Microsoft Intune Deployment for Mobile Devices

Deployment Guide for Pulse Secure Mobile VPN
Pulse Secure, LLC
2700 Zanker Road, Suite 200
San Jose, CA 95134
www.pulsesecure.net

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.

Microsoft Intune Deployment Guide

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 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
Set Up Mobile Device Groups ..................................................................................................................... 6
Set Up Policies ............................................................................................................................................. 7
  Creating Trusted Certificate Profile (applicable to both Android and iOS devices) ......................................... 7
  Creating PKCS Certificate Profile (applicable to both Android and iOS devices) ........................................ 11
  Creating VPN Profile (applicable to both Android and iOS devices) ......................................................... 15
  Configuring Per App VPN On-Demand (for iOS device) ...................................................................... 18
Launching Intune on Mobile Device ............................................................................................................ 23
# Table of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Deployment Steps</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>Create Group</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>Create Policy</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>Create Trusted Certificate Profile - for Android / iOS Devices</td>
<td>8</td>
</tr>
<tr>
<td>5</td>
<td>Trusted Certificate Profile Details</td>
<td>9</td>
</tr>
<tr>
<td>6</td>
<td>Select Mobile Device Groups to Deploy the Policy</td>
<td>10</td>
</tr>
<tr>
<td>7</td>
<td>Prompt to Deploy the Policy</td>
<td>10</td>
</tr>
<tr>
<td>8</td>
<td>PKCS Certificate Profile – for Android / iOS Devices</td>
<td>11</td>
</tr>
<tr>
<td>9</td>
<td>PKCS Certificate Profile – General Settings</td>
<td>13</td>
</tr>
<tr>
<td>10</td>
<td>PKCS Certificate Profile – Extended Key Usage</td>
<td>13</td>
</tr>
<tr>
<td>11</td>
<td>PKCS Certificate Profile – Select Root Certificate</td>
<td>14</td>
</tr>
<tr>
<td>12</td>
<td>VPN Profile – for Android /iOS Devices</td>
<td>15</td>
</tr>
<tr>
<td>13</td>
<td>VPN Profile – General Settings</td>
<td>16</td>
</tr>
<tr>
<td>14</td>
<td>VPN Profile – VPN Settings</td>
<td>17</td>
</tr>
<tr>
<td>15</td>
<td>Select PKCS Certificate</td>
<td>17</td>
</tr>
<tr>
<td>16</td>
<td>Configure Per App VPN</td>
<td>18</td>
</tr>
<tr>
<td>17</td>
<td>Valid Safari Domain</td>
<td>18</td>
</tr>
<tr>
<td>18</td>
<td>On-demand Rule</td>
<td>19</td>
</tr>
<tr>
<td>19</td>
<td>Add Apps</td>
<td>20</td>
</tr>
<tr>
<td>20</td>
<td>Specify Platform and Location of Software Files</td>
<td>21</td>
</tr>
<tr>
<td>21</td>
<td>Specify VPN Policy</td>
<td>22</td>
</tr>
</tbody>
</table>
Introduction

Microsoft Intune is a cloud-based enterprise mobility management (EMM) service that helps you to enable your workforce to be productive while keeping your corporate data protected.

Using Intune, you can:

- Manage the mobile devices your workforce uses to access company data.
- Manage the mobile apps your workforce uses.
- Protect your company information by helping to control the way your workforce accesses and shares it.
- Ensure mobile devices and apps are compliant with company security requirements.

This guide helps PCS administrators to deploy MS Intune and PCS to work together. For L3 VPN secure access, VPN tunneling should be configured in PCS server. For L4 Per App VPN secure and seamless access, Secure Application Manager should be configured in PCS server.

A high-level overview of the configuration steps needed for Microsoft Intune deployment is shown below.

