Lumen® SD-WAN with Versa Networks

SAML Integration

LUMEN®

General Disclaimer

Although Lumen has attempted to provide accurate information in this guide, Lumen does not warrant or guarantee the accuracy of the information provided herein. Lumen may change the programs or products mentioned at any time without prior notice. Mention of non-Lumen products or services is for information purposes only and constitutes neither an endorsement nor a recommendation of such products or services or of any company that develops or sells such products or services.

ALL INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED “AS IS,” WITH ALL FAULTS, AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED OR STATUTORY. LUMEN AND ITS SUPPLIERS HEREBY DISCLAIM ALL WARRANTIES RELATED TO THIS GUIDE AND THE INFORMATION CONTAINED HEREIN, WHETHER EXPRESSED OR IMPLIED OR STATUTORY INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT, OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

LUMEN AND ITS SUPPLIERS SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR REVENUES, COSTS OF REPLACEMENT GOODS OR SERVICES, LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OF THE GUIDE OR ANY LUMEN PRODUCT OR SERVICE, OR DAMAGES RESULTING FROM USE OF OR RELIANCE ON THE INFORMATION PROVIDED IN THIS GUIDE, EVEN IF LUMEN OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and other information used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Many of the Lumen products and services identified in this guide are provided with, and subject to, written software licenses and limited warranties. Those licenses and warranties provide the purchasers of those products with certain rights. Nothing in this guide shall be deemed to expand, alter, or modify any warranty or license or any other agreement provided by Lumen with any Lumen product, or to create any new or additional warranties or licenses.

Services not available everywhere. Business customers only. Lumen may change, cancel, or substitute products and services, or vary them by service area at its sole discretion without notice. ©2021 Lumen Technologies. All Rights Reserved.

Overview

This document provides an overview of the steps a customer will need to perform in support of SSO access using the SAML 2.0 protocol. This is currently the only supported method for dynamic customer logins to the Versa Director (customer management portal). This document will give an overview of the Lumen Operations team's role and a detailed list of the customer steps necessary to configure the customer IDP environment. **NOTE**: Not all IDPs are covered or certified in this guide and Lumen provides examples and guidance for Azure Active Directory, OneLogin, and Okta. Other IDP configurations may vary and will require customer knowledge to provision.

Summary

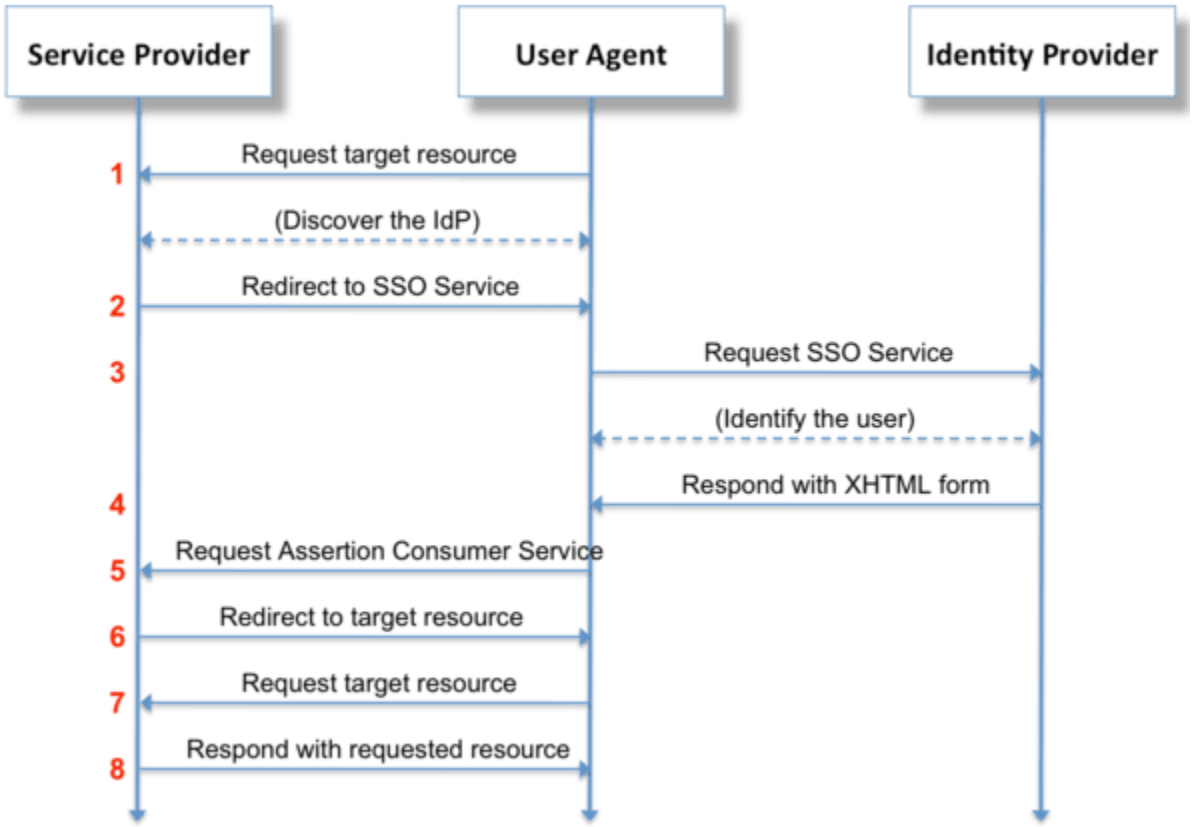
To configure SSO with SAML, it is important to cover a few important terms and also an overview of the authentication process.

