Using Okta for Hybrid Microsoft AAD Join

Cloud or On-premise? You Probably Need Both.

okta

The New Normal: Hybrid Domain Join

Suddenly, we're all remote workers. Everyone. Purely on-premises organizations or ones where critical workloads remain on-prem, can't survive under shelter in place. And most firms can't move wholly to the cloud overnight if they're not there already. So? Everyone's going hybrid. Remote work, cold turkey. It's now reality that hybrid IT, particularly hybrid domain join scenarios, is the rule rather than the exception.

As we straddle between on-prem and cloud, now more than ever, enterprises need choice. They need choice of device — managed or unmanaged, corporate-owned or BYOD, Chromebook or MacBook, and choice of tools, resources, and applications. And they also need to leverage to the fullest extent possible all the hybrid domain joined capabilities of Microsoft Office 365, including new Azure Active Directory (AAD) features.

As the premier, independent identity and access management solution, Okta is uniquely suited to do help you do just that. By adopting a hybrid state Okta can help you not only move to the cloud for all your identity needs, but also take advantage of all the new functionalities that Microsoft is rolling out in AAD.

AAD Domain Join or AD Hybrid Domain Join?

It's rare that an organization can simply abandon its entire on-prem AD infrastructure and become cloud-centric overnight. Rather, transformation requires incremental change towards modernization, all without drastically upending the end-user experience. For this reason, many choose to manage on-premise devices using Microsoft Group Policy Objects (GPO), while also opting for AAD domain join to take advantage of productivity boosting Azure apps and cloud resources like Conditional Access, Windows Hello for Business, and Windows Autopilot. To learn more, read Azure AD joined devices.

Hybrid domain join is the process of having machines joined to your local, on-prem AD domain while at the same time registering the devices with Azure AD. See Hybrid Azure AD joined devices for more information.

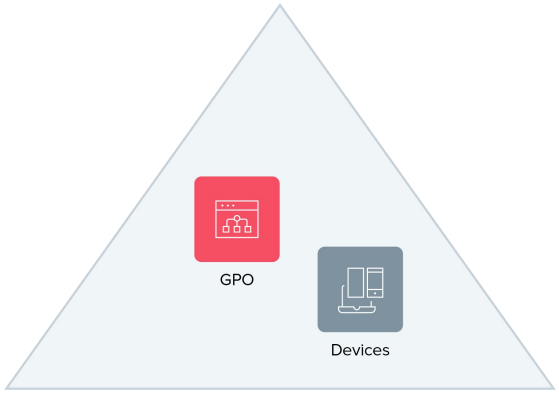
AAD Join Benefits	Hybrid Join Benefits
Device Management via Microsoft Intune	Device Management via GPO
Leverage New Azure Features	Maintain Existing On-prem Investments

The Building Blocks of Hybrid Azure AD Join

Going forward, we'll focus on hybrid domain join and how Okta works in that space. But first, let's step back and look at the world we're all used to: An AD-structured organization where everything trusted is part of the logical domain and Group Policy Objects (GPO) are used to manage devices. What's great here is that everything is isolated and within control of the local IT department. Fast forward to a more modern space and a lot has changed: BYOD is prevalent, your apps are in the cloud, your infrastructure is partially there, and device management is conducted using Azure AD and Microsoft Intune. What were once simply managed elements of the IT organization now have full-blown teams. It's a space that's more complex and difficult to control. So, let's first understand the building blocks of the hybrid architecture.

Active Directory (AD)

Active Directory is the Microsoft on-prem user directory that has been widely deployed in workforce environments for many years. AD creates a logical security domain of users, groups, and devices. Anything within the domain is immediately trusted and can be controlled via GPOs.

