

DUO Deployment Guide

Table of Content

DUO Deployment Guide	1
Introduction	1
DUO side configuration	1
NSO Side Config	5
<i>Native NSO SSO Installation – Clear Text Communication</i>	5
<i>Containerized NSO SSO Installation – Assertion Encryption</i>	5
Verify the Setup	7

Introduction

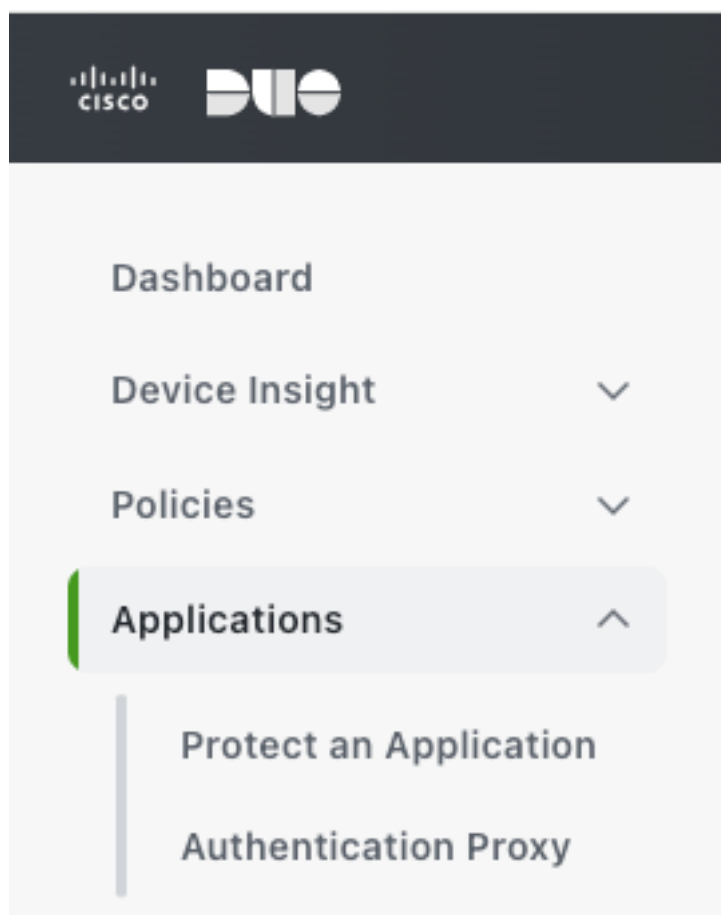
For NSO as a Service Provider, it handles the following path throughout the SAML communication inside “cisco-nso-saml2-auth/scripts/authenticate”. In other words, the “cisco-nso-saml2-auth” package gives the SSO feature to the NSO via packages authentication.

- LOGIN_PATH and LOGOUT_PATH is the path that used to handle login/logout request.
- ACS_PATH is the path towards ACS after success or failed authentication on the IDP side
- METADATA_PATH is the path that store NSO Service Provider Metadata that can be used for automatic metadata parsing from the IDP side.

```
LOGIN_PATH = "/saml/login/"
LOGOUT_PATH = "/saml/logout/"
ACS_PATH = "/saml/acs/"
METADATA_PATH = "/saml/metadata/"
```

DUO side configuration

The two most important parameter that need on DUO and NSO side configuration is the Metadata URL from each of them. In this chapter we call it DUO_URL and NSO_URL. Both DUO and NSO side can benefit from these URL to auto-populate the configuration by learning each other's metadata. To obtain the Metadata from the DUO side and configure the DUO side configuration, one need to add the NSO as an Application that protected by DUO. Start with Click on “Protect an Application” from the left side of the DUO admin panel



Select “Generic SAML Service Provider”. After entering the “Generic SAML Service Provider” configuration page, one can obtain the necessary configuration that NSO need include the Metadata URL. For our example here, we only need the Metadata URL to auto populate rest of the field from the metadata.

Generic SAML Service Provider - Single Sign-On

See the [Generic SSO documentation](#) to integrate Duo into your SAML-enabled service provider.

Metadata

Entity ID	<input type="text" value="/metadata"/>	Copy
Single Sign-On URL	<input type="text" value="/sso"/>	Copy
Single Log-Out URL	<input type="text" value="/slo"/>	Copy
Metadata URL	<input type="text" value="/metadata"/>	Copy

Certificate Fingerprints


SHA-1 Fingerprint	<input type="text"/>	Copy
SHA-256 Fingerprint	<input type="text"/>	Copy

Downloads

Certificate	Download certificate	Copy certificate	Expires: 01-19-2038
SAML Metadata	Download XML		

Afterwards, we need to configure the Service Provider field. Choose Metadata XML URL and provide the Public Metadata URL of your NSO instance that can be access by DUO and other external network. Click on “Populate” to auto populate rest of the fields. One thing that need to watch out here is you need a successfully log in cookies before the “Populate” can be success. In this case, log into your WebUI One once and then “Populate” in DUO without log out the WebUI One.

