

How to guide:

Deploy the Okta Secure Web Authentication Plug-In for Microsoft Edge via the System Center Configuration Manager App Model

Okta’s Secure Web Authentication plug-in for Microsoft Edge 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 Edge which can be downloaded via the Microsoft Store—[Okta Secure Web Authentication Plug-In](#).

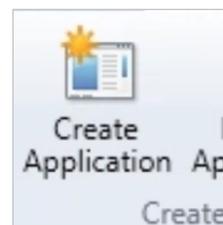
The guide below outlines how you can use the System Center Configuration Manager application model to deploy the Okta Secure Web Authentication Plug-In for Microsoft Edge.

Step 1 — Create the Okta Secure Web Authentication Plug-In app

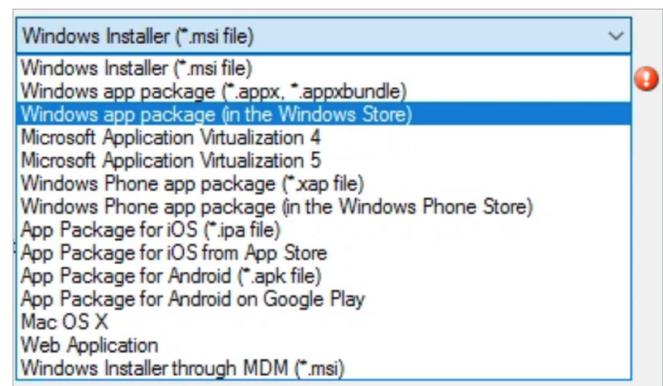
1. In the System Center Configuration Manager console, go to **Software Library—Application Management—Applications**.



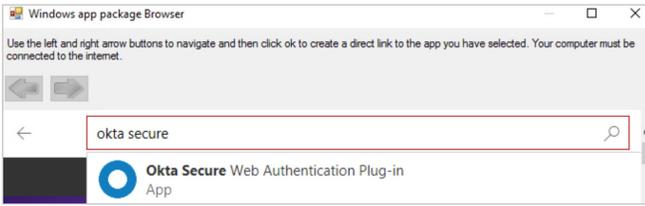
2. Click on **Create Application**.



3. In the Type dropdown, choose **Windows app package (in the Windows Store)**.



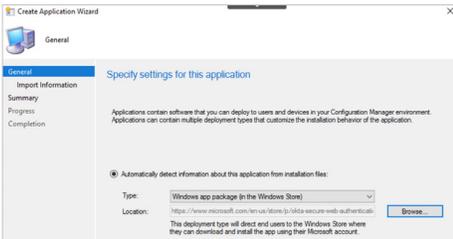
- Click **Browse**. In the Windows app package Browser, search for **Okta Secure Web Authentication Plug-in**.



- A browser window will open here, choose **Get the app**.

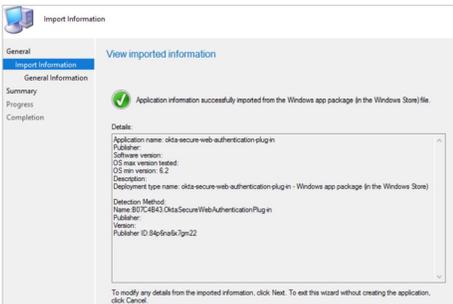


- Close out of the browser window and click **OK**.

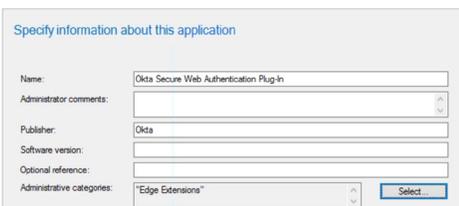


- In the Create Application Wizard, click **Next**.

- On the Import Information page, click **Next**.



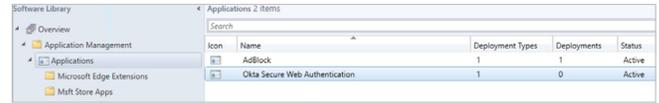
- On the General Information page, choose a Name for the Okta Secure Web Authentication Plug-In. You can also choose to include any of the other optional fields. Click **Next**.



