

# Okta IDP Integration with Dotcom-Monitor

This is the SAML SSO integration Step By Step Guide to enable Single SignOn access to your Dotcom-Monitor service:

## Step 1:

### Login to your Okta Admin dashboard:

Go to your Okta domain: <https://YourOktaDomain.okta.com/>  
Go to: Admin (<https://YourOktaDomain-admin.okta.com/admin/dashboard>)  
You should need at least App Admin Access on your Okta Account.

### Okta Permissions Overview

## Step 2:

### Adding Custom SAML Application and Initial Configuration

Go to Applications Panel.  
From Add Application button in this menu you access the Okta OIN and Apps  
Select Platform Web and Sign on method SAML 2.0

Create a New Application Integration

Platform: Web

Sign on method:

- Secure Web Authentication (SWA)  
Uses credentials to sign in. This integration works with most apps.
- SAML 2.0  
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.
- OpenID Connect  
Uses the OpenID Connect protocol to log users into an app you've built.

Create Cancel

## Create

The first Menu is for App name, App visibility and Logo

okta Dashboard Directory Applications OMM Security Workflow Reports Settings

Create SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

1 General Settings

App name: [text input]

App logo (optional): [gear icon] [Browse...]

Upload Logo

App visibility:

- Do not display application icon to users
- Do not display application icon in the Okta Mobile app

Cancel Next

App name: Dotcom-Monitor

Go Next

The next menu is where the SAML settings get enforced.  
Use the following values in the corresponding fields.


Single Sign On URI: <https://userauth.dotcom-monitor.com/Login.ashx>

Audience URI (Entity ID): <https://userauth.dotcom-monitor.com/>

Name ID format: Transient


**A** SAML Settings


**GENERAL**

Single sign on URL 


Use this for Recipient URL and Destination URL


Allow this app to request other SSO URLs

Audience URI (SP Entity ID) 

Default RelayState 

If no value is set, a blank RelayState is sent

Name ID format 

Application username 

Update application username on

[Show Advanced Settings](#)

Proceed to the ATTRIBUTE STATEMENTS

In the GROUP ATTRIBUTE STATEMENTS we need to add Roles for group Role distribution.

We add a variable Name: Roles

With Filter for groups that Starts with: Dotcom-Monitor

**GROUP ATTRIBUTE STATEMENTS (OPTIONAL)**

Name	Name format (optional)	Filter
<input type="text" value="Roles"/>	<input type="text" value="Unspecified"/>	<input type="text" value="Starts with"/> <input type="text" value="Dotcom-Monitor"/>

Go Next

In the Feedback Menu:

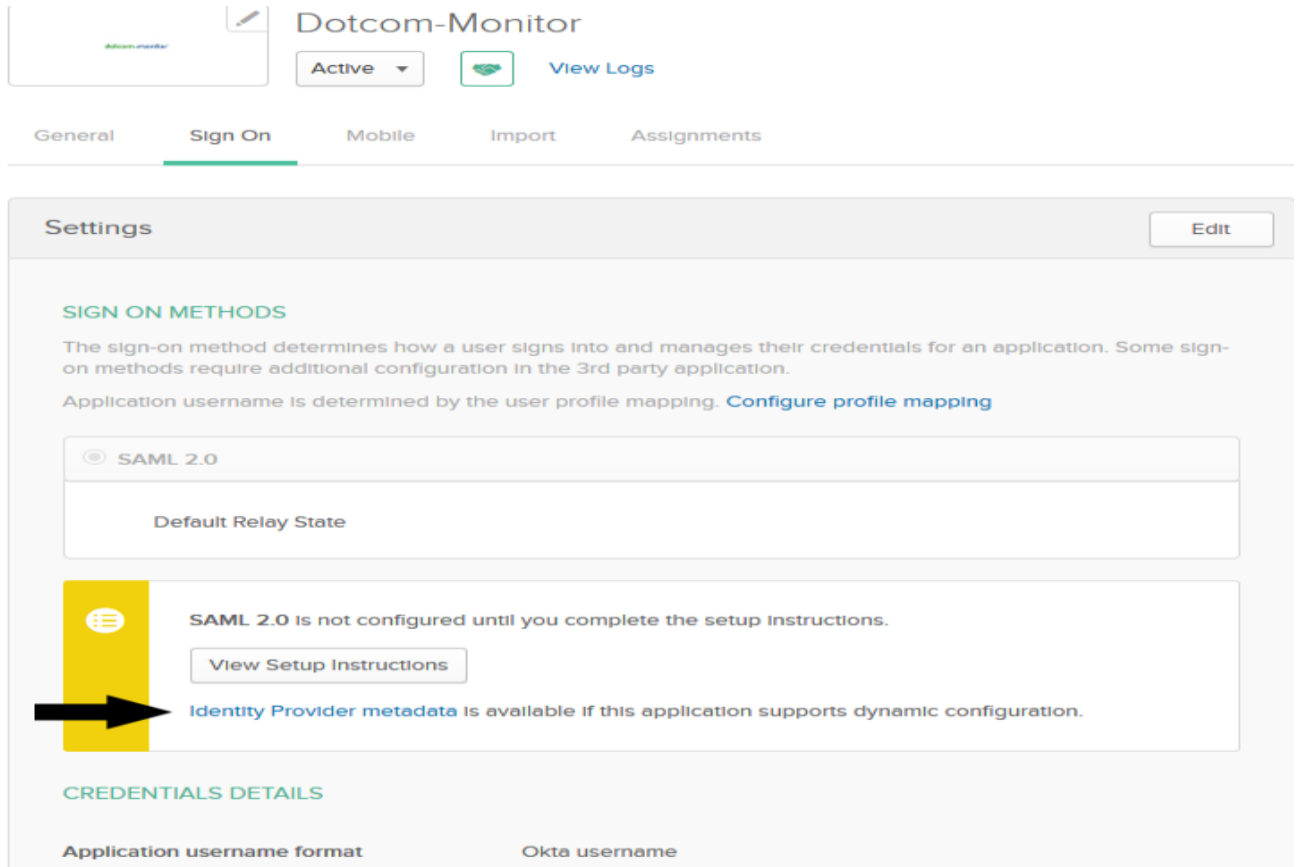
Are you a customer or partner?: I'm an Okta customer adding an internal app  
App type: This is an internal app that we have created