- **Identity Provider (IDP)** - The service that is performing the authentication (username/password, authenticator app, etc). This would be the likes of Active Directory, Okta, etc as examples of IDPs. The portal page to this service would be displayed when the user attempts to login to the Director via its SSO interface.
- **Service Provider (SP)** - The web application that the user is trying to access. In our case, the SP would always be the Versa Director.
- **SAML Request** - The URL relay sent by the SP containing a request ID to ask the IDP if the user is authorized.
- **SAML Assertion** - The message sent by the IDP asserting a user's identity and any other specific attributes for that user that the SP is looking for.

The relationship between the SP and IDP can operation in two modes: SP initiated SAML, or IDP initiated SAML. This guide will be based on SP initiated SAML and all instructions below are based on that method.

The high-level process is based on a system of browser redirects. An SP initiated request begins with a user navigating to the Versa Director login portal and selecting the SSO option to login. The user will need to input their Versa organization name (will be provided by Lumen technical design engineer (TDE)). The user is then redirected to the IDP's portal login page, which is the SAML Request. The user then enters their username and password on the IDP's portal age, as well as any 2FA challenges that are configured. Upon successful user authentication, the IDP responds with the SAML assertion, which will contain the information the Versa Director portal uses to handle the login request and authenticate the user. The SP then redirects the user to the Versa Director portal page associated to the proper organization the user is authenticated to. The SAML messaging is all encrypted via x.509 certificate during this process. This is included the metadata XML that is uploaded to the Versa Director, which is described later in this document.

Services not available everywhere. Business customers only. Lumen may change, cancel, or substitute products and services, or vary them by service area at its sole discretion without notice. ©2021 Lumen Technologies. All Rights Reserved.



NOTE: During this entire process, the SP does not have any knowledge as to how many authentication mechanisms (or how rigorous they are) that are used to verify the user from the IDP, nor does the SP even know what user it is until the IDP tells it via the SAML Assertion. This provides some additional security as it leaves all credential information from the IDP, with no per user login information stored on the Director. This makes this unique from RADIUS or other network-based authentication mechanisms as there is no direct exchange of credentials between the IDP and SP.

Services not available everywhere. Business customers only. Lumen may change, cancel, or substitute products and services, or vary them by service area at its sole discretion without notice. ©2021 Lumen Technologies. All Rights Reserved.

Summary of Responsibilities

Customer Steps Summary

1. Customer will provide Lumen TDE team the name or type of the IDP system that is being used. Ex. Azure AD, Okta, etc.
2. Customer will provide the Lumen TDE team with the 'IDP Metadata XML' that will be required to be uploaded to the Versa Director portal.
3. Customer will need to configure the IDP in their environment. Lumen provides guidance and 3 example configurations below.
4. Customer may be required to assist Lumen TDE with role mapping, as required, based on the user setup and configuration. This exercise would map a 'role' from the customer IDP to the appropriate role in the Versa Director portal.
5. See Appendix for sample IDP configurations.

Lumen TDE (Technical Design Engineer) steps summary

1. Lumen TDE will manage the build and configuration of the Versa Director SSO connector. This connector is required per customer organization to enable SAML SSO. In order to complete this step, the customer 'IDP Metadata XML' will be required.
2. Lumen TDE will also make sure this SSO connector is associated to the customer organization in Versa and confirm the customer organization name. Ex. 'CUSTA-2-YG123'
    - Customer will need to take note of the organization name and provide it to all users that will eventually need to login via SSO.
3. If required, the Lumen TDE will work with the customer on RBAC role mapping. This will require the roles from the IDP to be mapped to the appropriate roles in the Versa Director RBAC roles.
    - Ex. SuperAdmin, NetworkAdmin, SecurityAdmin, Dashboard_only, Read_only, etc.
4. Lumen TDE will provide customer with all needed information for the IDP configuration, such as the Versa Director URL and the Customer organization name.

Customer IDP Configuration

As there are many different IDPs out there, Lumen doesn't provide exact configuration guidance for every IDP. However, based on the testing that was performed for certification of this feature, there are base config components that will apply to all IDPs to meet the minimum requirement for a SP initiated SAML connector. This guidance will be provided, along with what other config components may be needed for certain IDPs, as well as more detailed config guidance examples for the 3 IDPs that were examined under test; Azure Active Directory, Onelogin, and Okta.

