# DigiCert® PKI Platform

## Integrate Microsoft Intune MDM Solution

December 06, 2021

# Legal Notice

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. DIGICERT, INC. SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The licensed software and documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the licensed software and documentation by the U.S. Government shall be solely in accordance with the terms of this documentation.

DigiCert, Inc.

2801 North Thanksgiving Way, Suite 500

Lehi, UT 84043

https://www.digicert.com

# Table of Contents

# Introduction

Microsoft Intune provides mobile device management and mobile application capabilities that let you determine the data different users in your organization can access. The integrated data protection and compliance capabilities define what users can do with the data within Microsoft Office and other mobile apps.

Integrating Microsoft Intune with DigiCert PKI Platform allows you to generate digital certificates that provide the trust without any usernames, passwords, or additional hardware tokens. In addition, DigiCert PKI Platform provides quick deployment and easy management and offers industry leading security that is unmatched by in-house PKI solutions.

This document helps you integrate Microsoft Intune with DigiCert PKI Platform 8.20 to issue end-entity certificates to mobile devices for client authentication.

# Pre-requisites

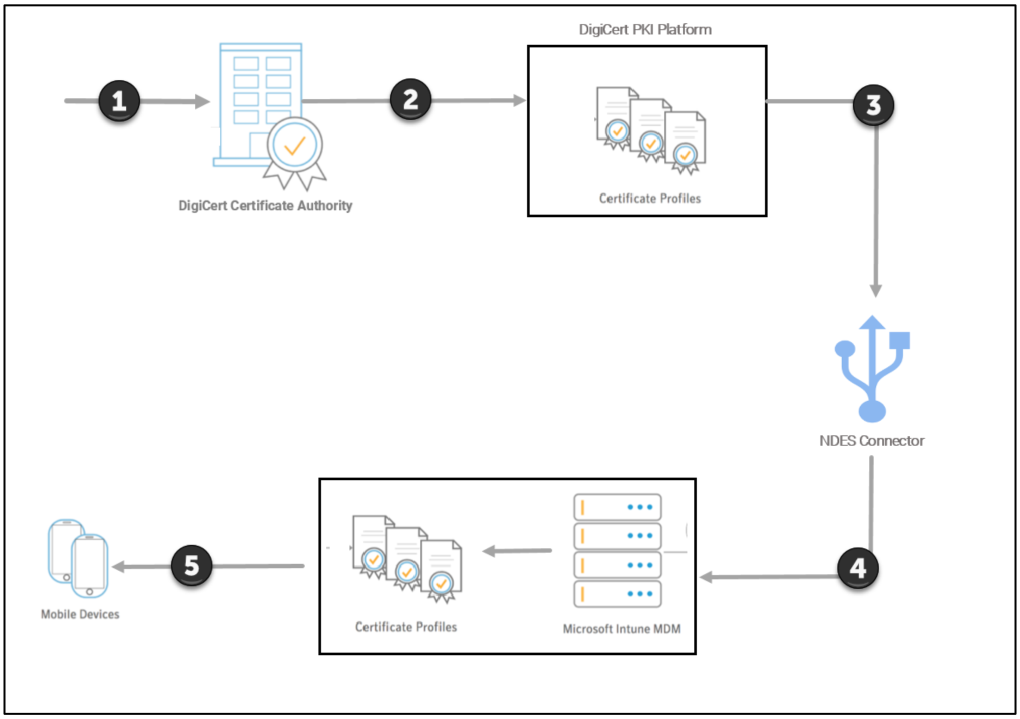
Before you start integrating Microsoft Intune with DigiCert PKI Platform, be sure to:

- Create a DigiCert PKI Platform account.
- Obtain a DigiCert Managed PKI Administrator certificate and verify that you can log in to https://pki-manager.symauth.com/pki-manager.
- Create a Microsoft Intune account. For information on creating a Microsoft Intune account, see https://docs.microsoft.com/en-us/intune/account-sign-up.
  - Once the Intune account is created, login to https://endpoint.microsoft.com.
  - If the account is new, please setup the MDM authority as Intune.
- Meet the system requirements.
- Please make sure that the BCT name is bound to a CA loaded onto your accoun

# Integrate Intune MDM Solution using PKI Web Services

## Integration Overview

The following illustration explains how Microsoft Intune integrates with DigiCert PKI Platform.



1. Generate a DigiCert RA Certificate from the DigiCert Certificate Authority to configure Intune.

3. Install and Configure the NDES Connector.
4. Create a trusted and PKCS Certificate profile in Microsoft End Point.
5. Assign the profiles to the Mobile Devices.

## Integrating DigiCert PKI Platform with Microsoft Intune

Follow these steps to integrate DigiCert PKI Platform with Microsoft Intune:

1. Review the pre-requisites. See "System Requirements".
2. Generate a DigiCert Registration Authority Certificate. See "Generating a DigiCert Registration Authority Certificate".
3. Create a Certificate Profile in DigiCert PKI Platform. See "Creating a Certificate Profile in DigiCert PKI Platform".
4. Set up the Microsoft Intune Connector. See "Setting up the Microsoft Intune Connector".
5. Create a Trusted Certificate Profile. See "Creating a Trusted Certificate Profile".
6. Create a PKCS Certificate Template Profile in Microsoft Intune. See "Creating a PKCS Certificate Profile in Microsoft Intune".
7. Assign Profiles to Users/Devices. See "Assigning Profiles".

## System Requirements

The following are the minimum system requirements to install the Microsoft Intune certificate connector:

- Microsoft Windows Server 2012 R2 or Microsoft Windows Server 2008 R2.
- Microsoft .NET Framework 3.5.
- ASP.NET.

## Generating a DigiCert Registration Authority Certificate

Intune acts as a Registration Authority while requesting for certificates for DigiCert PKI Platform. To configure Intune as a Registration Authority (RA), you must generate a DigiCert Registration Authority Certificate.

You can follow two different methods to generate the require RA certificate:

1. Using OpenSSL via a command-line interface – see Appendix-A for details.
2. Using the Microsoft 'certreq' tool, as detailed within the following steps.

## To generate a DigiCert Registration Authority Certificate:

1. Create a Certificate Signing Request (CSR).

    a) First, create a **certreq.ini** file on the machine where the connector will be installed.

    Save the following code snippet and replace the Subject (in CN format) as required and then save the file.

    ```
    [Version]
    Signature="$Windows NT$"
    [NewRequest]
    ;Change to your,country code, company name and common name
    Subject = "Subject Name in CN format"
    KeySpec = 1
    KeyLength = 2048
    Exportable = TRUE
    MachineKeySet = TRUE
    SMIME = False
    PrivateKeyArchive = FALSE
    UserProtected = FALSE
    UseExistingKeySet = FALSE
    ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
    ProviderType = 12
    RequestType = PKCS10
    KeyUsage = 0xa0
    [EnhancedKeyUsageExtension]
    OID=1.3.6.1.5.5.7.3.2 ; Client Authentication  // Uncomment if you need
    a mutual TLS authentication
    ```

    b) Open an elevated command prompt and generate CSR content using the following command:

    ```
    Certreq.exe -new certreq.ini request.csr

    Open the request.csr file in Notepad and copy the CSR content which must
    be in the following format:

    -----BEGIN NEW CERTIFICATE REQUEST-----
    MIID8TCCAtkCAQAwbTEMMAoGA1UEBhMDVVNBMQswCQYDVQQIDAJXQTEQMA4GA1UE
    …
    …
    fzpeAWo=
    -----END NEW CERTIFICATE REQUEST-----
    ```

2. Log in to **DigiCert PKI Manager**.

3. In the **PKI Manager** dashboard, click the **Tasks** icon and select **Get an RA Certificate**.

4. Paste the content **from** the CSR you created earlier.

5. Specify a certificate friendly name and click **Continue**.
6. Click **Download** and download the RA certificate.
7. Click **Done**.

### Obtain a Trusted Root certificate from DigiCert PKI Platform:

1. In the **PKI Manager** dashboard, click the **Tasks** icon and select **Manage CAs**.
2. Select the appropriate CA from the list.
3. Click **Download root certificate** and save it for later use in Microsoft Endpoint Manager Portal.

**NOTE:** For multi-level CAs both the Issuer as well as the Root certificate must be trusted.

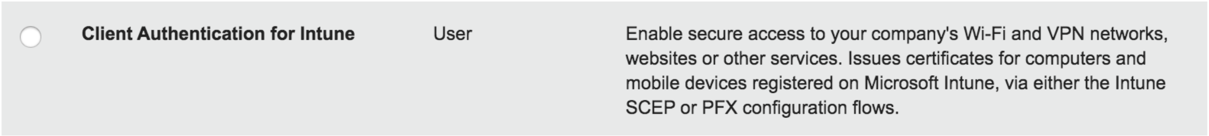
## Creating a Certificate Profile in DigiCert PKI Platform

Certificate profile determines the type of certificate that you want to install on the mobile devices.

### To create a certificate profile in DigiCert PKI Platform:

To create a certificate profile in DigiCert PKI Platform:

1. In the PKI Manager dashboard, click Manage certificate profiles.
2. Click **Add certificate profiles**.
3. Select the mode of the profile and click **Continue**.
4. Select the **Client Authentication for Intune** certificate template that you want to use and click **Continue**.



| | | | |
|---|---|---|---|
| ○ | **Client Authentication for Intune** | User | Enable secure access to your company's Wi-Fi and VPN networks, websites or other services. Issues certificates for computers and mobile devices registered on Microsoft Intune, via either the Intune SCEP or PFX configuration flows. |

**NOTE:** If you do not see these profiles, contact support to have them added to your account.

6. Select the enrollment method as "**PKI Web Services**".

**NOTE**: By default, the CN option on Subject DN will take the format firstname/lastname. If you need the common name format instead, remove and re-add the Common name attribute in the SDN section).

7. Provide additional details and save the certificate profile.
8. After the certificate profile is created, note the Certificate Profile OID.

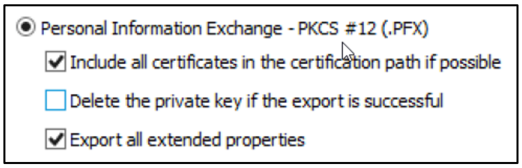
   **NOTE:** The Certificate Profile OID is required to configure the profile in Microsoft Intune.

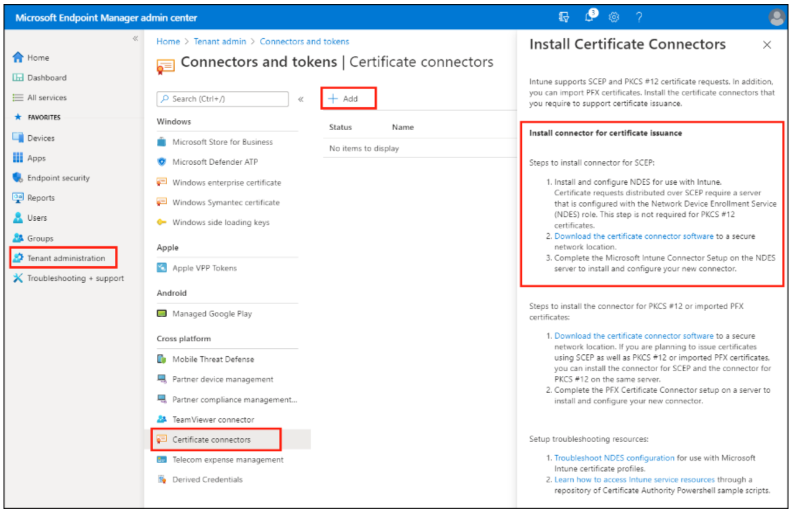
## Setting up the Microsoft Intune Connector

Before installation of the certificate connector, complete the following tasks:

*Table1: Before you install*

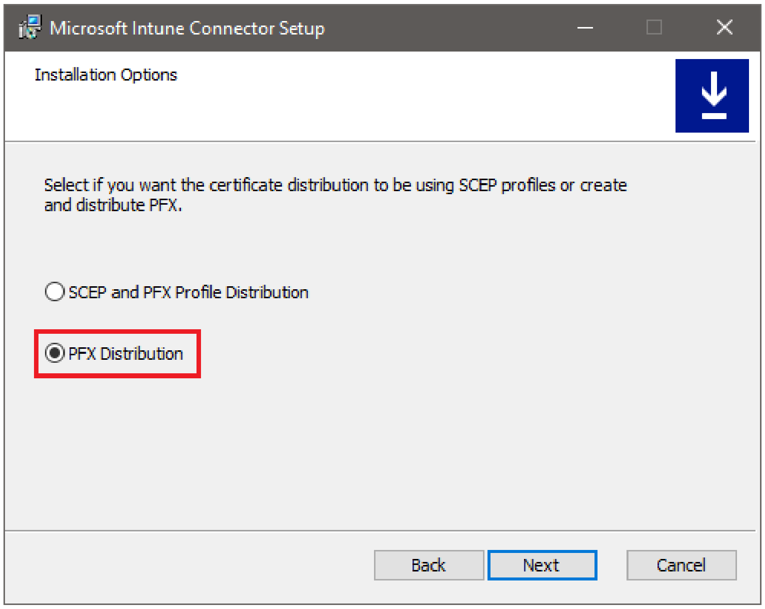
| Task | Procedure |
|---|---|
| Install .NET Framework 3.5. | Follow these steps:<br>1. Open **Control Panel**>**Programs and Features**>**Turn Windows features on or off**<br>2. Select**.NETFramework3.5** and install it. |
| Enable ASP.NET | Follow these steps:<br>1. On the Start page, click the Server Manager tile, and then click **OK**.<br>2. In Server Manager, select **Dashboard**, and click **Add roles and features**.<br>3. In the **Add Roles and Features** Wizard, on the **Before you begin** page, click Next.<br>4. On the **Select installation type** page, select **Role-based or feature-based installation**, and click **Next**.<br>5. On the **Select destination server** page, select **Select a server from the server pool**, select your server, and click **Next**.<br>6. On the **Select server roles** page, select **Web Server** IIS), and click **Next**.<br>7. On the **Select features** page, click **Next**.<br>8. On the **Web Server Role (IIS)** page, click **Next**.<br>9. On the **Select role services** page, note the pre-selected role services that are installed by default, |

| | |
|---|---|
| | expand the **Application Development** node, and then select **ASP.NET3.5**.<br>10. On the **Summary of Features to Install page**, confirm your selections, and then click **Install**.<br>11. In the Add features that are required for ASP.NET4.5? box, click **Add Features**.<br>12. Click **Next**. |
| Import the RA certificate to establish the authentication chain for the Windows computer to make Web Service calls to DigiCert PKI Platform. | Follow these steps:<br>1. Open **Microsoft Management Console**.<br>2. Go to **File**->**Add or Remove Snap-ins**.<br>3. Select **Certificates** from the available Snap-ins and the click **Add**.<br>4. Select **Computer account** and then click **Next** and then **Finish**.<br>5. Click **OK** on Snap-ins window.<br>6. Click **Certificate** > **Personal**.<br>7. Right-click and select **All Tasks** > **Import**.<br>8. Import the RA certificate that you earlier downloaded along with the private key to console.<br>It is always recommended to export the imported RA as PKCS#12 (along with the exported key parameters) and then re-import the .pfx file to the Personal certificate store. (if you have imported the RA in .pfx created from the steps listed in Appendix-A, skip the below steps and proceed to point 9.)<br>To do this:<br>a) Right-click and select **All Tasks** > **Export**.<br>b) Select "**Yes, export the private key**".<br>c) Select the Export file format.<br><br>● Personal Information Exchange - PKCS #12 (.PFX)<br>☑ Include all certificates in the certification path if possible<br>☐ Delete the private key if the export is successful<br>☑ Export all extended properties |

| | |
|---|---|
| | d) Enter a secured password to download and save the PFX.<br>Now, import the private key to personal certificate store.<br>e) Right-click and select **All Tasks** > **Import**.<br>f) Locate the PFX file, enter the password and click Next.<br>g) Browse the certificate store path and click Next.<br>9. Once the key is imported, open the RA certificate and copy the RA thumbprint value, removing all spaces between the characters.<br>10. Save it for later use. |
| Download the Intune Certificate Connector. | Follow these steps:<br>1. Sign in at https://endpoint.microsoft.com<br>2. Select **Tenant administration** > **Connectors and tokens** > **Certificate connectors** > **Add**.<br>3. Download and save the connector for SCEP file. Save it to a location accessible from the server where you're going to install the connector.<br><br> Microsoft Endpoint Manager admin center<br>Home<br>Dashboard<br>All services<br>FAVORITES<br>Devices<br>Apps<br>Endpoint security<br>Reports<br>Users<br>Groups<br>Tenant administration<br>Troubleshooting + support<br>Home > Tenant admin > Connectors and tokens<br>Connectors and tokens \| Certificate connectors<br>Search (Ctrl+/)<br>+ Add<br>Windows<br>Microsoft Store for Business<br>Microsoft Defender ATP<br>Windows enterprise certificate<br>Windows Symantec certificate<br>Windows side loading keys<br>Apple<br>Apple VPP Tokens<br>Android<br>Managed Google Play<br>Cross platform<br>Mobile Threat Defense<br>Partner device management<br>Partner compliance management...<br>TeamViewer connector<br>Certificate connectors<br>Telecom expense management<br>Derived Credentials<br>Status<br>Name<br>No items to display<br>Install Certificate Connectors<br>Intune supports SCEP and PKCS #12 certificate requests. In addition, you can import PFX certificates. Install the certificate connectors that you require to support certificate issuance.<br>**Install connector for certificate issuance**<br>Steps to install connector for SCEP:<br>1. Install and configure NDES for use with Intune. Certificate requests distributed over SCEP require a server that is configured with the Network Device Enrollment Service (NDES) role. This step is not required for PKCS #12 certificates.<br>2. Download the certificate connector software to a secure network location.<br>3. Complete the Microsoft Intune Connector Setup on the NDES server to install and configure your new connector.<br>Steps to install the connector for PKCS #12 or imported PFX certificates:<br>1. Download the certificate connector software to a secure network location. If you are planning to issue certificates using SCEP as well as PKCS #12 or imported PFX certificates, you can install the connector for SCEP and the connector for PKCS #12 on the same server.<br>2. Complete the PFX Certificate Connector setup on a server to install and configure your new connector.<br>Setup troubleshooting resources:<br>1. Troubleshoot NDES configuration for use with Microsoft Intune certificate profiles.<br>2. Learn how to access Intune service resources through a repository of Certificate Authority Powershell sample scripts. |

## Installing and Configuring the Microsoft Intune Connector

1. On the server where you want to install the connector, run **NDESConnectorSetup.exe** with elevated privileges.
2. Select **PFX Distribution** as the installation option and follow on the on-screen instructions to complete the installation.



Microsoft Intune Connector Setup

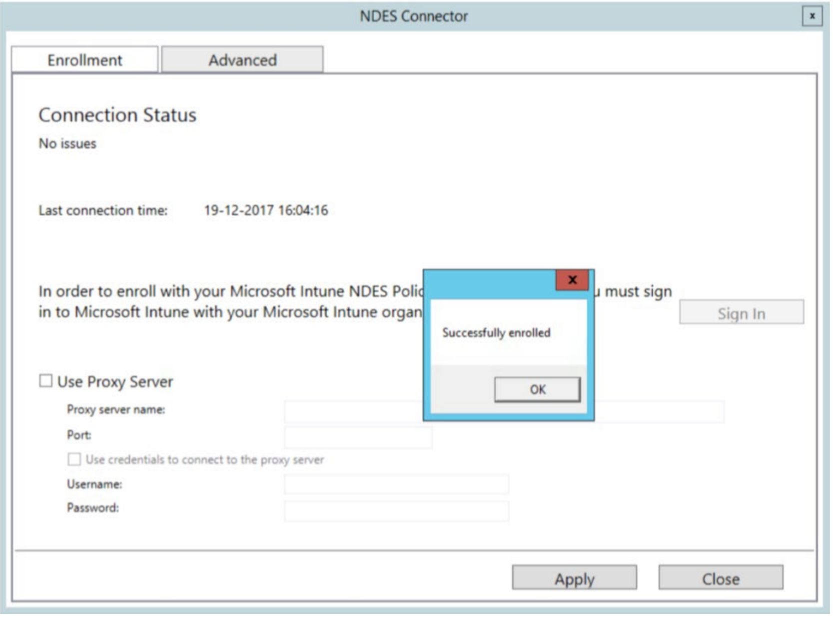
Installation Options

Select if you want the certificate distribution to be using SCEP profiles or create and distribute PFX.

