

KB11514, EFT SAML SSO USING OKTA AS THE IDP

Security Assertion Markup Language (SAML) Single Sign On (SSO) provides the end user with a seamless login, allowing access to multiple applications without having to remember multiple credentials. SSO can reduce costs by saving time on password resets and reducing the amount of time end users spend logging on to different applications.

SAML is the standard behind SSO. The current standard is SAML 2.0. This is the only version supported by EFT. SAML uses XML to standardize communications between the Identity Provider (IdP) and the service provider.

This document provides instructions for setting up Globalscape as an application in Okta. Globalscape EFT will be your SAML Service provider (SP).

TERMS TO UNDERSTAND

- SERVICE PROVIDER - The end application requesting authentication (WTC, SharePoint, Office 365, etc.)
- IDENTITY PROVIDER - The identity provider performs the authentication and verifies the end user is who they say they are. (Okta, Active Directory, Gluu)
- ENTITY ID - This is usually an URL or other identifier provided by and exchanged between the Service and Identity Providers
- ASSERTION - The XML document that the Identity Provider sends to the Service Provider that contains the user authorization*

EFT REQUIREMENTS

- EFT Enterprise, v7.3.3. or later
- The Advanced Security Module
- Ensure that SAML / Web SSO is [enabled](#) in EFT.
- Ensure that you have enabled HTTPS in EFT.
- Ensure that you have already created an SSL certificate in EFT

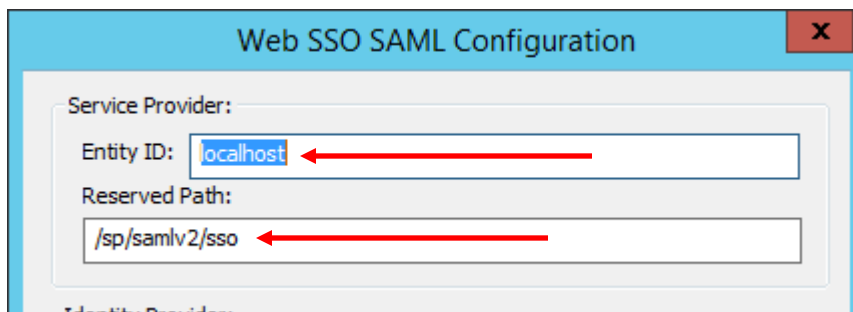
SAML - SETTING UP A GLOBALSCAPE APPLICATION IN OKTA

INITIAL CONFIGURATION

- Gather the Service Provider information from EFT
 - Entity ID
 - Reserved Path
- Create the App
 - Platform: Web
 - Sign on Method: SAML 2.0
 - Single sign on URL: <https://entityid/reservedpath>
 - Audience URI: <https://entityid>
- Optional: Preview the SAML Assertion
 - Assign users to the application (Assignments)
- Provide SAML 2.0 setup instructions to EFT

Before you begin, you will need some information from EFT:

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Site you want to configure.
3. In the right pane, click the **General** tab.
4. Click **SAML (WebSSO)**, click **Configure**. The **Web SSO SAML Configuration** dialog box appears.

