



# SAML Authentication with Pulse Connect Secure and Pulse Secure Virtual Traffic Manager

Deployment Guide

Published

**20 September, 2018**

Document Version

**1.1**

Pulse Secure, LLC  
2700 Zanker Road,  
Suite 200 San Jose  
CA 95134

[www.pulsesecure.net](http://www.pulsesecure.net)

© 2017 by Pulse Secure, LLC. All rights reserved.

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

*SAML Authentication with Pulse Connect Secure and Pulse Secure Virtual Traffic Manager*

The information in this document is current as of the date on the title page.

## **END USER LICENSE AGREEMENT**

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at <http://www.pulsesecure.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Contents

---

INTRODUCTION.....	1
PURPOSE OF THIS GUIDE.....	1
PREREQUISITES.....	1
OVERVIEW.....	1
SUMMARY OF CONFIGURATION.....	2
CONFIGURING THE TRAFFIC MANAGER WITH PCS AS AN IDENTITY PROVIDER (IDP)....	3
CONFIGURING PULSE CONNECT SECURE AS A SAML IDP.....	9
CONFIGURING A TRAFFIC MANAGER VIRTUAL SERVER AS A SAML SP ENDPOINT.....	13
USE CASES AND EXAMPLES.....	19
BROWSER ACCESS – SIMPLE USER AUTHENTICATION.....	19
ADDING COMPLIANCE CHECKING AND TOTP TO THE AUTHENTICATION.....	19
CLOUD SECURE – “REUSE EXISTING NC (PULSE) SESSION”.....	20
CLOUD SECURE – “REUSE EXISTING NC (PULSE) SESSION” AND “REUSE EXISTING IF-MAP SESSION”.....	21
REFERENCES.....	23



# Introduction

---

## Purpose of this Guide

An enterprise can deploy a secure SAML-based Identity Provider (IdP) to handle authentication for web services, applications, and resources delivered by one or more Service Providers (SPs).

This guide describes how to configure Pulse Secure Virtual Traffic Manager (the Traffic Manager) for SP-initiated SAML authentication with Pulse Connect Secure (PCS) acting as the IdP.

## Prerequisites

This guide assumes you are familiar with the SAML protocol, SAML-based authentication methods, and terms such as SP and IdP.

The Traffic Manager supports configuration as a SAML SP from version 17.4 or later.

PCS supports configuration as a SAML IdP from version 8.2R1 or later.

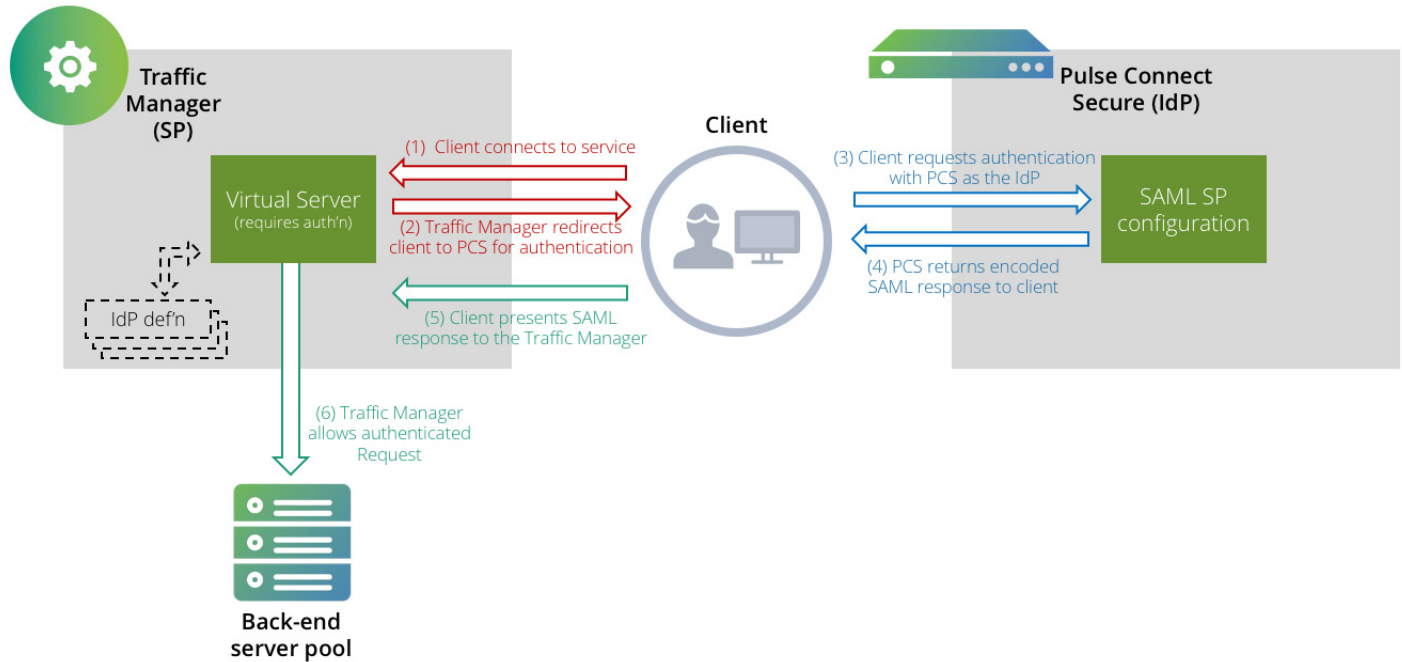
## Overview

The Traffic Manager can function as a SAML SP to control access to your secure back-end web services. Access to these services is permitted only when the client presents a valid Traffic Manager authentication cookie.

In a typical scenario, a user's browser connects to the Traffic Manager to access a service. For the requested service, the Traffic Manager is configured to obtain prior validation, and thus redirects the browser to PCS to be authenticated. PCS checks the identity of the user against its own records, and obtains verification that the user has appropriate privileges for the desired service. If successful, PCS returns the browser to the Traffic Manager with a SAML assertion that the user is legitimate and has the declared identity (typically the email address).

An SP requires a SAML response from the IdP only during the initial authentication exchange.

FIGURE 1 The SAML message exchange between a client, the Traffic Manager, and PCS.



## Summary of Configuration

The Traffic Manager requires certain IDP-derived details from PCS as part of its SAML configuration, and must also provide PCS with specific configuration items in return. To operate successfully, your SAML configuration must match on both the Traffic Manager and PCS.