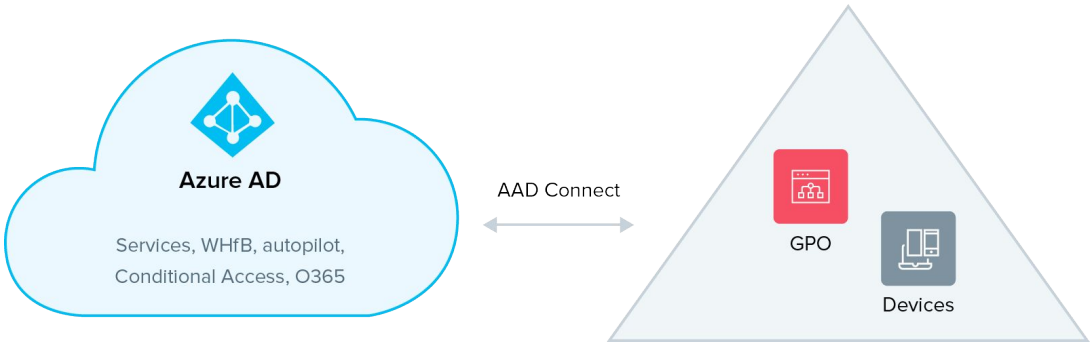


Azure Active Directory (AAD)

Azure AD is Microsoft's cloud user store that powers Office 365 and other associated Microsoft cloud services. In addition to the users, groups, and devices found in AD, AAD offers complementary features that can be applied to these objects. But in order to do so, the users, groups, and devices must first be a part of AAD, much the same way that objects need to be part of AD before GPOs can be applied. AAD interacts with different clients via different methods, and each communicates via unique endpoints. For example, when a user authenticates to a Windows 10 machine registered to AAD, the machine is logged in via an/username13 endpoint; when authenticating Outlook on a mobile device the same user would be logged in using Active Sync endpoints.

Azure AD Connect

Azure AD Connect (AAD Connect) is a sync agent that bridges the gap between on-premises Active Directory and Azure AD. It's responsible for syncing computer objects between the environments. For more info read: [Configure hybrid Azure Active Directory join for federated domains](#).



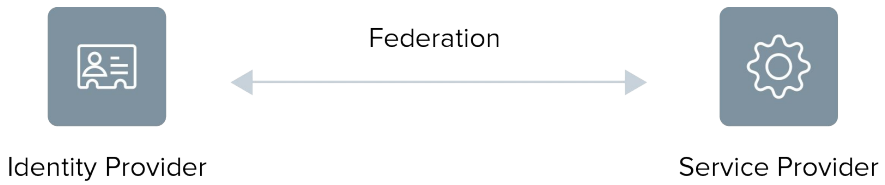
Authentication

There are two types of authentication in the Microsoft space:

- **Basic authentication,** aka legacy authentication, simply uses usernames and passwords. Historically, basic authentication has worked well in the AD on-prem world using the WS-Trust security specification, but has proven to be quite susceptible to attacks in distributed environments.
- **Modern authentication** uses a contextualized, web-based sign-in flow that combines authentication and authorization to enable what is known as multi-factor authentication (MFA). With the end-of-life approaching for basic authentication, modern authentication has become Microsoft's new standard.

Okta Federation

Mapping identities between an identity provider (IDP) and service provider (SP) is known as federation. Connecting both providers creates a secure agreement between the two entities for authentication. In an Office 365/Okta-federated environment you have to authenticate against Okta prior to being granted access to O365, as well as to other Azure AD resources.



A hybrid domain join requires a federation identity. The identity provider is responsible for sending ID information needed to register a device.

Okta Sign-in Policy

Okta sign-in policies play a critical role here and they apply at two levels: the organization and application level. Office 365 application level policies are unique. This is because authentication from Microsoft comes in various formats (i.e., basic or modern authentication) and from different endpoints such as WS-Trust and ActiveSync. Here are some of the endpoints unique to Okta's Microsoft integration.

Type	Endpoint (https://company.okta.com/app/office365/...)	Use	Authentication Type
PassiveLogOnUri	.../sso/wsfed/passive	Login	Modern
ActiveLogOnUri	.../sso/wsfed/active	Login	Basic
LogOffUri	.../sso/wsfed/signout	Sign-out Use Cases	Basic
Username	.../sso/wsfed/username13	Windows 10 Machine Logins	Basic
Windows Transport	.../sso/wsfed/windowstransport	Kerberos-based Logins	Basic

