Pulse Secure®

Microsoft Intune Deployment for Mobile Devices

Deployment Guide for Pulse Secure Mobile VPN

Product Release	**1.0**
Document	**1.2**
Published	**March 2017**

Pulse Secure, LLC
2700 Zanker Road, Suite 200
San Jose, CA 95134
www.pulsesecure.net

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

Table of Contents

Table of Figures

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.

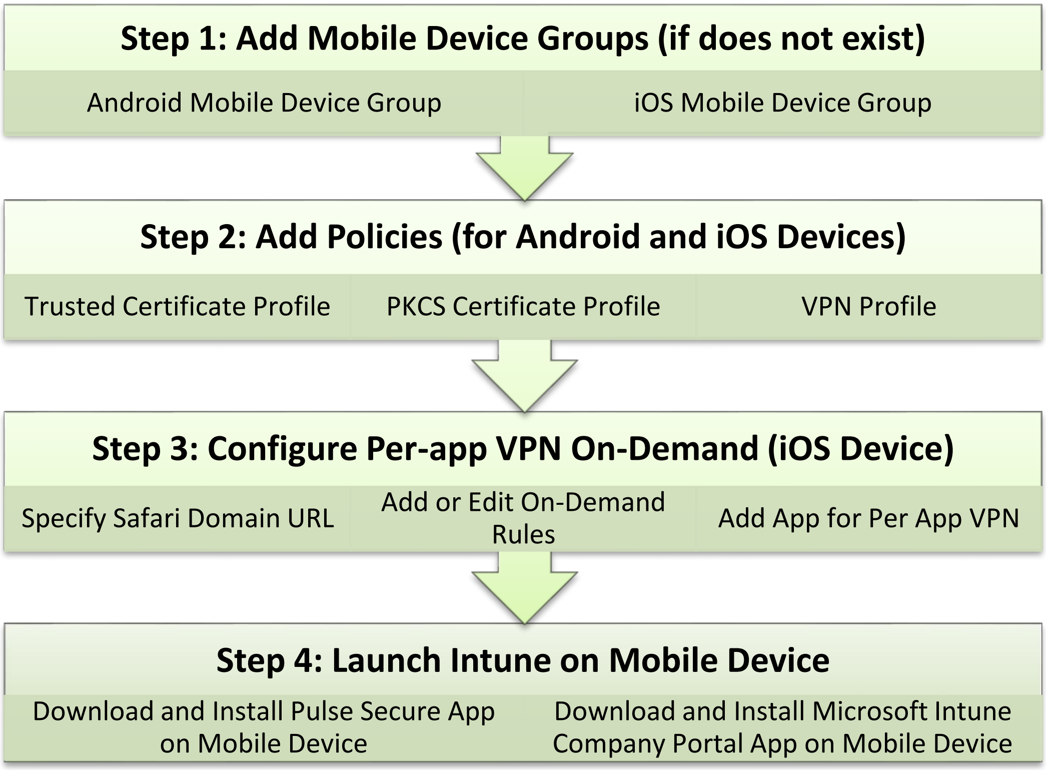
Using Intune, you can:

- 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


Step 1: Add Mobile Device Groups (if does not exist)
Android Mobile Device Group
iOS Mobile Device Group
Step 2: Add Policies (for Android and iOS Devices)
Trusted Certificate Profile
PKCS Certificate Profile
VPN Profile
Step 3: Configure Per-app VPN On-Demand (iOS Device)
Specify Safari Domain URL
Add or Edit On-Demand Rules
Add App for Per App VPN
Step 4: Launch Intune on Mobile Device
Download and Install Pulse Secure App on Mobile Device
Download and Install Microsoft Intune Company Portal App on Mobile Device

Note: Ensure you have Intune admin console login credentials.

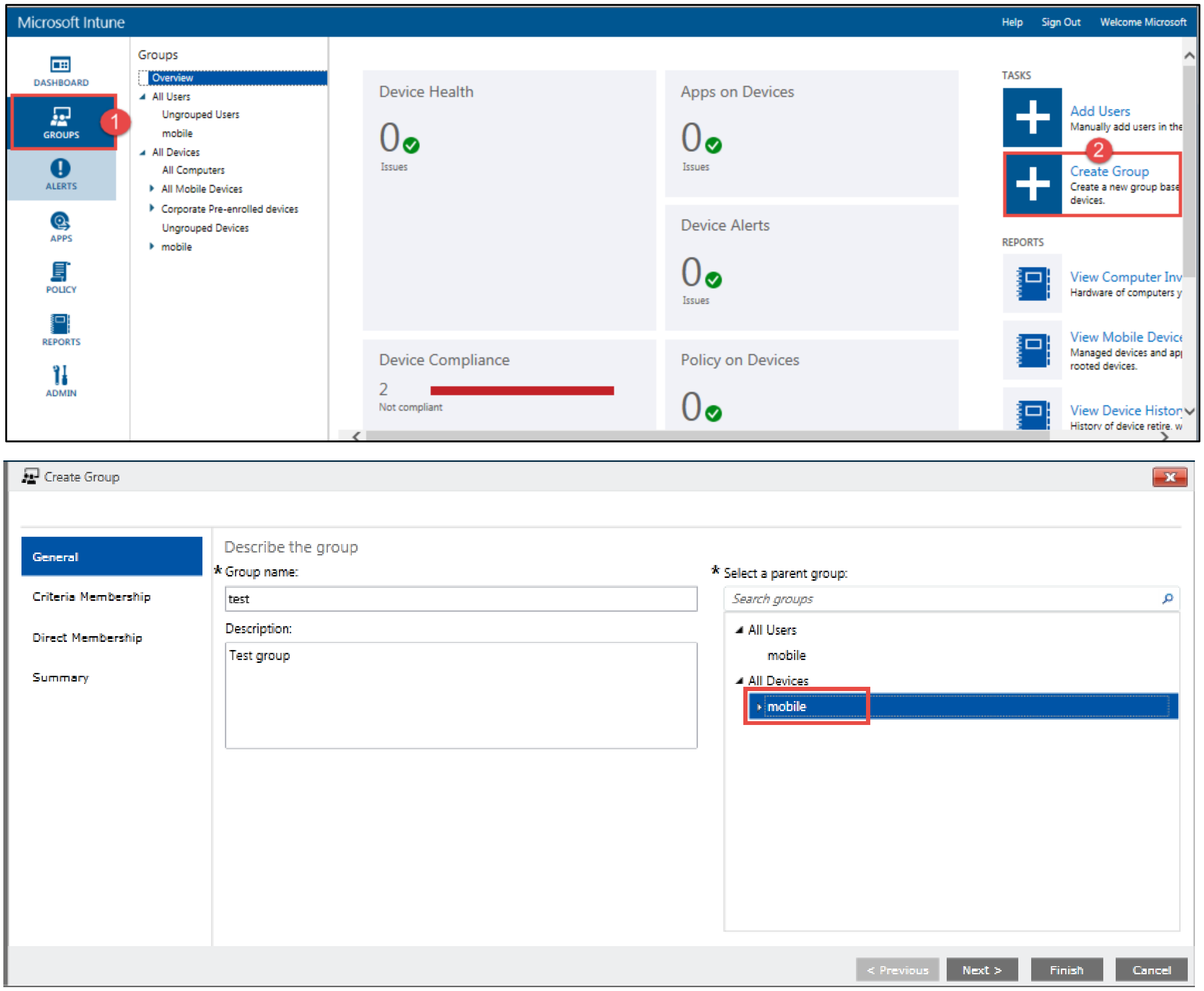
Set Up Mobile Device Groups

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



Describe the group

* Group name: test

Description: Test group

* Select a parent group:

- All Users
  - mobile
- All Devices
  - mobile

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.

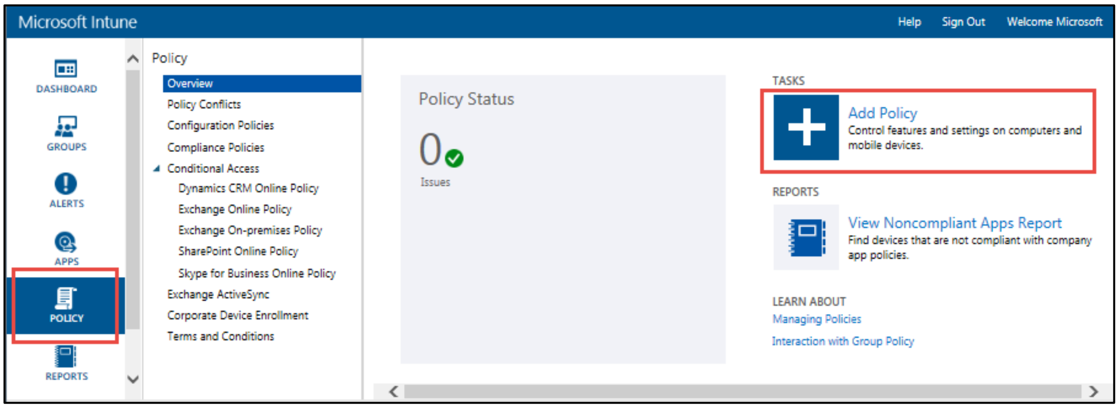
Creating Trusted Certificate Profile (applicable to both Android and iOS devices)

