Integrate OKTA with ESA for SAML Authentication

Contents

Introduction

This document describes the integration of Email Security Appliance (ESA) and OKTA for Security Assertion Markup Language (SAML) authentication.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- OKTA, more information can be found at Understand SAML | Okta Developer
- General Public Key Infrastructure (PKI) Knowledge

Components Used

The information in this document is based on these software and hardware versions:

- Active Directory
- Cisco Email Security Appliance 13.x.x or later versions
- OKTA

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

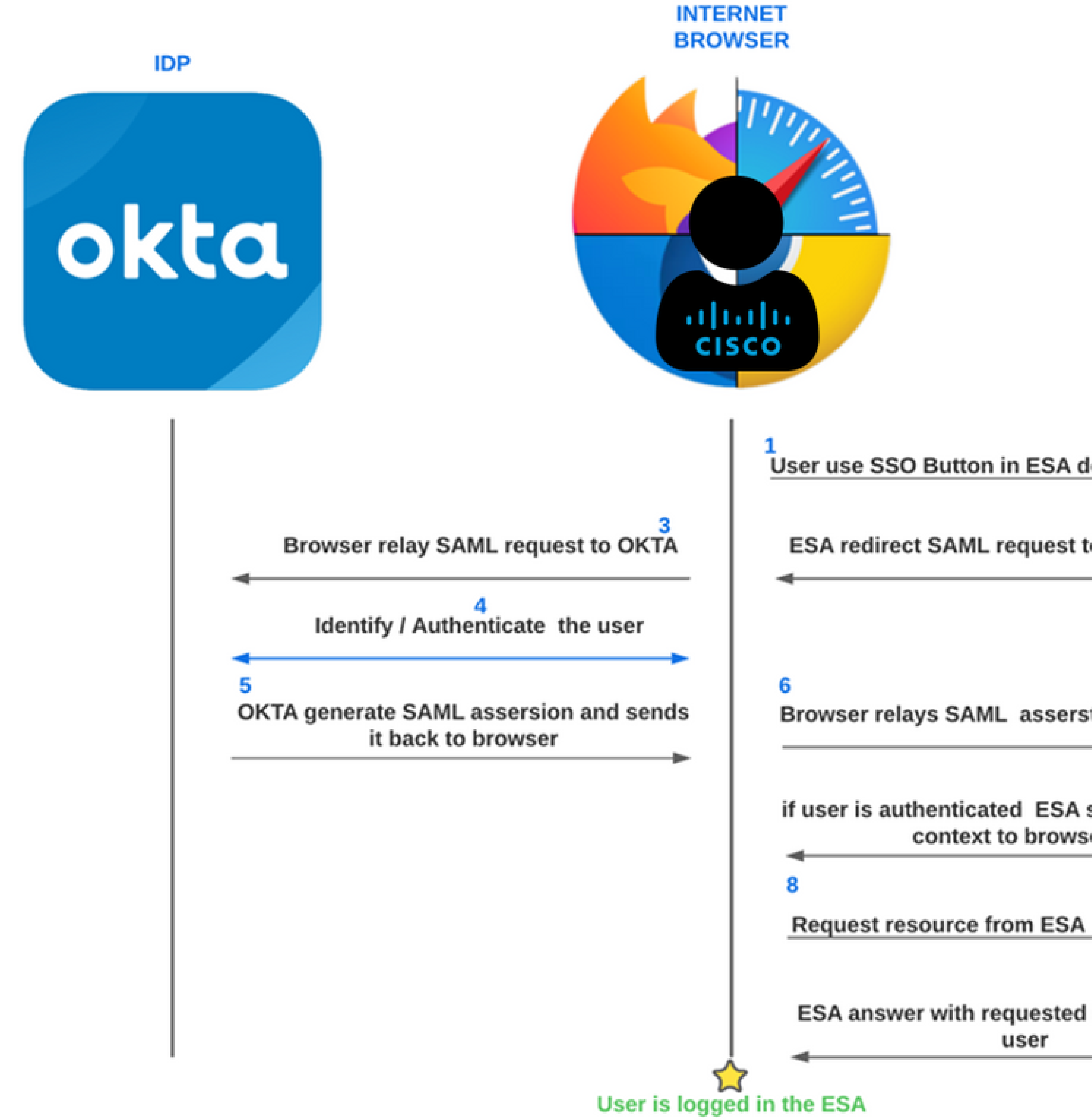
Background Information

OKTA is a two-factor authentication service provider that adds a layer of security to SAML authentication.

SAML is a federation method for authentications. It was developed to give secure access and separate the identity provider and service provider.

The Identity Provider (IdP) is the Identity that stores all the information of users in order to permit the authentication (which means OKTA has all the user information to confirm and approve an authentication request).

The Service Provider (SP) is the ESA.

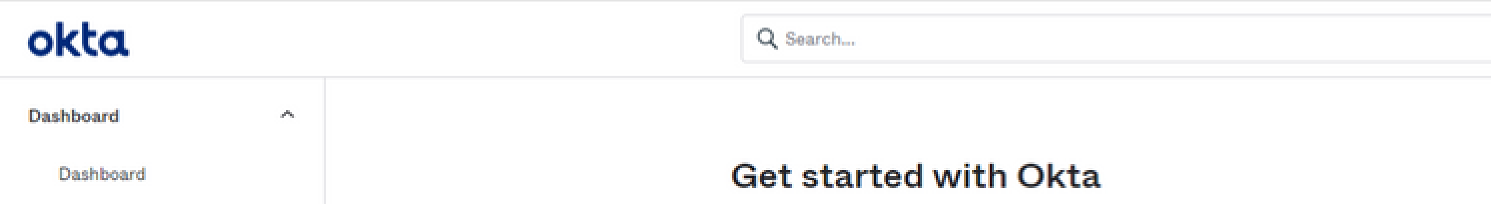

IDP
okta
INTERNET BROWSER
CISCO
1
User use SSO Button in ESA d
3
Browser relay SAML request to OKTA
ESA redirect SAML request t
4
Identify / Authenticate the user
5
OKTA generate SAML assersion and sends it back to browser
6
Browser relays SAML asserst
if user is authenticated ESA s
context to brows
8
Request resource from ESA
ESA answer with requested
user
User is logged in the ESA

ESA OKTA SAML process

Configure

OKTA Configuration

1. Create OKTA Application. Then navigate to Applications.



on Windows or Linux. If you want to configure a self-signed certificate, you can do that with the next steps or you can use your certificate:

1. Create the private key. This helps to enable encryption or decryption.

```
openssl genrsa -out domain.key 2048
```

2. Create a Certificate Signing Request (CSR).

```
openssl req -key domain.key -new -out domain.csr
```

3. Create the self-signed certificate.

```
openssl x509 -signkey domain.key -in domain.csr -req -days 365 -out domain.crt
```

If you want more days, you can change the value after -days .

> **Note**: Remember, by best practices, you must not put more than 5 years for the certificates.

After that, you have the certificate and keys to upload on the ESA in the option upload certificate and key.