To apply authentication control to your services, perform the following steps:

1. Configure the Traffic Manager with PCS as the defined IdP.
2. Configure PCS to operate as a SAML IdP, with details of the Traffic Manager as an active SP.
3. Configure your designated Traffic Manager virtual servers as SAML SP endpoints.

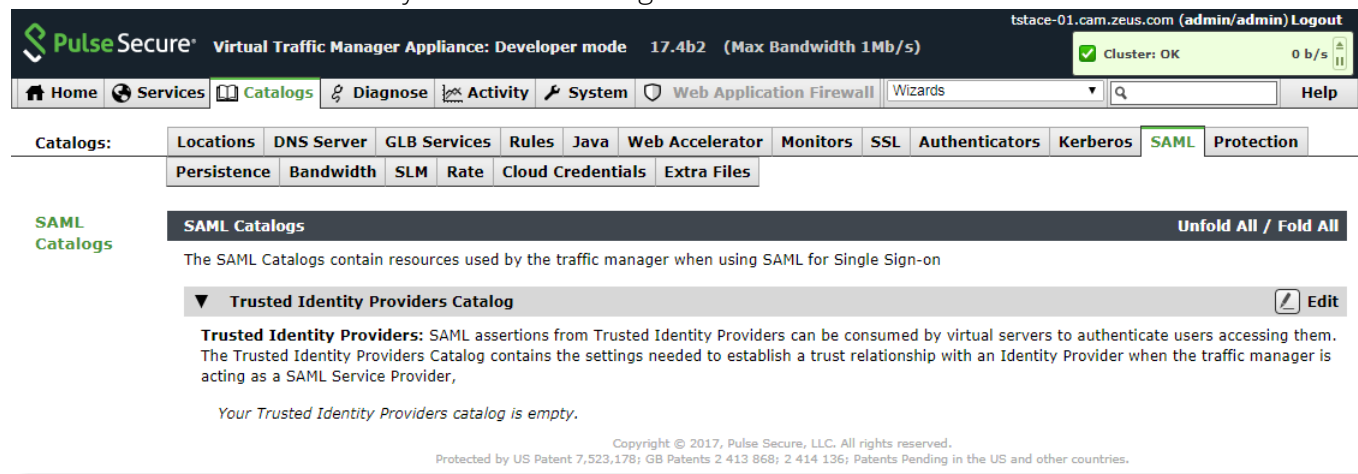
The remainder of this guide describes each of these steps in detail.

# Configuring the Traffic Manager with PCS as an Identity Provider (IdP)

To configure Pulse Connect Secure as a Trusted Identity Provider in the Traffic Manager, perform the following steps:

1. Login to the Traffic Manager Admin UI and navigate to **Catalogs > SAML > Trusted Identity Providers Catalog**.

FIGURE 2 The Trusted Identity Providers Catalog



2. Type the details for your PCS instance into the **Create new Trusted Identity Provider** dialog.

FIGURE 3 Creating a new Trusted Identity Provider

**Create new Trusted Identity Provider**

Name:

The entity id of the IDP  
entity\_id:

The IDP URL to which Authentication Requests should be sent  
url:

The certificate used to verify Assertions signed by the identity provider

```

-----BEGIN NEW CERTIFICATE REQUEST-----
MIICChDCCAWwCAQAwPzELMAkGA1UEBhMCRR0IxIjAQBgNVBAcTCUNhbWJyaWRnZTEN
MAeGA1UEChMEDGVzdDENMAeGA1UEAxMEDGVzdDCCASIdDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAL1UmJbB7MhykL5nXrSvLFoq07+iz5c2wNYePPMp9BE8dcBh
SOLCJv8T3hIso0e39timRA7iUUzoUbiGZnT4InwvYxpTuqfUNmq5ECDTISO7aA5Z
1GMnvCOW7uJBLQ0T80JnL9rzIbKnmOkm/UbuAz+47CHyR2Rjj3q4iu0W2V33ivmp
vjbeBc3vLAvp7NwW/hIJ1ssq4RTudB6Bnes10S/hvEPcl2P++558eUnzitVv86pq
YW8wV1Pwf2aeFa3/L3uIx1W+DcSfg149KU422xzNypikZY89oX4oei5keq7BtWSK
ZhwNwr03QTzqKc7EliW8NISsoslkwfQ3LtzdAf0CAwEAAAARMA0GCSqGSIb3DQEB
CwUAA4IBAQCXubd4gseLP5QBeNPhOV12JAm7QulVNwgUALoV1hW8eOzOvwg0o1k1
D0mwgTfW9mumx6zJ94wXSbi2Chs14Cge75zj25yT+bQVNeDIiyfmmFuB01MUv87T2
k84xOmUa6UyyQbciXw8j39+kvb0LqZwgo17StEkvliKdrBgeq2Me+f4taPod5bHD
sZz0CseGg1271kKDVtGUDj0ZWYKaR8uANYEHOaZrY8tglPVE083ITiDVVm2/rHuB
AZr7qX3+gepMopCoz3oRYAIT0jEiyoF2Lr9TsBkxaIEhfd1RLgc07XXUN3zMO9Kv
pnr39r446lXpRvWiw1TVp98zCX1DnMXI
-----END NEW CERTIFICATE REQUEST-----
    
```

3. Type an identifying name for this IdP.
4. Set **entity\_id** to the unique SAML identifier for the PCS. To obtain the SAML identifier, login to the PCS Admin UI and navigate to **Authentication > Signing In > Sign-in SAML > Metadata Provider**.

FIGURE 4 Obtaining the PCS Entity ID

**Signing In**

Sign-in Policies | Sign-in Pages | Sign-in Notifications | **Sign-in SAML**

**Metadata Provider** Identity Provider

This is configuration of Pulse Connect Secure (SA) SAML Metadata provider.

\*Entity Id:  Unique SAML identifier of the Connect Secure. By default uses host name configured at [SAML Settings](#).

\*Metadata Validity:  days 1 - 9999. Specifies the maximum duration for which a peer SAML entity can cache the Connect Secure metadata file.

Do Not Publish IdP in Metadata Prevents the Connect Secure metadata file to be published at the location specified by the Entity Id.

The Entity ID uses the URL format:

https://<PCS-FQDN>/dana-na/auth/saml-endpoint.cgi.



