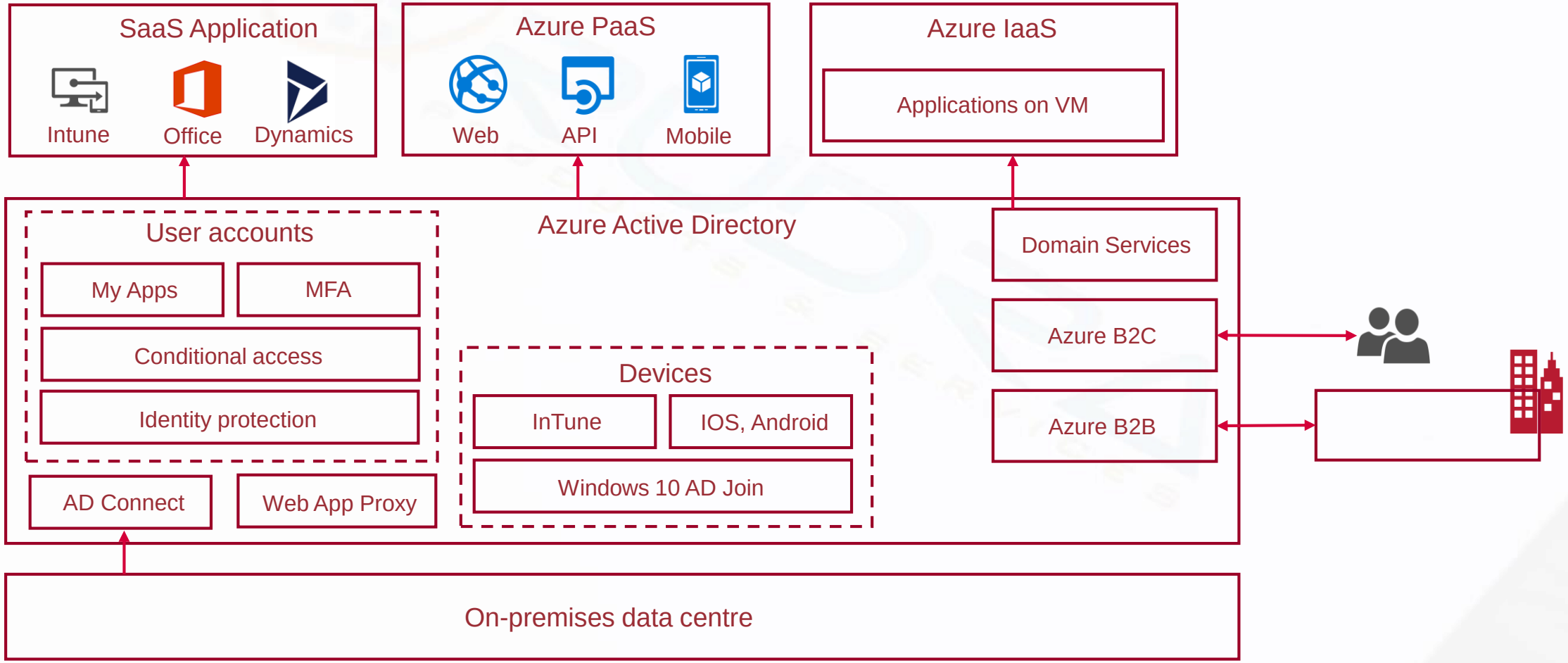
Azure Active Directory Overview

Azure Active Directory overview

Azure AD is a leading provider of cloud-based Identity as a Service (IDaaS) and provides a broad range of capabilities for enterprise organizations.



