Pulse Secure

Cloud Secure – Salesforce

Configuration Guide

Document Revisions	3.0
Published Date	December 2018

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

https://www.pulsesecure.net

Cloud Secure – Salesforce Configuration Guide

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

END USER LICENSE AGREEMENT

Introduction

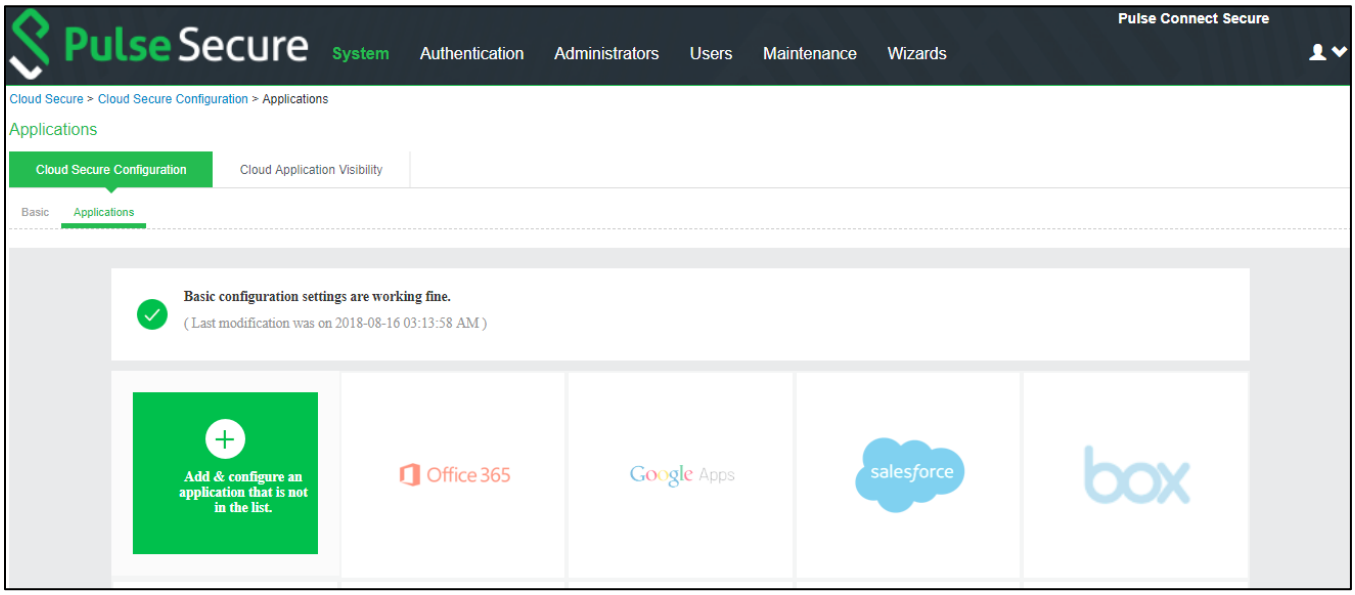
This document describes the configuration required on Salesforce cloud service and configuration of Salesforce Service Provider on Pulse Connect Secure to provide Secure Single Sign-On access to Salesforce users. This document does not cover basic configurations on Pulse Connect Secure (PCS) and Pulse 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 *Cloud Secure Admin Guide*.

Pulse Connect Secure Configuration

For basic configurations details, refer to the following sections:

- **Configuring Pulse Connect Secure - Basic Configurations (Mandatory)**
- **Configuring Pulse Workspace**

