ahead

Factsheet – ahead User Management

This factsheet provides a comprehensive exploration of the various scenarios in which users obtain access to ahead via Microsoft Entra ID (formerly Azure Active Directory (AAD)) for authentication and authorization.

Author: Pascal Grossniklaus
Contact: pascal@aheadintranet.com

Version: 1.1
Date: 01.12.2023

ahead

Table of Contents

Overview

ahead Intranet is an intranet/employee app platform running on Microsoft Azure to simplify internal communication, find information across the organization, engage employees, and integrate information from 3rd party systems.

This document describes the scenarios of user management within ahead Intranet. It outlines the processes for granting access (authentication) and managing user permissions (authorization) when integrated with Microsoft Entra ID[1] (formerly Azure Active Directory (AAD)). The overview graph below illustrates the ahead system architecture and its interaction with the customers IT landscape. The system architecture and its integration capabilities are described the the "Technical Factsheet ahead Intranet"
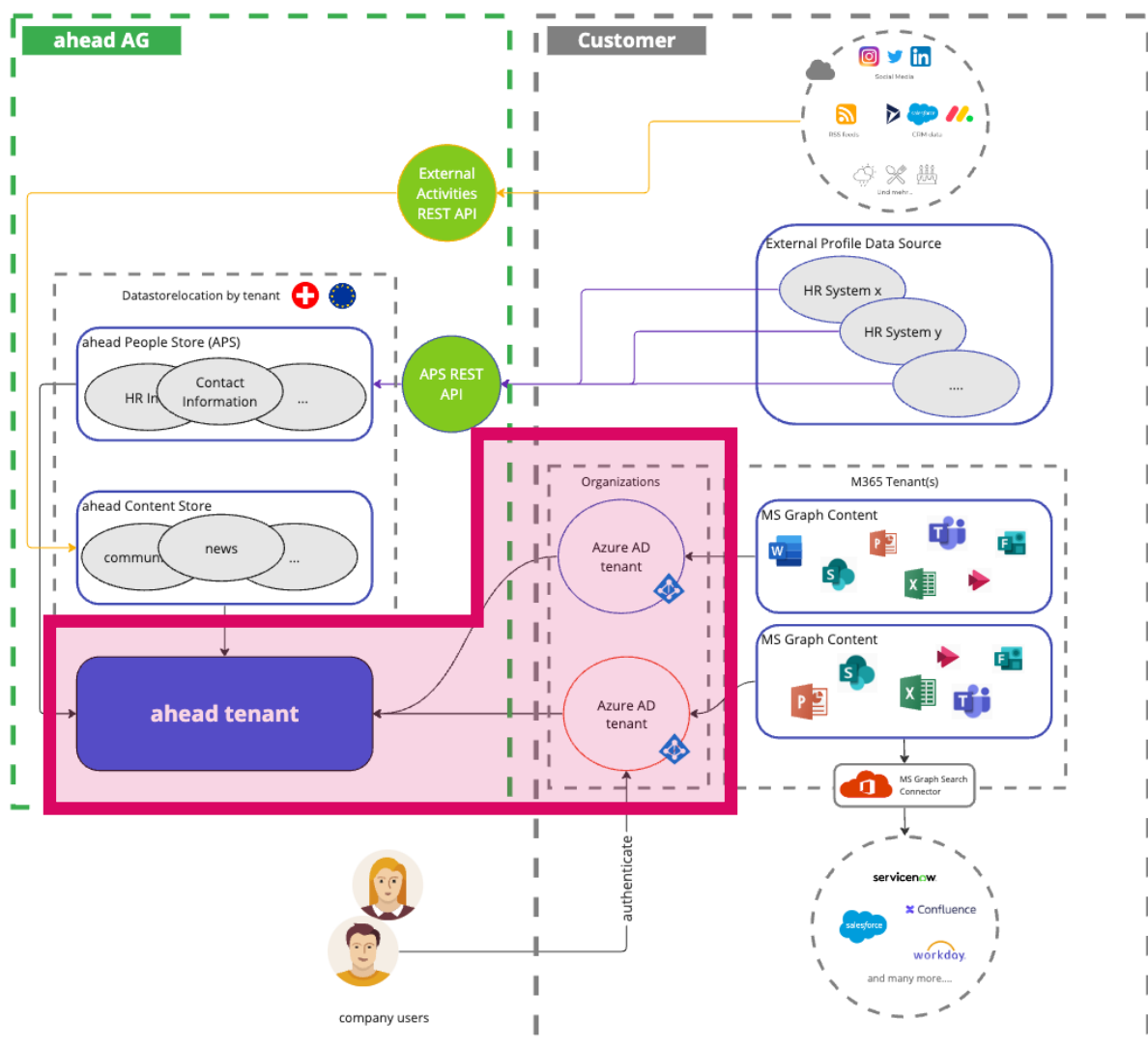