AD Identities

An Identity in Azure Active directory can be

- User – Individual who can be given access to apps, app resources based on your business requirements
- Managed identity
  - System assigned managed identity
  - User assigned managed identity
- Devices
  - Device based conditional access
- Group

Groups

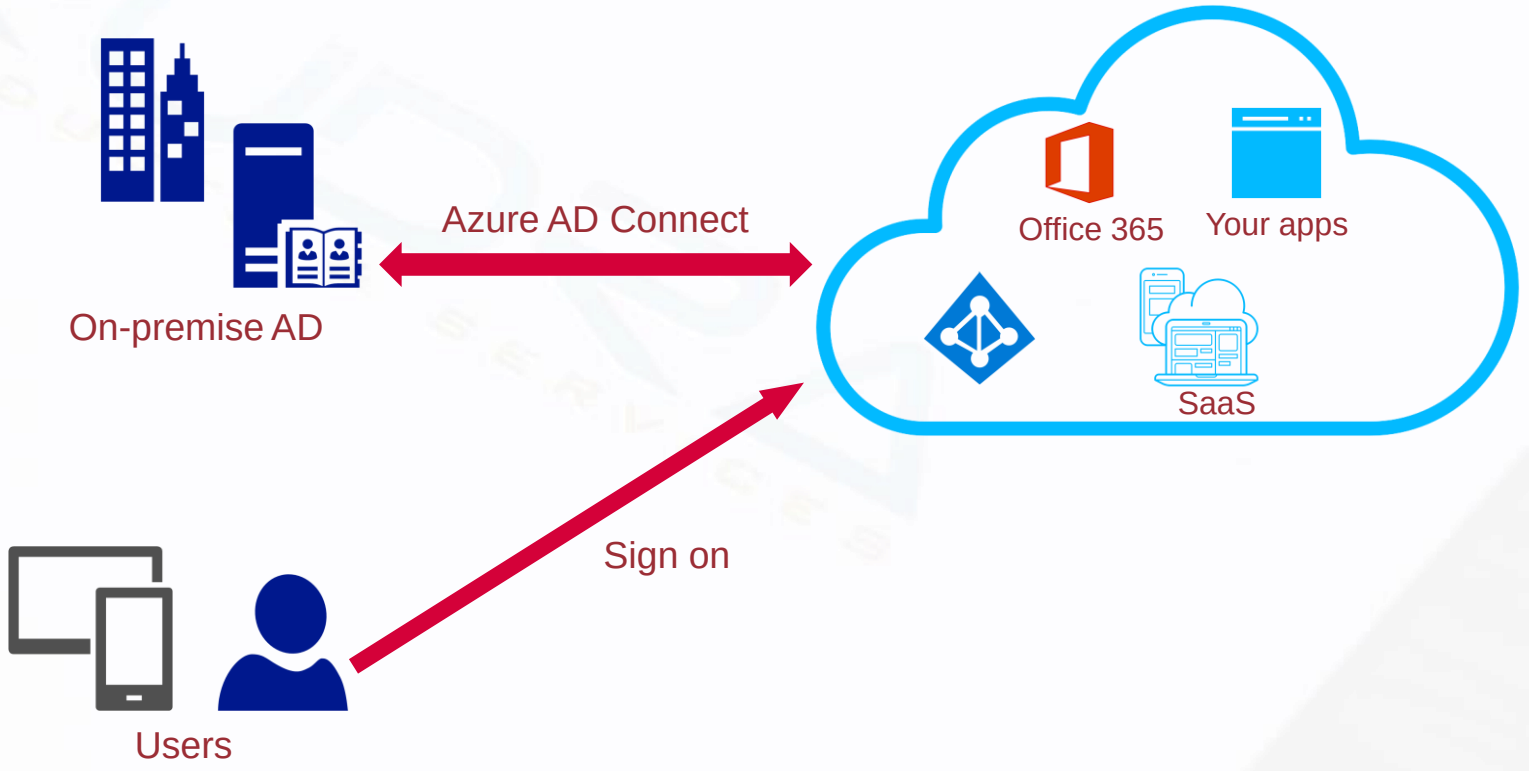
Azure AD helps you give access to your organization's resources by providing access rights to an entire Azure AD group. Using groups lets the resource owner (or Azure AD directory owner), assign a set of access permissions to all the members of the group, instead of having to provide the rights one-by-one. Four ways to assign resource access rights to user..

