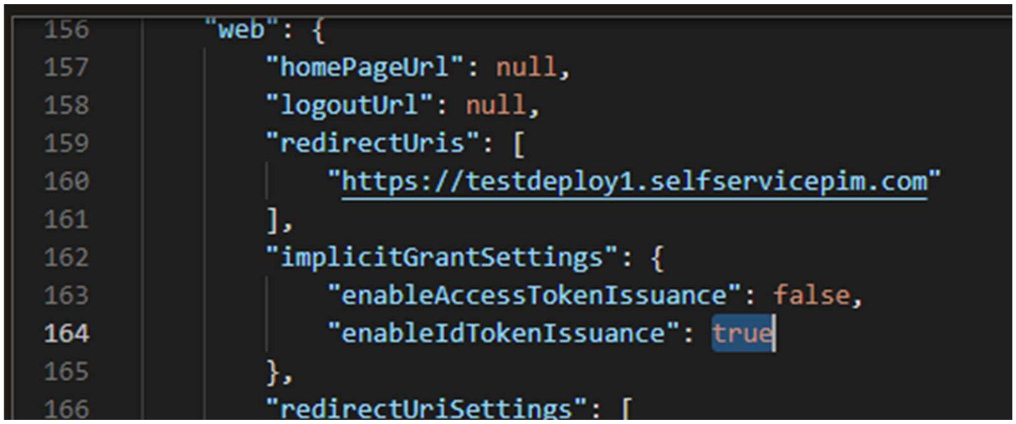
☐ Access tokens (used for implicit flows)

☑ ID tokens (used for implicit and hybrid flows)

Note: if this section is missing from the user interface, you will need to enable Implicit Grant through the Manifest file.

Entra ID >> App Registrations >> Your App >> Authentication >> Manifest

Set the "**enableIdTokenIssuance**" (under Web >> implicitGrantSettings) setting to **true**.



```
"web": {
    "homePageUrl": null,
    "logoutUrl": null,
    "redirectUris": [
        "https://testdeploy1.selfservicepim.com"
    ],
    "implicitGrantSettings": {
        "enableAccessTokenIssuance": false,
        "enableIdTokenIssuance": true
    },
    "redirectUriSettings": [
```

After saving this setting, the ID token checkbox will be visible and already checked.

G. Recommendation: enable MFA on the app

Entra ID >> Security >> Conditional Access >> New Policy

As a security best practice, enable MFA for the application. You can perform this with the help of Conditional Access.

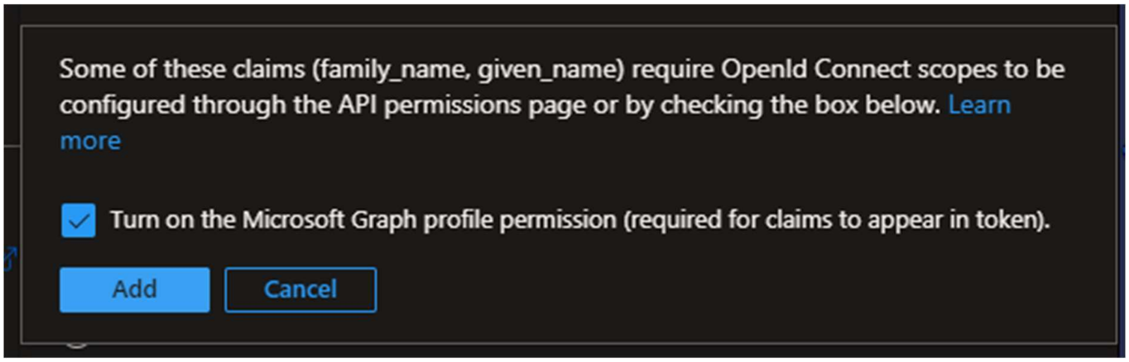
H. Configure Optional Claims

The SSPIM Control Panel has a feature that enables you to use a user’s first- and lastname in a regular expression in order to conform to more complex naming conventions. By default, first- and lastname are not a part of a basic Open ID token. Therefore, we need to configure these attributes as optional claims.

Entra ID >> App Registrations >> Your App >> Token Configuration >> Add optional claim

Add the **given_name** and **family_name** Open ID claims.

Make sure to let Entra ID configure the necessary Graph API permissions so that claims will appear in the token.

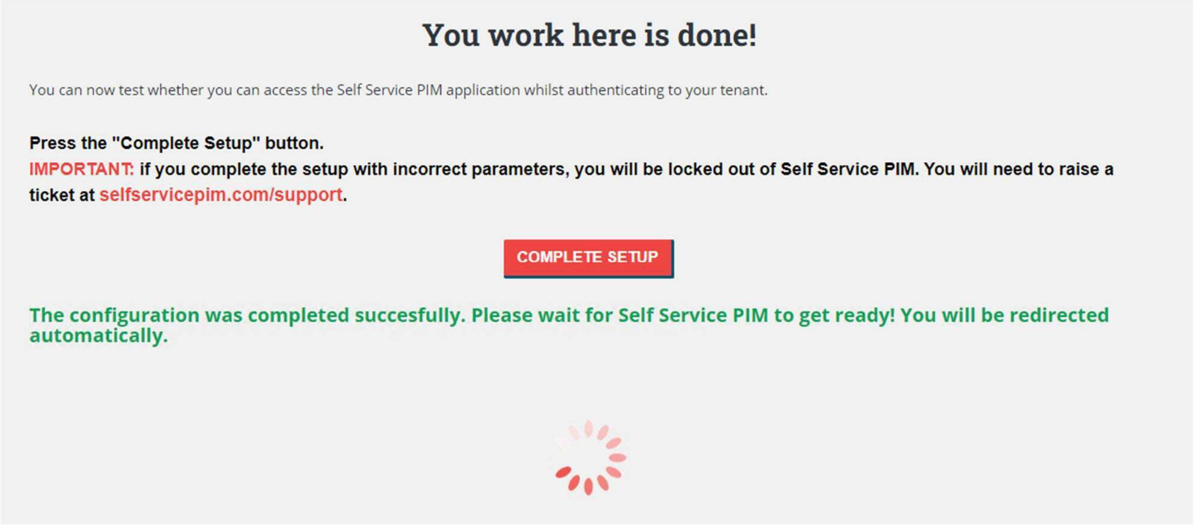


Some of these claims (family_name, given_name) require OpenId Connect scopes to be configured through the API permissions page or by checking the box below. Learn more

☑ Turn on the Microsoft Graph profile permission (required for claims to appear in token).

I. Complete the setup

Completing the setup will save your authentication and authorization setup to SSPIM. SSPIM will use your Tenant ID, Tenant Name, Client ID and Client Secret to perform AuthN, AuthZ and Graph Calls.



You work here is done!

You can now test whether you can access the Self Service PIM application whilst authenticating to your tenant.

Press the "Complete Setup" button.
IMPORTANT: if you complete the setup with incorrect parameters, you will be locked out of Self Service PIM. You will need to raise a ticket at selfservicepim.com/support.

The configuration was completed succesfully. Please wait for Self Service PIM to get ready! You will be redirected automatically.

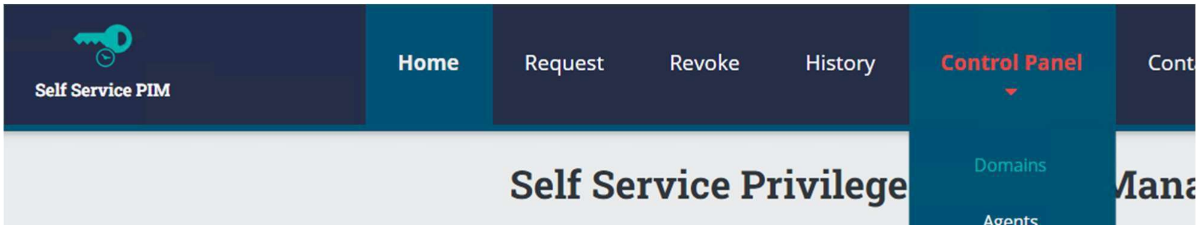
IMPORTANT: it will take SSPIM up to 5 minutes to setup in the background. When this is finished, you will be automatically redirected to **https://[yourinstance].selfservicepim.com**. If this should fail, be patient and try to navigate to the URL a bit later.

2.3. SSPIM Configuration

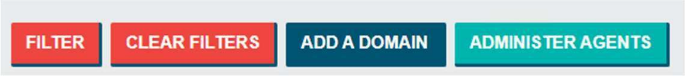
Now that the Initial Setup is finished, you can configure domains, agents, groups, privileges and schedules.

A. Create a domain

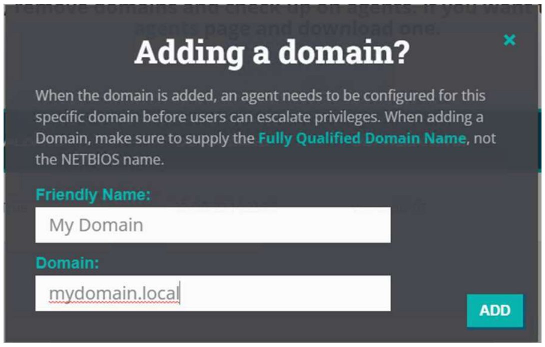
Authenticate to SSPIM using an Entra ID account that was granted the **Admin** App Role. This will enable the SSPIM Control Panel. Navigate to **Control Panel >> Domains.**



Click the **Add A Domain** button.



