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: Okta Secure Web Authentication Plug-In.

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.

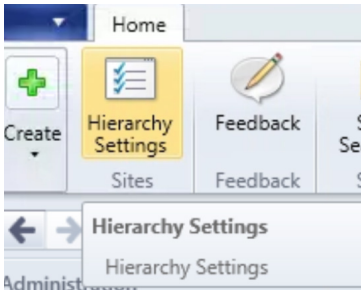
Integrate the Windows Store for Business with System Center Configuration Manager and deploy Okta Secure Web Authentication Plug-In as an "Online" install

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

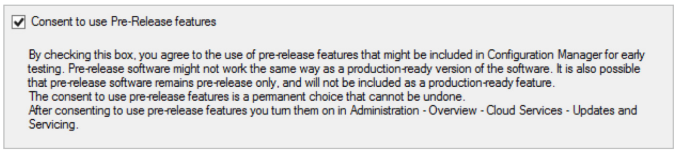
Step 1 — Enable your System Center Configuration Manager site for pre-release features and add the Windows Store for Business feature

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

1. 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.

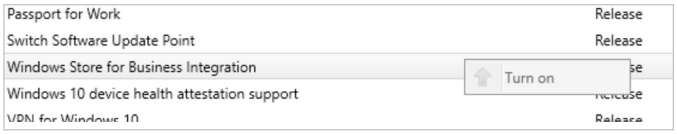


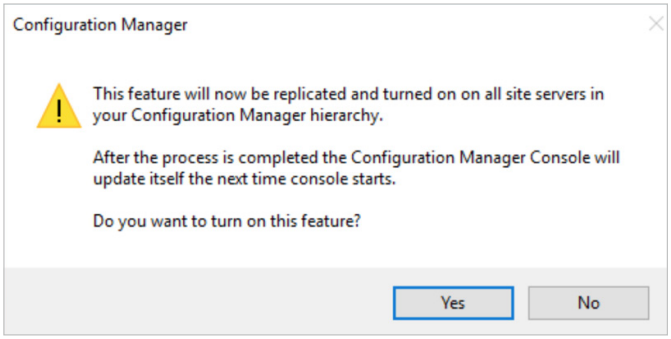
2. Check the box for **Consent to use Pre-Release Features.** This will allow you to turn on the Windows Store for Business Integration feature in the next step.



3. Now go to **Administration—Updates and Servicing—Features.** You will see the Windows Store for Business Integration feature listed here. Choose Turn On.

4. 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.





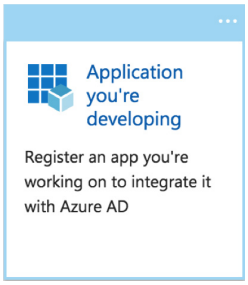
5. After re-opening the Configuration Manager console, you'll see the Windows Store for Business node available under **Administration—Cloud Services.**

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

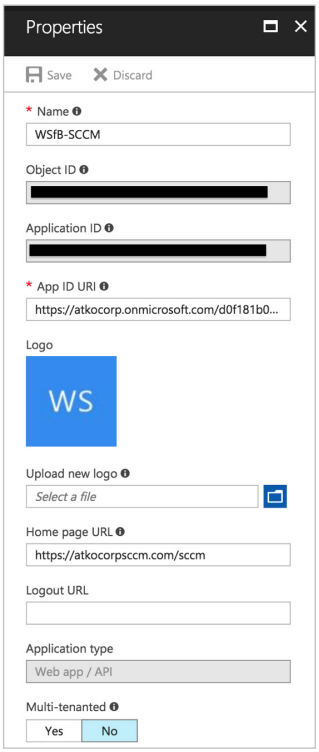
1. In your browser, go to https://portal.azure.com. Find the **Azure Active Directory** node on the left. Click on **Enterprise Applications**.

2. Choose the option for **New Application**, and under the Add your own app section, choose **Application you're developing**.



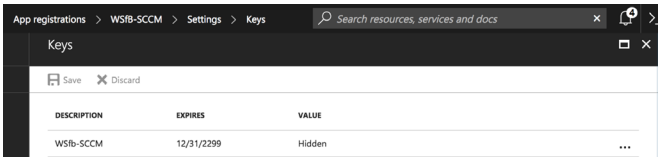
3. Choose **New Application Registration** and enter the following:
Name (you will use this in the Store for Business later)
Application Type: Web Application/Web API
Sign-on URL: This can be any URL and doesn't need to resolve to an external address (for example, https://atkodemotest.com/sccm)

4. 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.