*Figure 1: Deployment Steps*

<table>
<thead>
<tr>
<th>Step 1: Add Mobile Device Groups (if does not exist)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android Mobile Device Group</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2: Add Policies (for Android and iOS Devices)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted Certificate Profile</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3: Configure Per-app VPN On-Demand (iOS Device)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify Safari Domain URL</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4: Launch Intune on Mobile Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download and Install Pulse Secure App on Mobile Device</td>
</tr>
</tbody>
</table>

*Note:* Ensure you have Intune admin console login credentials.
Set Up Mobile Device Groups

Groups in Intune provide great flexibility for managing the mobile devices and users. You can set up Android / iOS specific mobile device groups based on your organizational requirements.

If the mobile device group does not already exist, then from the Intune admin console:

1. Select the **GROUPS** icon from the left menu options and click **Create Group**.
2. Add a group by giving an appropriate group name and selecting the mobile device option.

*Figure 2: Create Group*

Later when the policies are created, you can deploy them to one or more device groups.
Set Up Policies

Microsoft Intune policies provide settings that help you control the security settings on mobile devices. Using its capability of controlling access to company resources, you can deploy certificates, VPN profiles, and so on.

This section provides detailed procedure to set up following profiles on Android and iOS devices:

- Trusted certificate profile
- PKCS certificate profile
- VPN profile

The section also provides procedure to configure Per App VPN on-demand on iOS devices.

Creating Trusted Certificate Profile (applicable to both Android and iOS devices)

Before proceeding, make sure you have exported the Trusted Root Certification Authorities (CA) certificate as a .cer file from the issuing CA.

To create trusted certificate profile:

1. In the Intune admin console, select the POLICY icon from the left menu options.
2. Click Add Policy.

Figure 3: Create Policy
3. In the Create a New Policy window, from Android (or iOS) list, select **Trusted Certificate Profile** and click **Create Policy**.

*Figure 4: Create Trusted Certificate Profile - for Android / iOS Devices*
4. In the General details, enter a name and description for the policy.
5. Click Import and select the trusted ROOT CA certificate file.

*Figure 5: Trusted Certificate Profile Details*
6. Click **Save Policy**.

7. Select the mobile device groups to deploy the policy and click **OK**.

*Figure 6: Select Mobile Device Groups to Deploy the Policy*

![Figure 6: Select Mobile Device Groups to Deploy the Policy](image)

8. Click **Yes** to deploy the policy to mobile device groups.

*Figure 7: Prompt to Deploy the Policy*

![Figure 7: Prompt to Deploy the Policy](image)

This completes creating trusted certificate profile. This profile will be used when creating PKCS certificate profile.
Creating PKCS Certificate Profile (applicable to both Android and iOS devices)

Before proceeding, make sure you have the following available:

- **Certification authority** - This is the FQDN name of the Enterprise Certificate Authority server.
- **Certification authority name** – This is the common name (CN) of the Certificate Authority.
- **Certificate template name** – template that is used to define the format and content of certificates, to specify which mobile devices can enroll for which types of certificates.

Creating Certificate Template is outside the scope of this document. Before proceeding, the certificate template MUST be created on the Certificate server. To know more about creating a template on the Certificate Server, refer to the Intune documentation.

To create PKCS certificate profile:

1. In the Intune admin console, select the **POLICY** icon.
2. Click **Add Policy**.
3. In the Create a New Policy window, from Android (or iOS) list, select **PKCS (.PFX) Certificate Profile** and click **Create Policy**.

*Figure 8: PKCS Certificate Profile – for Android / iOS Devices*
4. In the General details, enter a name and description for the policy.

5. In the Certificate Settings section, enter the following details:
   - Certification authority
   - Certification authority name
   - Certificate template name
6. Select **Certificate validity period** as per your requirement.

7. Under the Extended Key Usage section, click **Select**. In the Add or edit Extended Key Usage window displayed, select **Client Authentication** and click **OK**.

**Figure 10: PKCS Certificate Profile – Extended Key Usage**
8. Under the Select Root Certification section, click **Select**. In the Select Certificate window displayed, choose **Root certificate**. This is the Trusted Certificate profile name created before; for details, see Creating Trusted Certificate Profile (applicable to both Android and iOS devices).