Figure 1 - System overview

---

[1] https://learn.microsoft.com/en-gb/azure/active-directory/?culture=en-us&country=ww

Authentication and Authorisation Overview with Entra ID

ahead Intranet uses Entra ID for authentication and authorization. This allows you to have full control over the authentication scenarios you provide for your users. Following the overview of the concepts that will be explained in later chapters:

- Single sign-on (SSO) is enabled through Entra ID.
- The Entra ID global administrator must grant app consent to ahead Intranet.
- A customer can link multiple Entra IDs to a single ahead Intranet tenant. (requires the ahead premium feature "Multitenancy")
- Authorisation is Entra ID group-based, with default groups for:
    - ahead Admins (for ahead Intranet Administrators)
    - ahead Editors (for content creators)
    - ahead Users (for all users that have access to ahead)
- ahead Intranet is compatible with both **Entra ID free and paid accounts**.
- In a scenario where your non-desk workers have no Microsoft Licences you can use Entra ID free accounts at no additional cost. You get the benefit of an enterprise grade and secure digital identity which can be used not only for ahead but also for accessing other software.

ahead

Entra ID readiness for ahead Intranet

In this section, we present various configurations to match your existing infrastructure. Use this guide to identify the steps needed to use ahead Intranet with Microsoft Entra ID.

The table below links to important resources from Microsoft and ahead intranet knowledge pages:

Name	Description	Link
Entra ID Overview	Official product website for Microsoft Entra ID (formerly Azure Active Directory).	Learn more…
What is Entra Connect?	How to manage on-premises and cloud identities (hybrid identity) with Entra Connect.	Learn more…
Entra Connect Overview	Microsoft Entra Connect is the successor of DirSync, Azure AD Sync, and Forefront Identity Manager with the Microsoft Entra Connector configured.	Learn more…
Entra Connect Sync Installation	How to use Entra Connect Sync to connect your on-premises Active Directory.	Learn more…
Entra Plans and Pricing	See the different pricing options (free and paid) for Microsoft Entra.	Learn more…
Roles and Permissions in ahead Intranet	See a complete list of all available permissions in ahead Intranet.	Learn more…
Content Targeting	Learn how content targeting is related to Entra ID.	Learn more…

