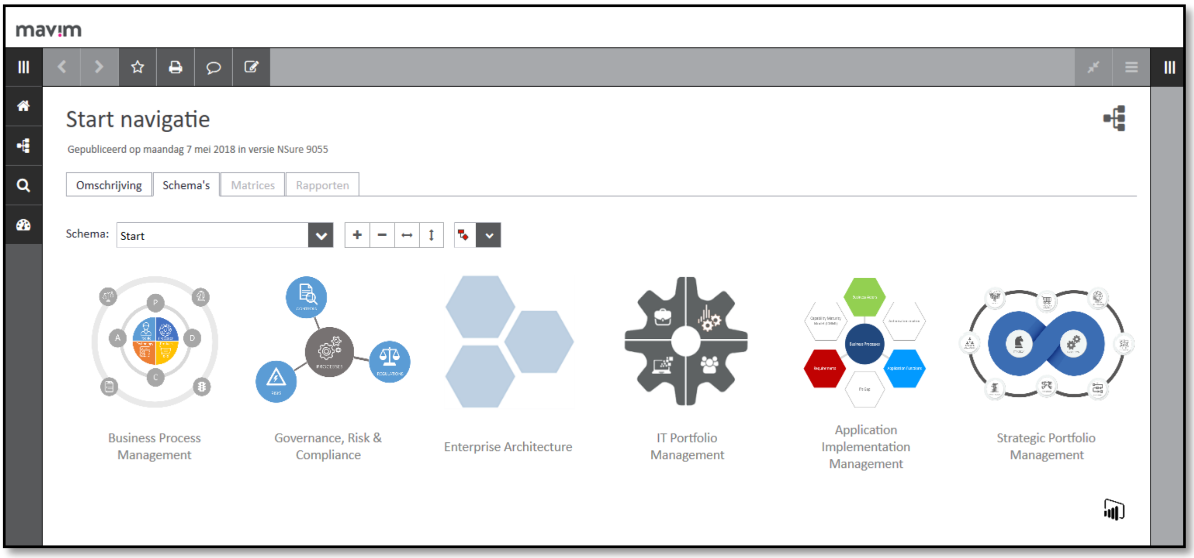
MAVIM PORTAL CONNECT

VERSION : Version 2.2
DATE : 08.12.2020

TABLE OF CONTENTS

1 INTRODUCTION

This document describes the methods of using the Mavim Portal within your organization. The Mavim Portal is a single tenant web app that is hosted in Microsoft Azure. It makes use of Azure active directory or an identity provider such as ADFS to create a connection.



Start navigatie

Gepubliceerd op maandag 7 mei 2018 in versie NSure 9055

Schema: Start

mavim
Omschrijving
Schema's
Matrices
Rapporten
Business Process Management
Governance, Risk & Compliance
Enterprise Architecture
IT Portfolio Management
Application Implementation Management
Strategic Portfolio Management

2 SUPPORTED CONFIGURATIONS

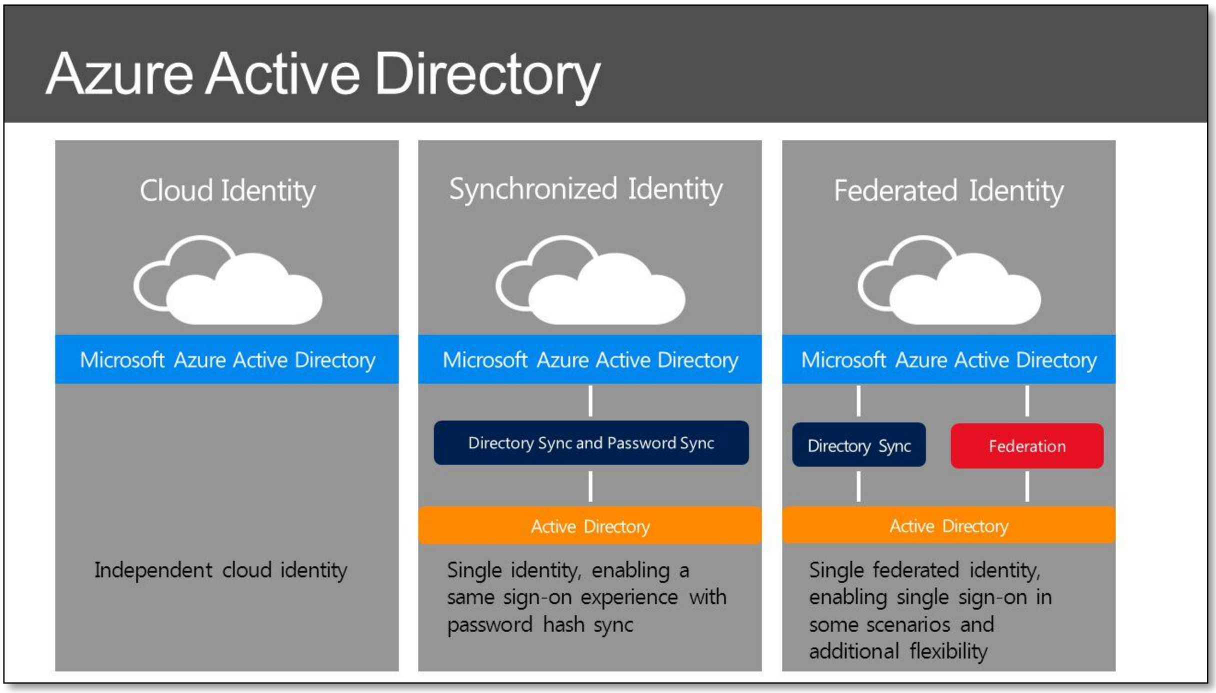
This chapter describes the configuration for connecting to the Mavim Portal.