A dialogue box appears. Fill in the **Fully Qualified Domain Name** of your AD domain. Optionally, you can also set a **Friendly Name** for easy reference. Click **Add**.



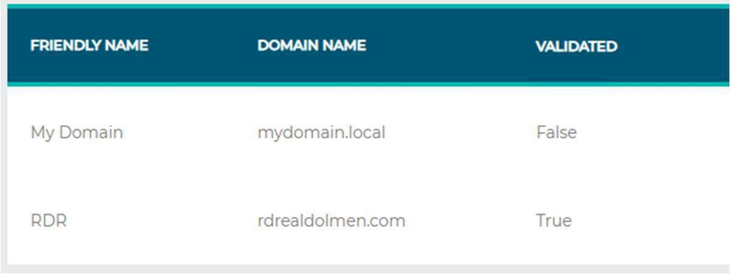
Adding a domain?

When the domain is added, an agent needs to be configured for this specific domain before users can escalate privileges. When adding a Domain, make sure to supply the **Fully Qualified Domain Name**, not the NETBIOS name.

Friendly Name: My Domain

Domain: mydomain.local

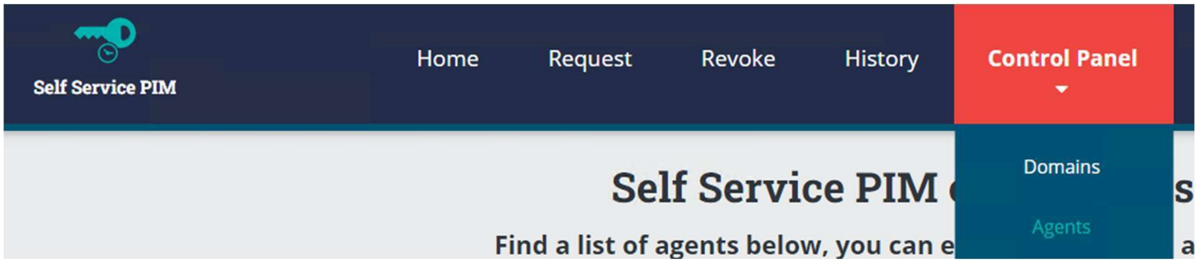
This results in the addition of the domain:



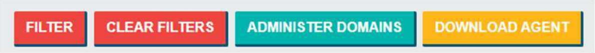
FRIENDLY NAME	DOMAIN NAME	VALIDATED
My Domain	mydomain.local	False
RDR	rdrealdolmen.com	True

B. Download and install an Agent

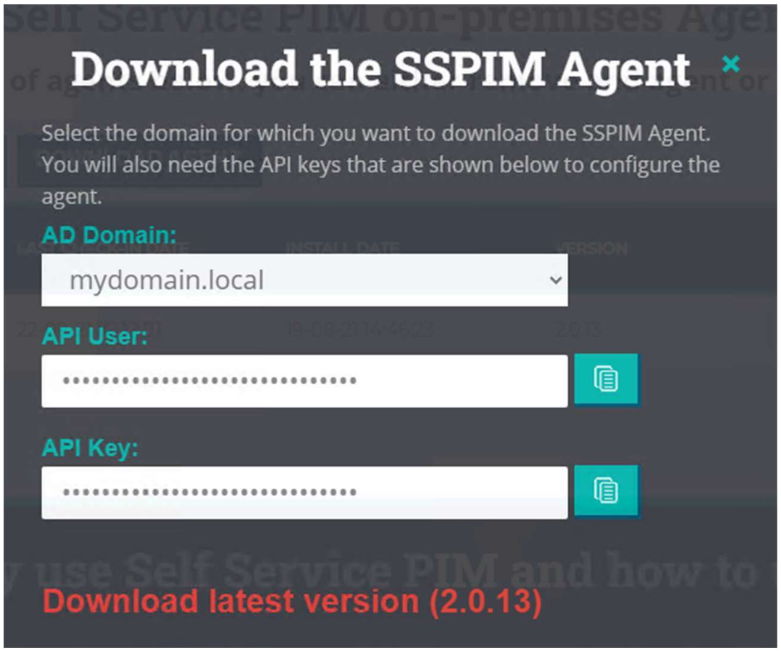
Now we have a Domain configured, we need to tie an agent to it (or multiple agents for redundancy). An SSPIM agent will perform privilege escalation requests for a specific domain. Navigate to **Control Panel >> Agents**



Click the **Download Agent** button.



A dialogue box appears. Here you can find a download link for the latest SSPIM agent version, as well as the 2 corresponding API keys. These keys will be needed later in the configuration of the agent.



Download the SSPIM Agent

Select the domain for which you want to download the SSPIM Agent. You will also need the API keys that are shown below to configure the agent.

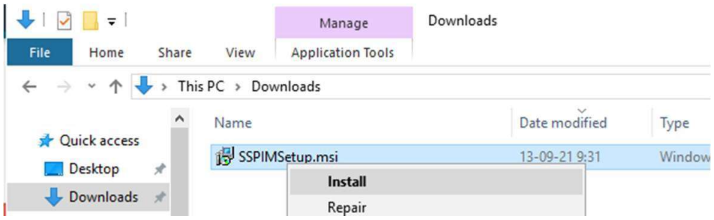
AD Domain: mydomain.local

API User: ••••••••••••••••••••••••••••••••

API Key: ••••••••••••••••••••••••••••••••

Download latest version (2.0.13)

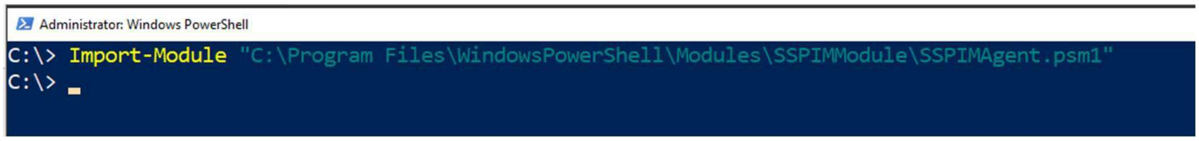
Copy the MSI to a server that is joined to the Domain that you created in SSPIM. **Do not install the agent on a Domain Controller!** Install the MSI.



C. Configure the SSPIM agent

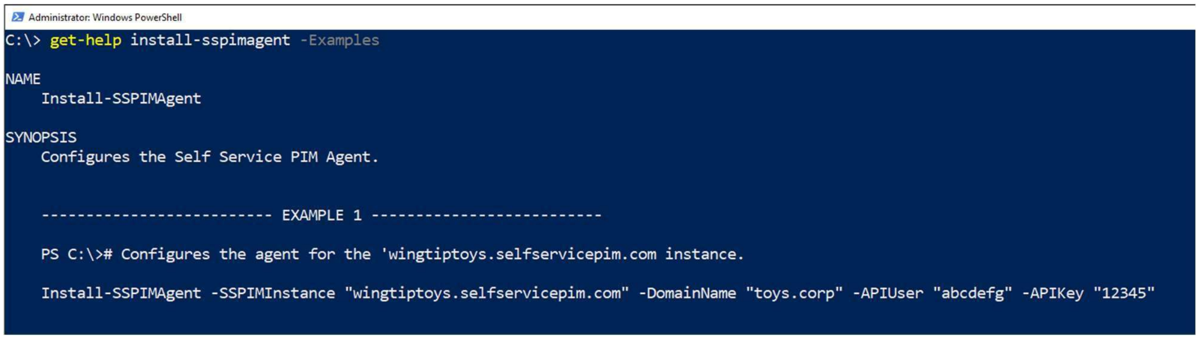
The MSI installation also installed a **Powershell module (SSPIMAgent)**. This module will enable you to configure the agent to communicate with your SSPIM instance.

Import the module:



```
C:\> Import-Module "C:\Program Files\WindowsPowerShell\Modules\SSPIMModule\SSPIMAgent.psm1"
C:\> _
```

Run the **`Install-SSPIMAgent`** cmdlet. You can use **`Get-Help Install-SSPIMAgent -examples`** to check out an example of the cmdlet.

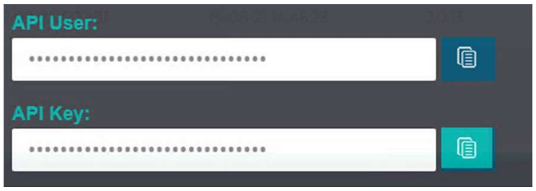


```
C:\> get-help install-sspimagent -Examples

NAME
    Install-SSPIMAgent

SYNOPSIS
    Configures the Self Service PIM Agent.


    ------------------------- EXAMPLE 1 -------------------------

    PS C:\># Configures the agent for the 'wingtiptoys.selfservicepim.com instance.

    Install-SSPIMAgent -SSPIMInstance "wingtiptoys.selfservicepim.com" -DomainName "toys.corp" -APIUser "abcdefg" -APIKey "12345"
```

You will notice that there are a number of required parameters:

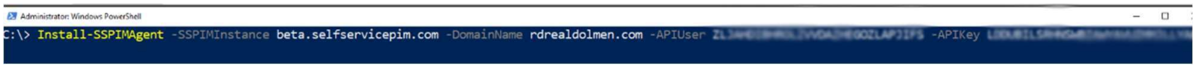
- SSPIMInstance: this is your instance name, for example wingtiptoys.selfservicepim.com
- DomainName: the FQDN of the domain for which the Agent will process requests
- APIUser: the first API key (**can be found in the SSPIM portal**)
- APIKey: the second API key (**can be found in the SSPIM portal**)

API keys can be retrieved from the same dialogue box you downloaded the agent from. Simply use the copy buttons to get the keys in your clipboard.



