

# Enable and Verify Single Sign-On for vManage

## Contents

---

[Introduction](#)

[Terminology](#)

[What are feature capabilities?](#)

[How to Enable it on vManage?](#)

[What is the workflow?](#)

[Does vManage support Two-Factor Authentication and how it is different from SSO?](#)

[How many roles are there as part of the solution?](#)

[Which IdPs do we support?](#)

[How to indicate user group membership in SAML assert?](#)

[How to enable/check whether SSO works?](#)

[SAML Tracer](#)

[How to log in to SSO enabled vManage?](#)

[What Encryption Algorithm is used ?](#)

[Related Information](#)

---

## Introduction

This document describes the basics in order to enable and verify Single Sign On (SSO) on vManage.

## Terminology

Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. As its name implies, SAML is an XML-based markup language for security assertions (statements that service providers use to make access-control decisions).

An Identity Provider (IdP) is “a trusted provider that lets you use single sign-on (SSO) in order to access other websites.” SSO reduces password fatigue and enhances usability. It decreases the potential attack surface and provides better security.

Service Provider - It is a system entity that receives and accepts authentication assertions in conjunction with an SSO profile of the SAML.

## What are feature capabilities?

- Starting with 18.3.0, vManage supports SSO. SSO allows a user to login to vManage by authenticating against an external Identity Provider (IP).
- Only SAML2.0 is supported
- Supported for - Single Tenant (standalone and cluster), Multi-Tenant (both at provider level and tenant level), Also, Multi-Tenant deployments are cluster by default. Provider-as-tenant is not applicable.
- Each tenant can have its own unique identity provider as long as the idp aligns with SAML 2.0 spec.

- Supports configuration of IDP metadata via file upload as well as plain text copy, and download of vManage metadata.
- Only browser based SSO is supported.
- Certificates used for vmanage metadata are not configurable in this release.  
it is a Self-signed Certificate, created the first time you enable SSO, with these parameters:

String CN = <TenantName>, DefaultTenant

String OU = <Org Name>

String O = <Sp Org Name>

String L = "San Jose";

String ST = "CA";

String C = "USA";

String validity = 5yrs;

Certificate Signing Algorithm: SHA256WithRSA

KeyPair Generation Algorithm: RSA

- Single Login - SP Initiated and IDP Initiated supported
- Single Logout - SP Initiated only

## How to Enable it on vManage?

To enable single sign-on (SSO) for the vManage NMS to allow users to be authenticated using an external identity provider:

1. Ensure that you have enabled NTP on the vManage NMS.
2. connect to vManage GUI with the URL which is configured on IdP  
(for example, vmanage-112233.example.net and do not use IP-Address, because this URL information is included in SAML Metadata)
3. Click the Edit button to the right of the Identity Provider Settings bar.
4. In the Enable Identity Provider field, click Enabled,
5. Copy and paste the identity provider metadata in the Upload Identity Provider Metadata box. Or click Select a File to upload the identity provider metadata file.
6. Click Save.

## What is the workflow?

1. User enables SSO via the Administration->Settings page by uploading the identity provider metadata.
2. User then downloads the corresponding vManage tenant metadata to be uploaded onto the identity provider ( Must be done at least once to generate vManage metadata).
3. User can disable or update metadata at any time if required.

Sample vManage Meta



It redirects you to the Cisco SSO, where you are prompted for PingID / DUO 2FA.

## How many roles are there as part of the solution?

We have 3 roles; basic, operator, netadmin.

### [Configuring User Access and Authentication](#)

## Which IdPs do we support?

- Okta
- PingID
- ADFS
- Microsoft Azure (20.9 and later)

Customers are able to use other IdPs and could see it working. This would come under the 'best effort'

Others include: Oracle Access Manager, F5 Networks

---

 **Note:** Please check the latest Cisco documentation for the latest IdPs supported by vManage

---

## How to indicate user group membership in SAML assert?

**Problem:** front-ending the vManage with a SAML IdP. When the user is successfully authenticated, the only thing that the user can access is the dashboard.

Is there a way to give the user more access (via user group RBAC) when the user is authenticated via SAML?