○ SCEP and PFX Profile Distribution

● PFX Distribution

3. In the NDES Connector UI, on the **Enrollment** tab, click **Sign In**.
4. Enter your Intune credentials. (Intune tenant admin)
5. On successful enrollment, the **Successfully enrolled** message is displayed.



Connection Status
No issues

Last connection time: 19-12-2017 16:04:16

In order to enroll with your Microsoft Intune NDES Polic u must sign in to Microsoft Intune with your Microsoft Intune organ

Successfully enrolled

□ Use Proxy Server
Proxy server name:
Port:
□ Use credentials to connect to the proxy server
Username:
Password:

6. Click **Apply and Close**.

**NOTE:** The DigiCert PKI RA certificate/key must be on the same computer where the Intune NDES Connector is installed.

7. Navigate to **C:\Program Files\Microsoft Intune\NDESConnectorSvc** and open **NDESConnector.exe.config** file.

8. Replace the highlighted value with the RA thumbprint value of your RA certificate

```
<add key="RACertThumbprint" value="2bad44960401b90ecf8d5265cf48cea6e8b8dd3f"
/>
```

9. Save the changes to **NDESConnector.exe.config** and restart the "**Intune Connector Service**" from services.msc.

## Creating a Trusted Certificate Profile in Microsoft End Point

The PKCS Certificates deployed for Intune managed devices must be chained with a Trusted Root Certificate. Create an Intune Trusted Certificate Profile with the root certificate obtained from the DigiCert PKI Platform.

1. Sign in to the https://endpoint.microsoft.com/

2. Navigate to **Devices** > **Configuration profiles** > **Create profile**.

3. Select the Platform of the device that will receive the profile and Select **Trusted certificate** from Profile dropdown list.

4. Click **Create**.
5. In **Basics**, enter Name and Description for the profile.
6. Click **Next**.
7. In **Configuration settings**, specify the .cer file for the trusted Root CA Certificate downloaded previously - refer to: Obtain a Trusted Root certificate

   For Windows 8.1 and Windows 10 devices only, select the **Destination Store** for the trusted certificate from:

   a) **Computer certificate store - Root**

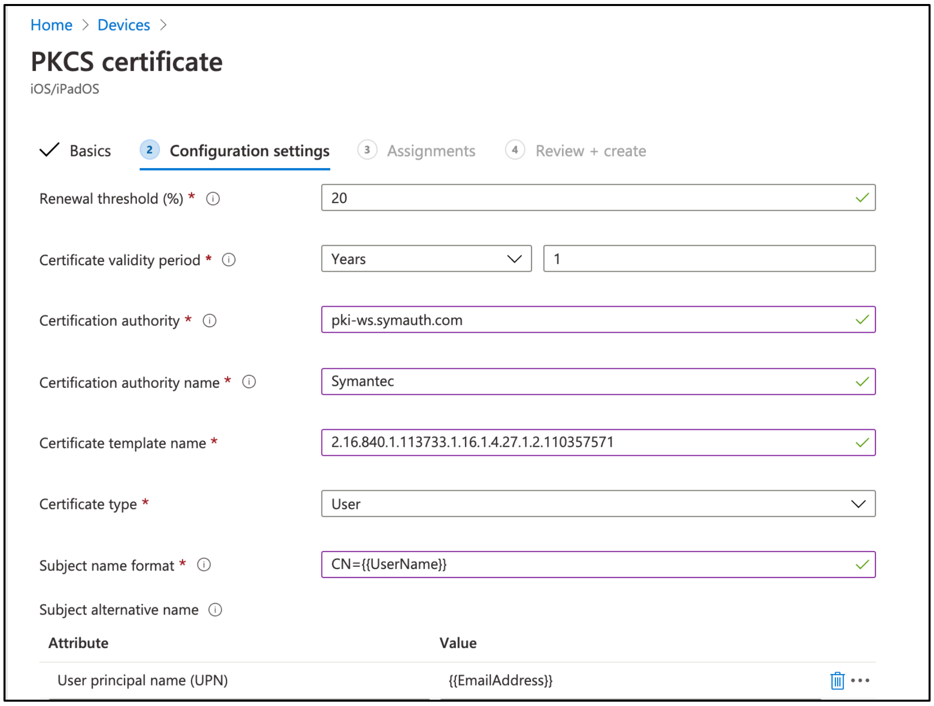
   b) **Computer certificate store - Intermediate**

   c) **User certificate store - Intermediate**
8. Click **Next**.
9. In **Scope tags** (optional) tab, Click **Next**.
10. In **Assignments**, select the user or groups that will receive your profile. Click **Next**.
11. (*Applies to Windows 10 only*) In **Applicability Rules**, specify applicability rules to refine the assignment of this profile. You can choose to assign or not assign the profile based on the OS edition or version of a device.
12. In **Review + create**, review your settings. When you click Create, your changes are saved, and the profile is assigned.

## Creating a PKCS Certificate Profile in Microsoft End Point

For every certificate profile that you created in DigiCert PKI Platform, you must create a corresponding PKCS certificate profile in Intune.

1. Sign in at https://endpoint.microsoft.com.
2. Select **Devices** > **Configuration profiles** > **Create profile**.
3. Select the Platform of the device that will receive the profile and Select **PKCS certificate** from Profile dropdown list.
4. Click **Create**.
5. In **Basics**, enter Name and Description for the profile.
6. Click **Next**.
7. In **Configuration Settings**, enter the following details.



PKCS certificate

iOS/iPadOS

| | |
|---|---|
| Renewal threshold (%) * | 20 ✓ |
| Certificate validity period * | Years 1 |
| Certification authority * | pki-ws.symauth.com ✓ |
| Certification authority name * | Symantec ✓ |
| Certificate template name * | 2.16.840.1.113733.1.16.1.4.27.1.2.110357571 ✓ |
| Certificate type * | User |
| Subject name format * | CN={{UserName}} ✓ |

Subject alternative name

| Attribute | Value |
|---|---|
| User principal name (UPN) | {{EmailAddress}} |

| Parameter | Value |
|---|---|
| Certification authority | pki-ws.symauth.com |
| Certification authority name | Symantec |
| Certificate template name | The certificate profile OID of the certificate profile template you created in DigiCert PKI Platform. |
| Subject name format | Common name or Common name as email |
| Subject alternative name | The SAN option that you selected in DigiCert PKI Platform. (Refer to Table 1.1) |

*Table:1.1 Supported Matrix of certificate fields: DigiCert PKI Platform solution vs Intune*

| Certificate Profile Field | DigiCert PKI Platform Certificate Attribute Name | Intune Support |
|---|---|---|
| Subject Alternative Name (SAN) | DNS Name | Supported |
| | RFC822 Name | Supported |

| | | |
|---|---|---|
| | User Principal Name | Supported |
| | Directory name | Not supported |
| | IP Address | Not supported |
| | Other Name (GUID) | Not supported |
| | Registered ID | Not supported |
| | Uniform Resource Locator (URI) | Not supported |

8. Click **Next**.
9. In **Assignments**, select the user or groups that will receive your profile
10. In **Review + create**, review your settings. When you click Create, your changes are saved, and the profile is assigned.

The next steps to be followed are:

A. Once the admin completes assigning profiles for the devices, the next step for you as a user is to enroll the device. For Apple device enrollment, refer Appendix-B.

B. After enrollment for the device is completed, you can install the Company Portal App on the device. This is done to install the profile and generate the certificate on the device. For more information, refer Appendix-C.

C. Once the profile is installed and the certificate is generated on the device, you can start deploying the profiles. For more information, refer Appendix-D.

D. After the profiles are deployed, you must validate the certificate issuance details in DigiCert PKI Platform. For more information, refer Appendix-E.

# Integrate Intune MDM Solution via SCEP

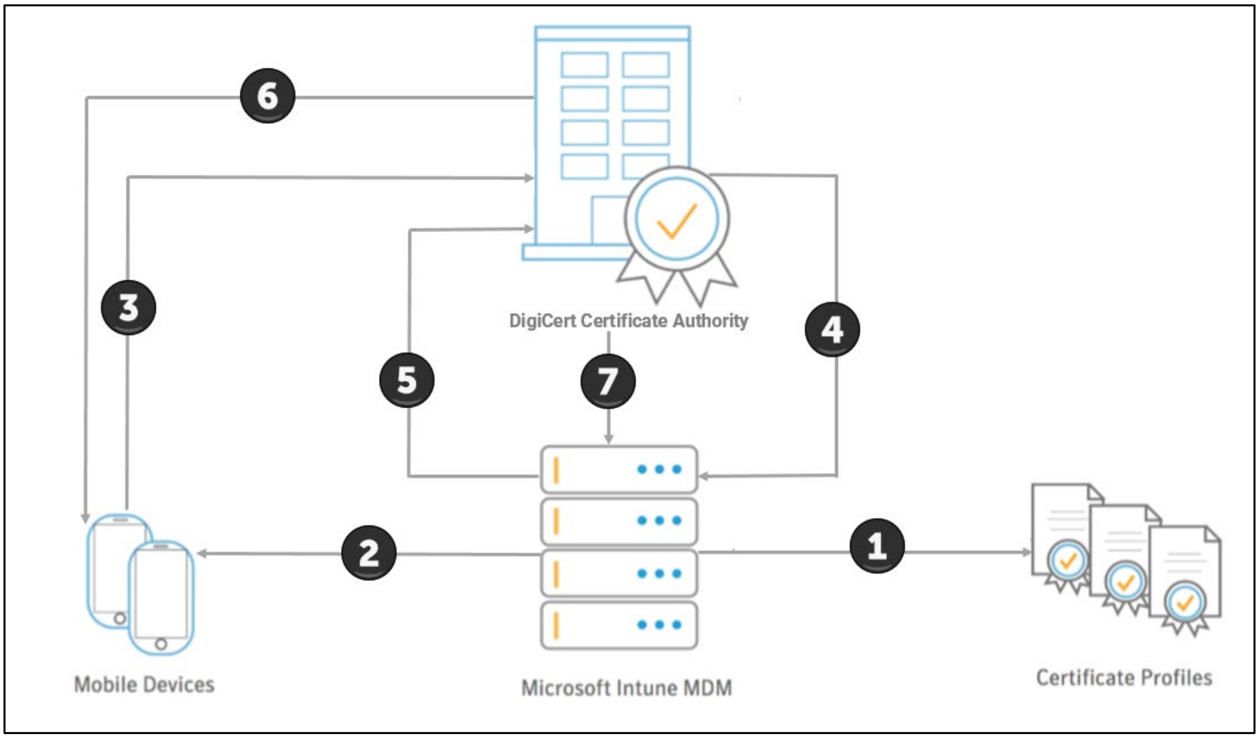
## Introduction

In the previous section we have seen how to issue certificates to devices using PKI Webservices through Microsoft Intune and NDES connector configuration.

As a next logical step, Intune has introduced SCEP support for non-Microsoft CAs. This guide details the steps required to integrate DigiCert PKI Platform and Intune to issue certificates using SCEP enrollments.

## Integration Overview

The following illustration explains how Microsoft Intune integrates with DigiCert PKI Platform via SCEP.



1. The Intune Administrator creates certificate templates in Microsoft Intune corresponding to the profiles created in DigiCert PKI Platform.
2. Microsoft Intune deploys the certificate profile to the specified group of mobile devices.
3. The Mobile Device will enroll for the certificate from DigiCert Certificate Authority.
4. DigiCert Certificate Authority will validate the request with Intune.

5. Microsoft Intune will provide the validation response to DigiCert PKI Platform SCEP service.
6. DigiCert Certificate Authority will issue the certificate to the requesting device.
7. Finally, DigiCert Certificate Authority will provide the confirmation message to Intune.

## Step 1: Register the Client Application

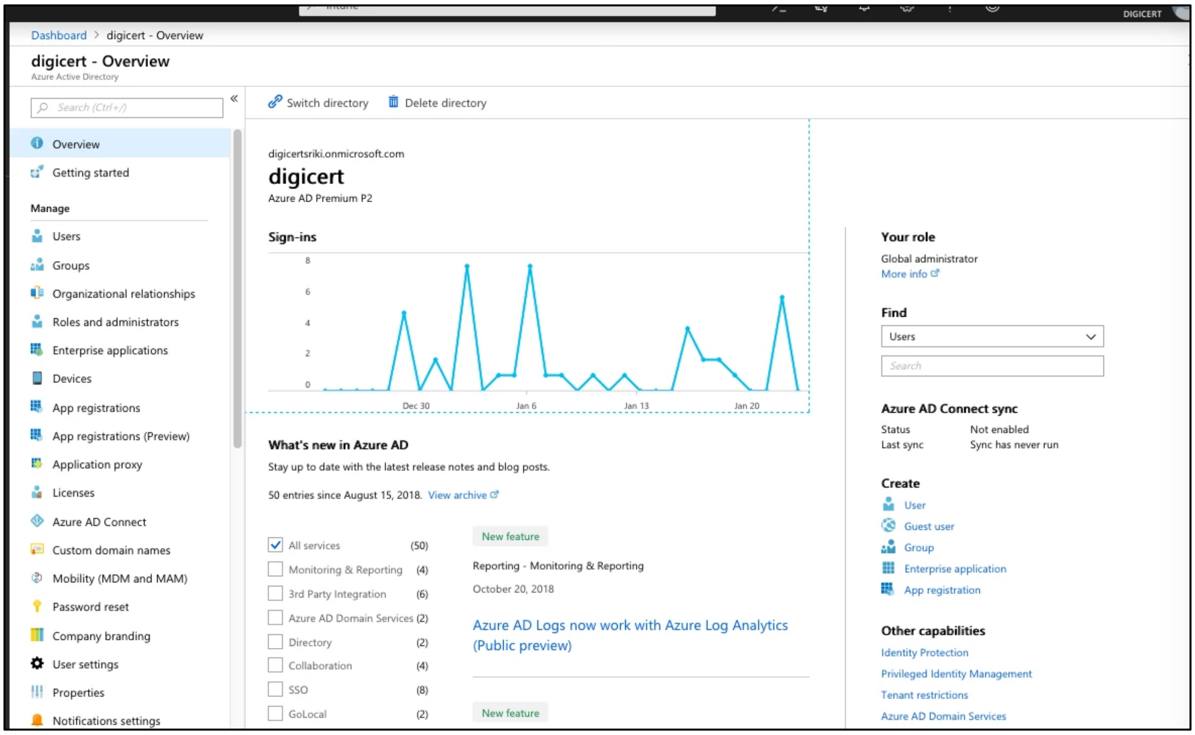
Firstly, we need to register the SCEP Service which will be making the call to the Intune API.

To do this –

1. On your Intune tenant, please make sure Azure Active Directory services is enabled. (This is enabled with P1/P2 license or Enterprise Mobility Suite (EMS).

   Please note that if you have EMS, then Azure Active Directory Premium P2 is enabled by default.

2. On the Azure portal, navigate to "Azure Active Directory".



digicertsriki.onmicrosoft.com

digicert

Azure AD Premium P2

Your role

Global administrator

More info

Azure AD Connect sync

Status Not enabled

Last sync Sync has never run

What's new in Azure AD

Stay up to date with the latest release notes and blog posts.

50 entries since August 15, 2018. View archive

☑ All services (50)
☐ Monitoring & Reporting (4)
☐ 3rd Party Integration (6)
☐ Azure AD Domain Services (2)
☐ Directory (2)
☐ Collaboration (4)
☐ SSO (8)
☐ GoLocal (2)

Reporting - Monitoring & Reporting

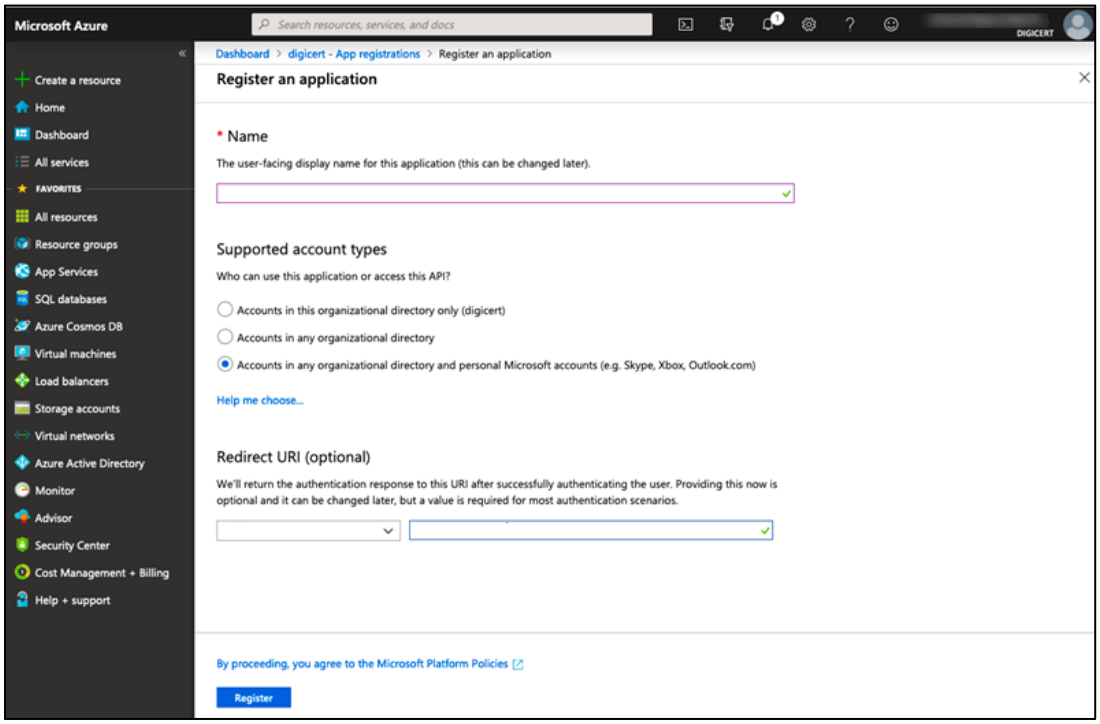
October 20, 2018

Azure AD Logs now work with Azure Log Analytics (Public preview)

3. Click on "App Registrations" link to start the application registration process.

   NOTE: Please note that you can register as many applications as you want using different application id and key params for more security.

4. Click on "**Register an application**" link.



Register an application

* Name

The user-facing display name for this application (this can be changed later).

Supported account types

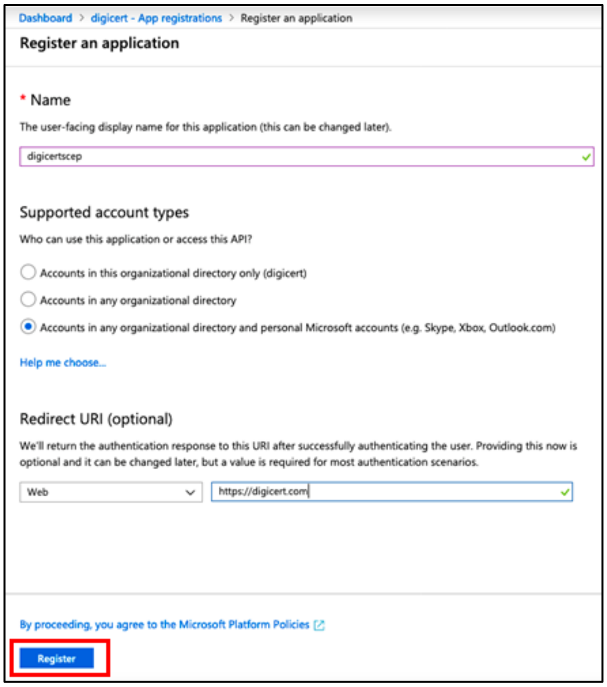
Who can use this application or access this API?

○ Accounts in this organizational directory only (digicert)
○ Accounts in any organizational directory
● Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

5. Provide a Name for the application and sign-on URL which can be identified with your application. For our purpose these can be arbitrary values.


Dashboard > digicert - App registrations > Register an application
Help me choose...
By proceeding, you agree to the Microsoft Platform Policies
Register

Register an application

* Name

The user-facing display name for this application (this can be changed later).

digicertscep

Supported account types

Who can use this application or access this API?