Readiness check

The flowchart below will help you to identify what needs to be done to use Entra ID for authentication and authorisation in the context of ahead Intranet.
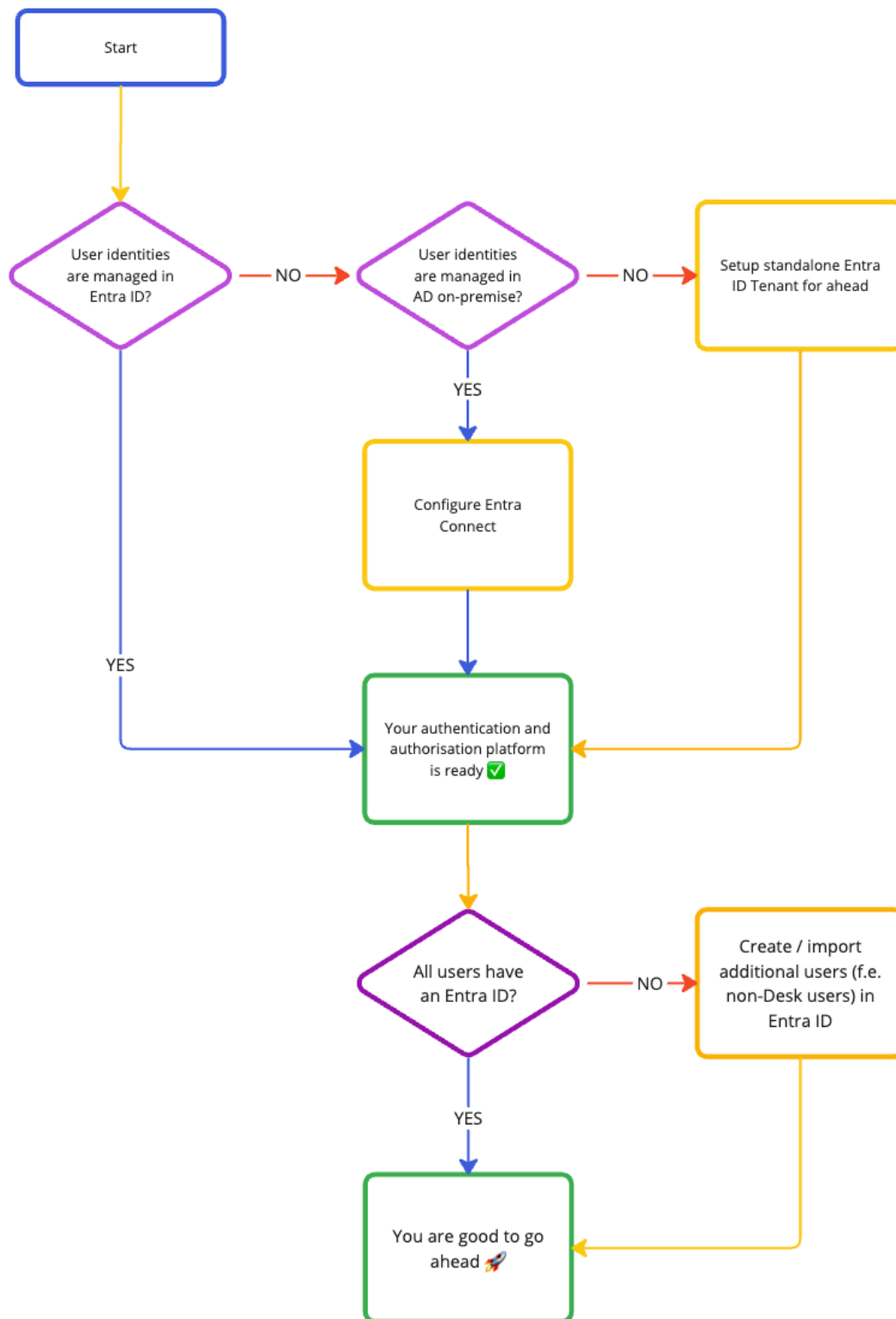
Figure 2 - Identify your Entra ID readiness to use ahead.

ahead

Configure Entra Connect

Microsoft's identity solutions span on-premises and cloud-based capabilities. These solutions create a common user identity for authentication and authorization to all resources, regardless of location. Microsoft calls this hybrid identity.

Hybrid identity is accomplished through provisioning and synchronization. Provisioning is the process of creating an object, keeping the object up to date and deleting the object when conditions are no longer met. Synchronization is responsible for making sure identity information for your on-premises users and groups is matching the cloud.

Follow these steps to configure Entra Connect: Tutorial

This scenario allows you, to create additional users f.e. non-desk users in Entra ID using the "Entra ID Free" account type.