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

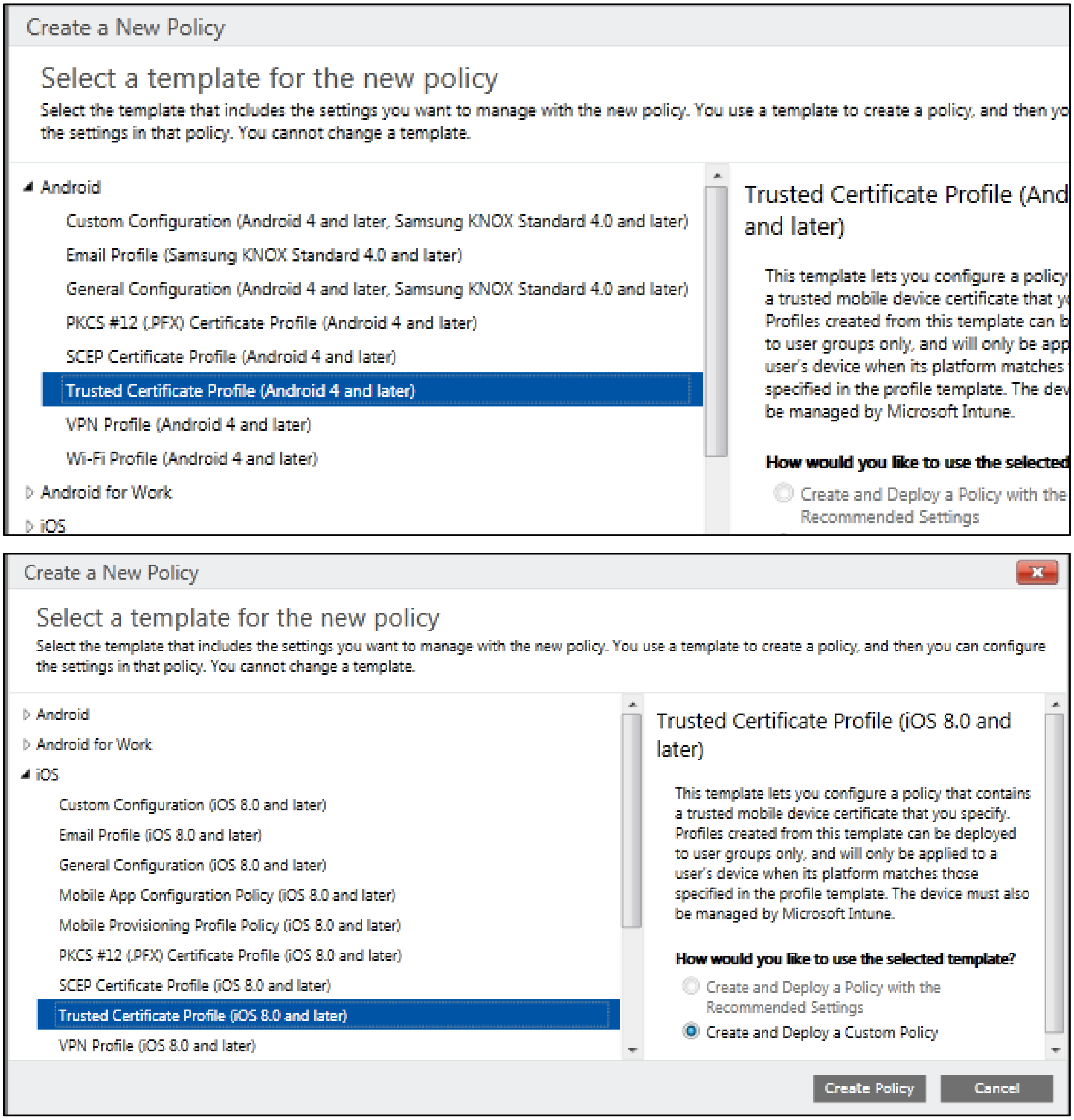


Control features and settings on computers and mobile devices.

Find devices that are not compliant with company app policies.

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



Create a New Policy

Select a template for the new policy

Select the template that includes the settings you want to manage with the new policy. You use a template to create a policy, and then yo the settings in that policy. You cannot change a template.

◢ Android
- Custom Configuration (Android 4 and later, Samsung KNOX Standard 4.0 and later)
- Email Profile (Samsung KNOX Standard 4.0 and later)
- General Configuration (Android 4 and later, Samsung KNOX Standard 4.0 and later)
- PKCS #12 (.PFX) Certificate Profile (Android 4 and later)
- SCEP Certificate Profile (Android 4 and later)
- Trusted Certificate Profile (Android 4 and later)
- VPN Profile (Android 4 and later)
- Wi-Fi Profile (Android 4 and later)

▷ Android for Work

▷ iOS

Trusted Certificate Profile (And and later)

This template lets you configure a policy a trusted mobile device certificate that y Profiles created from this template can b to user groups only, and will only be app user's device when its platform matches specified in the profile template. The dev be managed by Microsoft Intune.

How would you like to use the selected

○ Create and Deploy a Policy with the Recommended Settings

Create a New Policy

Select a template for the new policy

Select the template that includes the settings you want to manage with the new policy. You use a template to create a policy, and then you can configure the settings in that policy. You cannot change a template.

▷ Android

▷ Android for Work

◢ iOS
- Custom Configuration (iOS 8.0 and later)
- Email Profile (iOS 8.0 and later)
- General Configuration (iOS 8.0 and later)
- Mobile App Configuration Policy (iOS 8.0 and later)
- Mobile Provisioning Profile Policy (iOS 8.0 and later)
- PKCS #12 (.PFX) Certificate Profile (iOS 8.0 and later)
- SCEP Certificate Profile (iOS 8.0 and later)
- Trusted Certificate Profile (iOS 8.0 and later)
- VPN Profile (iOS 8.0 and later)

Trusted Certificate Profile (iOS 8.0 and later)

This template lets you configure a policy that contains a trusted mobile device certificate that you specify. Profiles created from this template can be deployed to user groups only, and will only be applied to a user's device when its platform matches those specified in the profile template. The device must also be managed by Microsoft Intune.

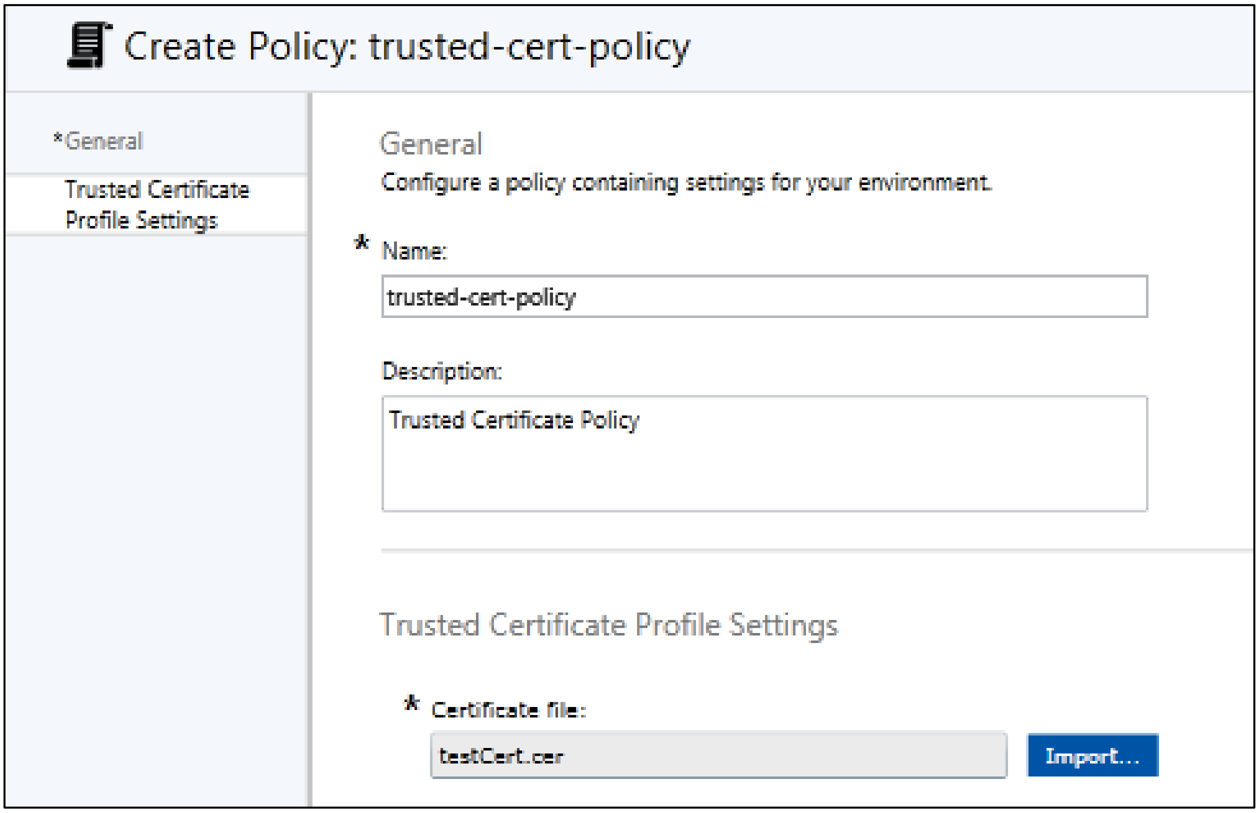
How would you like to use the selected template?