○ Accounts in this organizational directory only (digicert)
○ Accounts in any organizational directory
● Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

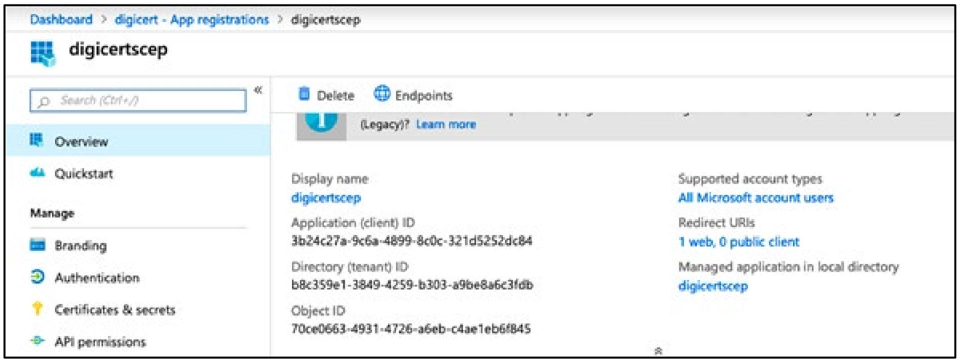
Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | https://digicert.com

6. Click on "**Register**" to complete the registration.

7. In the resulting screen below, please copy and save the application id value in a secure file for later use.



Display name
digicertscep

Application (client) ID
3b24c27a-9c6a-4899-8c0c-321d5252dc84

Directory (tenant) ID
b8c359e1-3849-4259-b303-a9be8a6c3fdb

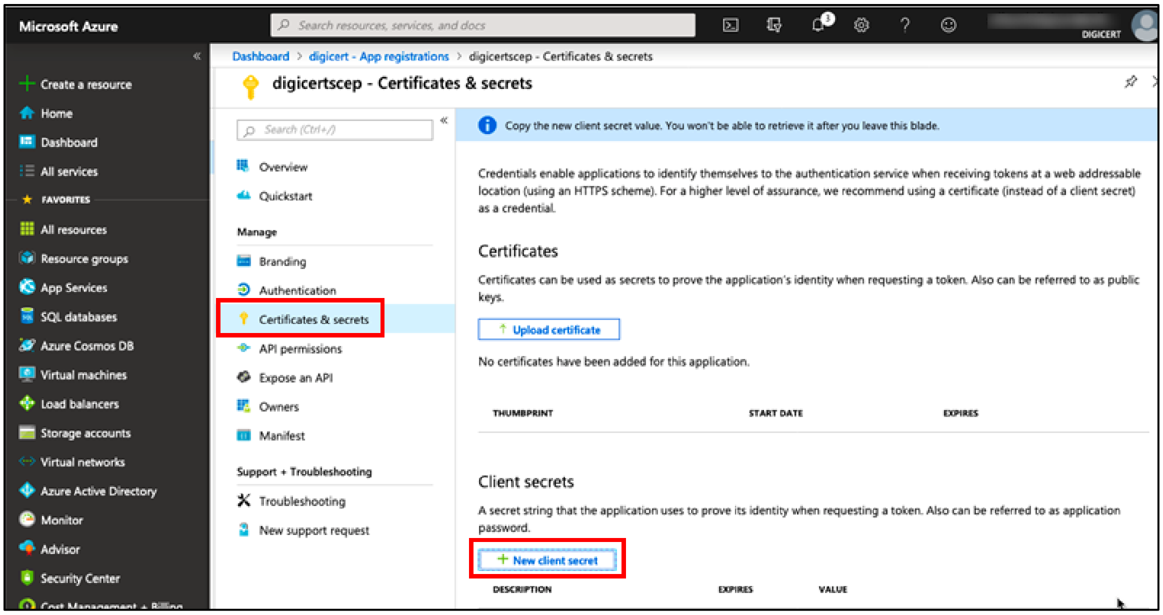
Object ID
70ce0663-4931-4726-a6eb-c4ae1eb6f845

Supported account types
All Microsoft account users

Redirect URIs
1 web, 0 public client

Managed application in local directory
digicertscep

8. Click on "**Certificates & secrets**" icon and then click on "**New Client Secret**" link.



Copy the new client secret value. You won't be able to retrieve it after you leave this blade.

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

No certificates have been added for this application.

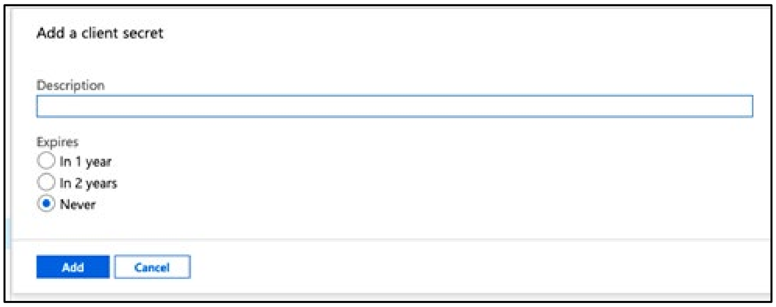
| THUMBPRINT | START DATE | EXPIRES |
|---|---|---|

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

| DESCRIPTION | EXPIRES | VALUE |
|---|---|---|

9. Provide the client secret (can be any string). Select desired expiration period for the client secret. (Please note that the client secret will need to be re-created after expiration) Then click **Add**.



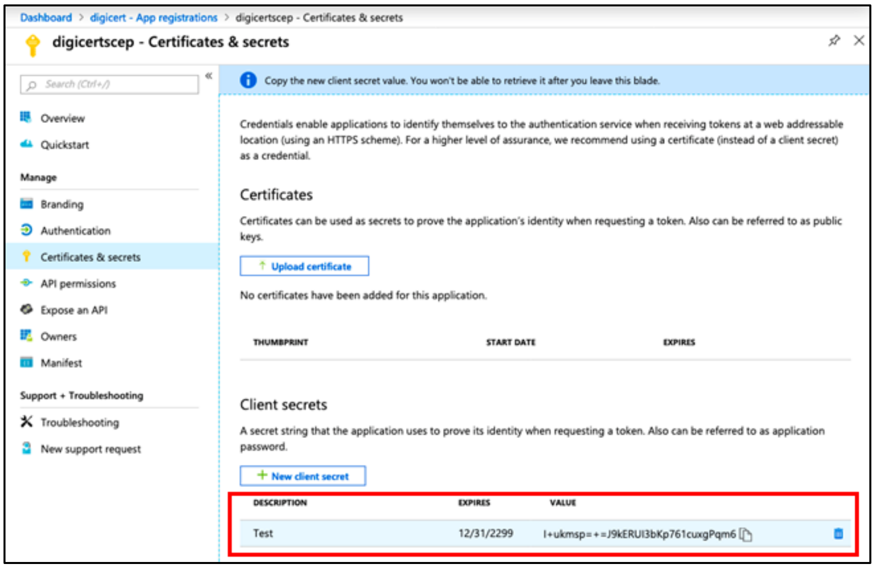
Add a client secret

Description

Expires
○ In 1 year
○ In 2 years
● Never

10. Saving the client secret information will create a random string as application key and will display it in the text box. Copy this key value and store it in the same file as the previously saved application id.

    NOTE: The client secret string cannot be viewed again as it remains hidden once this view is closed. If this value is not saved, a new client secret will need to be created if lost.



Copy the new client secret value. You won't be able to retrieve it after you leave this blade.

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

No certificates have been added for this application.

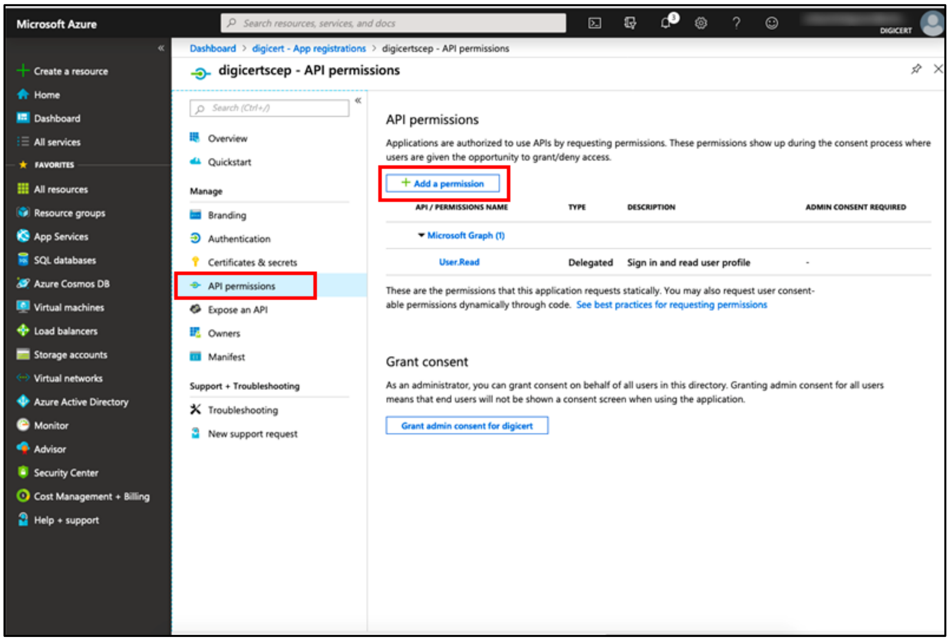
| THUMBPRINT | START DATE | EXPIRES |
|---|---|---|

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

| DESCRIPTION | EXPIRES | VALUE |
|---|---|---|
| Test | 12/31/2299 | l+ukmsp=+=J9kERUI3bKp761cuxgPqm6 |

11. Once the client secret is saved, click on "API Permissions->Add a permission".



API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up during the consent process where users are given the opportunity to grant/deny access.

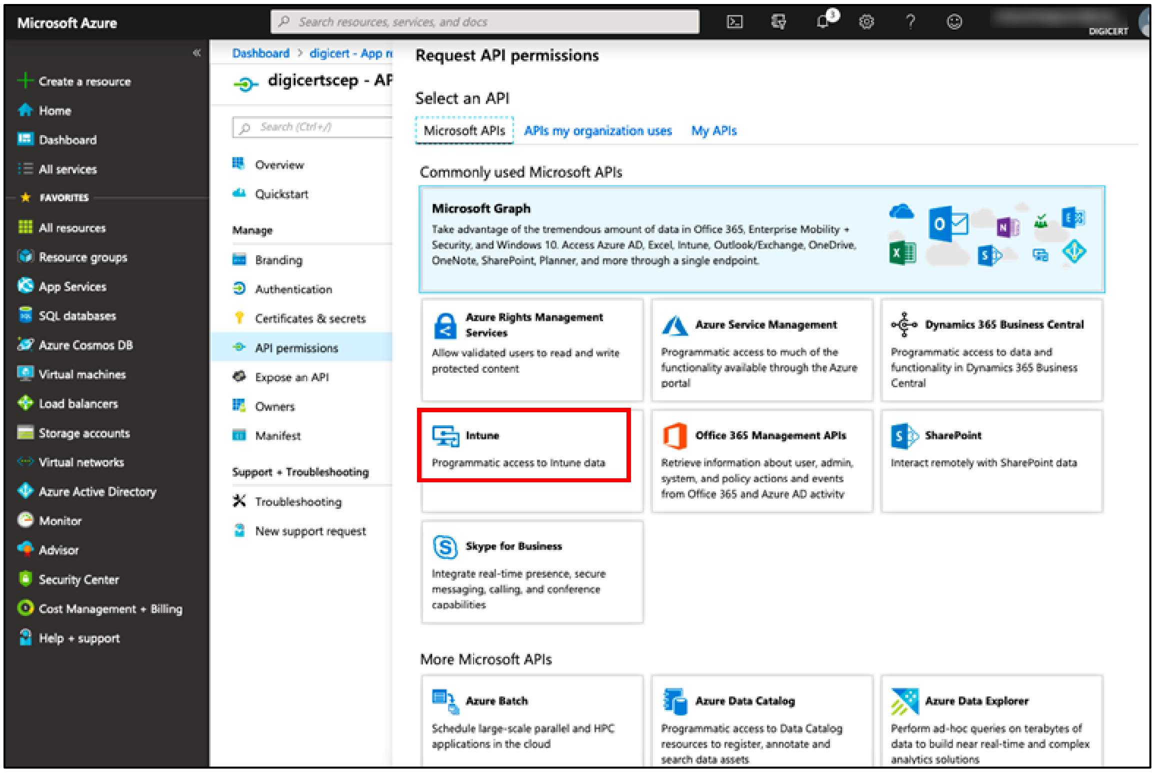
| API / PERMISSIONS NAME | TYPE | DESCRIPTION | ADMIN CONSENT REQUIRED |
|---|---|---|---|
| Microsoft Graph (1) | | | |
| User.Read | Delegated | Sign in and read user profile | - |

These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. See best practices for requesting permissions

Grant consent

As an administrator, you can grant consent on behalf of all users in this directory. Granting admin consent for all users means that end users will not be shown a consent screen when using the application.

12. Select "Intune".



Request API permissions

Select an API

Microsoft APIs | APIs my organization uses | My APIs

Commonly used Microsoft APIs

**Microsoft Graph**
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

**Azure Rights Management Services**
Allow validated users to read and write protected content

**Azure Service Management**
Programmatic access to much of the functionality available through the Azure portal

**Dynamics 365 Business Central**
Programmatic access to data and functionality in Dynamics 365 Business Central

**Intune**
Programmatic access to Intune data

**Office 365 Management APIs**
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

**SharePoint**
Interact remotely with SharePoint data

**Skype for Business**
Integrate real-time presence, secure messaging, calling, and conference capabilities

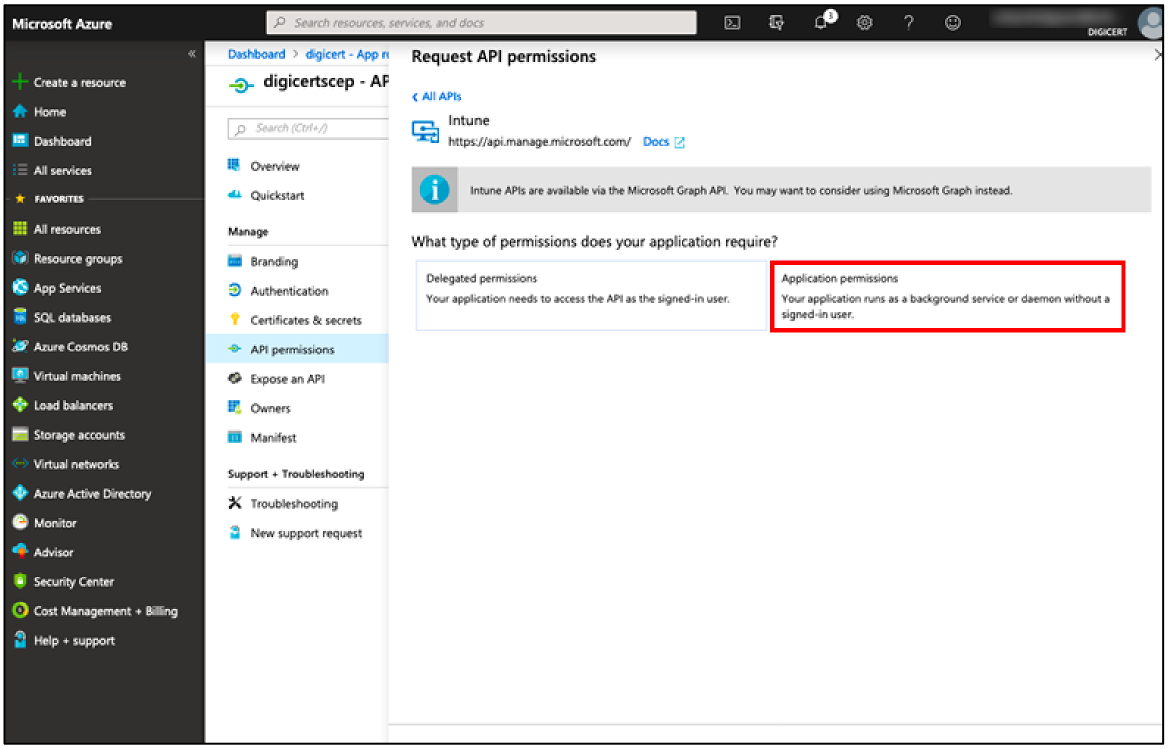
More Microsoft APIs

**Azure Batch**
Schedule large-scale parallel and HPC applications in the cloud

**Azure Data Catalog**
Programmatic access to Data Catalog resources to register, annotate and search data assets

**Azure Data Explorer**
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

13. Click on "Application permissions".



Request API permissions

< All APIs

Intune
https://api.manage.microsoft.com/ Docs

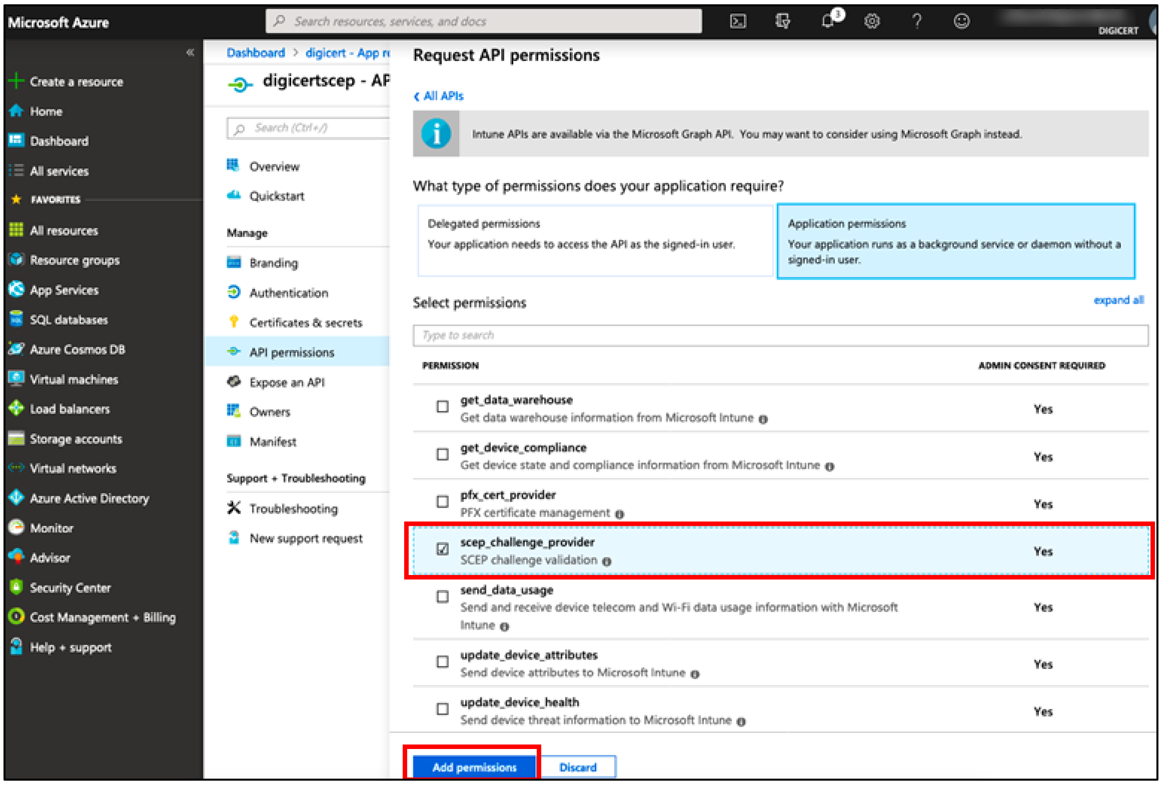
Intune APIs are available via the Microsoft Graph API. You may want to consider using Microsoft Graph instead.

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

14. Select "**scep_challenge_provider**" and then click on "**Add permissions**".



Request API permissions

Intune APIs are available via the Microsoft Graph API. You may want to consider using Microsoft Graph instead.

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

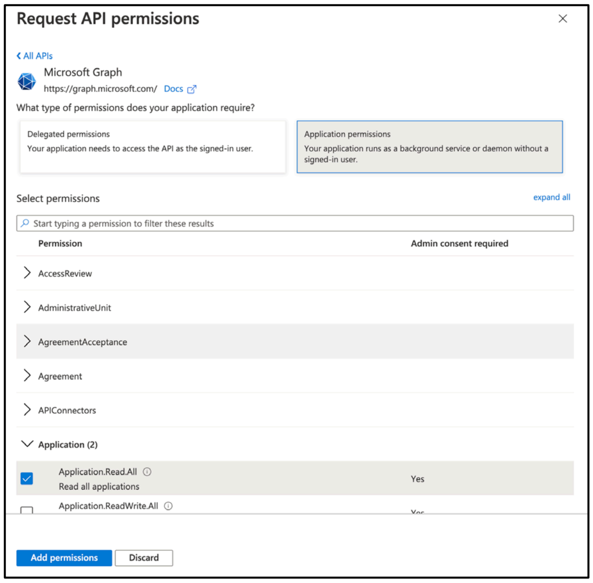
Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

| PERMISSION | ADMIN CONSENT REQUIRED |
|---|---|
| □ get_data_warehouse<br>Get data warehouse information from Microsoft Intune | Yes |
| □ get_device_compliance<br>Get device state and compliance information from Microsoft Intune | Yes |
| □ pfx_cert_provider<br>PFX certificate management | Yes |
| ☑ scep_challenge_provider<br>SCEP challenge validation | Yes |
| □ send_data_usage<br>Send and receive device telecom and Wi-Fi data usage information with Microsoft Intune | Yes |
| □ update_device_attributes<br>Send device attributes to Microsoft Intune | Yes |
| □ update_device_health<br>Send device threat information to Microsoft Intune | Yes |

15. Click **Add permissions** button to add the **Microsoft Graph** permission:

- On the Request API permissions page, select **Microsoft Graph** > **Application permissions**.
- Expand **Application** and select the checkbox for **Application.Read.All** (Read all applications).
- Select **Add permissions** to save this configuration.