5. Set **url** to the URL to which the client is redirected for authentication. Use the format:

`https://<Alternate Host FQDN for SAML>/dana-na/auth/saml-sso.cgi`

To obtain the <Alternate Host FQDN for SAML>, login to the PCS Admin UI and navigate to **System > Configuration > SAML > Settings**. Use the value shown in "Alternate Cluster FQDN for SAML".

FIGURE 5 Obtaining the Alternate Host FQDN

SAML >  
**Settings**

▼ Metadata Server Configuration

Timeout value for metadata fetch request:  seconds 1 - 600. Specifies the time in seconds to wait for response of SAML metadata fetch request.

Validity of uploaded/downloaded metadata file:  days 0 - 9999. Specifies the time in days after which downloaded/uploaded metadata file expires. 0 means that Connect Secure does not enforce any validity on the peer metadata file.

Cluster FQDN for SAML:  The FQDN used for generating URLs for SAML services.

Alternate Cluster FQDN for SAML:  The FQDN used for generating SA's Single Sign-On Service URL when Pulse(NC) Session detection is enabled.

6. Set **add\_zlib\_header** to "No".

7. Set **strict\_verify** to "Yes".

8. For **certificate**, use the SAML Signing certificate used by PCS.

To obtain the certificate, login to the PCS Admin UI and navigate to **Authentication > Signing In > Sign-in SAML > Identity Provider**.

FIGURE 6 Locating the name of the SAML Signing certificate

## Signing In

Sign-in Policies    Sign-in Pages    Sign-in Notifications    **Sign-in SAML**

Metadata Provider    **Identity Provider**

▼ **Basic Identity Provider (IdP) Configuration (Published in Metadata)**

**Protocol Binding to use for SAML Response**

Post  
 Artifact

\*Signing Certificate: **SA CL SAN** ▼ Certificate to use for signing SAML messages sent by this IdP

In this example, the certificate is named "SA CL SAN".

Then, navigate to **System > Configuration > Certificates > Device Certificate** and click on the certificate name to see the details.

FIGURE 7 Getting the certificate details

Device Certificates    Trusted Client CAs    Trusted Server CAs    Code-signing Certificates    Client Auth Certificates    Certificates Validity Check

Specify the Device Certificate(s). If you don't have a certificate yet, you can create a CSR and import the resulting signed certificate. If necessary, you can add custom

**Import Certificate & Key...**    **Delete...**

10 records per page

<input type="checkbox"/>	Certificate issued to	Issued by	Valid Dates
<input type="checkbox"/>	SA CL SAN	Golden1665	Nov 25 11:25:56 2017 GMT to Nov 25 11:25:56 2019 GMT

To obtain the certificate text, use the "Download" link.

FIGURE 8 Downloading the certificate

Certificates > Certificate Details

## Certificate Details

### ▼ Certificate

Issued To: ▼ SA CL SAN

Org Unit Name: IT  
Org Name: example.org  
Locality: Somewhere  
State: State  
Country: US  
Email Address: someone@example.com

Issued By: ▶ Golden1665

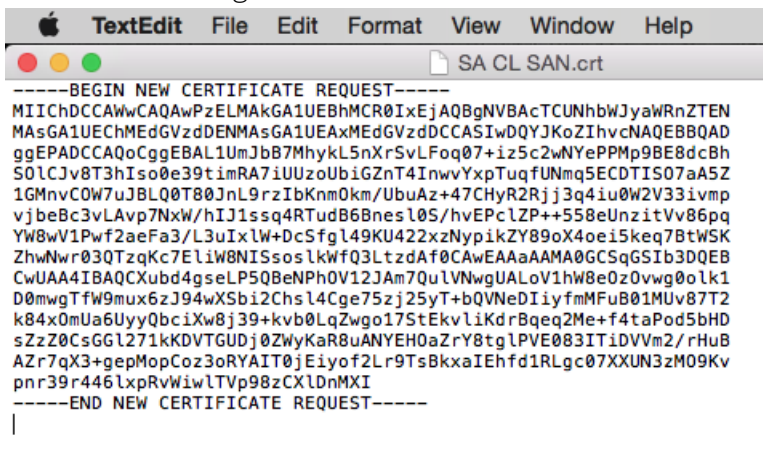
Valid: Nov 25 11:25:56 2017 GMT to Nov 25 11:25:56 2019 GMT

Details: ▶ Other Certificate Details

[Download](#)

Open the downloaded certificate data in a text editor.