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

6. 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.

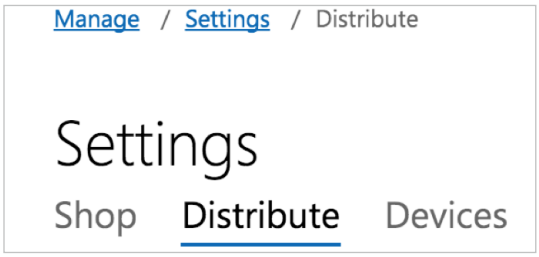


The next step is to add Configuration Manager as a management tool in the Windows Store for Business.

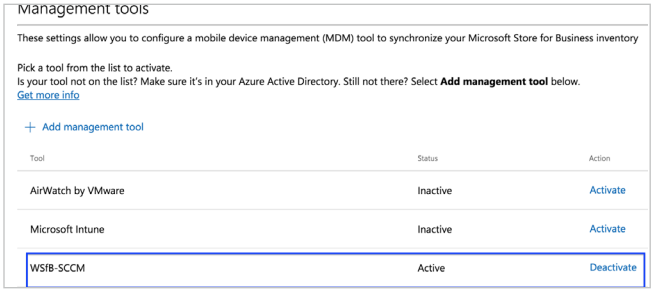
Step 3 — Add System Center Configuration Manager as a management tool in the Windows Store for Business

1. Login to the Windows Store for Business at https://www.microsoft.com/en-us/business-store.

2. Go to **Manage—Settings—Distribute**. You'll see a Management tools section here. Choose **Add management tool**.



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



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

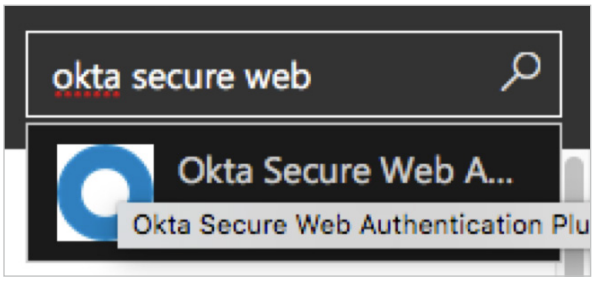
   Note: only one management tool can be active at a time, so if you already have another management tool activated, it will need to be deactivated before going through the next steps.

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.

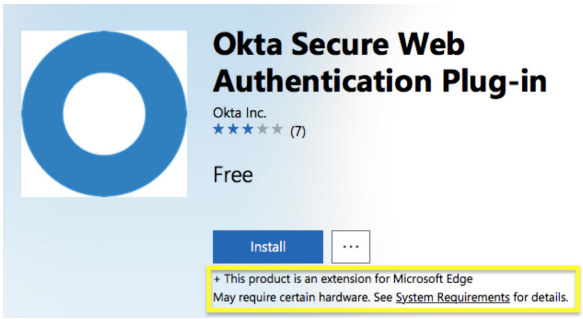
Step 4 — Add the Okta Edge Extension to your private Windows Store for Business

1. In the Windows Store for Business portal, click on **Shop for my group** in the top right.

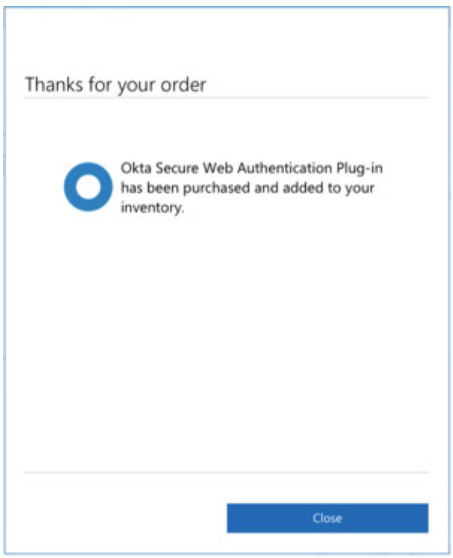
2. Search for the application you want to install—in this case it is *Okta Secure Web Authentication Plug-In*.