Request API permissions

‹ All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

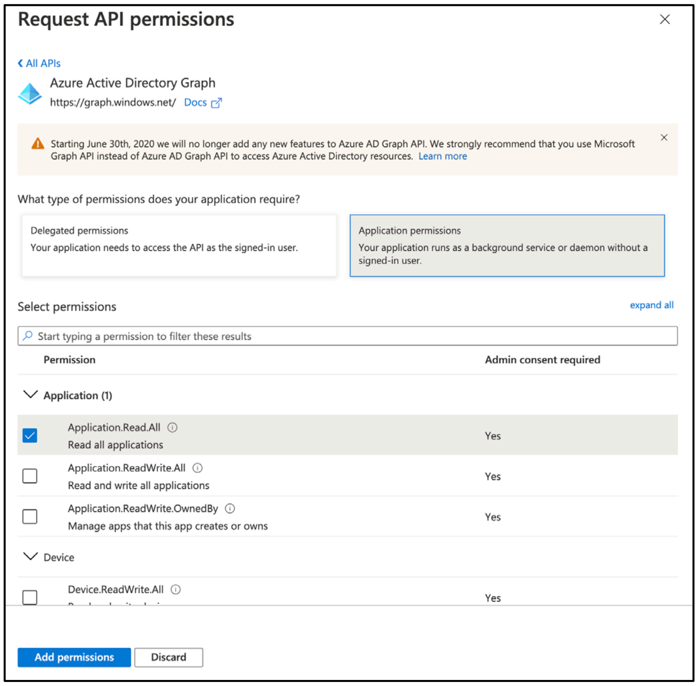
Select permissions

Start typing a permission to filter these results

| | Permission | Admin consent required |
|---|---|---|
| | › AccessReview | |
| | › AdministrativeUnit | |
| | › AgreementAcceptance | |
| | › Agreement | |
| | › APIConnectors | |
| | ⌄ Application (2) | |
| ☑ | Application.Read.All<br>Read all applications | Yes |
| □ | Application.ReadWrite.All | Yes |

16. Click on the **Add permissions** button to add the **Azure Active Directory Graph** permission:

    - On the Request API permissions page, select **Azure Active Directory Graph > Application permissions**.
    - Expand **Application** and select the checkbox for **Application.Read.All** (Read all applications).
    - Select **Add permissions** to save this configuration.



Request API permissions

‹ All APIs

Azure Active Directory Graph
https://graph.windows.net/ Docs

Starting June 30th, 2020 we will no longer add any new features to Azure AD Graph API. We strongly recommend that you use Microsoft Graph API instead of Azure AD Graph API to access Azure Active Directory resources. Learn more

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

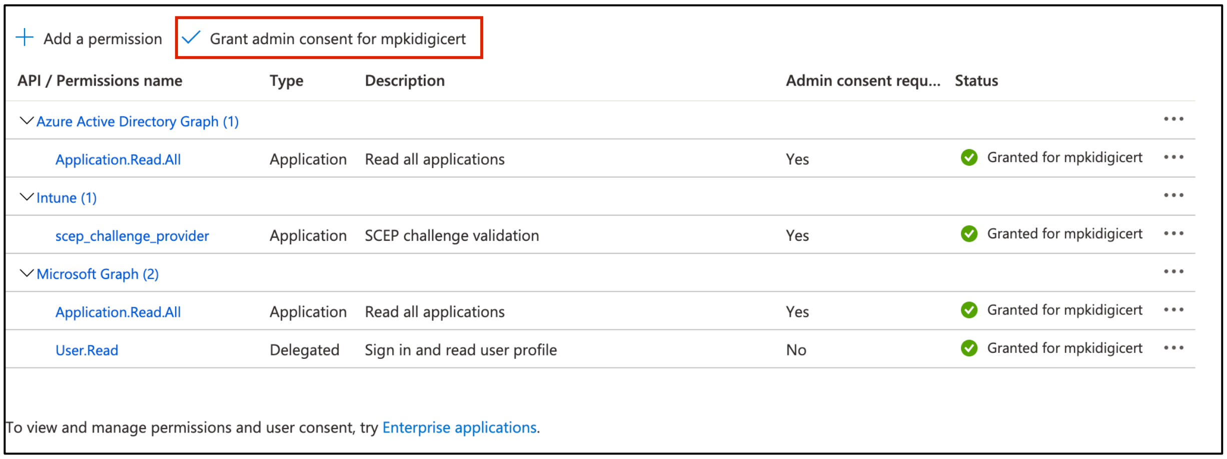
Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

Start typing a permission to filter these results

| | Permission | Admin consent required |
|---|---|---|
| | ⌄ Application (1) | |
| ☑ | Application.Read.All<br>Read all applications | Yes |
| □ | Application.ReadWrite.All<br>Read and write all applications | Yes |
| □ | Application.ReadWrite.OwnedBy<br>Manage apps that this app creates or owns | Yes |
| | ⌄ Device | |
| □ | Device.ReadWrite.All | Yes |

Remain on the API permissions page and select **Grant admin consent** for <your tenant>, and then select **Yes**.

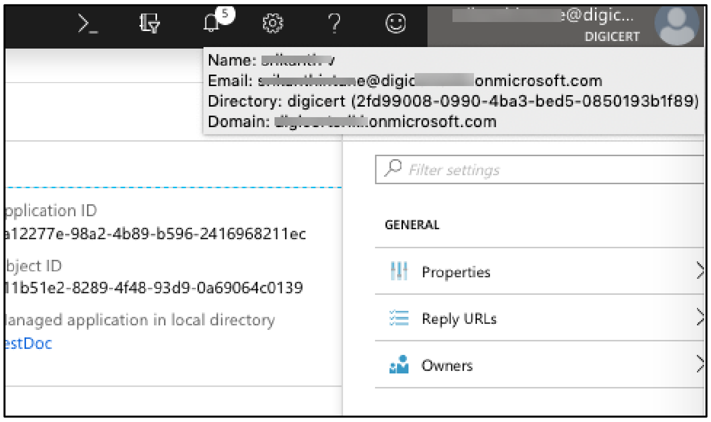


| API / Permissions name | Type | Description | Admin consent requ... | Status | |
|---|---|---|---|---|---|
| Azure Active Directory Graph (1) | | | | | ••• |
| Application.Read.All | Application | Read all applications | Yes | ✓ Granted for mpkidigicert | ••• |
| Intune (1) | | | | | ••• |
| scep_challenge_provider | Application | SCEP challenge validation | Yes | ✓ Granted for mpkidigicert | ••• |
| Microsoft Graph (2) | | | | | ••• |
| Application.Read.All | Application | Read all applications | Yes | ✓ Granted for mpkidigicert | ••• |
| User.Read | Delegated | Sign in and read user profile | No | ✓ Granted for mpkidigicert | ••• |

To view and manage permissions and user consent, try Enterprise applications.

The app registration process in Azure AD is complete.

NOTE: Please note that on the right-hand top corner when you click on your user account, you will see the account details.



Name: [redacted]
Email: [redacted]e@digic[redacted]onmicrosoft.com
Directory: digicert (2fd99008-0990-4ba3-bed5-0850193b1f89)
Domain: [redacted].onmicrosoft.com

pplication ID
a12277e-98a2-4b89-b596-2416968211ec

bject ID
11b51e2-8289-4f48-93d9-0a69064c0139

lanaged application in local directory
estDoc

17. Take a note of the email domain in the Email value (which is after the '@' sign). In the screenshot it is 'xxxx.onmicrosoft.com'. This is the value for your Tenant ID.

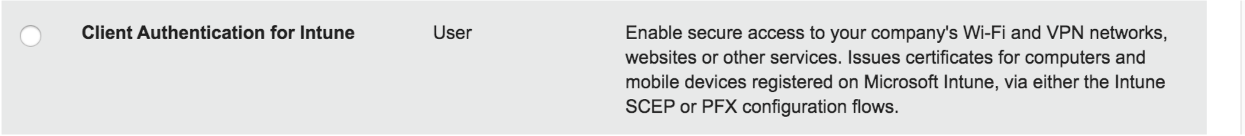
18. Save this value along with the Application ID and Application Key values saved before.

19. These values need to be entered while creating a certificate profile in DigiCert PKI Platform.

## Step 2: Create a SCEP URL

1. Create a SCEP profile in DigiCert PKI Platform and make note of the SCEP URL for the profile.

   a) Create a profile of the Client Authentication for Intune BCT.



○ **Client Authentication for Intune** User Enable secure access to your company's Wi-Fi and VPN networks, websites or other services. Issues certificates for computers and mobile devices registered on Microsoft Intune, via either the Intune SCEP or PFX configuration flows.

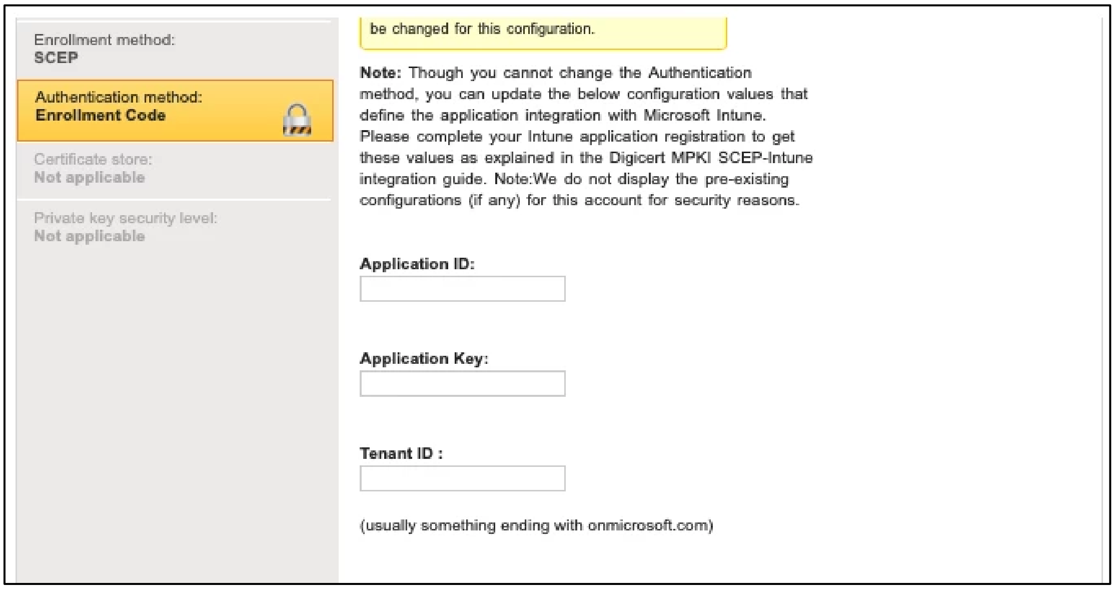
NOTE:

- If you do not see these profiles, contact support to have them added to your account.
- Please note that the certificate template "Client Authentication for Intune" supports Intune Integration in MacOS as well.

   b) Provide a name for the profile.

   c) Select the enrolment method as "SCEP".

   d) Authentication method is defaulted to "Enrollment code" - click on the Authentication method to enter the values of Application registration from Intune.



Enrollment method: **SCEP**

Authentication method: **Enrollment Code**

Certificate store: **Not applicable**

Private key security level: **Not applicable**

be changed for this configuration.

**Note:** Though you cannot change the Authentication method, you can update the below configuration values that define the application integration with Microsoft Intune. Please complete your Intune application registration to get these values as explained in the Digicert MPKI SCEP-Intune integration guide. Note:We do not display the pre-existing configurations (if any) for this account for security reasons.

**Application ID:**

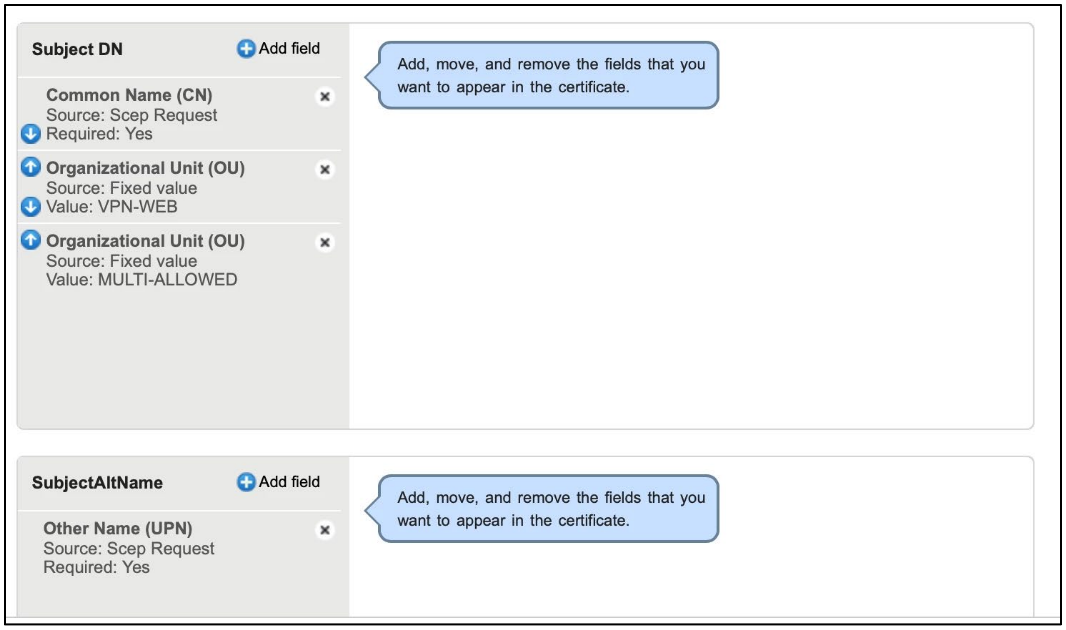
**Application Key:**

**Tenant ID :**

(usually something ending with onmicrosoft.com)

   e) In the Subject DN, select common name and other required attributes.

   f) In the SubjectAltName, select UPN and Email as required. Please note that if you select both, the Email will be taken as the SeatID. (Ensure that this matches the Intune profile configuration as detailed in the next steps).



**Subject DN**

**Common Name (CN)**
Source: Scep Request
Required: Yes

**Organizational Unit (OU)**
Source: Fixed value
Value: VPN-WEB

**Organizational Unit (OU)**
Source: Fixed value
Value: MULTI-ALLOWED

Add, move, and remove the fields that you want to appear in the certificate.

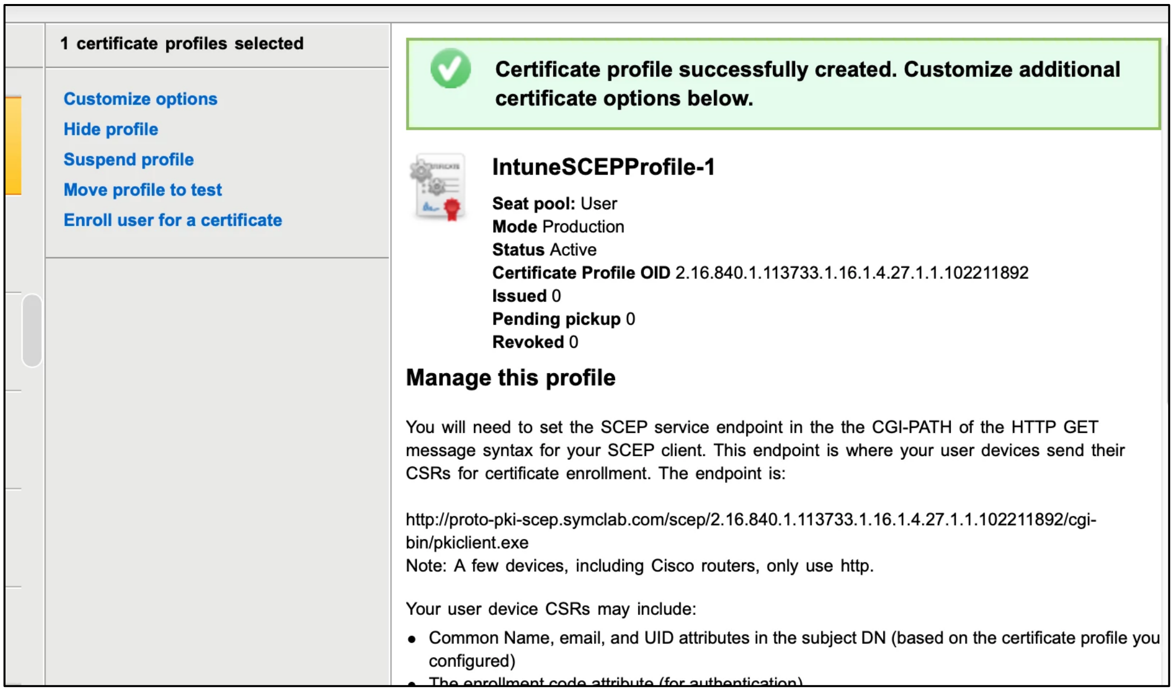
**SubjectAltName**

**Other Name (UPN)**
Source: Scep Request
Required: Yes

Add, move, and remove the fields that you want to appear in the certificate.

g) Keep all the other attributes as is and then save the profile.

h) Make a note of the **SCEP URL** displayed (without the "/pkiclient.exe" suffix[1]), as it is required in the next steps for configuring Intune profiles.



**Certificate profile successfully created. Customize additional certificate options below.**

**IntuneSCEPProfile-1**

**Seat pool:** User
**Mode** Production
**Status** Active
**Certificate Profile OID** 2.16.840.1.113733.1.16.1.4.27.1.1.102211892
**Issued** 0
**Pending pickup** 0
**Revoked** 0

**Manage this profile**

You will need to set the SCEP service endpoint in the the CGI-PATH of the HTTP GET message syntax for your SCEP client. This endpoint is where your user devices send their CSRs for certificate enrollment. The endpoint is:

http://proto-pki-scep.symclab.com/scep/2.16.840.1.113733.1.16.1.4.27.1.1.102211892/cgi-bin/pkiclient.exe
Note: A few devices, including Cisco routers, only use http.

Your user device CSRs may include:

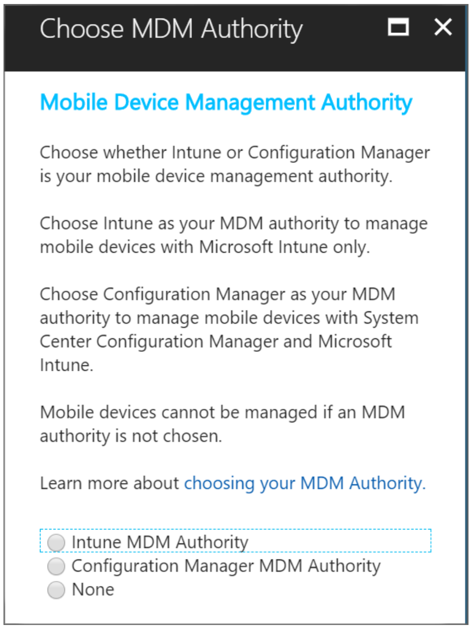
- Common Name, email, and UID attributes in the subject DN (based on the certificate profile you configured)
- The enrollment code attribute (for authentication)

[1] This is ONLY required for Windows 10 profiles. All other platforms (iOS, Android, macOS) require the full SCEP Server URL displayed on the certificate profile.

Once the certificate profile configuration on DigiCert PKI Platform is complete, the following Intune configuration steps are needed:

## Step 3: Configure Intune

1. Login to https://endpoint.microsoft.com, select the orange banner to open the Mobile Device Management Authority setting. The orange banner is only displayed if you haven't yet set the MDM authority. Under Mobile Device Management Authority, choose your MDM authority as "Intune MDM Authority".