FIGURE 9 Viewing the certificate file in a text editor



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICDCCAwwCAQAwPzELMAkGA1UEBhMCR0IxExjAQBgNVBAcTCUNhbWJyZXRnZTEN
MA5GA1UEChMEDGVzdDENMA5GA1UEAxMEDGVzdDCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAL1UmJbB7MhykL5nXrSvLFoq07+iz5c2wNYePPMp9BE8dcBh
S0lCJv8T3hIso0e39timRA7iUUzoUbiGZnT4InwvYxpTuqfUNmq5ECDTIS07aA5Z
1GMnvCOW7uJBLQ0T80JnL9rzIbKnm0km/UbuAz+47CHyR2Rjj3q4iu0W2V33ivmp
vjbeBc3vLAvp7Nxw/hIJ1ssq4RTudB68nesl0S/hvEPcLZP++558eUnzitVv86pq
YwBwV1Pwf2aeFa3/L3uIxlw+DcSfgl49KU422xzNypikZY89oX4oei5keq7BtWSK
ZhwNwr03QTzqKc7ELiWBNISsoslkWfQ3LtzdAf0CAwEAAaAAMA0GCSqGSIb3DQEB
CwUAA4IBAQCxubd4gseLP5QBENPh0V12JAm7QuLVNwgUALoV1hW8e0z0vvg0lk1
D0mWgTfW9mux6zJ94wXSbi2ChsL4Cge75zj25yT+bQVNeDIiyfMfFuB01Muv87T2
k84x0mUa6UyyQbcixW8j39+kvb0LqZwgo17StEkvliKdrBqeq2Me+f4taPod5bHD
sZzZ0CsGGL271kKDVtGUDj0ZWyKaR8uANYEH0aZrY8tgLPVE083ITiDvVm2/rHuB
AZr7qX3+gepMopCoz3oRYAIT0jEiyoF2Lr9TsBkxaIEhfd1RLGc07XXUN3zMO9Kv
pnr39r446lXpRvWiwLTVp98zCXLDnMXI
-----END NEW CERTIFICATE REQUEST-----
```

Finally, copy the certificate text and paste it into the **Certificate** field in the Traffic Manager Trusted Identity Provider definition.

9. To save the Trusted Identity Provider definition, click **Create New Trusted Identity Provider**.



# Configuring Pulse Connect Secure as a SAML IdP

To configure PCS as a SAML IdP to the Traffic Manager, perform the following steps:

1. Login to the PCS Admin UI and navigate to **Authentication > Signing In > Sign-in SAML > Identity Provider**.
2. Scroll to the bottom of the page to add a new Service Provider.
3. Select **Manual** configuration mode.

FIGURE 10 Adding a new Service Provider

## New Peer Service Provider

\*Configuration Mode:  Manual  Metadata If metadata is selected, uses metadata files uploaded/added at [Peer SAML Metadata Providers](#).

▼ Service Provider Configuration

\*Entity Id:  Unique SAML Identifier of the SP.

\*Assertion Consumer Service URL:  URL of the service on SP that receives the assertion/artifact generated by the IdP.

Protocol Binding supported by the Assertion Consumer Service at the SP.

Post  
 Artifact

\*Default Binding:  Post  Artifact

Signature Verification Certificate: This certificate is used by IdP to verify the signature in the incoming SAML Message incoming message is used to verify the signature.

Issued To:  
Issued By:  
Valid:  
Details: ▶ Other Certificate Details

Upload Certificate:  No file chosen

Encryption Certificate: The certificate to use if the the assertions from this IdP need to be encrypted.

Issued To:  
Issued By:  
Valid:  
Details: ▶ Other Certificate Details

Upload Certificate:  No file chosen

4. Set **Entity Id** and **Assertion Consumer Service** URL to the equivalent values used by your Traffic Manager SAML SP configuration (see [“Configuring a Traffic Manager Virtual Server as a SAML SP Endpoint”](#) on page 13).

For Entity ID, ensure you match the value stored in **auth!saml!sp\_entity\_id**, and Assertion Consumer Service URL, use the value stored in **auth!saml!sp\_acs\_url**.

5. Select only POST protocol binding.

- The Traffic Manager does not sign the authentication request so there is no requirement to add a Signature Verification Certificate or Encryption Certificate. Ensure "Accept unsigned AuthnRequest" is enabled.

FIGURE 11 Enabling "Accept unsigned AuthnRequest"

**▼ Certificate Status Checking Configuration**

Enable signature verification certificate status checking Check this to enable revocation checks for the signing certificate. (Uses configuration in [Trusted Client CAs.](#))

Enable encryption certificate status checking Check this to enable revocation checks for the Encryption certificate. (Uses configuration in [Trusted Client CAs.](#))