Configuration Steps:

The below are considered the standard minimum *required config* for setting up the IDP side for SP initiated:

Services not available everywhere. Business customers only. Lumen may change, cancel, or substitute products and services, or vary them by service area at its sole discretion without notice. ©2021 Lumen Technologies. All Rights Reserved.

- Creating the application - Versa will not show up as a standard application in any IDP today. It will have to be custom created.
- Login URL - The Versa SSO login URL. This is used in many different aspects of the config, and should be filled in for fields that have attribute names like the below in the IDP:
    - Single Sign on URL
    - Recipient URL
    - Destination URL
    - ACS Consumer URL/Validator
    - Reply URL
    - **NOTE:** Lumen TDE will provide the <director_url> value to the customer.

https://<director_url>/versa/sso/loginConsumer

- Entity ID - The Versa URI that uniquely defines the Versa Director as the correct audience of the SAML assertion. This value is a constant no matter which Director the connector is trying to interface with. This typically needs to be only specified once in the IDP and can have the following names:
    - Audience URI
    - Identifier

http://versa-networks.com/sp

- Single Logout URL - The Versa SSO logout URL. This is usually considered optional in most of the IDP configs, but will be required to setup due to how Versa director handles SP initiation.

https://<director_url>/versa/sso/logoutConsumer

- User Attributes/Parameters - Additional custom parameters as part of the SAML Assertion that further describe the authenticated user. These are essentially key-value pairs that line up with the SSO User Attributes tab. The exact naming of these can varry between IDP, but the following 4 attributes from the Director MUST be defined in some way:
    - email
    - org
    - role
    - idleTimeOut
- Define User Attributes per user - The above attributes in the IDP must then be defined per user account.

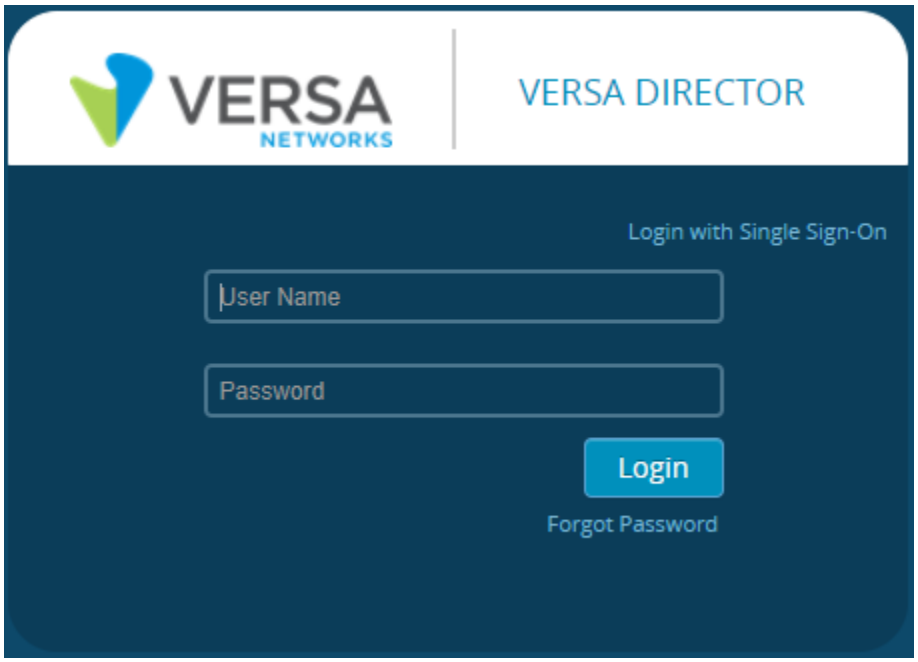
Services not available everywhere. Business customers only. Lumen may change, cancel, or substitute products and services, or vary them by service area at its sole discretion without notice. ©2021 Lumen Technologies. All Rights Reserved.

The below is currently known config needed by *some IDP providers* but not all:

- Single Logout Certificate - Some IDPs require that the SLO request contain a digital signature from the SP. The certificate from the Versa Director can be obtained in two different ways to hand back to the customer:
    - Obtain a copy of the certificate from the 'Metadata' tab on the SSO Connector in the Director. This would be the long certificate text shown in "SP Certificate". This string can be saved to a text file, named with .crt extension, and transferred. **NOTE:** This can be provided by Lumen TDE as required. Certificate can expire and may need to be refreshed by the customer contacting Lumen support and obtaining an updated certificate.

