

vManage: Überprüfen und Überprüfen der einmaligen Anmeldung

Inhalt

[Einführung](#)

[Terminologie](#)

[Welche Funktionen stehen zur Verfügung?](#)

[Wie wird sie in vManage aktiviert?](#)

[Was ist der Workflow?](#)

[Unterstützt vManage die Zwei-Faktor-Authentifizierung und wie unterscheidet sich diese von SSO?](#)

[Wie viele Rollen hat die Lösung?](#)

[Welche IDs unterstützen wir?](#)

[Wie kann die Benutzergruppenmitgliedschaft in SAML-Assert angegeben werden?](#)

[Wie kann ich die SSO-Funktion aktivieren/überprüfen?](#)

[SAML-Tracer](#)

[SAML-Beispielnachricht](#)

[Wie meldet man sich bei SSO-aktiviertem vManage an?](#)

[Welcher Verschlüsselungsalgorithmus wird verwendet?](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument werden die Grundlagen für die Aktivierung der Single Sign On (SSO) bei vManage sowie die Überprüfung bei vManage beschrieben, wenn diese Funktion aktiviert ist. Ab Version 18.3.0 unterstützt vManage SSO. SSO ermöglicht es Benutzern, sich bei vManage anzumelden, indem sie sich über einen externen Identitätsanbieter (IP) authentifizieren. Diese Funktion unterstützt die SAML 2.0-Spezifikation für SSO.

Unterstützt von Shankar Vemapalli, Cisco TAC Engineer.

Terminologie

Security Assertion Markup Language (SAML) ist ein offener Standard für den Austausch von Authentifizierungs- und Autorisierungsdaten zwischen Parteien, insbesondere zwischen einem Identitätsanbieter und einem Dienstanbieter. Wie der Name bereits andeutet, ist SAML eine XML-basierte Markupsprache für Sicherheitsassertionen. (Anweisungen, die Service Provider verwenden, um Entscheidungen zur Zugriffskontrolle zu treffen).

Ein Identitätsanbieter (IdP) ist "ein vertrauenswürdiger Anbieter, bei dem Sie Single Sign-On (SSO) für den Zugriff auf andere Websites verwenden können." SSO reduziert die Kennwortmüdigkeit und verbessert die Benutzerfreundlichkeit. Sie reduziert die potenzielle Angriffsfläche und bietet mehr Sicherheit.

Service Provider - Es ist eine Systemeinheit, die Authentifizierungsassertionen in Verbindung mit

einem SSO-Profil des SAML empfängt und akzeptiert.

Welche Funktionen stehen zur Verfügung?

- Nur SAML2.0 wird unterstützt
- Unterstützt für EinzelTenant (Standalone und Cluster), Multi-Tenant (sowohl auf Provider- als auch auf Tenant-Ebene), Multi-Tenant-Bereitstellungen sind ebenfalls standardmäßig Cluster. Provider-as-Tenant ist nicht anwendbar.
- Jeder Tenant kann über einen eigenen eindeutigen Identitätsanbieter verfügen, solange die IP-Adresse den SAML 2.0-Spezifikationen entspricht.
- Unterstützt die Konfiguration von IDP-Metadaten über Datei-Upload, Textkopien und das Herunterladen von vManage-Metadaten.
- Es wird nur eine browserbasierte SSO unterstützt.
- Zertifikate, die für verwaltete Metadaten verwendet werden, können in dieser Version nicht konfiguriert werden.

Es handelt sich um ein selbstsigniertes Zertifikat, das beim ersten Aktivieren der SSO-Funktion erstellt wurde und folgende Parameter enthält:

```
String CN = <TenantName>, DefaultTenant
```

```
string OU = <Org Name>  
string O = <SP-Org-Name>  
string L = "San Jose";  
String ST = "CA";  
string C = "USA";  
Zeichenfolgengültigkeit = 5 Jahre;  
Zertifikatsignaturalgorithmus: SHA256WithRSA  
KeyPair-Generierungsalgorithmus: RSA
```

- Single Login (Einmalanmeldung) - SP Initiated und IDP Initiated Support
- Single Logout - nur SP Initiated

Wie wird sie in vManage aktiviert?