○ Create and Deploy a Policy with the Recommended Settings

● Create and Deploy a Custom Policy

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



Create Policy: trusted-cert-policy

General

Configure a policy containing settings for your environment.

* Name: trusted-cert-policy

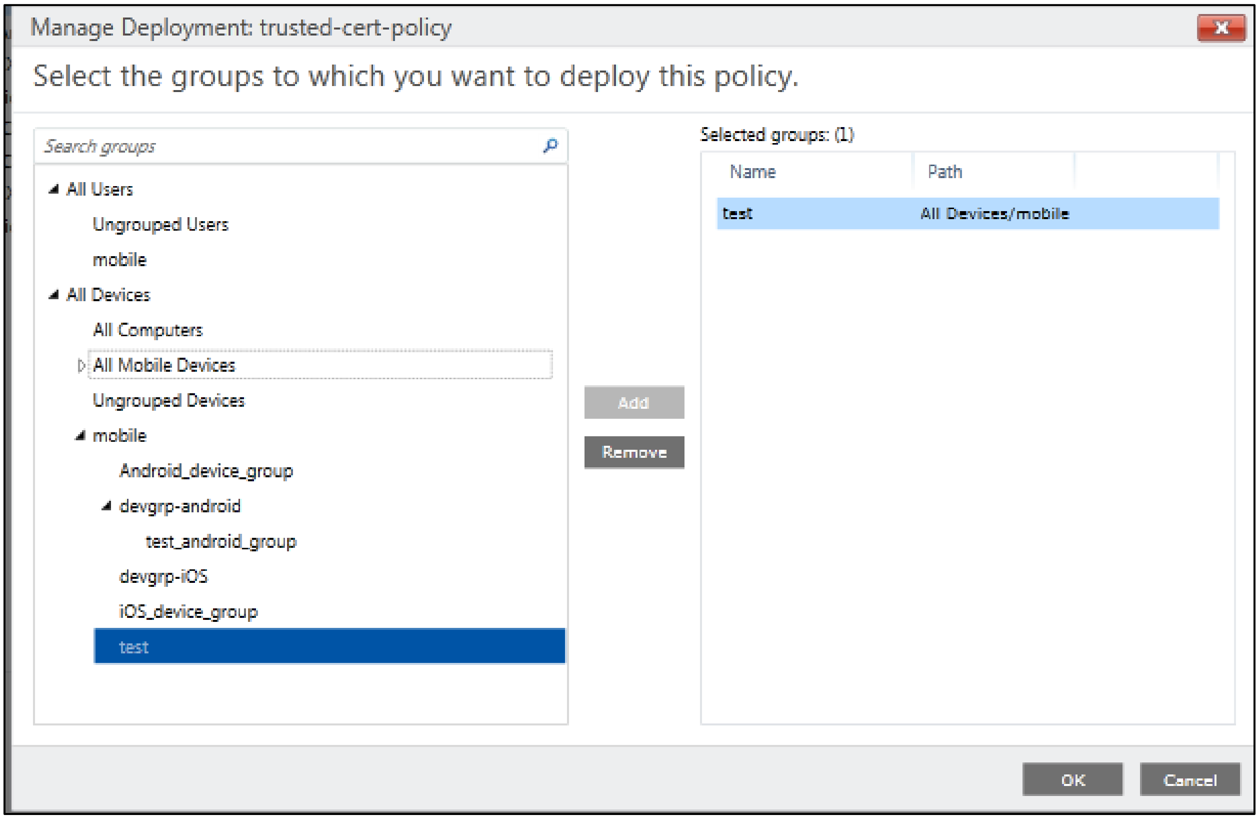
Description: Trusted Certificate Policy

Trusted Certificate Profile Settings

* Certificate file: testCert.cer

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



Manage Deployment: trusted-cert-policy

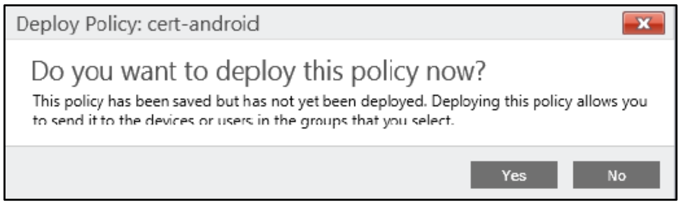
Select the groups to which you want to deploy this policy.

Selected groups: (1)

Name	Path
test	All Devices/mobile

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

Figure 7: Prompt to Deploy the Policy



Deploy Policy: cert-android

Do you want to deploy this policy now?

This policy has been saved but has not yet been deployed. Deploying this policy allows you to send it to the devices or users in the groups that you select.

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:

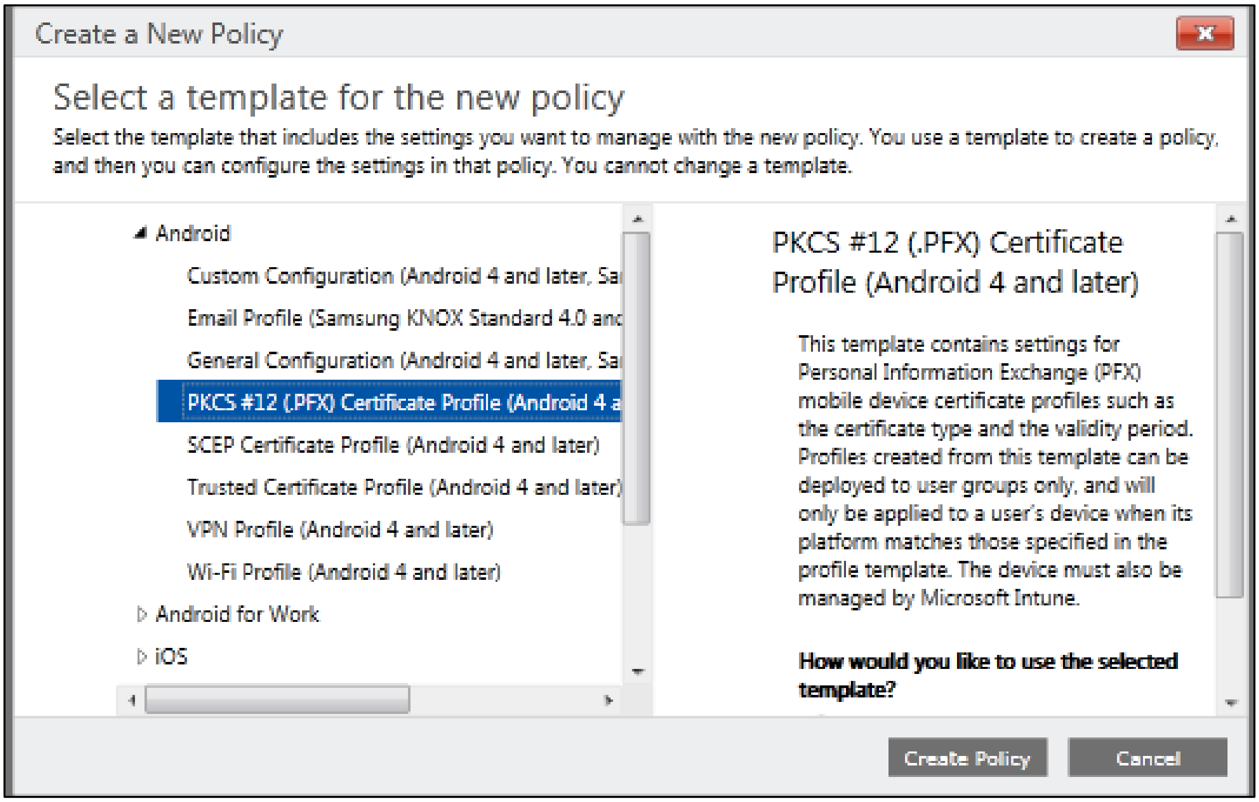
- Certification authority - This is the FQDN name of the Enterprise Certificate Authority server.
- Certification authority name – This is the common name (CN) of the Certificate Authority.
- Certificate template name – template that is used to define the format and content of certificates, to specify 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



