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. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.
# Table of Contents

- **Introduction** ................................................................................................................................. 5
  - About this guide ................................................................................................................................. 5
- **Pulse Connect Secure Configuration** ............................................................................................. 6
- **Salesforce Configuration** ................................................................................................................. 9
- **End-User flow on Mobile Devices** .................................................................................................. 14
- **End-User flow on Desktops** ............................................................................................................ 15
- **Troubleshooting** ............................................................................................................................... 16
List Of Figures

Figure 1 New Metadata Provider ................................................................. 7
Figure 2 Add Service Provider ................................................................. 8
Figure 3 Enable SAML ........................................................................... 10
Figure 5 Configure Service Provider ....................................................... 11
Figure 4 Authentication Configuration .................................................. 12
Figure 6 Create User ............................................................................ 13
Introduction

About this guide

This document describes the configuration required on Salesforce cloud service and configuration of Salesforce Service Provider on Pulse Connect Secure to provide Secure Single Sign-On access to Salesforce users. This document does not cover basic configurations on Pulse Connect Secure (PCS) and Pulse Workspace (PWS) Server which are required to be enabled before configuring Service Provider specific configurations outlined in this document. Basic configurations of PCS and PWS are covered as part of Common Components Configuration Guide.
Pulse Connect Secure Configuration

Pulse Connect Secure (PCS) should be enabled as SAML Identity Provider for supporting Single Sign-On. For Cloud Secure solution PCS should be configured with:

- Network Settings
- Certificates
- Registration with Pulse One
- Pulse Workspace MDM Authentication Server configured as device attribute server
- SAML configurations
- Role and Realm configurations

For details on above configurations of Pulse Connect Secure, refer to Common Components Configuration Guide.

In addition to above configurations, Salesforce should be configured as Service Provider on Pulse Connect Secure.

Follow below steps to configure Salesforce SP on PCS:

1. Login to Pulse Connect Secure admin console
2. Navigate to System→Configuration→SAML. Click on ‘New Metadata Provider’
   a. Provide Name
   b. Upload the downloaded Metadata file from SalesForce.com (Step 6 of Salesforce Configuration) by clicking Browse
   c. Enable Accept Unsigned Metadata
   d. Enable Service Provider under Roles
   e. Click Save Changes
3. Navigate to Authentication->Signing In->Sign-in SAML->Identity Provider. Click on ‘Add SP’ on the configuration page:

   a. Select Configuration mode as Metadata
   b. Select the Entity ID (the Entity ID will be the Salesforce domain)
   c. Select Override Default Configuration (Optional). This configuration is required only if you wish to make SP specific changes (say, override Subject Name specified in Basic Identity Provider configuration at Authentication->Signing In->Sign-in SAML->Identity Provider)
   d. Assign required roles
   e. Click Save Changes
Figure 2 Add Service Provider
Salesforce Configuration

Salesforce should be enabled as SAML Service Provider for supporting Single Sign-On. For Cloud Secure solution Salesforce should be configured with:

- Admin account
- Register Domain
- SAML configurations
- Users

Steps to Configure

Follow below steps to configure Salesforce as Service Provider:

1. Signup for a new Salesforce account. Register a new Salesforce domain
2. Once domain is registered, login to the domain (Ex: cloudsecure-dev-ed.my.salesforce.com). Click on “Setup” on top right corner of the page
3. Navigate to Security Controls -> Single Sign-On Settings on the left panel. Click on ‘Edit’, check ‘SAML Enabled’ and click ‘Save’
4. Navigate to **Security Controls-> Single Sign-On Settings**. Click ‘**New**’ under ‘SAML Single Sign-On Settings’. Enter the following details:

   a. Name: `<Name>`
   b. API Name: `<Name>`
   c. Issuer: [https://<Host FQDN for SAML>/dana-na/auth/saml-endpoint.cgi](https://<Host FQDN for SAML>/dana-na/auth/saml-endpoint.cgi)
   d. Entity ID: `<Salesforce Domain>`; Example: [https://cloudsecure-dev-ed.my.salesforce.com](https://cloudsecure-dev-ed.my.salesforce.com)
   e. Identity Certificate:
      - Download PCS Metadata file from Authentication->Signing-in->Sign-in SAML->Metadata Provider. Copy Certificate content out of PCS Metadata to a file, save it, generate X509 Certificate out of it and upload it here (or)
      - Choose the IdP Signing Certificate configured under Authentication-> Signing-in-> Sign-in SAML-> Identity Provider page of PCS and upload it here
   f. Service Provider Initiated Request Binding: HTTP Redirect
   g. Identity Provider Login URL: [https://<Alternate Host FQDN for SAML /dana-na/auth/saml-sso.cgi](https://<Alternate Host FQDN for SAML /dana-na/auth/saml-sso.cgi)
   h. Leave rest of the fields with default values and click ‘**Save**’
5. Navigate to Domain Management -> My Domain on the left panel. Click on ‘Edit’ under ‘Authentication Configuration’ section, check ‘<Name>’ (configured in Step 4a) and click ‘Save’.

7. Navigate to Administer-> Manage Users-> Users. Click on ‘New User’ to create a new Salesforce user if user does not exist. Provide following details:
   a. Provide First Name
   b. Provide Last Name. Alias will get populated automatically
   c. Provide Email. Username and Nickname will get populated automatically
   d. Select Role for the user
   e. Select User License as ‘Salesforce’
   f. Select Profile for the user
   g. Click Save
Figure 6 Create User
End-User flow on Mobile Devices

Once administrator does the above configurations and creates a new user if not present in Pulse Workspace, user has to follow below steps to register the mobile device with Pulse Workspace and get seamless secure Single Sign-On access to Salesforce Application:

1. User receives Welcome Mail with registration details
2. Follow the instructions in the mail and register the user device
3. Once registration of mobile device with Pulse Workspace is successful, configured profile will get installed on the device along with VPN certificate
4. Install Salesforce managed application when prompted
5. Install Pulse Client on the mobile device. VPN profile will get configured automatically on Pulse Client
6. On Android devices, open Pulse Client and establish VPN connection manually. VPN tunnel will automatically get established on iOS devices when managed application configured with Per App VPN is accessed
7. Access Salesforce application, select ‘Use Custom Domain’ link in the Salesforce application and provide the Salesforce URL details (Ex: cloudsecure-dev-ed.my.salesforce.com)
8. Click on 'sso' link at the bottom of the application. Single Sign-On will happen and user will get access to the Salesforce
End-User flow on Desktops

Once administrator does the above configurations, user can access Salesforce URL via browser from Windows/MAC OS X Desktops. Follow below steps to enable Secure Single Sign-On browser-based access to Salesforce Cloud Service:

1. Launch Pulse Client and establish a VPN session with PCS
2. Open any web browser on the desktop, access Salesforce URL (Ex: cloudsecure-dev-ed.my.salesforce.com) and click on ‘SSO’

   a. If user has an existing VPN session, ‘Re-use existing Pulse Session’ will kick in,
      PCS will send SAML response to Salesforce SP and user will be granted access to Salesforce Cloud Service

   b. If user did not establish Pulse VPN session as mentioned in Step 1, user will be redirected to Pulse Connect Secure user login page or user will be prompted to select user certificate for authentication depending on the PCS configuration. Once authenticated, PCS will send SAML response to Salesforce SP and user will be granted access to Salesforce Cloud Service
Troubleshooting

Single Sign-On for a Salesforce user can fail due to configuration issues on Pulse Connect Secure, Salesforce Service Provider, Pulse Mobile Client or Pulse Workspace. To troubleshoot issues with Single Sign-On:

- On PCS, under Maintenance-> Troubleshooting, enable the event codes – “saml, auth” at level “50” and collect debug logs. Enable Policy Tracing and capture the Policy traces for the specific user.
- Check System-> Log/Monitoring-> User Access-> Log for SAML AuthNRequest and Response for the specific user. Verify if ‘Subject Name’ is proper in the SAML Response.
  a. Click ‘SAML Assertion Validator’.
  b. Select ‘sso’ and click ‘Validate’
  c. Check Results and fix if any issues reported
  d. If any issue related to timestamp is reported, verify that the time zone configured on Pulse Connect Secure and Salesforce SP is in sync. Configuring NTP Server on Pulse Connect Secure can also resolve this issue.
- On mobile device, open Pulse Client and Send Logs to your administrator.