

Changing Identity [providers]

Migrating from Okta to Microsoft Entra ID

The Benefits



Reduced Cost

Native to **Microsoft Entra ID**, you may already have the functionality rather than need to use a **3rd party IDP**.



Reduced Risk

Migrating provides a **single pane of glass**, reduces the need to understand multiple solutions and reduces the likelihood of a **security gap** between systems.



Simplified Management

A single provider can **simplify management** overheads, saving your in-house team time.



Greater Security

New controls such as **Passwordless Sign-In, Windows Hello for Business** give companies the edge in stopping threats such as Business Email Compromise at the start of the attack chain.

The History

For the large percentage of today's workforce, the concept of having a single identity in the format of [firstname].[lastname] or similar has been the norm. This provides a single solution for user **Authentication, Authorization** to resources and **Audit** of activity (**AAA**) and has been around generally since the days of Novell in the last century. As we moved into the noughties, organisations implemented or migrated to Active Directory, yet the ability to provide a centralized AAA across all applications has been a problem; even Microsoft solutions such as MS CRM and companies were regularly required to invest in complex solution to integrate with Active Directory or to have multiple accounts with multiple passwords – leaving risks of user accounts being left open, audits being decentralized etc.

With the advent of Cloud, this has changes. Identity providers such as **Okta, Duo, Microsoft Entra ID, Google Cloud Identity** and others have leveraged technology to allow organisations to fully outsource the control of **AAA** to a single provider – in effect a user can log into not only their machine but also SAP, Salesforce, Box etc. seamlessly.

Change is a constant and as identified above, there are a number of reasons to change their Identity provider however it's not something that an organisation does regularly which is where Performanta can help.

Case Study- Energy Sector Firm

In this example, we will use the live example of a US energy sector firm that had underpinned their entire solution with Okta but wanted to migrate to Microsoft Entra ID to reduce cost and simplify management. Performanta were identified through the Microsoft marketplace as a suitable provider to help navigate them from **Okta to Microsoft Entra ID** and after a quick discussion, we started to get the project underway.

Assess

Before making any changes, Performanta carried out an assessment of the environment to understand the complexity of the existing build and identify any major risks to the company.

60 applications, using **five different protocols**, were identified. Complications around, user provisioning, access within applications and AAA mechanisms were mapped and it was clear that, whilst the project would require testing, there were no major risks to the organisation that could not be overcome with due diligence.

Migrate

Due to a need for minimum downtime, the migration was planned with a target of zero downtime to all end users. As a UK based firm, Performanta were perfectly placed to support this migration as changes could be made in the early hours so that the experience was mostly seamless to end users. The project was split into three phases.

Phase 1

Design and Build

Performanta **consulted** with the client to **design** Microsoft Entra ID controls, from privileged accounts to guests, to ensure that the model fitted the business. Subsequently, the environment was built out in **audit mode** before deploying in anger.

The agreement was to implement a **Zero trust** model. From **passwordless sign-in** to strong **Conditional Access** controls, the environment was fully hardened at the start to ensure that the tenant was secure without impact to productivity or user experience.

Phase 2

Migrate Microsoft

The most complex element of the migration, changing the identity provider from Okta to Microsoft Entra ID, was made considerably simpler by taking advantage of **Microsoft's Staged Migration** – a solution originally designed for ADFS. Performanta took advantage of the granular controls available to cut over users in stages, removing the impact that a big bang approach would have on end-users and the support desk.

Despite the complexity, all users moved cleanly from Okta to Microsoft Entra ID - the few snags resulting from users failing to fully follow instructions, all of which were identified before cutover. The only requirement from end users was the need to register for MFA and all users were cleanly cutover in less than a month.

Phase 3

Staged Application migration

With the hardest challenge out of the way and security controls in place, Performanta are now cutting over applications for the client while they sleep - as with any good First Class service, the end users have been waking up with the Identity Provider for their applications in a new place without any impact to their sleep or start of the day, the applications magically appearing in their My Apps portal with seamless Single Sign-On integrated with their PCs and Macs.

Summary


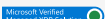
Changing Identity Provider doesn't have to be hard but remember the keys to a great user experience is good planning, testing and communication.


Why Performanta?

Founded in 2010, Performanta is a leading Microsoft Solutions Partner for both Modern Work and Security, with Security Specialisations Identity and Access Management, and in Threat Protection. Performanta became one of the world's first FastTrack Ready Security Partners (FRSPs) and joined the Microsoft Intelligent Security Association (MISA), placing Performanta firmly as a leader in the cyber security space. Performanta has also achieved Microsoft verified MXDR solution status.

As an award-winning Managed Cyber Security Service Provider, Performanta has been pioneering cyber safety, working tirelessly to achieve two things for our clients: lowering the risk and limiting the impact of a successful cyber attack. We work with large and small clients across the world and are experts in cyber security and cyber safety. Our Microsoft Consultancy, Managed Sentinel SOC and MDR teams are experts in their fields, and our services are essential to our customers in today's world where cyber threat is greater than ever.

Member of
Microsoft Intelligent
Security Association


Microsoft Intelligent
Security Association
 

 Microsoft
FastTrack
Partner

