
okta

+


dotcom-monitor®

dotcom-monitor + Okta

Configuration Steps

Create a custom SAML application by using the AIW (Application Integration Wizard)

1. Verify that you are using the Admin Console. If you are using the Developer Console, you need to switch over to the Admin Console. If you see < > Developer Console in the top left corner of your console, click it, then click **Classic UI** to switch.

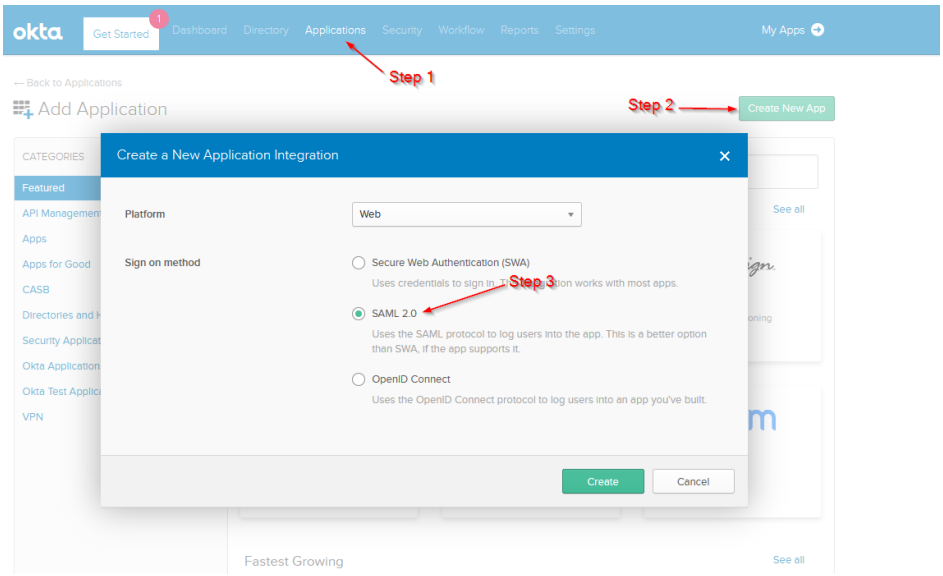
2. In the Admin Console, go to **Applications** > **Applications**.

