

# Okta to Entra ID Migration

Issue Date: December 7, 2023



# Overview

In the early days of cloud SaaS (software delivered as a service), a company's options for authentication were limited, and very few identity solutions even provided Single Sign-on. This was an indication of the maturity in the cloud and less of a technical deficiency. Back then cloud solutions were seen as outside the perimeter of traditional InfoSec boundaries, and IT lived by the SaaS solutions IdM (Identity Management) or try to integrate into an on-premises IdP (Identity Provider). This all changed when Okta, Ping Federate, and Microsoft hit the scene and started offering cloud- first SAML integrations to SaaS solutions. Fast forward to today where cloud solutions are the norm, and companies are demanding tighter integration, more security, and visibility into their cloud vendors. Okta and Microsoft now offer thousands of apps in their app catalogs, and offer features like Lifecycle Management, Identity Governance, SSO, and enhanced threat detection and response. These two providers have similar features in these key areas, as well as being easy to use for users. This feature parity has prompted companies using Okta to re-evaluate their IdP solution and look to tools they already own to do the job. Entra ID continues to be the most popular solution to migrate to and can increase security posture along the way.

## Why Migrate to Entra ID?

Microsoft is one of the largest identity providers in the world, and chances are your organization already has an Entra ID footprint. Entra ID is trusted by over 200,000 organizations and manages over 610M monthly active users, with over 30 billion daily authentication requests. Entra ID excels in the four principal areas organizations evaluate when choosing an IdP.

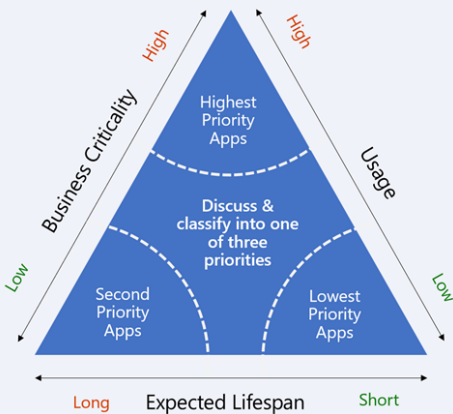
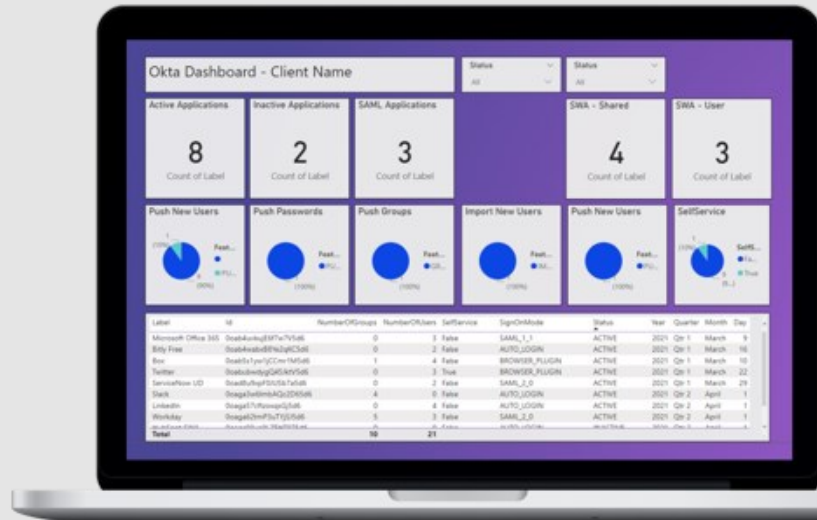
Secure Adaptive Access	Seamless User Experience	Unified IdM	Identity Governance
Conditional Access policies that evaluate context and risk	Password-less credentials to fight credential harvesting	Access applications in any cloud and across a hybrid environment	Privileged identity management and role-based access control
Multiple secure multi-factor authentication (MFA) methods	Single sign-on (SSO) for all users and use cases	Efficient identity management and administration for employees, partners, and customer	Entitlement management for granting and reviewing access
User behavior analytics to protect against identity compromise	Self-service portal to discover and launch applications, request access and manage security methods	Uses Open standards such as SAML and FIDO, and supports interoperability across	Automatic users and guest's lifecycle management, connected to the HR platfor

# Process Overview

Netwoven’s migration framework consists of four central phases: **Envision, Onboard, Migration, and Drive Value**. This framework is proven to reduce project risk, focus on a seamless user experience, and deliver ROI within Entra ID. This is the same approach that is used throughout Netwoven’s project management.