Go Finish

### Step 3:

## Metadata exchange and handling.

From Sign On you will need to export the Okta Dotcom-Monitor app metadata file. You can right click on the Identity Provider Metadata and Save link as for ex. OktaDotcom-MonitorMetadata this will export the required file.



With the metadata file ready from the app we just created, the Dotcom-Monitor team need to be notified via a Support ticket submission.

Go to: <https://user.dotcom-monitor.com/ticket/createticket.aspx>

Upload the Oktametadata file and wait for the Support response with their Metadata file, which we need for the Certificate used to Encrypt the SAML assertion from Okta.

After the support reply with the DMSPMetadata.xml file, we need to export the x509 certificate

```
<?xml version="1.0" encoding="utf-8"?>
<EntityDescriptor xmlns:saml="urn:oasis:names:to:SAML:2.0:protocol" xmlns:saml2="urn:oasis:names:to:SAML:2.0:assertion" entityID="https://userauth.dotcom-monitor.com/" ID="1d70440d8a6e6410cbe9e56750ae106b" validUntil="2020-04-24T13:35:06.0830279Z" xmlns="urn:oasis:names:to:SAML:2.0:metadata">
  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:to:SAML:2.0:protocol" AuthnRequestsSigned="true" WantAssertionsSigned="true">
    <KeyDescriptor use="samlping">
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <X509Data>
          <X509Certificate>
            MIIDRjCCAlEgAwIBAgIQ/kroA1oYPLJa001+HT3LjANBgkqhkiG9w0BAQsFAADCAQEAggEBAMLS1vT7+ZDAAMust0tospTI/xrnVADu7uocPb1LEobYaDXCnVam1oALL8789QLkQhFkhdjMAJkFPS+107XEtYcCoq8oha174oVGL4xFav+9v7Pj3vW72ooFZ2PFFlmcXBA3tE2DBVCoq2aE1VgQBNFOParV4elqgkXK/CMB01M8B7WZtC3F8/8uLYrBOSMCI921lDzoakPSB9wXkDzDhD71v5dA5ArYrFRBnta8+qJkVnuG7vmlYzrn3d08vavjM9QjM8Y34YvDCBqPFEZd+68kaP/ADQ10001eulRw/8m461vq4wCwAAANlMGwXqITVRC88FowYAgQ1SMka25Y1D7vXYTtqgWMCkRzAgq8vNvAMTlmbhbw809Y291LlJ1vml0b31oY291lFNLlGtYmMhDMSCEPv9K3A7K0CrdMUNEnDby4wQYJW0Z1lvnAQJ8N9QdggEBAB080nLlPveceRQvY+1DuCtAkBwh0xwhw1k2ba7Ypnb-mDwcl/gpyDRo488Rf8a/Oz6hd07380/Kk54Tj3Vqg0MeL3dqi0cEzrD1C8FXVvokaD870tp04Ea78axTelvoPQp3g8k5+Tl0w4d3hd0c0M1K0cE1j0Fw676SEYahZyY/48kPm/bn8k8n8+n1lFry3vPM4D40p0u+MSDv3KXV927G8dLdp9TE155e462b30d8F8E6p3Qg01RoY21qahz5vAq578e91185e4v8vW8e38C1Q103113X189vLvg8L6Vw0z9v78kag0=</X509Certificate>
          </X509Data>
        </KeyInfo>
      </KeyDescriptor>
    <KeyDescriptor use="encryption">
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <X509Data>
