



eMAM- OKTA SSO INTEGRATION

Configuration Document

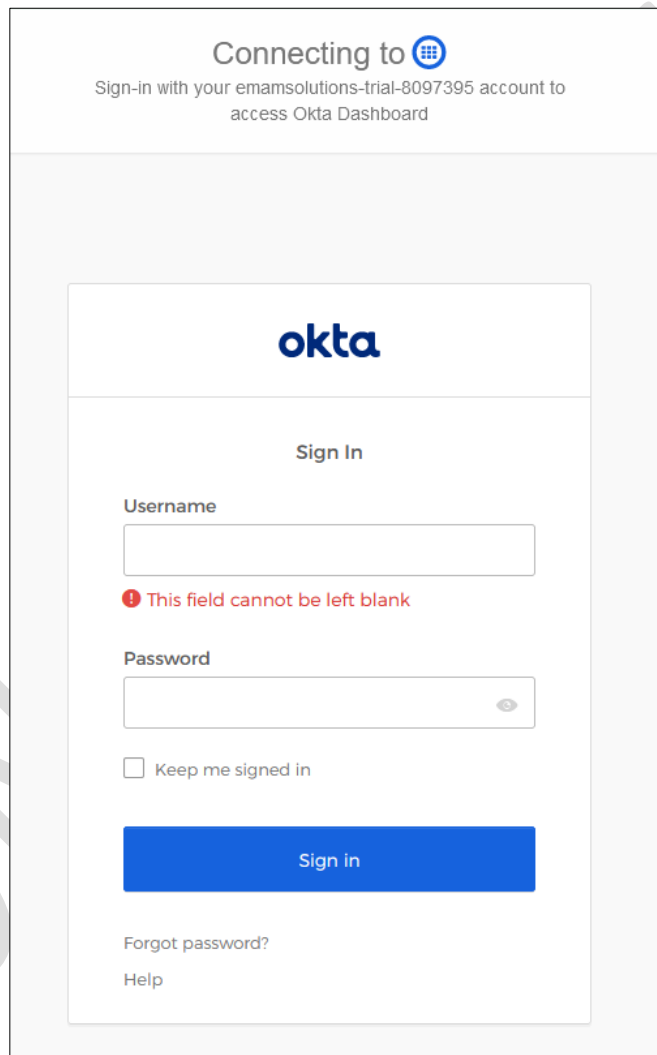
Prerequisites

You need an account in Okta.

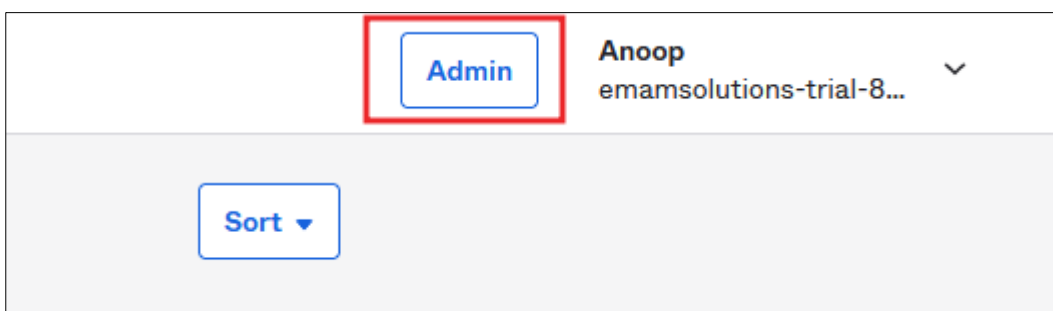
Get Started

Follow the below steps to integrate eMAM with Okta.