*Figure 11: PKCS Certificate Profile – Select Root Certificate*

**NOTE**: Leave other fields in the form to the default values.

This completes creating PKCS certificate profile. This profile will be used when creating VPN profile.
Creating VPN Profile (applicable to both Android and iOS devices)

Mobile devices use a VPN connection profile to initiate a connection with the VPN server. Use VPN profiles in Microsoft Intune to deploy VPN settings to mobile devices in your organization, so they can easily and securely connect to the network.

Before proceeding, make sure you have IP address or FQDN name of Pulse Connect Secure (PCS) server that mobile devices will connect to.

To create VPN profile:

1. In the Intune admin console, select the POLICY icon.
2. Click Add Policy.
3. In the Create a New Policy window, from Android (or iOS) list, select VPN Profile.

Figure 12: VPN Profile – for Android /iOS Devices
4. In the General details, enter a name and description for the policy.

*Figure 13: VPN Profile – General Settings*

5. In the VPN settings, enter a name for the connection.

6. From the **Connection type** drop-down list, select **Pulse Secure**.

7. For **VPN server description**, enter the PCS server description.

8. For **Server IP address or FQDN** name, enter the PCS sign-in URL.

9. From the **Authentication method**, drop down list, select **Certificates**.
10. Click **Select** and choose client certificate for authentication. This is the PKCS Certificate profile name created before; for details, see Creating PKCS Certificate Profile (applicable to both Android and iOS devices).

**Figure 15: Select PKCS Certificate**

This completes creating VPN profile.

For L3 VPN, in PCS server navigate to **Users > User Roles > General**. In the Access features section, enable **VPN tunneling**. For more details, refer to the section “Configuring General Role Options” in *Pulse Connect Secure Administration Guide*.

This completes configuration for Android and iOS mobile devices.

For configuration of per app VPN for iOS mobile devices, proceed with the next section, Configuring Per App VPN On-Demand (for iOS device).
Configuring Per App VPN On-Demand (for iOS device)

You can set up on-demand VPN for iOS 8.0 and later devices.

To configure Per App VPN, do the following:

1. Select the Per App VPN check box.

Figure 16: Configure Per App VPN

2. For Safari domain, click Add and enter a valid Safari domain.

Figure 17: Valid Safari Domain
3. For On-demand rule, click **Add** and enter the rule. This is applicable to L3 VOD.

*Figure 18: On-demand Rule*
Adding App for Per App VPN

To add an App for Per App VPN:

1. Select the **Apps** icon from the left menu options and click **Add Apps**.

Figure 19: Add Apps
2. In the Software Setup window, select **Managed iOS App from the App Store** and specify the Pulse Secure app URL. Click **Next** and complete the upload.

*Figure 20: Specify Platform and Location of Software Files*

3. From the Apps list, double-click the app, and click **Manage Deployment** link.

4. In the window that is displayed, click **VPN Profile** and choose the VPN policy.
This completes L4 Per App VPN configuration in Microsoft Intune.

For L4 Per App VPN proxy, in PCS server navigate to Users > User Roles > General. In the Access features section, enable Secure Application Manager (Windows version). For more details, refer to the section “Configuring General Role Options” in Pulse Connect Secure Administration Guide.

In PCS server, configure access control policies (ACLs) by navigating to Users > Resource Policies > SAM > Access Control. For more details, refer to the section “Specifying Application Servers that Users Can Access” in Pulse Connect Secure Administration Guide.
Launching Intune on Mobile Device

On the mobile device, do the following:

1. Download and install Pulse Secure app and Intune company portal app.

   **For Android devices:**

   **For iOS devices:**
   Pulse Secure app: https://itunes.apple.com/in/app/pulse-secure/id945832041?mt=8

2. Launch the Intune app.

3. Click **Sign-In** and enter the user name and password provided to you by your IT administrator.

Intune is ready for use.