How UNIFYConnect enhances Azure integration capabilities

At UNIFY Solutions in 2022 our focus is firmly on improving the security posture of our many clients, and adopting a "Zero Trust" approach to Identity and Access. This is particularly relevant for everything we do within my Microsoft Workplace Identity Practice at UNIFY, in particular remote worker enablement, and the "hero" of our offering is our **UNIFYConnect** service. Let me explain ….

Without UNIFYConnect you could wait years to realise the full potential of Lifecycle Management and Governance for Identity in Azure AD.

While today UNIFY Solutions maintains a strong alignment with Microsoft and their published Security principles, it hasn't always been this way. Our business was established on the core concepts repeatable Identity Lifecycle solutions, and Continuous Compliance for digital identities (i.e. at all times any workforce should have just enough access to do their jobs, and only for the time they are expected to perform them). However it is only in the last few years that Microsoft has acknowledged the key role of identity in achieving its vision of Zero Trust for its corporate customers worldwide by re-aligning both its business structure and its Microsoft Certification program under "Security, Compliance and Identity". Furthermore the UNIFY focus was firmly on aligning HR workforce activity (joiners/movers/leavers) with Microsoft's Active Directory (AD) … but now in a Microsoft context it is much more than that as they build out the Microsoft Azure Identity Framework to achieve this at a global scale.

The Microsoft Identity Framework is built on 4 core concepts which work together to drive a Zero Trust outcome:

- Azure HR Provisioning
- Azure App Provisioning (with SCIM)
- Azure Identity Governance (IGA)
- B2B Guest Provisioning (trusted partners and vendors not in HR)

With these elements in place, organizations can confidently align to clearly published Identity Architecture patterns, and plug into the roadmap as it rapidly evolves, ultimately ensuring "Modern Authentication" concepts (multifactor authentication, conditional access, etc.) are built into each and every enterprise application user interaction.

However, in the short to near term, as the Microsoft roadmap is constantly developed and refined, organizations looking to adopt are invariably running into the inevitable feature/capability limitations that exist today. To address these "gaps", organizations must be confident that anything that is put in place is

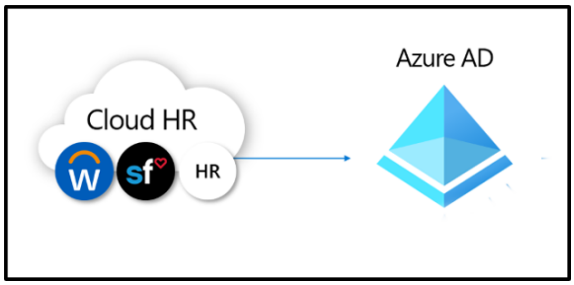
- enterprise grade
- easily supportable
- does not add to existing technical debt
- can readily be adjusted or swapped out completely as requirements change and new Microsoft features come online.

With **UNIFYConnect**, you can be confident you can address these same gaps today, in a way that comfortably **satisfies all these criteria**.

Let's see how …

AZURE HR PROVISIONING

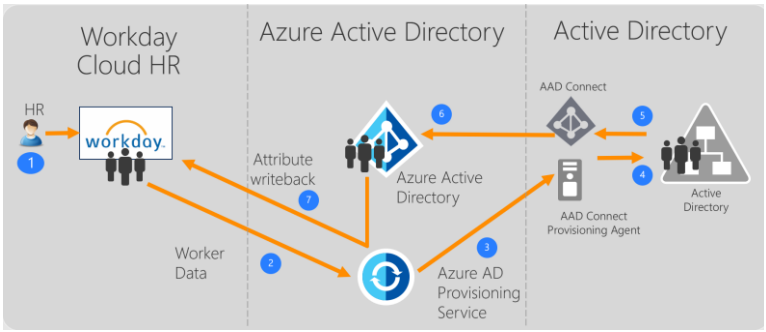
HR driven provisioning is the process of creating digital identities based on a human resource (HR) platform - specifically in a Microsoft context in Active Directory (AD on premises) and/or Azure Active Directory (Azure AD).



From [What is HR driven provisioning with Azure Active Directory? | Microsoft Docs]

Very few organizations do not have an on-premises AD that they do not need to maintain lockstep in line with their Microsoft Azure AD, and Microsoft call this "Hybrid Identity". The key to successful implementation of Azure HR Provisioning is to understand the identity lifecycle that must be followed, as articulated by Microsoft below for one of ***only 2*** HR systems supported today …

UNIFY has been providing the same solution for a variety of HR vendors for the last 2 decades as the concept of hybrid identity has taken shape. Today, with our **UNIFYConnect** service, UNIFY offers a comparable hosted approach for not only familiar global HR platforms such as Workday and SAP SuccessFactors, but also more regionally focused HR platforms such as Frontier's chris21, Aurion and ELMO. There is no need to wait for Microsoft to address your organization's own HR scenario when you can implement the **UNIFYConnect** option today - in the confidence that if and when a Microsoft alternative comes online you will be able to seamlessly transition because we have been at pains to build our solution to the same solution pattern that Microsoft today has now branded Azure HR Provisioning.