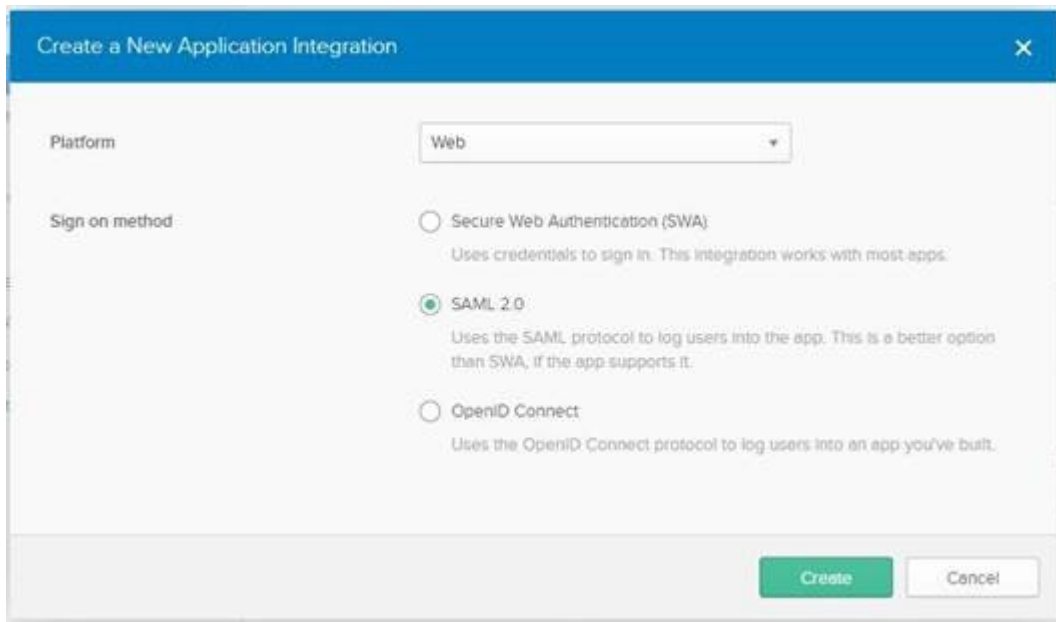


- **Entity ID** - The default is the host name value specified for the EFT Site being configured, e.g., MySite. Any string value can be provided, up to 255 characters, including UTF-8 encoded characters.
- **Reserved Path** - The base address followed by the SSO path, e.g., [hostaddress]/sp/samlv2/sso.

To configure Globalscape as an application in Okta

1. Log in to your Okta organization as a user with administrative privileges.
2. Click **Admin**.

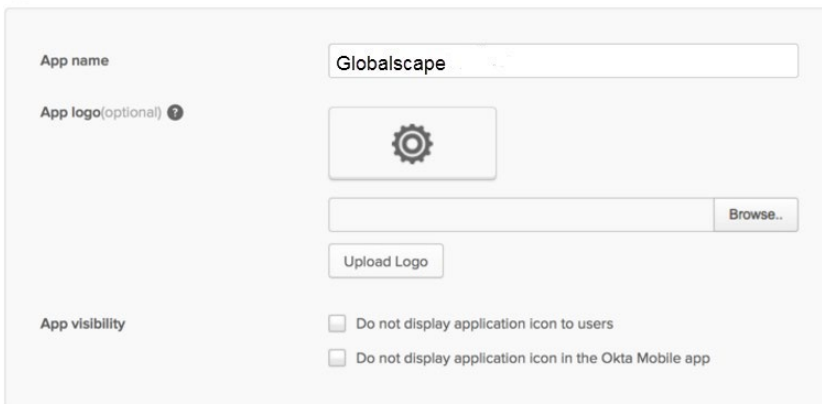
3. Click **Add Applications**.
4. Click **Create New App**. The **Create a New Application** dialog box appears.



The screenshot shows a dialog box titled "Create a New Application Integration". It has a blue header with a close button (X). The main content area is white. There are two sections: "Platform" with a dropdown menu set to "Web", and "Sign on method" with three radio button options. The "SAML 2.0" option is selected. Below the radio buttons are descriptive text lines for each option. At the bottom right, there are two buttons: "Create" (green) and "Cancel" (grey).

5. Leave Platform as is, and select the **SAML 2.0** option, then click **Create**.
6. In the General Setting App name field, type Globalscape, then click Next. (You can also, at this screen, upload the Globalscape logo.)

1 General Settings



The screenshot shows a "General Settings" form. It has a light grey background. The "App name" field is a text input containing "Globalscape". Below it is the "App logo(optional)" section, which includes a gear icon, a text input field, and a "Browse.." button. Below that is an "Upload Logo" button. The "App visibility" section has two checkboxes: "Do not display application icon to users" and "Do not display application icon in the Okta Mobile app", both of which are unchecked.

7. In Okta, type the **Entity ID** and **Reserved path** from the **EFT Web SSO SAML Configuration** dialog box into the **Single sign on URL** and **Audience URI (SP Entity ID)** fields.

