### How to guide:

Deploy Okta's SWA Plug-In for Microsoft Edge with System Center Configuration Manager and the Windows Store for Business

Okta's Secure Web Authentication (SWA) plug-in for the Microsoft Edge browser offers a seamless login experience to applications that do not support federated single sign on. When you enable SWA for an app, end users see a link below their app icon on their My Applications page. Selecting the link enables them to set up and update their credentials for that app. Okta stores the end user's credentials in an encrypted format using strong AES encryption combined with a customer-specific private key. When end users click an application icon, Okta securely posts their credentials to the app login page over SSL and the user is automatically signed in.

We have introduced a Secure Web Authentication plug-in for the Windows Edge browser, which can be downloaded via the Microsoft Store: <u>Okta Secure Web Authentication Plug-In.</u>

For customers using the Windows Store for Business integration with System Center Configuration Manager, this guide outlines how to deploy the Secure Web Authentication plug-in for Edge via the Windows Store for Business integration. Integrate the Windows Store for Business with System Center Configuration Manager and deploy Okta Secure Web Authentication Plug-In as an "Online" install

**Note:** The Okta Secure Web Authentication plug-in is an Online licensed application. Please see the requirements on <u>Microsoft's documentation</u> for device management options to install Online licensed applications when using the Windows Store for Business with Configuration Manager.

#### Step 1 — Enable your System Center Configuration Manager site for pre-release features and add the Windows Store for Business feature

The first thing that you will want to do is enable the site for pre-release features.

 In Configuration Manager, navigate to Administration—Site Configuration—Sites. Choose the top-level site in your hierarchy, and choose Hierarchy Settings across the top ribbon.



 Check the box for Consent to use Pre-Release Features. This will allow you to turn on the Windows Store for Business Integration feature in the next step.

✓ Consent to use Pre-Release features By checking this box, you agree to the use of pre-release features that might be included in Configuration Manager for early testing. Pre-release software might not work the same way as a production-ready version of the software. It is also possible that pre-release software mains pre-release only, and will not be included as a production-ready feature. The consent to use pre-release features is a permanent choice that cannot be undore. After consenting to use pre-release features you turn them on in Administration - Overview - Cloud Services - Updates and Servicing.

- Now go to Administration—Updates and Servicing— Features. You will see the Windows Store for Business Integration feature listed here. Choose Turn On.
- You will be notified that the feature will be replicated and enabled across all site servers in your System Center Configuration Manager hierarchy. Click OK if you want this feature to be enabled on all site servers.

Passport for Work		Release
Switch Software Update Point		Release
Windows Store for Business Integration	Turn on	se
Windows 10 device health attestation support	Turn on	nercose
VPN for Windows 10		Release



 After re-opening the Configuration Manager console, you'll see the Windows Store for Business node available under Administration—Cloud Services.

After the Windows Store for Business feature has been activated in your Configuration Manager site, you will need to register Configuration Manager as a web application management tool for the Store for Business. This is done using the Azure portal, and will allow for Windows Store for Business apps to sync to Configuration Manager.

## Step 2 — Add Configuration Manager as a web application management tool

- In your browser, go to <u>https://portal.azure.com</u>.
   Find the Azure Active Directory node on the left.
   Click on Enterprise Applications.
- Choose the option for New Application, and under the Add your own app section, choose Application you're developing.
- Choose New Application Registration and enter the following:



Register an app you're working on to integrate it with Azure AD

Name (you will use this in the Store for Business later) Application Type: Web Application/Web API Sign-on URL: This can be any URL and doesn't need to resolve to an external address (for example, https://atkodemotest.com/sccm)

 Go ahead and choose
 Create the application.
 We'll need to note down the ApplicationID and Key associated with the app. Click on Properties, and note down the value for ApplicationID.
 We will need to enter this into Configuration Manager later.

Properties	□ ×
R Save X Discard	
* Name 0	
WSfB-SCCM	
Object ID 🖲	
Application ID 0	
* App ID URI 🛛	
https://atkocorp.onmicrosof	t.com/d0f181b0
Logo	
WS	
Select a file	
Home page URL 0	
https://atkocorpsccm.com/se	ccm
Logout URL	
Application type	
Web app / API	
Multi-tenanted 0	

 Go back one page to the Settings for this app, and under the API Access section, choose Keys.

API A	CCESS	
ሔ	Required permissions	>
Ŷ	Keys	>

 Enter a description and expiration & choose Save. The key value will be displayed now—note this value down as we will need to enter it to Configuration Manager later.

A	pp registrations	> WSfB-SCCM	> Settings >	Keys	${\cal P}$ Search resources, services and docs	<b>₽</b>
	Keys					
	Save	🗙 Discard				
	DESCRIPT	ION	EXPIRES	VAL	UE	
	WSfb-SC	CM	12/31/2299	Hid	den	

The next step is to add Configuration Manager as a management tool in the Windows Store for Business.