3. Click **Add Application**.

4. Click **Create New App**.

5. To create a SAML integration, select **Web** as the Platform and **SAML 2.0** for the **Sign on method**.

6. Click Create.

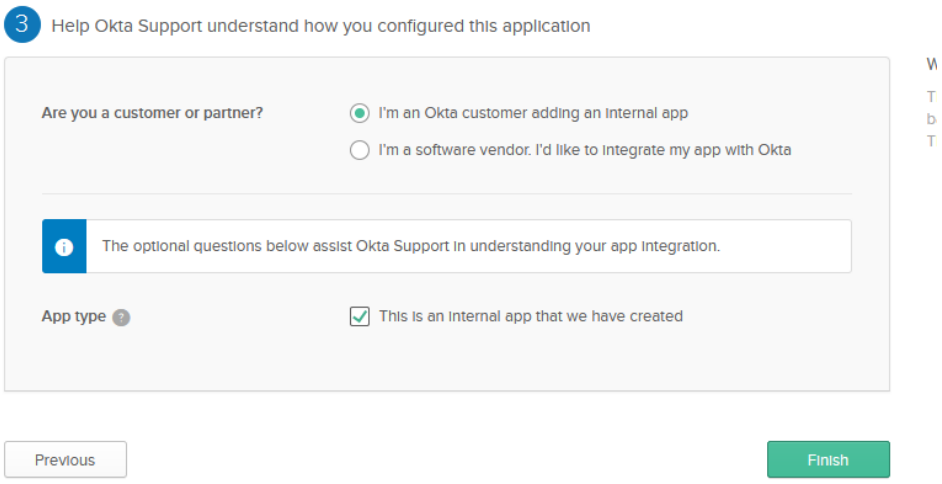


7. Specify a name for your application (ex: dotcom-monitor) and add a logo if required, afterwards hit **Next**.

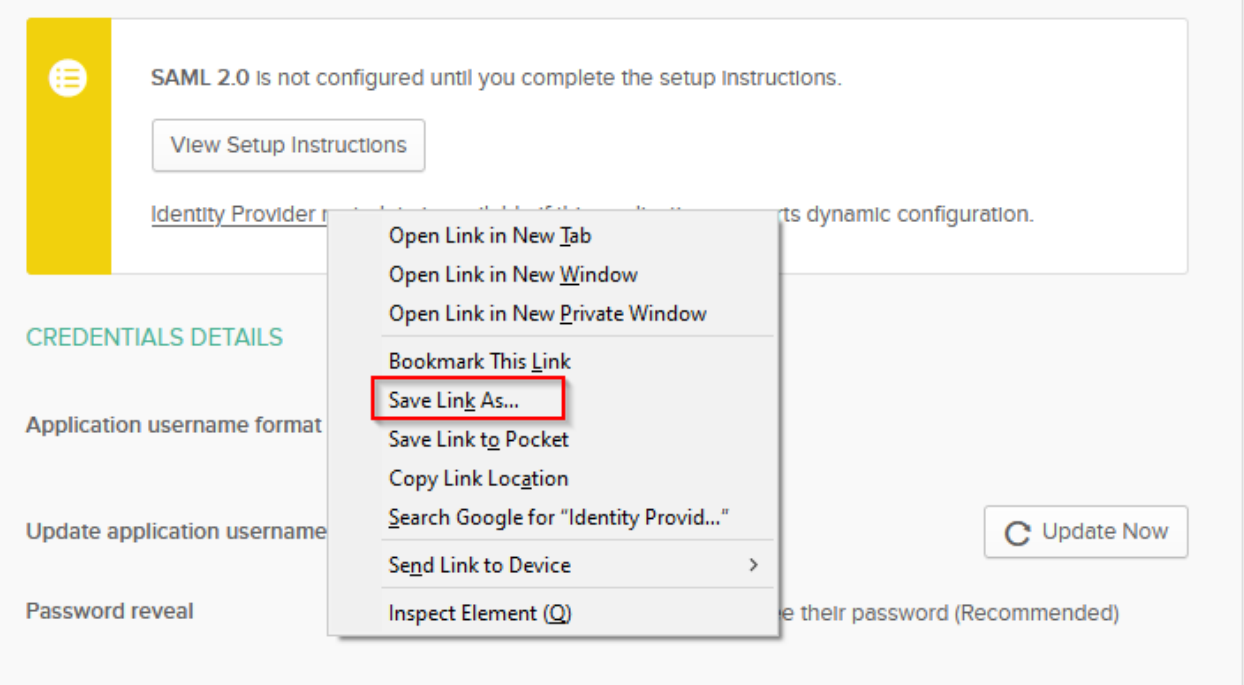
8. Under **General**, in **Single sign on URL** add **https://userauth.dotcom-monitor.com/Login.ashx**

