# Table of Contents

Introduction .................................................................................................................. 5  
  About this Guide ..................................................................................................... 5  
  Cloud Secure Overview ......................................................................................... 5  
  Microsoft Office 365 Overview .............................................................................. 5  

Supported Platforms .................................................................................................. 6  

Prerequisites ................................................................................................................. 6  

Cloud Secure SSO Solution ......................................................................................... 8  
  Understanding SAML and SSO ............................................................................ 8  
  Deployment using Web Browser SSO ................................................................. 9  
  Deployment using ECP ....................................................................................... 10  
  Applications SSO Support Matrix ....................................................................... 11  

End-User Flow ........................................................................................................... 12  
  iOS Mobile (iOS Native Mail Client) ................................................................. 12  
  Android Mobile (Divide Productivity App) ...................................................... 12  
  Microsoft Outlook Application (Android & iOS) ............................................ 12  
  Desktops/Laptops .............................................................................................. 13  

Configurations for Office 365 Deployment ............................................................. 14  
  Configuring Office 365 ....................................................................................... 14  
  Configuring Pulse Connect Secure ................................................................... 16  
    Configuring LDAP Server ............................................................................. 16  
    Enable PCS as SAML IDP Server .................................................................. 19  
    Establish Connection between PCS and MDM ........................................... 23  
    Enable Secure Connectivity between PCS and Pulse Client .................... 25  
    Configure Secure Access from End User Devices ....................................... 26  
    Configure Service Provider on PCS ............................................................ 37  
    Configuring Pulse Workspace ...................................................................... 40  

Third Party MDM Server ......................................................................................... 44  

Troubleshooting ....................................................................................................... 44  
  Troubleshooting TIPS ....................................................................................... 44  

Requesting Technical Support .................................................................................. 45
List of Figures

Figure 1: Secure Sign-on to SaaS ................................................................. 9
Figure 2: Secure Sign-on to Office 365 using ECP ................................................. 10
Figure 3: LDAP Server Settings ........................................................................ 17
Figure 4: Task Guide ............................................................................................ 18
Figure 5: Task Guide Step-1 ................................................................................ 19
Figure 6: Device Certificate .................................................................................. 20
Figure 7: SAML Settings ...................................................................................... 21
Figure 8: Identity Provider ................................................................................... 22
Figure 9: Task Guide – Step 2 ............................................................................. 23
Figure 10: Trusted Client CA ............................................................................... 24
Figure 11: Pulse One Settings ............................................................................. 24
Figure 12: MDM Auth Server ............................................................................... 25
Figure 13: Task Guide – Step 3 ........................................................................... 25
Figure 14: Certificate Server ............................................................................... 26
Figure 15: Task Guide – Step 4 ........................................................................... 26
Figure 16: Configure User Role for L4 VPN ......................................................... 27
Figure 17: SAM Allowed Servers ....................................................................... 28
Figure 18: Configure User Realm ....................................................................... 29
Figure 19: Configure Role Mapping Rules ............................................................ 30
Figure 20: SAM Resource Policy ........................................................................ 31
Figure 21: Cloud Secure Configuration ............................................................... 32
Figure 22: Configure User Role for L3 VPN ......................................................... 33
Figure 23: Split Tunnel Rules .............................................................................. 34
Figure 24: Enable Split Tunneling ....................................................................... 35
Figure 25: Connection Profile ............................................................................. 36
Figure 26: Office 365 Metadata Upload ............................................................... 37
Figure 27: Office 365 Service Provider ............................................................... 39
Figure 28: Registration ......................................................................................... 40
Figure 29: Modify VPN Properties ...................................................................... 41
Figure 30: Modify Active Sync Properties .......................................................... 41
Figure 31: Modify iOS Active Sync Properties ................................................... 42
Figure 32: Edit APP Rule .................................................................................... 42
Figure 33: Publish .............................................................................................. 43
Figure 34: Create New User ................................................................................ 43
Figure 35: VPN Certificate ................................................................................ 43
Introduction

About this Guide
This guide provides information on the deployment, configuration, and administration of Office 365 for seamless access over mobile and desktop devices for Cloud Secure solution. It does not cover information related to third party MDM configurations.

Cloud Secure Overview
Cloud Secure provides secure access to anyone, anytime on a hybrid IT environment where enterprise companies are combining the best of the cloud with their own localized data centers. Cloud Secure supports O365 deployment. It has features such as:

- Single sign-on (SSO), which allows users to use one set of login credentials (for example, name and password) to access multiple applications.
- Inter-operability with third party identity and access management (IAM) vendors for added service flexibility.
- Endpoint compliance to ensure a good health status of user devices.
- Pulse Workspace to ensure that mobile workers store applications and data in a secure container under enterprise control.

