



Microsoft Entra ID

Microsoft Entra ID is a cloud-based identity and access management solution. It is a directory and identity management service that operates in the cloud and offers authentication and authorization services to various Microsoft services such as Microsoft 365, Dynamics 365, and Microsoft Azure.

Functionality

Connectivity between Omada and Microsoft Entra ID enables organizations to:

- Register and onboard any number of Microsoft Entra ID instances.
- Load information about Users, Groups, group memberships, and used licenses.
- Automate the provisioning and de-provisioning of Microsoft Entra ID users, groups (Security, Teams, and SharePoint), and memberships.
- Extraction of assignments between:
 - Directory roles and users
 - Teams groups, members, and owners
 - SharePoint groups, members, and owners
 - Security groups, members, and owners
 - Distribution groups, members, and owners
 - Mail-enabled Security groups, members, and owners
 - Groups
- Extraction of Teams Channels and parent/child between Teams and Channels
- Extraction of resource owners of each group (Teams, SharePoint, Security, Distribution, Mail-enabled Security)
- Extraction of Stock Keeping Units (SKUs) and included service plans
- Extraction of user's assigned licenses
- Extraction of user's assigned service plans
- Extraction of user accounts
 - Sign-in activity
- User provisioning
 - Password reset
- Groups provisioning
 - Teams groups
 - SharePoint groups
 - Security groups
- Assignments
 - Add and remove assignments between groups (Security, Teams and SharePoint) and users
 - Add and remove assignments between directory roles and users

Supported Objects and Operations

Object	Possible operations
Users	Create, read, update, delete (**)
User passwords	Create, update
Security groups	Create, read, update, delete
Distribution groups	Read*
Mail-enabled groups	Read*
Sharepoint	Create, read, update, delete
Teams	Create, read, update, delete
Channels	Read
Security group memberships	Create, read, delete
Distribution group memberships	Read*
Mail-enabled group memberships	Read*
Team group memberships	Create, read, delete
Sharepoint group memberships	Create, read, delete
Directory roles	Read
Directory roles Assignments	Create, read, update, delete

(*) The Microsoft Graph API does not provide support for provisioning of distribution groups and mail-enabled security groups. See the [Microsoft Exchange Online/Hybrid](#) connectivity section for details how to manage these groups.

(**) When a user is deleted from Microsoft Entra ID, Omada automatically revokes sign-in sessions for the deleted user. If revoking the sign-in session fails for any reason, Omada logs a warning for the task. This functionality is available without any additional configuration.

The Omada Configurable Connectivity offers:

- Template-driven connectivity for ease of implementation
- Flexible data model
- Adaptable and extensible data fields and attributes
- Choice of multiple authentication methods

A configurable connectivity approach provides an efficient, reliable and fast alternative that is better suited to the dynamic, hybrid IT environment where connectivity is a continuous activity. Connectors for Omada and Microsoft Entra ID can be leveraged using Omada's configurable connectivity framework, which supports standard connectors for SCIM, REST, OData, LDAP, PowerShell, .CSV, .NET, SQL, and SOAP.