2.1 AZURE ACTIVE DIRECTORY

In order to register the Mavim Portal as an enterprise application within Azure active directory, an Azure active directory is needed. If your organization does not have access to an Azure active directory, the included Azure active directory can be used with the Mavim Portal.

If you are already making use of Microsoft cloud services such as Microsoft Office 365 or Microsoft Azure, you already have access to an Azure active directory.

In Azure active directory, hereafter Azure AD, various identities are possible, namely **Cloud ID**, **Synchronized ID** and **Federated ID**.


Azure Active Directory
Cloud Identity
Microsoft Azure Active Directory
Independent cloud identity
Synchronized Identity
Microsoft Azure Active Directory
Directory Sync and Password Sync
Active Directory
Single identity, enabling a same sign-on experience with password hash sync
Federated Identity
Microsoft Azure Active Directory
Directory Sync
Federation
Active Directory
Single federated identity, enabling single sign-on in some scenarios and additional flexibility

2.2 CLOUD ID

The cloud identity only exists in Azure AD and does not have any connections with an on premise directory such as active directory. The Mavim Portal is registered as an enterprise application in Azure AD. The user can login to the Mavim Portal using their cloud identity. These accounts for the Mavim Portal are managed from the (included) Azure AD. There is no seamless single sign-on available.

Requirements:

- Customer
  - There are no requirements for the on premise customer infrastructure
- Azure AD
  - If the customer already makes use of an Azure AD, an app registration must be created. If the customer does not yet have an Azure AD, one can be supplied in which the app registration has already been created. Only the (cloud) identities need to be created in Azure AD to allow the users to log in to the Mavim Portal.

2.3 SYNCHRONIZED ID

A synchronized ID is created when accounts from an on premise active directory are synchronized to Azure AD. This synchronization is achieved through Azure AD Connect which is installed in the same environment as the on premise active directory. The selected user accounts and password hashes are synchronized.

This gives access to seamless single sign-on.
The Azure AD Connect tool can be downloaded for free via Microsoft. The tool offers a wizard to bring about the synchronization of on premise active directory and Azure AD.

Requirements:

- Customer
  - Configuration active directory
  - Server with Azure AD Connect
- Azure AD
  - If the customer already has an Azure AD, an app registration must be made. If the customer does not yet have Azure AD, one can be supplied in which the app registration has already been created.
    Azure AD Connect must be configured so that identities can be synchronized to Azure AD and allow logging in to the Mavim Portal.

2.4 FEDERATED ID

For a federated ID, the domain of the synchronized identities in Azure AD are converted to be federated. This makes single sign-on possible.
Next to the use of Azure AD Connect, an Active Directory Federation Services (ADFS) is also needed.

Requirements:

- Customer
  - Configuration Active Directory
  - Server with Azure AD Connect
  - Server with ADFS
  - A Web Application Proxy server to unlock ADFS
- Azure AD
  - If the customer already has an Azure AD, an app registration must be made. If the customer does not yet have Azure AD, one can be supplied in which the app registration has already been created.
    Azure AD Connect must be configured so that identities can be synchronized to Azure AD and allow logging in to the Mavim Portal.
  - The updated domain in Azure AD must be converted to be federated.