Microsoft Office 365 Overview
Office 365 is Microsoft’s cloud offering which is a cloud version of Microsoft Office software services such as Office, Lync, Yammer, Exchange, and SharePoint. O365 aims to reduce the on-premises footprint previously required to run these services and uses Azure Active Directory service to manage users. Azure Active Directory extends on-premises Active Directory into the cloud, enabling users to use the primary organizational account to not only sign in to the domain-joined devices and company resources, but also the web and SaaS applications.
Supported Platforms

Cloud Secure is supported on the following platforms:

- iOS 9.x onwards
- Android with AFW support (5.1.1 onwards)
- Windows 7, Windows 8, Windows 8.1, and Windows 10
- Mac 10.11 onwards

Prerequisites

Before enabling Cloud Secure Solution for Office 365 deployments, you should have Microsoft subscriptions and few other tools which are outlined below. The following are the minimum requirements needed before deploying Cloud Secure Solution for Office 365.

Few of these components would have been setup already if you have existing Office 365 deployment in your Enterprise. In such case, you just have to enable Single Sign-On settings to get it working.

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Domain registered with Office 365</td>
<td>Office 365 SSO requires an Internet-resolvable domain name to use as the suffix in each user’s username. In Office 365 for business, you can use a custom domain name with your email address. To set up a domain to use with Office 365, you must own a domain and change some of the DNS records for your domain. You can easily buy one from Office 365, or from another domain reseller or registrar. For details on buying a new domain, refer to <a href="https://support.office.com/en-us/article/How-to-buy-a-domain-name-1561140a-16a9-4a02-822d-a989250e479d?ui=en-US&amp;rs=en-US&amp;ad=US">https://support.office.com/en-us/article/How-to-buy-a-domain-name-1561140a-16a9-4a02-822d-a989250e479d?ui=en-US&amp;rs=en-US&amp;ad=US</a></td>
</tr>
<tr>
<td>Windows Local AD/LDAP Server</td>
<td>Local LDAP Server is required to maintain on-premises Active Directory users which are synchronized with Azure Active Directory.</td>
</tr>
<tr>
<td>Windows PowerShell</td>
<td>Remote PowerShell allows you to manage your Exchange Online settings from the command line. You use Windows PowerShell on your local computer to create a remote PowerShell session to Exchange Online. Single sign-on configuration process for hybrid Office 365 requires</td>
</tr>
<tr>
<td>Requirements</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PowerShell to federate to Exchange. PowerShell</td>
<td>Windows PowerShell 3.0 arrives installed, configured, and ready to use on Windows 8, Windows 10 and Windows Server 2012</td>
</tr>
<tr>
<td>Microsoft Online Services Sign-In Assistant for IT Professionals</td>
<td>Microsoft Online Services Sign-In Assistant provides admin the capability to sign in to Microsoft Online Services, such as Office 365. The MOS SIA installs components that allow common applications, such as Microsoft Outlook and Lync, to authenticate to Microsoft Online Services. You can download MOS SIA at <a href="https://www.microsoft.com/en-us/download/details.aspx?id=41950">https://www.microsoft.com/en-us/download/details.aspx?id=41950</a></td>
</tr>
<tr>
<td>Azure Active Directory Module for Windows PowerShell (64-bit version)</td>
<td>Microsoft Azure Active Directory Module for Windows PowerShell is a download for managing your organization's data in Azure AD. This module installs a set of cmdlets to Windows PowerShell; you run those cmdlets to set up single sign-on access to Azure AD and in turn to all of the cloud services you are subscribed to. You can download the module at <a href="http://go.microsoft.com/fwlink/p/?linkid=236297">http://go.microsoft.com/fwlink/p/?linkid=236297</a></td>
</tr>
<tr>
<td>Azure AD Connect for Directory Synchronizations</td>
<td>Directory Synchronization tool is required to synchronize your on-premises Active Directory users to the Azure Active Directory tenant associated with an Office 365 subscription. For procedure to synchronize on-premises AD users to Azure AD, refer to: <a href="https://www.microsoft.com/en-us/download/details.aspx?id=47594">https://www.microsoft.com/en-us/download/details.aspx?id=47594</a></td>
</tr>
<tr>
<td>Directory Synchronization</td>
<td>User accounts should be synchronized between on-premises Active Directory server to Azure Active Directory server for Office 365 SSO. To do directory synchronization refer to: <a href="https://support.office.com/en-us/article/Set-up-directory-synchronization-for-Office-365-1b3b5318-6977-42ed-b5c7-96fa74b08846?ui=en-US&amp;rs=en-US&amp;ad=US">https://support.office.com/en-us/article/Set-up-directory-synchronization-for-Office-365-1b3b5318-6977-42ed-b5c7-96fa74b08846?ui=en-US&amp;rs=en-US&amp;ad=US</a></td>
</tr>
<tr>
<td>Pulse Connect Secure</td>
<td>Pulse Connect Secure (PCS) enables security and controlled access to corporate data and applications for external users. In the Cloud Secure deployments, Pulse Connect Secure acts as SAML Identity Provider for supporting Single Sign-On. Refer to Configuring Pulse Connect Secure for detailed configuration.</td>
</tr>
<tr>
<td>Wild Card/SAN certificate for Office 365 domain</td>
<td>Wild card certificate or Subject Alternative Name certificate is required for the Office 365 domain.</td>
</tr>
</tbody>
</table>

**Note:** It is good to install all the above mentioned Microsoft related components in the same AD/LDAP server used for directory synchronization.
Cloud Secure Single Sign-On Solution

Cloud Secure is designed to provide seamless access to Office 365 users on their mobile and desktop devices. Cloud Secure leverages existing PCS authentication and authorization infrastructure to provide seamless access to Office 365. When user tries to access a Cloud Application, compliance posture of the device is evaluated before providing access. On mobile devices, compliance posture is done based on the attributes information received from MDM server. On desktops, compliance posture is done using the host checker functionality provided by Pulse client. Once authentication and the compliance check of the device completes, access to the resources are provided.