This problem is caused by improper configuration of IDP. The key here is that the info sent by IDP during authentication must contain "Username" and "Groups" as attributes in the xml. If other strings are used in place of "Groups", then, the usergroup is default to "Basic". "Basic" users only have access to the basic dashboard.

Make sure IDP sends "Username/Groups", instead of "UserId/role" to vManage.

This is an example as seen in /var/log/nms/vmanage-server.log file:

Non-Working Example:

We see "UserId/role" been sent by IdP and the user is mapped to *basic* group.

```
01-Mar-2019 15:23:50,797 UTC INFO [vManage] [SAMLAuthenticationProvider] (default task-227) |default| /
01-Mar-2019 15:23:50,797 UTC INFO [vManage] [SAMLAuthenticationProvider] (default task-227) |default| /
01-Mar-2019 15:23:50,797 UTC INFO [vManage] [SAMLAuthenticationProvider] (default task-227) |default| /
```

Working example:

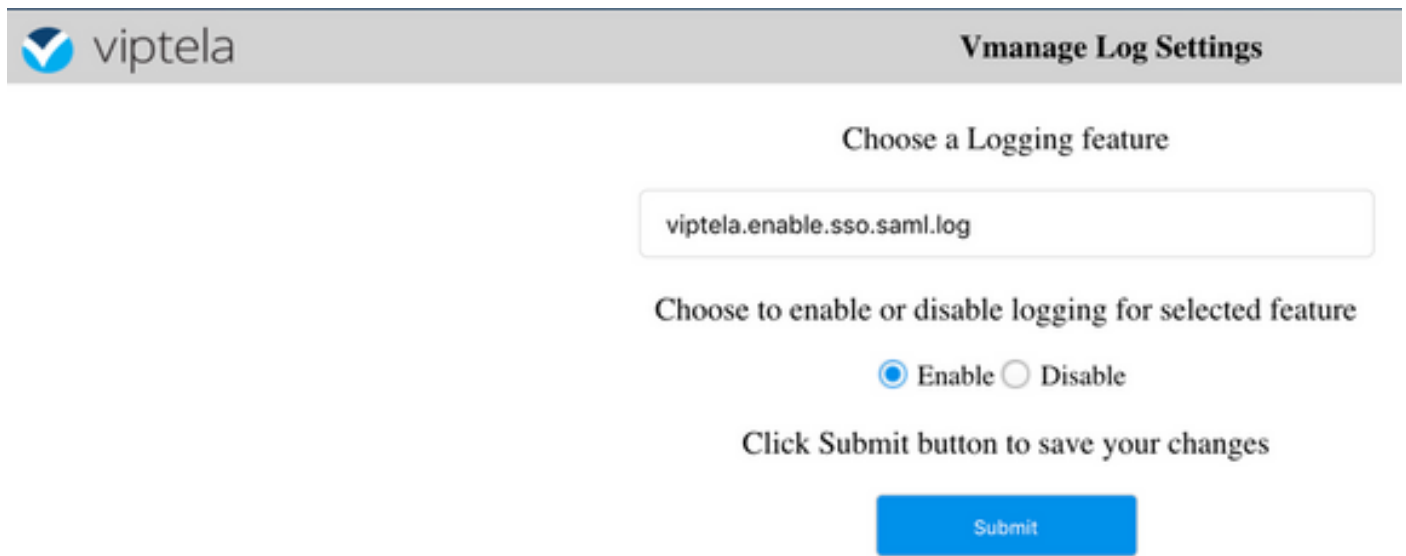
In this you see "Username/Groups" and the user is mapped to netadmin group.

05-Mar-2019 21:35:55,766 UTC INFO [vManage] [SAMLAuthenticationProvider] (default task-90) |default| A  
05-Mar-2019 21:35:55,766 UTC INFO [vManage] [SAMLAuthenticationProvider] (default task-90) |default| A  
05-Mar-2019 21:35:55,766 UTC INFO [vManage] [SAMLAuthenticationProvider] (default task-90) |default| R