9. Inside the **Audience URI (SP Entity ID)** field add **https://userauth.dotcom-monitor.com/**

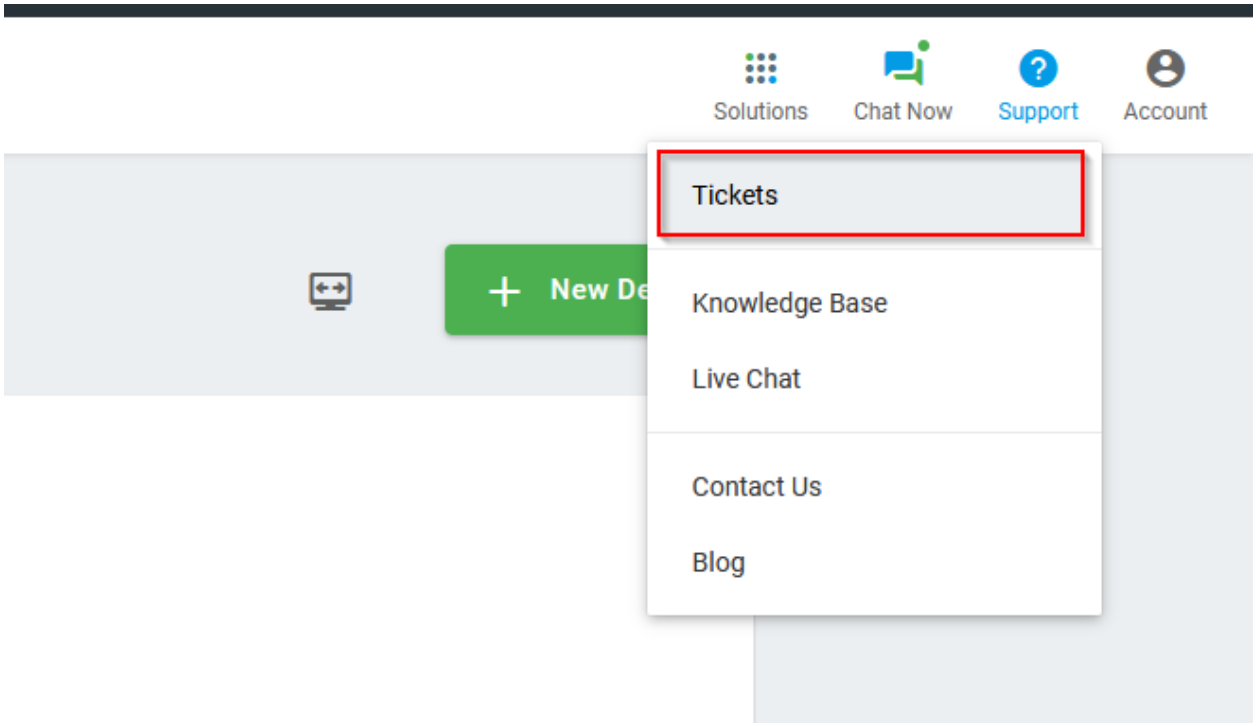
10. Hit next and select **I'm an Okta customer adding an internal** app and **This is an internal app that we have created** and then hit Finish.



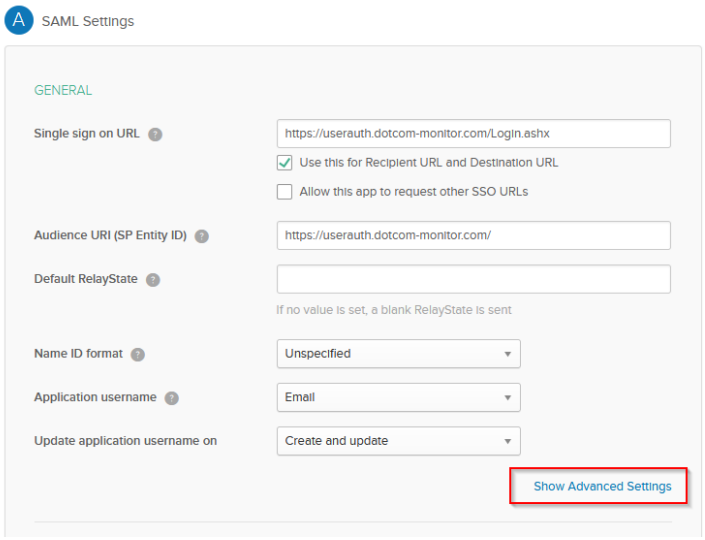
11. Go to the **Sign On** tab on the newly created app, right-click **Identity Provider metadata** and hit **Save Link as**. Save the metadata on your computer as we will need it on the next step.