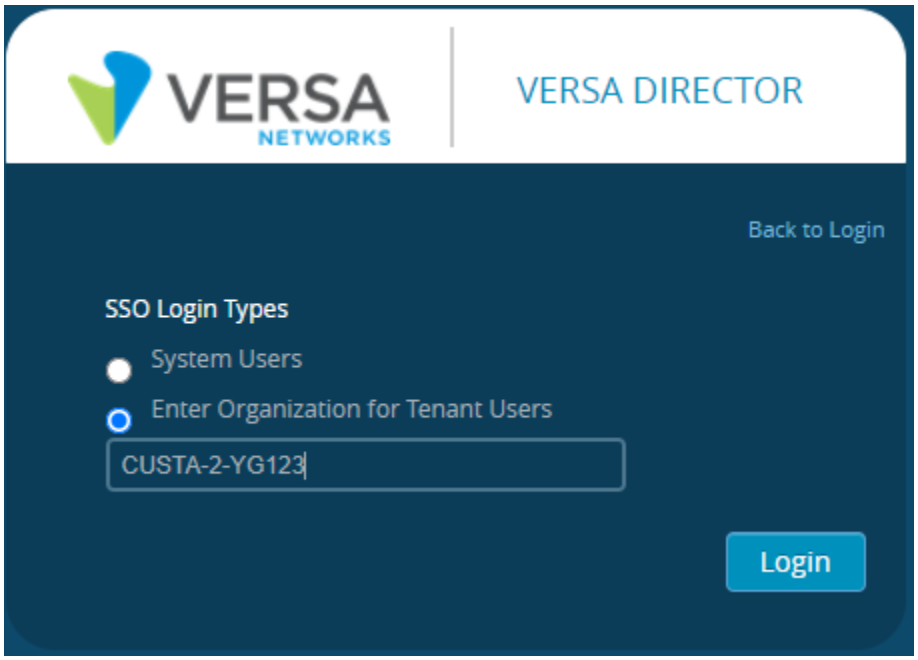
Login Experience after SSO setup

After setup is complete, the customer's users will begin the login by selecting the "Login with Single Sign-On" on the upper right of the login screen.



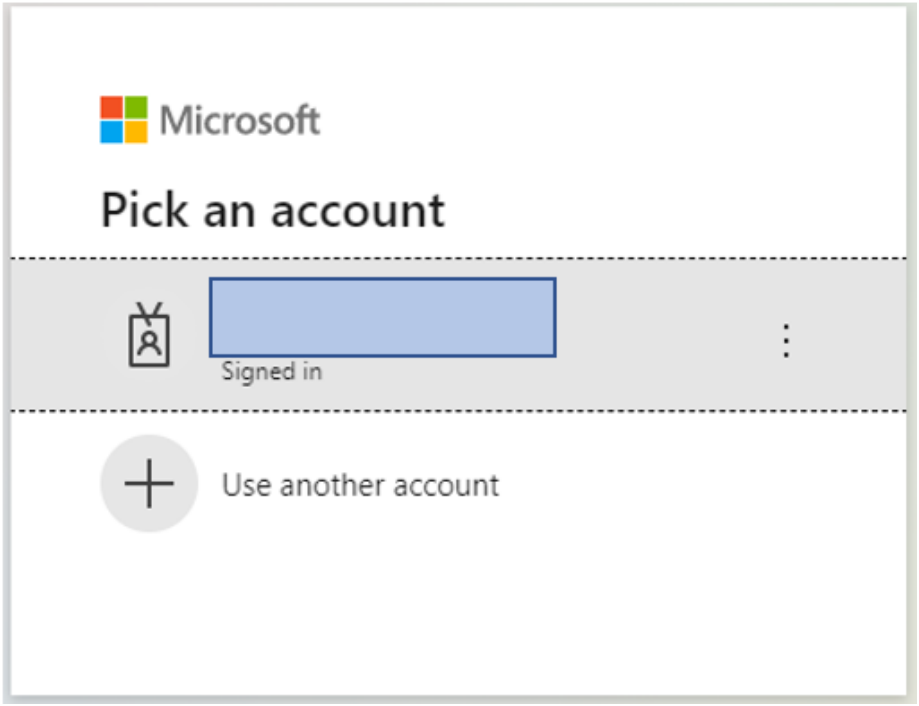
The customer user must then select the second radio button for "Enter Organization for Tenant Users" and must enter the customer organization name before selecting login. **NOTE:** This field is case-sensitive and will need to be entered accurately to proceed.

Services not available everywhere. Business customers only. Lumen may change, cancel, or substitute products and services, or vary them by service area at its sole discretion without notice. ©2021 Lumen Technologies. All Rights Reserved.



After selecting the login button, the browser will redirect to the customer IDP for user authentication and the process will continue with redirects until the user is logged into the Versa Director portal.

Example Microsoft redirect below:



Services not available everywhere. Business customers only. Lumen may change, cancel, or substitute products and services, or vary them by service area at its sole discretion without notice. ©2021 Lumen Technologies. All Rights Reserved.

