Solution Brief

Okta to Azure AD Migration

Issue Date: June 6, 2022

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. Azure AD continues to be the most popular solution to migrate to and can increase security posture along the way.

Why Migrate to Azure Active Directory?

Microsoft is one of the largest identity providers in the world, and chances are your organization already has an Azure AD footprint. Azure AD is trusted by over 200,000 organizations and manages over 425M monthly active users, with an average of 30 billion daily authentication requests. Azure AD excels in the four principal areas organizations evaluate when choosing an IdP.

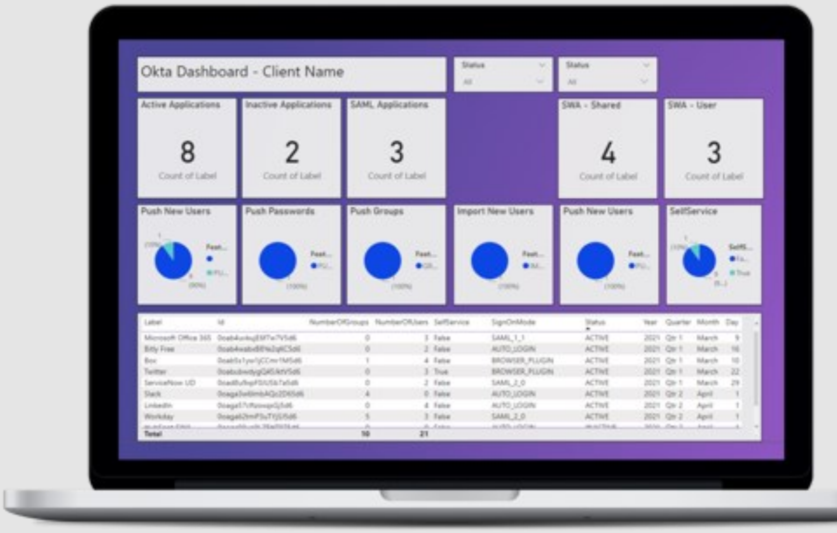
Secure Adaptive Access	Seamless User Experience	Unified IdM	Identity Governance
Conditional Access policies that evaluate context and risk Multiple secure multi-factor authentication (MFA) methods User behavior analytics to protect against identity compromise	Password-less credentials to fight credential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

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 Azure AD. 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 Azure AD. 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.


Okta Dashboard - Client Name

Status: All

Status: All

Active Applications: 8 (Count of Label)

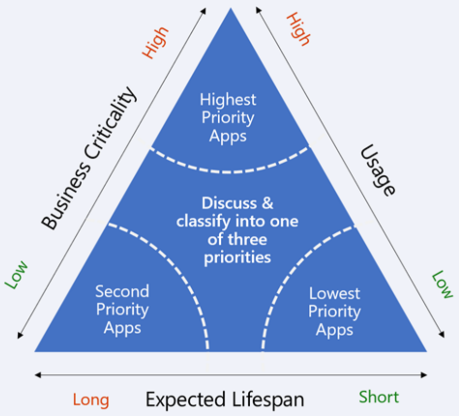
Inactive Applications: 2 (Count of Label)

SAML Applications: 3 (Count of Label)

SWA - Shared: 4 (Count of Label)

SWA - User: 3 (Count of Label)

Label	Id	NumberOfGroups	NumberOfUsers	SelfService	SignOnMode	Status	Year	Quarter	Month	Day
Microsoft Office 365	0oab4uxkujEM7w7V5d6	0	3	False	SAML_1_1	ACTIVE	2021	Qtr 1	March	9
Bitly Free	0oab4wabvBtNs2qKC5d6	0	2	False	AUTO_LOGIN	ACTIVE	2021	Qtr 1	March	16
Box	0oab5s1ywYjCCmr1M5d6	1	4	False	BROWSER_PLUGIN	ACTIVE	2021	Qtr 1	March	10
Twitter	0oabubwdygQ45AtV5d6	0	3	True	BROWSER_PLUGIN	ACTIVE	2021	Qtr 1	March	22
ServiceNow UD	0oad8u9xpFSiUSk7a5d6	0	2	False	SAML_2_0	ACTIVE	2021	Qtr 1	March	29
Slack	0oaga3w6mbAQc2D65d6	4	0	False	AUTO_LOGIN	ACTIVE	2021	Qtr 2	April	1
LinkedIn	0oaga57vRoswpGj5d6	0	4	False	AUTO_LOGIN	ACTIVE	2021	Qtr 2	April	1
Workday	0oaga62tmPSuTYjSi5d6	5	3	False	SAML_2_0	ACTIVE	2021	Qtr 2	April	1
Total		10	21							