          <X509Certificate>
            MIIDRjCCAlEgAwIBAgIQ/kroA1oYPLJa001+HT3LjANBgkqhkiG9w0BAQsFAADCAQEAggEBAMLS1vT7+ZDAAMust0tospTI/xrnVADu7uocPb1LEobYaDXCnVam1oALL8789QLkQhFkhdjMAJkFPS+107XEtYcCoq8oha174oVGL4xFav+9v7Pj3vW72ooFZ2PFFlmcXBA3tE2DBVCoq2aE1VgQBNFOParV4elqgkXK/CMB01M8B7WZtC3F8/8uLYrBOSMCI921lDzoakPSB9wXkDzDhD71v5dA5ArYrFRBnta8+qJkVnuG7vmlYzrn3d08vavjM9QjM8Y34YvDCBqPFEZd+68kaP/ADQ10001eulRw/8m461vq4wCwAAANlMGwXqITVRC88FowYAgQ1SMka25Y1D7vXYTtqgWMCkRzAgq8vNvAMTlmbhbw809Y291LlJ1vml0b31oY291lFNLlGtYmMhDMSCEPv9K3A7K0CrdMUNEnDby4wQYJW0Z1lvnAQJ8N9QdggEBAB080nLlPveceRQvY+1DuCtAkBwh0xwhw1k2ba7Ypnb-mDwcl/gpyDRo488Rf8a/Oz6hd07380/Kk54Tj3Vqg0MeL3dqi0cEzrD1C8FXVvokaD870tp04Ea78axTelvoPQp3g8k5+Tl0w4d3hd0c0M1K0cE1j0Fw676SEYahZyY/48kPm/bn8k8n8+n1lFry3vPM4D40p0u+MSDv3KXV927G8dLdp9TE155e462b30d8F8E6p3Qg01RoY21qahz5vAq578e91185e4v8vW8e38C1Q103113X189vLvg8L6Vw0z9v78kag0=</X509Certificate>
          </X509Data>
        </KeyInfo>
      </KeyDescriptor>
    <NameIDFormat urn:oasis:names:to:SAML:2.0:nameid-format:transient</NameIDFormat>
    <AssertionConsumerService Binding="urn:oasis:names:to:SAML:2.0:bindings:HTTP-POST" Location="https://userauth.dotcom-monitor.com/Login.ashx" index="0" isDefault="true" />
  </SPSSODescriptor>
  <ContactPerson contactType="administrative">
    <Company>dotcom-monitor.com</Company>
    <GivenName>Support</GivenName>
    <Surname />
    <EmailAddress>support@dotcom-monitor.com</EmailAddress>
    <TelephoneNumber>1-888-479-0741</TelephoneNumber>
  </ContactPerson>
</EntityDescriptor>
```

Create a text document that has the first line as:

-----BEGIN CERTIFICATE-----

Last line as:

-----END CERTIFICATE-----

Paste the certificate encryption between the BEGIN CERTIFICATE and END CERTIFICATE

Save as file as crt ex. dcmstp.crt

```
-----BEGIN CERTIFICATE-----
MIIDRjCCAi6gAwIBAgIQW/krcAlcYKtJa001+HT3LjANBgkqhkiG9w0BAQ0FADAtMSswKQYDVQQDEyJzYWlsLkRvdGNvbS1Nb25pdG9yLmN
ASIwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM151vJU7+ZUAKMRutGtqcsptI/xrnVAUA7ucqPMh1IEcbYaUXaCnVGmloAL1s78PqX
3FR/8uLYrHOSNCNI92z1UfzoknKBSdNjseXrDzPnZDTlvSdAfsAryrfRhNtm8+QjA+vufg4YvmZIyzrna3dsONxvqPM0QrjN8YS4VyUSCXB
Y29tLU1vbm10b3IuY29tIFNlbGZTaWduZWSCEFv5K3AJXGCrSWtNNfh09y4wDQYJKoZIhvcNAQENBQADggEBABoDB0nlPwiecsNcQV8+1Uu
j+TL0w2d3bu0zOXOtKcGE1jGFwK6J6SEYahGEzY/eRkKnm/bnRxKmnB+niiff+yjwFMJD6U0pDu+WSUvjKXVRG7GEqKDLdpa9TE15Sm46Zu
-----END CERTIFICATE-----
```