Understanding SAML and SSO

Cloud Secure uses Security Assertion Markup Language (SAML) for exchange of authentication information between Client device (Mobile, Desktops, and other devices), Service Provider (Cloud applications like Office 365, Box etc.) and Identity Provider (Pulse Connect Secure) to provide SSO.

Desktop and mobile client platforms use below mentioned mechanism for SSO.

- **Web Browser SSO**
The web browser SSO comes into picture when the user is accessing the cloud service through a browser on the mobile or desktop. In web browser SSO IDP and SP exchanges SAML messages over user browser. Here the web browser requests for a service from the service provider. As part of authentication flow the service provider requests and receives an identity assertion from the identity provider through the browser. Before providing identity assertion to SP, the IDP requests web user for the credentials to authenticate the web user.

- **Enhanced Client or Proxy**
The Enhanced Client or Proxy (ECP) is similar to web browser SSO but it is designed for applications other than browsers. Here instead of exchanging SAML messages over user’s browser, SP and IDP communicate directly.
Deployment using Web Browser SSO

For web browser SSO, Pulse VPN client on mobile or desktop is used to deliver strong authentication and device compliance check. On mobile devices, cloud applications can be configured with per-app VPN client which is launched automatically when cloud application tries to access cloud service. On desktop, Pulse client may be connected manually by an end user. On mobile devices, users authenticate using certificates to eliminate the need to enter password. For mobile device compliance check, Pulse Workspace or third party MDM servers such as MobileIron or AirWatch is used. Pulse client host checker is used for desktop device's compliance check.

Once authentication and compliance check completes successfully, application data flow directly between the endpoint and the service provider.

*Figure 1: Secure Sign-on to SaaS*
Deployment using Enhanced Client or Proxy Profile

The native outlook applications on mobile devices use ECP, unlike web browser SSO mechanism, for authentication. For ECP, Cloud Secure solution uses the unique token, generated by Pulse Workspace for authentication and to retrieve device compliance details. As part of mobile device registration with Pulse workspace, a unique token gets provisioned to mobile device. Once mobile device gets registered, the native outlook application is automatically provisioned to connect with Office 365 using the username and unique token. This generates a login request to Office 365. Upon receiving a login request, Office 365 delegates the authentication responsibility to PCS by providing user name and unique token through ECP. PCS verifies the user and checks the device compliance through PWS using this unique token. Once authentication and compliance check is successful, PCS provides an assertion to Office 365 which provides an email access to native outlook application.

Note: For Outlook desktop clients prior to Outlook 2013, which support ECP, use AD credentials for authentication

Figure 2: Secure Sign-on to Office 365 using ECP
Applications SSO Support Matrix

The user experience for SSO access is seamless. However, the SSO mechanism used, i.e web browser or ECP, varies based on the platform and the application usage. This section outlines details on the supported mechanism on different client applications.

The SAML web browser SSO is supported on:

- All Browsers (Chrome, Safari, Firefox, Internet Explorer)
- Microsoft applications such as Word, PowerPoint, Excel etc. on desktops and mobiles.
- Microsoft Outlook 2016
- Microsoft Outlook 2013 with a registry update. Refer to Desktop/Laptop section in End-User-Flow for more information on registry update.

The SAML ECP is supported on:

- iOS Native Mail Client
- Divide Productivity application on Android.
- Microsoft Outlook 2013 on desktops.
End-User Flow

End user can access o365 services from both mobile and desktops and flow varies depending on the platform type. User flow for iOS, Android and desktop platforms is listed below.

iOS Mobile (iOS Native Mail Client)

1. User receives a welcome email once admin creates an account in Pulse Workspace.
2. Follow the instructions outlined in the email and register the mobile device.
3. Upon successful registration, user is notified to install the enterprise applications from Pulse Workspace. In addition to this Active Sync and VPN profiles are installed on the client device.
4. Go to Setting > Mail, Contact, Calendars > Accounts and verify that Active Sync Profile is added with required details.
5. Launch the iOS Native Mail client application for accessing the emails using SSO which doesn't require credentials.

Android Mobile (Divide Productivity App)

1. User receives a welcome email once admin creates an account in Pulse Workspace.
2. Follow the instructions outlined in the email and register the mobile device.
3. Upon successful registration, user is notified to install the enterprise applications from Pulse Workspace. In addition to this Active Sync and VPN profiles are installed on the client device.
4. Launch the Divide Productivity Application for accessing the emails using SSO which doesn't require credentials.