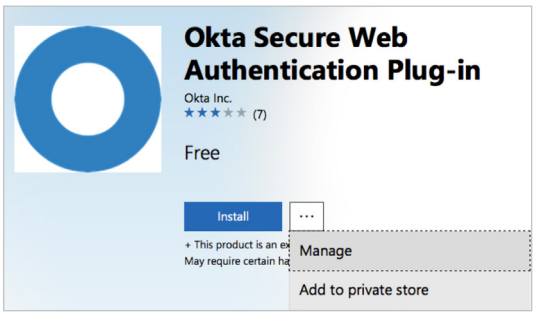
3. Click on **Get the app**. You'll also see a note that this app is an extension for Microsoft Edge.



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



5. Next, click the ··· 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.



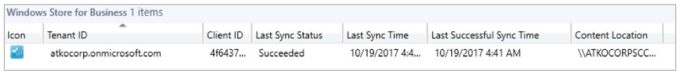
Now you can head back to Configuration Manager, where we will finalize the integration.

Step 5 — Complete the Windows Store for Business Integration with Configuration Manager

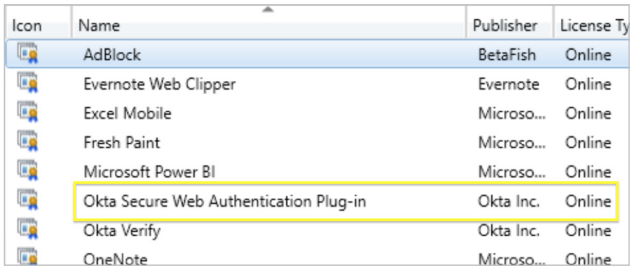
1. Go to **Administration—Cloud Services—Windows Store for Business**. Choose the option to **Add Windows Store for Business Account**.

2. 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.

3. 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.**



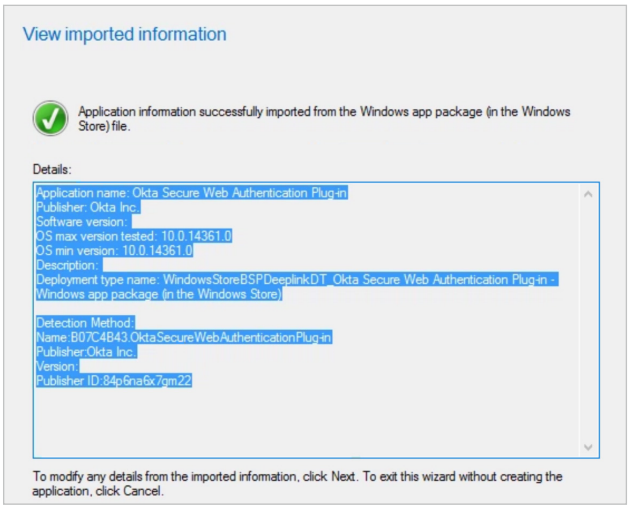
4. When the sync is complete, go to **Software Library—Application Management—License Information for Store Apps,** you will see all the applications from your private Store for Business inventory

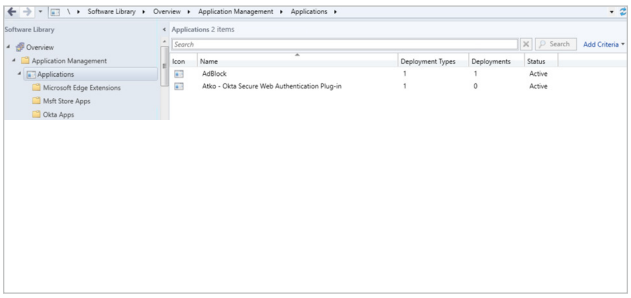


Now we can go ahead and create and deploy the Okta Secure Web Authentication Plug-In.

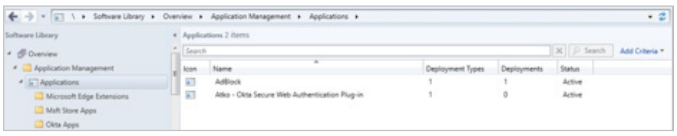
Step 6 — Create and deploy the Okta Secure Web Authentication Plug-In with Configuration Manager

1. 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.