#### Step 4:

### Okta SAML App Encryption Enablement

From the Dotcom-Monitor App in the General menu, Choose SAML Settings and Edit.

From the SAML Settings Menu Show Advanced Settings.

Select Assertion Encryption: Encrypted

Browse and upload the crt file we made in Step 3.

Application username ?	Okta username	
Update application username on	Create and update	
		Hide Advanced Settings
Response ?	Signed	
Assertion Signature ?	Signed	
Signature Algorithm ?	RSA-SHA1	
Digest Algorithm ?	SHA256	
Assertion Encryption ?	Encrypted	
Encryption Algorithm ?	AES256-CBC	
Key Transport Algorithm ?	RSA-OAEP	
Encryption Certificate ?		Browse files...

Go Next and Finish.

## Step 5:

### Finishing the Assignments and Group setup.

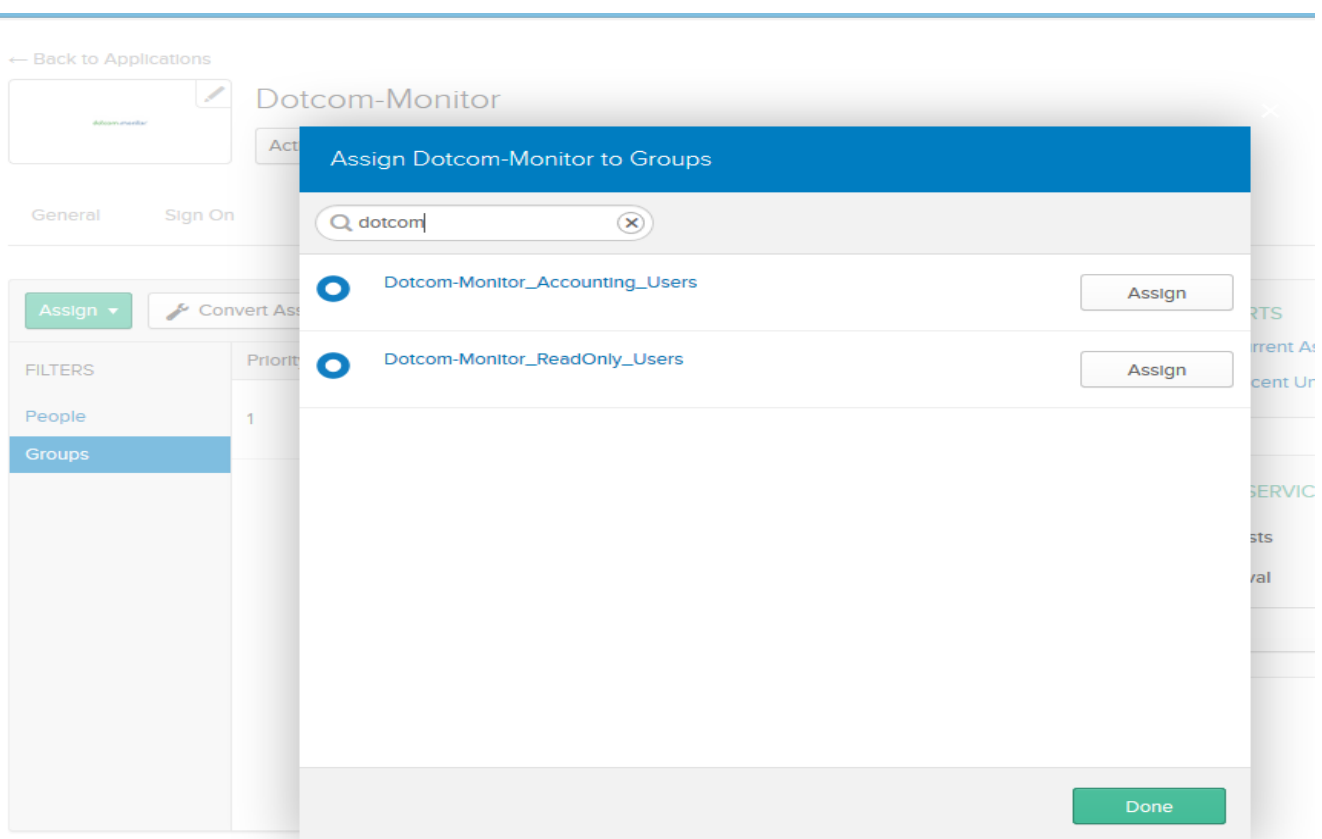
Inside the Okta Admin Dashboard go to Directory and Groups.