## How to enable/check whether SSO works?

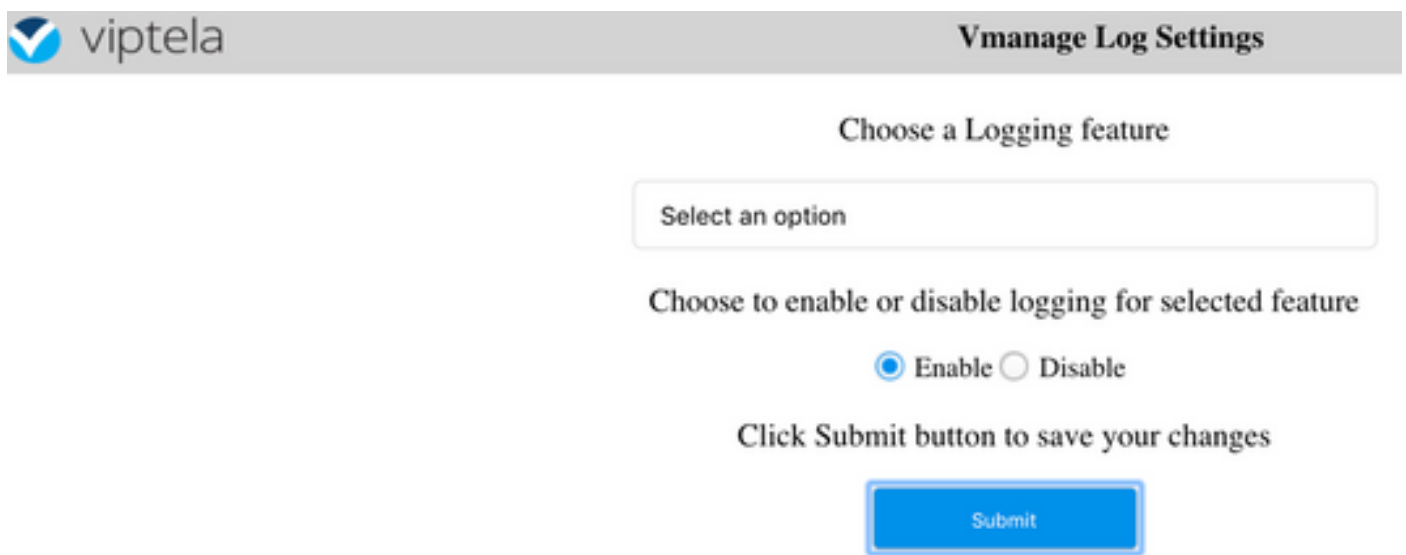
SSO feature debug logging can be enabled by these steps:

1. Navigate to **https://<vManage\_ip\_addr:port>/logsettings.html**
2. Select the SSO logging and enable it as shown in the image.



The screenshot shows the Vmanage Log Settings interface. At the top left is the viptela logo. The page title is "Vmanage Log Settings". Below the title, it says "Choose a Logging feature". A text input field contains "viptela.enable.sso.saml.log". Below this, it says "Choose to enable or disable logging for selected feature". There are two radio buttons: "Enable" (which is selected) and "Disable". Below the radio buttons, it says "Click Submit button to save your changes". At the bottom, there is a blue "Submit" button.

3. Once Enabled, hit the **Submit** button.



This screenshot is identical to the previous one, showing the Vmanage Log Settings page with the "Enable" radio button selected and the "Submit" button highlighted with a blue border.

### List of Logging features updated

viptela.enable.sso.saml.log: true

- The SSO related logs are saved to the vManage log file **/var/log/nms/vmanage-server.log** of

particular interest is the "Groups" setting for IDP authorization. If there is no match, the user defaults to the "Basic" group, which has read-only access;