# Step 3 — Add System Center ConfigurationManager as a management tool in the WindowsStore for Business

- Login to the Windows Store for Business at <u>https://www.microsoft.com/en-us/business-store</u>.
- Go to Manage—Settings—Distribute. You'll see a Management tools section here. Choose Add management tool.



 Type in the name of the web application that you had created in Azure earlier and click Add

hese settings allow you to configure a mobile device	management (MDM) tool to synchronize your Microsoft Store	for Business invento
rick a tool from the list to activate. s your tool not on the list? Make sure it's in your Azur set more info	re Active Directory. Still not there? Select Add management to	ool below.
+ Add management tool		
Tool	Status	Action
AirWatch by VMware	Inactive	Activate
	Inactive	Activate
Microsoft Intune	mactive	

4. Make sure you click Activate next to the application, or the upcoming steps will result in errors.

Note: only one management tool can be active at a time, so if you already have another management tool activated, it will need to be deactivated before going through the next steps.

The next step is to add applications to your private store in the Windows Store for Business, so that those applications can sync with Configuration Manager. In this case, we'll add the Okta Secure Web Authentication Plug-In.

## Step 4 — Add the Okta Edge Extension to your private Windows Store for Business

- In the Windows Store for Business portal, click on Shop for my group in the top right.
- 2. Search for the application you want to install—in this case it is *Okta Secure Web Authentication Plug-In*.



3. Click on **Get the app**. You'll also see a note that this app is an extension for Microsoft Edge.

0	Okta Secure Web Authentication Plug-in Okta Inc. ***** (7)
	Install     This product is an extension for Microsoft Edge May require certain hardware. See <u>System Requirements</u> for details.

4. You'll see a notification that the extension has been added to your inventory.



Next, click the initial button and choose Add to private store. You will see a notification that adding this app to the private store could take up to 36 hours.



Now you can head back to Configuration Manager, where we will finalize the integration.

## Step 5 — Complete the Windows Store forBusiness Integration with Configuration Manager

 Go to Administration—Cloud Services—Windows Store for Business. Choose the option to Add Windows Store for Business Account.



- Enter your Microsoft tenant ID(xyz.onmicrosoft.com) and the ApplicationID and client key from the Azure Active Directory application which was created earlier. Also, specify a location to which Offline Windows Store for Business applications will be downloaded (this should be a UNC path accessible by the server). Complete the setup wizard.
- In the console, you'll see an entry for your Windows Store for Business account. You can now right click on the account and choose the option to Sync from Windows Store for Business.

Windo	ws Store for Business 1 items					
lcon	Tenant ID	Client ID	Last Sync Status	Last Sync Time	Last Successful Sync Time	Content Location
	atkocorp.onmicrosoft.com	4f6437	Succeeded	10/19/2017 4:4	10/19/2017 4:41 AM	\\ATKOCORPSCC

 When the sync is complete, go to Software Library– Application Management–License Information for Store Apps, you will see all the applications from your private Store for Business inventory

lcon	Name	Publisher	License Ty
	AdBlock	BetaFish	Online
	Evernote Web Clipper	Evernote	Online
	Excel Mobile	Microso	Online
	Fresh Paint	Microso	Online
	Microsoft Power Bl	Microso	Online
	Okta Secure Web Authentication Plug-in	Okta Inc.	Online
	Okta Verify	Okta Inc.	Online
	OneNote	Microso	Online

Now we can go ahead and create and deploy the Okta Secure Web Authentication Plug-In. Step 6 — Create and deploy the Okta Secure Web Authentication Plug-In with Configuration Manager

 Right click on the Okta Secure Web Authentication Plug-In, and choose Create Application. Follow the application wizard to complete create the application for the Okta Secure Web Authentication Plug-In.

