Technical Documentation

Federated login

Opus Neo

RESUME

This document is to describe and document the changes and products that is implemented in a clients server environment in regards to Federated login using IBM Domino and OKTA.

...opus neo -
Opus Neo Aps
Dr. Neergaards Vej 5B
2970 Hoersholm
+45 70 27 10 66
info@opusneo.dk
www.opusneo.com
facebook.com/neodashboard

Table Of Content

...opus neo -
Opus Neo Aps
Dr. Neergaards Vej 5B
2970 Hoersholm
+45 70 27 10 66
info@opusneo.dk
www.opusneo.com
facebook.com/neodashboard

Introduction

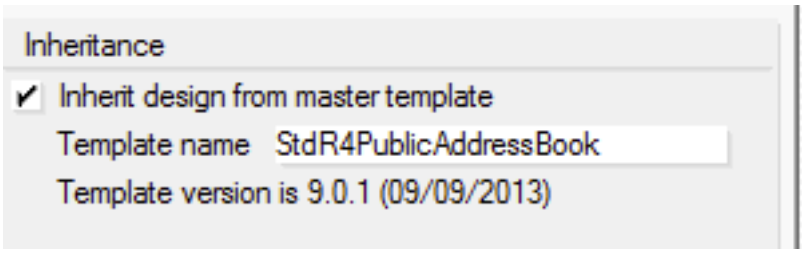
This document is to describe and document the changes and products that has been implemented by Opus Neo in the client server environment in regards to Federated Login using IBM Domino and OKTA.

1. IBM Domino

The implementations in IBM Domino requires experienced Domino Administrator knowledge. When relevant, links to the standard documentation from IBM is added.

1.1 Design version for Names.nsf

Verify that design is based on the StdRxxxPublicAddressBook Template 9.0.1, 09/09/2013 or newer on your web server. From this version Domino is SAML enabled.



1.2 Idp catalog

Create a new Idp catalog database based on the template. Follow the instructions here to:
- Create Idpcat.nsf
- Add Idp config document
- **NOTE!** Choose "TFIM" as the Fedaration Product

How to retrieve the Metadata.xml file is described in section 2.2.
NOTE! Check the certificate string in Notepad as there can be hidden carriage returns in the text

...opus neo -
Opus Neo Aps
Dr. Neergaards Vej 5B
2970 Hoersholm
+45 70 27 10 66
info@opusneo.dk
www.opusneo.com
facebook.com/neodashboard

1.3 Notes.ini – Debug SAML

For debugging purposes, insert the following settings in Notes.ini on the SAML server:

DEBUG_SAML=31

Other SAML Settings:

SAML_NotOnOrAfterSkewInMinutes=[#]
Allows extra minutes in the 'not on or after' timestamp check on the SAML assertion.

SAML_NotBeforeSkewInMinutes=[#]
Allows extra minutes in the 'not before' timestamp check on the SAML assertion.

0x0001 (1) -Debug output contains information from http side.
0x0002 (2) -Debug output contains SAML parse information.
0x0004 (4) -Debug output only contains errors.
0x0008 (8) -Debug to dump decoded assertion.
0x0010 (16) -Debug to trace idpcatactivity
0x0020 (32) -Trace replay prevention
0x0080 (128) -Dump the entire XML tree
0x0100 (256) -Dump canonicalizedbuffers
0x0200 (512) -Debug for the library sort
0x0800 (2048) -Debug for namespace use
0x2000 (8192) -Debug output for certificate management

1.4 Internet Site Document

Create a new Internet Site Document or use an existing document for your site. Follow the instructions here.

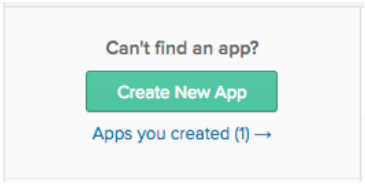
NOTE! Verify your Internet Site is working before switching to SAML

...opus neo -
Opus Neo Aps
Dr. Neergaards Vej 5B
2970 Hoersholm
+45 70 27 10 66
info@opusneo.dk
www.opusneo.com
facebook.com/neodashboard