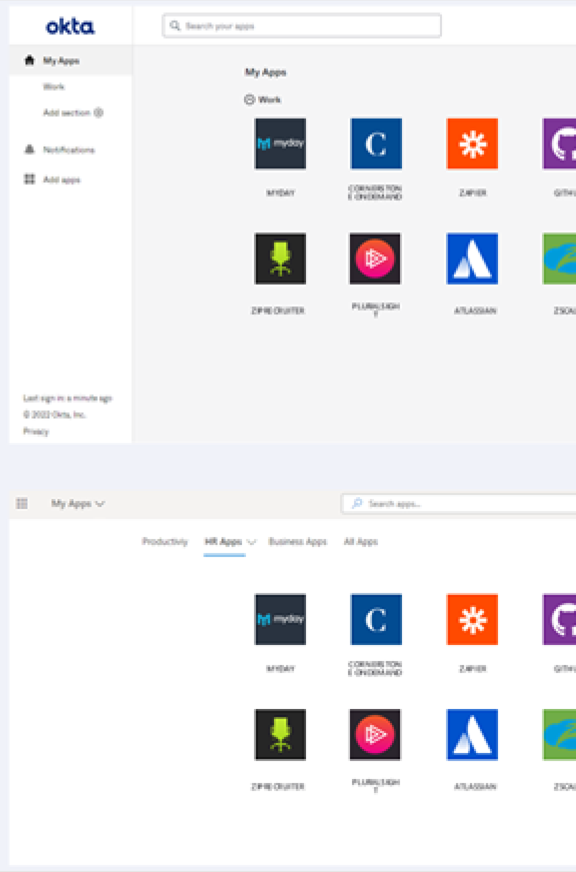
Onboard

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 Azure AD 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.

Azure AD 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.

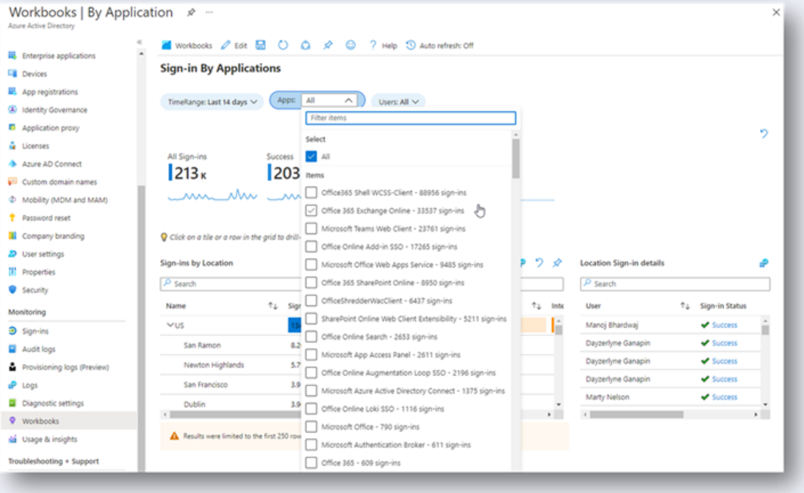
Migration

All applications that are marked for migration are recreated as Linked apps in Azure AD first. This allows us to point the AAD application back to Okta during the migration period, thus allowing users to see all their applications in Azure AD 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 Azure AD first regardless of whether the application has migrated or not. After each migration, the Okta chicklet is modified to point at the Azure AD URL for the application.



Drive Value

After the migration of all applications, the ROI of Azure AD 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 AAD workbooks around key applications to highlight user-impacting sign-in issues, adoption rates, and potential attacks.



Sign-in By Applications

Select

☑ All

Items

☐ Office365 Shell WCSS-Client - 88956 sign-ins
☑ Office 365 Exchange Online - 33537 sign-ins
☐ Microsoft Teams Web Client - 23761 sign-ins
☐ Office Online Add-in SSO - 17265 sign-ins
☐ Microsoft Office Web Apps Service - 9485 sign-ins
☐ Office 365 SharePoint Online - 8950 sign-ins
☐ OfficeShredderWacClient - 6437 sign-ins
☐ SharePoint Online Web Client Extensibility - 5211 sign-ins
☐ Office Online Search - 2653 sign-ins
☐ Microsoft App Access Panel - 2611 sign-ins
☐ Office Online Augmentation Loop SSO - 2196 sign-ins
☐ Microsoft Azure Active Directory Connect - 1375 sign-ins
☐ Office Online Loki SSO - 1116 sign-ins
☐ Microsoft Office - 790 sign-ins
☐ Microsoft Authentication Broker - 611 sign-ins
☐ Office 365 - 609 sign-ins

User	Sign-in Status
Manoj Bhardwaj	✓ Success
Dayzerlyne Ganapin	✓ Success
Dayzerlyne Ganapin	✓ Success
Dayzerlyne Ganapin	✓ Success
Marty Nelson	✓ Success

Challenges companies face while migrating to Azure AD

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 Azure AD. 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 Azure AD. Once users are enrolled, we can reduce the prompts by using Risk-based MFA, and/or implement Silent SSO with compliant Azure AD Joined devices. The other area is around the application, and it's a bility 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

Contact us today for Okta to Azure AD Migration →

Available on Microsoft AppSource

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: Microsoft 365, Dynamics 365 and Azure.