## Envision

In the first phase, the goal is to start with inventorying the current environment for use cases, features in use, and custom integrations where more effort might be needed. Once the use cases have been defined the team will then prioritize the scenarios to make sure all scenarios are accounted for in Entra ID. This includes a full application evaluation to ensure that no app is left behind due to custom authentication or access management. There are typically integrations and applications discovered during this time that IT was previously unaware of.



## Onboard

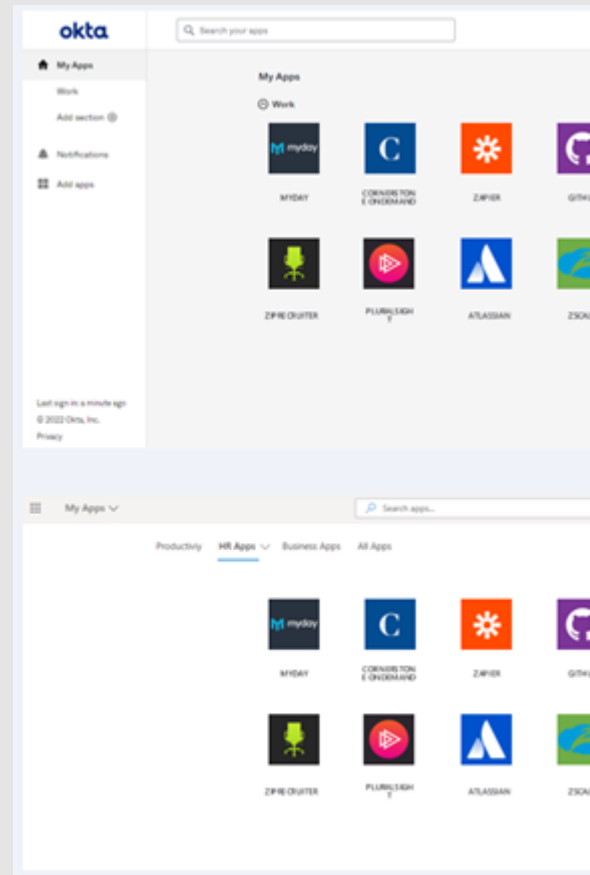
After the full inventory is complete and priority is given to the use cases, the focus is on planning the migration and setting up the Entra ID environment. Some applications require vendors to update their side of SAML auth flow, so time is accounted for with these known SaaS applications. Other applications get earmarked for dual IdP support, which minimizes the user cutover experience. Unfortunately, not all applications use SAML to provide SSO capabilities, so those SWA applications are noted and bucketed together.

Entra ID is prepared for onboarding users, applications, and identity governance at this time too. Information Security’s requirements are primarily implemented through tenant settings and conditional policies. Users will be set up for combined security registration, which allows them to use SSPR and MFA on day one of the migrations without interruption.



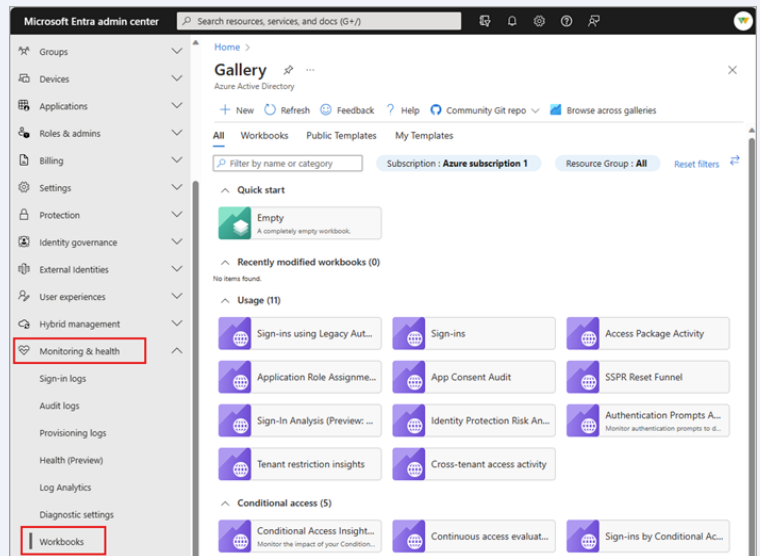
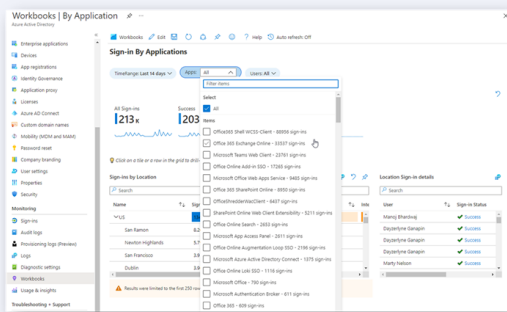
## Migration