Create a New Policy

Select a template for the new policy

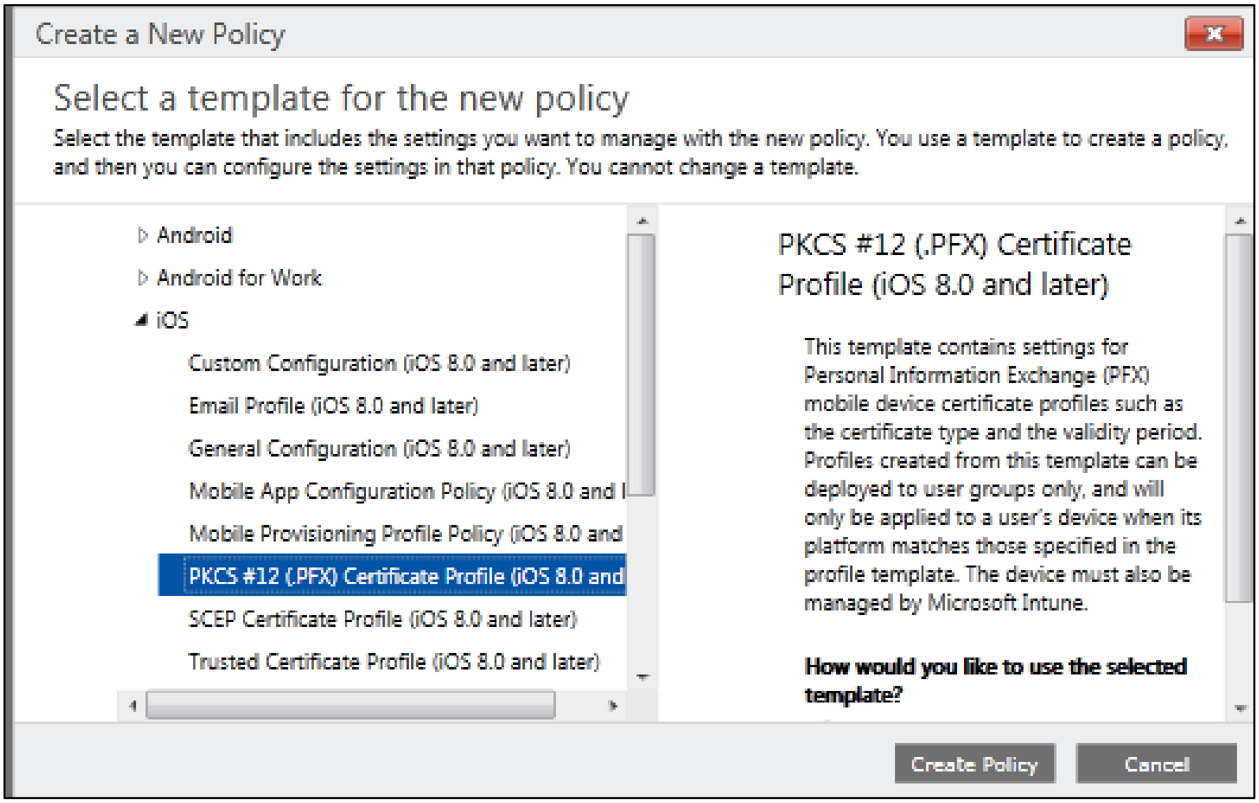
Select the template that includes the settings you want to manage with the new policy. You use a template to create a policy, and then you can configure the settings in that policy. You cannot change a template.

PKCS #12 (.PFX) Certificate Profile (Android 4 and later)

This template contains settings for Personal Information Exchange (PFX) mobile device certificate profiles such as the certificate type and the validity period. Profiles created from this template can be deployed to user groups only, and will only be applied to a user's device when its platform matches those specified in the profile template. The device must also be managed by Microsoft Intune.

How would you like to use the selected template?

Android
Custom Configuration (Android 4 and later, Sa
Email Profile (Samsung KNOX Standard 4.0 anc
General Configuration (Android 4 and later, Sa
PKCS #12 (.PFX) Certificate Profile (Android 4 a
SCEP Certificate Profile (Android 4 and later)
Trusted Certificate Profile (Android 4 and later)
VPN Profile (Android 4 and later)
Wi-Fi Profile (Android 4 and later)
Android for Work
iOS
Create Policy
Cancel



Create a New Policy

Select a template for the new policy

Select the template that includes the settings you want to manage with the new policy. You use a template to create a policy, and then you can configure the settings in that policy. You cannot change a template.

▷ Android
▷ Android for Work
◢ iOS
Custom Configuration (iOS 8.0 and later)
Email Profile (iOS 8.0 and later)
General Configuration (iOS 8.0 and later)
Mobile App Configuration Policy (iOS 8.0 and l
Mobile Provisioning Profile Policy (iOS 8.0 and
PKCS #12 (.PFX) Certificate Profile (iOS 8.0 and
SCEP Certificate Profile (iOS 8.0 and later)
Trusted Certificate Profile (iOS 8.0 and later)

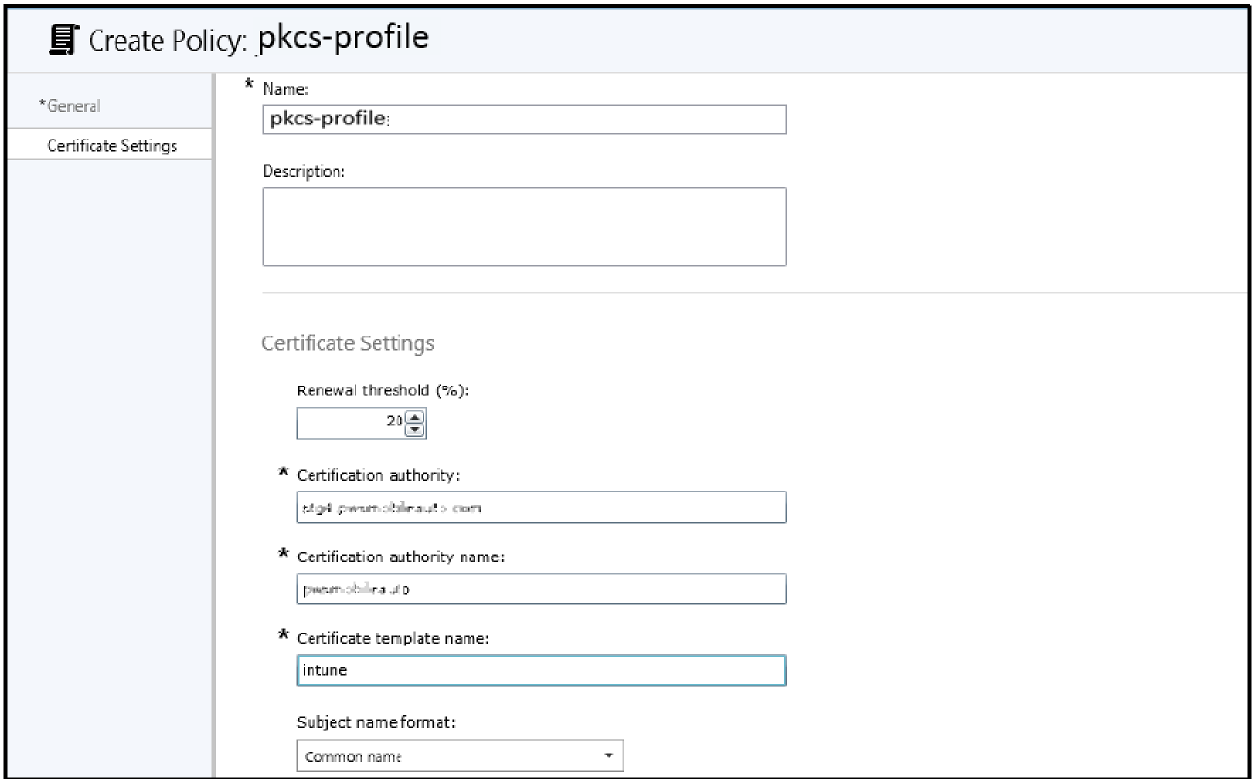
PKCS #12 (.PFX) Certificate Profile (iOS 8.0 and later)

This template contains settings for Personal Information Exchange (PFX) mobile device certificate profiles such as the certificate type and the validity period. Profiles created from this template can be deployed to user groups only, and will only be applied to a user's device when its platform matches those specified in the profile template. The device must also be managed by Microsoft Intune.

How would you like to use the selected template?

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

Figure 9: PKCS Certificate Profile – General Settings



Create Policy: pkcs-profile

* Name: pkcs-profile

Description:

Certificate Settings

Renewal threshold (%): 20

* Certification authority: [redacted]

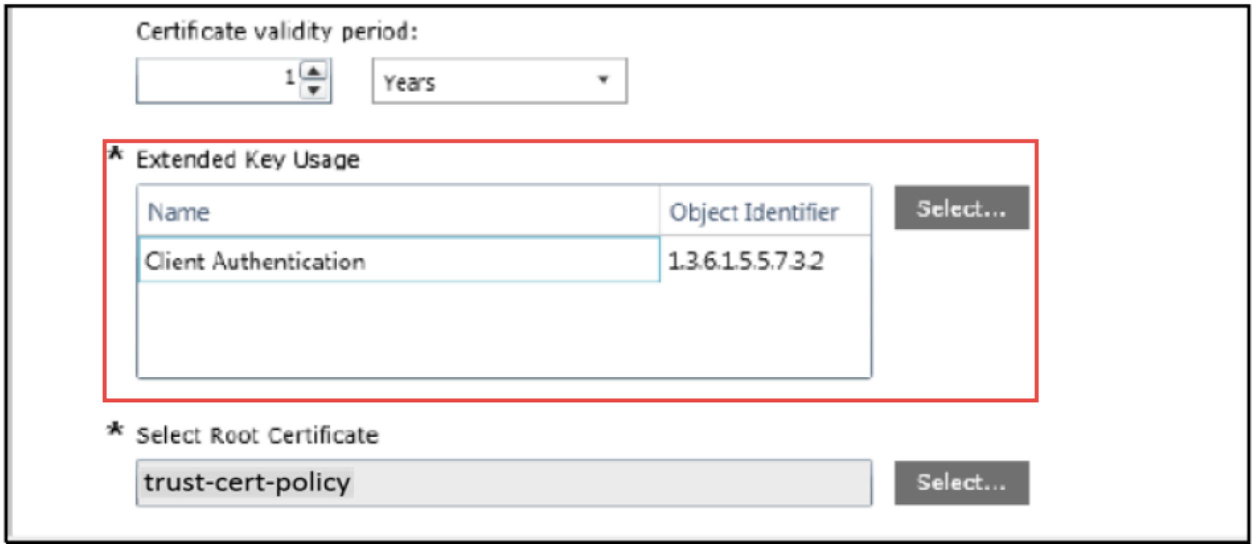
* Certification authority name: [redacted]