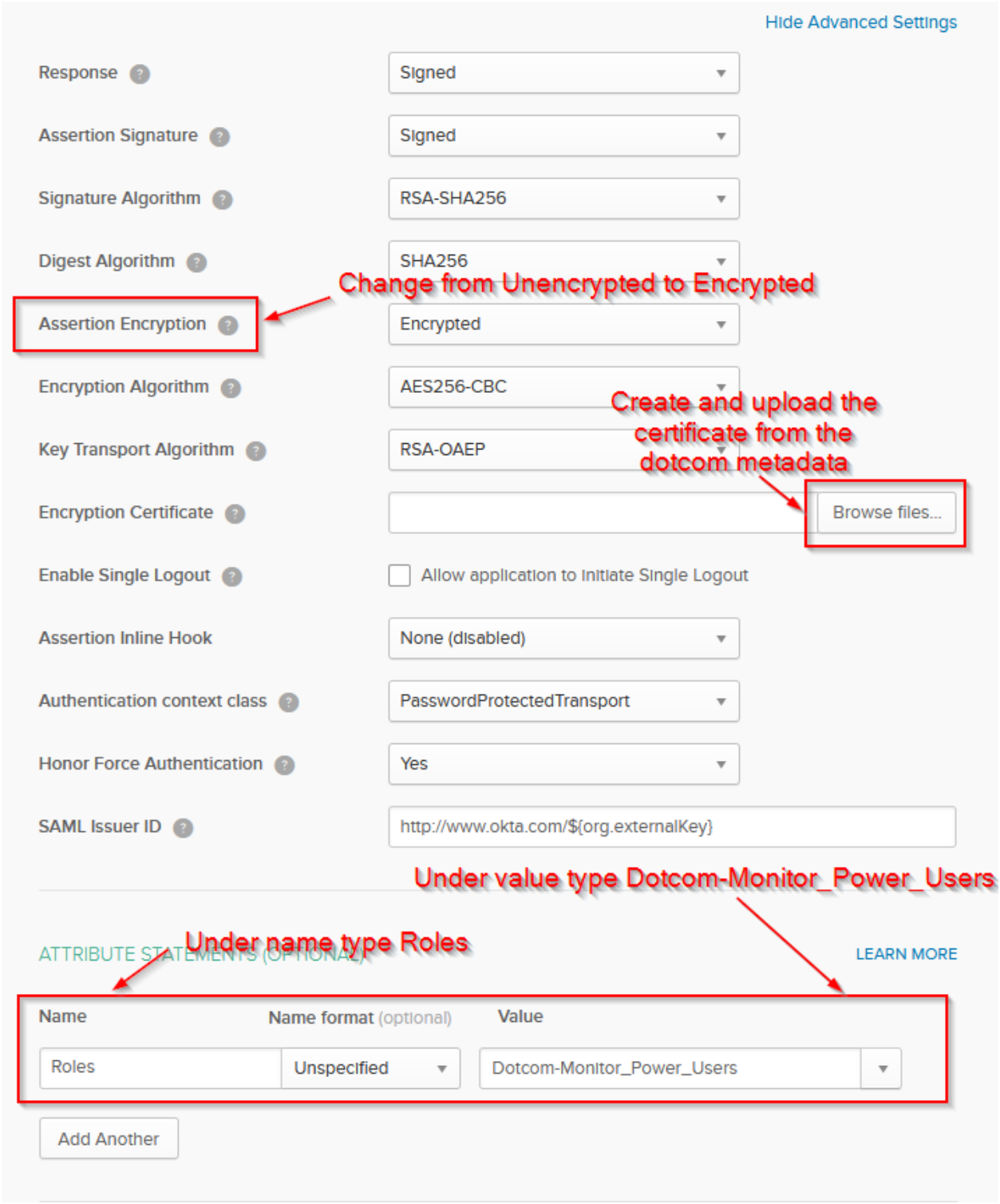
12. Sign into Dotcom-Monitor and open a ticket with their support team, (you can do this by going to **Support** > **Tickets** > **+New Ticket**) and mention the fact that you want to enable Single Sign-on. Attach the Okta metadata that you downloaded on step 11 and request Dotcom-Monitor their metadata, which will be required later.