- **Direct assignment** - The resource owner directly assigns the user to the resource
- **Group assignment** - The resource owner assigns an Azure AD group to the resource, which automatically gives all of the group members access to the resource.
- **Rule-based assignment** - The resource owner creates a group and uses a rule to define which users are assigned to a specific resource. The rule is based on attributes that are assigned to individual users
- **External authority assignment** - Access comes from an external source, such as an on-premises directory or a SaaS app

Hybrid identities & Azure AD connect

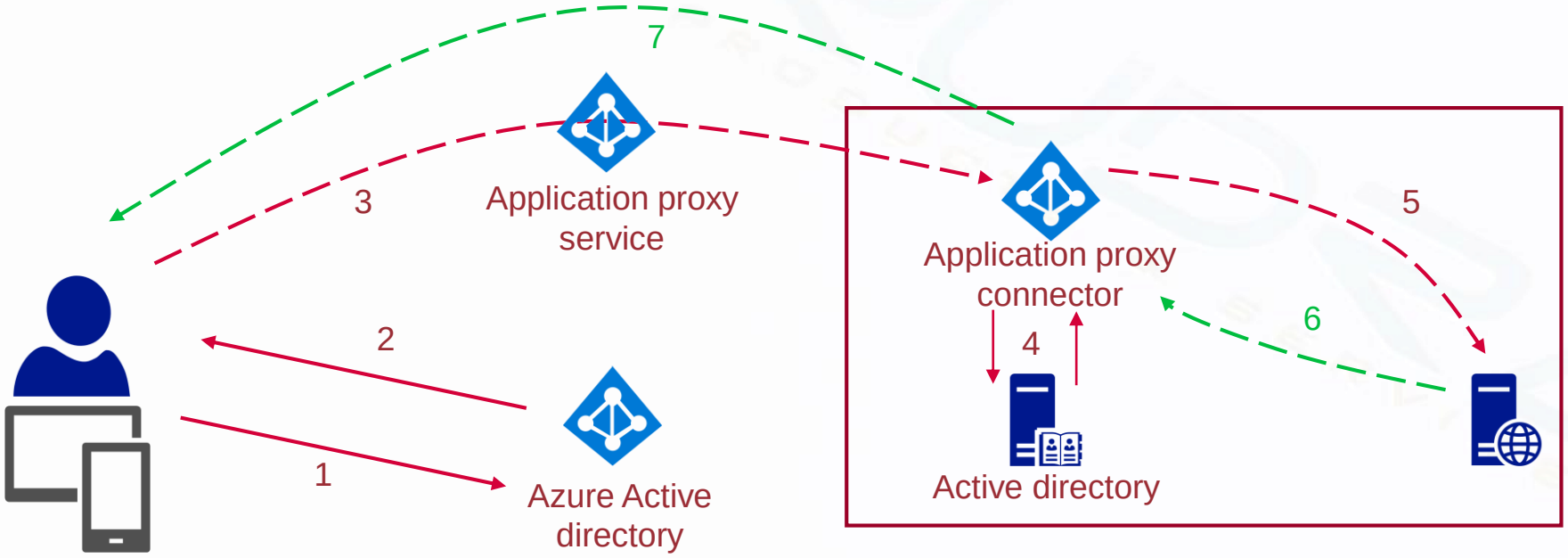
Hybrid identity is a common identity for authentication and authorization to all resources regardless location

- Password hash synchronisation
- Pass through authentication
- Federation integration
- Synchronisation
- Health Monitoring



Web app proxy

Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client. Application Proxy includes both the Application Proxy service which runs in the cloud, and the Application Proxy connector which runs on an on-premises server.



1. After the user has accessed the application through an endpoint, the user is directed to the Azure AD sign-in page.
2. After a successful sign-in, Azure AD sends a token to the user's client device.
3. The client sends the token to the Application Proxy service, which retrieves the user principal name (UPN) and security principal name (SPN) from the token. Application Proxy then sends the request to the Application Proxy connector.
4. If you have configured single sign-on, the connector performs any additional authentication required on behalf of the user.
5. The connector sends the request to the on-premises application.
6. The response is sent through the connector and Application Proxy service to the user.