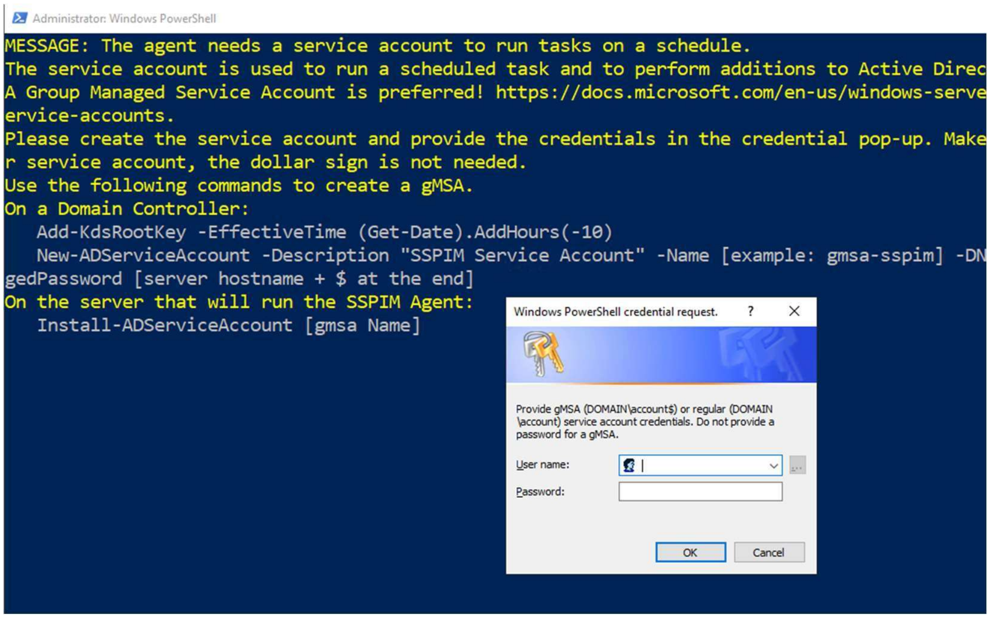
API User: ••••••••••••••••••••••••••••••••

API Key: ••••••••••••••••••••••••••••••••



```
C:\> Install-SSPIMAgent -SSPIMInstance beta.selfservicepim.com -DomainName rdrealdolmen.com -APIUser [redacted] -APIKey [redacted]
```

Entering this command will result in a credential box. This credential is needed to run the SSPIM scheduled task.



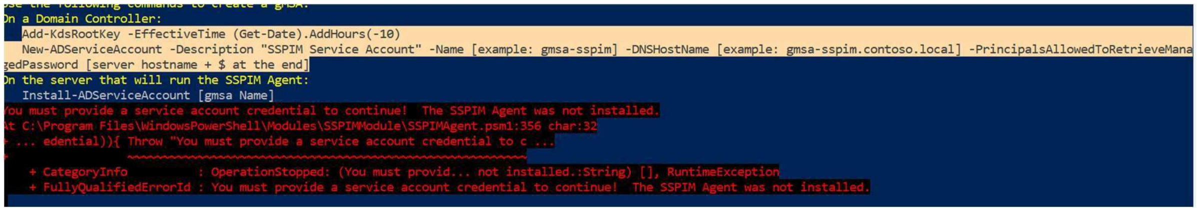
```
MESSAGE: The agent needs a service account to run tasks on a schedule.
The service account is used to run a scheduled task and to perform additions to Active Direc
A Group Managed Service Account is preferred! https://docs.microsoft.com/en-us/windows-serve
ervice-accounts.
Please create the service account and provide the credentials in the credential pop-up. Make
r service account, the dollar sign is not needed.
Use the following commands to create a gMSA.
On a Domain Controller:
   Add-KdsRootKey -EffectiveTime (Get-Date).AddHours(-10)
   New-ADServiceAccount -Description "SSPIM Service Account" -Name [example: gmsa-sspim] -DN
gedPassword [server hostname + $ at the end]
On the server that will run the SSPIM Agent:
   Install-ADServiceAccount [gmsa Name]
```

Provide gMSA (DOMAIN\account$) or regular (DOMAIN \account) service account credentials. Do not provide a password for a gMSA.

User name:

Password:

You can choose to use a GMSA or a regular Service Account. We highly recommend using a Group Managed Service Account. The commands for the creation of a GMSA are shown by the wizard. You can cancel the credential box to halt the cmdlet and then copy and execute the GMSA commands (after modifying them slightly to account for your preferences). Afterwards, execute the install cmdlet again.

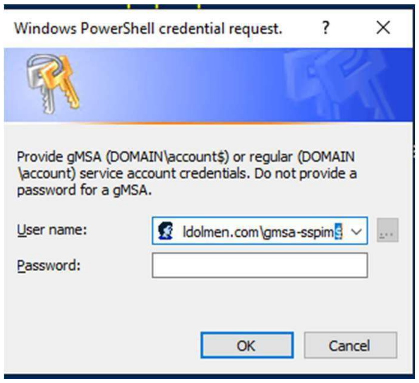


```
On a Domain Controller:
   Add-KdsRootKey -EffectiveTime (Get-Date).AddHours(-10)
   New-ADServiceAccount -Description "SSPIM Service Account" -Name [example: gmsa-sspim] -DNSHostName [example: gmsa-sspim.contoso.local] -PrincipalsAllowedToRetrieveMana
gedPassword [server hostname + $ at the end]
On the server that will run the SSPIM Agent:
   Install-ADServiceAccount [gmsa Name]
You must provide a service account credential to continue!  The SSPIM Agent was not installed.
At C:\Program Files\WindowsPowerShell\Modules\SSPIMModule\SSPIMAgent.psm1:356 char:32
+ ... edential)){ Throw "You must provide a service account credential to c ...
+                 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : OperationStopped: (You must provid... not installed.:String) [], RuntimeException
    + FullyQualifiedErrorId : You must provide a service account credential to continue!  The SSPIM Agent was not installed.
```

Note 1: it might be that there is already a KDS rootkey generated in the domain. If that’s the case, you do not need to create an extra one.

Note 2: you might need to install the AD Powershell cmdlets on the server that will be running the agent. Running `Add-WindowsFeature RSAT-AD-PowerShell` will do the trick.

If you chose a GMSA, make sure to use the correct notation (**dollar sign at the end, no password**):

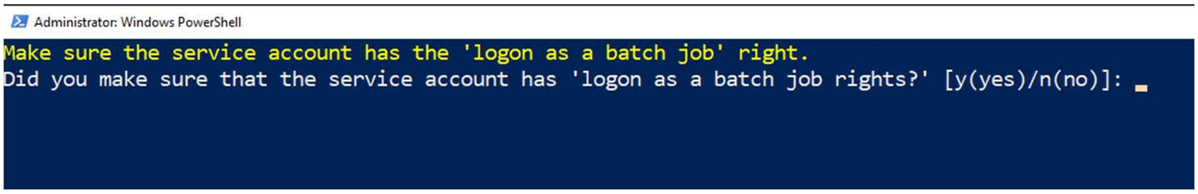


Provide gMSA (DOMAIN\account$) or regular (DOMAIN \account) service account credentials. Do not provide a password for a gMSA.

User name: ldolmen.com\gmsa-sspim$

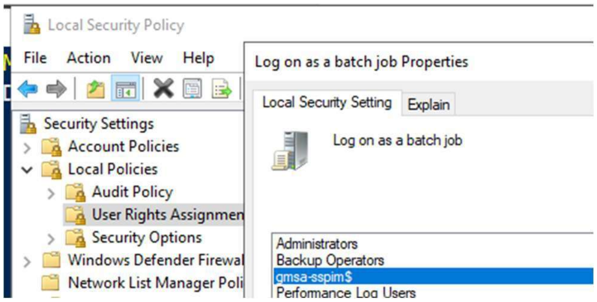
Password:

As explained, the SSPIM agent is executed with the help of a scheduled task. Therefore, the service account needs to be granted **Logon as a batch job** rights. You can grant this privilege while the window below remains open. Type **y** and press enter when you are ready.