Microsoft Outlook Application (Android & iOS)

1. User receives a welcome email once admin creates an account in Pulse Workspace.
2. Follow the instructions outlined in the email and register the mobile device.
3. Upon successful registration, user is notified to install the outlook application from Pulse Workspace. In addition to this, VPN profile gets installed on the client device.
4. Launch the Microsoft Outlook Application. VPN tunnel gets established automatically in iOS whereas in Android user has to manually establish VPN connection from Pulse client. Choose ‘Office 365’ from the list of Email services and input Username. User should get redirected automatically and will be given access to Emails without asing for credentials again.
**Desksops/Laptops**

Cloud Secure requires Microsoft Office 2013 or 2016 client for providing SSO access to emails through modern authentication. In Office 2016 client, Microsoft has added support for modern authentication (for doing web browser SSO) and is enabled by default. Prior to this, earlier versions of outlook client supports only ECP profile for SAML exchange.

Follow below steps for enabling modern authentication in Office 2013 clients on Windows platform:

1. Update Office 2013 client to obtain the update that includes the new Azure Active Directory Authentication Libraries (ADAL) based authentication features.
2. Set the following registry keys.

<table>
<thead>
<tr>
<th>Registry Key</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKCU\SOFTWARE\Microsoft\Office\15.0\Common\Identity\EnableADAL</td>
<td>REG_DWORD</td>
<td>1</td>
</tr>
<tr>
<td>HKCU\SOFTWARE\Microsoft\Office\15.0\Common\Identity\Version</td>
<td>REG_DWORD</td>
<td>1</td>
</tr>
</tbody>
</table>

**Note:** End-Users are usually not recommended to change the registry settings.

Below steps need to be performed once for setting up Outlook client to access emails:

1. Install Pulse Desktop Client and establish VPN connection with PCS.
2. Add email account in Outlook client by navigating to File > Add Account. Provide only the name and email address (without password) and click Next.
3. Outlook client starts searching for server settings and once the details are obtained, new browser windows is opened and gets redirected to PCS login page.
4. Provide user credentials and ‘Sign In’ for authenticating with PCS.
5. After successful authentication with PCS, SAML SSO is triggered and email account gets added to Outlook.

**Note:** End user needs to manually establish VPN connection with PCS before accessing emails through Outlook client.
Configurations for Office 365 Deployment

This section covers the configurations that are involved in the deployment. The admin needs to configure PCS as an Identity Provider, O365 as a Service Provider and PWS to provision and push the profile information on mobile clients.

To support office 365 SSO with Cloud Secure solution, you must complete:

- Configuring Office 365
- Configuring Pulse Connect Secure
- Configuring Pulse Workspace

Configuring Office 365

To enable Single Sign-On on Office 365 Service Provider login to Local Windows AD/LDAP Server (where all the components mentioned in Prerequisites section are installed) and:

1. Open Windows Powershell and execute the command “connect-msolservice” and Provide Microsoft Admin credentials to connect to Microsoft Azure Active Directory.
2. Run the following command to enable SSO for the domain

   ```
   Set-MsolDomainAuthentication -Authentication managed -DomainName <Domain Name>(Ex: pulsesecure.net>)
   ```
3. Execute the following commands in PowerShell Prompt for SSO configuration

   ```
   $dom="<Domain Name>"
   $FedBrandName="<Name>"
   $url=https://< Alternate Host FQDN for SAML>/dana-na/auth/saml-sso.cgi
   $logouturl=https ://< Host FQDN for SAML>/dana-na/auth/logout.cgi
   $issuer = https://<Host FQDN for SAML>/dana-na/auth/saml-endpoint.cgi
   $ecpUrl=https://< Host FQDN for SAML>/dana-ws/samlecp.ws
   $certData=<Domain Certificate Data>
   ```

Note: Domain Certificate Data can be obtained from PCS by navigating to Authentication->Signing In->Sign-in SAML->Metadata Provider and clicking on ‘Download Metadata’. The Certificate content from the downloaded file should be assigned to $certData parameter

4. To verify the SSO configuration run the following command

   Get-MsolDomainFederationSettings -DomainName <Domain Name>

5. To enable modern authentication for Exchange Online, which supports SAML web browser based SSO profile for certain clients such as Outlook 2016 in desktops, execute the following commands:

   a. Run the following command and give Office 365 Admin credentials

      $UserCredential = Get-Credential

      In the Windows PowerShell Credential Request dialog box, type your Office 365 Admin credentials, and then click OK.

   b. Run the following command to provide required connection settings


   c. Run the following command to import the Exchange Online cmdlets into your local Windows PowerShell session

      Import-PSSession $Session

   d. Run the following command to enable modern authentication for Exchange Online

      Set-OrganizationConfig -OAuth2ClientProfileEnabled:$true

   e. Run the following command to verify that change was successful

      Get-OrganizationConfig | ft name, *OAuth*

   f. Be sure to disconnect the remote powershell when you are finished

      Remove-PSSession $Session
Configuring Pulse Connect Secure

PCS should be enabled as SAML Identity Provider for supporting Single Sign-On. Configuring PCS as an identity provider comprises the below settings:

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

Steps to Configure

1. Login to Pulse Connect Secure admin console
2. Select System > Network and configure Internal port and External ports on respective tabs. Verify that the configured external IP address is reachable

Note: Pulse VPN tunnel will be established with External Interface of PCS and users accessing SAML SSO enabled cloud service will be redirected to Internal Interface of PCS for authentication.