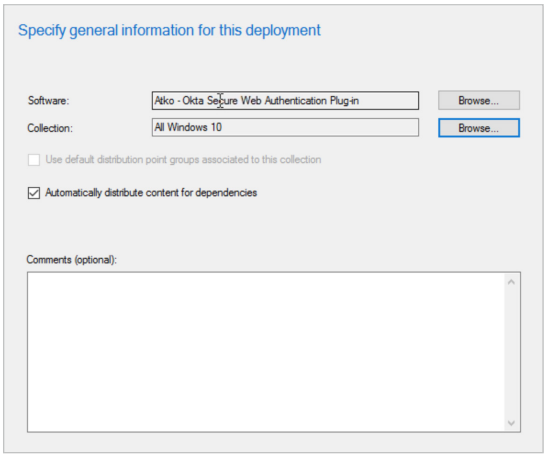


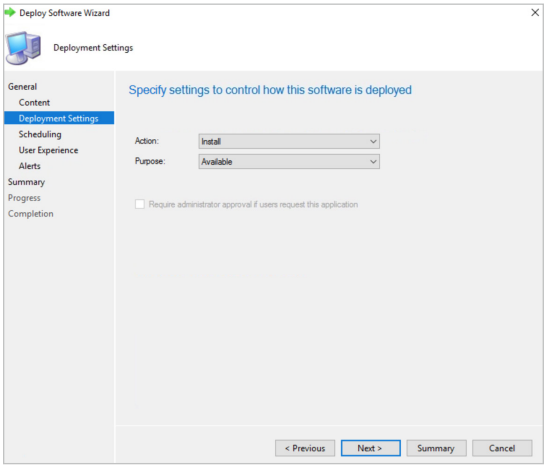


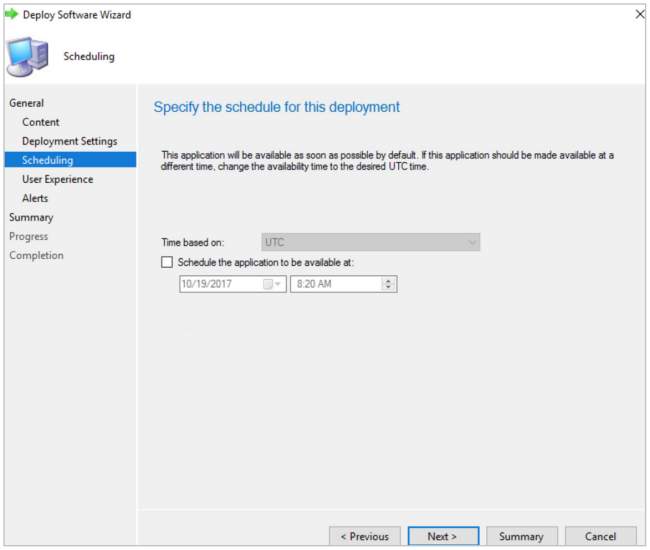
2. The application you just created will be in the top-level **Applications** node in the console.

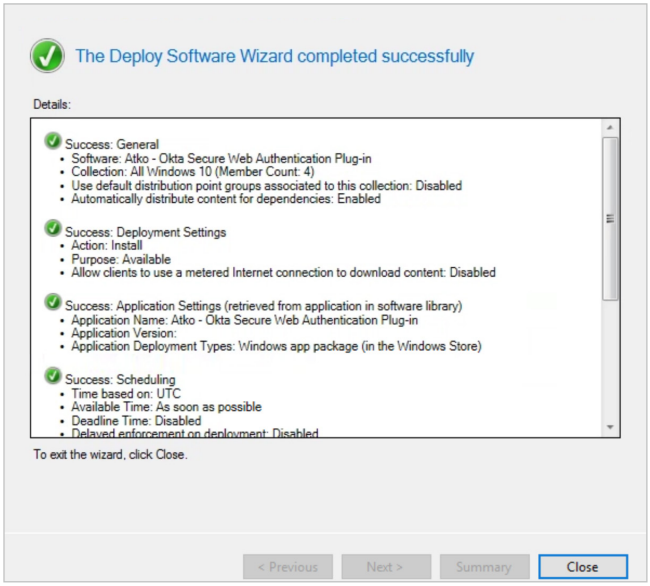


3. Now we can deploy the Okta Secure Web Authentication Edge extension to a Windows 10 machine. Right click on the Okta Edge extension, **Deploy**, and choose a collection to which this application will be deployed. Follow the deployment wizard to complete the deployment, just as you would for any other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









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