Service Provider

Metadata Discovery	<input type="text" value="Metadata XML URL"/>
Metadata XML URL	<input type="text" value="/metadal"/> Populate
Paste and populate the Metadata XML URL provided by your service provider.	
 Successfully populated: ACS URL, Entity ID, Single Logout URL	

After the Metadata configuration, maps the group that synced from the Active Directory through Directory Sync to the NSO NACM group name in the Role attributes field. In the Figure below, one can see we map the Domain Admin to “admin” group while the Domain Guests to the “oper” group.

Role attributes Map Duo groups to different roles in this service provider. A Duo group can be mapped to multiple roles and each role can have multiple groups mapped to it. Optional. [Learn more about Duo groups.](#)

Attribute name
groups

The name of the attribute which will carry the mapped roles.

Service Provider's Role	Duo groups
admin	<div><div>Domain Admins (from AD sync "AD Sync") (3 users)</div><div>⊖</div></div>
oper	<div><div>Domain Guests (from AD sync "AD Sync") (1 user)</div><div>⊖ ⊕</div></div>

Choose a suitable name for this application instance in DUO under the Settings and press “Save” at the bottom of the page

Settings

Type Generic SAML Service Provider - Single Sign-On

Name NSO DUO Testing - Native Instance

Duo Push users will see this when approving transactions.

If Assertion Encryption is needed for extra layer of security, set the “Existing certificate” to the Certificate that used on the Service Provider side. At the same time select “AES256-GCM” for the “Assertion encryption algorithm” and “RSA-OAEP (with fixed SHA mask)” for “Key transport encryption algorithm”.

Assertion encryption ☒ Encrypt the SAML assertion

Existing Certificate *

C=AU/O=Internet Widgits Pty Ltd/ST=Some-State - 2025-08-05 13:00:30+00:00

No file chosen

Assertion encryption algorithm

AES256-GCM

Key transport encryption algorithm

RSA-OAEP (with fixed SHA mask)

That conclude the DUO configuration. Since now we have both DUO and NSO Metadata URL in hand, let's proceed with NSO installation. NSO installation can either be done via Native Installation on the barebone machine or via the Containerized NSO inside Docker Container. The guide below is based on the example usecase that is provided by Cisco. You can use it as a starting point to proceed forward.

NSO Side Config

Two examples are provided by Cisco. Native NSO SSO Installation provides a use case with local install NSO on the barebone machine and clear text communication between NSO and IDP. At the same time, Containerized NSO SSO Installation focuses on distributed cloud NSO installation with container. In Containerized NSO SSO Installation, the communication between NSO and IDP is done with Assertion Encryption.

For both examples, the Makefile will also generate the keys and certification via the “keys.gen” file. The Service Provider private key is named as “sp.key” while the certificate is named as “sp.crt”. At the same time, the ncs.conf has preset by enable the single-sign-on and package-authentication based on the NSO guide below.

<https://developer.cisco.com/docs/nso/guides/single-sign-on/#single-sign-on>

<https://developer.cisco.com/docs/nso/guides/the-aaa-infrastructure/#ug.aaa.packageauth>

Sample configuration in ncs.conf can be found as below. In this sample configuration, we set the package that used in this guide - “cisco-nso-saml2-auth” in “package-authentication/packages/package” to make sure NSO use the correct package for SSO.

```
<aaa>
  <single-sign-on>
    <enabled>true</enabled>
  </single-sign-on>

  <package-authentication>
    <enabled>true</enabled>
    <packages>
      <package>cisco-nso-saml2-auth</package>
    </packages>
  </package-authentication>
</aaa>
```

Native NSO SSO Installation – Clear Text Communication

Example Repository: <https://github.com/NSO-developer/nso-ssso-duo-integration---native>

Packages Repository: <https://github.com/NSO-developer/nso-ssso-duo-integration-package>

The important part to enable SSO in NSO is the

- SAML configuration include Service Provider and IDP
- Key/Cert that can be used during the SAML communication,
- ncs.conf to enable the package authentication and SSO feature on the NSO
- the AAA/PAM configuration

In this example, we automated all the part that mentioned above by execute the “Makefile” with DUO_URL and NSO_URL parameter. By specify these two parameters, the correct configuration “cisco-nso-saml2-auth.xml” will be generated and “load replace” to the NSO. Sample command can be found as below

```
DUO_URL=--<DUO Metadata URL> NSO_URL=--<NSO External access URL> make clean all
```

Containerized NSO SSO Installation – Assertion Encryption

Example Repository: <https://github.com/NSO-developer/nso-ssso-duo-integration---containerized-nso>

Packages Repository: <https://github.com/NSO-developer/nso-ssso-duo-integration-package>

Similarly to the “Native NSO SSO Installation” the SAML configuration (SP and IDP), keys and certificates, ncs.conf and the AAA/PAM configuration are necessary for this enablement. All which were also automated in the example. Additionally, we are also automating the installation of containerized NSO where one needs to include the pre-built images for production and development in the “images” folder. The sample command will be the same as for the native example:

```
DUO_URL=--<DUO Metadata URL> NSO_URL=--<NSO External access URL> make clean all
```

This example also enabled the Assertion Encryption feature. Therefore the “private-key-encryption” configuration is also needed. The key that needs to fill into the “private-key-encryption” is the private key of the Service Provider. With the same private key, Service Provide Certification is generated and need to provide to the DUO side. These steps have been automated in this example.