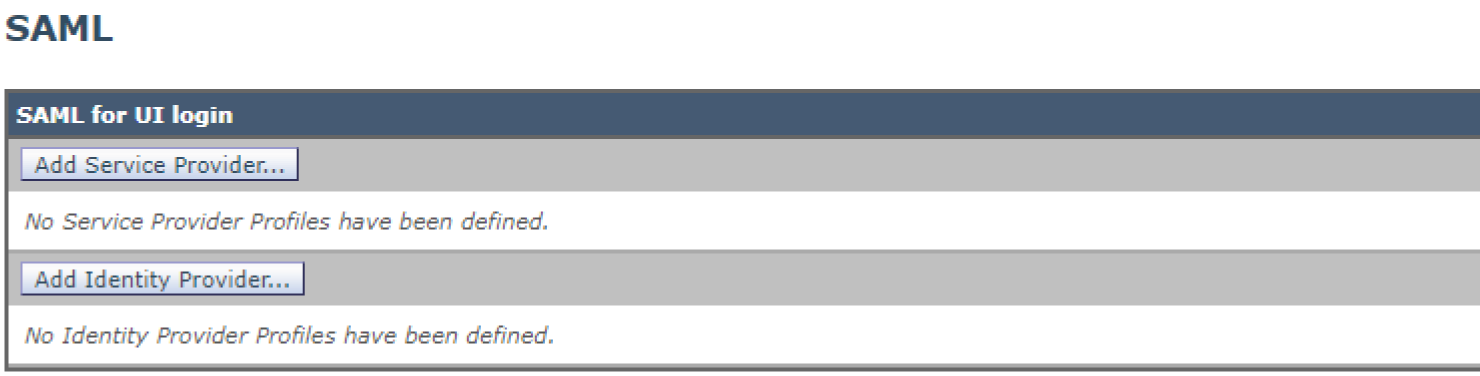
> **Note**: If you want to upload the certificate in PKCS #12 format, it is possible to create it after Step 3.

(Optional) From PEM format to PKCS#12 format.

```
openssl pkcs12 -inkey domain.key -in domain.crt -export -out domain.pfx
```

For organization details, you can fill it as you want and click submit.

3. Navigate to System Administration > SAML and choose Add Identity Provider.



SAML

SAML for UI login

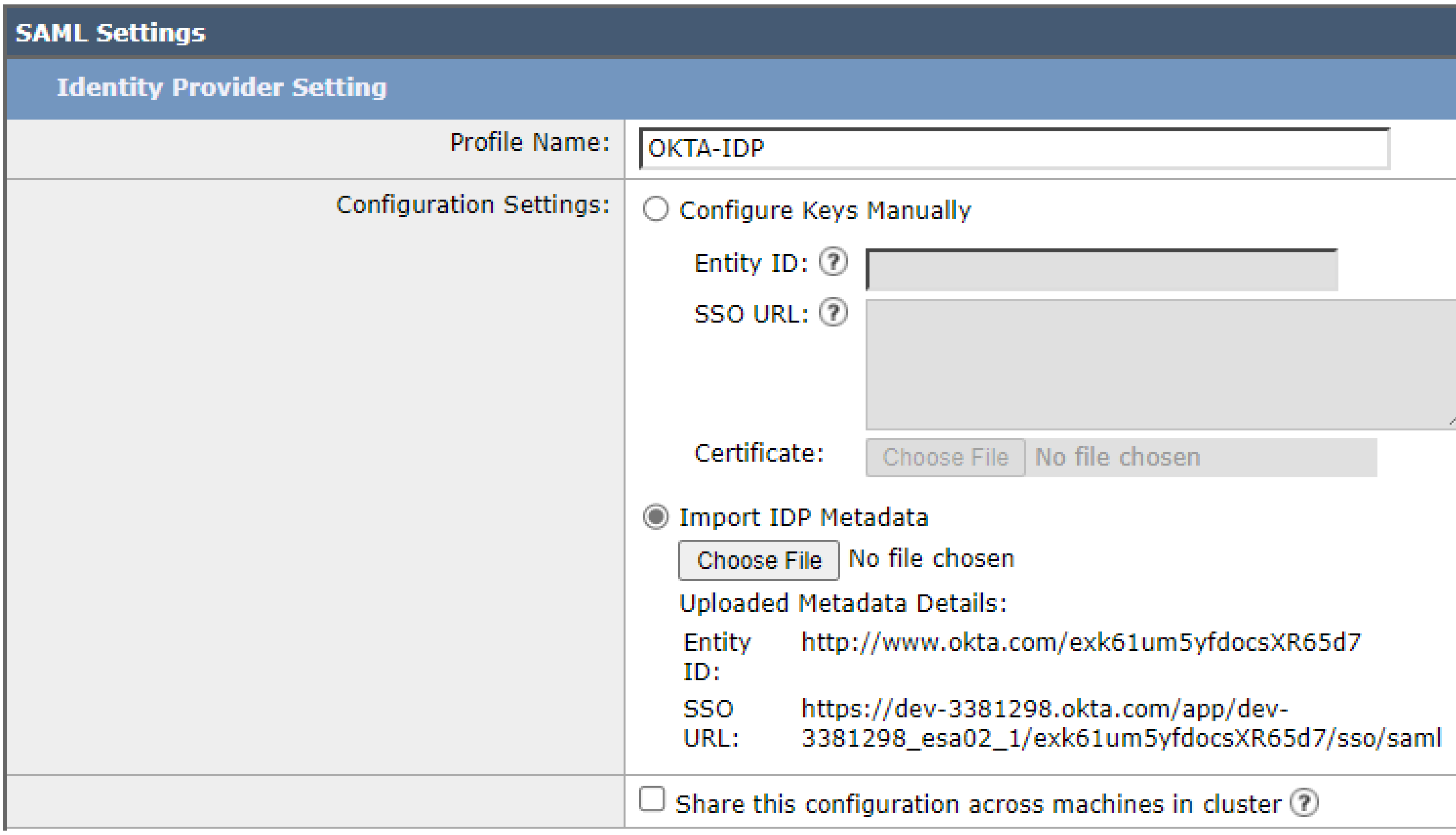
Add Service Provider...