Choose MDM Authority

Mobile Device Management Authority

Choose whether Intune or Configuration Manager is your mobile device management authority.

Choose Intune as your MDM authority to manage mobile devices with Microsoft Intune only.

Choose Configuration Manager as your MDM authority to manage mobile devices with System Center Configuration Manager and Microsoft Intune.

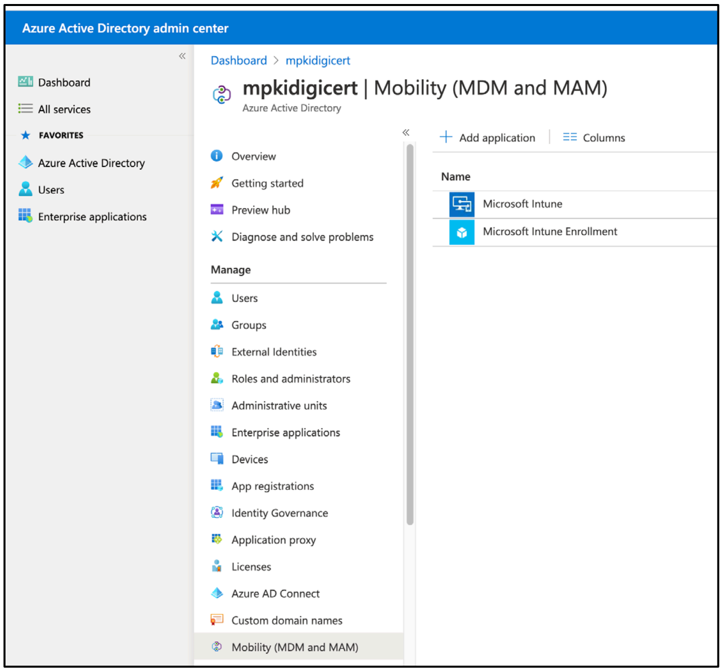
Mobile devices cannot be managed if an MDM authority is not chosen.

Learn more about choosing your MDM Authority.

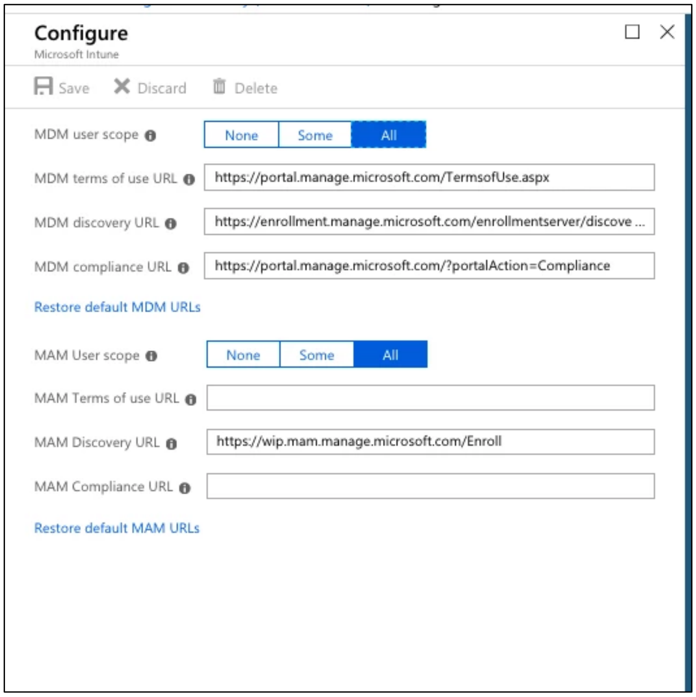
○ Intune MDM Authority
○ Configuration Manager MDM Authority
○ None

2. For Windows 10 device (machine) enrollments - Mobility Management should be set to "**All**" so that all types of users and devices are managed by Intune MDM.

3. Navigate to "**Azure Directory Services**" on Azure portal and then select Mobility (**MDM AND MAM**). Once there, select "**Microsoft Intune**".



4. In the next configuration page, select “All” for both MDM and MAM sections and leave the rest to be default values. Click on “Save”.



MDM user scope: None | Some | [✓ All]

MDM terms of use URL: https://portal.manage.microsoft.com/TermsofUse.aspx

MDM discovery URL: https://enrollment.manage.microsoft.com/enrollmentserver/discove ...

MDM compliance URL: https://portal.manage.microsoft.com/?portalAction=Compliance

MAM User scope: None | Some | [✓ All]

MAM Terms of use URL:

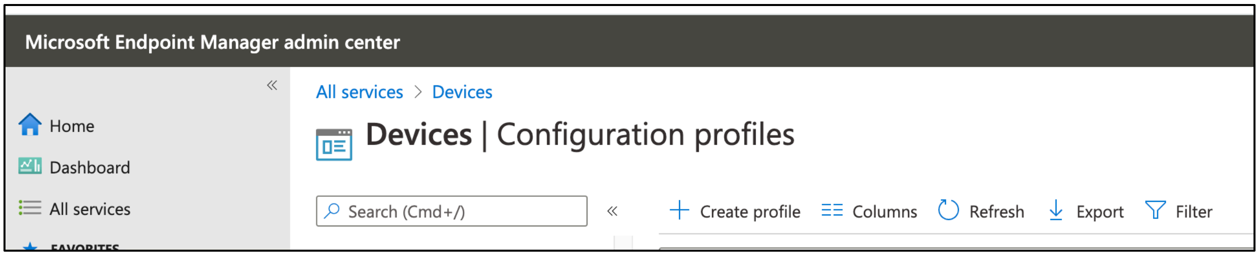
MAM Discovery URL: https://wip.mam.manage.microsoft.com/Enroll

MAM Compliance URL:

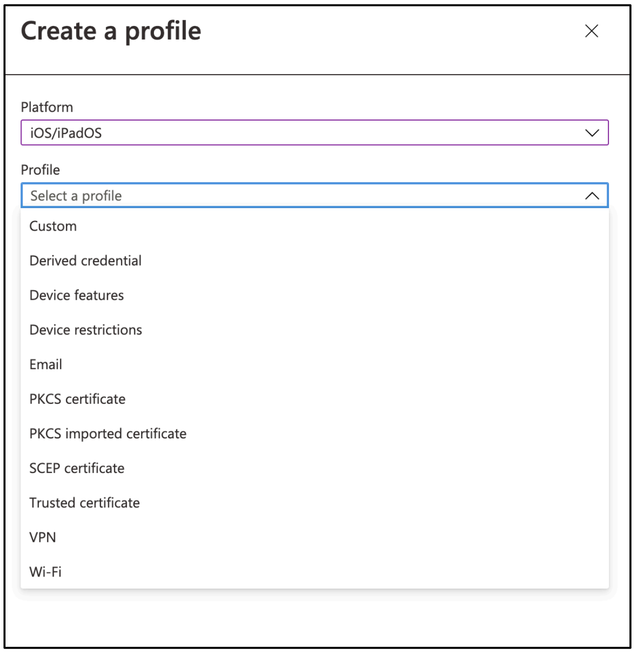
5. Once MDM authority is set, we will be configuring two profiles per device type (iOS and Android), i.e. one profile for the CA certificate and one profile for the end entity certificate.

## Profile - 1: Creating “Trusted Certificate” Profile

1. Sign in at https://endpoint.microsoft.com/
2. Select **Devices** > **Configuration profiles** > **Create profile**.



3. Select the Platform of the device that will receive the profile and Select **Trusted certificate** from Profile dropdown list.



Create a profile

Platform: iOS/iPadOS

Profile: Select a profile

4. Select **Create**.
5. In **Basics**, enter Name and Description for the profile.
6. Select **Next**.
7. In **Configuration settings**, specify the .cer file for the trusted Root CA Certificate that was downloaded earlier (Refer to: Obtain a Trusted Root certificate).

   For Windows 8.1 and Windows 10 devices only, select the **Destination Store** for the trusted certificate from:

a) Computer certificate store - Root

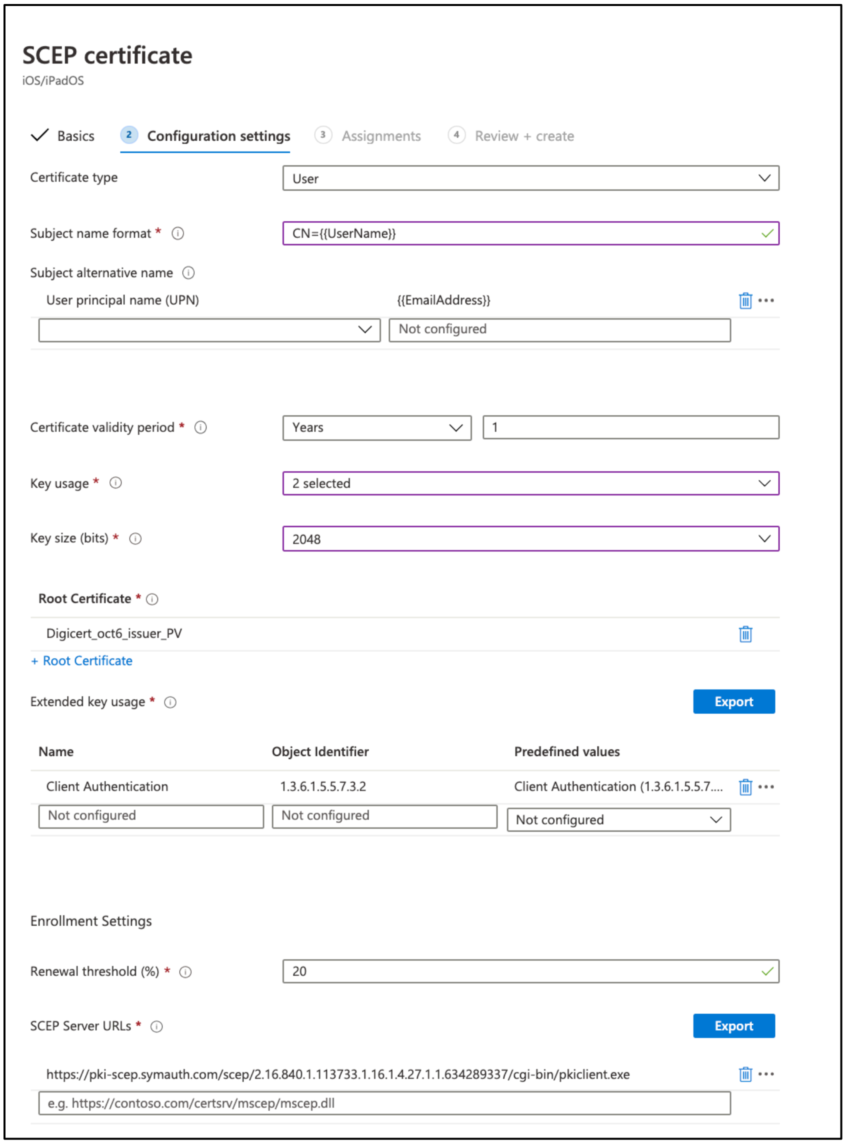
b) Computer certificate store - Intermediate

c) User certificate store - Intermediate

8. Select **Next**.
9. In **Scope tags** (optional) tab, Select **Next**.
10. In **Assignments**, select the user or groups that will receive your profile
11. (*Applies to Windows 10 only*) In **Applicability Rules**, specify applicability rules to refine the assignment of this profile. You can choose to assign or not assign the profile based on the OS version of a device.
12. In **Review + create**, review your settings. When you select Create, your changes are saved, and the profile is assigned.

### Profile - 2: Creating a SCEP Profile

1. Sign in at https://endpoint.microsoft.com.
2. Navigate to **Devices** > **Configuration profiles** > **Create profile**.
3. Select the Platform of the device that will receive the profile and Select **SCEP certificate** from Profile dropdown list.
4. Click **Create**.
5. In **Basics**, enter Name and Description for the profile.
6. Click **Next**.
7. In Configuration Settings, provide corresponding certificate attributes as per the certificate profile you would have configured in PKI Manager in Step 2 above.



SCEP certificate

iOS/iPadOS

✓ Basics | 2 Configuration settings | 3 Assignments | 4 Review + create

Certificate type: User

Subject name format *: CN={{UserName}}

Subject alternative name

| | |
|---|---|
| User principal name (UPN) | {{EmailAddress}} |
| | Not configured |

Certificate validity period *: Years | 1

Key usage *: 2 selected

Key size (bits) *: 2048

Root Certificate *

Digicert_oct6_issuer_PV

+ Root Certificate

Extended key usage * — Export

| Name | Object Identifier | Predefined values |
|---|---|---|
| Client Authentication | 1.3.6.1.5.5.7.3.2 | Client Authentication (1.3.6.1.5.5.7.... |
| Not configured | Not configured | Not configured |

Enrollment Settings

Renewal threshold (%) *: 20

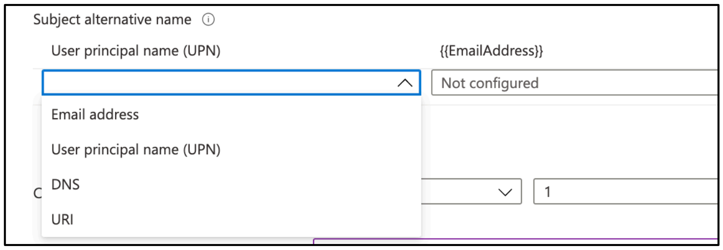
SCEP Server URLs * — Export

https://pki-scep.symauth.com/scep/2.16.840.1.113733.1.16.1.4.27.1.1.634289337/cgi-bin/pkiclient.exe

e.g. https://contoso.com/certsrv/mscep/mscep.dll

a) **For Subject name format** - Provide the CN format chosen in DigiCert's PKI Manager (usually email or firstname / lastname or similar).

b) For SAN, select the options that correspond with the DigiCert certificate profile configuration, being either UPN/Email or both.

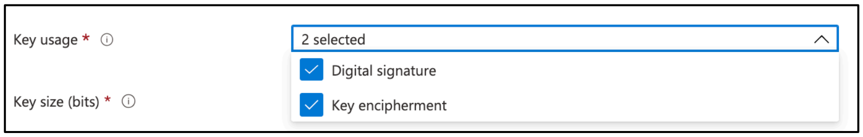


Subject alternative name

User principal name (UPN) — {{EmailAddress}}

Not configured

- Select Key usage (usually both)



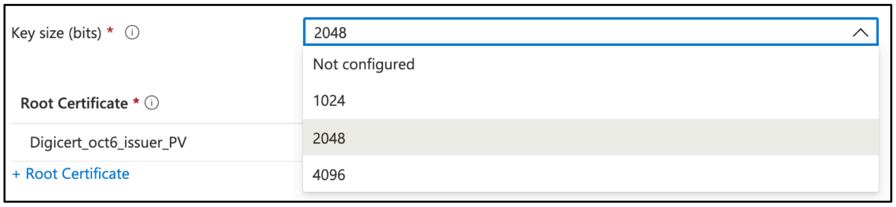
Key usage * ⓘ: 2 selected

☑ Digital signature

☑ Key encipherment

Key size (bits) * ⓘ

- Select Key size

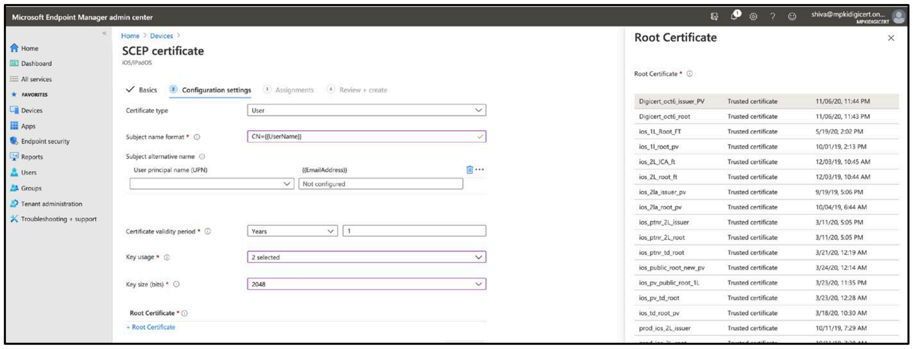


Key size (bits) * ⓘ: 2048

Root Certificate * ⓘ

Digicert_oct6_issuer_PV

- **For Root certificate** -When you create an end entity certificate profile (eg SCEP certificate) - select the most immediate issuing CA as the root certificate property.



SCEP certificate

iOS/iPadOS

Certificate type: User

Subject name format * ⓘ CN={{UserName}}

Subject alternative name ⓘ

User principal name (UPN) {{EmailAddress}}

Not configured

Certificate validity period * ⓘ: Years 1

Key usage * ⓘ: 2 selected

Key size (bits) * ⓘ: 2048

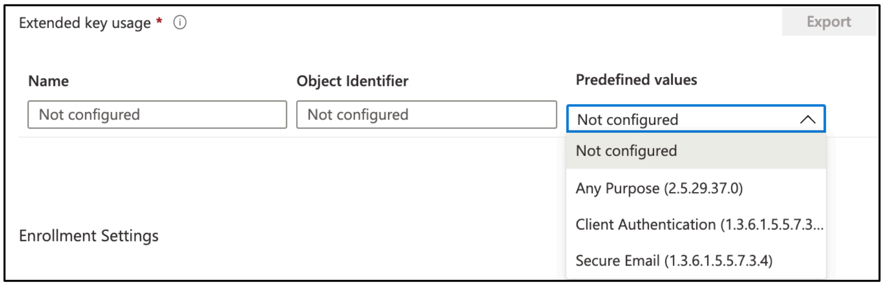
Root Certificate * ⓘ

Root Certificate

Root Certificate * ⓘ

| | | |
|---|---|---|
| Digicert_oct6_issuer_PV | Trusted certificate | 11/06/20, 11:44 PM |
| Digicert_oct6_root | Trusted certificate | 11/06/20, 11:43 PM |
| ios_1L_Root_FT | Trusted certificate | 5/19/20, 2:02 PM |
| ios_1l_root_pv | Trusted certificate | 10/01/19, 2:13 PM |
| ios_2L_ICA_ft | Trusted certificate | 12/03/19, 10:45 AM |
| ios_2L_root_ft | Trusted certificate | 12/03/19, 10:44 AM |
| ios_2la_issuer_pv | Trusted certificate | 9/19/19, 5:06 PM |
| ios_2la_root_pv | Trusted certificate | 10/04/19, 6:44 AM |
| ios_ptnr_2L_issuer | Trusted certificate | 3/11/20, 5:05 PM |
| ios_ptnr_2L_root | Trusted certificate | 3/11/20, 5:05 PM |
| ios_ptnr_td_root | Trusted certificate | 3/21/20, 12:19 AM |
| ios_public_root_new_pv | Trusted certificate | 3/24/20, 12:14 AM |
| ios_pv_public_root_1L | Trusted certificate | 3/23/20, 11:35 PM |
| ios_pv_td_root | Trusted certificate | 3/23/20, 12:28 AM |
| ios_td_root_pv | Trusted certificate | 3/18/20, 10:30 AM |
| prod_ios_2L_issuer | Trusted certificate | 10/11/19, 7:29 AM |

- Select **EKU as required** - (Usually client authentication for VPN profiles).



Extended key usage * ⓘ

| Name | Object Identifier | Predefined values |
|---|---|---|
| Not configured | Not configured | Not configured |

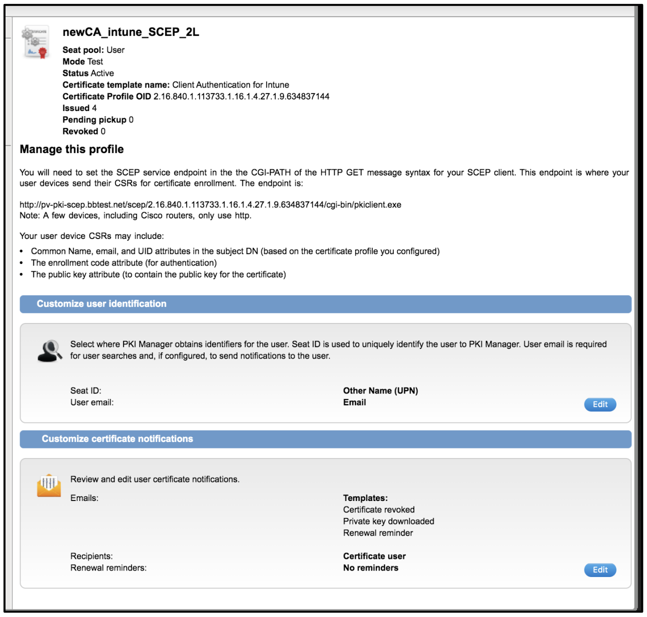
Not configured
Any Purpose (2.5.29.37.0)
Client Authentication (1.3.6.1.5.5.7.3...
Secure Email (1.3.6.1.5.5.7.3.4)

Enrollment Settings

8. In Enrollment settings > **Renewal Threshold (%),** leave the default value set to 20%, which means the renewal of the certificate will be attempted when the certificate reaches 80% of its validity period.