Authentication and Sign On in the Federated Model

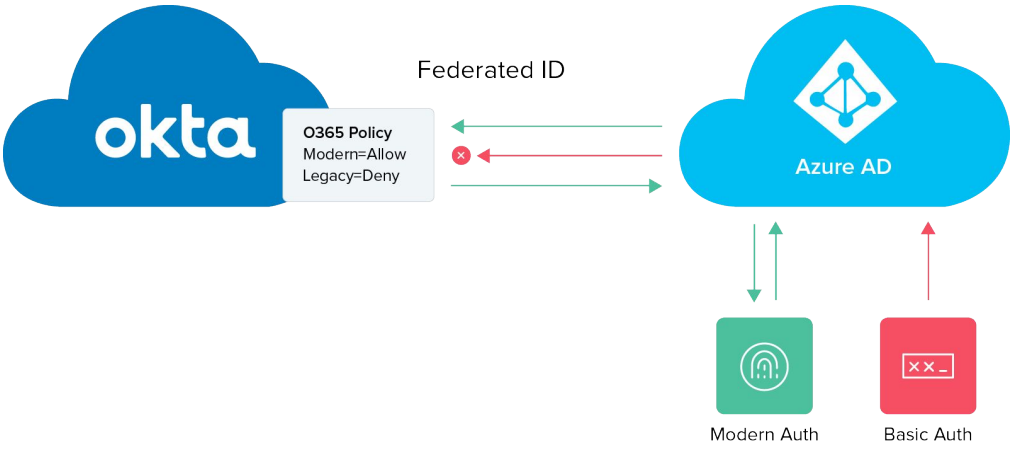
In a federated model, authentication requests sent to AAD first check for federation settings at the domain level. If a domain is federated with Okta, traffic is redirected to Okta. Traffic requesting different types of authentication come from different endpoints. Okta's sign-in policy understands the relationship between authentication types and their associated source endpoints and makes a decision based on that understanding. For example:

Basic Authentication

1. An end user opens Outlook 2007 and attempts to authenticate with his or her user@domainA.com username.
2. AAD receives the request and checks the federation settings for domainA.com.
3. domainA.com is federated with Okta, so the username and password are sent to Okta from the basic authentication endpoint (/active).
4. Okta's O365 Sign On policy sees inbound traffic from the /active endpoint and, by default, blocks it.

Modern Authentication

1. An end user opens Outlook 2016 and attempts to authenticate using his or her user@domainA.com username.
2. AAD receives the request and checks the federation settings for domainA.com.
3. domainA.com is federated with Okta, so the user is redirected via an embedded web browser to Okta from the modern authentication endpoint (/passive).
4. Okta's O365 sign-in policy sees inbound traffic from the /passive endpoint, presents the Okta login screen, and, if applicable, applies MFA per a pre-configured policy.

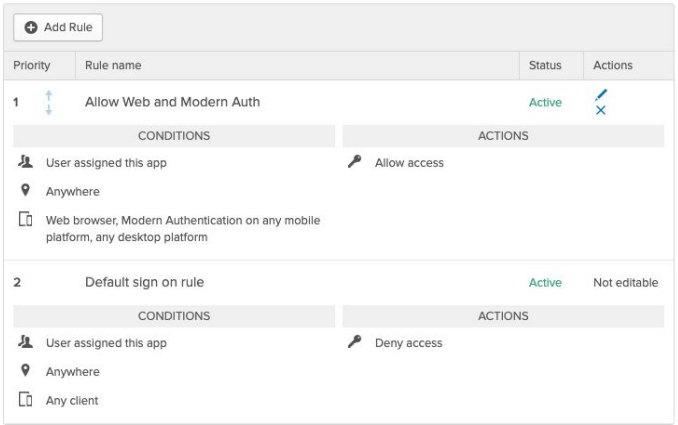


Authentication in the Federated Model

Understanding the Okta Office 365 sign-in policy in federated environments is critical to understanding the integration between Okta and Azure AD. Different flows and features use diverse endpoints and, consequently, result in different behaviors based on different policies.

NOTE: The default O365 sign-in policy is explicitly designed to block all requests, those requiring both basic and modern authentication. The policy described above is designed to allow modern authenticated traffic. (Policy precedents are based on stack order, so policies stacked as such will block all basic authentication, allowing only modern authentication to get through.)