* Certificate template name: intune

Subject name format: Common 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



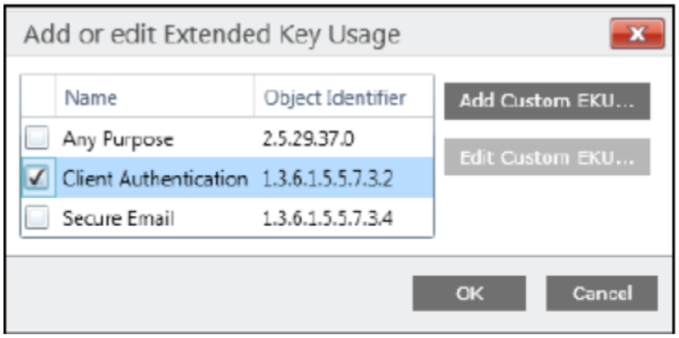
Certificate validity period: 1 Years

* Extended Key Usage

Name	Object Identifier
Client Authentication	1.3.6.1.5.5.7.3.2

* Select Root Certificate

trust-cert-policy

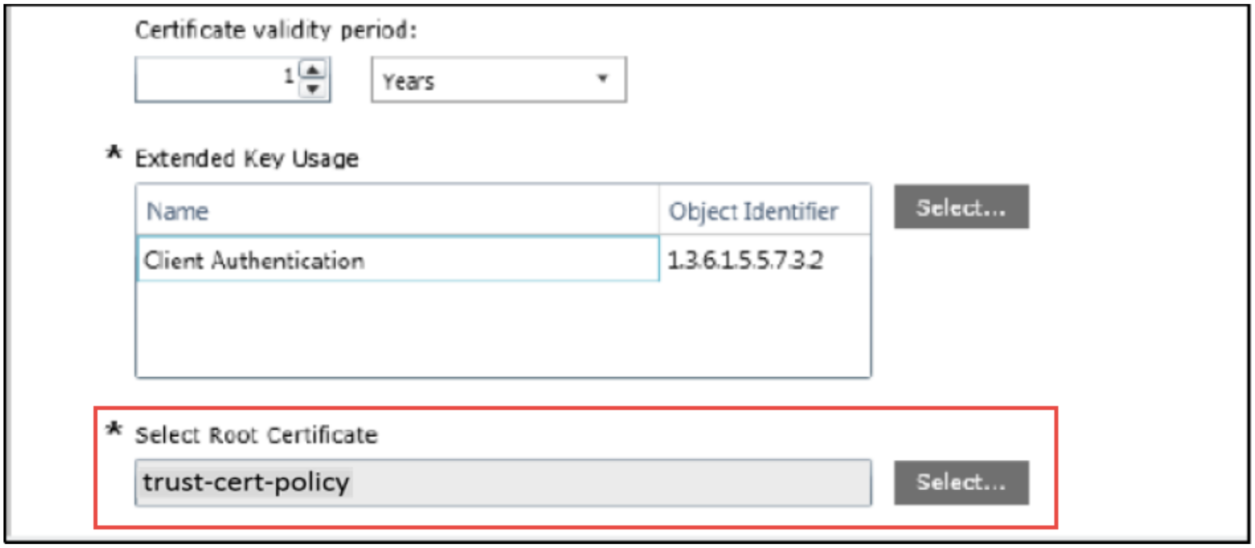


Add or edit Extended Key Usage

	Name	Object Identifier
□	Any Purpose	2.5.29.37.0
☑	Client Authentication	1.3.6.1.5.5.7.3.2
□	Secure Email	1.3.6.1.5.5.7.3.4

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



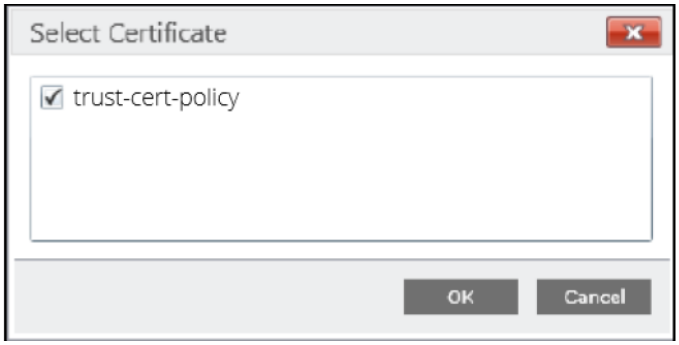
Certificate validity period: 1 Years

* Extended Key Usage

Name	Object Identifier
Client Authentication	1.3.6.1.5.5.7.3.2

* Select Root Certificate

trust-cert-policy



Select Certificate

☑ trust-cert-policy

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)

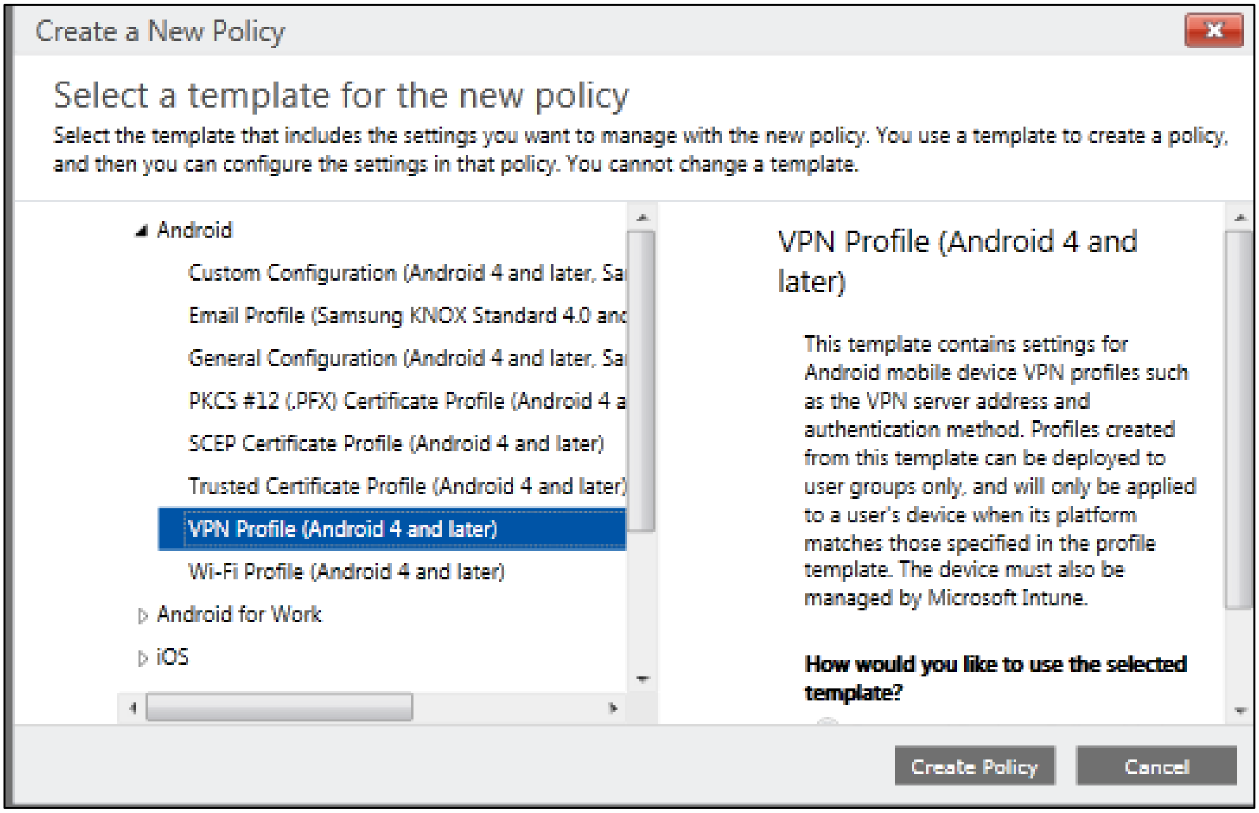
Mobile devices use a VPN connection profile to initiate a connection with the VPN server. Use VPN profiles in Microsoft Intune to deploy VPN settings to mobile devices in your organization, so they can easily and securely connect to the network.

