PWS setup

PWS Prerequisites

Connections to MDM services that must be set up prior to installing PWS. The customer only needs to set up the services for device types they want to manage. For example, if they only want to manage iOS devices they do not need to set up an AfW domain.

Applie ID	

https://appleid.apple.com/account

The Apple ID is used to create an MDM certificate that is used to manage iOS devices. This certificate is liked to the Apple ID and must be renewed each year. Because of this the account should be made with a distribution list rather an an individuals email account.

Android for Work Domain	

https://www.google.com/a/signup/?enterprise_product=ANDROID_WORK

The AfW domain must match the users email address domain. For example, the pulse AfW Domain is pulsesecure.net.

Registering PCS Appliance with Pulse One

This is only needed if the customer wants to see the PCS appliance in pulse one, plans to use the PCS EAS proxy or would like to use PWS compliance information in VPN connections.

Name for PCS appliance	

https://mobilespaces.screenstepslive.com/s/PulseOne/m/39781/l/380747-appliance-registration

VPN config

This is only needed if the customer would like to configure VPN connections for their mobile devices, but almost all PWS customers do this.

PCS Version	

If the PCS Version is below 8.1r5 the customer must either upgrade or we need to create a PAC license so the appliance can terminate per-app VPN connections. I don't think this is likely because it's a new appliance, but it may.

Auth Server

Certificate Auth Server name	

Only needed if the customer plans to use cert auth.

MDM Auth Server name	

Only needed if the customer plans to use device info for role assignment. This is recommended because it allows them to block non-compliant devices.

Role Config

User role name	
Enable WSAM	☐ Yes ☐ No

This is required if they will be using an App Proxy typr iOS per-app VPN. The app-proxy iOS per-app VPN does not support UDP and should not be used with apps that require UDP(e.g. Lync)

Enable VPN Tunneling	☐ Yes ☐ No

This is required for Android per-app VPN and iOS L3 VPN connections.

Enable Secure Mail	☐ Yes ☐ No

This should only be enabled if the customer is using the PWS EAS proxy.

Enable Web Bookmarks	☐ Yes ☐ No

Some customers use this to give their end users easy access to internal web sites on mobile devices.

List of Web bookmarks to create	

Realm Config

PWS user realm name	
Primary auth server	

Device attributes: This will be the PWS MDM server if created.

Role mapping rules:

The simplest rule set is to block users who's devices are not compliant(i.e. isCompliant is false) and send all other users to the PWS Role

Signing in Policy

Sign in policy path	

I recommend creating a separate Sign-In policy for PWS.

Access Control

SAM Resources	
VPN Tunneling Resources	

PCS EAS Proxy Config

Secure Mail Virtual Hostname	
Excahnge Server	

This feature requires the appliance be registered with PulseOne and that the appliance be selected as the EAS proxy.

PCS LDAP Config

LDAP auth Server name	
LDAP Server Name/IP	
LDAP port	
Backup LDAP Server Name/IP 1	
Backup LDAP Server Name/IP 2	
Admin DN	
Base DN	

Using an LDAP server is recommended because PWS looks up user attribute information using LDAP when the user account is created. This is also used for policy assignment.

PCS EAS Proxy Config

Android apps	
iOS apps	

Realm Config

EAS policy - If the customer is using the PWS EAS proxy this should match the config there.

VPN policy - This should match the Config created on the PCS appliance.

Password policy - I recommend reviewing this with customers so there are no suprises.

Device security policies - I recommend going over the Root detection actions. These are set to wipe by most customers.