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

8. In the **Attribute Statements** section, add three attribute statements:

- “FirstName” set to “user.firstName”
- LastName set to “user.lastName”
- Email set to “user.email”

ATTRIBUTE STATEMENTS (OPTIONAL) [LEARN MORE](#)

Name	Name format (optional)	Value	
<input type="text" value="FirstName"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.firstName"/>	×
<input type="text" value="LastName"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.lastName"/>	×
<input type="text" value="Email"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.email"/>	×

9. Click **Next** to continue.

10. In **Feedback**, select **I'm an Okta customer adding an internal app** and **This is an internal app that we have created** then click **Finish**.

3 Help Okta Support understand how you configured this application

The screenshot shows a feedback form with the following elements:

- Question: "Are you a customer or partner?" with two radio button options:
 - I'm an Okta customer adding an internal app
 - I'm a software vendor. I'd like to integrate my app with Okta
- Information box: "The optional questions below assist Okta Support in understanding your app integration."
- Question: "App type" with a help icon and a checked checkbox:
 - This is an internal app that we have created

11. The **Sign On** section of your newly created SAML Application appears.

The screenshot shows the "Settings" page for a SAML application. The "SIGN ON METHODS" section is highlighted, showing:

- Selected method: SAML 2.0
- Default Relay State: (empty field)
- Warning message: "SAML 2.0 is not configured until you complete the setup instructions." with a "View Setup Instructions" button. A red arrow points to this button.
- Information: "Identity Provider metadata is available if this application supports dynamic configuration."

The "CREDENTIALS DETAILS" section is partially visible below, showing:

- Application username format: Email
- Password reveal: Allow users to securely see their password (Recommended)

12. Right-click on the **Identity Provider metadata** link and click **Copy** and save that link for later.
13. Click **View Setup Instructions**.