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



Create a New Policy

Select a template for the new policy

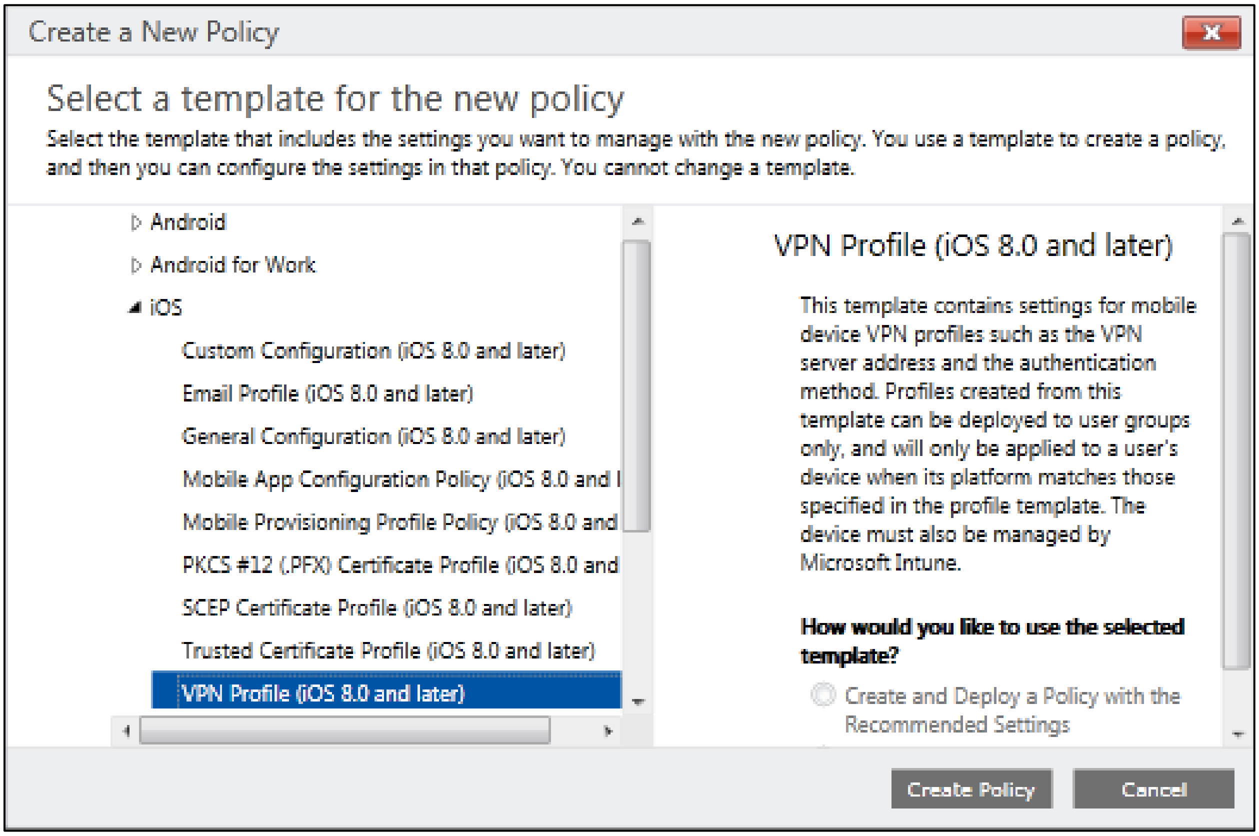
Select the template that includes the settings you want to manage with the new policy. You use a template to create a policy, and then you can configure the settings in that policy. You cannot change a template.

Android
Custom Configuration (Android 4 and later, Sa
Email Profile (Samsung KNOX Standard 4.0 and
General Configuration (Android 4 and later, Sa
PKCS #12 (.PFX) Certificate Profile (Android 4 a
SCEP Certificate Profile (Android 4 and later)
Trusted Certificate Profile (Android 4 and later)
VPN Profile (Android 4 and later)
Wi-Fi Profile (Android 4 and later)
Android for Work
iOS

VPN Profile (Android 4 and later)

This template contains settings for Android mobile device VPN profiles such as the VPN server address and authentication method. Profiles created from this template can be deployed to user groups only, and will only be applied to a user's device when its platform matches those specified in the profile template. The device must also be managed by Microsoft Intune.

How would you like to use the selected template?



Create a New Policy

Select a template for the new policy

Select the template that includes the settings you want to manage with the new policy. You use a template to create a policy, and then you can configure the settings in that policy. You cannot change a template.

▷ Android
▷ Android for Work
◢ iOS
Custom Configuration (iOS 8.0 and later)
Email Profile (iOS 8.0 and later)
General Configuration (iOS 8.0 and later)
Mobile App Configuration Policy (iOS 8.0 and l
Mobile Provisioning Profile Policy (iOS 8.0 and
PKCS #12 (.PFX) Certificate Profile (iOS 8.0 and
SCEP Certificate Profile (iOS 8.0 and later)
Trusted Certificate Profile (iOS 8.0 and later)
VPN Profile (iOS 8.0 and later)

VPN Profile (iOS 8.0 and later)

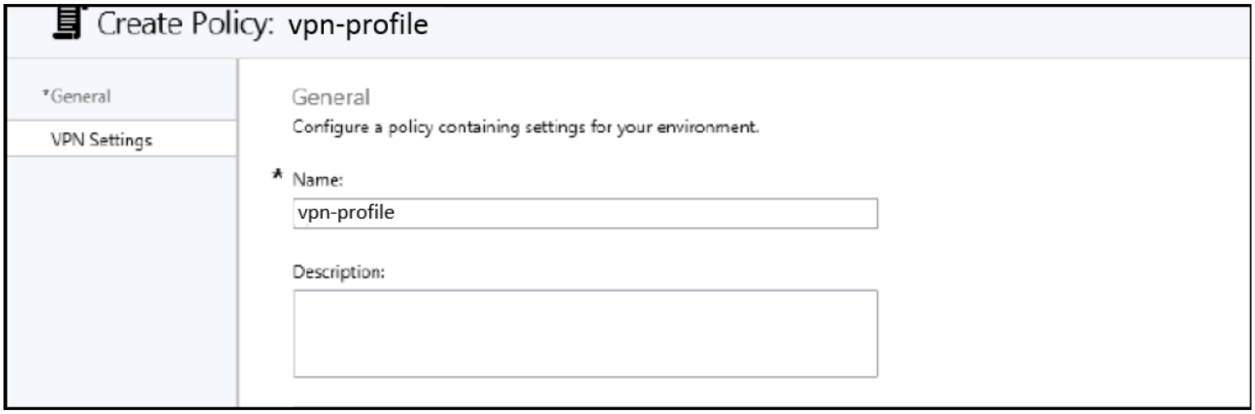
This template contains settings for mobile device VPN profiles such as the VPN server address and the authentication method. Profiles created from this template can be deployed to user groups only, and will only be applied to a user's device when its platform matches those specified in the profile template. The device must also be managed by Microsoft Intune.

How would you like to use the selected template?

○ Create and Deploy a Policy with the Recommended Settings

4. In the General details, enter a name and description for the policy.

Figure 13: VPN Profile – General Settings



Create Policy: vpn-profile

General

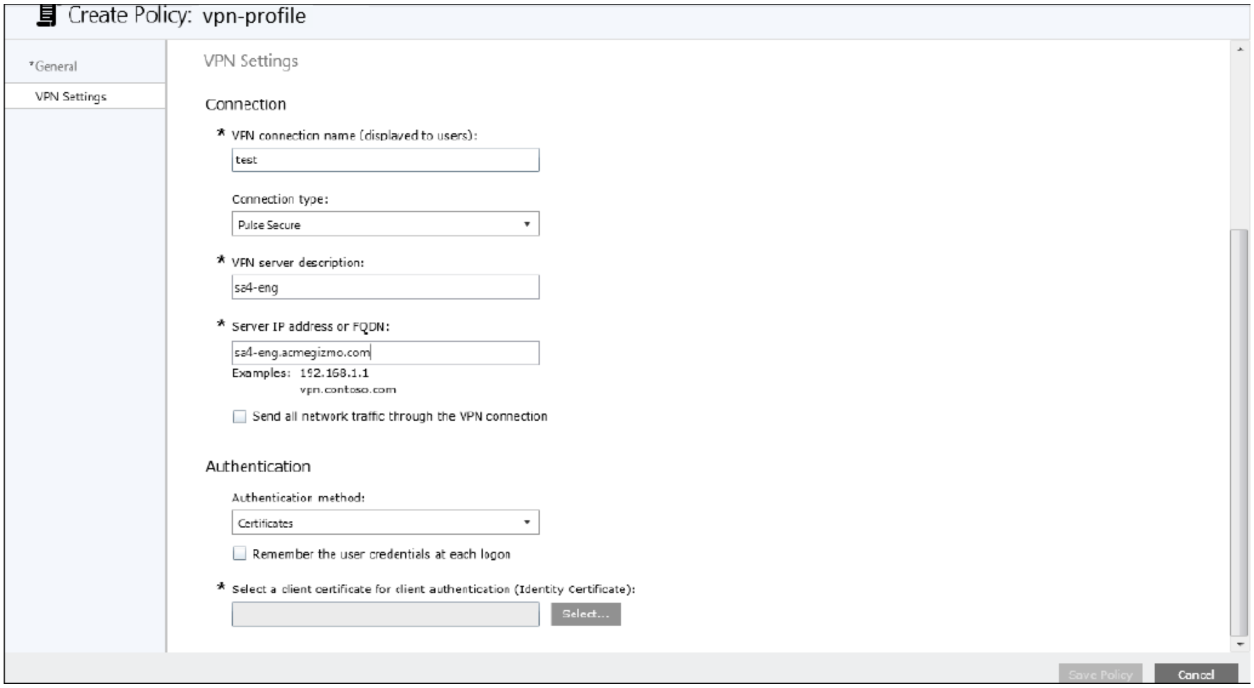
Configure a policy containing settings for your environment.