Sign On Policy



Azure Services with Domain Join

Here are a few Microsoft services or features available to use in Azure AD once a device is properly hybrid joined.

Microsoft Intune

Microsoft's cloud-based management tool used to manage mobile devices and operating systems.

Windows Autopilot

Enables organizations to deploy devices running Windows 10 by pre-registering their device Universal Directories (UD) in AAD.

Windows Hello for Business

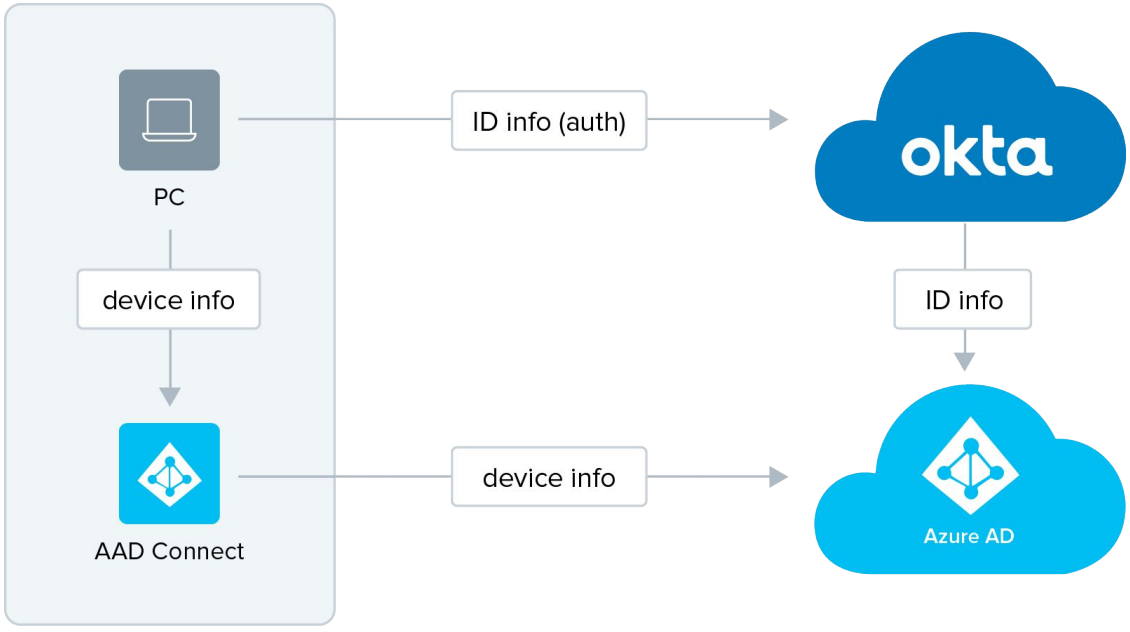
The enterprise version of Microsoft's biometric authentication technology.

Conditional Access Policies

Creates policies that provide if/then logic on refresh tokens as well as O365 application actions.

Putting It All Together in a Hybrid Domain Joined Space

We'll start with hybrid domain join because that's where you'll most likely be starting. You already have AD-joined machines. Now you have to register them into Azure AD. First off, you'll need Windows 10 machines running version 1803 or above. In addition, you need a GPO applied to the machine that forces the auto enrollment info into Azure AD. With everything in place, the device will initiate a request to join AAD as shown here.



Hybrid Domain Join for Existing Computers

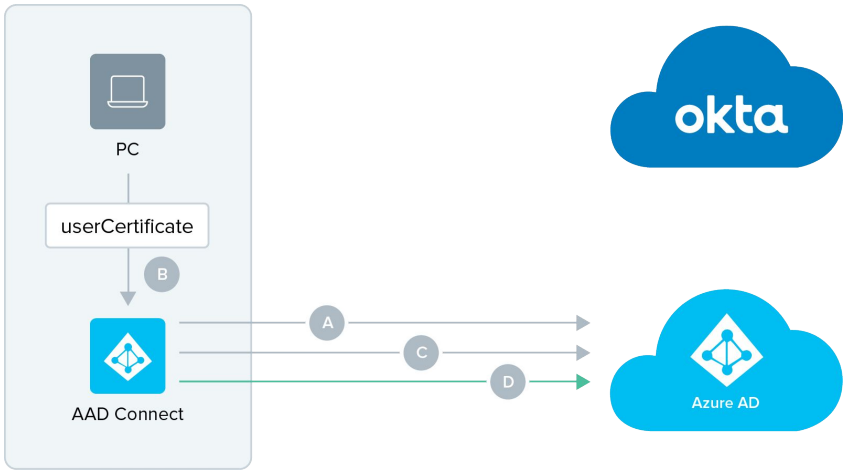
A. The device will attempt an immediate join by using the service connection point (SCP) to discover your AAD tenant federation info and then reach out to a security token service (STS) server. The authentication attempt will fail and automatically revert to a synchronized join.