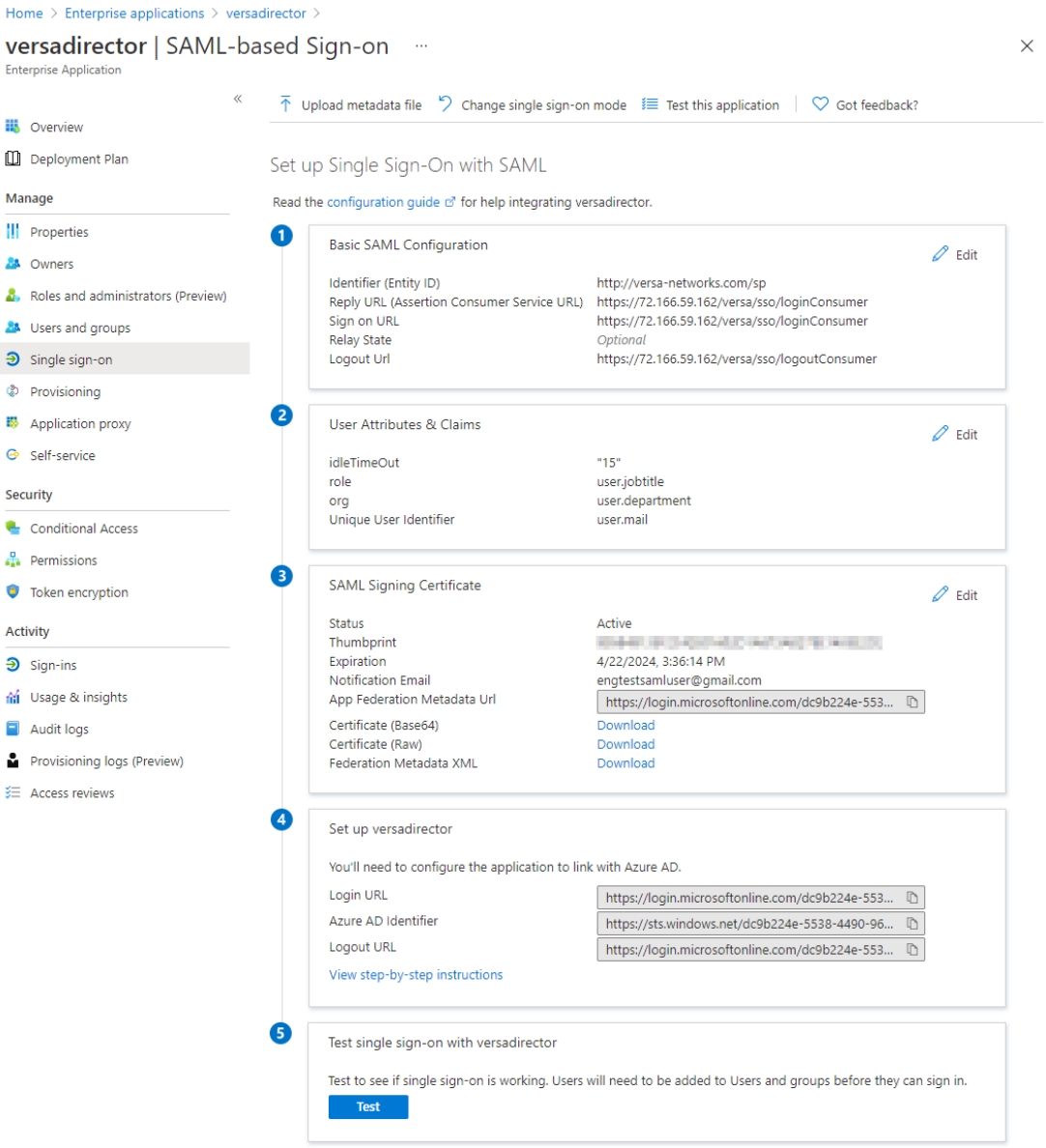
Appendix – Example IDP Configurations

Azure Active Directory Configuration

Azure Active Directory has a customer friendly wizard. As a result, configuring SAML SSO is done in just a few steps.