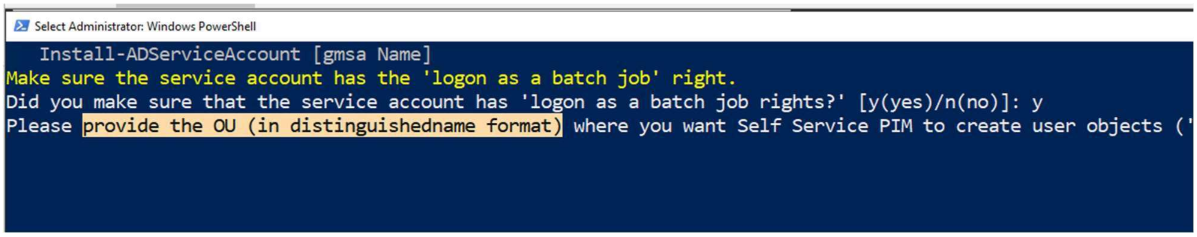
```
Make sure the service account has the 'logon as a batch job' right.
Did you make sure that the service account has 'logon as a batch job rights?' [y(yes)/n(no)]: _
```

Use either Local Security Policy (secpol.msc) or Group Policy Management to configure this. Be sure to perform a gpupdate afterwards.



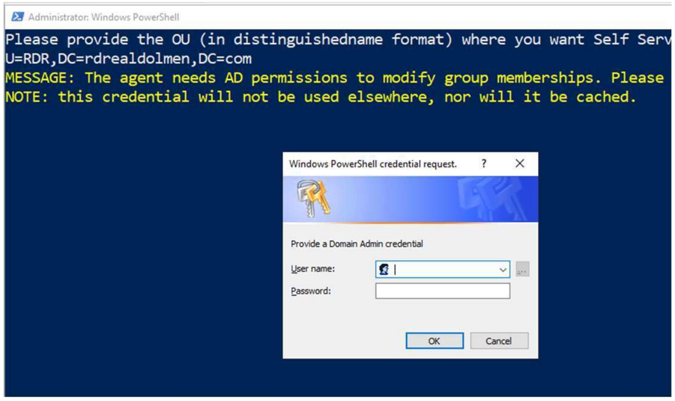
Administrators
Backup Operators
gmsa-sspim$
Performance Log Users

Next you are prompted for an OU in DistinguishedName format. This OU will be the location where SSPIM will create credentials when a privilege is created with the **Credential Generation Escalation Type.** You can create the OU while the window is open and press **y** and enter when ready.



```
   Install-ADServiceAccount [gmsa Name]
Make sure the service account has the 'logon as a batch job' right.
Did you make sure that the service account has 'logon as a batch job rights?' [y(yes)/n(no)]: y
Please provide the OU (in distinguishedname format) where you want Self Service PIM to create user objects ('
```

Lastly, a Domain Admin credential is prompted. **This credential is not cached, and merely used to configure Delegation actions for the service account**. These actions include writing to the member attribute of groups and creating/removing user accounts in the designated SSPIM OU.



Administrator: Windows PowerShell
Windows PowerShell credential request.
?
X
OK
Cancel

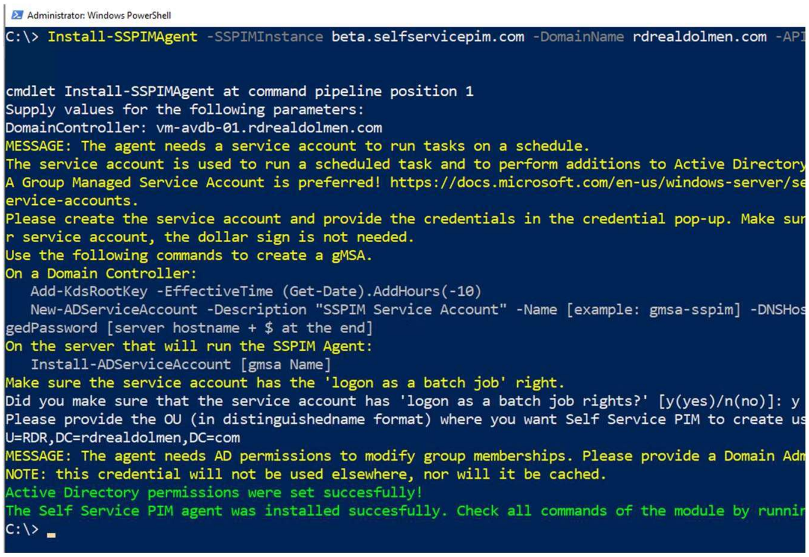
```
Please provide the OU (in distinguishedname format) where you want Self Serv
U=RDR,DC=rdrealdolmen,DC=com
MESSAGE: The agent needs AD permissions to modify group memberships. Please
NOTE: this credential will not be used elsewhere, nor will it be cached.
```

Provide a Domain Admin credential

User name:

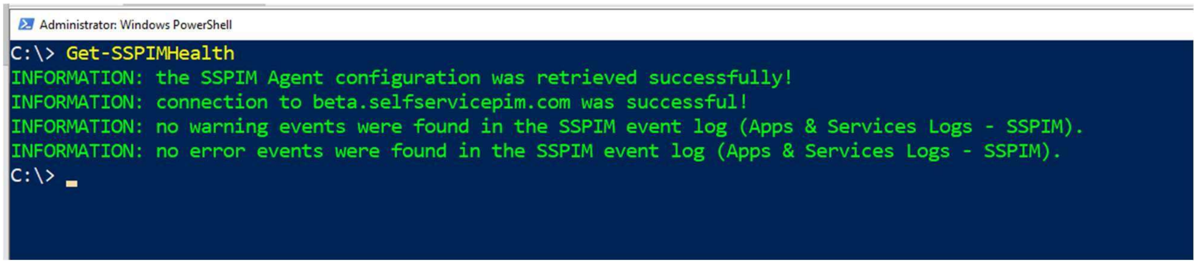
Password:

After supplying the credential, the setup completes.



```
C:\> Install-SSPIMAgent -SSPIMInstance beta.selfservicepim.com -DomainName rdrealdolmen.com -API


cmdlet Install-SSPIMAgent at command pipeline position 1
Supply values for the following parameters:
DomainController: vm-avdb-01.rdrealdolmen.com
MESSAGE: The agent needs a service account to run tasks on a schedule.
The service account is used to run a scheduled task and to perform additions to Active Directory
A Group Managed Service Account is preferred! https://docs.microsoft.com/en-us/windows-server/se
ervice-accounts.
Please create the service account and provide the credentials in the credential pop-up. Make sur
r service account, the dollar sign is not needed.
Use the following commands to create a gMSA.
On a Domain Controller:
   Add-KdsRootKey -EffectiveTime (Get-Date).AddHours(-10)
   New-ADServiceAccount -Description "SSPIM Service Account" -Name [example: gmsa-sspim] -DNSHos
gedPassword [server hostname + $ at the end]
On the server that will run the SSPIM Agent:
   Install-ADServiceAccount [gmsa Name]
Make sure the service account has the 'logon as a batch job' right.
Did you make sure that the service account has 'logon as a batch job rights?' [y(yes)/n(no)]: y
Please provide the OU (in distinguishedname format) where you want Self Service PIM to create us
U=RDR,DC=rdrealdolmen,DC=com
MESSAGE: The agent needs AD permissions to modify group memberships. Please provide a Domain Adm
NOTE: this credential will not be used elsewhere, nor will it be cached.
Active Directory permissions were set succesfully!
The Self Service PIM agent was installed succesfully. Check all commands of the module by runnir
C:\> _
```

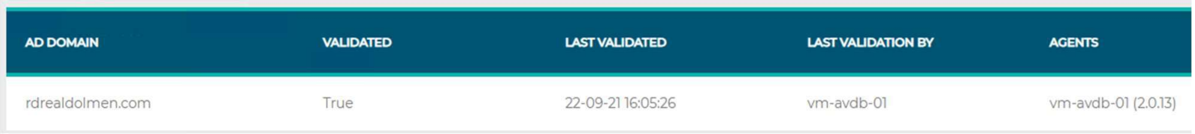
You can perform connectivity tests with the help of the cmdlet **Get-SSPIMHealth**



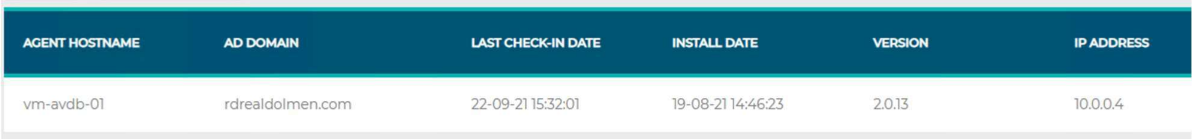
```
C:\> Get-SSPIMHealth
INFORMATION: the SSPIM Agent configuration was retrieved successfully!
INFORMATION: connection to beta.selfservicepim.com was successful!
INFORMATION: no warning events were found in the SSPIM event log (Apps & Services Logs - SSPIM).
INFORMATION: no error events were found in the SSPIM event log (Apps & Services Logs - SSPIM).
C:\> _
```

Make sure that the server running the agent can connect outbound on port 443 towards your SSPIM instance. In case URL filtering is active within your environment, you will need to create an exclusion. If there are errors/warnings concerning the event log, you can navigate to event viewer (eventvwr.msc) and look for the SSPIM log under **Applications and Services Logs**.