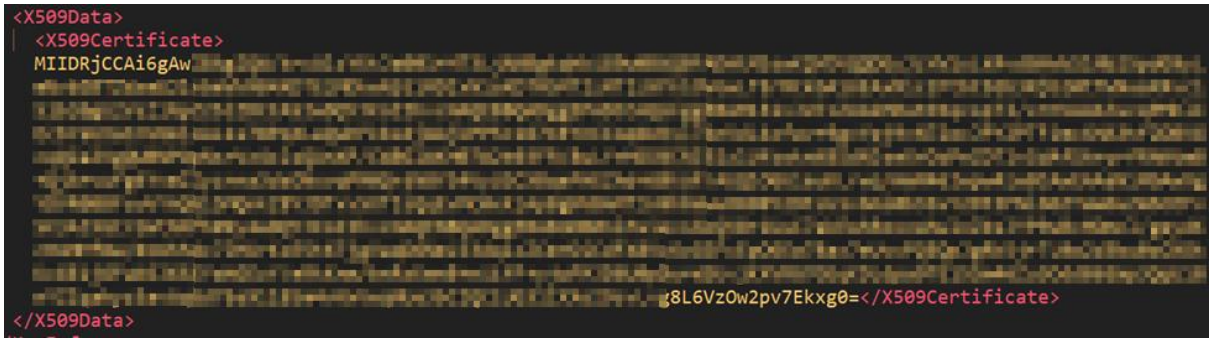
13. After Dotcom-Monitor support replies and provides you their metadata, go back to Okta, on the Dotcom-Monitor application, on the **General** tab > **SAML Settings** > **Edit** > **Next** > **Show Advanced Settings**. Change **Assertion Encryption** to **Encrypted** and from the Dotcom-Monitor metadata grab the certificate, save it in a *.crt* format and upload it under Encryption certificate.



14. After uploading the certificate, scroll down to **Attribute Statements (optional)** and add in the **Name** field **Roles** and in the filter field **Dotcom-Monitor_Power_Users.**

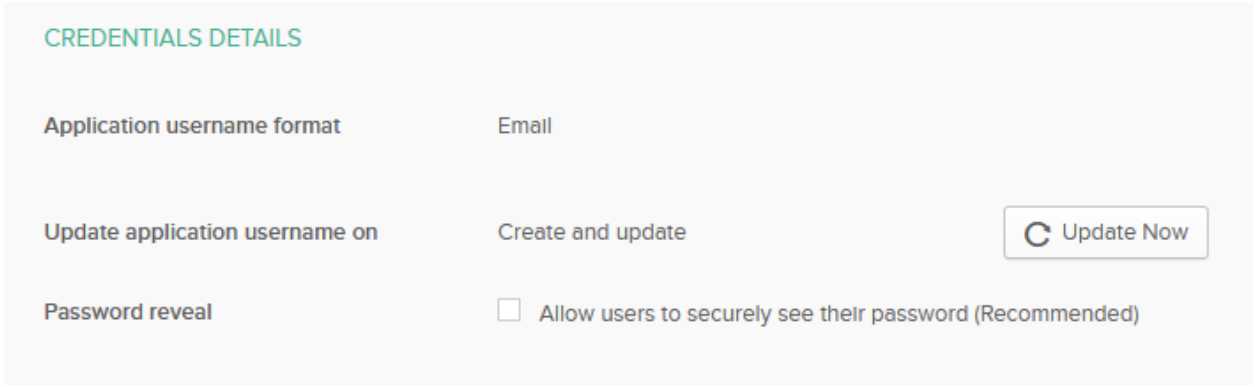


To create the certificate from dotcom-monitor metadata just grab the certificate information which should look like this:



Afterwards be sure to open a txt file and save it in a .crt format while adding -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----

15. Doublecheck the Username format, on the Okta application, to be sure that it has the same format as the one from Dotcom-Monitor. This can be verified on the **Sign on** tab and can vary depending on the username format that your users have in Dotcom-Monitor.



16. Assign the application to the users, and they now will be able to see the Dotcom-Monitor application on their dashboard. Authentication is going to work seamlessly and SSO will ease the whole authentication process. *(Be aware that if they choose a SP initiated sign in flow, they will get redirected to your Okta.org login page, and in case you do not have DSSO, they will have to sign into Okta manually as usual).*

This integration will not provision users or assign roles inside Dotcom-Monitor from Okta, this will strictly modify their login experience due to having Single Sign-on enabled.