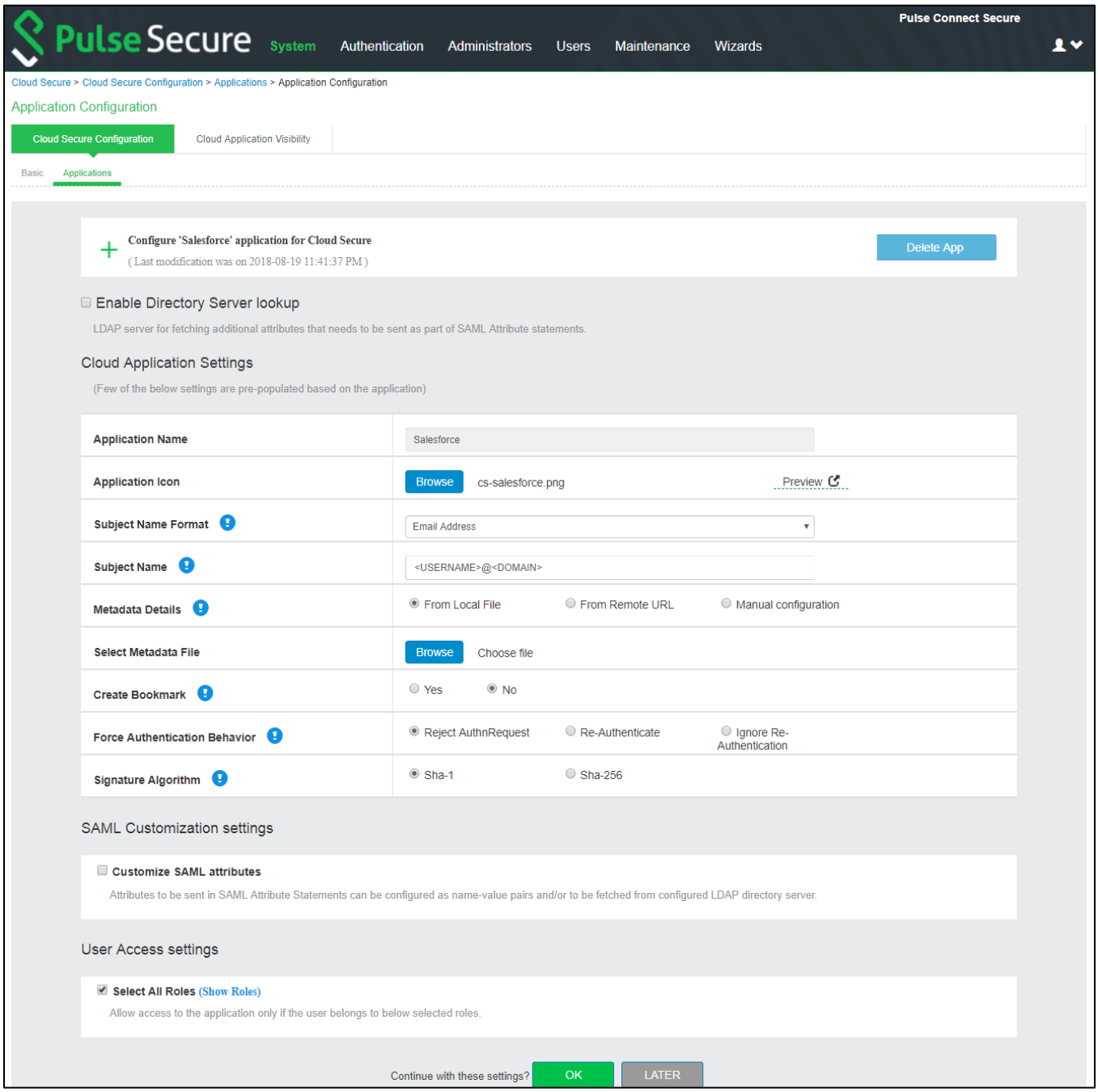
The Admin can configure the Salesforce Cloud Applications as Peer SP once the basic configurations are completed. The Salesforce application is available with some pre-populated application settings for ease of configuration.



To configure Salesforce application:

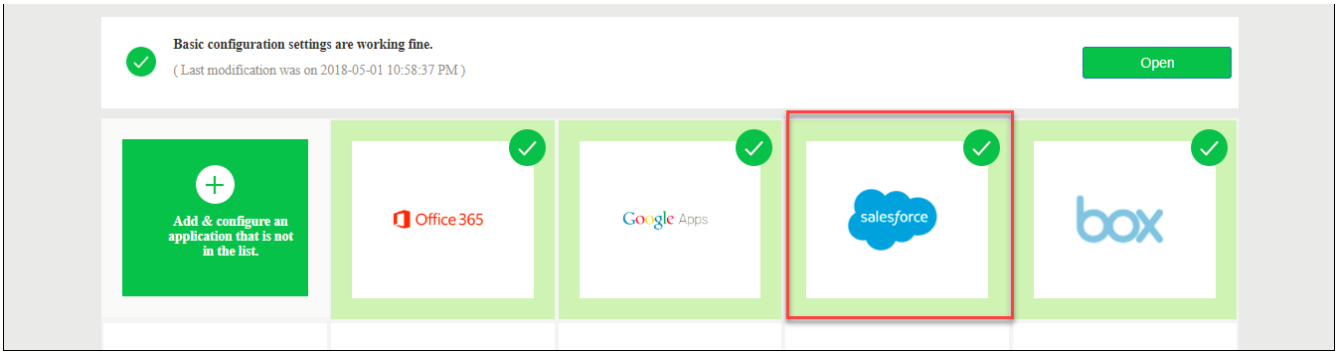
1. Click the **salesforce** icon to configure the application.
2. Under Cloud Application Settings:
   a. Enter the application name.
   b. Click Browse and select the application icon.
   c. Select the Subject Name Format =Email Address.
   d. Enter the Subject Name.
   e. Provide the metadata details.
   f. (Optional) Set **Create Bookmark** to **Yes** to support IdP initiated SSO.
   g. Set the Force Authentication Behaviour to **Reject AuthnRequest**.
   h. Set the Signature Algorithm to Sha-1 or Sha-256.
3. Under **User Access settings**, assign the application to applicable roles.
4. Click **OK**.