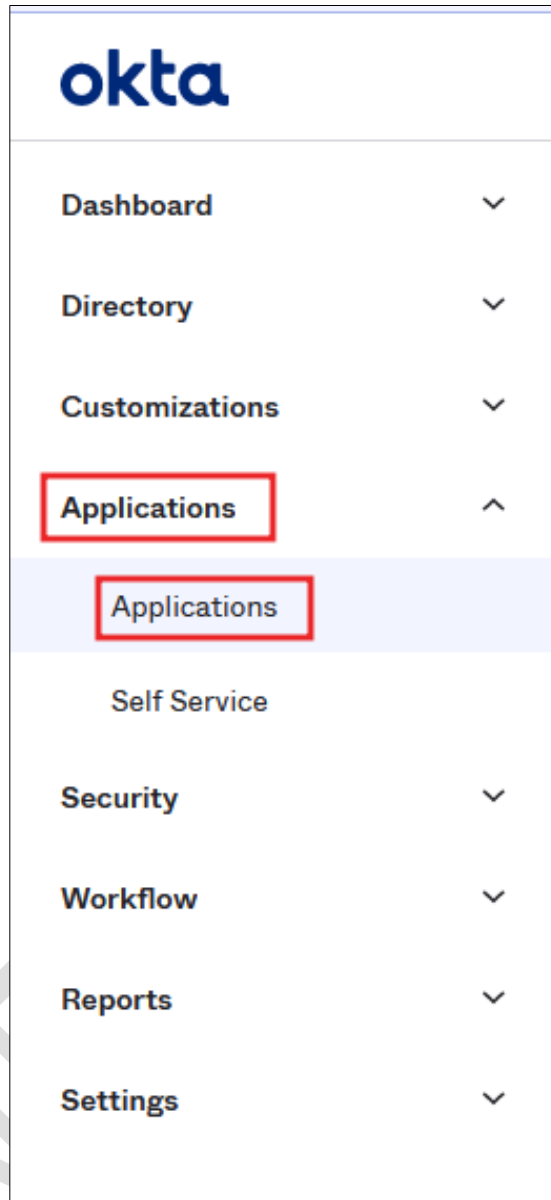
1. Login to Okta Interface by providing the username and password.



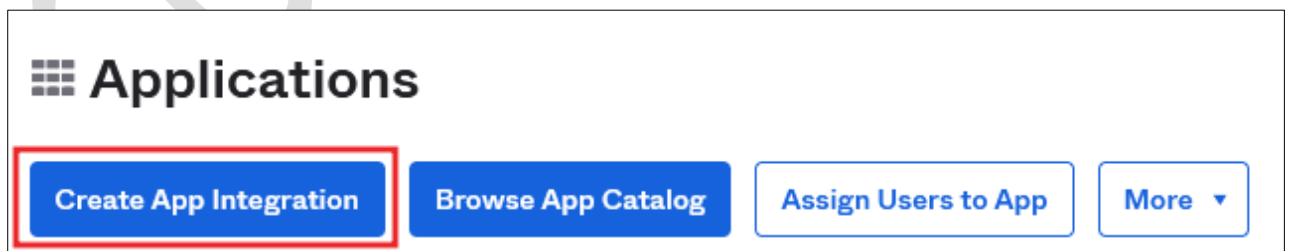
2. Click on the **Admin** button to navigate to the Admin interface



3. Go to **Applications**



4. Click on **Create App Integration**



5. Choose **SAML 2.0** and click on **Next**

Create a new app integration

Sign-in method

[Learn More](#)

☐ **OIDC - OpenID Connect**
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

☒ **SAML 2.0**
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

☐ **SWA - Secure Web Authentication**
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

☐ **API Services**
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

[Cancel](#) [Next](#)

6. Give an **App Name** and **Upload Logo**. Click on **Next**

Create SAML Integration

1 General Settings

2 Configure SAML


3 Feedback

1 General Settings

App name

eMAM Cloud

App logo (optional)



App visibility

☐ Do not display application icon to users

[Cancel](#) [Next](#)

7. Enter below details:

- **Single sign on URL** (Example - <https://cp.emamcloud.com/eMAMGateway/Login.aspx>)
- **Audience URI (SP Entity ID)** (Example - <https://cp.emamcloud.com/eMAMGateway/>)
- **Name ID format** – EmailAddress
- **Application username** – Email

8. Click on **Show Advanced Settings**

9. Enter below details:

- **Enable Single Logout** – Enable it
- **Enter Single Logout URL** (Example - <https://cp.emamcloud.com/eMAMGateway/Logout.aspx>)
- **Enter SP Issuer** (Example - <https://cp.emamcloud.com/eMAMGateway/>)
- Click on **Download Okta Certificate** (*Keep the certificate handy. Need to install this on eMAM Web server*)

A SAML Settings

General

Single sign on URL ?

https://cp.emamcloud.com/eMAMGateway/Login.aspx

☒ Use this for Recipient URL and Destination URL
 ☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

https://cp.emamcloud.com/eMAMGateway/

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

EmailAddress

Application username ?