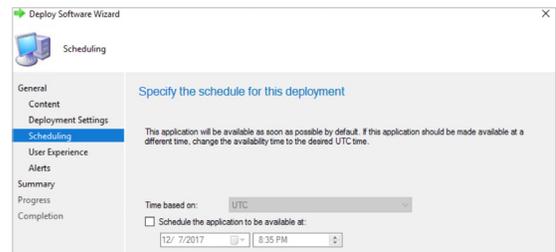
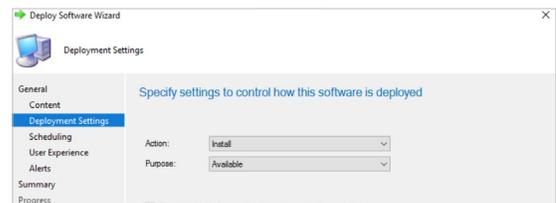
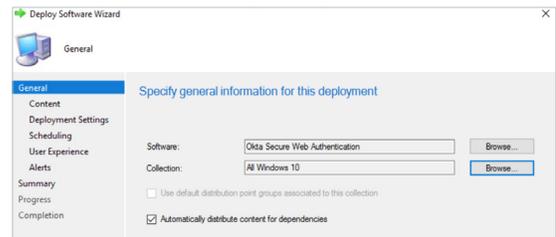
- Click **Next** on the Summary page. Click **Close** on the Completion page.

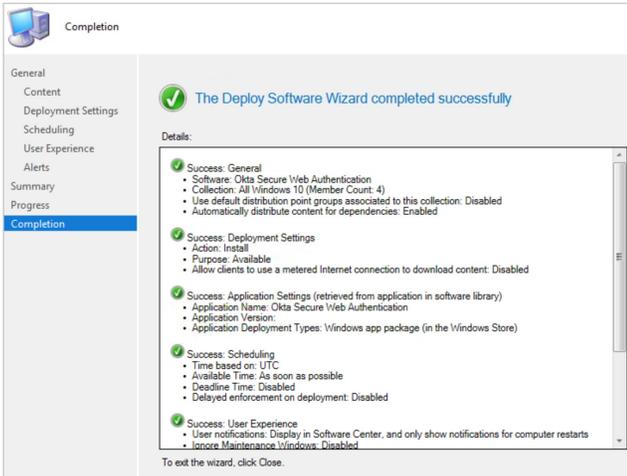
Step 2 — Deploy the Okta Secure Web Authentication Plug-In

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



- Now we can deploy the Okta Secure Web Authentication Plug-In to your Windows 10 machines. Right click on the application, **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.

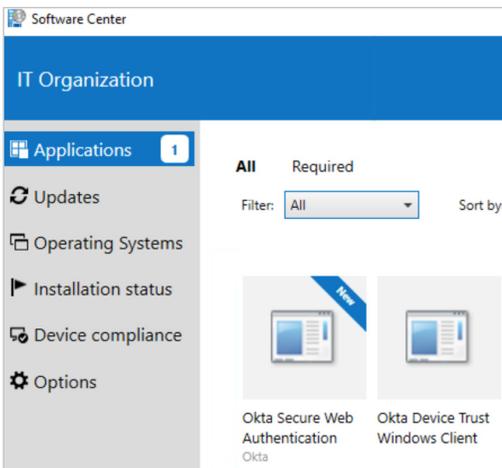




Now we're ready to install the Okta Secure Web Authentication Plug-in to our Windows 10 machines.

Step 3 – Verify the Okta Secure Web Authentication Plug-In Installation on Windows 10

1. Login to a Windows 10 machine that was in the collection that you had deployed the Okta Secure Web Authentication Plug-In to.
2. Open Software Center and you will see the Okta Secure Web Authentication Plug-In.



Note: Depending on your Client Settings in Configuration Manager, the Okta Secure Web Authentication Plug-In may not show up in Software Center yet. To force the client to sync with your Management Point, go to Control Panel & search for **Configuration Manager**. In the **Actions** tab, choose the option for **Machine Policy Retrieval & Evaluation Cycle**.

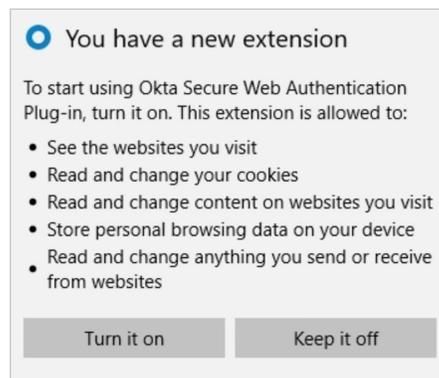
3. If you chose the install type as 'Available', you can initiate the install from Software Center. If you chose the install type of 'Required', the installation should start automatically, after the policy has been evaluated by Configuration Manager for download and install of the Okta Secure Web Authentication extension.
4. During the install process, you will see a Microsoft Store window pop-up. Click **Get** here.



5. When the installation is complete, click the **Launch** button.



6. You will see a notification Edge that indicates the extension was installed. Click **Turn it on**.



7. Log into your Okta org and verify that you can log into SWA applications successfully.