On the SSPIM portal, on both the **Control Panel-Domains** and **Control Panel-Agents** page, you will find info of the agent (last check in times, version, install date…) after performing the configuration (can take up to a minute to see this feedback).



AD DOMAIN	VALIDATED	LAST VALIDATED	LAST VALIDATION BY	AGENTS
rdrealdolmen.com	True	22-09-21 16:05:26	vm-avdb-01	vm-avdb-01 (2.0.13)



AGENT HOSTNAME	AD DOMAIN	LAST CHECK-IN DATE	INSTALL DATE	VERSION	IP ADDRESS
vm-avdb-01	rdrealdolmen.com	22-09-21 15:32:01	19-08-21 14:46:23	2.0.13	10.0.0.4

SSPIM agent configuration can be altered at any time either by re-running the **Install-SSPIMAgent** cmdlet or by running **Set-SSPIMConfiguration** to set a single parameter. You can use the Get-Help method to get information about parameters and to see examples.

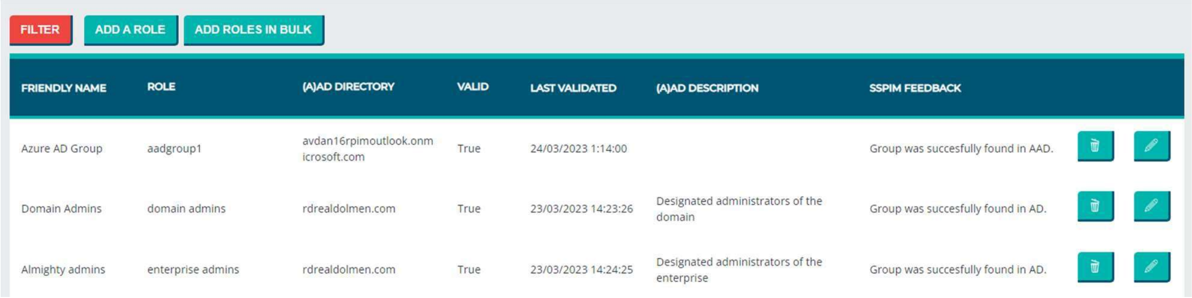
D. (Optional/Recommended) install an extra agent

For redundancy purposes, you might want to install a second or even a third agent. The procedure you would follow would be mostly identical to what is described in 2.3.C. However, consider these changes:

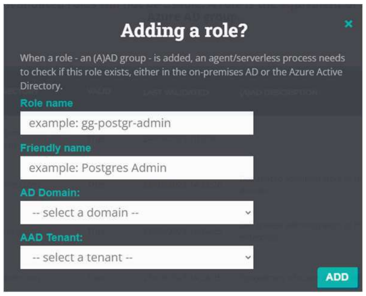
- You do not need to create another service account; you can simply reuse the account you configured for the first SSPIM server
- When using a GMSA, you will need to make sure that the extra server(s) that will host the agent, also has access to the GMSA password. You would therefore need to run the following command to make sure that all agents can retrieve that password: `Set-ADServiceAccount gmsa-sspim -PrincipalsAllowedToRetrieveManagedPassword server1$,server2$,server3`

E. Configure Entra ID / Active Directory Groups

SSPIM will provide membership to Entra/AD groups to grant privileges. Therefore, you need to define these groups. This can be performed using the **Groups** page under **Control Panel >> Groups.**



FRIENDLY NAME	ROLE	(A)AD DIRECTORY	VALID	LAST VALIDATED	(A)AD DESCRIPTION	SSPIM FEEDBACK
Azure AD Group	aadgroup1	avdan16rpimoutlook.onmicrosoft.com	True	24/03/2023 1:14:00		Group was succesfully found in AAD.
Domain Admins	domain admins	rdrealdolmen.com	True	23/03/2023 14:23:26	Designated administrators of the domain	Group was succesfully found in AD.
Almighty admins	enterprise admins	rdrealdolmen.com	True	23/03/2023 14:24:25	Designated administrators of the enterprise	Group was succesfully found in AD.



Adding a role?

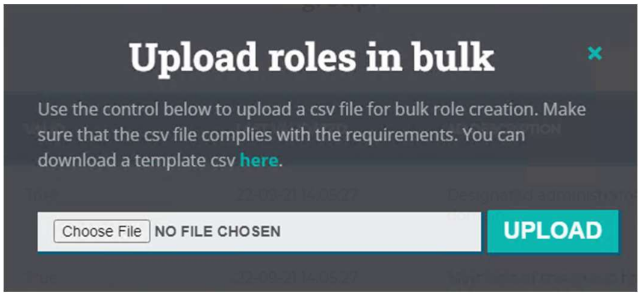
When a role - an (A)AD group - is added, an agent/serverless process needs to check if this role exists, either in the on-premises AD or the Azure Active Directory.

Role name: example: gg-postgr-admin

Friendly name: example: Postgres Admin

AD Domain: -- select a domain --

AAD Tenant: -- select a tenant --



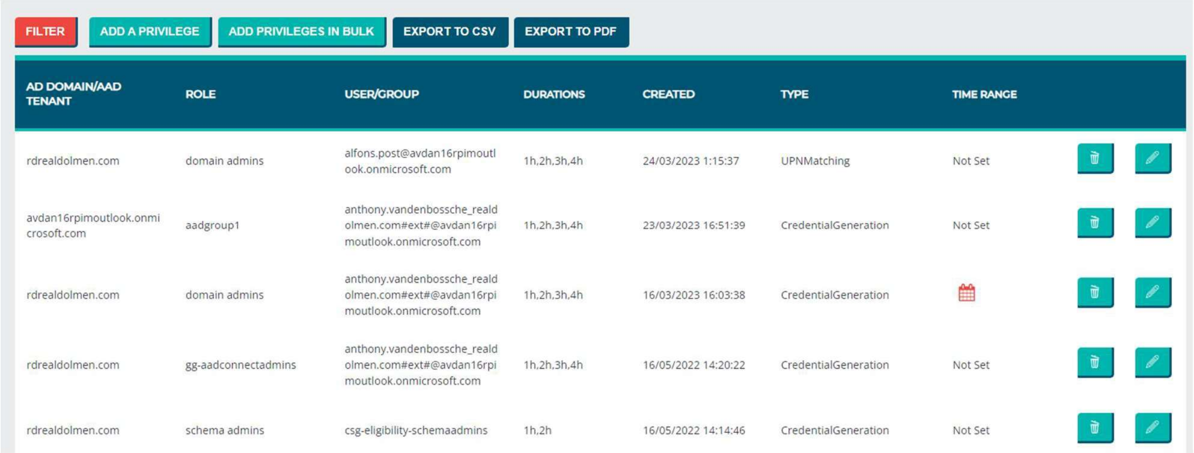
Upload roles in bulk

Use the control below to upload a csv file for bulk role creation. Make sure that the csv file complies with the requirements. You can download a template csv here.

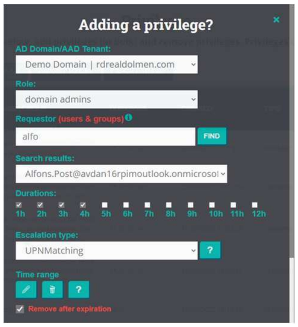
Groups can easily be added (in bulk) or removed. Before we can tie a privilege to this group, an SSPIM agent (or the serverless process in case of a tenant) needs to validate the group and make sure it exists in the directory. Once this validation occurs (every 1 minute), this group can be used to create privileges.

F. Configure Privileges

Once groups are validated, you can create privileges for them. Use the **Privileges** page for this purpose. **Control Panel >> Privileges.**



AD DOMAIN/AAD TENANT	ROLE	USER/GROUP	DURATIONS	CREATED	TYPE	TIME RANGE
rdrealdolmen.com	domain admins	alfons.post@avdan16rpimoutlook.onmicrosoft.com	1h,2h,3h,4h	24/03/2023 1:15:37	UPNMatching	Not Set
avdan16rpimoutlook.onmicrosoft.com	aadgroup1	anthony.vandenbossche_realdolmen.com#ext#@avdan16rpimoutlook.onmicrosoft.com	1h,2h,3h,4h	23/03/2023 16:51:39	CredentialGeneration	Not Set
rdrealdolmen.com	domain admins	anthony.vandenbossche_realdolmen.com#ext#@avdan16rpimoutlook.onmicrosoft.com	1h,2h,3h,4h	16/03/2023 16:03:38	CredentialGeneration	📅
rdrealdolmen.com	gg-aadconnectadmins	anthony.vandenbossche_realdolmen.com#ext#@avdan16rpimoutlook.onmicrosoft.com	1h,2h,3h,4h	16/05/2022 14:20:22	CredentialGeneration	Not Set
rdrealdolmen.com	schema admins	csg-eligibility-schemaadmins	1h,2h	16/05/2022 14:14:46	CredentialGeneration	Not Set



Adding a privilege?