The following is needed to configure Globalscape

1 Identity Provider Single Sign-On URL: This will go to the [POST URL] of the "Identity Provider"

https://idp.example.com:4400/saml2/POST/idp

2 Identity Provider Issuer: This will be entered into the [Entity ID] of the "Identity Provider"

https://idp.example.com:4400/saml2

3 X.509 Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDuCCAQgAwIBAgIGAWGrcncspMA0GCSqGSIb3DQEBCwUAMIGcMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcn5pYXV0eWwvZm9udGVudD1kZXI1xHTAbBgNVBAMFG0sb2JhbHNjYXNjaXNjb2ENMA0G
A1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdn1kZXI1xHTAbBgNVBAMFG0sb2JhbHNjYXNjaXNjb2ENMA0G
A1UECgwET2t0YTEU
KoZiInvcNAQkBFg1pbmZvQ99rd9EuY29tMB4XDTA4MDI0MTAxMTA0MFA0XDTI0MTAxMTA0MFA0
gZwxZzA1BgNVBAATA1VIMRMRwEQYDVQQIDAp0YXZpZm9udGVudD1kZXI1xHTAbBgNVBAMFG0sb2JhbHNj
c2NwMQswCQYDVQQKIDARPa3RHRHRQwEgYDVQQkDAtTU09Qcm92aWR1c2JEdMBSGA1UEAwU22xvYmFs
c2NhcGUtamtYdWNoYXZlbnR0eWwvZm9udGVudD1kZXI1xHTAbBgNVBAMFG0sb2JhbHNjYXNjaXNjb2EN
MA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQCITTBUS0CA1PQ6wqz9300PoRc0101v1BLu0PUHbvUeWETfLzFL
AJOV4qzHrGcSU0gkXG+r/byUv10MrJL8YDShQqfMZXDTnULgD2nb1Dk8A80g9D1ErRocjXAtQbH
7NE97QbnEEzWQ71Jf7z2EWqYAhzV4nseSIWp21cgbTL0T9mc8rMqX25vAdpfCIe4WdFJoXrakSxG
KH24uZbI9de82ryz4++XEgT/JQ689e8D5c+4i0ap1V0PA0mS6x1d1VDiPNCB+5wdh1yh2kXuYLpQ
pRdqfAI fNnhoMppciA92f80UplQ4++iM4S81rzZnbTMR0RgzHbse0Z1ITjbd05Xu/AgMBAEEwDQYJ
KoZiInvcNAQELBQADggEBAHh0zZG5h0pFrcuFpIhIZLLetykh+auPxx++Z21ACRFbX6VU48YDX/
f7R09dehuzotZmoeJiQ0G1hfvcvGbxNehSwe0i0ckflpEv+9f1k+Tr0r1VhbRr5mWbpm6ukUZelP
XUGW0s4byXYq76fNmWaP97-gvzcxqokn0ayJXbCQ5/Za6ICElZr1dkXK9Lg7XxIx0EskTYJGZQ
CKoZu6iH0CSY1DDD/XG3ox2zaRwLGVJR1xGfm3LyHh0P1sCqi1Hdt+9c/UnGHMsaFany9dNk1J2
DQE4yH0PRaHff4PoUz5iqP1FS1ColRDZ1PN0IrgkE5gRX9u140GHsaA=
-----END CERTIFICATE-----
```

Download this Certificate, and put in the EFT Data Directory, it's Location will go in the [Public Key] of the "Identity Provider"

Download certificate

14. Click **View Setup Instructions**.

NOTE: You will need to provide the **Single Sign-On URL** and **Identity Provider** to EFT.

The **Entity ID** and **Reserved path** need to be accessible URL from your EFT computer. For example, if you're using a specific port, make sure you are pointing SSO to that port. You also might need to connect to the FQDN to avoid a certificate error.

CONFIGURE EFT

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Site you want to configure.
3. In the right pane, click the **General** tab.
4. Click **SAML (WebSSO)**, click **Configure**. The **Web SSO SAML Configuration** dialog box appears.

Web SSO SAML Configuration

Service Provider:

Entity ID: localhost

Reserved Path: /sp/samlv2/sso

Identity Provider:

Entity ID: https://idp.example.com:4400/saml2

POST URL: https://idp.example.com:4400/saml2/POST/idp

Public Key: []

Username:

Location in assertion: NameID Attribute

Attribute name: []

Identifier format: Unspecified

Parse the username using the regular expression: []

Extend username lookup to authentication provider

Just in Time (JIT) provisioning (if not found) into: Default Setting

Turn on Trace for SAML logger in logging.cfg

OK Cancel

5. Under Identity Provider, provide the **Entity ID** and **POST URL** from the Okta **Setup Instructions**.

TROUBLESHOOTING

When a user clicks the **SSO login** button in the WTC:

- If the user is redirected to the SSO Login provider page, usually the issue isn't with EFT.
- If EFT provides an error message, you need to verify the configuration.

The verbiage used to identify fields can be different between Identity providers but the basic principles remain the same.

WHAT THE EFT LOGS PROVIDE

1. In the [EFT logging.cfg](#) file, enable trace logging:

```
log4cplus.logger.SAMLSSO=TRACE
```

2. When a user clicks **SSO** on the WTC login page, the EFT.log can show the following entries, depending on whether it was successful:

```
EFT user was authenticated by IdP and successfully logged in
```

or failed:

```
ERROR SAMLSSO <HTTP.ProcessRequest> - Issuer ID  
http://www.okta.com/exk2dm7ah76ccEQIE357 does not match expected  
value of http://www.okta.com/exk2dm7ah76ccEQIE35
```

```
01-02-20 16:55:43,302 [5996] DEBUG SAMLSSO <HTTP.ProcessRequest> - authnstatement count  
= 1
```

```
01-02-20 16:55:43,302 [5996] DEBUG SAMLSSO <HTTP.ProcessRequest> - notBefore 1578005536  
notOnOrAfter 1578006136 (now is
```

```
1578005743)
```

```
01-02-20 16:55:43,302 [5996] DEBUG SAMLSSO <HTTP.ProcessRequest> - Assertion::Conditions  
Condition count 0
```

```
01-02-20 16:55:43,302 [5996] DEBUG SAMLSSO  
<HTTP.ProcessRequest> - Assertion::Conditions OneTimeUse count  
0 01-02-20 16:55:43,302 [5996] DEBUG SAMLSSO  
<HTTP.ProcessRequest> - ProcessAssertion returns  
AssertionSuccess, numSuccessfulAuthnStatements = 1
```

```
01-02-20 16:55:43,302 [5996] DEBUG SAMLSSO  
<HTTP.ProcessRequest> - final check: Status code is  
'urn:oasis:names:tc:SAML:2.0:status:Success', username is  
'eleenheer@globalscape.com', numSuccessfulAuthnStatements = 1
```