When users are logged in to their computers which are members of the on premise active directory domain, logging in to the Mavim Portal will no longer be necessary.
Completely seamless single sign-on is achieved through this configuration.

2.5 PROTOCOLS AND IDENTITY PROVIDERS

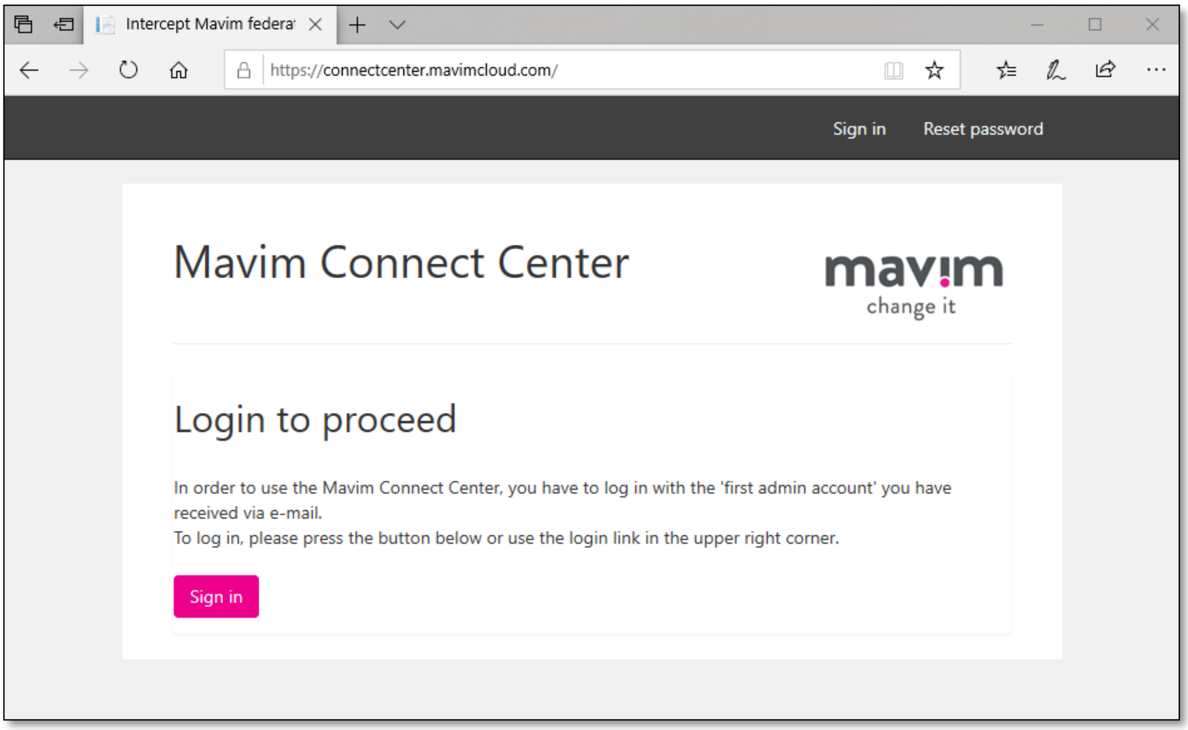
Other supported protocols and identity providers:

- ADFS
- OKTA
- SimpleSAML
- HelloID

More information: Custom work

3 MAVIM CONNECT CENTER

The **Mavim Connect Center** (MCC) has been developed to simplify connecting to the Mavim Portal. Using a wizard, this website automatically configures the correct settings so that the Portal is made suitable for seamless single sign-on. Of course you are still responsible for changes to your browser (e.g. add domain to a certain zone).
The MCC is available for our Mavim Online customers.



Mavim Connect Center

Login to proceed

In order to use the Mavim Connect Center, you have to log in with the 'first admin account' you have received via e-mail.
To log in, please press the button below or use the login link in the upper right corner.

The **Mavim Connect Center** supports the following configurations out of the box:

- Included Azure AD with cloud identities (**Option1**)
- App registration in customer's Azure AD (**Option 2**)
  Choose '*Federate with Azure AD automatically*' for the fastest and easiest configuration!
- OKTA in combination with OpenID Connect (**Option 3**)
- ADFS via MetaData endpoint (**Option 9**)

Note: Log in to the **Mavim Connect Center** with your *First Admin* account for more information.
Click the exclamation mark on the right for the appropriate federation option.

