okco. * 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.

okta	Get Started Dashboard Director	Applications Security Workflow Reports Settings	Му Аррз 🔿
Back to Applica	ations	Step 1	Step 2 Create New App
CATEGORIES	Create a New Application In	tegration	×
Featured API Managemer	n' Platform	Web *	See all
Apps Apps for Good CASB	Sign on method	Secure Web Authentication (SWA) Uses credentials to sign in 2 Step 3 ion works w	ign.
Directories and Security Applica	F	SAML 2.0 Uses the SAML protocol to log users into the app. T than SWA. If the app supports it.	oning
Okta Application Okta Test Applic	n 21	OpenID Connect Uses the OpenID Connect protocol to log users into	o an app you've built.
VPN			m
		Crea	Cancel
	Fastes	Growing	See all

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 <u>https://userauth.dotcom-</u> 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.

Are you a customer or partner?	 I'm an Okta customer adding an Internal app
	\bigcirc I'm a software vendor. I'd like to integrate my app with Okta
The optional questions below	w assist Okta Support In understanding your app integration.
App type 📀	\checkmark This is an internal app that we have created

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.

•	SAML 2.0 Is not conf	igured until you complete the setup ins	tructions.	
	Identity Provider r	Open Link in New <u>T</u> ab	ts dyna	amic configuration.
		Open Link in New <u>W</u> indow		
CREDENTIALS DETAILS		Open Link in New <u>P</u> rivate Window		
		Bookmark This Link		
Application username format		Save Lin <u>k</u> As		
		Save Link t <u>o</u> Pocket		
		Copy Link Location		
Update application username		Search Google for "Identity Provid"		C Update Now
		Send Link to Device	>	
Password reveal		Inspect Element (Q)	e their	password (Recommended)

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 Signon. Attach the Okta metadata that you downloaded on step 11 and request Dotcom-Monitor their metadata, which will be required later.

	Solutions Chat Now Support Account
	Tickets
👥 🕂 New De	Knowledge Base
	Live Chat
	Contact Us
	Blog

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.

GENERAL			
Single sign on URL 👔	https://userauth.dotcom-monitor.com/Login.ashx		
	Use this for Recipient UF	L and Destination URL	
	Allow this app to reques	t other SSO URLs	
Audience URI (SP Entity ID) 🕘	https://userauth.dotcom-monitor.com/		
Default RelayState 👔			
	If no value is set, a blank Rel	ayState is sent	
Name ID format 👩	Unspecified	-	
Application username 👔	Email	-	
Update application username on	Create and update	•	

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**.

		Hide Advanced Settings
Response 📀	Signed	•
Assertion Signature 👩	Signed	Ŧ
Signature Algorithm (2)	RSA-SHA256	v
Digest Algorithm 👔	SHA256 ange from Unencrypted to Er	ncrypted
Assertion Encryption (2)	Encrypted	-
Encryption Algorithm (2)	AES256-CBC Create an	nd upload the
Key Transport Algorithm 💿	RSA-OAEP certification	ate from the n metadata
Encryption Certificate 💿		Browse files
Enable Single Logout 💿	Allow application to Initiate Single Log	gout
Assertion Inline Hook	None (disabled)	T
Authentication context class 👔	PasswordProtectedTransport	T
Honor Force Authentication 📀	Yes	Y
SAML Issuer ID 👔	http://www.okta.com/\${org.externalKey}	
	Under value type Dotcom	-Monitor_Power_Users
ATTRIBUTE STATEMENTS OF THE AVE	e Roles	LEARN MORE
Name Name format	optional) Value	
Roles Unspecifie	d • Dotcom-Monitor_Power_Use	ers 🔻
Add Another		

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-----

BEGIN CERTIFICATE
MIIDR†CCAi6gAwIBAgIOW/
lange waar kees a problem water with an her bank in which was a first hit is a second of the second s
ete ur ven besten. Nom net eller verset te svirri och den stande stander et beste som den som beer beste som b
news the sub-the well-ball as denoted in the bary "fermion", in original is the birth of the product of the bar
a se a construction de la co
a sector sector sector per sus administrative sector sector sector sector sector sector sector sector sector sec
ah dina 1 yang sebah ta kanan menangkan galapakan dari sebah di di basar kanan kanan kanang pang menangkan di s
en en gen an ben ment e l'esterne principal et sonr (Charles) with principal and (Charles) (Charles) in the basis der Charly d'es
le3bCIQCiUG31IXXoI9svLvg8L6Vz0w2pv7Ekxg0=
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.

CREDENTIALS DETAILS		
Application username format	Email	
Update application username on	Create and update	C Update Now
Password reveal	Allow users to securely see their password (R	ecommended)

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.