B. Upon failure, the device will update its userCertificate attribute with a certificate from AAD.

C. On its next sync interval (may vary — default interval is one hour), AAD Connect sends the computer object to AAD with the userCertificate value. The device will show in AAD as joined but not registered.

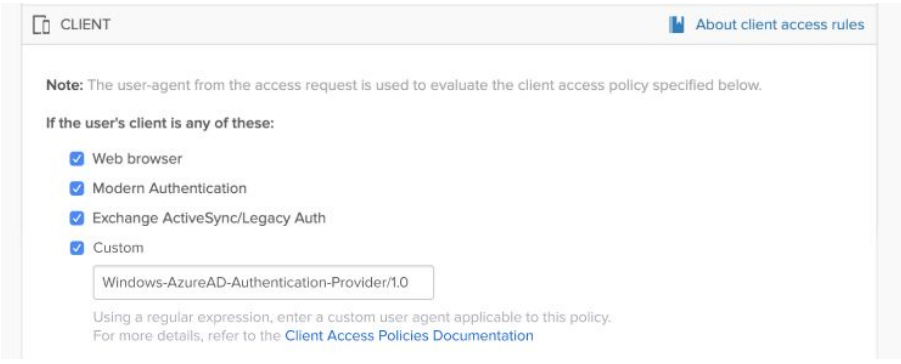
D. Using a scheduled task in Windows from the GPO an AAD join is retried.

E. Since the object now lives in AAD as joined (see step C) the retry successfully registers the device. Congrats!



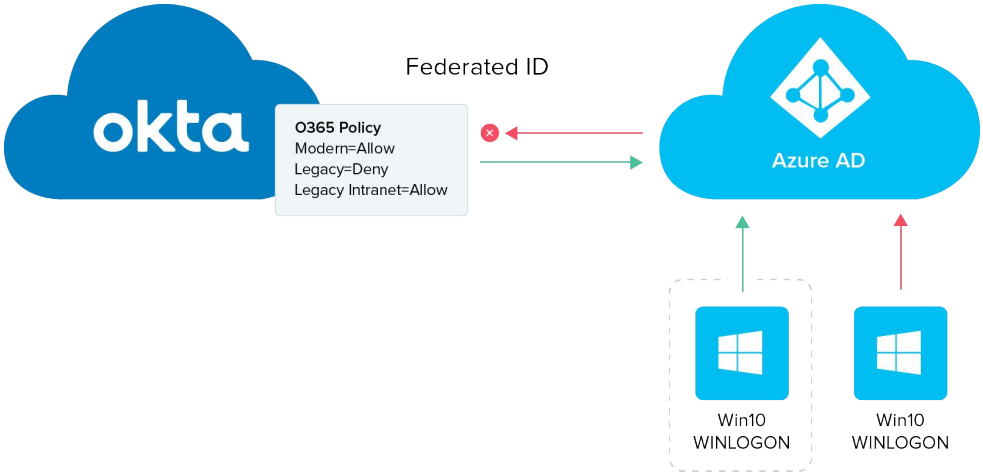
Login to a Windows 10 Hybrid Domain Joined Machine with Okta

Now that your machines are Hybrid domain joined, let's cover day-to-day usage. Daily logins will authenticate against AAD to receive a Primary Refresh Token (PRT) that is granted at Windows 10 device registration, prompting the machine to use the WINLOGON service. Since WINLOGON uses legacy (basic) authentication, login will be blocked by Okta's default Office 365 sign-in policy. Okta provides the flexibility to use custom user agent strings to bypass block policies for specific devices such as Windows 10 (Windows-AzureAD-Authentication-Provider/1.0). Watch our video.