Email

Update application username on

Create and update

Response ?

Signed

Assertion Signature ?

Signed

Hide Advanced Settings

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Service Provider if required.

[Download Okta Certificate](#)

10. Click on **Upload Certificate** (Upload the one which is downloaded in the previous step)

Signature Algorithm ?

RSA-SHA256

Digest Algorithm ?

SHA256

Assertion Encryption ?

Unencrypted

Enable Single Logout ?

☒ Allow application to initiate Single Logout

Single Logout URL ?

https://cp.emamcloud.com/eMAMGateway/Logout.aspx

SP Issuer ?

https://cp.emamcloud.com/eMAMGateway/

Signature Certificate ?

Browse

Upload Certificate

Assertion Inline Hook

None (disabled)

Authentication context class ?

PasswordProtectedTransport

Honor Force Authentication ?

Yes

SAML Issuer ID ?

https://cp.emamcloud.com/eMAMGateway/

11. Enter **SAML Issuer ID** (Example - <https://cp.emamcloud.com/eMAMGateway/>)

12. Under Attribute Statements (optional)

- Create the attribute statements like below.

Attribute Statements (optional) [LEARN MORE](#)

Name	Name format (optional)	Value	
<input type="text" value="http://schemas.xmlsoap."/>	<input type="text" value="Basic"/>	<input type="text" value="user.firstName"/>	
<input type="text" value="http://schemas.xmlsoap."/>	<input type="text" value="Basic"/>	<input type="text" value="user.lastName"/>	×
<input type="text" value="http://schemas.xmlsoap."/>	<input type="text" value="Basic"/>	<input type="text" value="user.email"/>	×
<input type="text" value="http://schemas.xmlsoap."/>	<input type="text" value="Basic"/>	<input type="text" value="user.login"/>	×

[Add Another](#)

Name	Name format	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	Basic	FirstName
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Basic	LastName
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	Basic	EmailID
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Basic	Username

13. Click on **Next**,

Name	Name format (optional)	Filter
<input type="text"/>	Unspecified ▼	Starts with ▼ <input type="text"/>
Add Another		

B Preview the SAML assertion generated from the information above

[<> Preview the SAML Assertion](#)

This shows you the XML that will be used in the assertion - use it to verify the info you entered above

[Previous](#)
[Cancel](#)
[Next](#)

14. Click on **Finish** to finish the configuration.

1 General Settings

2 Configure SAML

3 Feedback

3 Help Okta Support understand how you configured this application

Are you a customer or partner?

☐ I'm an Okta customer adding an internal app
☒ I'm a software vendor. I'd like to integrate my app with Okta

Once you have a working SAML integration, submit it for Okta review to publish in the OIN.

[Submit your app for review](#)

[Previous](#)
[Finish](#)

Why are you asking me this?

This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

15. Go the created application and click on **Assignments** tab and add the users to the application.

The screenshot shows the eMAM Cloud interface. At the top, there's a header with the eMAM logo, the text "eMAM Cloud", and buttons for "Active", "View Logs", and "Monitor Imports". Below the header, a message states: "Once you have a working SAML integration, submit it for Okta review to publish in the OAN." with a "Submit your app for review" button. The main navigation bar includes "General", "Sign On", "Import", and "Assignments" (which is highlighted with a red box). The "Assignments" section contains a table with columns "Person" and "Type". The table lists two users: "Anoop Thomas" (athomas@emamsolutions.com) and "Alex Baby" (alex@empressmam.com), both of type "Individual". The "Assign" and "Convert assignments" buttons are at the top left of the table. The "Reports" section on the right shows "Current Assignments" and "Recent Unassignments". The "Self Service" section at the bottom right indicates "You need to enable self".