Figure 1 Salesforce Configuration



The following screen with a green tick mark on the Salesforce application is displayed after a successful configuration.

Figure 2 Salesforce Configuration Completed



Salesforce Configuration

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

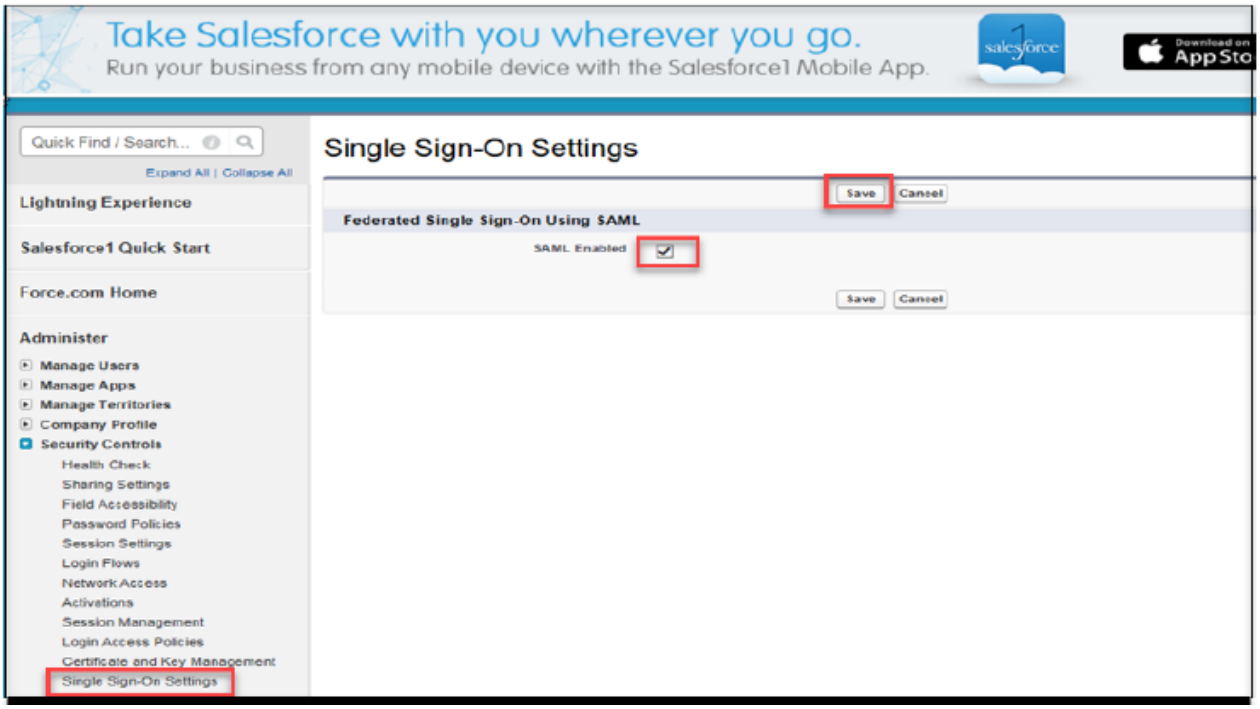
- Admin account
- Register Domain
- SAML configurations
- Users

Steps to Configure

To configure Salesforce as Service Provider, do the following:

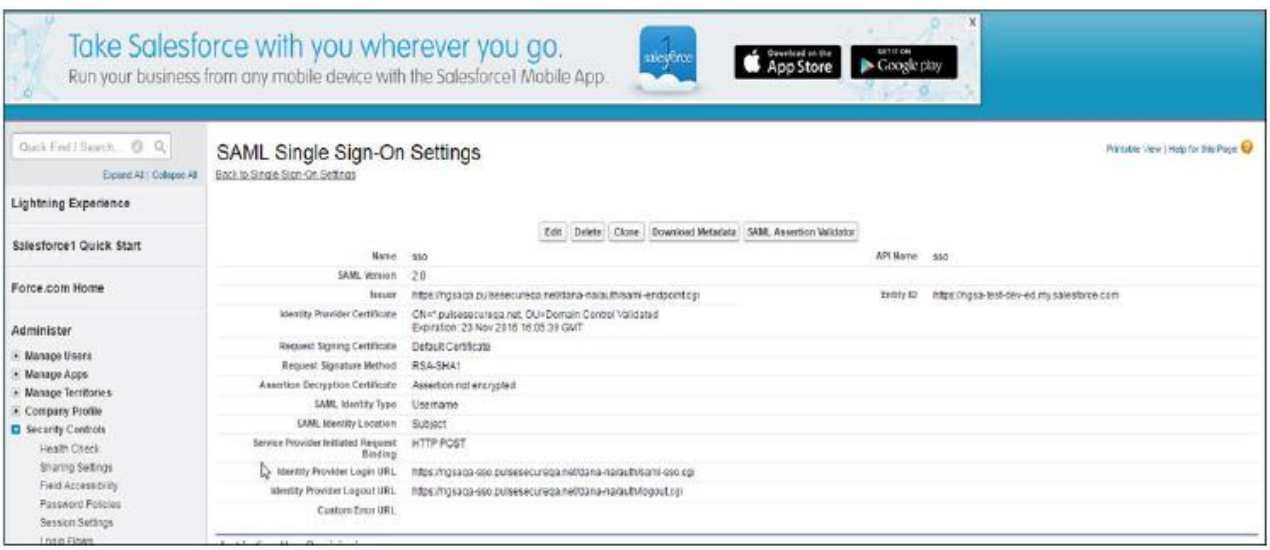
1. Sign up for a new Salesforce account. Register a new Salesforce domain.
2. Once domain is registered, log in to the domain (Example: cloudsecure-dev-ed.my.salesforce.com). Click **Setup** located on top right corner of the page.
3. Navigate to Security Controls-> Single Sign-On Settings on the left panel. Click on 'Edit', check 'SAML Enabled' and click 'Save'.

Figure 3 Enable SAML



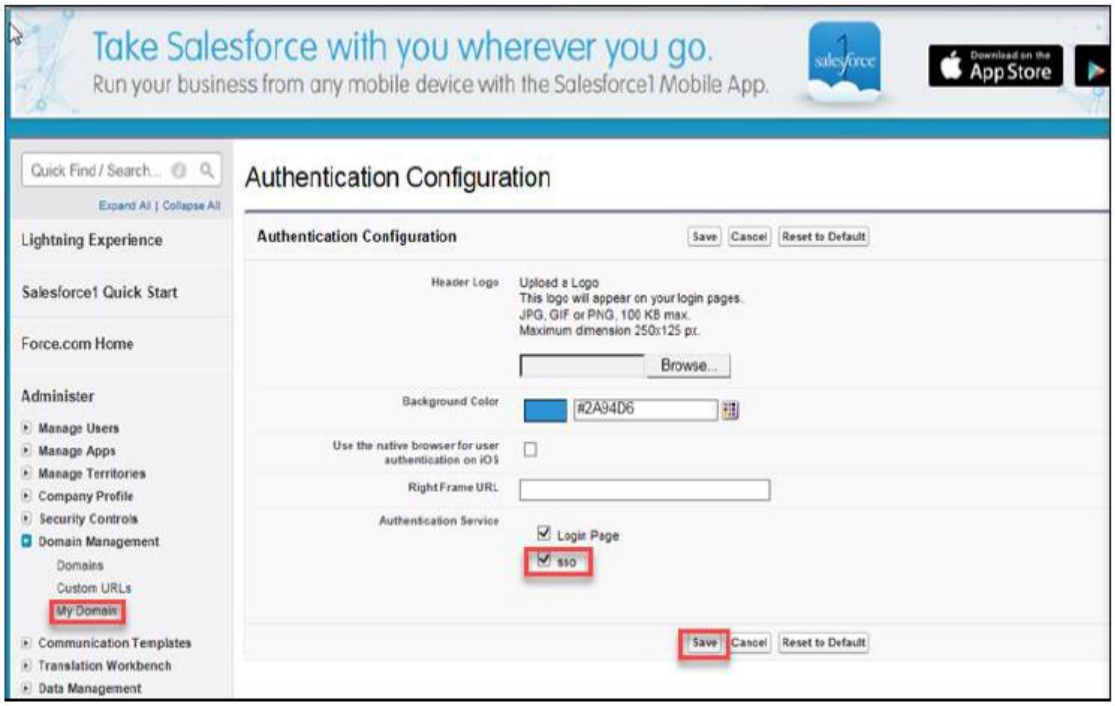
4. Navigate to **Security Controls > Single Sign-On Settings**.
5. Click **New** under **SAML Single Sign-On Settings**. Enter the following details:
   a. Name: <Name>
   b. API Name: <Name>
   c. Issuer: https://<Host FQDN for SAML>/dana-na/auth/saml-endpoint.cgi
   d. Entity ID: <Salesforce Domain>; Example: 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
   h. Leave rest of the fields with default values and click **Save**.