**▼ Customize IdP Behavior**

Override Default Configuration

Reuse Existing NC (Pulse) Session If enabled, the user's existing NC (Pulse) session if any will be used in the SP-initiated SSO scenario, instead of authenticating the user.

Reuse Existing IF-MAP Session If enabled, the user's existing IF-MAP session if any will be imported and used in the SP-initiated SSO scenario, instead of authenticating the user. If both options are selected, the priority is given to "Reuse Existing NC (Pulse) Session".

Accept unsigned AuthnRequest

Sign SAML Assertion If enabled, SAML assertion will also be signed along with signing the SAML response by default.

Relay State:  'RelayState' sent to SP in IdP-initiated SSO scenario. If left blank, the (URL) identifier of the resource being accessed will be used.

\*Session Lifetime:  None Suggested maximum duration of the session at the SP created due to SAML SSO.

Role Based

Customize

\*SignIn Policy:  The SignIn Policy used by this IdP to authenticate the user in SP-initiated SSO scenario.

\*Force Authentication Behavior:  Reject AuthnRequest SA behavior if SP sends an authentication request with ForceAuthn set to true for a user with valid browser session.

Re-Authenticate User

- The settings **Reuse Existing NC (Pulse) Session** and **Reuse Existing IF-MAP Session** are covered in the use cases section in this document.
- Select the **SignIn Policy** from the drop-down list to be used by users as they authenticate. In this example, "\*/adc/" is selected.
- Select the User Identity to be used. In this example, the **Subject Name Format** is "DN" and **Subject Name** is "uid=<username>".
- Finally, select for which **Roles** the IdP must issue SAML Assertions.

FIGURE 12 Selecting Roles for which SAML Assertions are issued

**User Identity**

\*Subject Name Format:  Format of 'NameIdentifier' field in generated Assertion.

\*Subject Name:  Template for generating user's identity as sent in 'NameIdentifier' field.

**Attribute Statement Configuration**

Send Attribute Statements If checked, Attribute statements will be sent for the SP.

Use IdP Defined Attributes

Customize IdP Defined Attributes

▼ Roles

Policy applies to ALL roles

Policy applies to SELECTED roles

Policy applies to all roles OTHER THAN those selected below

Available roles: Selected roles:

ActiveSync	Add ->	adc-role
adc-role-web		
Admin-Access	Remove	
Android4W		
Android_CloudSecure_R		
ADP-SAMV		

11. Save the new SAML SP configuration.



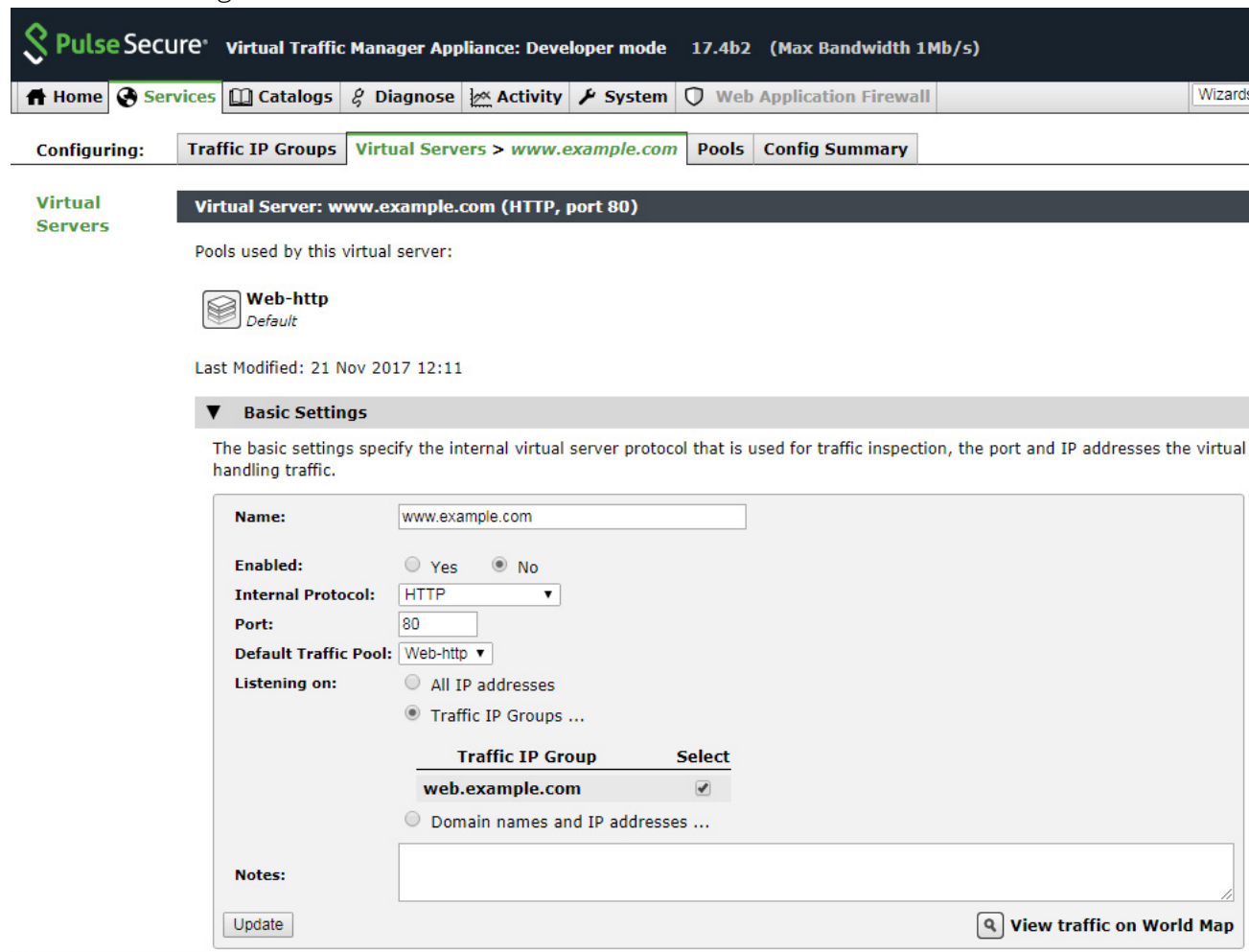


# Configuring a Traffic Manager Virtual Server as a SAML SP Endpoint

To configure a Traffic Manager service with SAML SP authentication, perform the following steps:

1. Designate a virtual server as your SAML SP endpoint. Navigate to **Services > Virtual Servers** and click the name of the required virtual server.

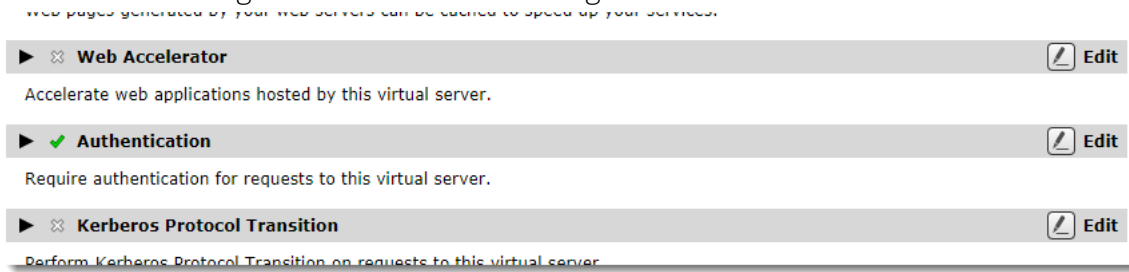
FIGURE 13 Editing a virtual server



Pulse Secure *strongly recommends* against using SAML authentication without TLS encryption. Your virtual server should therefore have SSL Decryption enabled.

2. Locate the **Authentication** section and click to edit.

FIGURE 14 Locating the Authentication Settings



3. Set **auth!type** to "SAML Service Provider".
4. For troubleshooting or testing purposes, optionally set **auth!verbose** to "Yes". Note that this setting generates a lot of log content, so is recommended to be disabled for a live service.
5. For a typical service, leave the settings under "Authentication Session Management" as their default values.

FIGURE 15 Virtual Server Authentication settings

**Virtual Server: www.example.com (HTTP, port 80)**

Your virtual server can require authentication.