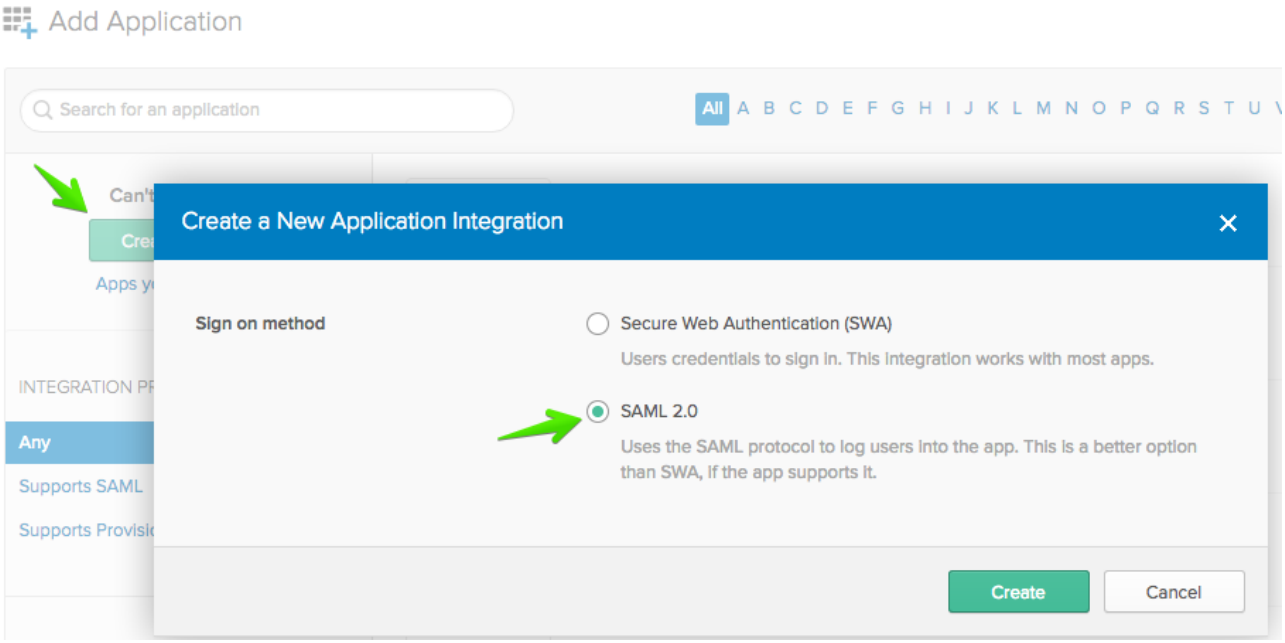
2. OKTA

2.1 OKTA APP SAML 2.0

Create a new App using the "SAML App integration Wizard". Start by clicking the "Create New App" button:

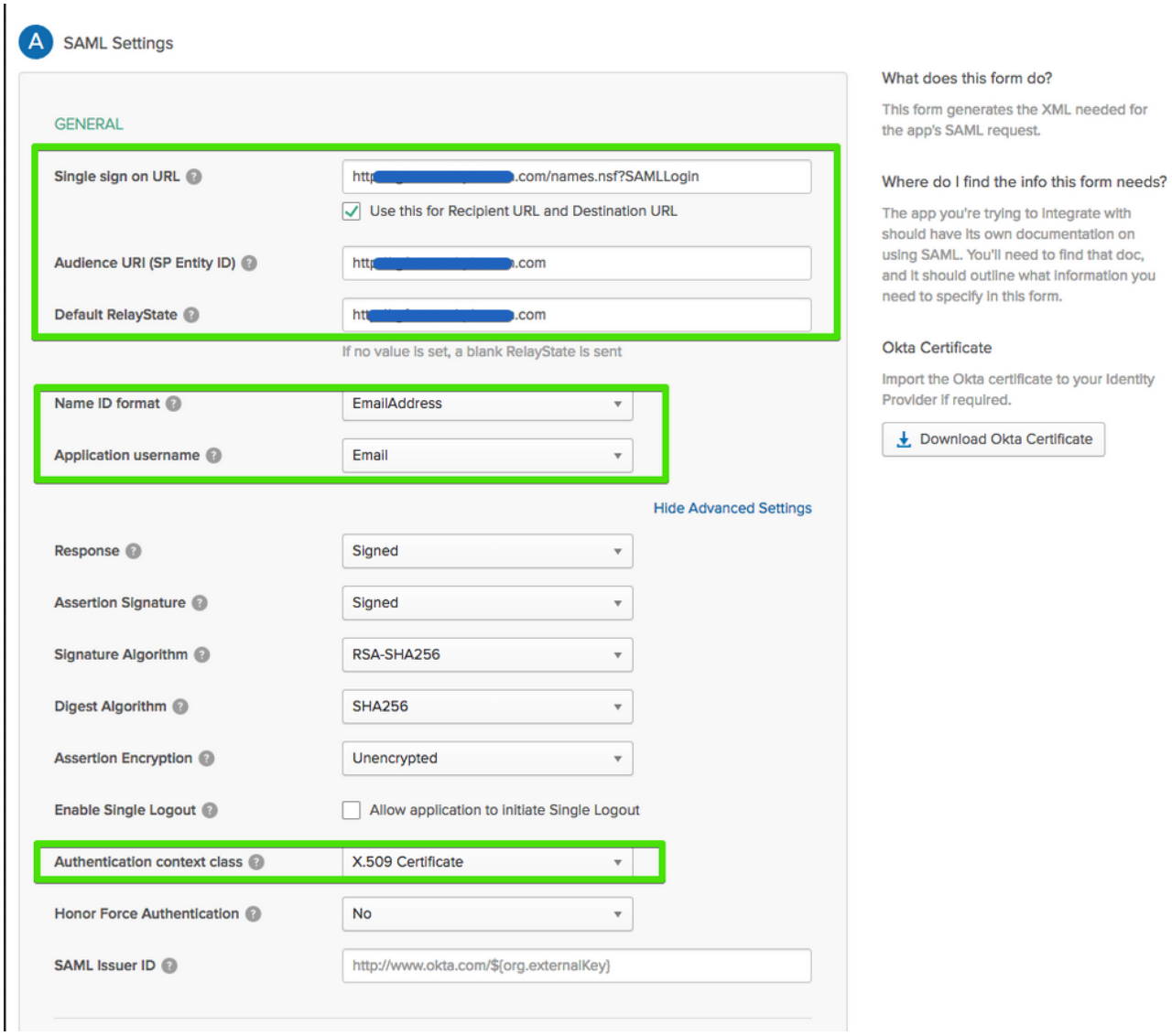


Choose SAML 2.0 to start the wizard.



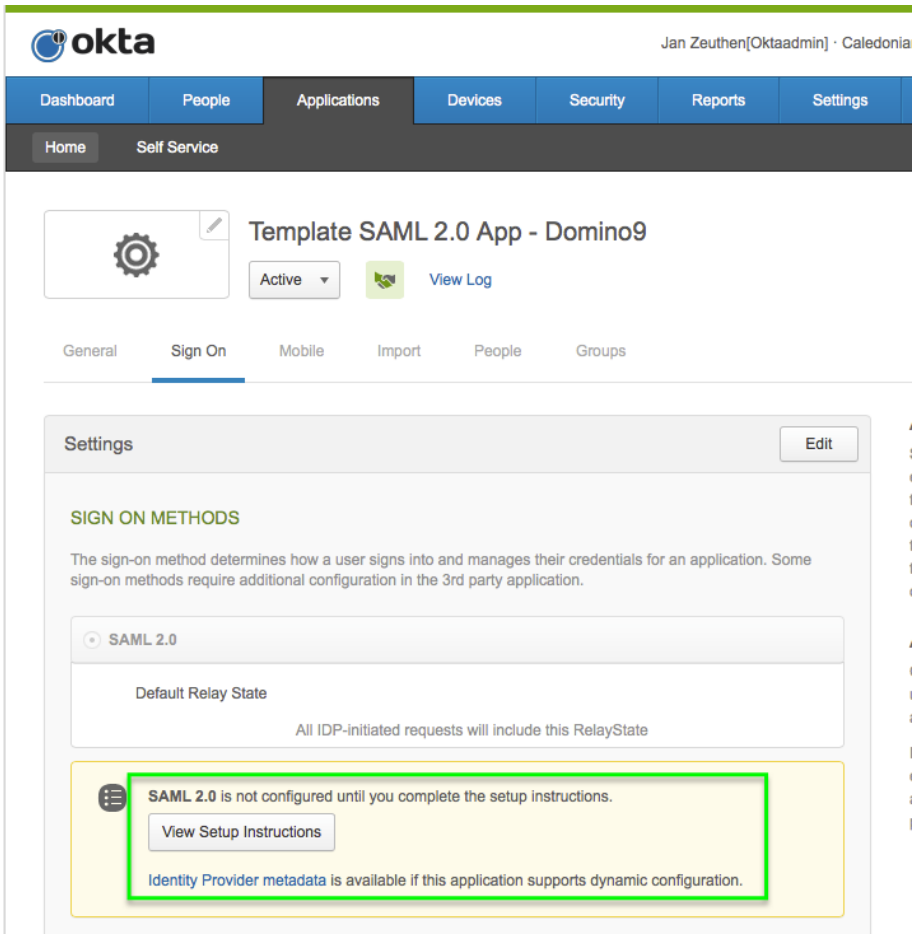
...opus neo -
Opus Neo Aps
Dr. Neergaards Vej 5B
2970 Hoersholm
+45 70 27 10 66
info@opusneo.dk
www.opusneo.com
facebook.com/neodashboard