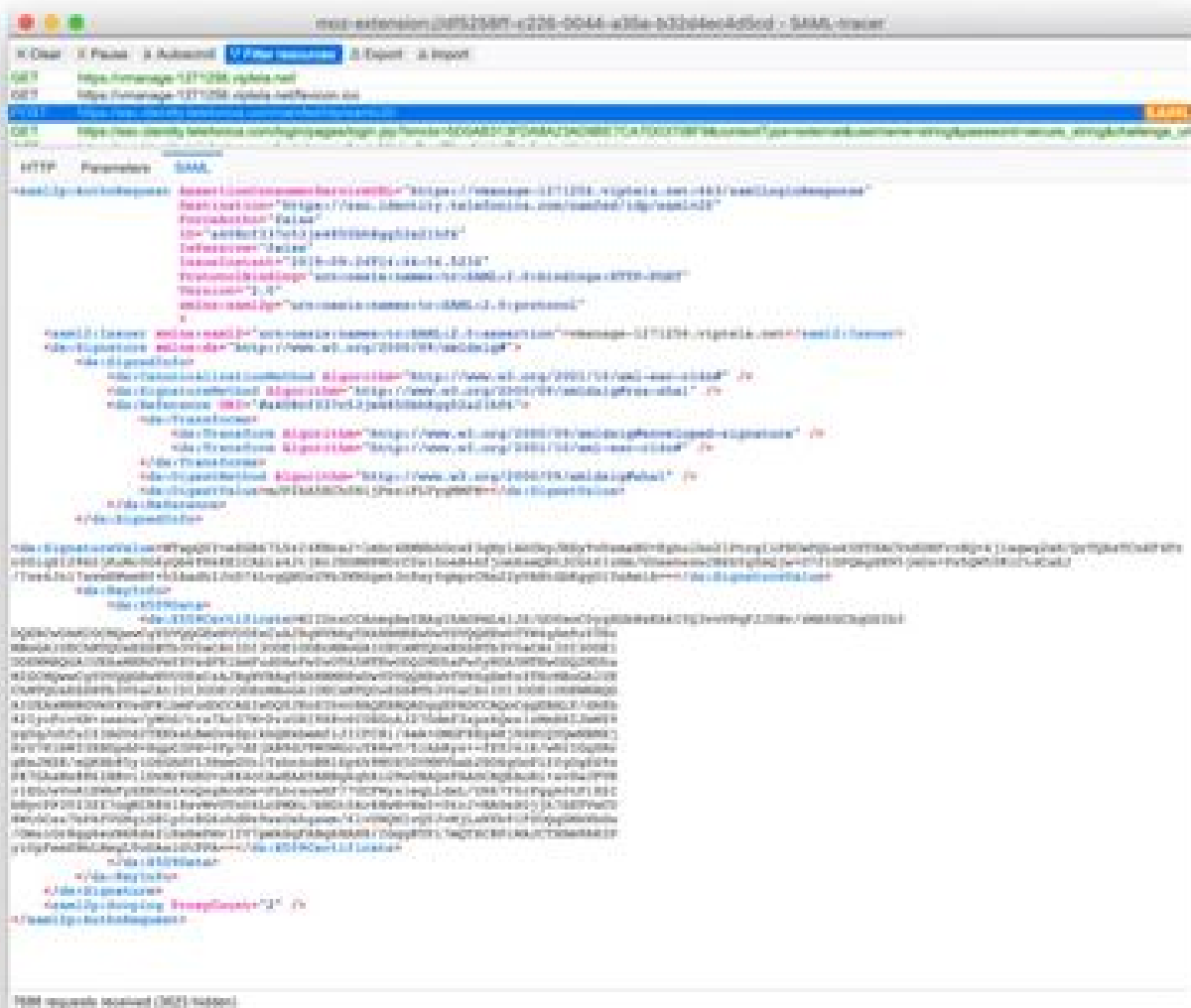
- In order to debug access privilege issue, check the log file and looking for string "SamlUserGroups". Subsequent output must be a list of strings of group names. One of them must match the group settings on the vManage. If no match is found, then the user has defaulted to the "Basic" group.

## SAML Tracer

A tool for viewing SAML and WS-Federation messages sent through the browser during single sign-on and single logout.

[FireFox SAML-Tracer Add-on](#)

[Chrome SAML-Tracer Extension](#)



sample SAML Message

## How to log in to SSO enabled vManage?

SSO is only for browser login. You can manually direct vManage to the traditional login page and bypass SSO in order to use only username and password: **https://<vmanage>:8443/login.html**.

## What Encryption Algorithm is used ?

Currently we support SHA1 as encryption Algorithm. vManage signs the SAML metadata file with SHA1 algorithm which IdPs need to accept it. The support for SHA256 is coming in future releases, which we do not have the support currently.

## Related Information

Configure Single Sign On: <https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-16/security-book-xe/configure-sso.html>

OKTA Login / Logout working logs attached to the case as a reference.