```
01-02-20 16:55:43,333 [5996] DEBUG SAMLSSO <HTTP.ProcessRequest> -  
CHTTPSocket::HandleSAMLSSO - RelayState is '/'
```

```
01-02-20 16:55:43,333 [5996] DEBUG SAMLSSO <HTTP.ProcessRequest> -  
CHTTPSocket::HandleSAMLSSO - RelayState is '/' and SavedPathCookie is  
'/'. SavedPathCookie is more specific so that takes precedence.
```

```
01-02-20 16:55:43,333 [5996] TRACE SAMLSSO <HTTP.ProcessRequest> -  
CHTTPSocket::HandleSAMLSSO - looking for absolute prefix  
https://test.churillo.com/
```

```
01-02-20 16:55:43,349 [5996] DEBUG SAMLSSO <HTTP.ProcessRequest> -  
CHTTPSocket::HandleSAMLSSO -
```

```
m_bEmbeddedDownloadLinkRequest = false for /
```

```
01-02-20 16:55:43,349 [5996] DEBUG SAMLSSO <HTTP.ProcessRequest> -  
CHTTPSocket::HandleSAMLSSO - EFT user was authenticated by IdP and successfully logged  
in
```

KB11514 - EFT SAML SSO USING OKTA AS THE IDP

```
01-02-20 16:55:43,349 [5996] DEBUG SAMLSSO <HTTP.ProcessRequest> -
CHTTPSocket::HandleSAMLSSO - redirecting to path /

01-02-20 16:59:12,787 [3560] DEBUG SAMLSSO <HTTP.ProcessRequest> - assertion count = 1

01-02-20 16:59:12,787 [3560] DEBUG SAMLSSO <HTTP.ProcessRequest> - encrypted assertion
count = 0

01-02-20 16:59:12,787 [3560] DEBUG SAMLSSO <HTTP.ProcessRequest> -
SAMLAntiReplay::ConfirmResponse - confirmed ID afe50491a-e8c7- 47e9-815f-4db8aadfbc78

01-02-20 16:59:12,787 [3560] DEBUG SAMLSSO
<HTTP.ProcessRequest> - SAMLResponse issuer
ID is
http://www.okta.com/exk2dm7ah76ccEQIE357

01-02-20 16:59:12,787 [3560] ERROR SAMLSSO <HTTP.ProcessRequest> - issuer ID
http://www.okta.com/exk2dm7ah76ccEQIE357
URL: / / www.okta.com/exk2dm7ah76ccEQIE357

01-02-20 16:59:12,787 [3560] DEBUG SAMLSSO <HTTP.ProcessRequest> -
CHTTPSocket::HandleSAMLSSO - WebSSO user login failed. SAMLResponse error -
Issuer Entity ID mismatch

01-02-20 16:59:12,944 [6960] TRACE SAMLSSO <HTTP.ProcessRequest> -
CHTTPSocket::HandleSAMLSSO - GET /

01-02-20 16:59:12,944 [6960] TRACE SAMLSSO <HTTP.ProcessRequest> -
CHTTPSocket::HandleSAMLSSO - request path '/' is not service provider reserved
path '/sp/samlv2/sso'

01-02-20 16:59:13,006 [840] TRACE SAMLSSO <HTTP.ProcessRequest> -
CHTTPSocket::HandleSAMLSSO - GET

/EFTClient/Account/Login.htm

01-02-20 16:59:13,006 [840] TRACE SAMLSSO <HTTP.ProcessRequest>
- CHTTPSocket::HandleSAMLSSO - request path
'/EFTClient/Account/Login.htm' is not service provider reserved
path '/sp/samlv2/sso'

01-02-20 16:59:13,006 [840] DEBUG SAMLSSO <HTTP.ProcessRequest> -
CHTTPSocket::SendLoginPageWithError - HTTP SAMLSSO ERROR COOKIE NAME present ...
enabling WTC SSO error message: There was a problem processing your single sign on
request. Please re-type your login credentials and try again. Contact your EFT
administrator if you continue to experience this error upon future login attempts.

01-02-20 16:59:13,006 [840] TRACE SAMLSSO
<HTTP.ProcessRequest> - CHTTPSocket::SendLoginPageWithError
- Enabling WebSSO Login button
```