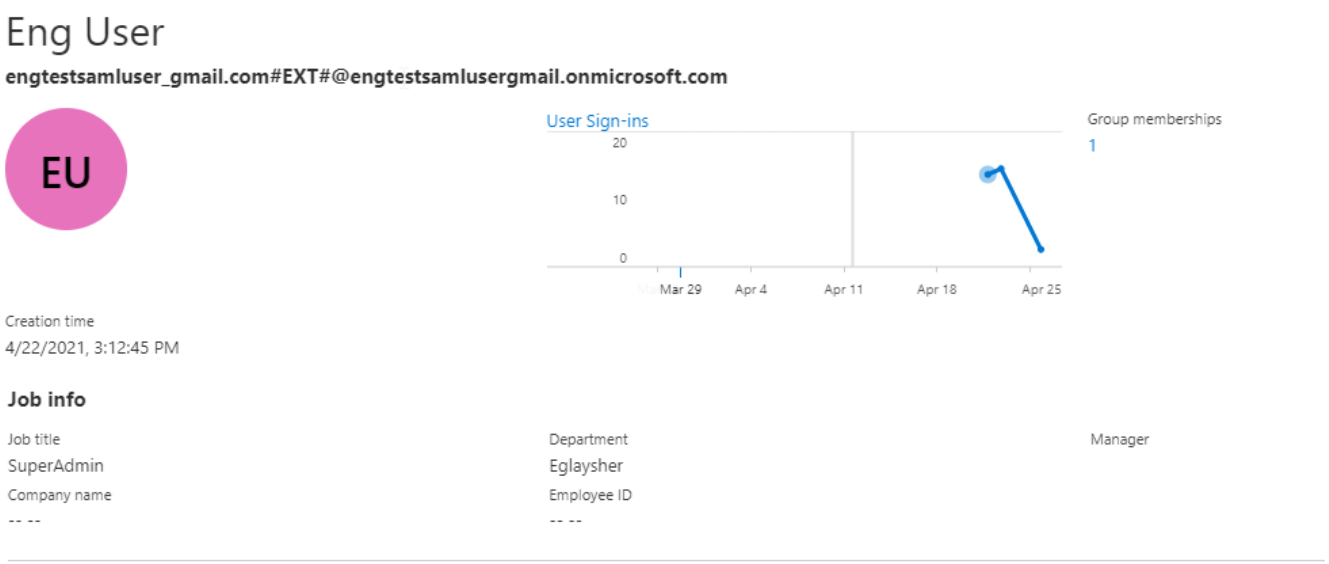
- Within Azure Portal, search for Enterprise Applications. Then select All Applications -> New Application. Versa is not currently included in the list by default, so it'll have to be custom configured via "Create your own Application"
- Create this as a 'non-gallery' application.
- Within Overview, select the step 2 of getting started for "Set up single sign on".
- This brings you to the SAML wizard screen. The fields here end up being configured very similar to the below screenshot, with the URL/URI attributes matching what would be provided as part of the prior guidance for IDP configuration.

Services not available everywhere. Business customers only. Lumen may change, cancel, or substitute products and services, or vary them by service area at its sole discretion without notice. ©2021 Lumen Technologies. All Rights Reserved.



- As seen in the screenshot for the 3rd step in the wizard, an option is available to download Federation Metadata XML. This would be the metadata XML file that the customer must provide to Lumen TDE to have loaded into the Versa Director portal.
- Users within Azure Active Directory need to then be configured to have the required attributes. 'Job Title' and 'Department' must be specified for the created versa application if not done so already, for the user to correctly be authorized into the correct organization in the Director.

Services not available everywhere. Business customers only. Lumen may change, cancel, or substitute products and services, or vary them by service area at its sole discretion without notice. ©2021 Lumen Technologies. All Rights Reserved.