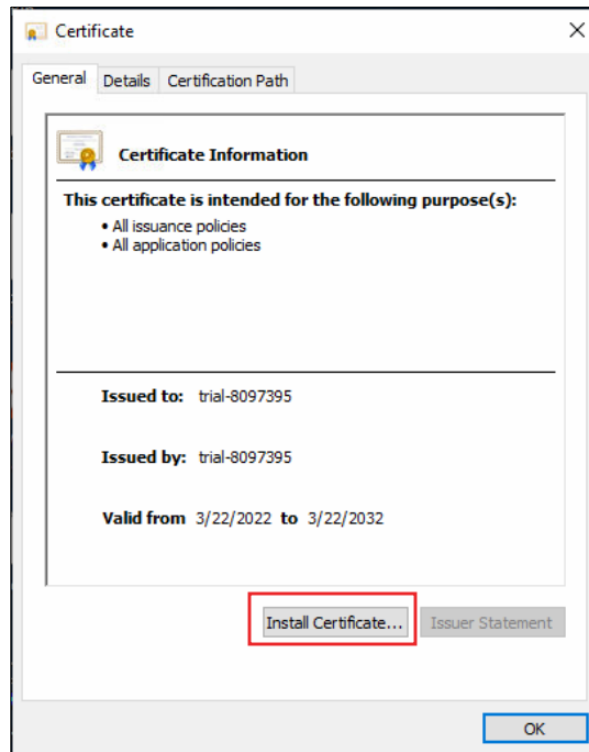
Filters	Person	Type
People	Anoop Thomas athomas@emamsolutions.com	Individual
Groups	Alex Baby alex@empressmam.com	Individual

16. Access the eMAM Web server and install the Okta certificate in the server (*The certificate downloaded from Okta interface*)

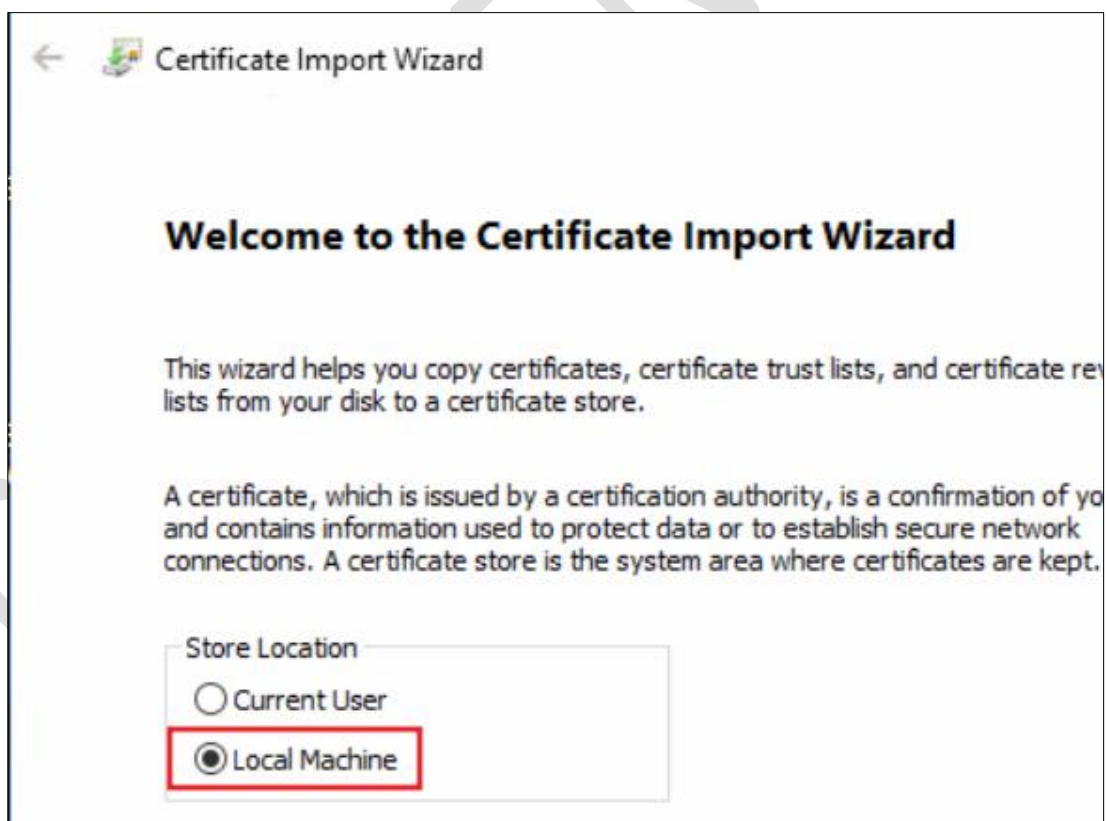
17. Name the certificate like **Okta.cer** and double click on it.