9. For SCEP Server URLs, provide the SCEP URL which was copied when the certificate profile was created in DigiCert PKI Platform (Refer: Step 2).

NOTE: The SCEP URL must be https:// (http URLs will not work)



**newCA_intune_SCEP_2L**

**Seat pool:** User
**Mode** Test
**Status** Active
**Certificate template name:** Client Authentication for Intune
**Certificate Profile OID** 2.16.840.1.113733.1.16.1.4.27.1.9.634837144
**Issued** 4
**Pending pickup** 0
**Revoked** 0

**Manage this profile**

You will need to set the SCEP service endpoint in the the CGI-PATH of the HTTP GET message syntax for your SCEP client. This endpoint is where your user devices send their CSRs for certificate enrollment. The endpoint is:

http://pv-pki-scep.bbtest.net/scep/2.16.840.1.113733.1.16.1.4.27.1.9.634837144/cgi-bin/pkiclient.exe
Note: A few devices, including Cisco routers, only use http.

Your user device CSRs may include:

- Common Name, email, and UID attributes in the subject DN (based on the certificate profile you configured)
- The enrollment code attribute (for authentication)
- The public key attribute (to contain the public key for the certificate)

**Customize user identification**

Select where PKI Manager obtains identifiers for the user. Seat ID is used to uniquely identify the user to PKI Manager. User email is required for user searches and, if configured, to send notifications to the user.

Seat ID: **Other Name (UPN)**
User email: **Email**

**Customize certificate notifications**

Review and edit user certificate notifications.

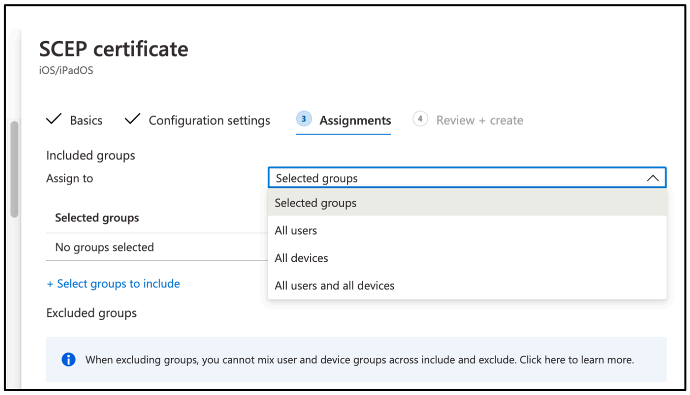
Emails: **Templates:**
Certificate revoked
Private key downloaded
Renewal reminder

Recipients: **Certificate user**
Renewal reminders: **No reminders**

a) Provide the **SCEP URL**, without the "/pkiclient.exe" suffix, and click "Add". e.g. https://proto-pki-scep.symauth.com/scep/2.16.840.1.113733.1.16.1.2.3.1.1/cgi-bin

b) Click **Next.**

10. In **Assignments**, select the user or groups that will receive your profile and click **Next.**



**SCEP certificate**
iOS/iPadOS

Included groups

Assign to: Selected groups

**Selected groups**

No groups selected

Excluded groups

When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more.

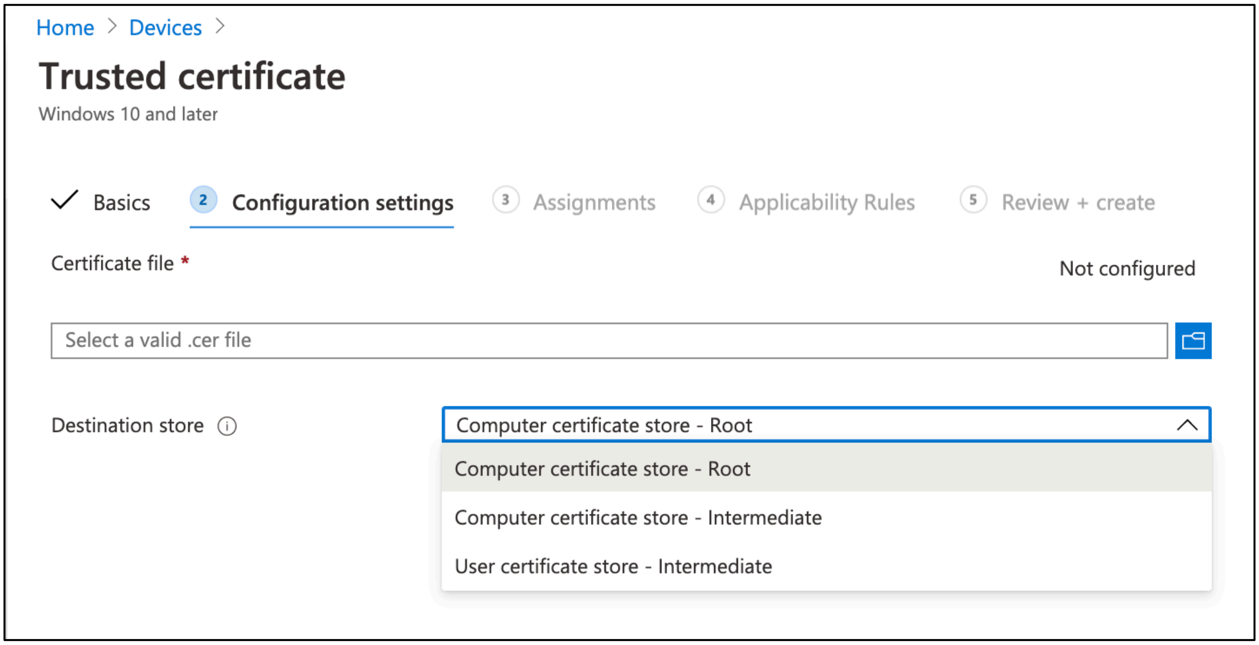
11. In **Review + create**, review your settings. When you click create, your profile is saved and assigned to the selected user or groups.

12. Once the profiles are created and assigned, you can start enrolling devices through Intune.

## Windows Machine enrollment

1. Select platform as Windows 10 or later (for Windows 10). For earlier windows, select Windows 8.1 or later.

2. In the Trusted profile configuration, you would also need to select the appropriate keystore (MMC trust store) - where certificates will be saved once it is deployed.



Home > Devices >

Trusted certificate

Windows 10 and later

✓ Basics | 2 Configuration settings | 3 Assignments | 4 Applicability Rules | 5 Review + create

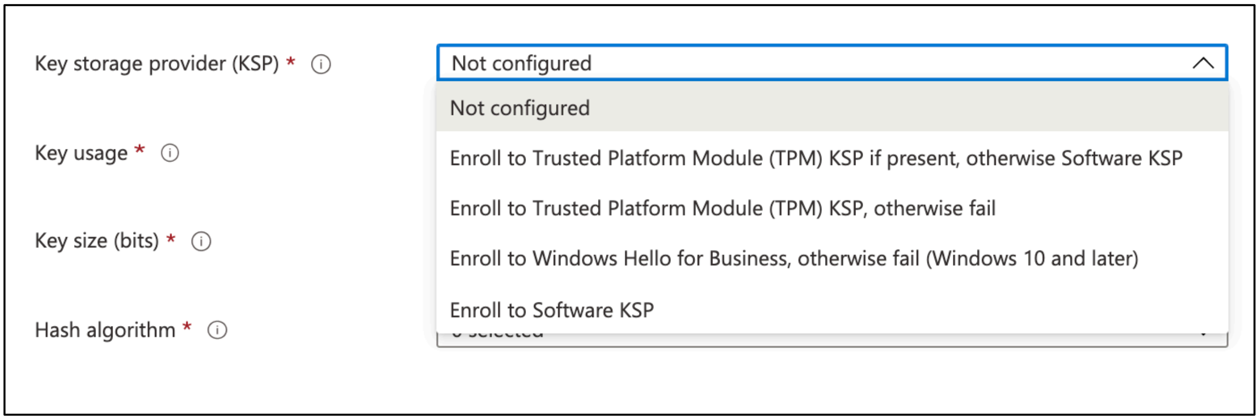
Certificate file * — Not configured

Select a valid .cer file

Destination store ⓘ — Computer certificate store - Root

- Computer certificate store - Root
- Computer certificate store - Intermediate
- User certificate store - Intermediate

3. For Windows enrollment, in SCEP certificate profile, you would also need to choose appropriate KSP (choose “Enroll to Software KSP” if no specific TPM requirements).



Key storage provider (KSP) * ⓘ — Not configured

- Not configured
- Enroll to Trusted Platform Module (TPM) KSP if present, otherwise Software KSP
- Enroll to Trusted Platform Module (TPM) KSP, otherwise fail
- Enroll to Windows Hello for Business, otherwise fail (Windows 10 and later)
- Enroll to Software KSP

Key usage * ⓘ

Key size (bits) * ⓘ

Hash algorithm * ⓘ — 0 selected

Now we have completed steps to:

1. Register the application and create an application id, application key and tenant id on Intune and use these values to configure the DigiCert certificate profile. (Step 1).

2. Configure the Microsoft Intune. (Step 3).
3. Create certificate profile for VPN-BCT using the BCT i.e. “Client Authentication for Intune-SCEP” loaded to the account and save the SCEP URL. (Step 2).
4. Create Intune profiles for Trusted certificate and SCEP certificate and assign these to respective devices. (Profile 1 and Profile 2).

Next steps are:

E. Once the admin completes assigning profiles for the devices, the next step for you as a user is to enroll the device. For Apple device enrollment, refer Appendix-B.

F. After enrollment for the device is completed, you can install the Company Portal App on the device. This is done to install the profile and generate the certificate on the device. For more information, refer Appendix-C.

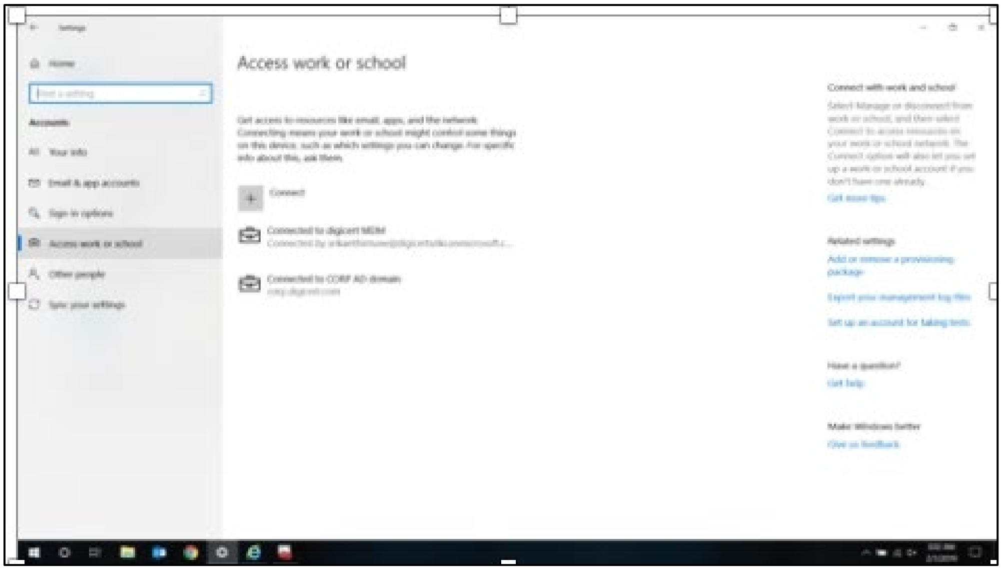
G. Once the profile is installed and the certificate is generated on the device, you can start deploying the profiles. For more information, refer Appendix-D.

H. After the profiles are deployed, you must validate the certificate issuance details in DigiCert PKI Platform. For more information, refer Appendix-E.

## Windows Machine Enrollment Steps

To enroll a windows machine to Intune:

1. Login to the Windows platform (device/machine).
2. Go to <**Star**t> - **Settings** – **Accounts**.
3. In the Accounts details, you will see the current account that you would have logged into.
4. Click on the "**Access work or school**" link on the left menu.



Settings

Home

Find a setting

Accounts

Your info

Email & app accounts

Sign-in options

Access work or school

Other people

Sync your settings

Access work or school

Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

Connect

Connected to digicert MDM
Connected by [illegible]

Connected to CORP AD domain
corp.digicert.com

Connect with work and school

Select Manage or disconnect from work or school, and then select Connect to access resources on your work or school network. The Connect option will also let you set up a work or school account if you don't have one already.

Get more tips

Related settings

Add or remove a provisioning package

Export your management log files

Set up an account for taking tests

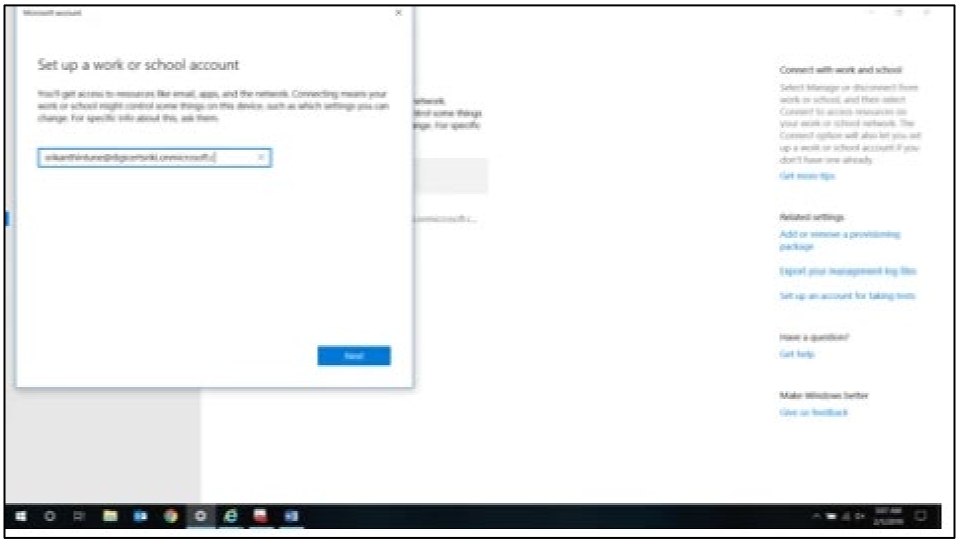
Have a question?

Get help

Make Windows better

Give us feedback

5. Login using your Azure portal credentials and the machine will be enrolled to be managed by MDM.



Microsoft account

Set up a work or school account

You'll get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

[illegible]

Next

Connect with work and school

Select Manage or disconnect from work or school, and then select Connect to access resources on your work or school network. The Connect option will also let you set up a work or school account if you don't have one already.

Get more tips

Related settings

Add or remove a provisioning package

Export your management log files

Set up an account for taking tests

Have a question?

Get help

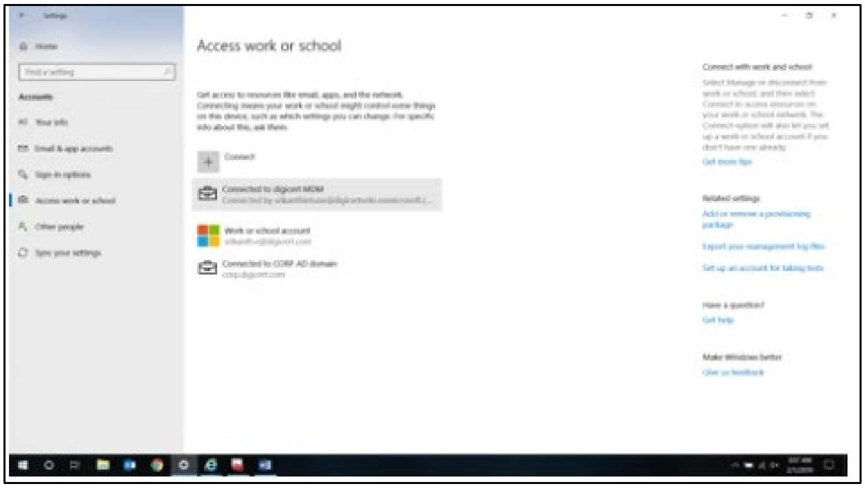
Make Windows better

Give us feedback

6. After some time (up to a few minutes), the applications, settings and profiles will be synced to the machine from the MDM.

7. Once enrolled, you can see the Azure account displayed on the "Access work or school" section along with other account(s).

8. To view the information of the Azure account, click on the account name and click on "Info".



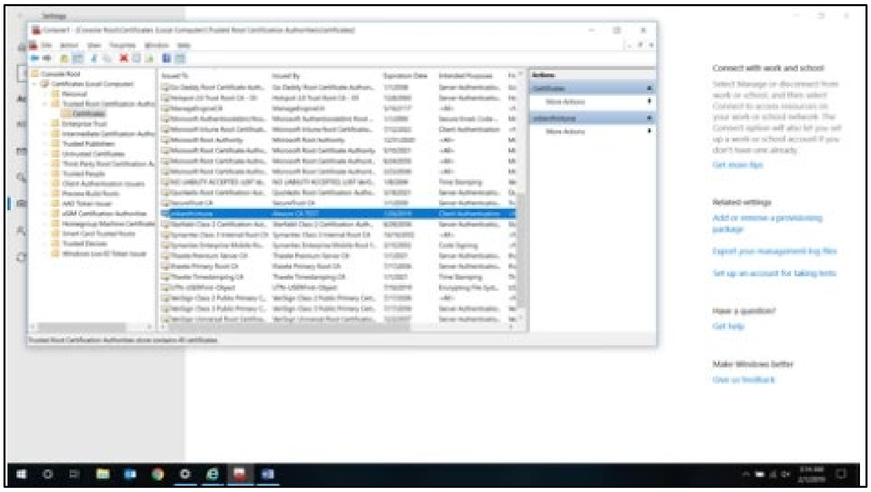
Access work or school

Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

9. To view the certificate issued to the machine, launch mmc.exe and add the “Certificates” snap-in (From File > Add/Remove Snap-Ins).

10. Once in mmc, select certificates and click on **Trusted Root Certification Authorities** to view Root CA certs, **Intermediate Certification Authorities** to view ICA and **Personal** section to see end entity certificates.

    (Please note that this is based on the store that was selected on Microsoft Endpoint Manager while creating profiles for Windows platform).



## Integrate Intune MDM Solution via Device Authentication

This section of the guide includes the steps to integrate Intune using “**Generic Device Authentication for Intune**” certificate template for SCEP and PKI Web Services.

# SCEP Integration

To integrate Intune using "**Generic Device Authentication for Intune**" certificate template via SCEP, follow the below steps:

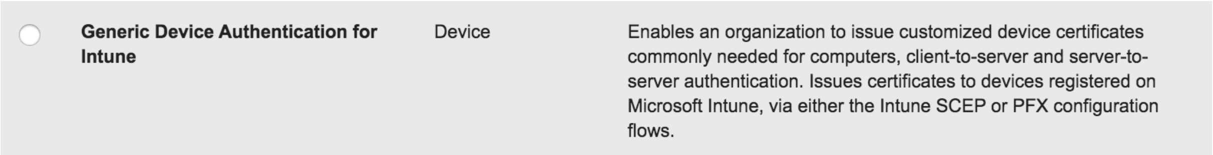
## Registering the Client Application.

Refer: Register the Client Application4

## Create a SCEP URL

1. Create a profile in DigiCert PKI Platform and make note of the SCEP URL for the profile.

   a) Create a profile using the **Generic Device Authentication for Intune** template.



| | | | |
|---|---|---|---|
| ○ | **Generic Device Authentication for Intune** | Device | Enables an organization to issue customized device certificates commonly needed for computers, client-to-server and server-to-server authentication. Issues certificates to devices registered on Microsoft Intune, via either the Intune SCEP or PFX configuration flows. |

NOTE:

- If you do not see this profile, contact support to have it added to your account.
- Please note that the certificate template "**Generic Device Authentication for Intune**" supports Intune Integration in MacOS as well.
- For "**Device**" certificate type, the SAN types supported are Email address, UPN and DNS.
  (Please note this must match the Intune profile configuration as detailed in the next steps).

For detailed steps, please refer to Create SCEP URL from the previous section.