AD Domain/AAD Tenant: Demo Domain | rdrealdolmen.com

Role: domain admins

Requestor (users & groups): alfo

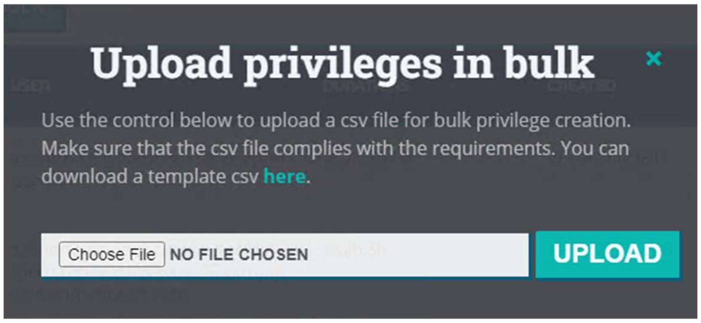
Search results: Alfons.Post@avdan16rpimoutlook.onmicrosol

Durations: ☑ 1h ☑ 2h ☑ 3h ☑ 4h □ 5h □ 6h □ 7h □ 8h □ 9h □ 10h □ 11h □ 12h

Escalation type: UPNMatching

Time range

☑ Remove after expiration



Upload privileges in bulk

Use the control below to upload a csv file for bulk privilege creation. Make sure that the csv file complies with the requirements. You can download a template csv here.

Privileges can be added one by one, or in bulk. You can download a template CSV for the bulk operation.

INFORMATIONAL

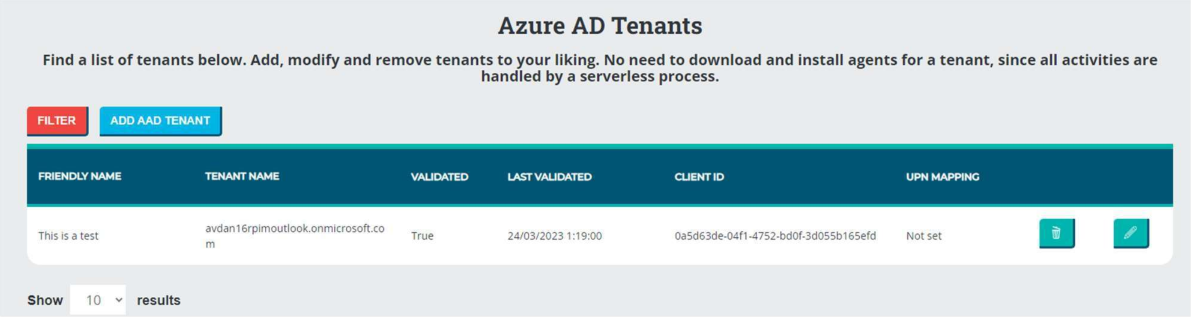
There are 4 Escalation Types:

- **UPN Matching**: with UPN Matching, Self Service PIM (agents) will look the exact same UPN in the Active Directory Domain. This is useful if you are syncing the user accounts of Self-Service PIM users towards Entra ID, with a routable UPN that is added as a verified domain on your tenant. If you have a mismatch of the UPN between the UPN in AD and Entra ID, you could always adjust the AD UPN to the desired value to ensure matching.
- **Credential Generation:** with Credential Generation, Self Service PIM (agents) will create a randomly generated credential in Active Directory. Self Service PIM will automatically purge this credential after the allotted escalation time. The credential itself will be shown as a detail of the escalation on the Revoke page, where your active escalations are listed.
- **UPN Mapping:** SSPIM will be allowed to leverage regular expression logic, to transform the UPN of the authenticated user to any desired format. This is particularly useful when you have discrepancies in UPNs. You will need to define the logic, according to your situation, with the help of the expression builder.
- **CredentialSharing:** When Credential Sharing is selected, Self Service PIM (agents) will lookup the specified UPN in Active Directory/Entra ID. This is useful when you have a group of people that need to share the same credential. Even though this is not the most secure option, it is helpful in situations where backend configuration (authorization mostly) is too extensive. Similar to UPNMatching, SSPIM will only assign/unassign privileges, and will not manipulate password and account state.

G. Create an Entra ID Tenant

Very similar to creating an Active Directory Domain, we can create an Entra ID Tenant. SSPIM will then be able to elevate privileges, directly on the tenant! An App Registration will need to be created in the tenant(s) you wish to manage.

Navigate to **Control Panel >> Tenants.**



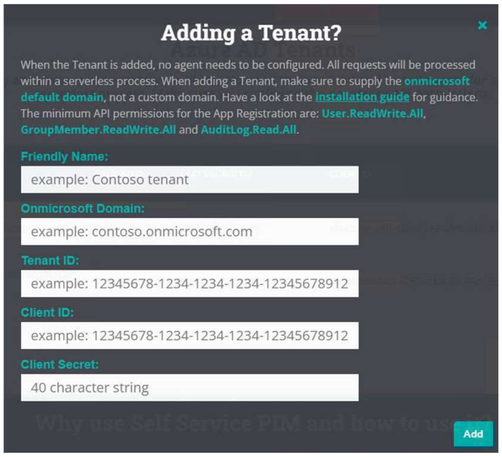
Azure AD Tenants

Find a list of tenants below. Add, modify and remove tenants to your liking. No need to download and install agents for a tenant, since all activities are handled by a serverless process.

FRIENDLY NAME	TENANT NAME	VALIDATED	LAST VALIDATED	CLIENT ID	UPN MAPPING
This is a test	avdan16rpimoutlook.onmicrosoft.com	True	24/03/2023 1:19:00	0a5d63de-04f1-4752-bd0f-3d055b165efd	Not set

Show 10 results

Click the **Add Entra ID Tenant** button.



Adding a Tenant?

When the Tenant is added, no agent needs to be configured. All requests will be processed within a serverless process. When adding a Tenant, make sure to supply the onmicrosoft default domain, not a custom domain. Have a look at the installation guide for guidance. The minimum API permissions for the App Registration are: User.ReadWrite.All, GroupMember.ReadWrite.All and AuditLog.Read.All.

Friendly Name: example: Contoso tenant

Onmicrosoft Domain: example: contoso.onmicrosoft.com

Tenant ID: example: 12345678-1234-1234-1234-12345678912

Client ID: example: 12345678-1234-1234-1234-12345678912

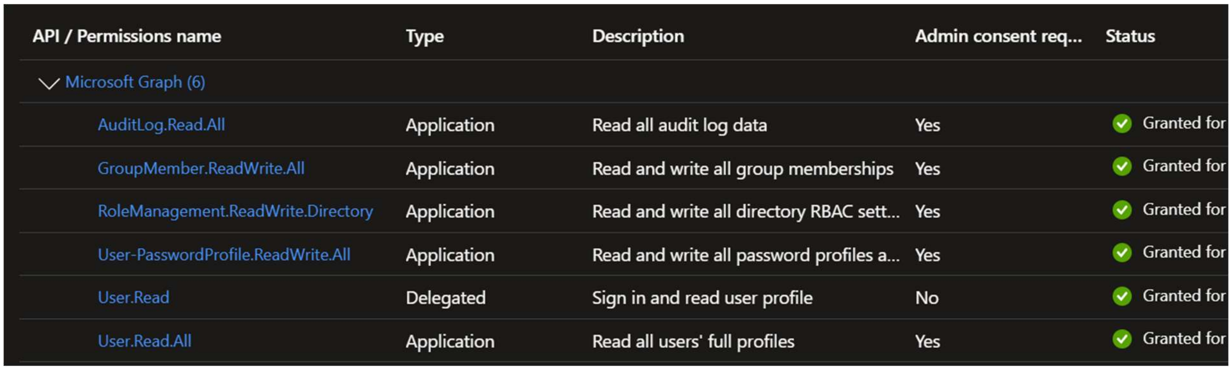
Client Secret: 40 character string

You will need to provide at least: the **Tenant ID, the Client ID, a Client Secret and the default (onmicrosoft) domain.** Click the **Add** button. This will result in the addition of the tenant, as long as the connection test to the tenant succeeds.

Creating an App Registration is already explained in the **2.2.A** section of the initial configuration (the App mentioned in that section is merely created for the Authentication and Authorization part of SSPIM). It is advised to create a separate App Registration for tenant management. This App Registration needs following API permissions:

API	Type	Permission Name	Function
Microsoft Graph	Application	User.ReadWrite.All	Needed to allow SSPIM to create user accounts in case of Credential Generation.
Microsoft Graph	Application	GroupMember.ReadWrite.All	Needed to allow SSPIM to add users to Entra ID Groups.

Microsoft Graph	Application	AuditLog.Read.All	Needed to allow SSPIM to check up on sign-in activity on generated credentials. Credential Lifecycle is a feature that will automatically remove stale accounts.
Microsoft Graph	Application	RoleManagement.ReadWrite.Directory	Needed to add users to groups that have Entra ID Roles assigned (like for example Global Administrator and User Administrator).
Microsoft Graph	Application	User-PasswordProfile.ReadWrite.All	Needed to reset passwords of generated tenant credentials.