So aktivieren Sie Single Sign-On (SSO) für das vManage NMS, damit Benutzer mithilfe eines externen Identitätsanbieters authentifiziert werden können:

1. Stellen Sie sicher, dass NTP auf dem vManage NMS aktiviert ist.
2. Verbindung zur vManage-GUI mit der URL herstellen, die auf IDP konfiguriert ist (z. B. vmanagement-112233.viptela.net und keine IP-Adresse verwenden, da diese URL-Informationen in SAML-Metadaten enthalten sind)
3. Klicken Sie auf die Schaltfläche Bearbeiten rechts neben der Leiste Identity Provider Settings (Einstellungen für Identitätsanbieter).
4. Klicken Sie im Feld Identitätsanbieter aktivieren auf Aktiviert,
5. Kopieren Sie die Identitätsanbieter-Metadaten und fügen Sie sie in das Feld Identitätsanbieter-Metadaten hochladen ein. Oder klicken Sie auf Datei auswählen, um die Metadatendatei des Identitätsanbieters hochzuladen.
6. Klicken Sie auf Speichern.

Website anmelden.

Sie wird zur Cisco SSO weitergeleitet, wo Sie zur Eingabe der PingID/DUO 2FA aufgefordert werden.

Wie viele Rollen hat die Lösung?

Wir haben 3 Rollen. Basic, Operator, netadmin.

[Konfigurieren von Benutzerzugriff und Authentifizierung](#)

Welche IDs unterstützen wir?

- Okta
- PingID
- ADFS

Kunden können andere IDs verwenden und sehen, wie diese funktionieren. Dies würde unter die "besten Anstrengungen" fallen

Ein Beispiel dafür wäre MSFT Azure AD ist NICHT unterstützt IDP (noch). Aber angesichts einiger Vorbehalte könnte es funktionieren.

Weitere Komponenten: Oracle Access Manager, F5 Networks

Hinweis: In der neuesten Cisco Dokumentation finden Sie die neuesten von vManage unterstützten IDs.

Wie kann die Benutzergruppenmitgliedschaft in SAML-Assert angegeben werden?

Problem: Front-End des vManage mit einer SAML-IDP. Wenn der Benutzer erfolgreich authentifiziert wurde, kann der Benutzer nur auf das Dashboard zugreifen.

Gibt es eine Möglichkeit, dem Benutzer mehr Zugriff (über die Benutzergruppe RBAC) zu gewähren, wenn der Benutzer über SAML authentifiziert wird?

Dieses Problem wird durch die unsachgemäße Konfiguration von IDP verursacht. Der Schlüssel ist, dass die Informationen, die von IDP während der Authentifizierung gesendet werden, "Benutzername" und "Gruppen" als Attribute im xml enthalten sollten. Wenn anstelle von "Groups" andere Zeichenfolgen verwendet werden, wird die Benutzergruppe standardmäßig auf "Basic" gesetzt. "Einfache" Benutzer haben nur Zugriff auf das grundlegende Dashboard.

Vergewissern Sie sich, dass IDP statt "UserId/role" "Username/Groups" an vManage sendet. Im Folgenden sehen Sie ein Beispiel in der Datei /var/log/nms/vmanage-server.log.

Nicht funktionierendes Beispiel:

Es wird angezeigt, dass "UserId/role" von IdP gesendet wurde und der Benutzer der

grundlegenden Gruppe zugeordnet ist.

```
01-Mar-2019 15:23:50,797 UTC INFO [vManage] [SAMLAuthenticationProvider] (default task-227)
|default| AttributeMap: {role=[netadmin], UserId=[Tester@Example.MFA.com]}
01-Mar-2019 15:23:50,797 UTC INFO [vManage] [SAMLAuthenticationProvider] (default task-227)
|default| AttributeMap: {role=[netadmin], UserId=[Tester@Example.MFA.com]}
01-Mar-2019 15:23:50,797 UTC INFO [vManage] [SAMLAuthenticationProvider] (default task-227)
|default| Roles: [Basic]
```

Arbeitsbeispiel:

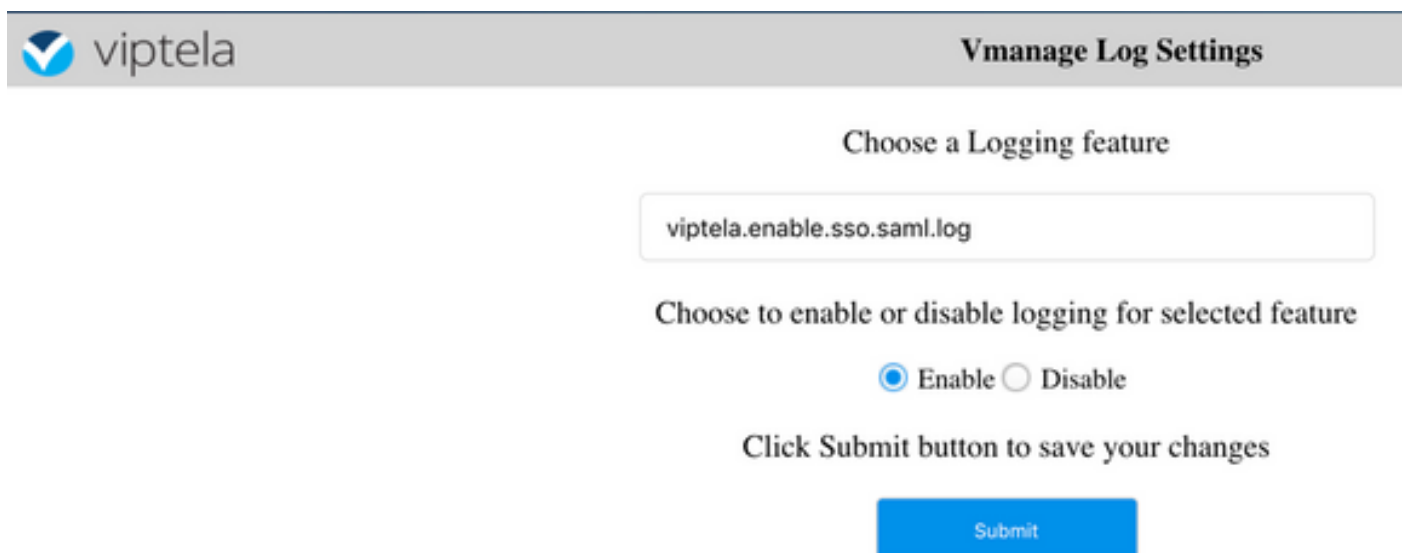
In diesem Fenster sehen Sie "Benutzername/Gruppen" und der Benutzer ist der netadmin-Gruppe zugeordnet.

```
05-Mar-2019 21:35:55,766 UTC INFO [vManage] [SAMLAuthenticationProvider] (default task-90)
|default| AttributeMap: {UserName=[Tester@Example.MFA.com], Groups=[netadmin]}
05-Mar-2019 21:35:55,766 UTC INFO [vManage] [SAMLAuthenticationProvider] (default task-90)
|default| AttributeMap: {UserName=[Tester@Example.MFA.com], Groups=[netadmin]}
05-Mar-2019 21:35:55,766 UTC INFO [vManage] [SAMLAuthenticationProvider] (default task-90)
|default| Roles: [netadmin]
```

Wie kann ich die SSO-Funktion aktivieren/überprüfen?

Die Protokollierung des SSO-Feature-Debuggens kann wie folgt aktiviert werden:

1. Navigieren Sie zu https://<vManage_ip_addr:port>/logsettings.html.
2. Wählen Sie die SSO-Protokollierung aus, und aktivieren Sie sie, wie im Bild gezeigt.



The screenshot shows the Vmanage Log Settings interface. At the top left is the Viptela logo, and at the top right is the title "Vmanage Log Settings". The main heading is "Choose a Logging feature". Below this, a text input field contains the value "viptela.enable.sso.saml.log". Underneath, the instruction "Choose to enable or disable logging for selected feature" is followed by two radio buttons: "Enable" (which is selected) and "Disable". At the bottom, there is a blue "Submit" button and the instruction "Click Submit button to save your changes".

3. Klicken Sie nach der Aktivierung auf die Schaltfläche **Senden**.

Choose a Logging feature

Select an option

Choose to enable or disable logging for selected feature

Enable Disable

Click Submit button to save your changes

Submit

List of Logging features updated

viptela.enable.sso.saml.log:

true

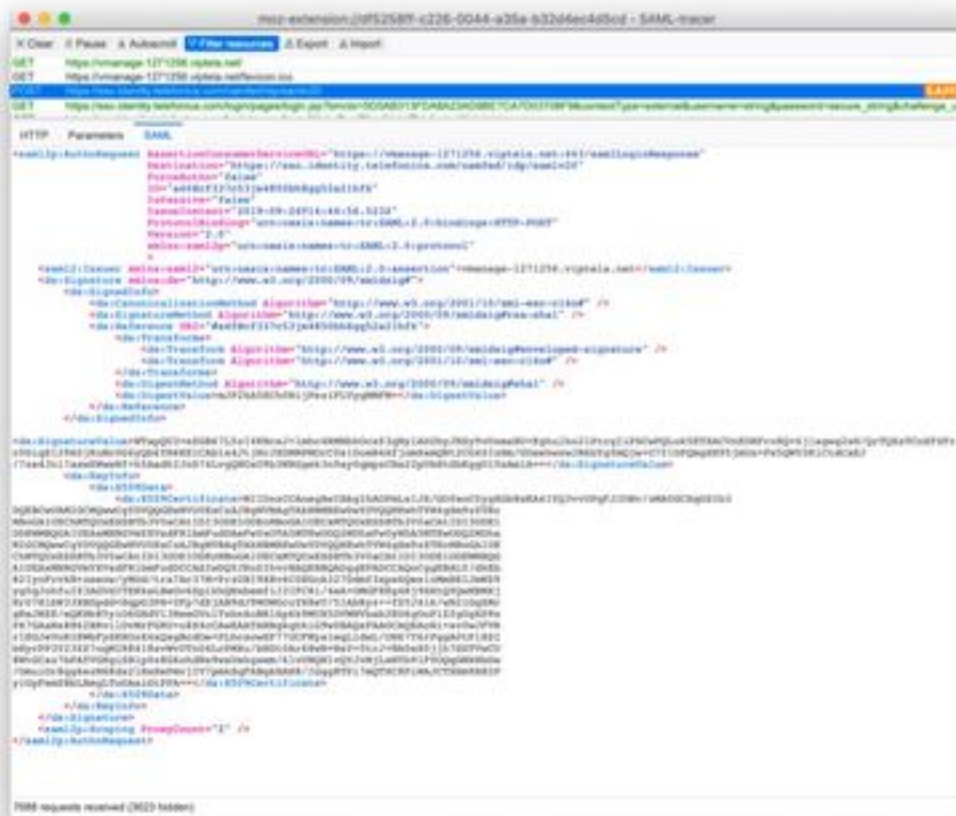
- Die SSO-bezogenen Protokolle werden jetzt in der vManage-Protokolldatei gespeichert. **/var/log/nms/vmanage-server.log** von besonderem Interesse ist die Einstellung "Groups" für die IDP-Autorisierung. Wenn keine Übereinstimmung vorliegt, wird der Benutzer standardmäßig auf die Gruppe "Basic" (Grundlegend) gesetzt, die über schreibgeschützten Zugriff verfügt.
- Um Zugriffsberechtigungsprobleme zu debuggen, überprüfen Sie die Protokolldatei und suchen Sie nach der Zeichenfolge "SamlUserGroups". Im Folgenden wird eine Liste mit Zeichenfolgen von Gruppennamen aufgeführt. Einer von ihnen sollte den Gruppeneinstellungen im vManage entsprechen. Wenn keine Übereinstimmung gefunden wird, wird der Benutzer standardmäßig in die Gruppe "Basic" (Grundlegend) geändert.

SAML-Tracer

Ein Tool zum Anzeigen von SAML- und WS-Federation-Nachrichten, die während der einmaligen Anmeldung und der einmaligen Abmeldung über den Browser gesendet werden.

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

[SAML-Tracer-Erweiterung für Chrome](#)



SAML-

Beispielnachricht

Wie meldet man sich bei SSO-aktiviertem vManage an?

SSO ist nur für Browser-Anmeldung. Sie können vManage manuell auf die herkömmliche Anmeldeseite weiterleiten und die SSO umgehen, um nur Benutzernamen und Kennwort zu verwenden: <https://<vmanagement>:8443/login.html>.

Welcher Verschlüsselungsalgorithmus wird verwendet?

Derzeit unterstützen wir SHA1 als Verschlüsselungsalgorithmus. vManage signiert die SAML-Metadatendatei mit dem SHA1-Algorithmus, den IDs akzeptieren müssen. Die Unterstützung für SHA256 kommt in zukünftigen Versionen, die wir derzeit nicht unterstützen.

Zugehörige Informationen

Einzelanmeldung konfigurieren:

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

OKTA-Login-/Logout-Arbeitsprotokolle als Referenz für das Ticket.