18. Click on **Install Certificate**.



19. Choose **Local machine**.



20. Choose '**Place all certificates in the following store**' and browse

←  Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

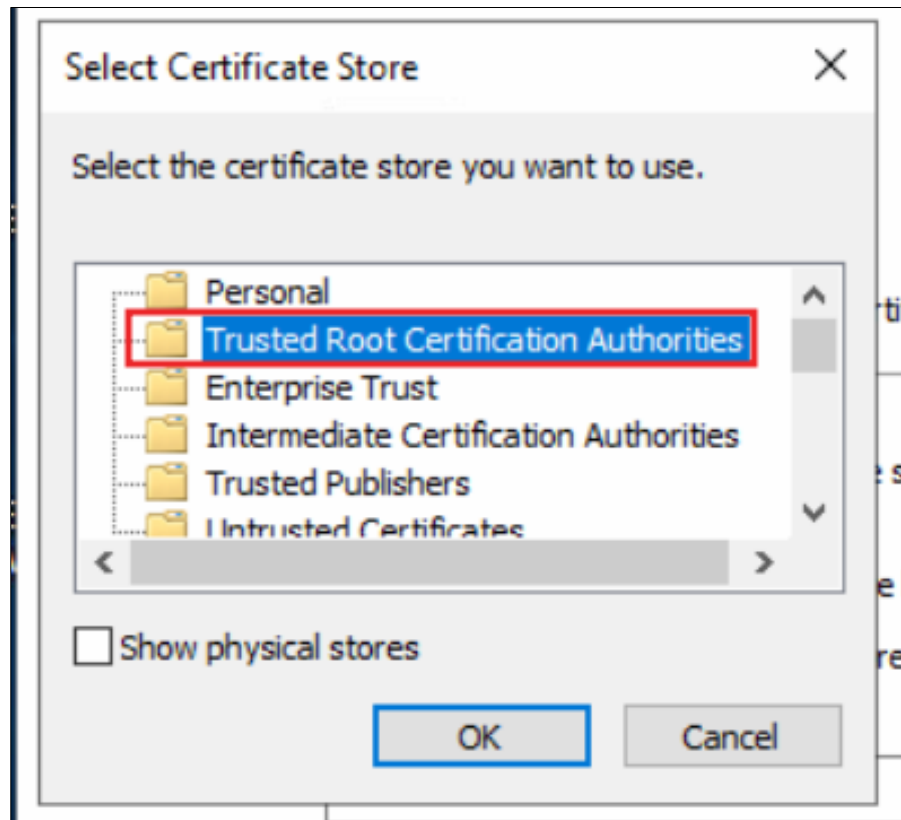
☐ Automatically select the certificate store based on the type of certificate