No Service Provider Profiles have been defined.

Add Identity Provider...

No Identity Provider Profiles have been defined.

ESA SAML IdP configuration



SAML Settings

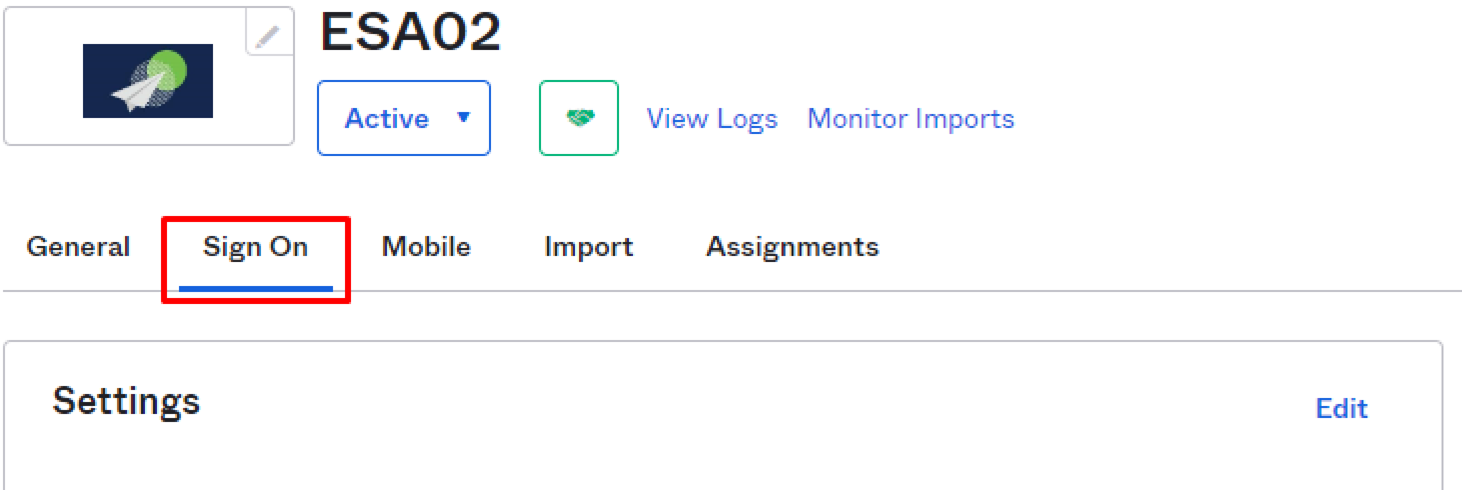
Identity Provider Setting

Profile Name:	OKTA-IDP
Configuration Settings:	○ Configure Keys Manually Entity ID: SSO URL: Certificate: Choose File No file chosen ● Import IDP Metadata Choose File No file chosen Uploaded Metadata Details: Entity ID: http://www.okta.com/exk61um5yfdocsXR65d7 SSO URL: https://dev-3381298.okta.com/app/dev-3381298_esa02_1/exk61um5yfdocsXR65d7/sso/saml
	□ Share this configuration across machines in cluster

ESA IdP settings configuration

In this step there are two options, you can upload that information manually or via an XML file.

In order to do that, you must navigate to your OKTA Application and find the IDP metadata .



