Clearlogin - Microsoft 365 Federation

In This Article

- Overview
- Planning for Microsoft 365 Federation

Overview

This article covers the steps to federate your Microsoft 365 tenant with Clearlogin. When you federate you Microsoft 365 tenant with Clearlogin, Microsoft 365 will use Clearlogin to authenticate and authorize users to access resource in the Microsoft 365 tenant.

> ⊘ It is strongly recommended that you review this entire article before moving forward. Performing the steps in this article without proper planning may cause you to lock yourself out of your Microsoft 365 tenant. If you lock yourself out of your Microsoft 365 tenant, only Microsoft can get you back in. Evolve IP will not be able to assist.

Planning for Microsoft 365 Federation

- Microsoft 365 federation is only supported when Clearlogin is using a Windows Active Directory domain controller as an identity source, and you are syncing your Windows Active Directory to Azure AD (Microsoft 365) using Microsoft's Azure AD Connect software.
- Microsoft 365 federation is not supported when Clearlogin is using Azure AD as an identity source.
- After activating the federation, all user account management must be performed in your Windows Active Directory. You cannot manage user account properties/attributes in the Microsoft 365 admin center or in the Azure AD portal. However, you can manage license assignments, roles, and other features.
- A Microsoft 365 federation is per domain. All user accounts using the federated domain in their User Principal Name (UPN) will be affected by the federation. This includes all user accounts and service accounts synced from your Windows AD to Azure AD.
- Modern Authentication must be enabled for all services in your Microsoft 365 tenant. Since August 2017, Microsoft has been enabling Modern Authentication by default for all new Microsoft 365 tenants. If your tenant was created before August 2017 you should verify that Modern Authentication is enabled for all services.
- The federated domain cannot be the default domain listed in the Microsoft 365 admin center. If the domain you are planning to federate is currently your default domain, you will need to change it to another verified domain, or change your default domain to the tenant's onmicrosoft. com domain.
- We strongly recommend you perform the Microsoft 365 configuration steps using an onmicrosoft.com cloud-only user account that's a global admin. Do not use a global admin account with a UPN using the federated domain.
- Configuring a Microsoft 365 federation requires the use of PowerShell, and this article assumes you have experience with PowerShell. If you are not comfortable with PowerShell you should not perform the configuration.
- To provide a seamless, unobtrusive end-user experience, it is recommended that all users complete their Clearlogin account recovery settings in their profile.