☒ Place all certificates in the following store

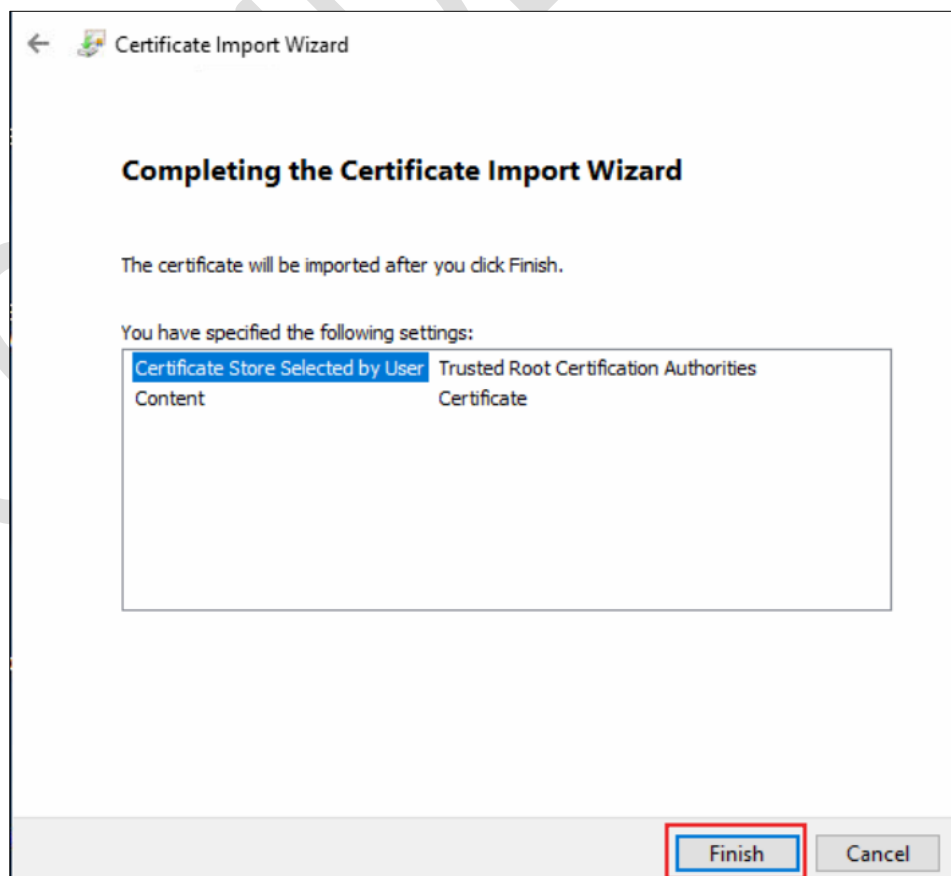
Certificate store:

Browse...

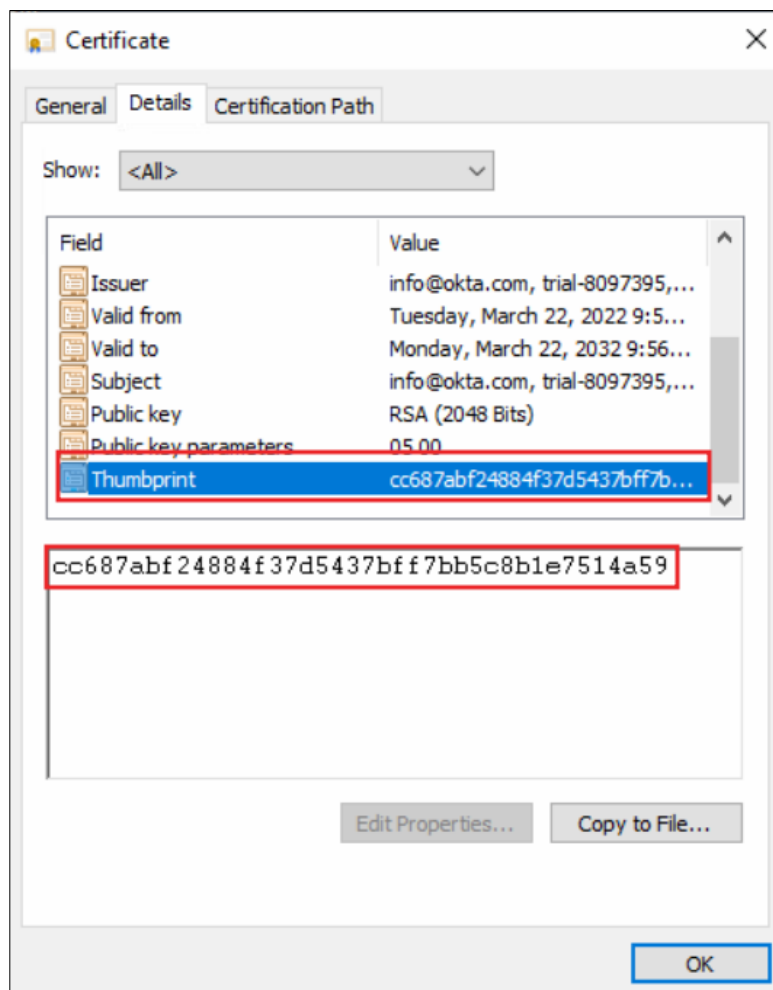
21. Choose **Trusted Root Certification Authorities** and click **Ok** and click **Next**.