▶ Scan for video

Additionally, a good solution is to disable all Microsoft services that use legacy authentication and adjust the O365 sign-in policy within Okta to allow only legacy authentication within the local intranet. Be sure to review any changes with your security team prior to making them. For a list of Microsoft services that use basic authentication see Disable Basic authentication in Exchange Online. For more information please visit support.help.com.



Your Device Is Now Hybrid AAD Joined. So, What New Things Can You Do?

Deploy device-based Conditional Access

Azure conditional access policies provide granular O365 application actions and device checks for hybrid domain joined devices. Many admins use conditional access policies for O365 but Okta sign-on policies for all their other identity needs. With Okta's ability to pass MFA claims to Azure AD, you can use both policies without having to force users to enroll in multiple factors across different identity stores.

1. Both Okta and AAD Conditional Access have policies, but note that Okta's policy is more restrictive. For example, let's say you want to create a policy that applies MFA while off network and no MFA while on network. In Okta you create a strict policy of ALWAYS MFA whereas in Conditional Access the policy will be configured for in and out of network.

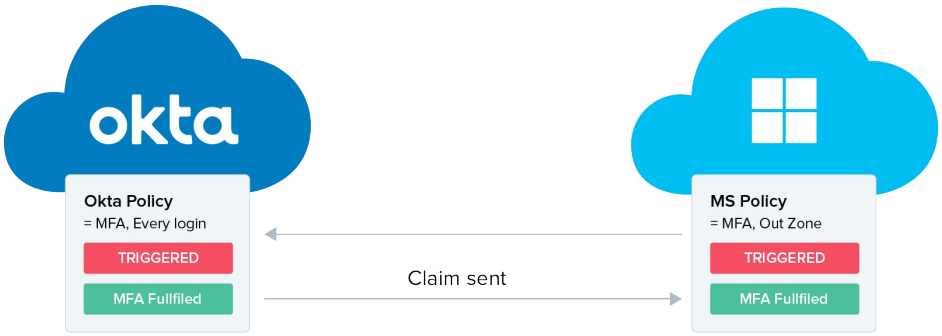
Okta Sign-on Policy	Conditional Access Policy
Every Login=MFA	Off Network=MFA On Network=No MFA

2. When a user moves off the network (i.e., no longer "in zone"), Conditional Access will detect the change and signal for a fresh login with MFA. Since the domain is federated with Okta, this will initiate an Okta login.

3. After Okta login and MFA fulfillment, Okta returns the MFA claim (/multipleauthn) to Microsoft.

4. The MFA requirement is fulfilled and the sign-on flow continues.

For more information read Device-based Conditional Access and Use Okta MFA to satisfy Azure AD MFA requirements for Office 365, and watch our video.



▶ Scan for video

Deploy Windows Hello for Business

For newly upgraded machines (Windows 10 v1803), part of the Out-of-the-Box Experience (OOTBE) is setting up Windows Hello for Business. During Windows Hello for Business enrollment, you are prompted for a second form of authentication (login into the machine is the first). Using Okta to pass MFA claims means that Okta MFA can be used for authorization eliminating the confusion of a second MFA experience. The flow will be as follows:

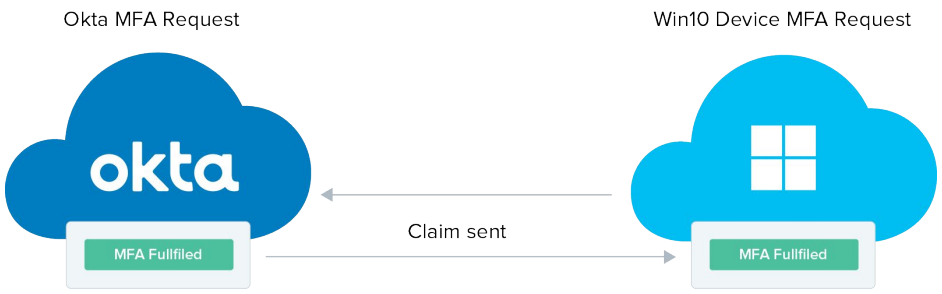
1. User initiates the Windows Hello for Business enrollment via settings or OOTBE.