3. Select System > Network > Overview and add DNS server if not configured already

Configuring LDAP Server

In hybrid Office365 deployments, User directory is maintained within the enterprise and the same will be synchronized to Azure Active Directory. Directory Synchronization tool is required to synchronize your on-premises Active Directory users to the Azure Active Directory tenant associated with an Office 365 subscription

4. Select Authentication > Auth. Servers, select New server of type ‘LDAP Server’ and click New Server. Configure LDAP server with following details:

   a. Enter Name: <name reference for LDAP server>
   b. Enter LDAP Server: <LDAP Server IP>
   c. Select Active Directory under LDAP Server Type
   d. Select Authentication required to search LDAP
   e. Enter Admin DN: cn=<admin user>,cn=users,dc=<domain>
f. Enter Admin Password.

g. Enter Base DN and Filter details: `dc=<domain>, dc=<domain>`

h. Save Changes

i. Click Test Connection to check if LDAP server is reachable.

*Figure 3: LDAP Server Settings*
**Note:** You must create user accounts in local LDAP Server (provide email address in email field while creating user) and perform a directory synchronization to sync the users with Azure Active Directory.

5. Navigate to **System > Cloud Secure > Cloud Secure Configuration**. Click ‘Guidance > Task Guide Index > Cloud Secure Configuration’. Task Guide with different steps involved in configuring Cloud Secure appears on the right side of the page. Follow steps mentioned in each section below.

*Figure 4: Task Guide*
Enable PCS as SAML IDP Server

In the Task Guide, click on the first step ‘Enable PCS as SAML IDP server’ as shown in Figure 4. List of all steps required to configure PCS as SAML IDP server will be displayed

Figure 5: Task Guide Step-1

6. Click **System > Configuration > Certificate > Device Certificate** under Step 1 as shown in Figure 5 to import IDP device certificate. Admin will be redirected to Device Certificates page. Import wildcard or Subject Alternative Name (SAN) device certificate that will be used for signing SAML messages sent by the PCS. Disassociate External Port if used by any other certificate and map it to the imported device certificate.
7. Click **System > Configuration > SAML > Settings** under Step 2 as shown in *Figure 5* to configure SAML Settings. Admin will be redirected to the SAML Settings page. Configure the following details:
   a. Enter **Host FQDN** for SAML (for example: cs.pulsesecure.net).
   b. Enter **Alternate Host FQDN** for SAML (for example: cs-sso.pulsesecure.net).
   c. Click **Save Changes**.
   d. Click **Update Entity Ids**.

**Note:** Host FQDN for SAML is DNS Host name for External Port IP and Alternate Host FQDN for SAML is DNS Host name for Internal Port which is configured in **Step 2** above. Alternate Host FQDN for SAML is used to redirect user to IDP login URL provided in Service Provider.
8. Click **Authentication > Signing In > Sign-in SAML > Identity Provider** under Step 3 as shown in Figure 5 to configure Identity Provider. Admin will be redirected to Identity Provider configuration page. Configure the following details:

   a. Enable 'Post' binding

   b. Select the device certificate uploaded in Step a. above as **Signing Certificate**

   c. Enable 'Reuse Existing NC(Pulse) Session' and 'Accept Unsigned AuthnRequest'.

   d. Select **SignIn Policy** used to authenticate the user (Example: */).

   e. Under User Identity, select Email Address as **Subject Name format** and provide **Subject Name** as `<USERNAME>@<DOMAIN>`

      (Example: `<USERNAME>@pulsesecure.net`)

   f. Click **Save Changes**

---

**Note:** Subject Name is used to identify a specific user in the Service Provider. Most of the Service Providers use 'Email Address' as the NameIdentifier. So in the Basic Identity Provider Configuration section, Subject Name Format is configured as 'Email Address'. In case of Microsoft Office 365 SP specific configuration, the Subject Name Format should be configured as 'Persistent' and Subject Name should be `<OBJECTGUID>`
Figure 8: Identity Provider

- **Basic Identity Provider (IdP) Configuration (Published in Metadata)**
  - Protocol Binding to use for SAML Response: Post
  - Signing Certificate: *pulsesecurega.net*
  - Decryption Certificate: No Encryption

- **Other Configurations**
  - Reuse Existing NC (Pulse) Session
  - Accept unsigned AuthnRequest