22. Click on **Finish** to complete the Certificate import.



23. Open certificate again and copy the **Thumbprint** and paste it to a notepad for now.



24. Go to - C:\Program Files\Empress Media\emAM Gateway\App_Data

25. Open - **SAMLConfiguration.xml**

26. Set the values like the below screenshot,

```
<?xml version="1.0" encoding="utf-8" ?>
<SAML2>
  <Configuration>
    <CertificateThumbprint></CertificateThumbprint>
    <IssuerThumbprint>cc687abf24884f37d5437bff7bb5c8b1e7514a59</IssuerThumbprint>
    <IssuerTrust>http://www.okta.com/exko0c527UKVXqqjX696</IssuerTrust>
    <AssertionConsumerServiceURL>https://cp.emamcloud.com/emAMGateway/Login.aspx</AssertionConsumerServiceURL>
    <Issuer>https://cp.emamcloud.com/emAMGateway/</Issuer>
    <TargetURL>https://trial-8097395.okta.com/app/trial-8097395_emamcloud_1/exko0c527UKVXqqjX696/sso/saml</TargetURL>
    <SigningCertificateThumbprint>cc687abf24884f37d5437bff7bb5c8b1e7514a59</SigningCertificateThumbprint>
    <!-- SAML provider logout URL -->
    <LogoutURL>https://trial-8097395.okta.com/app/trial-8097395_emamcloud_1/exko0c527UKVXqqjX696/slo/saml</LogoutURL>
    <!-- Signature algorithm used to sign SAML request -->
    <SignatureAlgorithm>SHA256</SignatureAlgorithm>
  </Configuration>
</SAML2>
```

<IssuerThumbprint> - Certificate thumbprint

<IssuerThumbprint> - <http://www.okta.com/> PORTION FROM THE LOGIN URL (Example - <http://www.okta.com/exko0c527UKVXqgjX696>)

<AssertionConsumerServiceURL> (Example - <https://cp.emamcloud.com/eMAMGateway/Login.aspx>)

<Issuer> (Example- <https://cp.emamcloud.com/eMAMGateway/>)

<TargetURL> - (Example - https://trial-8097395.okta.com/app/trial-8097395_emamcloud_1/exko0c527UKVXqgjX696/sso/saml)

<SigningCertificateThumbprint> - Certificate thumbprint

<LogoutURL> (Example - https://trial-8097395.okta.com/app/trial-8097395_emamcloud_1/exko0c527UKVXqgjX696/slo/saml)

*Note: Login and Logout URL can be obtained from Okta Metadata. For that take the App and open **Identity Provider Metadata**.*

The screenshot shows the 'eMAM Cloud' configuration interface. At the top, there's a header with the 'eMAM Cloud' logo, a status 'Active', and links for 'View Logs' and 'Monitor Imports'. Below the header, a message states: 'Once you have a working SAML integration, submit it for Okta review to publish in the OAN.' with a 'Submit your app for review' button. The main content area has tabs for 'General', 'Sign On', 'Import', and 'Assignments'. The 'Sign On' tab is selected, showing 'Settings' for SAML 2.0. The 'Sign on methods' section explains that the sign-on method determines how a user signs into and manages their credentials. It notes that the application username is determined by the user profile mapping, with a link to 'Configure profile mapping'. Under 'SAML 2.0', there's a 'Default Relay State' field. A yellow banner indicates 'SAML 2.0 is not configured until you complete the setup instructions.' with a 'View Setup Instructions' button. Below this, a red box highlights 'Identity Provider metadata' with the text 'Identity Provider metadata is available if this application supports dynamic configuration.' To the right, the 'About' section explains that SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. The 'Application Username' section advises choosing a format for the default username value and notes that selecting 'None' will prompt for manual entry.

eMAM Cloud
Active View Logs Monitor Imports

Once you have a working SAML integration, submit it for Okta review to publish in the OAN. [Submit your app for review](#)

General **Sign On** Import Assignments

Settings [Edit](#)

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

☒ SAML 2.0

Default Relay State

SAML 2.0 is not configured until you complete the setup instructions. [View Setup Instructions](#)

Identity Provider metadata is available if this application supports dynamic configuration.