*Table 1.2: Supported Matrix of certificate fields: DigiCert PKI Platform solution vs Intune*

| Certificate Profile Field | DigiCert PKI Platform Certificate Attribute Name | Intune Support |
|---|---|---|
| Subject Alternative Name (SAN) | DNS Name | Supported (Device only) |
| | RFC822 Name | Supported |
| | User Principal Name | Supported |
| | Directory name | Not supported |
| | IP Address | Not supported |
| | Other Name (GUID) | Not supported |
| | Registered ID | Not supported |
| | Uniform Resource Locator (URI) | Not supported |

## Configure Intune

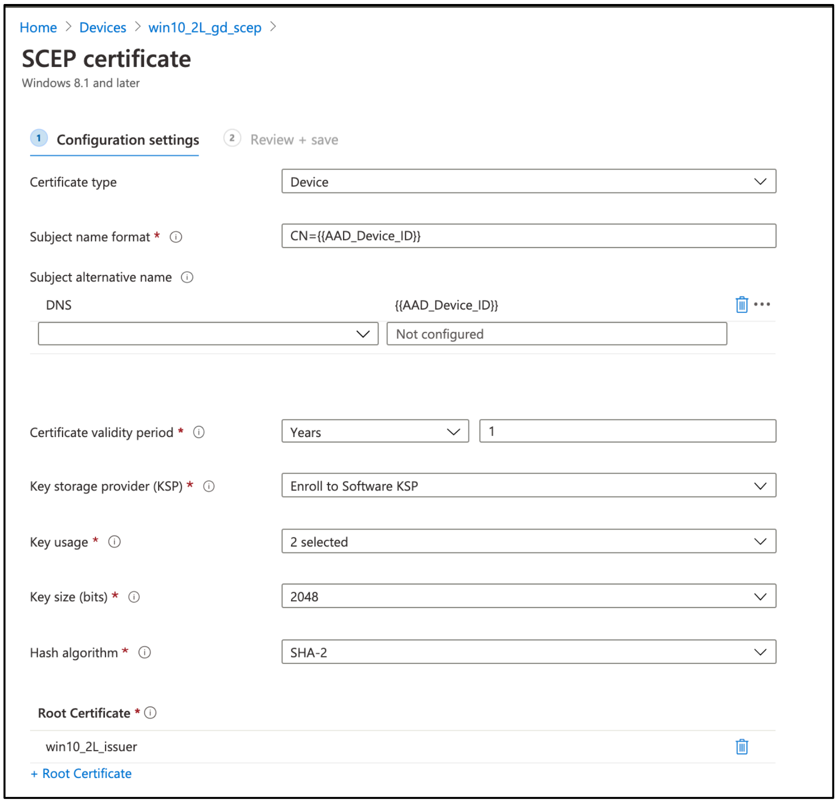
Follow the steps provided in the section “Configure Intune”.

### Profile -1: Creating “Trusted Certificate” Profile

Refer to the steps provided in the section: Create “Trusted Certificate” Profile

### Profile -2: Creating a SCEP Profile

Refer to the steps provided in the section: Creating SCEP Profile



SCEP certificate

Windows 8.1 and later

Certificate type: Device

Subject name format *: CN={{AAD_Device_ID}}

Subject alternative name

| | |
|---|---|
| DNS | {{AAD_Device_ID}} |
| | Not configured |

Certificate validity period *: Years 1

Key storage provider (KSP) *: Enroll to Software KSP

Key usage *: 2 selected

Key size (bits) *: 2048

Hash algorithm *: SHA-2

Root Certificate *

win10_2L_issuer

**NOTE:** For Windows, if you select the **Certificate Type**: Device, then the Certificate will reside in the Certificates folder under Local computer.

## PKI Web Services Integration

This section explains the steps to integrate Intune using "**Generic Device Authentication for Intune**" certificate template via PKI Web Services.
For detailed steps, please refer below:

Step 1: Generate a DigiCert Registration Authority Certificate

Step 2: Create a Certificate Profile in DigiCert PKI Platform (Select the certificate template as "**Generic Device Authentication for Intune**")

Step 3: Set up the Microsoft Intune Connector

Step 4: Install and Configure the Microsoft Intune Connector

Step 5: Create a Trusted Certificate Profile in Microsoft Intune

Step 6: Create a PKCS Certificate Profile in Microsoft Intune

Step 7: Assign Profiles for Android/iOS/Windows

# Integrate Intune MDM Solution for S/MIME (signing only)

This section of the guide explains the steps to integrate Intune using "S/MIME (Digital Signature only) for Intune" certificate template for SCEP and PKI Web Services.

## SCEP Integration

To integrate Intune using "S/MIME (Digital Signature only) for Intune" certificate template via SCEP, follow the below steps:

Step 1: Register the Client Application

Step 2: Create a SCEP URL.

Step 3: Configure Intune

Profile -1: Create "Trusted Certificate" Profile

Profile -2: Create SCEP Profile

## PKI Web Services Integration

This section explains the steps to integrate Intune using "S/MIME (Digital Signature only) for Intune" certificate template via PKI Web Services.
For detailed steps, please refer below:

Step 1: Generate a DigiCert Registration Authority Certificate

Step 2: Create a Certificate Profile in DigiCert PKI Platform (Select the certificate template as "S/MIME (Digital Signature only) for Intune")

Step 3: Set up the Microsoft Intune Connector

Step 4: Install and Configure the Microsoft Intune Connector

Step 5: Create a Trusted Certificate Profile in Microsoft Intune

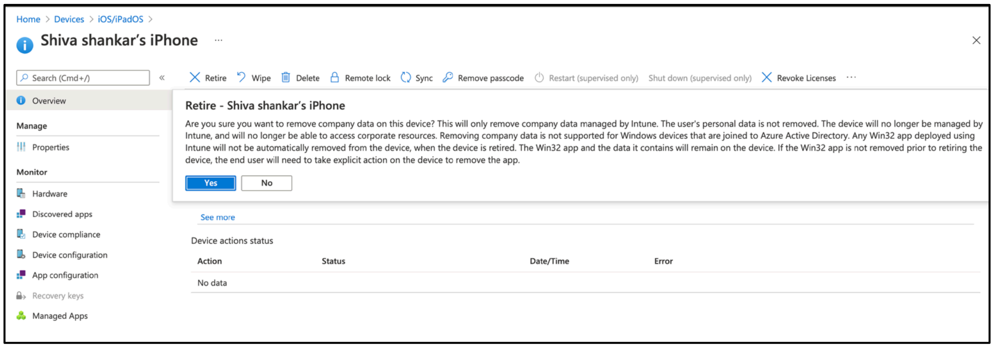
Step 6: Create a PKCS Certificate Profile in Microsoft Intune

Step 7: Assign Profiles for Android/iOS/Windows

## Revocation of Certificates in Intune

Certificates can be revoked in various ways. This section details the steps for one of the possible revocation flows (e.g. ‘retiring a device’) initiated by Intune Administrators:

1. Login to https://endpoint.microsoft.com/
2. Navigate to **Devices** > **All devices**
3. Click on the target device and click on the **Retire** action:



Retire - Shiva shankar’s iPhone

Are you sure you want to remove company data on this device? This will only remove company data managed by Intune. The user's personal data is not removed. The device will no longer be managed by Intune, and will no longer be able to access corporate resources. Removing company data is not supported for Windows devices that are joined to Azure Active Directory. Any Win32 app deployed using Intune will not be automatically removed from the device, when the device is retired. The Win32 app and the data it contains will remain on the device. If the Win32 app is not removed prior to retiring the device, the end user will need to take explicit action on the device to remove the app.

Device actions status

| Action | Status | Date/Time | Error |
|---|---|---|---|
| No data | | | |

4. Click **Yes** on the confirmation dialog which initiates the retire process.
5. All the certificates bound to that device will be added to the revocation list by Intune.
6. DigiCert PKI Platform will fetch the revocation list for all the tenants at a frequent interval, as part of an asynchronous process, which will revoke all the certificates from the retrieved list.

   The updated status of the certificate will be available via DigiCert’s validation services (CRL/OCSP), once the revocation process is complete.

# Appendix

The below sections are applicable to both the Web Services and SCEP integration.

## Appendix-A. Generating a DigiCert Registration Authority Certificate using OpenSSL

Intune acts as a Registration Authority while requesting for certificates for DigiCert PKI Platform. To configure Intune as a Registration Authority (RA), you must generate a DigiCert Registration Authority Certificate.

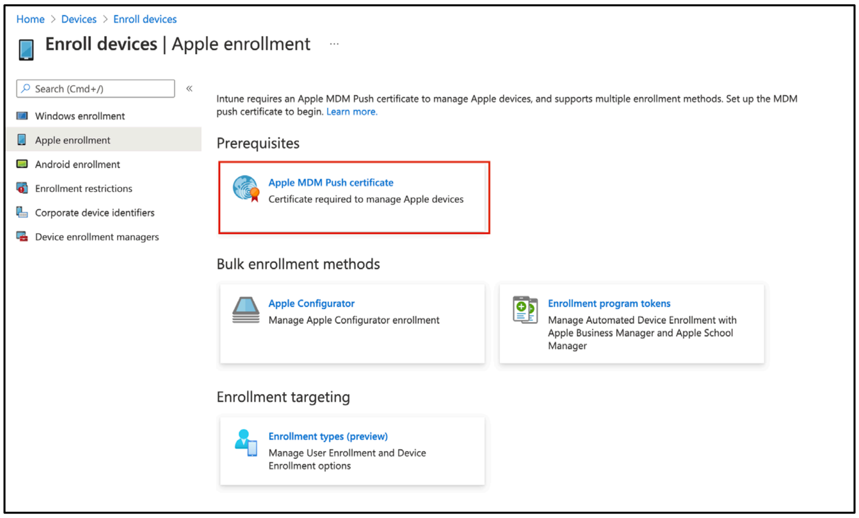
Follow the steps to generate the DigiCert RA certificate:

1. openssl req -new -newkey rsa:2048 -nodes -keyout priv.key -out request.csr
2. Log in to DigiCert PKI Manager.
3. In the **PKI Manager** dashboard, click the **Tasks** icon and select **Get an RA Certificate**.
4. Paste the content from the CSR you created earlier.
5. Specify a certificate friendly name and click **Continue**.
6. Click **Download** and download the RA certificate (RA-Certificate.p7b).
7. openssl pkcs7 -print_certs -in RA-Certificate.p7b -out cerfile.cer
8. openssl pkcs12 -export -out RA-Cert.pfx -inkey priv.key -in certfile.cer.

# Appendix-B. Apple Enrollment for iOS

1. If not already associated with the Apple certificate for your Apple id, Login to https://endpoint.microsoft.com/ and Choose Devices > Enroll devices > Apple enrollment  (for iPhone).

2. Click on "**Apple MDM Push Certificate**".


Home > Devices > Enroll devices
Enroll devices | Apple enrollment ...
Search (Cmd+/)
Windows enrollment
Apple enrollment
Android enrollment
Enrollment restrictions
Corporate device identifiers
Device enrollment managers
Prerequisites
Apple MDM Push certificate
Bulk enrollment methods
Apple Configurator
Enrollment program tokens
Enrollment targeting
Enrollment types (preview)

Intune requires an Apple MDM Push certificate to manage Apple devices, and supports multiple enrollment methods. Set up the MDM push certificate to begin. Learn more.

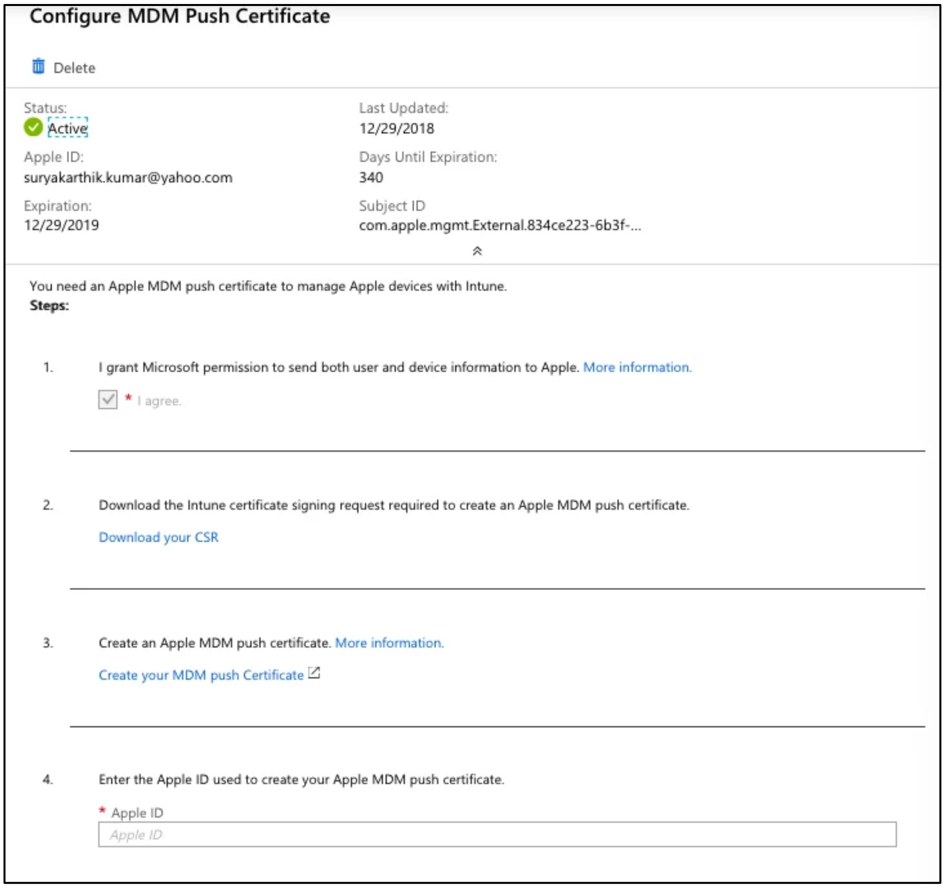
Certificate required to manage Apple devices

Manage Apple Configurator enrollment

Manage Automated Device Enrollment with Apple Business Manager and Apple School Manager

Manage User Enrollment and Device Enrollment options

3. If you have already configured an Apple id for use, it will show the details on this page. Otherwise, proceed to download the CSR and then click the "**Create your MDM push certificate**" **link**.



Configure MDM Push Certificate

Delete

Status:
Active

Last Updated:
12/29/2018

Apple ID:
suryakarthik.kumar@yahoo.com

Days Until Expiration:
340

Expiration:
12/29/2019

Subject ID
com.apple.mgmt.External.834ce223-6b3f-...

You need an Apple MDM push certificate to manage Apple devices with Intune.
**Steps:**

1. I grant Microsoft permission to send both user and device information to Apple. More information.

   ☑ * I agree.

2. Download the Intune certificate signing request required to create an Apple MDM push certificate.

   Download your CSR

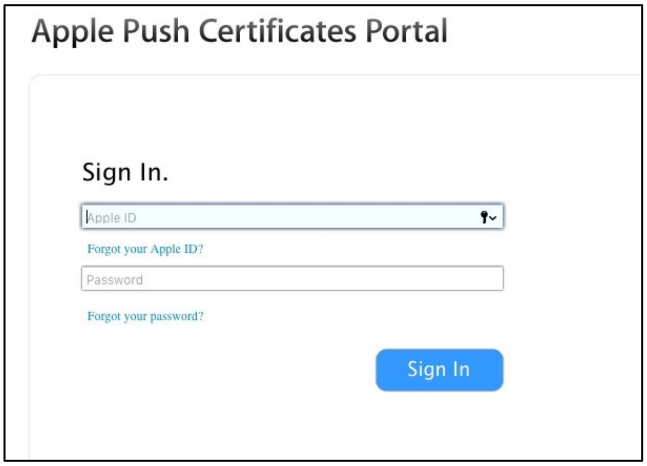
3. Create an Apple MDM push certificate. More information.

   Create your MDM push Certificate

4. Enter the Apple ID used to create your Apple MDM push certificate.

   * Apple ID
   Apple ID

4. Clicking on "Create your MDM push certificate" will take you to an Apple login screen where you need to login with your Apple ID and password.



Apple Push Certificates Portal

Sign In.

Apple ID

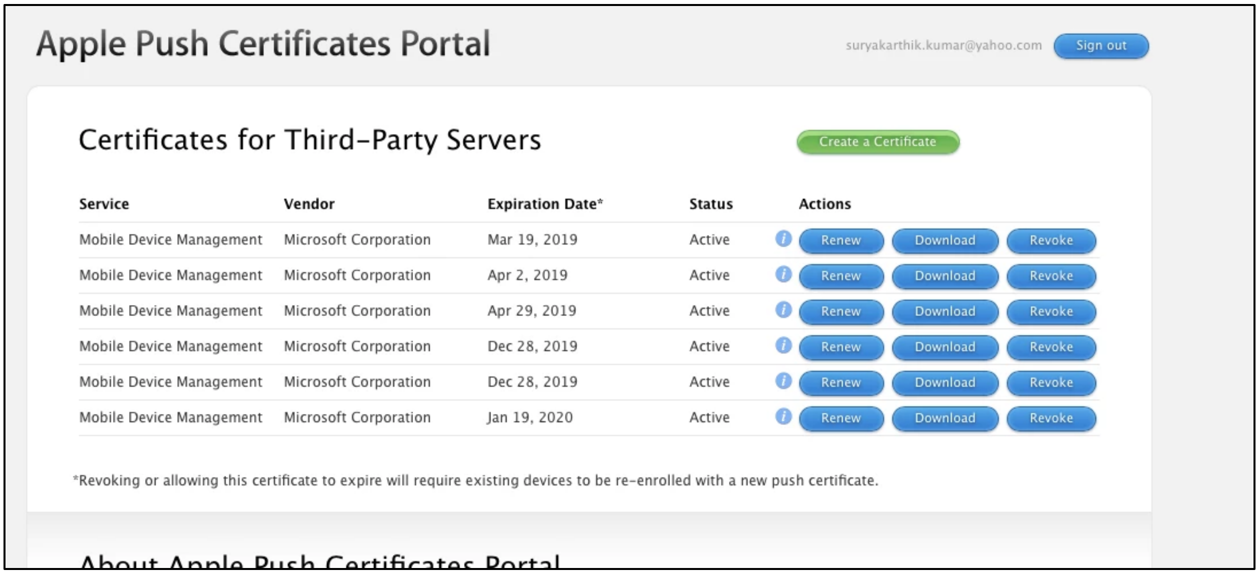
Forgot your Apple ID?

Password

Forgot your password?

Sign In

5. Once logged in, click on “Create certificate”.



Apple Push Certificates Portal

suryakarthik.kumar@yahoo.com

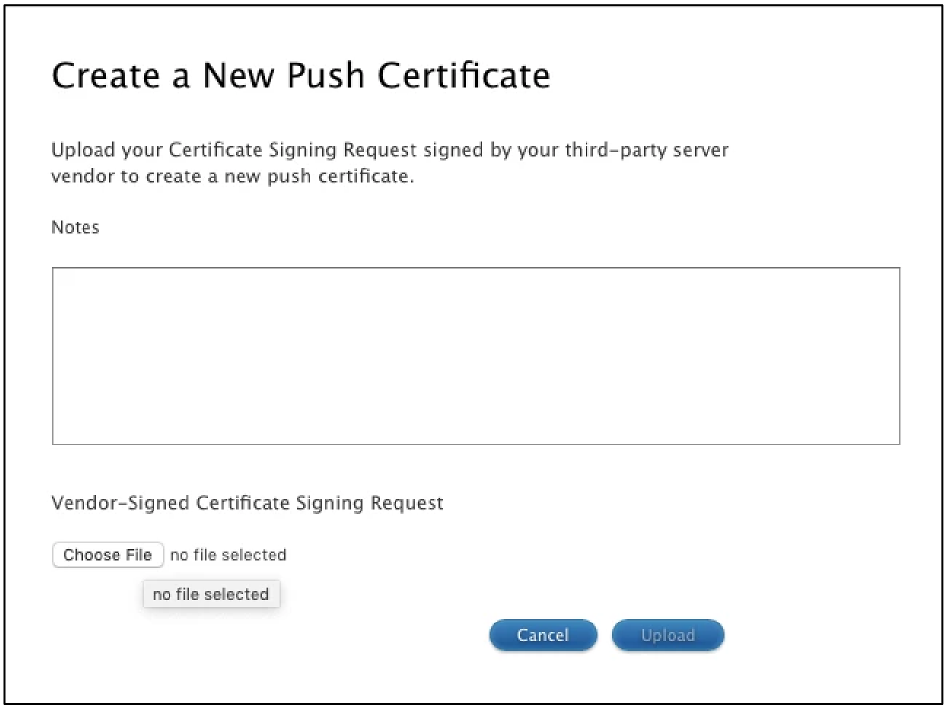
Certificates for Third-Party Servers

| Service | Vendor | Expiration Date* | Status | Actions |
|---|---|---|---|---|
| Mobile Device Management | Microsoft Corporation | Mar 19, 2019 | Active | ⓘ Renew Download Revoke |
| Mobile Device Management | Microsoft Corporation | Apr 2, 2019 | Active | ⓘ Renew Download Revoke |
| Mobile Device Management | Microsoft Corporation | Apr 29, 2019 | Active | ⓘ Renew Download Revoke |
| Mobile Device Management | Microsoft Corporation | Dec 28, 2019 | Active | ⓘ Renew Download Revoke |
| Mobile Device Management | Microsoft Corporation | Dec 28, 2019 | Active | ⓘ Renew Download Revoke |
| Mobile Device Management | Microsoft Corporation | Jan 19, 2020 | Active | ⓘ Renew Download Revoke |

*Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.