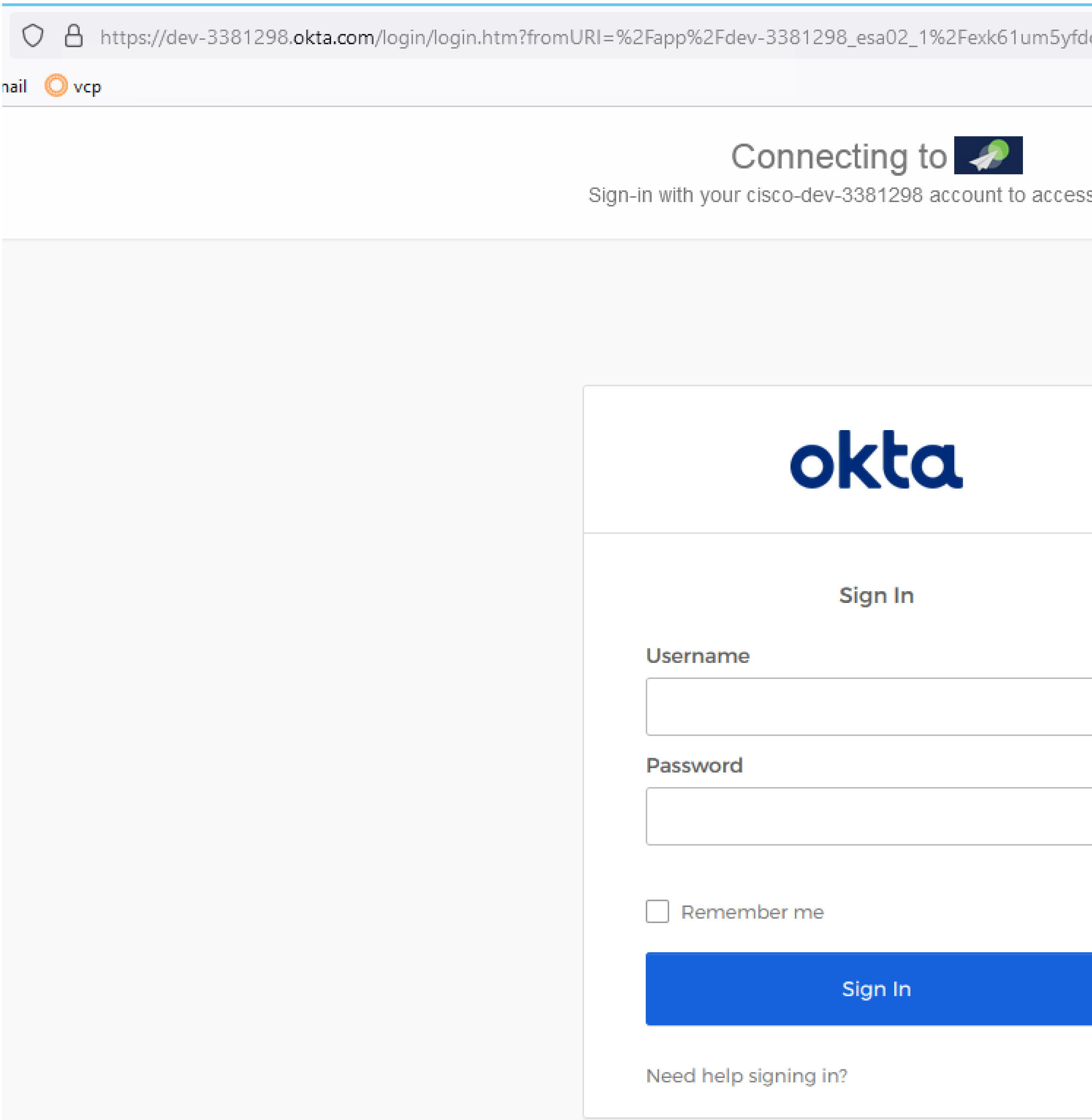
ESA02

Active ▾ View Logs Monitor Imports

General Sign On Mobile Import Assignments

Settings Edit

button, you are redirected to the IdP service (OKTA) and you must provide the username and password to authenticate, or, if you have fully integrated with your domain, you are automatically authenticated in the ESA.



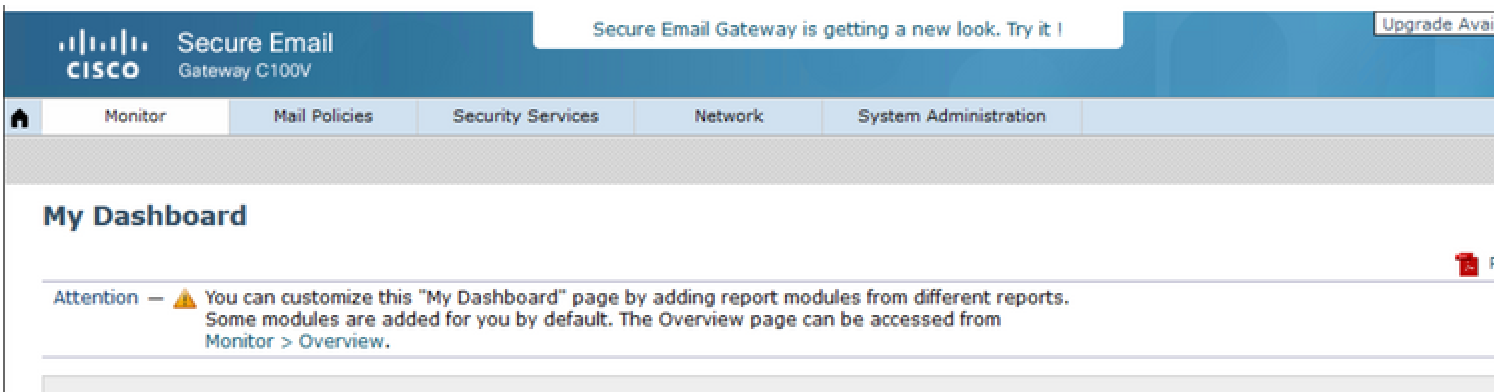
https://dev-3381298.okta.com/login/login.htm?fromURI=%2Fapp%2Fdev-3381298_esa02_1%2Fexk61um5yfd

Connecting to

Sign-in with your cisco-dev-3381298 account to access

ESA OKTA authentication

After you enter your OKTA login credentials, you are redirected to the ESA and authenticated as in the next image.



My Dashboard

Attention — ⚠ You can customize this "My Dashboard" page by adding report modules from different reports. Some modules are added for you by default. The Overview page can be accessed from Monitor > Overview.