- **Service-Provider-related IdP Configuration**
  - The following settings apply to all Service Providers by default. Can be overridden in Peer SP configuration:
    - **Session Lifetime:**
      - None
      - Role Based
      - Customized
    - **SignIn Policy:**
      - By
    - **Force Authentication Behavior:**
      - Reject AuthnRequest
      - Re-Authenticate User
  - **User Identity**
    - **Subject Name Format:** Email Address
    - **Subject Name:** <USERNAME>@pulsesecure.net

- **Attribute Statement Configuration**
  - Attributes to be sent in SAML Attribute Statements can be configured as name-value pairs and/or to be fetched from a Directory server.
  - Name-Value based configuration, here values can be system variables available in SSO parameter fields:

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Friendly Name</th>
<th>Attribute Value</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Single-Valued</td>
</tr>
</tbody>
</table>

- **Directory server based configuration:**
  - Directory Server: None
Establish Connection between PCS and MDM

To establish connection between PCS and MDM:

Click ‘Return to the previous guide’ in the Task Guide. Click Step 2 ‘Establish Connection between PCS and MDM’ of Task Guide as shown in Figure 4. List of all steps required to establish connection between PCS and MDM Server will be displayed.

9. Click System > Configuration > Certificates > Trusted Client CAs under Step 1 as shown in Figure 9 to import Pulse One VPN Certificate. Admin will be redirected to Trusted Client CAs page. Click on ‘Import CA Certificate...’, browse to the Pulse Workspace VPN Certificate downloaded in Step 10 of Pulse Workspace Configuration and click ‘Import Certificate’.
10. Click System > Configuration > Pulse One > Settings under Step 2 as shown in Figure 9 to register PCS with Pulse One.
   a. Enter Registration Host and Registration Code details from Step 2 of Pulse Workspace Configuration.
   b. Click Save Changes.
   c. Registration Status and Notification Channel Status under Status Information section should turn green after few seconds.

11. Click Authentication > Auth Servers under Step 2 as shown in Figure 9 to create Pulse Workspace MDM Authentication Server. Select New Server of Type ‘MDM Server’. Click New Server
   a. Enter Name.
   b. Select ‘Pulse Workspace’.
   c. Click Save Changes.

Note: MobileIron and AirWatch Third-Party MDM Servers can also be used as device attribute servers on user realm for device compliance checks.
Enable Secure Connectivity between PCS and Pulse Client

To enable secure connectivity between PCS and Pulse Client:

Click ‘Return to the previous guide’ in the Task Guide. Click the third Step ‘Enable secure connectivity between PCS and Pulse Client’ of Task Guide as shown in Figure 4. List of all steps required to enable secure connection between PCS and Pulse Client will be displayed.

12. Click Authentication > Auth Servers under Step 1 as shown in Figure 13 to configure Certificate Authentication Server. Select New Server of Type ‘Certificate Server’ and click New Server.
   a. Enter Name
   b. Click Save Changes
Configure Secure Access from End User Devices

To configure secure access from end user devices:

Click ‘Return to the previous guide’ in the Task Guide. Click the fourth step ‘Configure Secure access from end user devices’ of Task Guide as shown in Figure 4. List of all steps required to configure Pulse Connect Secure to enable end users and to make connection with PCS will be displayed.

Figure 14: Certificate Server

![Certificate Server](image)

Figure 15: Task Guide – Step 4

![Task Guide](image)
13. Click **Users > User Roles** under Step 1 as shown in *Figure 15* to configure user role. Select the desired role or create a new user role and configure following options:

   a. Select **Pulse Secure Client**
   b. Select **Secure Application Manager** and then select **Windows Version for L4/WSAM tunnel** (Applicable to iOS/Desktops).
   c. Click **Save Changes**.
   d. To configure WSAM Split tunneling rules, navigate to **SAM** tab under user role. Click **Add Server** and enter the following details as shown in *Figure 17*
      - Enter **Name** to identify the server
      - Enter **Allowed Server** and **Ports** (Internal Port IP created in **Step 2**. For example, if Internal Port is 1.1.1.1, configure Allowed Servers as 1.1.1.1/32:*)

*Figure 16: Configure User Role for L4 VPN*
14. Click **Users > User Realms** under Step 2 as shown in *Figure 15* to configure user realm. Select the desired realm or create a new user realm, and configure following options:
   a. Select **Certificate Server** created in *Step 12* for Authentication.
   b. Select **Pulse Workspace MDM Server** created in *Step 11* as Device Attribute Server.
   c. Click **Save Changes**.
   d. Navigate to **Role Mapping** tab of the user realm and configure role mapping rules. Create **New Rule** based on Device attribute for managed mobile clients. Create another role mapping rule based on other available options to be applied to Desktop clients. To create rule based on Device Attribute
      - Select Rule based on Device attribute and click **Update**
      - Enter Name
      - Select an Attribute and provide a value
      - Assign required roles
      - Click **Save Changes**
Figure 18: Configure User Realm
Figure 19: Configure Role Mapping Rules

**Note:** Compliance checks with MDM Server is applicable only for mobile devices. For desktops, classic Host Checker functionality can be used for compliance checks. Hence, Device Attribute Server configuration is not applicable for realms used for authenticating Desktop users.

