okta

How to guide: Okta + Windows 10 Azure AD Join

Federating your Office 365 environment with Okta is an easy choice. Okta offers simplified administration and setup, with enhanced lifecycle management features. You can also use Microsoft technologies in combination with Okta to implement a full, enterprise ready solution.

Adoption of Windows 10 is quickly growing in the enterprise, and Microsoft is committed to making Windows 10 an enterprise grade operating system that provides seamless access to corporate resources for end users. With a shift to modern device management, companies are taking advantage of the Azure AD join capability in Windows 10 no longer are you tied to keeping up with GPOs and other Active Directory policies. Azure Active Directory Join, in combination with mobile device management tools like Intune, offer a lightweight but secure approach to managing modern devices.

Let's take a look at how Azure AD Join with Windows 10 works alongside Okta.

First, we want to setup WS-Federation between Okta and our Microsoft Online tenant. A custom domain in the Microsoft Online tenant has already been verified, and with just a click of a button, I'm able to federate with Okta, with no on-premises infrastructure required.



In our Microsoft Online tenant, we've allowed all users to join devices to Azure Active Directory. In this setup, we're requiring multi-factor authentication for Okta sign-ons, and to avoid a double MFA prompt, we won't require multi-factor authentication in the device settings here.

This can be configured in your Azure portal, under Azure Active Directory—Devices—Device Settings.

Devices - Device settings atkodemo - Azure Active Directory		
MANAGE	R Save X Discard	
All devices	Users may join devices to Azure AD O All Selected None	
Device settings	Selected	
ACTIVITY	No member selected	
Audit logs		
TROUBLESHOOTING + SUPPORT	Additional local administrators on Azure AD joined devices Selected None	
★ Troubleshoot	Selected	>
New support request	1 member selected	
	Users may register their devices with Azure AD	
	Learn more on how this setting works	
	Require Multi-Factor Auth to join devices Yes No	
	Maximum number of devices per user	\sim
	Users may sync settings and app data across devices All Selected None	
	Selected No member selected	>

We're also going to configure our Windows 10 devices to automatically enroll to Intune during the Azure AD join process (note that automatic device enrollment requires Azure AD Premium). In the **Azure Portal, go to Azure Active Directory—Mobility (MDM and MAM)**. Here, you will want to set the MDM user scope to users. The options you'll see here are—

- None MDM automatic enrollment disabled
- Some Select the Groups that can automatically enroll their Windows 10 devices
- All All users can automatically enroll their Windows 10 devices

The default URLs were kept for MDM terms of use URL, MDM discovery URL, and MDM compliance URL.

Before continuing, verify that you have enabled Intune for Windows enrollment. In the Azure Portal, head to Intune— Device enrollment—Windows enrollment.

Click on the **CNAME Validation**, and check that your custom domain name is verified. If you see a success message, you're ready to go.

Putting it all together

In the video below, notice that although the Microsoft Online tenant is federated with Okta, Azure AD Join is successful the end user is prompted for Okta MFA & the device is also managed by Intune as a result of the Azure AD join process.

Video – <u>Azure AD Join</u>

And lastly, if we take a look at our list of devices in Azure Active Directory, we can see the device was just joined.

Device	×	
🗗 Manage	e 🗸 Enable 🗴 Disable 🗴 Delete	
Name	WIN10ENT64	
ID	7408e382-e6b4-411b-8afc-13e556078fde	
Enabled	Yes	
OS	Windows	
Version	10.0.16299.15	
Join Type	Azure AD joined	
Owner	Teju Shyamsundar	
User name	teju@atkodemos.com	
MDM	Microsoft Intune	
Compliant	Yes	
Registered	1/29/2018, 5:14:32 PM	
BITLOCKER KEY ID BITLOCKER RECOVERY KEY DRIVE TYPE		
No BitLocker key found for this device		