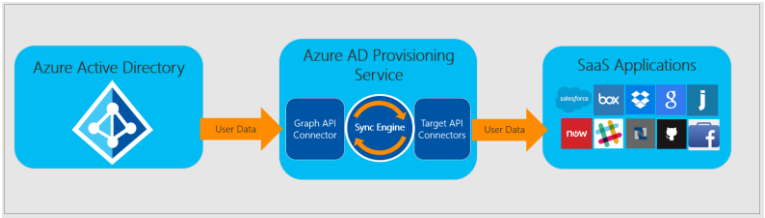


From [Tutorial: Configure Workday for automatic user provisioning with Azure Active Directory | Microsoft Docs]

Furthermore, for some customers the core solution is all that is required, and the appliance version of **UNIFYConnect** known as UNIFYAssure can be implemented quickly without the need for any customization.

AZURE APP PROVISIONING

Azure App(lication) provisioning is the process of creating digital identities (user profiles) in a target application that authenticates users to Azure AD. As is the case for an increasing number of applications (ServiceNow, Salesforce, etc.) this requires an API that implements the SCIM protocol.



From [Understand how Application Provisioning in Azure Active Directory | Microsoft Docs]

This is very good news if you too are not only wanting to eliminate costly manual onboarding costs, but also meet compliance and licensing optimisation mandates. However, while applications are increasing publishing APIs, many do not yet support SCIM, and some do not have this on their product roadmap at all. Furthermore many business-critical applications are still on premises with limited integration options, and while they may be considered legacy and you have plans to deprecate, this takes precious time and resources. From an enterprise perspective, no SCIM support is obviously a deal breaker for App Provisioning.

Thanks to **UNIFYConnect**, however, you don't have to wait any longer - let our technology integrate using options are possible today (whether that's REST, WS, SQL or even file based), and let us broker SCIM for you. And all without adding to your on-premises footprint by leveraging your existing Microsoft AAD Connect infrastructure.

Of course there are other on prem identity integration options, and you may already have technology at least partially fulfilling this role today. Over the years UNIFY has architected and built many solutions where the integration point is

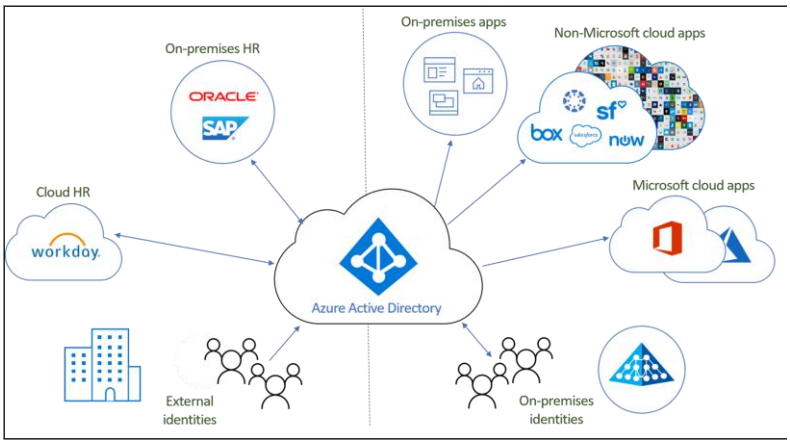
another identity platform such as Microsoft Identity Manager (MIM and its forerunners MIIS/ILM/FIM). Typically such integrations have been built using the same underlying **UNIFYConnect** technology but using a different API gateway protocol (e.g. LDAP). Today, those same integrations can be unplugged from MIM and plugged into Azure using the above App Provisioning model, essentially by simply interchanging the LDAP gateway with a SCIM one. This way **UNIFYConnect** allows you to transition existing integration to Azure App Provisioning.

Azure Identity Governance (IGA)

When it comes to meeting Compliance, Security and Audit requirements for Azure identity, Azure IGA's Entitlements Management suite (for P2 licensed users) is the "cherry on top". It provides the request based access, access review and now segregation of duty features necessary to ensure the right access at the right time for Azure AD fronted application access.

With Identity Lifecycle Management in place (for HR provisioned identities now driving modern Azure authentication and access services beyond Azure itself where SCIM support exists) we now have the solid foundation required for Azure Identity Governance (IGA).

But how can Azure IGA deliver the outcomes required of an organisation where many of its apps either on premises or in the cloud …



From [What is identity lifecycle management with Azure Active Directory? | Microsoft Docs]

- still authenticate and authorize users with on premises AD?
- do not yet support SCIM?
- require on-premises AD access for external (e.g. vendor) accounts which are not and probably can never be mastered in your HR system?
- require the ability to auto-assign access based on HR-sourced attributes (ABAC)?

In each of the above scenarios, **UNIFYConnect** provides an answer today:

- by syncing group membership back to on-premises AD
- by brokering SCIM (as explained earlier) or syncing group membership beyond Azure AD (including back to on-premises AD)
- by provisioning and synchronizing Azure AD guest accounts (and associated group membership) back to on-premises AD
- by providing a working ABAC support model while this feature evolves natively in Azure IGA

While on-premises sync back from Azure AD is also supported by MIM, **UNIFYConnect** delivers the same functionality today without adding any further on-premises "technical debt".

B2B Guest Provisioning

Where no authoritative source exists for an identity in your HR system, a solid alternative for vendors, partners and suppliers can be provided by establishing a B2B trust with the 3rd party organisation to streamline onboarding. By then overlaying IGA, B2B Guest policy can be used for controlling access post on-boarding, thereby enabling Access Reviews and a degree of lifecycle management afforded to HR-sourced identities. This can include assigning guests to org units and managers within the trusting organisation.

However, where guest onboarding and lifecycle management is required for on premises guest access, Microsoft guidance once again turns to MIM. **UNIFYConnect** provides the same functionality to provide this same capability today, again without adding any further unwanted on-premises footprint.