### Authentication

These settings control additional authentication for HTTP requests

Type of authentication to apply to requests to the virtual server.  
**auth!type:**

Whether or not detailed messages about virtual server authentication should be written to the error log.  
**auth!verbose:**  Yes  No

### Authentication Session Management

These settings control the behavior of sessions used by the authentication system

Name of cookie used for authentication session.  
**auth!session!cookie\_name:**

Timeout on authentication session.  
**auth!session!timeout:**  seconds

Whether or not to include state of authentication sessions stored encrypted on the client as plaintext in the logs.  
**auth!session!log\_external\_state:**  Yes  No

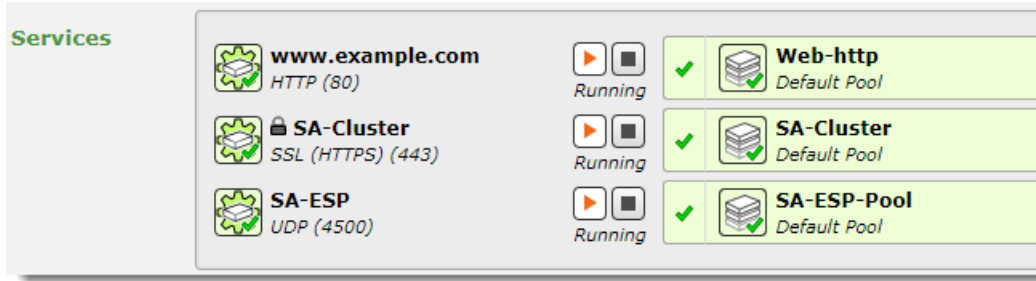
Attributes of cookie used for authentication session.  
**auth!session!cookie\_attributes:**

- In the "SAML Service Provider" section, set **auth!saml!sp\_entity\_id** to an HTTPS URL that the IdP uses to identify the Traffic Manager as the SAML SP (that redirected a user agent for authentication). Then set **auth!saml!sp\_acs\_url** to the HTTPS URL of the SAML Assertion Consumer Service (ACS). In other words, the URL at which the Traffic Manager should handle SAML assertions.

These values must match the equivalent fields specified in your PCS Service Provider configuration (see "Configuring Pulse Connect Secure as a SAML IdP" on page 7).

In the following example, SAML Authentication is added to a Traffic Manager virtual server named "www.example.com". This virtual server is configured to listen on an IP address that resolves to a URL of the same name.

FIGURE 16 Your currently running services



The following example values can then be used:

- Entity ID:

`https://www.example.com/saml/metadata`

- Assertion Consumer Service URL:

`https://www.example.com/saml/consume`

When the Traffic Manager receives an HTTP request through the "www.example.com" virtual server, it first checks if the URL corresponds to the ACS URL. If yes, the Traffic Manager handles this URL as the SAML ACS endpoint; otherwise it forwards the request to the pool nodes.

7. Select the **auth!saml!idp** that was created in the first step in this guide.
8. As SAML is sensitive to time, Pulse Secure recommends that both the Traffic Manager and PCS are set to use Network Time Protocol (NTP). When using NTP, the tolerance of 5 seconds should be sufficient for the service.
9. Set **auth!saml!nameid\_format** to "unspecified".

FIGURE 17 SAML Service Provider endpoint settings

### SAML Service Provider

These settings control the behavior of the SAML Service Provider endpoint

The entity ID to be used by the SAML service provider function on this virtual server. This should usually be a URL, or a URN, however it may be any string. It must match the entity ID placed by the identity provider in the 'Audience' field in the SAML assertion.

**auth!saml!sp\_entity\_id:**

The 'Assertion Consumer Service' endpoint for the SAML service provider on this virtual server, ie the endpoint to which the identity provider will cause the user agent to send SAML assertions. This should be an HTTPS URL, must be in the same cookie domain as all hostnames used by the end user to access the virtual server (see cookie configuration) and the port must be the port on which this virtual server is listening. It must match the URI placed by the identity provider in the 'Recipient' attribute in the SAML assertion, if present.

**auth!saml!sp\_acs\_url:**

Name of the Trusted Identity Provider configuration to use. To create Identity Providers, please visit section **Trusted Identity Providers**

	Name	Entity Id
<b>auth!saml!idp:</b>	<input type="radio"/> None	