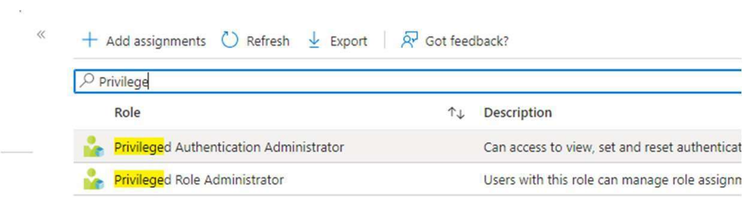


API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (6)				
AuditLog.Read.All	Application	Read all audit log data	Yes	✓ Granted for
GroupMember.ReadWrite.All	Application	Read and write all group memberships	Yes	✓ Granted for
RoleManagement.ReadWrite.Directory	Application	Read and write all directory RBAC sett...	Yes	✓ Granted for
User-PasswordProfile.ReadWrite.All	Application	Read and write all password profiles a...	Yes	✓ Granted for
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for

In order for SSPIM to manipulate users that have a privileged role assigned (or recently had a privilege role assigned), we need to add this app registration to the **Privileged Authentication Administrator** role.

Navigate to **Privileged Identity Management (under Identity Governance) >> Entra ID Roles >> Assign eligibility**

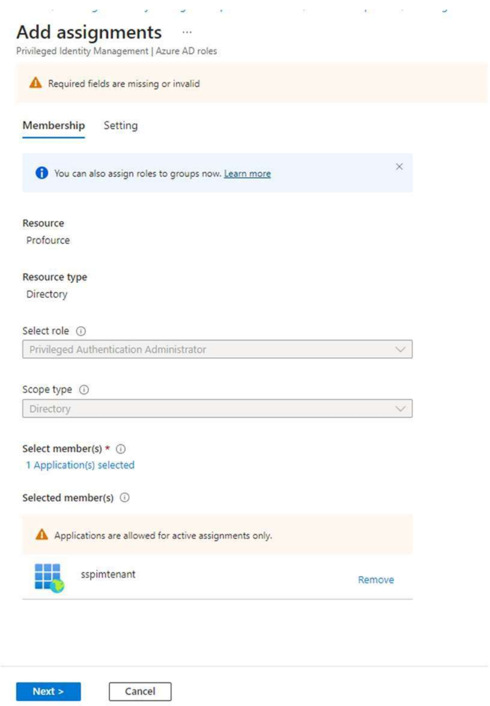
Select the Privileged Authentication Administrator role.



Privilege

Role	Description
Privileged Authentication Administrator	Can access to view, set and reset authenticat
Privileged Role Administrator	Users with this role can manage role assignn

Click **Add assignments** and select app registration.



Add assignments ...

Privileged Identity Management | Azure AD roles

⚠ Required fields are missing or invalid

Membership Setting

ⓘ You can also assign roles to groups now. Learn more ×

Resource
Profource

Resource type
Directory

Select role ⓘ
Privileged Authentication Administrator

Scope type ⓘ
Directory

Select member(s) * ⓘ
1 Application(s) selected

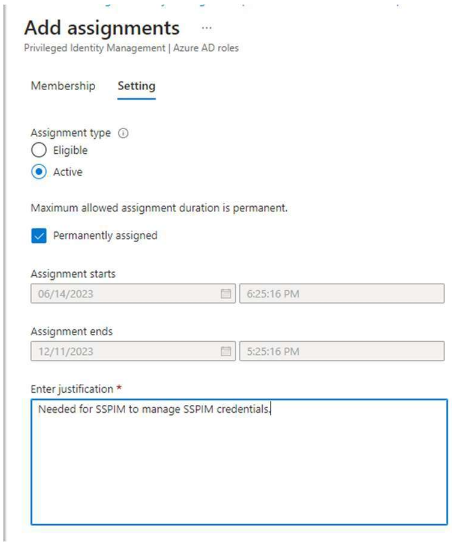
Selected member(s) ⓘ

⚠ Applications are allowed for active assignments only.

sspimtenant Remove

Next > Cancel

Make sure to provide a proper justification and click **Assign.**



Add assignments ...

Privileged Identity Management | Azure AD roles

Membership Setting

Assignment type ⓘ
○ Eligible
● Active

Maximum allowed assignment duration is permanent.

☑ Permanently assigned

Assignment starts
06/14/2023 6:25:16 PM

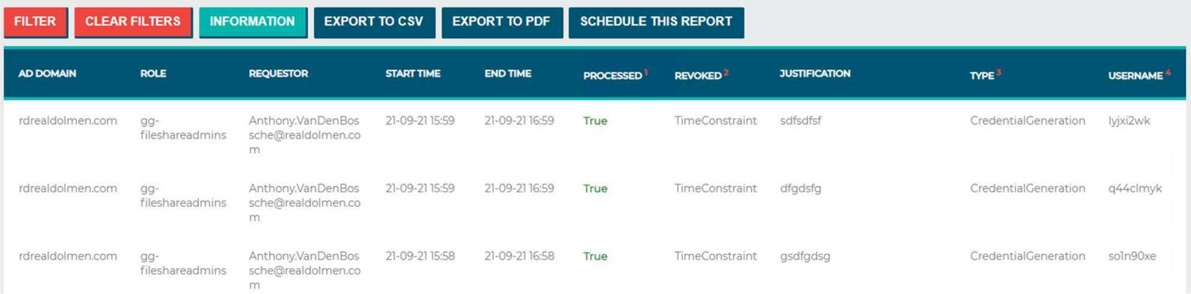
Assignment ends
12/11/2023 5:25:16 PM

Enter justification *
Needed for SSPIM to manage SSPIM credentials.

After the tenant is added, you can go ahead and add groups and privileges for that tenant. After groups were added, it takes up to 1 minute for groups to get validated.

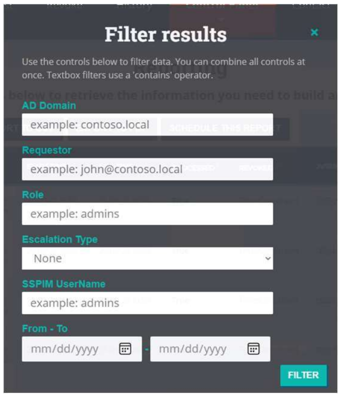
H. Report on escalations

SSPIM administrators can retrieve reports on past and current escalations using the **Reporting** page. **Control Panel >> Reporting.**



AD DOMAIN	ROLE	REQUESTOR	START TIME	END TIME	PROCESSED [1]	REVOKED [2]	JUSTIFICATION	TYPE [3]	USERNAME [4]
rdrealdolmen.com	gg-fileshareadmins	Anthony.VanDenBossche@realdolmen.com	21-09-21 15:59	21-09-21 16:59	True	TimeConstraint	sdfsdfsf	CredentialGeneration	lyjxi2wk
rdrealdolmen.com	gg-fileshareadmins	Anthony.VanDenBossche@realdolmen.com	21-09-21 15:59	21-09-21 16:59	True	TimeConstraint	dfgdsfg	CredentialGeneration	q44clmyk
rdrealdolmen.com	gg-fileshareadmins	Anthony.VanDenBossche@realdolmen.com	21-09-21 15:58	21-09-21 16:58	True	TimeConstraint	gsdfgdsg	CredentialGeneration	so1n90xe

Admins can filter the reports to their liking, export them to CSV or PDF and even schedule them (daily, weekly, monthly, quarterly, yearly).



Filter results

Use the controls below to filter data. You can combine all controls at once. Textbox filters use a 'contains' operator.

AD Domain: example: contoso.local

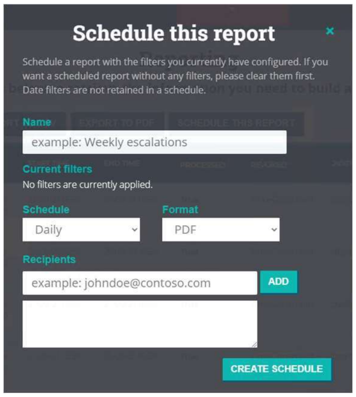
Requestor: example: john@contoso.local

Role: example: admins

Escalation Type: None

SSPIM UserName: example: admins

From - To: mm/dd/yyyy - mm/dd/yyyy



Schedule this report

Schedule a report with the filters you currently have configured. If you want a scheduled report without any filters, please clear them first. Date filters are not retained in a schedule.

Name: example: Weekly escalations

Current filters

No filters are currently applied.

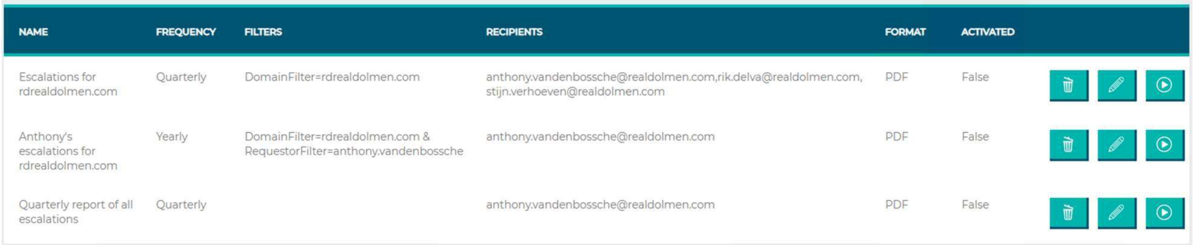
Schedule: Daily

Format: PDF

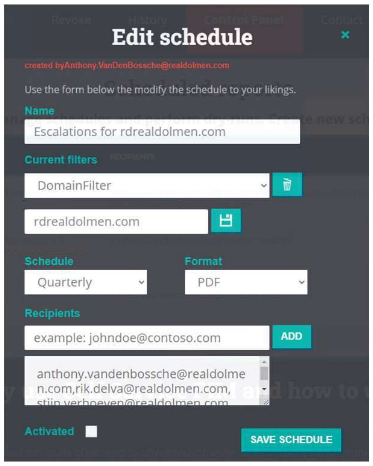
Recipients: example: johndoe@contoso.com

I. Manage and dry-run schedules

Using the **Schedules** page, **Control Panel >> Schedules**, an admin can adjust schedules created from the reporting section and even dry-run them.