4 CUSTOM WORK

If the customer configuration does not allow the use of the **MCC** and the automatic creation of a single sign-on environment, custom work can be done to achieve this. The identity providers and protocols mentioned in this chapter have already been successfully implemented on several customer sites.

4.1 ADFS

The Mavim Portal web app supports ADFS as an identity provider. When an identity provider such as ADFS is used, an Azure AD is not needed. The relying party trust in ADFS can be created manually. But the use of a meta-data URL is also supported. In combination with ADFS, the Mavim Portal makes use of the SAML protocol.

The Mavim Portal web app in combination with ADFS makes use of the following claims:

- http://schemas.microsoft.com/identity/claims/displayname
- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier
- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn

4.2 OKTA

The Mavim Portal web app supports OKTA as an identity provider. OKTA can make use of the SAML protocol (custom work) or Open ID Connect (MCC).

4.3 SIMPLE SAML

The Mavim Portal web app supports Simple SAML as an identity provider. Simple SAML makes use of the SAML protocol.

- The Mavim Portal web app in combination with Simple SAML makes use of the following claims:

    - http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn

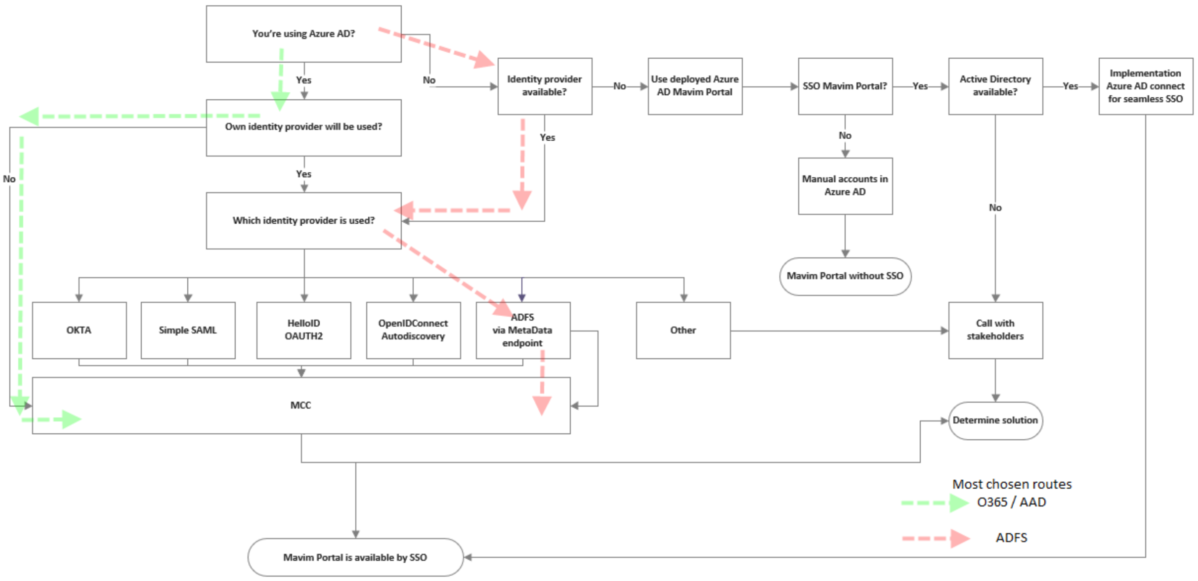
4.4 HELLO ID

The Mavim Portal web app supports HelloID as an identity provider. HelloID uses the OpenID Connect protocol.

- The Mavim Portal web app in combination with Hello ID makes use of the following claims:
    - Display name
    - Email
    - Given name
    - Identifier
    - Name
    - Surname
    - UPN

4.5 CHECKLIST

The following checklist may be used to help customers decide the best option for them.



You're using Azure AD?
Yes
No
Own identity provider will be used?
No
Yes
Which identity provider is used?
Identity provider available?
Yes
No
Use deployed Azure AD Mavim Portal
SSO Mavim Portal?
Yes
No
Manual accounts in Azure AD
Mavim Portal without SSO
Active Directory available?
Yes
No
Implementation Azure AD connect for seamless SSO
OKTA
Simple SAML
HelloID OAUTH2
OpenIDConnect Autodiscovery
ADFS via MetaData endpoint
Other
Call with stakeholders
Determine solution
MCC
Mavim Portal is available by SSO
Most chosen routes
O365 / AAD
ADFS