	<input checked="" type="radio"/> SA-IdP	https://sa.example.com/dana-na/auth/saml-endpoint.cgi

Time tolerance on authentication checks. When checking time-stamps and expiry dates against the current time on the system, allow a tolerance of this many seconds. For example, if a SAML response contains a 'NotOnOrAfter' that is 4 seconds in the past according to the local time, and the tolerance is set to 5 seconds, it will still be accepted. This is to prevent a lack of clock synchronization from resulting in rejection of SAML responses.

**auth!saml!time\_tolerance:**  seconds

The NameID format to request and expect from the identity provider.

**auth!saml!nameid\_format:**

### Apply Changes

10. To save the configuration, click **Update**.

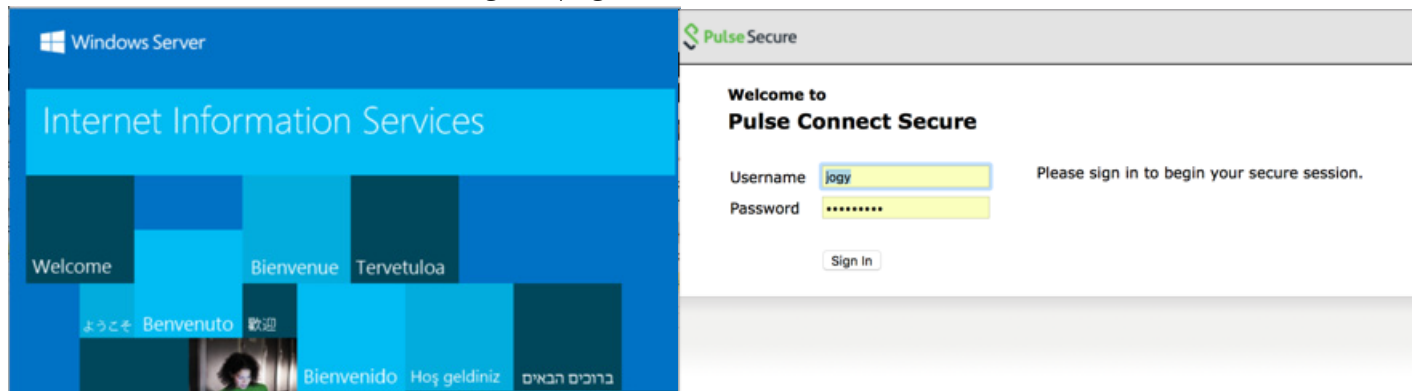


# Use Cases and Examples

## Browser Access – Simple User Authentication

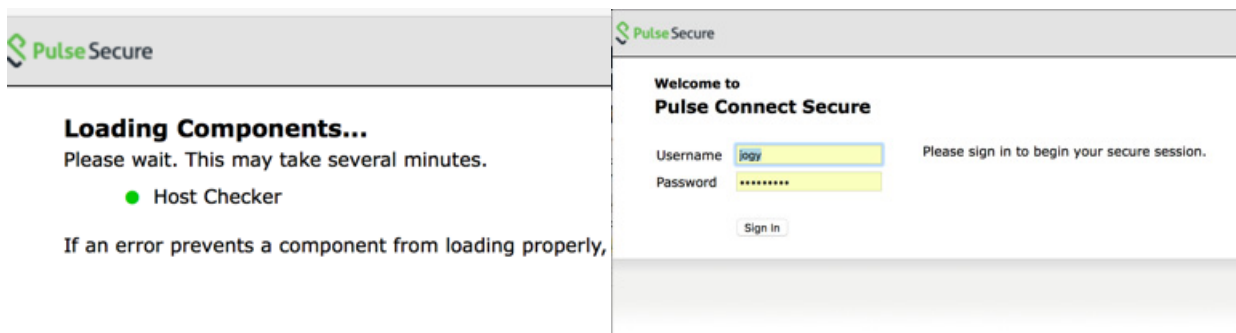
A user attempts to access the Traffic Manager-served "www.example.com". As this service is configured as a SAML SP endpoint, the user's browser is redirected to the PCS sign-in page for authentication.

FIGURE 18 The PCS authentication sign-in page



After passing authentication, PCS returns the user's browser to the Traffic Manager, complete with a SAML assertion that the user is legitimate, to access the back-end pool resource originally requested.

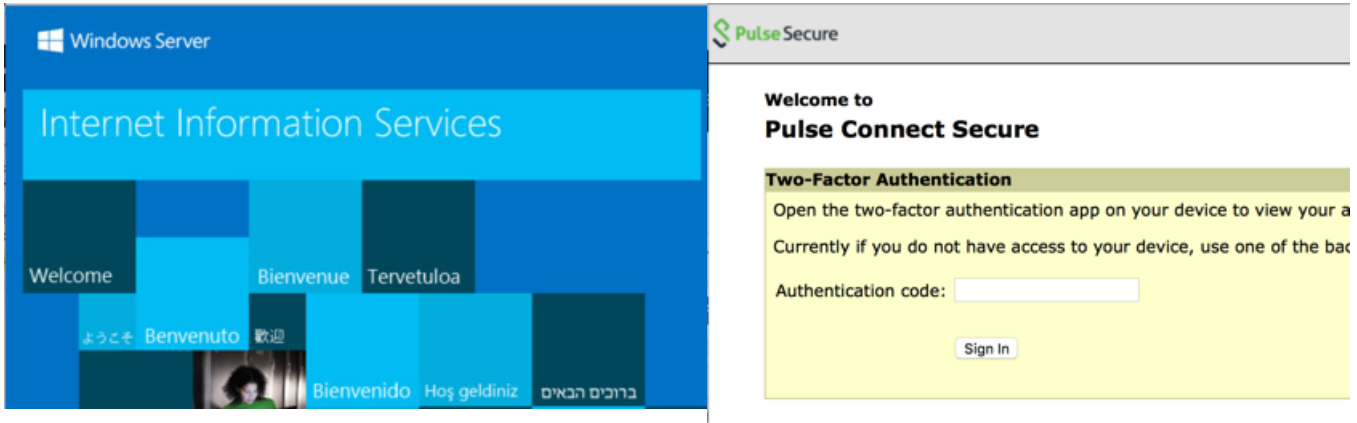
FIGURE 19 Authentication successful



## Adding Compliance Checking and TOTP to the Authentication

A user attempts to access the Traffic Manager-served "www.example.com". As this service is configured as a SAML SP endpoint, the user's browser is redirected to the PCS sign-in page for a compliance check, and both Active Directory and TOTP authentication.

FIGURE 20 Performing two-factor authentication

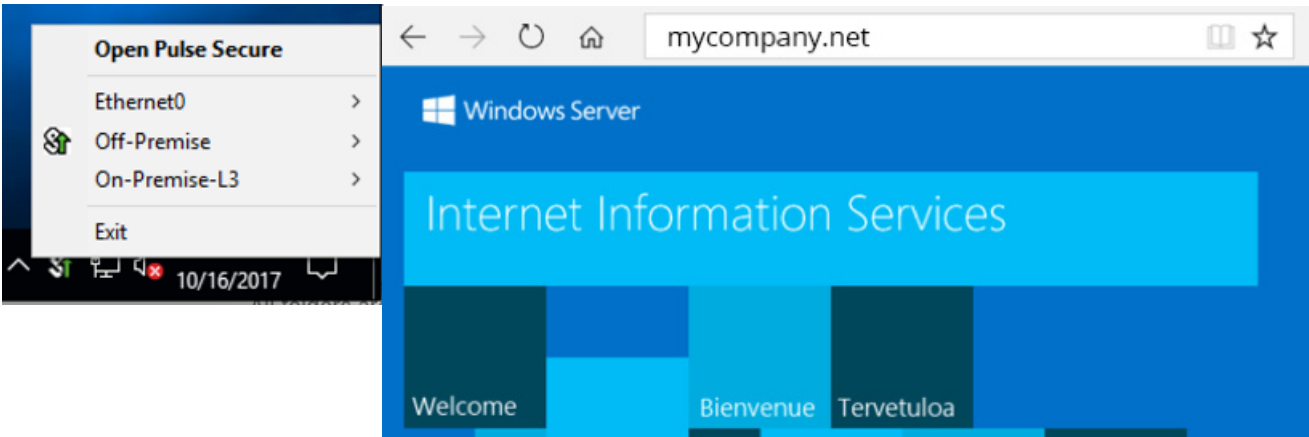


## Cloud Secure – “Reuse Existing NC (Pulse) Session”

By configuring the SAML SP in PCS to reuse an existing session, any user with an existing VPN or AppVPN session uses Single Sign-On (SSO) to the protected resource served by the Traffic Manager virtual server.

The user has a Pulse Secure VPN connection to PCS and accesses the virtual server.

FIGURE 21 Connecting to a VPN



User logs from PCS, acting as a SAML IdP.

FIGURE 22 PCS user logs showing SAML authentication activity

Severity	ID	Message
Info	SML20974	2017-10-16 12:38:30 - ive - [127.0.0.1] System() [] - Sending SAML response for Username: [jogj], User Agent: [Pulse-Secure/8.3.3.919 (Windows 10) Pulse/5.3.3.919], Subject Name: [jid=jogj], Source IP: [192.168.1.1], Type: [SP-Initiated], SP EntryID: [http://www.gillnet.com/keat/saml/metadata], Session ID: [c0229fb912d5f3fc1c09f8ad039f860c938b20e06ee26], Relay State: [7T2XK06-3pPRGSC1U0yJyH2Kya4KhcTwXW7bw5Wg0glew4XEJU+WNSA/Buc6oY2bSRdAWfGm2IK409Bw+KBGpuyq2RDMGukRiJh6FUX9WAWOBLUKB4J4XUJkBPk21AGw0m930Cw==], AuthnRequest ID: [_c09ffc67-de79-cb42-e1d6-7fd0584ae974], Remote IP: [10.0.1.225]
Info	AUT30799	2017-10-16 12:38:30 - ive - [127.0.0.1] System() [] - 'NC/Pulse' session detected for SAML AuthnRequest id '_c09ffc67-de79-cb42-e1d6-7fd0584ae974'
Info	AUT30797	2017-10-16 12:38:30 - ive - [127.0.0.1] System() [] - SAML AuthnRequest received '<?xml version="1.0"?><samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="_c09ffc67-de79-cb42-e1d6-7fd0584ae974" Version="2.0" IssueInstant="2017-10-16T10:38:29Z" ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" AssertionConsumerServiceURL="http://www.gillnet.com/keat/saml/consume"><saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://www.gillnet.com/keat/saml/metadata</saml:Issuer-><samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" AllowCreate="true"/></samlp:AuthnRequest>

The user's browser is redirected to PCS with the SAML AuthnRequest.