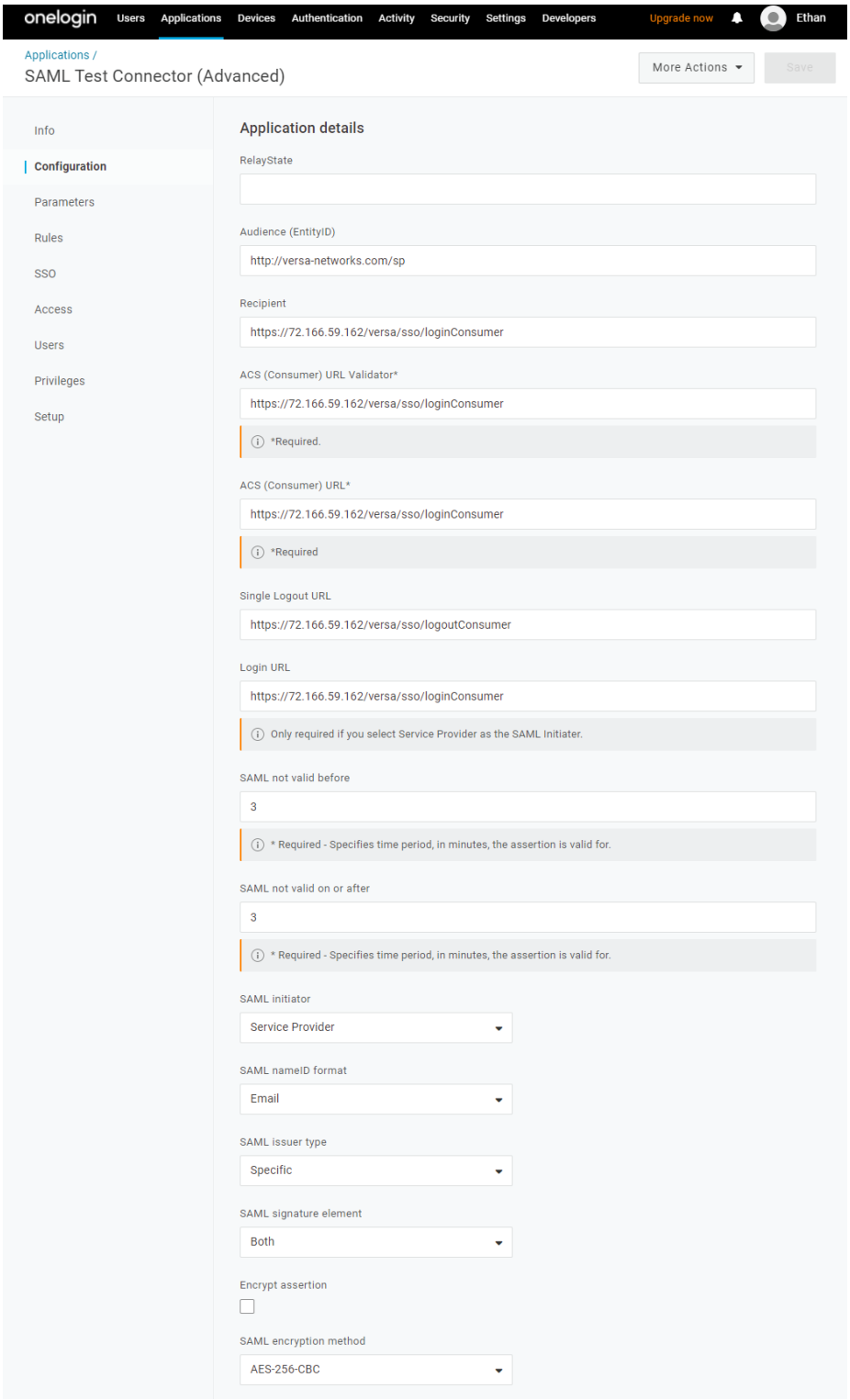


Onelogin Configuration

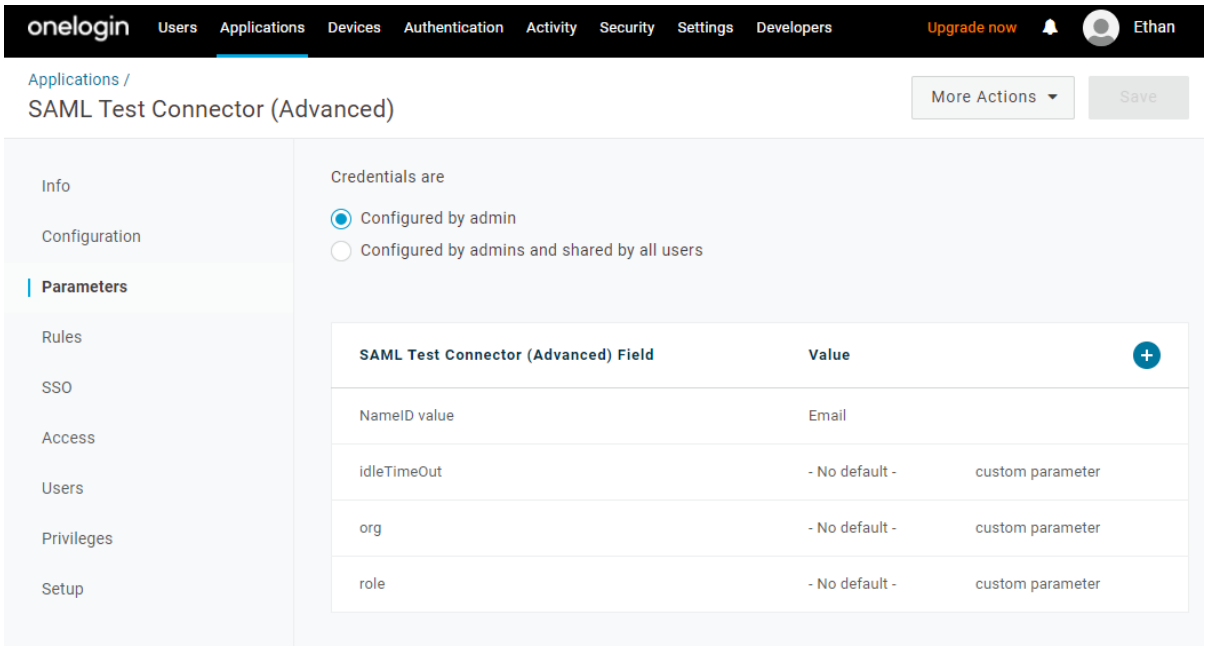
Onelogin does not use a wizard for its SAML SSO build process and ends up being a bit more complex.