Setup standalone Entra ID Tenant for ahead Intranet

In case you don't have Entra ID or Active Directory on-premise in place, you can setup a standalone Entra ID for free and use it for authentication and authorization for ahead. Keep in mind, that single-sign-on (SSO) won't be possible with this setup.

Create / import additional users in Entra ID

If Entra ID is operational but not all users, such as non-desk users, have an Entra Account, these accounts must be set up. Consider two key decisions:

1. Account Type: Are these "Entra ID Free" or "Entra ID Licensed" accounts? Typically, use "Entra ID Free" accounts if users only require secure access to ahead Intranet.

2. Account Creation Method: Will these accounts be manually managed in Entra ID or automatically integrated (e.g., from an HR System)? This choice largely hinges on the volume of accounts to be created initially and monthly due to employee turnover. The following Account creation methods exists:

   a. Manual entry in Entra ID

   b. Batch creation of users by Excel / CSV import

   c. Automate creation of Entra ID accounts when a person is created in your HR System. We can provide you with some best practices of how this can be done. Get in touch with us in case you wish to plan an integration.

ahead

Supported Entra ID Account Types and Licensing

ahead Intranet is designed to be a versatile and inclusive platform, accommodating various user roles and requirements. To align with this flexibility, ahead Intranet is compatible with all account types offered by Entra ID. This ensures that regardless of the account type your organization employs, users will be able to access and utilize ahead Intranet effectively.

Entra ID Free Accounts:

- Ideal for users who do not have a Microsoft Licence (e.g. Office 365) and a digital identity.
- Suitable for organizations looking to provide secure access (authentication) to their ahead intranet and other software without additional costs.
- Best for non-desk or part-time employees who only access information through ahead and do not need to create e.g. Office Documents (read only)

Entra ID Free accounts are eligible for read-only access to documents and other resources on Microsoft Office 365. In case you have a Microsoft Subscription your organization is eligible to use Entra ID Free Accounts at no additional Microsoft licensing cost. Please check the latest Information on the corresponding Microsoft sites about the different Entra ID Account Types [here](#).)

Disclaimer: Depending on the setup of the tenant, certain Microsoft security features are not included in the free plan. These are not related to the ahead product but rather due to the used Microsoft features. Typical scenarios are:

- Conditional Access Policies (e.g. access only from managed devices, access from abroad restricted, etc.) Get in touch with us if you plan to use Conditional Access Policies.
- MFA with SMS (users without Microsoft account can use the Microsoft Authenticator App)
- Self-Service Password Reset (users without license must be reset by admin, if necessary)

If such functions would be used, we recommend to buy the lowest possible Microsoft license or talk the ahead team to discuss different options.

Entra ID Licensed Accounts:

- Recommended for desk users who utilize ahead Intranet for a wide range of activities, including accessing third-party integrations especially Microsoft Office 365. The Entra ID Licensed accounts are typically already included in your Microsoft subscription (desk-user scenario)

Learn more about the different Entra ID Account Types [here](#).

ahead

Permission Management (Authorization)

In ahead Intranet, the management of user roles and their corresponding permissions is made possible using Entra ID groups. By default, three primary groups are required:

- **ahead Users:** This group includes the general user base, granting access to standard features and functionalities within ahead.

- **ahead Editors:** Members of this group are provided with permissions that allow them to create and manage content, reflecting their more active role in maintaining the intranet's resources.

- **ahead Administrators:** This group holds the highest level of access, with comprehensive permissions to configure and administer the platform in its entirety.

In ahead Intranet, each group has specific permissions assigned to it, ensuring a clear separation of roles and responsibilities. For organizations requiring a more nuanced approach to permission management, ahead offers the flexibility to create additional groups. These groups can be tailored with a more granular set of permissions, allowing for a customized authorization structure that aligns with the specific requirements of your organization.

For a complete list of all available permissions, please refer to our detailed ahead knowledge base article [here](#).