Verify the Setup

After all configuration is done, access the NSO_URL from your browser than click on cisco-nso-saml2-auth as shown in the screenshot below.



Crosswork Network Service Orchestrator

Username *

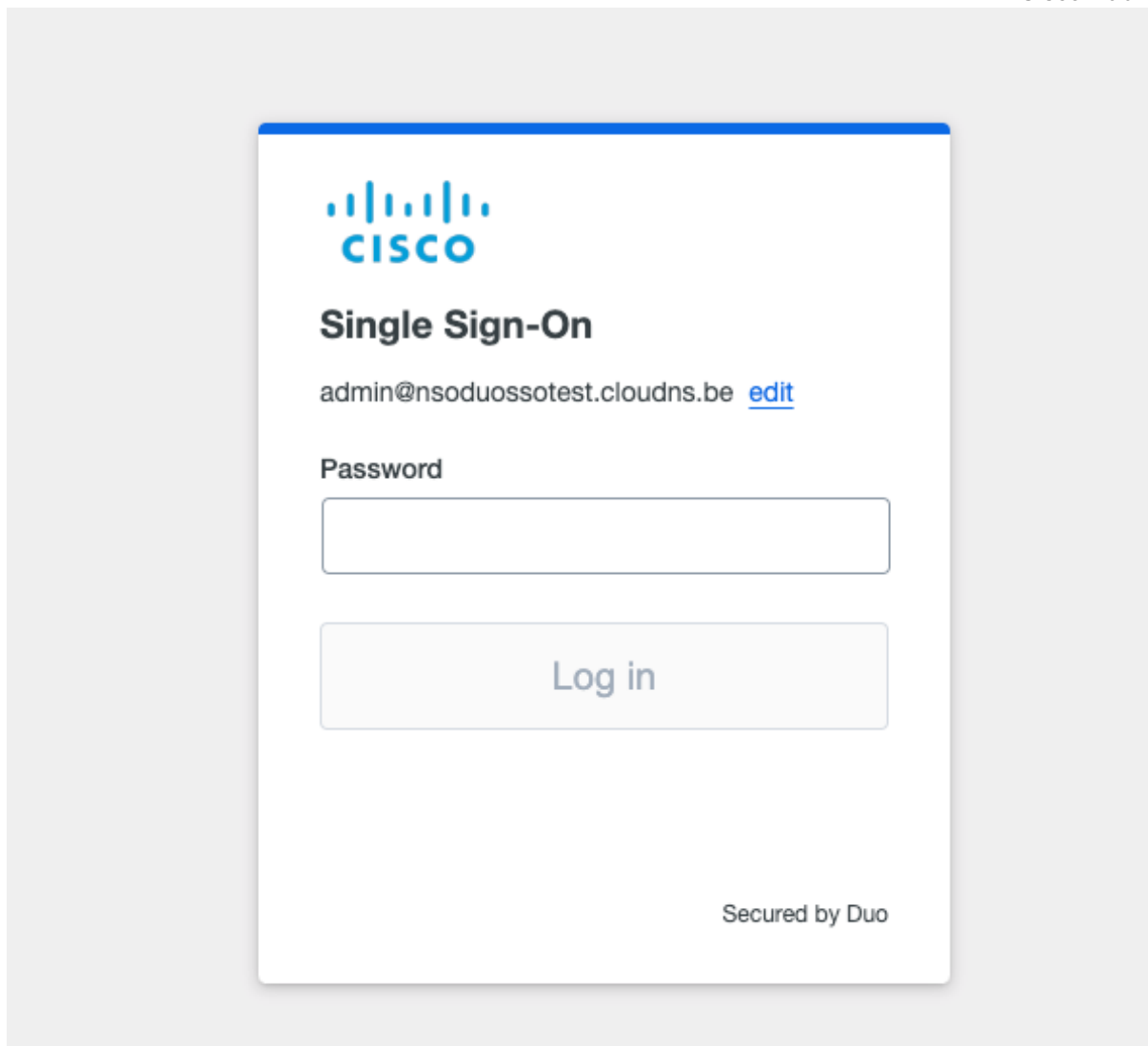
Password *

 [Show](#)

Login

[cisco-nso-saml2-auth](#)

If everything configured correctly, you will be redirected to DUO SSO page. Otherwise, it will show “No Auth Method”.



After successfully logged in, one will get redirect to the Home of the WebUI One(Redirect only available after 6.3).