2. Windows 10 seeks a second factor for authentication. In a federated scenario, users are redirected to Okta based on the domain federation settings pulled from AAD.

3. Okta prompts the user for MFA then sends back MFA claims to AAD.

4. AAD authenticates the user and the Windows Hello for Business enrollment process progresses to request a PIN to complete enrollment.

Using Okta to pass MFA claims back to AAD you can easily roll out Windows Hello for Business without requiring end users to enroll in two factors for two different identity sources. For more information on Windows Hello for Business see Hybrid Deployment and watch our video.

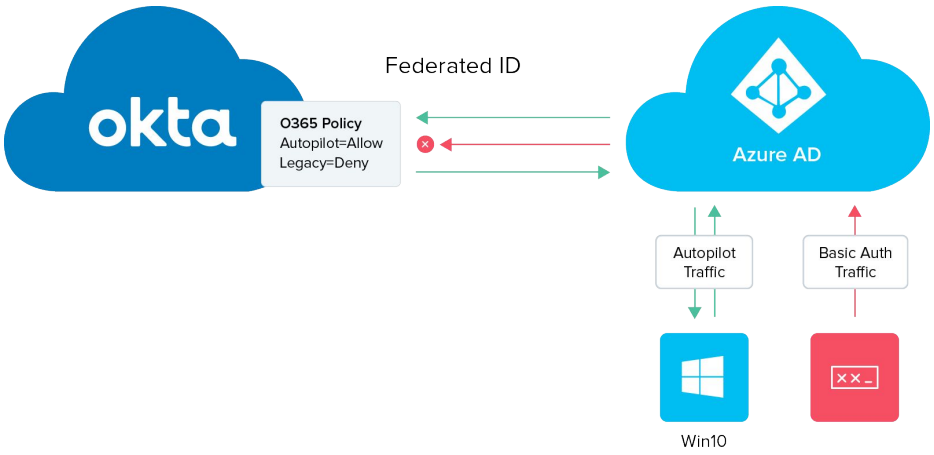


▶ Scan for video

Achieve low-touch device issuance with Windows Autopilot

The imminent end-of-life of Windows 7 has led to a surge in Windows 10 machines being added to AAD. Windows Autopilot can be used to automatically join machines to AAD to ease the transition. If a machine is connected to the local domain as well as AAD, Autopilot can also be used to perform a hybrid domain join.

Okta's Autopilot enrollment policy takes Autopilot traffic (by endpoint) out of the legacy authentication category, which would normally be blocked by the default Office 365 sign-in policy. Breaking out this traffic allows the completion of Windows Autopilot enrollment for newly created machines and secures the flow using Okta MFA. If you're using Okta Device Trust, you can then get the machines registered into AAD for Microsoft Intune management. Watch our video.



▶ Scan for video

Okta and Microsoft Integration: The Best of Both Worlds

One way or another, many of today's enterprises rely on Microsoft. Whether it's Windows 10, Azure Cloud, or Office 365, some aspect of Microsoft is a critical part of your IT stack. At the same time, while Microsoft can be critical, it isn't everything. Most organizations typically rely on a healthy number of complementary, best-of-breed solutions as well.

By leveraging an open and neutral identity solution such as Okta, you not only future-proof your freedom to choose the IT solutions you need for success, you also leverage the very best capabilities that Microsoft has to offer through Okta's deep integrations.

Windows Hello for Business, Microsoft Autopilot, Conditional Access, and Microsoft Intune are just the latest Azure services that you can benefit from in a hybrid AAD joined environment. But they won't be the last. Okta's commitment is to always support the best tools, regardless of which vendor or stack they come from. It's always what's best for our customers — individual users and the enterprise as a whole.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers and customers. With deep integrations to over 6,500 applications, the Okta Identity Cloud enables simple and secure access for any user from any device.

Thousands of customers, including 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn, and News Corp, trust Okta to help them work faster, boost revenue and stay secure. Okta helps customers fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work.

Learn more at: www.okta.com