Store) trie.         Details:         Application name: Okta Secure Web Authentication Plug+in Publisher: Okta Inc.         OS max version:         03 max version:         05 max version:         05 max version:         05 may version:         06 poment type name: Windows Store BSPDeeplinkDT_Okta Secure Web Authentication Plug+in -         Windows app package (in the Windows Store)         Detection:         Detection:         Name: B0724843 Okta Secure:         Version:         Publisher:         Publisher:         10:84p6ma6k07gm22	Application	information	ation	the Windows app pack	kage (in the	e Windows	
Details:         Application name: Okta Secure Web Authentication Plug+n         Software version:         OS max version tested: 100.14361.0         OS max version:         Description:         Deployment type name: WindowsStoreBSPDeepinkDT_Okta Secure Web Authentication Plug+n-Windows app package (in the Windows Store)         Detection Method:         Name: B07:04843 Okta Inc.         Version*         Publisher Okta Inc.         Version*         Publisher ID: 84p6na6k/7gm22	Store) file.						
Application name: Okta Secure Web Authentication Plug+in Publisher: Okta Inc. Software version: 100.14361.0 OS min version: 100.14361.0 OS min version: 100.14361.0 Deployment type name: WindowsStoreBSPDeeplinkDT_Okta Secure Web Authentication Plug+in - Windows app package (in the Windows Store) Detection Method I Name: ID0:24843 Okta Secure Web AuthenticationPlug+in Publisher: Okta Inc. Version I Publisher ID: 84p6na6k7gm22	Details:						
	Publisher: Okta Inc. Software version: OS max version test OS min version: 10. Description: Deployment type na Windows app pack Detection Method	ed: 10.0.1 0.14361.0 me: Wind age (in the	14361.0 owsStoreBSPDeeplinkDT e Windows Store)	Okta Secure Web Auth	entication F	Plug-in -	
	Name 807C4843 O Publisher Okta Inc. Version: Publisher ID:84p6n To modify any details application, click Ca	kta Secure a6x7gm22 s from the ncel.	WebAuthenticationPlug-in	Next. To exit this wizard	without cre	ating the	~
are Library 4 Applications 2 items	Name B07C4843 0 Publisher CAta Inc. Version I Publisher ID:84p6m Publisher ID:84p6m To modify any details application, click Ca	kta Secure a6x7gm22 s from the ncel.	WebAuthenticationPlug-in	Next. To exit this wizard	without cre	tating the	~
(*) * [2] (*) Some Unity * Verene * Application medgement, * Applications * see Ubarry < Applications 22 tems Dearbox	Name B07C4843 O Publisher Okta Inc. Version, Publisher ID: 84p6na To modify any details application, click Ca Compared States Compared States Forward	kta Secure a6x7gm22 s from the ncel.	WebAuthenticationPlug-in	Next. To exit this wizard	without cre	vating the	Add Ci
You like ' monetarian' apparation anggineen ' regeneration '     Add Co     Add Co	Name B07C4843 0 Publisher CKta Inc. Version I Publisher ID:84p6m Publisher ID:84p6m To modify any details application, click Ca	kta Secure s from the ncel.	WebAuthenticationPlug-in	Next. To exit this wizard	without cre	ating the	V Add Ci
Image: Constraint of the second of	Name B07C4843 0 Publisher Okta Inc. Version: Publisher ID:84p6na To modify any details application, click Ca **********************************	kta Secure sform the ncel.	WebAuthenticationPlug-in	Next. To exit this wizard	without cre	ating the	V Add Cr
Application     Anote     Active	Name B07C4843 0 Publisher CK1a Inc. Version I Publisher ID: 84p6n Publisher ID: 84p6n To modify any details application, click Ca	kta Secure s from the ncel.	WebAuthenticationPlugrin	Next. To exit this wizard	Deployments 0	ating the	V Add Ci
Add Color Stars Service S	Name B07C4843 0 Publisher/Okta Inc. Version: Publisher ID:84p6n To modify any details application, click Ca	kta Secure a6x7gm22 s from the ncel.	WebAuthenticationPilugrin	Next. To exit this wizard	Deployments 1 0	ating the	V Add Ci

2. The application you just created will be in the top-level **Applications** node in the console.

🗲 🔶 * 📰 🔪 + Software Library +	Over	view +	Application Management + Applications +				• 2
Software Library	4	Applie	ations 2 items				
* @ Overview		Search				X P Search	Add Criteria *
# 🧾 Application Management	- 11	loon	Name	Deployment Types	Deployments	Status	
* 🕞 Applications		83	AdBlock	1	1	Active	
Microsoft Edge Extensions Maft Stove Apps		1	Adio - Okta Secure Web Authentication Plug-in	1	0	Active	

 Now we can deploy the Okta Secure Web Authentication Edge extension to a Windows 10 machine. Right click on the Okta Edge extension, Deploy, and choose a collection to which this application will be deployed. Follow the deployment wizard to complete the deployment, just as you would for any other Configuration Manager application deployment.

	and any and the rear and a data in a gain	Browse
Collection:	All Windows 10	Browse
Use default distrib	ution point groups associated to this collection	
Automatically dist	ribute content for dependencies	
Comments (optional):		
		·

General	0				
Content	Specify se	ettings to control now tr	is software is	deployed	
Deployment Settings					
Scheduling	Action:	Install		~	
User Experience	Purpose:	Available		~	
immary					
oaress					
mpletion	riequire a	administrator approval it users requ	est this application		





Now you can install the Okta Secure Web Authentication Plug-In extension on your Windows 10 machines.