About

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

Application Username

Choose a format to use as the default username value when assigning the application to users.

If you select **None** you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

Credentials Details

[illegible]

Create Reg Form

Form Name :

[Fields](#)
[Details](#)
[Ingest Profile](#)
[Delivery Profile](#)
[Groups](#)
[Projects](#)
[Logo & Css](#)

Field	Default Value	Display
Email ID * :	<input type="text"/>	<input checked="" type="checkbox"/>
Domain Username * :	<input type="text"/>	<input checked="" type="checkbox"/>
First Name * :	<input type="text"/>	<input checked="" type="checkbox"/>
Last Name * :	<input type="text"/>	<input checked="" type="checkbox"/>
Phone * :	<input type="text" value="1"/>	<input type="checkbox"/>
Mobile :	<input type="text"/>	<input type="checkbox"/>
Address 1 * :	<input type="text" value="NY"/>	<input type="checkbox"/>
Address 2 :	<input type="text"/>	<input type="checkbox"/>
Country * :	<input type="text" value="United States"/>	<input type="checkbox"/>
State * :	<input type="text" value="NY"/>	<input type="checkbox"/>
City * :	<input type="text" value="NY"/>	<input type="checkbox"/>
Zip Code :	<input type="text"/>	<input type="checkbox"/>
Comments :	<input type="text"/>	<input type="checkbox"/>

Registration Link :

Address 2 :	<input type="text"/>	<input type="checkbox"/>
Country * :	United States	<input type="checkbox"/>
State * :	NY	<input type="checkbox"/>
City * :	NY	<input type="checkbox"/>
Zip Code :	<input type="text"/>	<input type="checkbox"/>
Comments :	<input type="text"/>	<input type="checkbox"/>
Registration Link :		
http://ec2-3-23-12-133.us-east-2.compute.amazonaws.com/emamgateway/registration/registrationform.aspx?url=4196ac38-c856-45d7-bde4-010f3c167525		
Update		Cancel

29. Go to - C:\Program Files\Empress Media\eMAM Gateway and open web.config

- EnableSAML - true
- AuthenticationType – SAML2
- SAMLRegistration – Enter the registration form url value (Example - 4196ac38-c856-45d7-bde4-010f3c167525)

```
<add key="EnableSAML" value="true" />
<add key="AuthenticationType" value="SAML2" />
<add key="SAMLRegistration" value="4196ac38-c856-45d7-bde4-010f3c167525" />
<add key="ExportAssetsPerPage" value="100" />
```

Comment the <location path="Login.aspx"> like below

```
</system.identityModel.services>
<!--<location path="Login.aspx">
  <system.web>
    <authorization>
      <deny users="?" />
    </authorization>
  </system.web>
</location> -->
</configuration>
```

30. Make sure the **SSO URL** in eMAM Director web.config and eMAM Super admin web.config are correct.

```
<add key="SSOResponseURL" value="https://cp.emamcloud.com/eMAMDirector/Login/Login.aspx" />
<add key="SSORequestURL" value="https://cp.emamcloud.com/eMAMGateway/emamservice.aspx" />
```

31. Access the eMAM Director URL (Example – <https://cp.emamcloud.com>)

32. It will be redirected to the **Okta SSO** and use your Okta credentials there.

Connecting to **eMAM**
You are in control

Sign-in with your emamsolutions-trial-8097395 account to
access eMAM Cloud

okta

Sign In

Username

Password

☐ Keep me signed in

Sign in

[Forgot password?](#)

[Help](#)

33. You will be redirected to the eMAM Director interface home page.