Fill in the appropiate fields for your setup. The settings are included in the source for the metadata.xml file:



...opus neo -
Opus Neo Aps
Dr. Neergaards Vej 5B
2970 Hoersholm
+45 70 27 10 66
info@opusneo.dk
www.opusneo.com
facebook.com/neodashboard

2.2 Retrieving the Metadata.xml



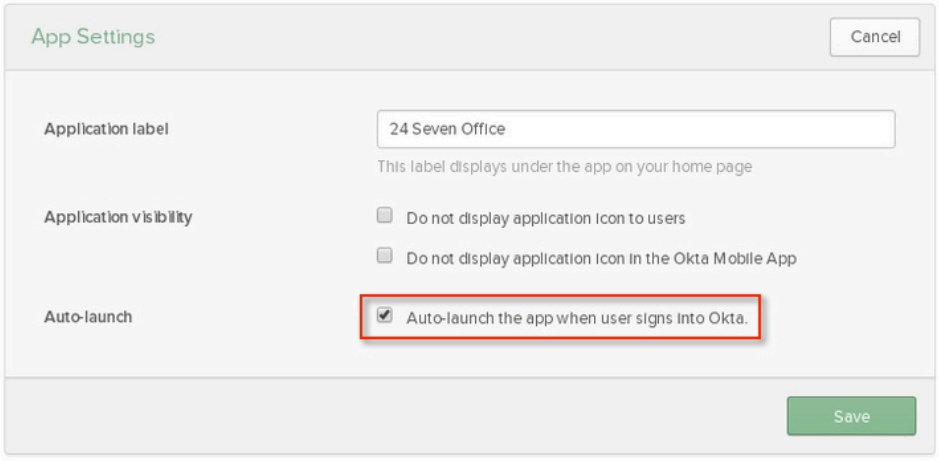
The text “Identity Provider metadata” is the link for the Metadata.xml file.

2.3 AUTO-Launch App

After testing the SAML assertion successfully, you can enable the App to Auto-Launch after the user logs in.

From Okta Help:
Admins can now auto-launch a specific app for all end users at sign in. Previously, this option was only available to end users. Now, admins can access this option from the specific **<*App*> page > General tab > App Settings**, as detailed in Using the Okta Applications Page.
Note: Checking this option only affects end users that are newly assigned to the app. Previously assigned users must manually choose auto-launch by accessing the app chiclet **<*App*> Settings** button.

...opus neo -
Opus Neo Aps
Dr. Neergaards Vej 5B
2970 Hoersholm
+45 70 27 10 66
info@opusneo.dk
www.opusneo.com
facebook.com/neodashboard



2.4 Next Step:

Test Test Test... :-)

...opus neo -
Opus Neo Aps
Dr. Neergaards Vej 5B
2970 Hoersholm
+45 70 27 10 66
info@opusneo.dk
www.opusneo.com
facebook.com/neodashboard