All applications that are marked for migration are recreated as Linked apps in Entra ID first. This allows us to point the EID application back to Okta during the migration period, thus allowing users to see all their applications in Entra ID regardless of their IdP. Test migrations follow to confirm the environments are set up properly, and the migration scripts are accounting for any exclusive use cases. After all, apps are created, users are enrolled in MFA, and test migrations are signed off by Business Owners, final migrations can begin. Migrations are usually split into 3 phases, with the low priority applications coming over first, followed by medium then high. This allows any kinks and environment quirks to be worked out before moving a mission-critical application. During the migration, users are recommended to log in to Entra ID first regardless of whether the application has migrated or not. After each migration, the Okta chicklet is modified to point at the Entra ID URL for the application.



## Drive Value

After the migration of all applications, the ROI of Entra ID can begin to be realized. Identity Governance and Protection elements are set up such as Access Reviews, Risky User playbooks, and SCIM provisioning. All these features reduce the IT burden and let end users do more with the tools IT-enabled. Custom reports are then built with EID workbooks around key applications to highlight user-impacting sign-in issues, adoption rates, and potential attacks.



# Challenges companies face while

There are a lot of moving parts to an IdP, but the most important are the users and applications served by the IdP. These are where we see the most challenges when migrating to Entra ID. From a user perspective, they just want their applications to work and be prompted the least number of times to log in. This is where Netwoven’s change management track helps coordinate Self Service Password Reset and Multi-factor Authentication rolling out before migrating apps to Entra ID. Once users are enrolled, we can reduce the prompts by using Risk-based MFA, and/or implement Silent SSO with compliant Entra ID Joined devices. The other area is around the application, and its ability to offer self-service SSO updates. Home-grown applications may need to be updated by the development team that created them, and some SaaS applications still require you to contact their support to update the SSO settings in their app. Luckily, the open standard for SAML is widely used in SaaS applications, so there aren’t many applications that “cannot migrate”, instead it is just a matter of coordinating with that application’s support.



## Key benefits of Migrating:

- ✔ Significant cost savings by reducing licenses, complexity, and maintenance
- ✔ More security within the Microsoft365 suite by allowing granular access controls
- ✔ Native integrations allow for streamlined provisioning of accounts and access
- ✔ Single pane of glass for Security Operations to scan Identities, Devices, and Information access
- ✔ Simplifies the path to Zero Trust, allowing the Microsoft stack to evaluate Risk and Device Health on every request

To learn about how Netwoven helped Relay GSE migrate from Okta to Entra ID, read the [case study](#)





## RELAY/GSE



Our experience working with the Netwoven team was excellent. They demonstrated a high level of expertise and admirable quality of work which helped us solve any challenges that occurred during the migration process and assisted us in the timely completion of the project. I'm extremely satisfied with the smooth execution of the project and the overall outcome achieved.



**Joaquin Alvarez**  
*Senior Director*

### About Netwoven, Inc.

Netwoven is a leading professional services provider that enables Digital transformation for businesses by leveraging the wide range of Microsoft products. We help organizations design and deploy comprehensive and cost-effective solutions for Collaboration, Analytics, Security, and Customer Relationships. We support our customers with their digital journey using Microsoft's leading cloud platforms- Dynamics 365, Microsoft 365, and Azure.