15. Click **Authentication > Signing In > Sign-in Policies** under Step 4 as shown in Figure 15 to configure Sign-in policy. Assign user realm configured in above step to the desired sign-in policy or create a new sign-in policy and map the user realm.

16. Click **Users > Resource Policies > Secure Application Manager Policies** under Step 5 as shown in Figure 15 to configure SAML Resource Access Policy. Click on ‘**New Policy**’ and create a new policy allowing all the resources applicable (Internal Port as configured in **Step 2**), assign required roles and **Save Changes**.
17. Click **Authentication > Signing In > Sign-in SAML > Identity Provider** under Step 6 as shown in Figure 15 to update Sign-in Policy for SAML. Select the Sign-in policy configured in Step 13 as shown in Figure 15.

18. Once all the above configurations are complete, navigate to **System > Cloud Secure > Cloud Secure Configuration** and verify if status of all the sections under Basic Settings is changed to ‘Configured’ and ‘Progress Completed’ bar is 100%.
19. (Optional) To configure L3 VPN instead of L4 VPN, skip Step 13 and follow the below steps:
   a. Navigate to Users > User Roles > <ROLE> or create a new role to configure user role with L3 VPN tunneling. Configure following options
      i. Select Pulse Secure Client.
      ii. Select VPN Tunneling for L3 VPN (Applicable to iOS/Android/Desktops).
      iii. Click Save Changes.
To configure L3 VPN Split tunneling rules, navigate to **Users > Resource Policies > VPN Tunneling > Split-tunneling Networks**. Create a new policy and provide following details:

i. Enter **Name**.
ii. Resources applicable (Internal Port as configured in **Step 2**).
iii. Apply the policy to required Roles.
iv. Click **Save Changes**.
c. Navigate to VPN Tunneling of desired user role and configure following details:
   i. Enable split tunneling mode.
   ii. Select Tunnel Routes.
   iii. Click Save Changes.
d. To configure connection profile, navigate to Users-> Resource Policies-> VPN Tunneling-> Connection Profiles. Create a new connection profile and provide following details:
   i. Enter Name
   ii. Select DHCP Server and provide DHCP Server IP Address or select IPv4 Address Pool and provide the IP pool
   iii. Click Save Changes
Figure 25: Connection Profile
Configure Service Provider on PCS

To configure Microsoft Office 365 Service Provider on PCS:

1. Navigate to Systems > Configuration > SAML.
2. Click New Metadata Provider and then:
   i. Enter the Name
   ii. Click Browse and upload ‘Office 365 metadata’ file
   iii. Enable Accept Unsigned Metadata
   iv. Enable ‘Service Provider’ under Roles.
   v. Click Save Changes

   *Figure 26: Office 365 Metadata Upload*

   ![Office 365 Metadata Configuration](image)

   **Note:** Download the Office 365 metadata from `https://login.microsoftonline.com/<TenantDomainName>/FederationMetadata/2007-06/FederationMetadata.xml`. The `<TenantDomainName>` represents a registered domain name or TenantID GUID of an Azure AD tenant.
3. Select **Authentication > Signing In > Sign-in SAML > Identity Provider.** Click **Add SP** and enter the configurations in New Peer Service Provider page.

   a. Select **Metadata** as Configuration mode
   b. Select Entity Id **urn:federation:MicrosoftOnline**
   c. Select **Override Default Configuration**
   d. Enable **Reuse Existing NC (Pulse) Session** and **Accept unsigned AuthnRequest** options
   e. Select the SignIn Policy used for authentication
   f. Under User Identity, Provide following details:
      - Subject Name Format = **Persistent**
      - Subject Name = `<OBJECTGUID>`
   g. Select **Customize IdP defined Attributes**
   h. Select **LDAP server** created in Step 6 as Directory Server and then enter the Username for Lookup as `<USERNAME>`
   i. Configure **Name Value attribute**: `"IDPEmail : <MAIL>"`. Select the type of the value as ‘Single-Valued’
   j. Create a set of attributes to be fetched from Directory Server: objectguid, mail, employeenumber are commonly used attributes
   k. Assign it to applicable roles
   l. Click **Save Changes**
Figure 27: Office 365 Service Provider
Configuring Pulse Workspace

Pulse Workspace is an MDM solution used for managing mobile devices. Cloud Secure uses Pulse Workspace for providing compliance and SSO access to end users accessing from mobile. PCS need to be registered with Pulse Workspace along with configuring App rules, VPN and Active Sync policies for providing this functionality.

Configuration on Pulse Workspace includes below settings:

- Registering Pulse Connect Secure with Pulse Workspace
- Creation of Workspace policy with the following profile settings
  1. VPN Profile configurations
  2. Active Sync Profile configurations
  3. Application profile
- Creation of an User and associating workspace policy to user

Follow below steps for configuring Pulse Workspace:

1. Login to the Pulse One as admin.

2. Select **Appliances > Add Appliance** and enter the appliance name and click **Save**. The registration page appears with Registration host and code, which should be configured in PCS for successful registration of Appliance.