- Add a new Application. Since Onelogin does not have a direct "custom application" form, select "SAML Test Connector (Advanced)" from the Add App pane.
- Fill out the Info sidenav with an appropriate name and description ('versadirector' for instance)
- From Configuration sidenav, this is where the majority of the SAML SSO URL info is configured and is pictured below. Ensure SAML initiator is specified as "Service Provider", this is critical for SP initiated SAML to work.
- Parameters sidenav should contain the the 4 SAML assertion parameters. Ensure "Configured by admin" is selected, otherwise this won't allow for per user attribute control.
- Users sidenav could then have per-user Parameters for this given IDP configured. This must be done for a user to be authorized using this IDP to the Versa Director.
- Once configuration is complete, generate the SAML XML metadata via "More Actions" -> SAML Metadata. This would be provided to Lumen TDE to have loaded to the Versa Director portal.

Services not available everywhere. Business customers only. Lumen may change, cancel, or substitute products and services, or vary them by service area at its sole discretion without notice. ©2021 Lumen Technologies. All Rights Reserved.



Services not available everywhere. Business customers only. Lumen may change, cancel, or substitute products and services, or vary them by service area at its sole discretion without notice. ©2021 Lumen Technologies. All Rights Reserved.



Okta SAML Configuration

Okta is created in a fairly similar way to Onelogin. There is no direct wizard and each piece needs to be individually configured.

- Add a new application. This would be done from the sidenav is Applications -> Applications -> Add Application. Select "Create New App" as Versa does not have a default SAML integration. Have Platform be flagged as 'Web' and the SAML 2.0 radio button selected.
- Select App name as 'versadirector'
- Within Configure SAML, ensure all of the standard URL settings are configured similar to below.
- On this same page, "Enable Single Logout" needs to be selected, with the SLO info filled out and the Signature Certificate added. This certificate is the Versa Director's SSO certificate.
- On this same page, ensure all Attribute statements are configured. This uses a specific value setup within okta that needs to be followed, similar to how IDPs also have their own.
- Once filled out, finish Application config.
- The metadata XML should then be retrieved. From sidenav, go to Applications -> Applications -> versadirector -> the Sign On tab, then select "Identity Provider Metadata". This would be provided to the Lumen TDE to have loaded in the Versa Director portal.
- User specific parameters can then be configured. From sidenav, select Directory and edit People or Groups to have the 4 SAML attributes populated.

Services not available everywhere. Business customers only. Lumen may change, cancel, or substitute products and services, or vary them by service area at its sole discretion without notice. ©2021 Lumen Technologies. All Rights Reserved.

SAML Settings

Edit

GENERAL

Single Sign On URL	https://72.166.59.162/versa/sso/loginConsumer
Recipient URL	https://72.166.59.162/versa/sso/loginConsumer
Destination URL	https://72.166.59.162/versa/sso/loginConsumer
Audience Restriction	http://versa-networks.com/sp
Default Relay State	
Name ID Format	Unspecified
Response	Signed
Assertion Signature	Signed
Signature Algorithm	RSA_SHA256
Digest Algorithm	SHA256
Assertion Encryption	Unencrypted
SAML Single Logout	Enabled
Signature Certificate	vnms_sso_public.crt (CN=L=Santa Clara, ST=California, C=US, OU=VersaDirector, O=versa-networks, CN=engineering-director-01)
authnContextClassRef	PasswordProtectedTransport
Honor Force Authentication	Yes
Assertion Inline Hook	None (disabled)
SAML Issuer ID	http://www.okta.com/${org.externalKey}

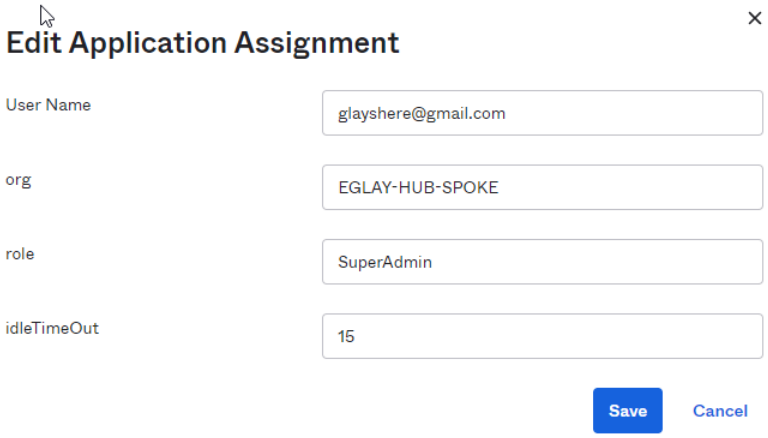
ATTRIBUTE STATEMENTS

Name	Name Format	Value
role	Unspecified	appuser.role
org	Unspecified	appuser.org
idleTimeOut	Unspecified	appuser.IdleTimeOut

GROUP ATTRIBUTE STATEMENTS

Name	Name Format	Filter

Services not available everywhere. Business customers only. Lumen may change, cancel, or substitute products and services, or vary them by service area at its sole discretion without notice. ©2021 Lumen Technologies. All Rights Reserved.



Services not available everywhere. Business customers only. Lumen may change, cancel, or substitute products and services, or vary them by service area at its sole discretion without notice. ©2021 Lumen Technologies. All Rights Reserved.