Figure 4 Configure Service Provider



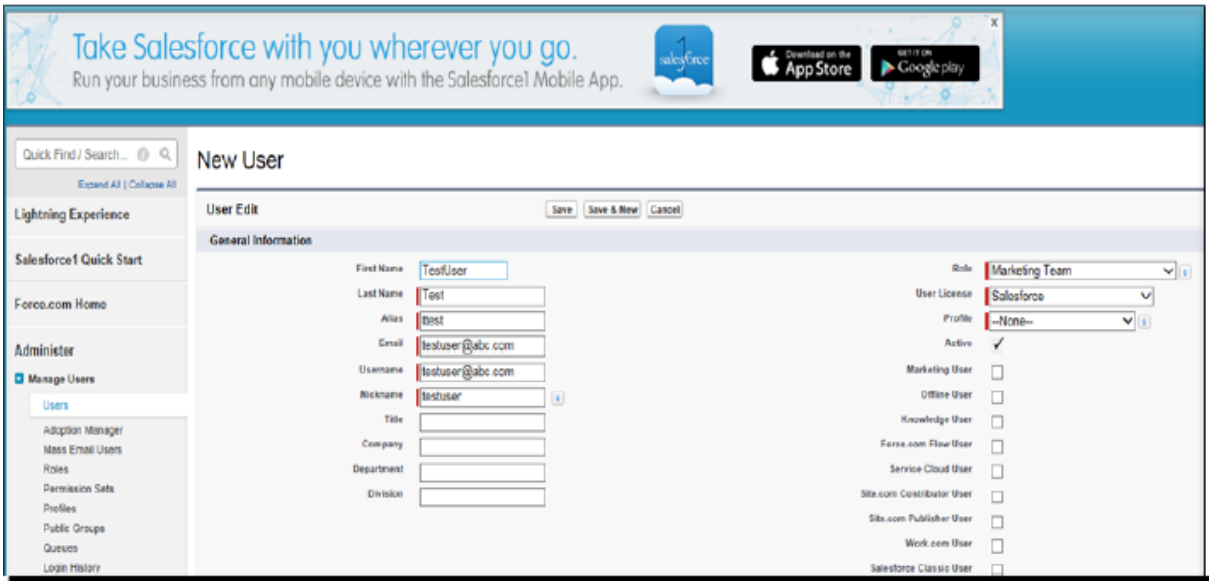
6. Navigate to **Domain Management > My Domain** on the left panel. Click **Edit** under the Authentication Configuration section, check '<Name>' (configured in Step 4a) and click **Save**.

Figure 5 Authentication Configuration



7. Navigate to **Security Controls > Single Sign-On Settings**. Click **Download Metadata** and save the metadata xml file.
8. Navigate to **Administer > Manage Users > Users**. Click **New User** to create a new Salesforce user if user does not exist. Provide the 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 1 Create User



End-User Flow on Mobile Devices

Once the administrator completes the Salesforce configurations and creates a new user in Pulse Workspace, user has to follow the 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 the 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 Common Domain** link in the Salesforce application and provide the Salesforce URL details (Example: **cloudsecure-dev-ed.my.salesforce.com**).
8. Click the **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 the administrator completes the Salesforce configurations, user can access Salesforce url through browser from Windows/MAC OS X Desktops. Follow the 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 (Example: cloudsecure-dev-ed.my.salesforce.com) and click SSO.
    a. If user has an existing VPN session, 'Re-use existing Pulse Session' will kick in. The 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, then the 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.
- Log in to Salesforce Domain. Navigate to Security Controls > Single Sign-On Settings.
  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.