* Name: vpn-profile

Description:

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.

Figure 14: VPN Profile – VPN Settings



Create Policy: vpn-profile

VPN Settings

Connection

* VPN connection name (displayed to users): test

Connection type: Pulse Secure

* VPN server description: sa4-eng

* Server IP address or FQDN: sa4-eng.acmegizmo.com

Examples: 192.168.1.1
vpn.contoso.com

☐ Send all network traffic through the VPN connection

Authentication

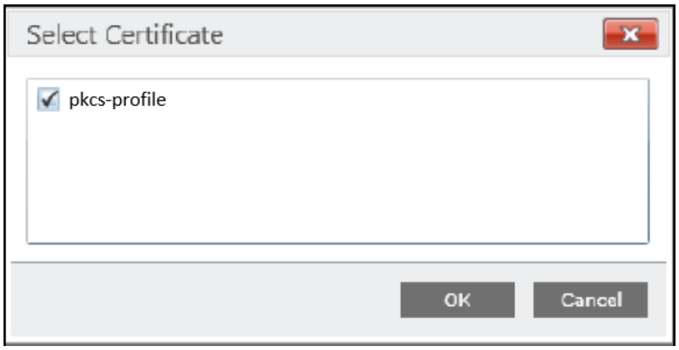
Authentication method: Certificates

☐ Remember the user credentials at each logon

* Select a client certificate for client authentication (Identity Certificate):

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



Select Certificate

☑ pkcs-profile

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).

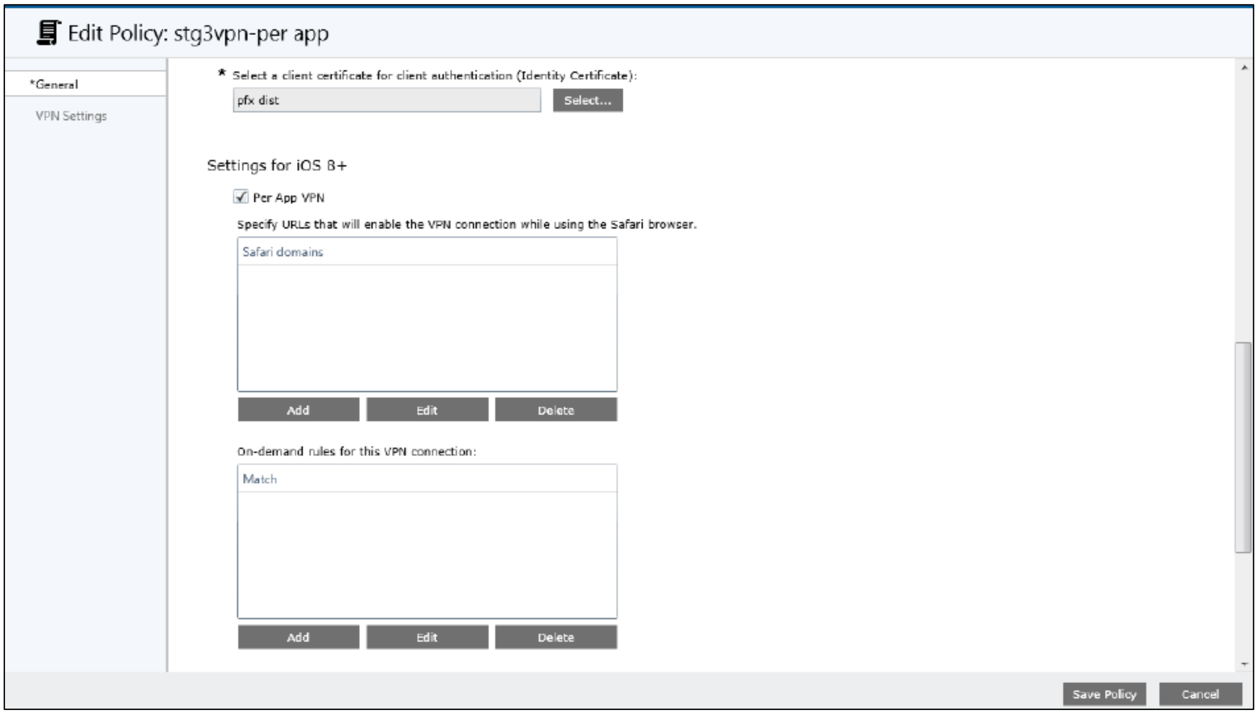
Configuring Per App VPN On-Demand (for iOS device)

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



Edit Policy: stg3vpn-per app

* Select a client certificate for client authentication (Identity Certificate):

pfx dist

Settings for iOS 8+

☑ Per App VPN

Specify URLs that will enable the VPN connection while using the Safari browser.

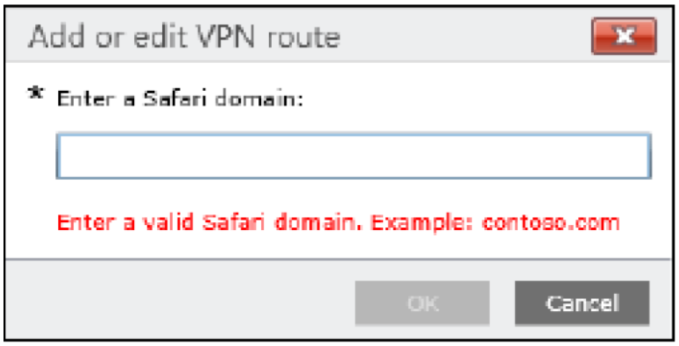
Safari domains

On-demand rules for this VPN connection:

Match

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

Figure 17: Valid Safari Domain



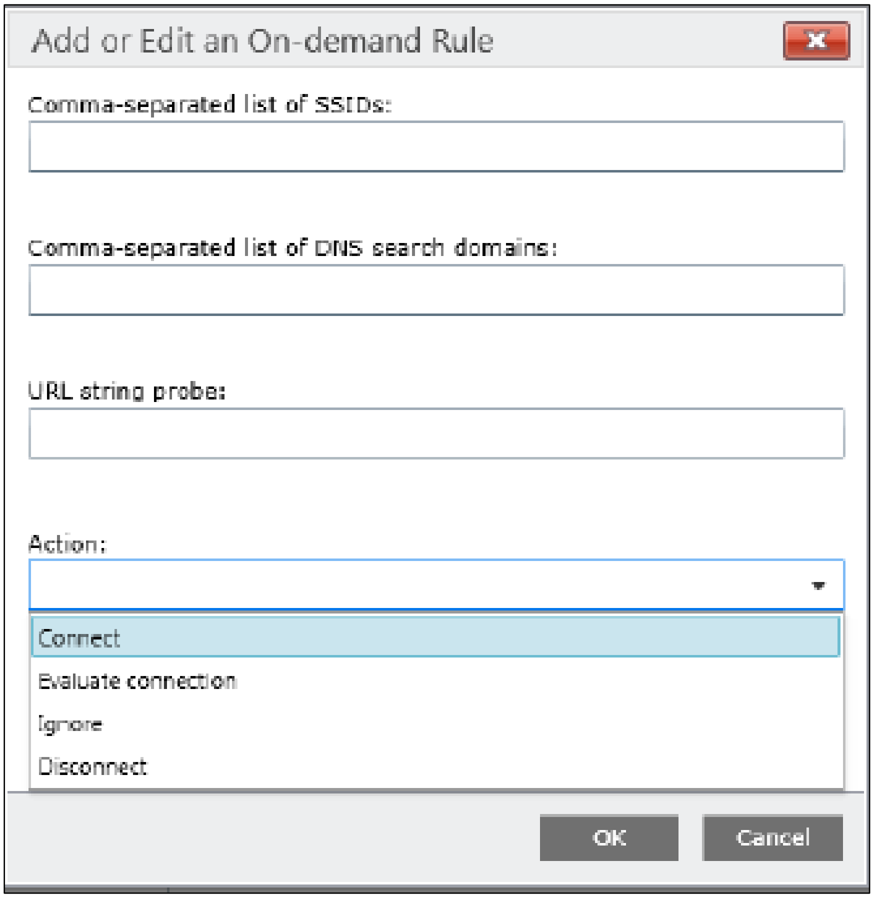
Add or edit VPN route

* Enter a Safari domain:

Enter a valid Safari domain. Example: contoso.com

3. For On-demand rule, click Add and enter the rule. This is applicable to L3 VOD.

Figure 18: On-demand Rule



Add or Edit an On-demand Rule

Comma-separated list of SSIDs:

Comma-separated list of DNS search domains:

URL string probe:

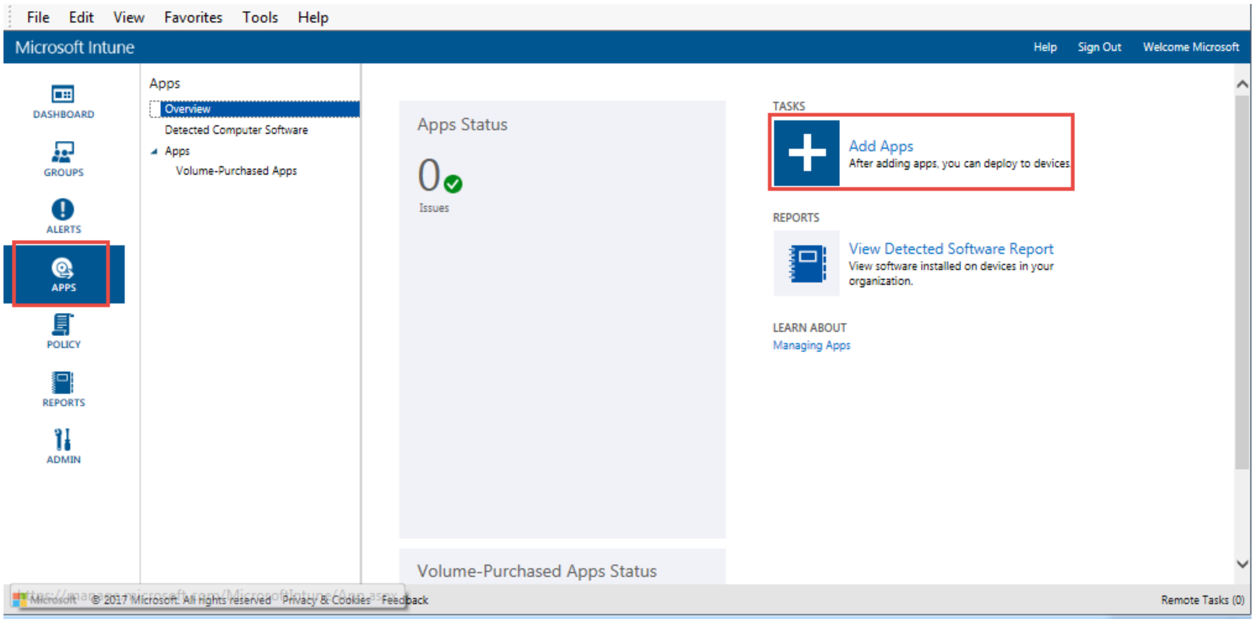
Action:

Adding App for Per App VPN

To add an App for Per App VPN:

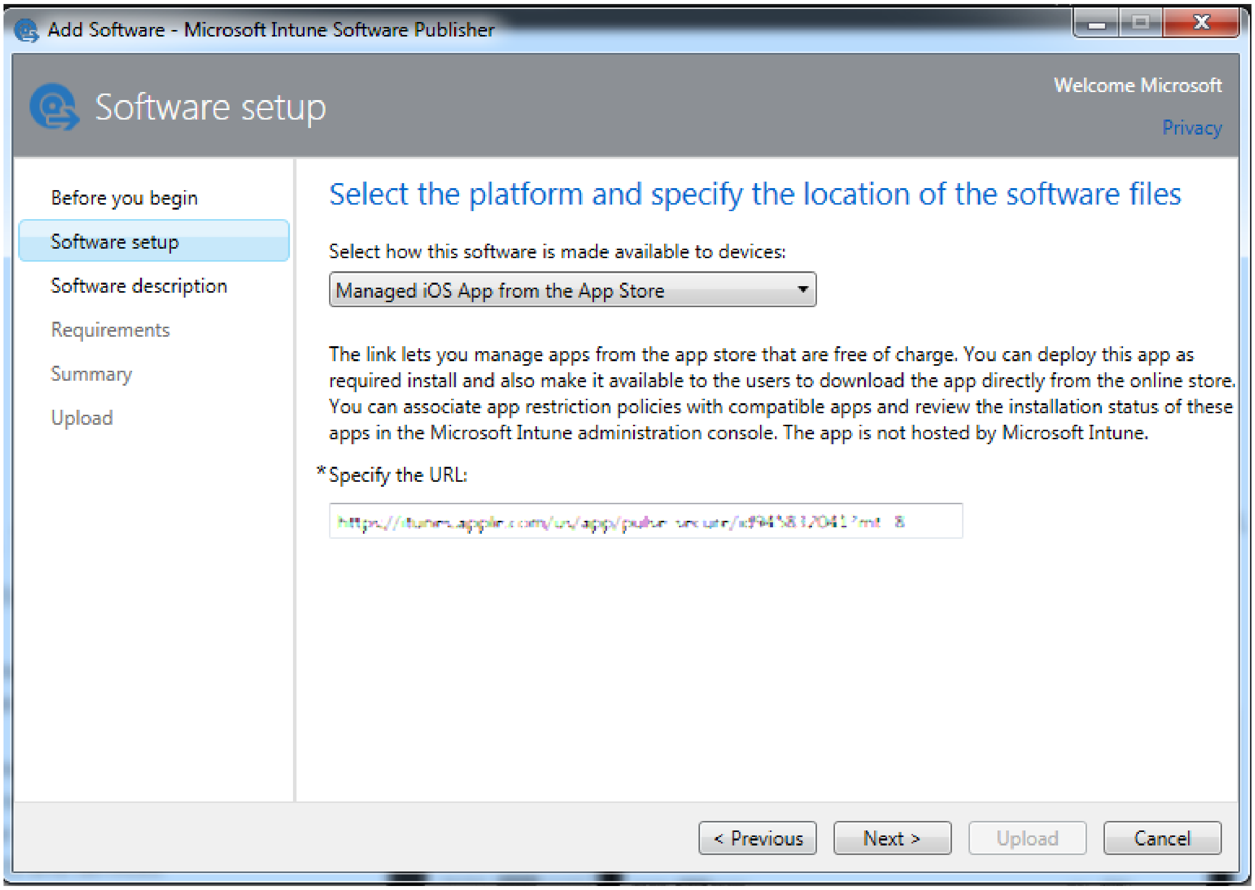
1. Select the **Apps** icon from the left menu options and click **Add Apps**.

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



Select the platform and specify the location of the software files

Select how this software is made available to devices:

Managed iOS App from the App Store

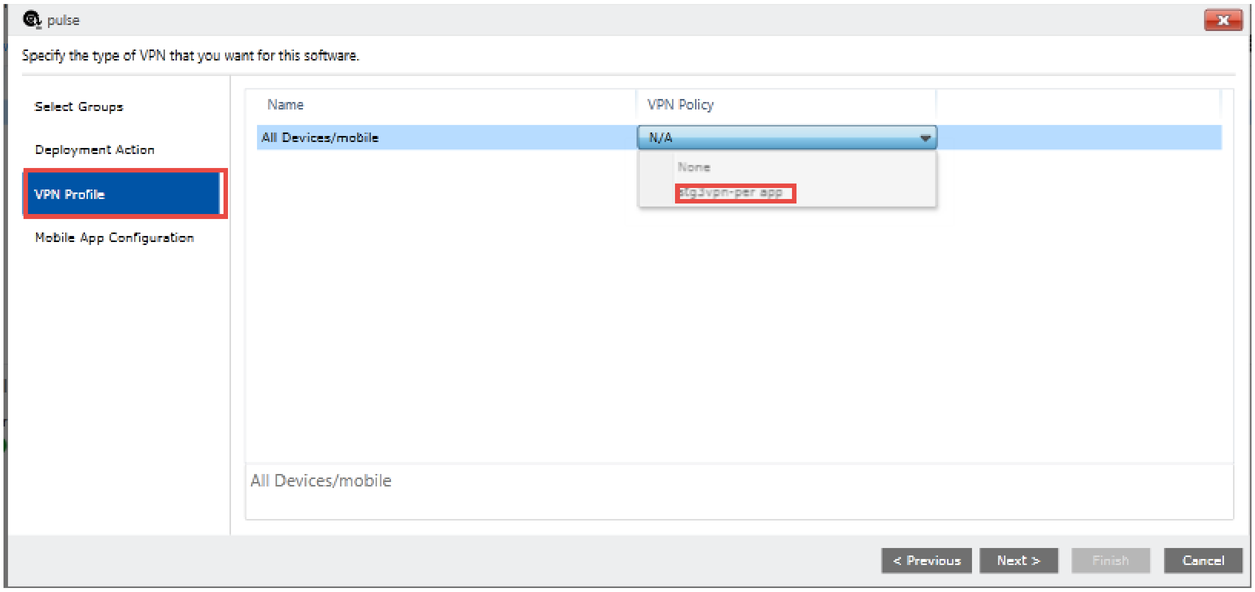
The link lets you manage apps from the app store that are free of charge. You can deploy this app as required install and also make it available to the users to download the app directly from the online store. You can associate app restriction policies with compatible apps and review the installation status of these apps in the Microsoft Intune administration console. The app is not hosted by Microsoft Intune.

*Specify the URL:

https://itunes.apple.com/us/app/pulse-secure/id945832041?mt=8

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.

Figure 21: Specify VPN Policy



pulse

Specify the type of VPN that you want for this software.

Name	VPN Policy
All Devices/mobile	N/A

All Devices/mobile

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:

   Pulse Secure app:

   https://play.google.com/store/apps/details?id=net.pulsesecure.pulsesecure&hl=en

   Intune app: https://play.google.com/store/apps/details?id=com.microsoft.windowsintune.companyportal&hl=en

   For iOS devices:

   Pulse Secure app:

   https://itunes.apple.com/in/app/pulse-secure/id945832041?mt=8

   Intune app: https://itunes.apple.com/in/app/microsoft-intune-company-portal/id719171358?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.