We will create 5 Groups based on the Roles name convention of Dotcom-Monitor:

Dotcom-Monitor\_Operators  
Dotcom-Monitor\_ReadOnly\_Users  
Dotcom-Monitor\_Accounting\_Users  
Dotcom-Monitor\_Users  
Dotcom-Monitor\_Power\_Users

This groups are in effect used to provide member users with the designated role for Dotcom-Monitor.

In the Dotcom-Monitor App and Assignments we proceed to assign this groups.

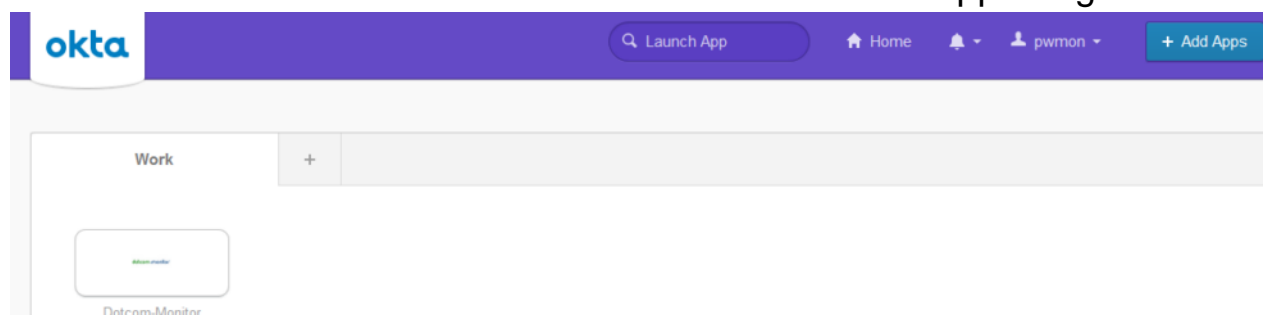


Done

## Step 6:


### Testing the SAML SSO flow.

From the EndUser Dashboard we now should have the App assigned and ready.




# Extra.

## Full Working Okta Application Config:



### Dotcom-Monitor

Active  [View Logs](#)

General | Sign On | Mobile | Import | Assignments

---

#### App Settings Edit

**Application label** Dotcom-Monitor

**Application visibility**  Do not display application icon to users  
 Do not display application icon in the Okta Mobile app

**Provisioning**  None  
 On-Premises Provisioning  
 SCIM

**Auto-launch**  Auto-launch the app when user signs into Okta.

**Application notes for end users**

**Application notes for admins**

---

#### SAML Settings Edit

**GENERAL**

**Single Sign On URL** https://userauth.dotcom-monitor.com/Login.ashx

**Recipient URL** https://userauth.dotcom-monitor.com/Login.ashx

**Destination URL** https://userauth.dotcom-monitor.com/Login.ashx

**Audience Restriction** https://userauth.dotcom-monitor.com/

**Default Relay State**

**Name ID Format** Transient

**Response** Signed

**Assertion Signature** Signed

**Signature Algorithm** RSA\_SHA1

**Digest Algorithm** SHA1

**Assertion Encryption** Encrypted

**Encryption Certificate** dcm.crt (CN=saml.Dotcom-Monitor.com SelfSigned)

**Encryption Algorithm** AES256\_CBC

**Key Transport Algorithm** RSA\_OAEP

**SAML Single Logout** Disabled

**authnContextClassRef** PasswordProtectedTransport

**Honor Force Authentication** Yes

**Assertion Inline Hook** None (disabled)

**SAML Issuer ID** http://www.okta.com/\${org.externalKey}

**ATTRIBUTE STATEMENTS**

Name	Name Format	Value
------	-------------	-------

**GROUP ATTRIBUTE STATEMENTS**

Name	Name Format	Filter
Roles	Unspecified	Starts with: Dotcom-Monitor