```
2017-10-16 12:38:30 - ive - [127.0.0.1] System() [] - SAML AuthnRequest received '<?xml version="1.0"?><samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="_c09ffc67-de79-cb42-e1d6-7fd0584ae974" Version="2.0" IssueInstant="2017-10-16T10:38:29Z" ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
```



```
AssertionConsumerServiceURL="http://www.example.com/saml/consume"><saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://www.example.com/saml/metadata</
saml:Issuer><samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified" AllowCreate="true"/></samlp:AuthnRequest>'
```

PCS finds an existing session from this user and reuses it.

```
2017-10-16 12:38:30 - ive - [127.0.0.1] System() [] - 'NC/Pulse' session detected for SAML
AuthnRequest Id '_c09ffc67-de79-cb42-e1d6-7fd0584ae974'
```

PCS generates a SAML Assertion giving the user SSO to the virtual server.

```
2017-10-16 12:38:30 - ive - [127.0.0.1] System() [] - Sending SAML response for Username:
[jogy], User Agent: [Pulse-Secure/8.3.3.919 (Windows 10) Pulse/5.3.3.919], Subject Name:
[uid=jogy], Source IP: [192.168.1.1], Type: [SP-Initiated], SP EntityID: [http://
www.example.com/saml/metadata], Session ID:
[sid225fb912dd5f3fc1cf09f3adc53df0860bf38b03e05eef26], Relay State: [/
T2lilQ6+3pIRGSCT1U0yzJ/yH2fKyl4/KhcTw/XW7lbw5Wg0gIexm4XEJU+WNSA/
8uc6oY2biSRdAWIfpM2IlK40t19x+KBGpuyql2iRDMGuKRu3HbfUX5WAW0BUKB4U4XUxKBPke21AGw0m930Cw==],
AuthnRequest ID: [_c09ffc67-de79-cb42-e1d6-7fd0584ae974], Remote IP: [10.0.1.225]
```

## Cloud Secure – “Reuse Existing NC (Pulse) Session” and “Reuse Existing IF-MAP Session”

This use case includes the Federation functionality provided by IF-MAP.

PCS and Pulse Policy Secure (PPS) are acting as IF-MAP clients and publish user sessions to the Federation (IF-MAP) server.

In this use case, the user is on the internal network and has an existing session with PPS. The user still gets SSO to the protected resource served by the Traffic Manager virtual server.

The user browser is redirected to Pulse Connect Secure with the SAML AuthnRequest

```
2017-10-16 13:17:42 - ive - [127.0.0.1] System() [] - SAML AuthnRequest received '<?xml
version="1.0"?><samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
ID="_16fca8ef-38ea-bcd1-6bb6-fb9fa601f613" Version="2.0" IssueInstant="2017-10-
16T11:17:43Z" ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
AssertionConsumerServiceURL="http://www.example.com/saml/consume"><saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://www.example.com/saml/metadata</
saml:Issuer><samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified" AllowCreate="true"/></samlp:AuthnRequest>'
```

PCS (the IdP) does not find any local session for the user. PCS queries the Federation (IF-MAP) server, finds a session, and imports it.

```
2017-10-16 13:17:43 - ive - [127.0.0.1] System() [] - 'IF-MAP' session detected for SAML
AuthnRequest Id '_16fca8ef-38ea-bcd1-6bb6-fb9fa601f613'
```

```
2017-10-16 13:17:43 - ive - [10.0.2.50] jogy(IF-MAP Import)[0365, Salesforce,
SecureAccess] - Imported session published by 1CgABCQ/- from IF-MAP
```

PCS generates a SAML Assertion giving the user SSO to the virtual server.

```
2017-10-16 13:17:43 - ive - [127.0.0.1] System() [] - Sending SAML response for Username:
[jogy], User Agent: [Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/
56.0], Subject Name: [uid=jogy], Source IP: [10.0.2.50], Type: [SP-Initiated], SP EntityID:
[http://www.example.com/saml/metadata], Session ID: [], Relay State: [/
T21lilQ6+3pIRGSCT1U0y3c7tqiB3U7+zyKi9eM2tdu23Q4ccJSMm6ct14DpjduwSSWYqo4tBwJDpw/
eqnDRXeEB6nSYpOz5ymDVpb/b20ukCT45GpNiTDZc5i/
tSGl61XFVhImpWMriLxcoxwfrtjWWH33QPU4qpXFXd6ptW/M=], AuthnRequest ID: [_16fca8ef-38ea-bcd1-
6bb6-fb9fa601f613]
```

**Note:** If no session is found locally or via the federation layer, the user is presented with the standard browser authentication experience.

# References

---

- <https://www.pulsesecure.net/download/techpubs/current/1022/Pulse-vADC-Solutions/Pulse-Virtual-Traffic-Manager/17.4/ps-vtm-17.4-releasenotes.pdf>
- <https://www.pulsesecure.net/download/techpubs/current/1027/Pulse-vADC-Solutions/Pulse-Virtual-Traffic-Manager/17.4/ps-vtm-17.4-userguide.pdf>
- <https://www.pulsesecure.net/download/techpubs/current/894/pulse-connect-secure/pcs/8.3rx/ps-pcs-sa-8.3-admin-guide.pdf>
- <https://www.pulsesecure.net/download/techpubs/current/935/pulse-connect-secure/pcs/8.3rx/ps-pcs-cloudsecure-8.3-common-components-configuration-guide.pdf>