   ![Figure 28: Registration](image)

3. Select **Policies > Add** to create a new policy.

4. Modify the **VPN properties** to support **Per App VPN**.
   a. Set **Vpn Host** to `<Host FQDN for SAML>`.
   b. Set **Vpn Safari Domains** to `https://<Alternate Host FQDN for SAML>`
   c. Select **VPN Type** to Pulse SSL.

   **Note:** VPN Safari Domains configuration is only required for iOS mobiles
5. Modify the Active Sync properties.
   a. Set **ActiveSync Accept All Certs** to Yes.
   b. Set **ActiveSync Server** to **outlook.office365.com**.
   c. Set **Use Pulse One for authentication (Override Active Sync Server)** to Yes.

---

**Note:** The option ‘Use Pulse One for authentication’ enables Pulse One to push token to the registered mobiles which is used in authenticating the user for Email Access.
6. Modify the iOS ActiveSync properties. Set **iOS Activesync Enabled** to Yes.

![Figure 31: Modify iOS Active Sync Properties](image)

**Note:** iOS Active Settings are applicable only to iOS devices

---

7. Navigate to **iOS app rules/ Android App rule > Add**, to add new application.
   a. Enter the application name on the search list and select to add and Click **Next**.
   b. Click **Save**

**Note:** On App rule settings page, select **Per app VPN** for all configured applications except **Divide Productivity (Android)** application.

![Figure 32: Edit APP Rule](image)
8. Click ‘Publish’  

![Figure 33: Publish](image)

9. Select **Workspaces > Action > Add User** to create a new user and Click **Create**.  

![Figure 34: Create New User](image)

   a. Enter the username, full name, email, phone number, and policy you created in PWS.  
   b. Click **Create**.

10. Click on the Settings gear on the top right corner, click VPN Cert. Click the ‘cert’ link to download Pulse Workspace certificate.  

![Figure 35: VPN Certificate](image)
Third Party MDM Server

Cloud Secure deployment with Web Browser SSO Profile works with Third-party Mobile Device Management (MDM) servers. Cloud Secure supports AirWatch and MobileIron MDM servers. MDM server must be registered and configured as device attribute server on Pulse Connect Secure. It is required to provide device details to Pulse Connect Secure for evaluating the compliance checks for end user devices before allowing access to the resources.

The device attributes of a registered and managed mobile device retrieved from AirWatch or MobileIron can be used in role mapping rules on PCS. It is used to match the user to assign appropriate role and applicable access.

Cloud Secure deployment with ECP Active-Sync profile is supported only through Pulse Workspace and not with Third-party MDM Servers.

Refer to PCS admin guide for configuration details of both AirWatch and MobileIron Third-party MDM Servers:

http://www.pulsesecure.net/techpubs

Troubleshooting

Cloud Secure deployment involves PCS, PWS/MDM, Cloud Service Provider and Pulse Mobile client. Troubleshooting starts with identifying the exact components/devices that might be causing the problem. Hence for troubleshooting any issue below set of logs has to be collected.

- On PCS: Enable the event codes - saml, auth, soap at level “50” and collect debug logs. You can also capture the Policy traces for the specific user.
- On Mobile Client: You can use Send Logs feature for collecting the client logs.
- On Browsers: You can download the SAML tracer plugin and use it to validate the SAML message flows.

Troubleshooting TIPS

1. Check User Access logs to see if SAML ECP response is sent by PCS

2. Check if PCS and O365 SP are in same time zone. NTP Server can also be configured on PCS to resolve time zone issues

3. Possible causes of error **“Cannot Get Mail. The connection to the server failed”** on the Native Mail App but User Access Logs on PCS shows SAML ECP response sent successfully
   - Signing Certificate configured in Basic Identity Provider settings in PCS is different from the certificate configured on O365 SP
   - IDPEmail attribute is not configured in Peer SP configuration on PCS
4. Possible causes of error "**Cannot Get Mail. The connection to the server failed**" on the Native Mail App and User Access Logs on PCS shows error ‘SAML ECP Login : Building of SAML ECP response failed for user <username>’
   - Check if LDAP server details are correct and LDAP server is configured as Directory Server in O365 Peer SP

5. Possible causes of error "**Cannot Get Mail. The connection to the server failed**" on the Native Mail App and User Access Logs on PCS shows error ‘SAML ECP Login : failed for user <username>’
   - Check if the compliance check passed on the user device and user role is assigned to the user

6. If there is an error '**No SP configured with entity ID : urn:federation:MicrosoftOnline**' on user device, check Event logs for similar error message. It implies that PCS is not configured with O365 Peer SP

**Requesting Technical Support**

Technical product support is available through the Pulse Secure Global Support Center (PSGSC). If you have a support contract, then file a ticket with PSGSC.

- Product warranties—for product warranty information, visit [https://www.pulsesecure.net](https://www.pulsesecure.net).