NAME	FREQUENCY	FILTERS	RECIPIENTS	FORMAT	ACTIVATED	
Escalations for rdrealdolmen.com	Quarterly	DomainFilter=rdrealdolmen.com	anthony.vandenbossche@realdolmen.com,rik.delva@realdolmen.com, stijn.verhoeven@realdolmen.com	PDF	False	🗑 ✎ ▶
Anthony's escalations for rdrealdolmen.com	Yearly	DomainFilter=rdrealdolmen.com & RequestorFilter=anthony.vandenbossche	anthony.vandenbossche@realdolmen.com	PDF	False	🗑 ✎ ▶
Quarterly report of all escalations	Quarterly		anthony.vandenbossche@realdolmen.com	PDF	False	🗑 ✎ ▶



Edit schedule

created byAnthony.VanDenBossche@realdolmen.com

Use the form below the modify the schedule to your likings.

Name: Escalations for rdrealdolmen.com

Current filters: DomainFilter

rdrealdolmen.com

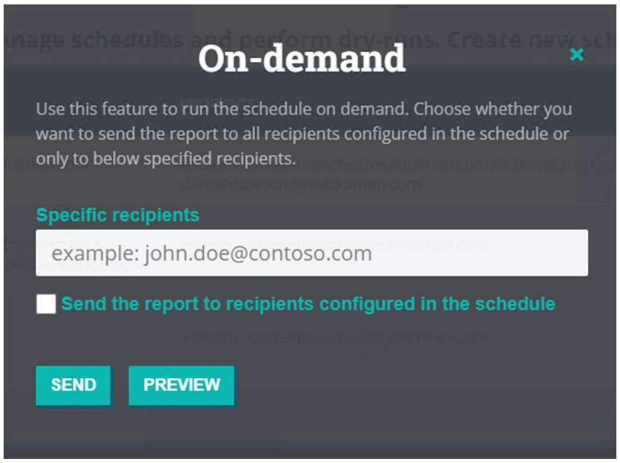
Schedule: Quarterly

Format: PDF

Recipients: example: johndoe@contoso.com

anthony.vandenbossche@realdolmen.com,rik.delva@realdolmen.com, stiin.verhoeven@realdolmen.com

Activated □



On-demand

Use this feature to run the schedule on demand. Choose whether you want to send the report to all recipients configured in the schedule or only to below specified recipients.

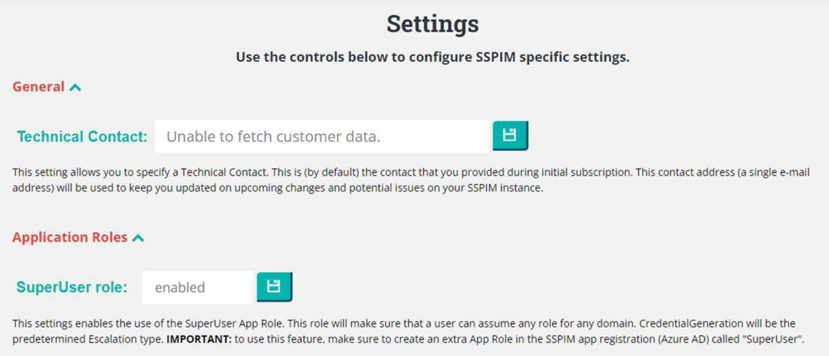
Specific recipients: example: john.doe@contoso.com

□ Send the report to recipients configured in the schedule

J. Adjust SSPIM settings

Under the Control Panel, you will find a **Settings** section. Here, you can manage a variety of settings, including:

- The SuperUser application role.
- Credential reusage
- Password and UserName length
- Naming Convention



Settings

Use the controls below to configure SSPIM specific settings.

General

Technical Contact: Unable to fetch customer data.

This setting allows you to specify a Technical Contact. This is (by default) the contact that you provided during initial subscription. This contact address (a single e-mail address) will be used to keep you updated on upcoming changes and potential issues on your SSPIM instance.

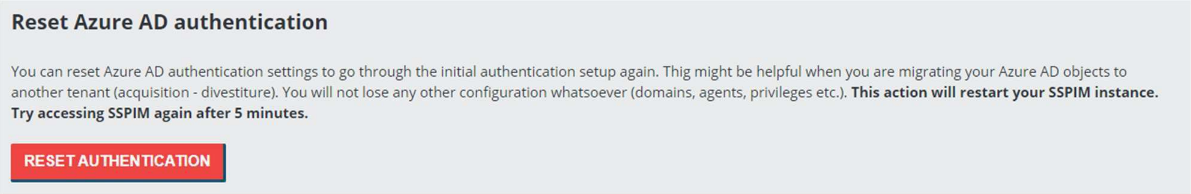
Application Roles

SuperUser role: enabled

This settings enables the use of the SuperUser App Role. This role will make sure that a user can assume any role for any domain. CredentialGeneration will be the predetermined Escalation type. **IMPORTANT:** to use this feature, make sure to create an extra App Role in the SSPIM app registration (Azure AD) called "SuperUser".

K. Adjust Entra ID authentication

It might occur that you are changing to a different Entra ID tenant. In that case, you can clear the AuthN configuration and perform it anew. All other configuration will be retained. **Control Panel >> Entra ID Authentication – Reset Entra ID Authentication**



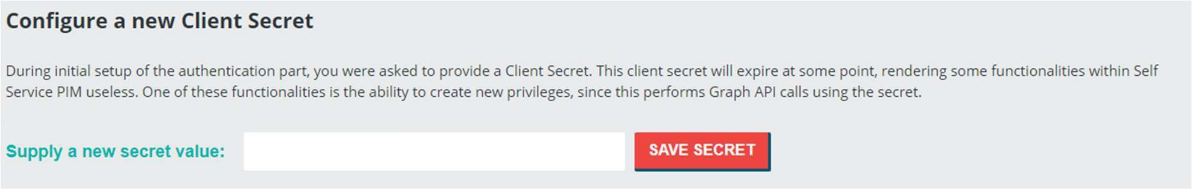
Reset Azure AD authentication

You can reset Azure AD authentication settings to go through the initial authentication setup again. Thig might be helpful when you are migrating your Azure AD objects to another tenant (acquisition - divestiture). You will not lose any other configuration whatsoever (domains, agents, privileges etc.). **This action will restart your SSPIM instance. Try accessing SSPIM again after 5 minutes.**

IMPORTANT: after the clearance, it will take up to 5 minutes for SSPIM to become available again.

L. Renew Client Secret for Graph API Calls

Client Secret for App Registrations inherently expire at some point in time. You will need to renew the secret as described in **2.2.D** and provide that new secret to SSPIM. **Control Panel >> Entra ID Authentication >> Configure a new Client Secret**



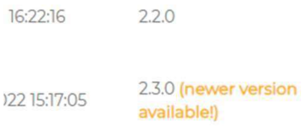
Configure a new Client Secret

During initial setup of the authentication part, you were asked to provide a Client Secret. This client secret will expire at some point, rendering some functionalities within Self Service PIM useless. One of these functionalities is the ability to create new privileges, since this performs Graph API calls using the secret.

3. Upgrade SSPIM Agent

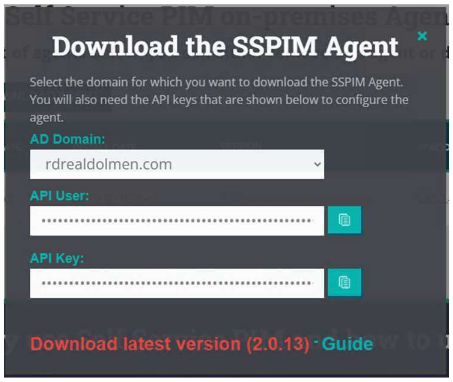
The Self Service PIM agent is not self-updating at this time. Therefore, a customer needs to apply an update manually. This will not occur often however.

On the agents page, you will notice whether there is a new version available:



16:22:16	2.2.0
)22 15:17:05	2.3.0 (newer version available!)

You can download the newest version of the agent by clicking the Download Agent button.



Download the SSPIM Agent

Select the domain for which you want to download the SSPIM Agent. You will also need the API keys that are shown below to configure the agent.

AD Domain: rdrealdolmen.com

API User: ••

API Key: ••

After performing the download, you can then uninstall the previous version and install the new version.

It is recommended to run the `Install-SSPIMAgent` cmdlet after the installation. This makes sure that, when there were changes to for example the Powershell module, these changes are applied as well. This step is not obligatory since configuration parameters are all retained.