About Apple Push Certificates Portal

6. Click on **Choose File** and select the Intune CSR that you downloaded above from the Azure portal and click **Upload**.



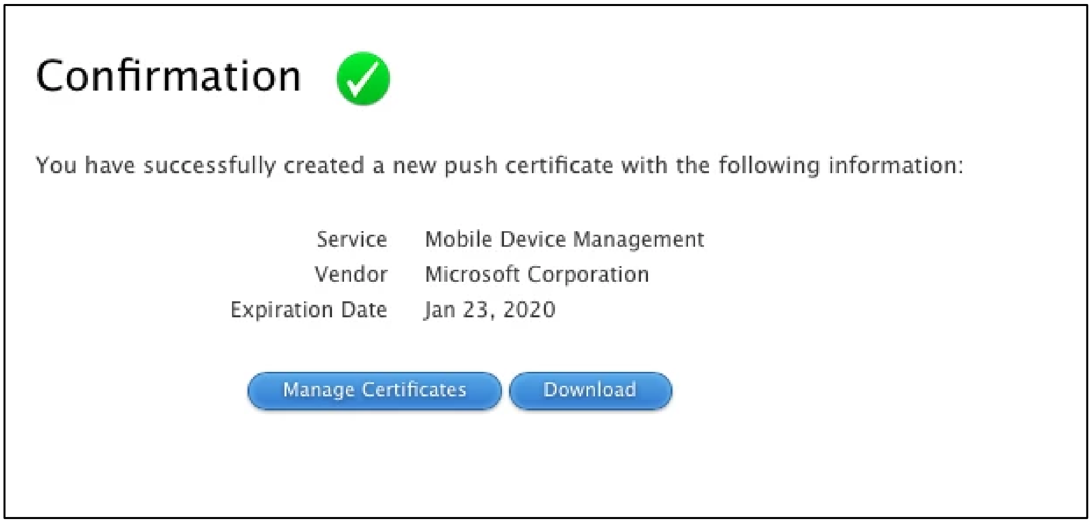
Create a New Push Certificate

Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

Notes

Vendor-Signed Certificate Signing Request

7. Download the generated certificate.

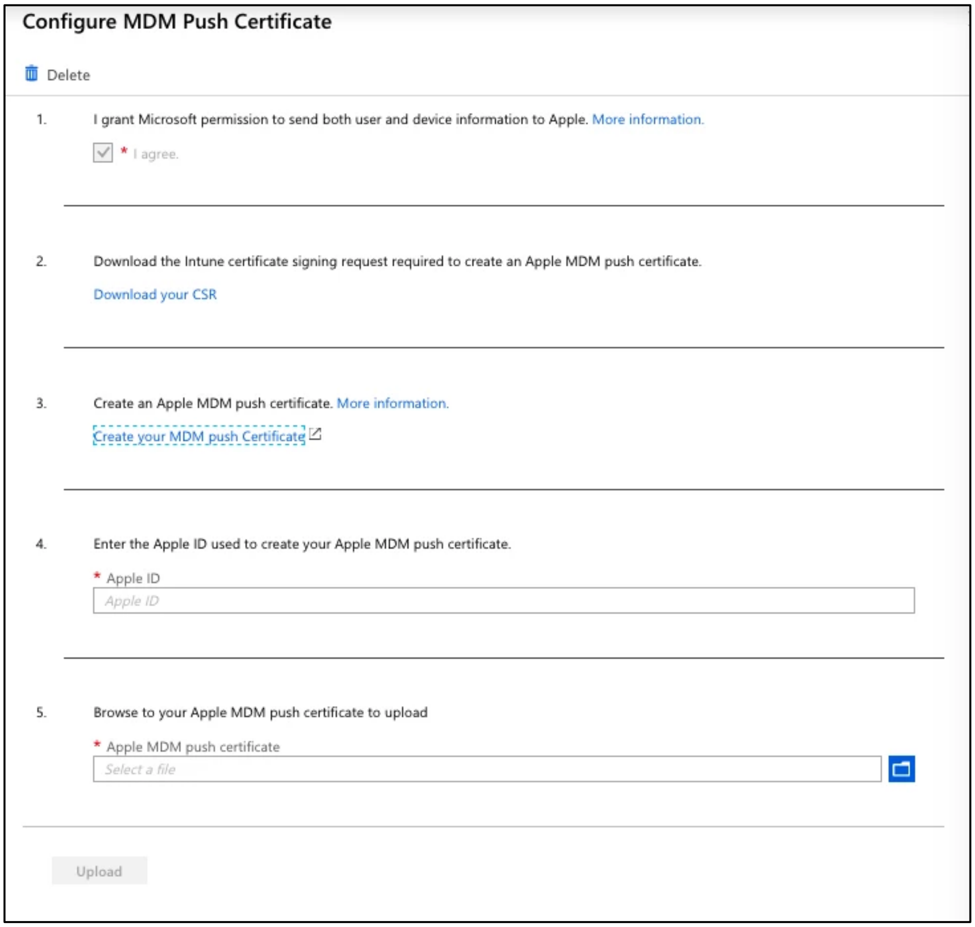


Confirmation ✓

You have successfully created a new push certificate with the following information:

| | |
|---|---|
| Service | Mobile Device Management |
| Vendor | Microsoft Corporation |
| Expiration Date | Jan 23, 2020 |

8. Once certificate is downloaded, return to the **Configure Apple MDM push certificate** page on Azure Portal.



Configure MDM Push Certificate

1. I grant Microsoft permission to send both user and device information to Apple. More information.

   ☑ * I agree.

2. Download the Intune certificate signing request required to create an Apple MDM push certificate.

   Download your CSR

3. Create an Apple MDM push certificate. More information.

   Create your MDM push Certificate

4. Enter the Apple ID used to create your Apple MDM push certificate.

   * Apple ID

   Apple ID

5. Browse to your Apple MDM push certificate to upload

   * Apple MDM push certificate

   Select a file

9. Provide your Apple ID and upload the downloaded MDM push certificate and click on **Upload**.

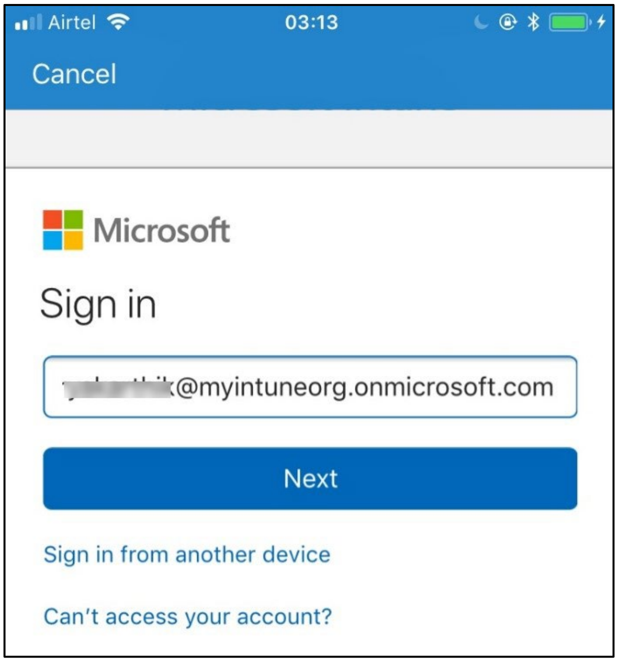
   **NOTE**: Please note that for Android, the conventional Android option can be chosen if enterprise management such as Work Profile Configuration is not needed. If a specific Work Profile is needed, the "**Android Enterprise**" option needs to be selected from the platform while creating profile in Intune.
   For simplicity, the conventional "**Android**" option is used for this guide.

# Appendix-C. Install Company Portal App on Device

## Configuration on the Android/iOS device

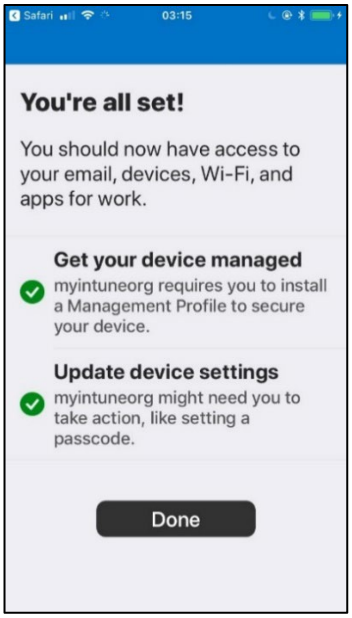
To configure the Android/iOS device and enroll with the MDM:

1. Download the application "**Intune company portal app**" provided by Microsoft Intune from the Play Store/ App Store and install it.
2. Once the application is installed, open the application and login with Intune credentials.



[redacted]@myintuneorg.onmicrosoft.com

3. Once logged in, on the setup page, proceed with the default option to install the profile and generate the certificate.



**You're all set!**

You should now have access to your email, devices, Wi-Fi, and apps for work.

✓ **Get your device managed**
myintuneorg requires you to install a Management Profile to secure your device.

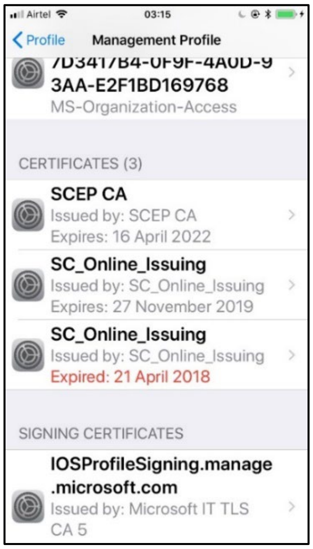
✓ **Update device settings**
myintuneorg might need you to take action, like setting a passcode.

NOTE: For Android device, there is no direct way to view and verify the certificate. For this, a third-party app "My Certificates" needs to be downloaded from the Play Store.

4. Once the application is configured and the enrolled with the MDM, Intune will push the assigned certificates to the device.

5. For Android, navigate to Trusted Certificate to view the certificate details.

6. For iOS, you can navigate to -> Settings -> General -> Device Management and see the details as below:



7D3417B4-0F9F-4A0D-9
3AA-E2F1BD169768
MS-Organization-Access

CERTIFICATES (3)

SCEP CA
Issued by: SCEP CA
Expires: 16 April 2022

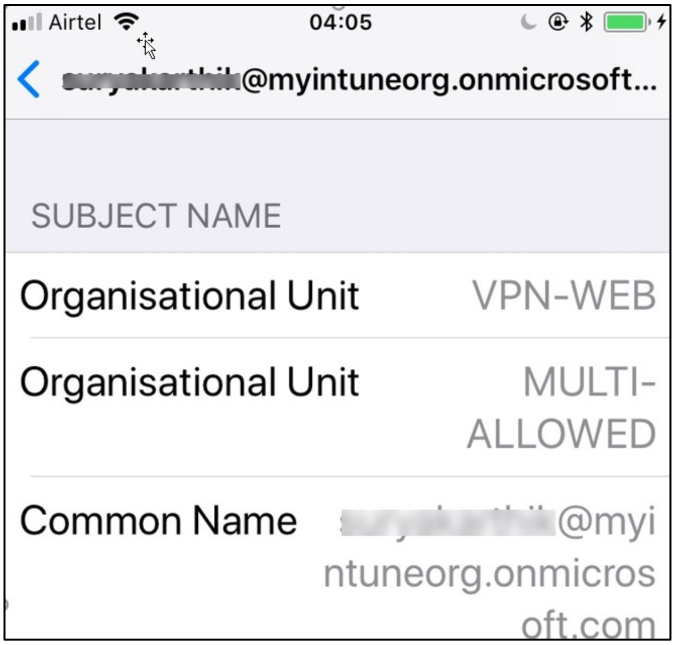
SC_Online_Issuing
Issued by: SC_Online_Issuing
Expires: 27 November 2019

SC_Online_Issuing
Issued by: SC_Online_Issuing
Expired: 21 April 2018

SIGNING CERTIFICATES

IOSProfileSigning.manage
.microsoft.com
Issued by: Microsoft IT TLS
CA 5

Certificate details in iOS



[redacted]@myintuneorg.onmicrosoft...

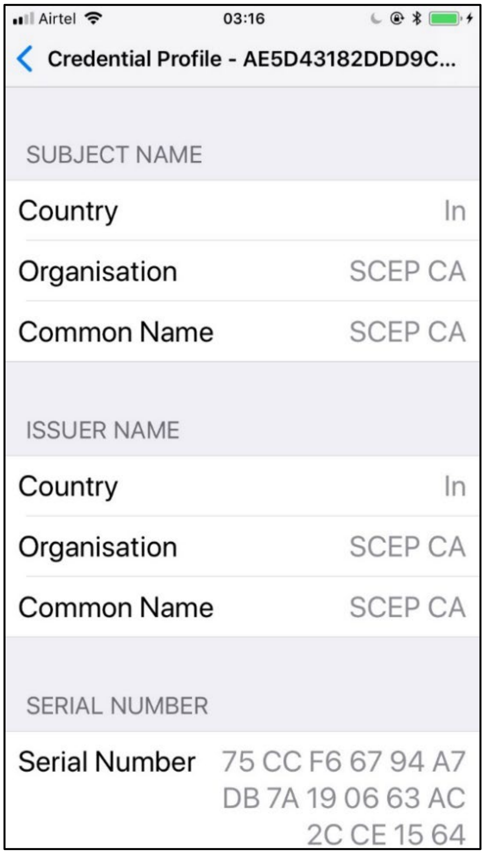
SUBJECT NAME

Organisational Unit VPN-WEB

Organisational Unit MULTI-ALLOWED

Common Name [redacted]@myintuneorg.onmicrosoft.com

Subject Name



Credential Profile - AE5D43182DDD9C...

SUBJECT NAME

Country In

Organisation SCEP CA

Common Name SCEP CA

ISSUER NAME

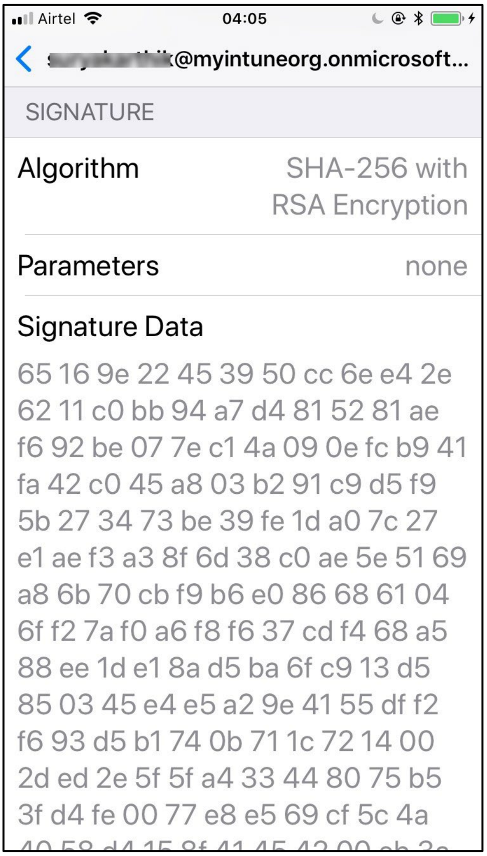
Country In

Organisation SCEP CA

Common Name SCEP CA

SERIAL NUMBER

Serial Number 75 CC F6 67 94 A7 DB 7A 19 06 63 AC 2C CE 15 64



[redacted]@myintuneorg.onmicrosoft...

SIGNATURE

Algorithm SHA-256 with RSA Encryption

Parameters none

Signature Data

```
65 16 9e 22 45 39 50 cc 6e e4 2e
62 11 c0 bb 94 a7 d4 81 52 81 ae
f6 92 be 07 7e c1 4a 09 0e fc b9 41
fa 42 c0 45 a8 03 b2 91 c9 d5 f9
5b 27 34 73 be 39 fe 1d a0 7c 27
e1 ae f3 a3 8f 6d 38 c0 ae 5e 51 69
a8 6b 70 cb f9 b6 e0 86 68 61 04
6f f2 7a f0 a6 f8 f6 37 cd f4 68 a5
88 ee 1d e1 8a d5 ba 6f c9 13 d5
85 03 45 e4 e5 a2 9e 41 55 df f2
f6 93 d5 b1 74 0b 71 1c 72 14 00
2d ed 2e 5f 5f a4 33 44 80 75 b5
3f d4 fe 00 77 e8 e5 69 cf 5c 4a
```

Credential Profile

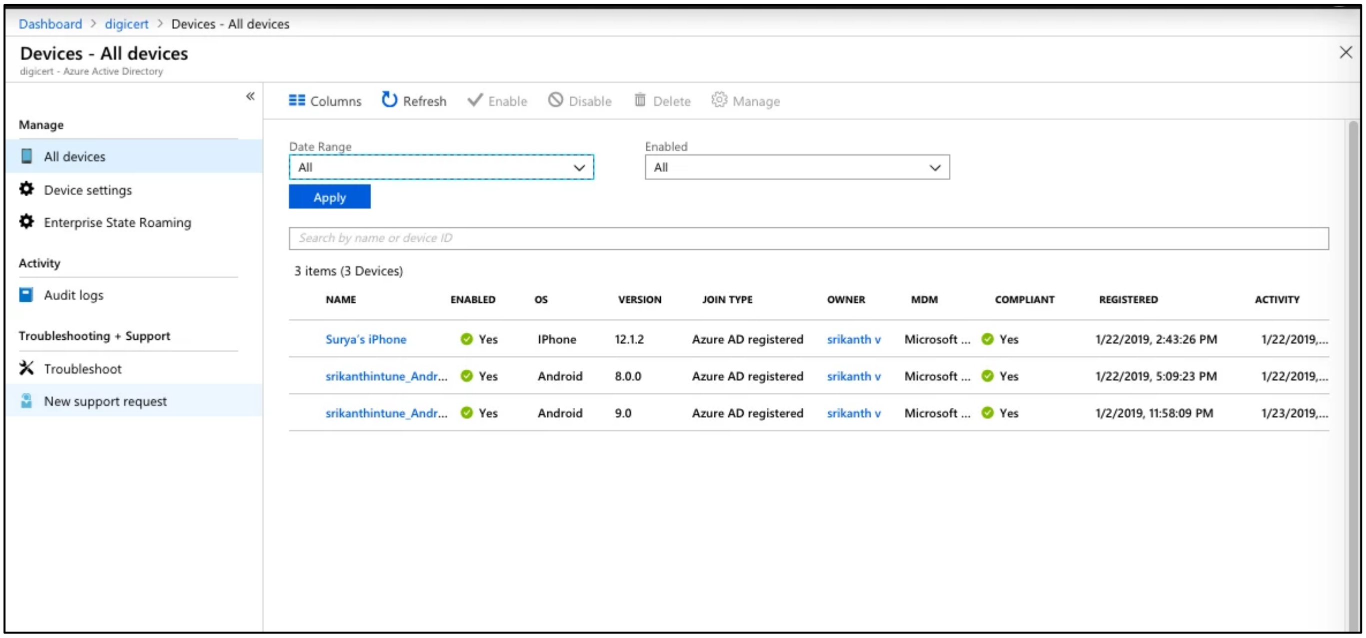
Signature details

# Appendix-D. Deployment of profiles to the devices

Profiles can be deployed to the devices using the following steps:

a) On the device, install the Company portal App application (for iOS and Android) and login to the application using the Intune credentials. Once you are logged in to the Company Portal App, the device will be registered with Intune and mobile management profiles will be installed to the device.

b) On the Azure portal, navigate to "**Azure Active Directory**" and click on "**Devices**".



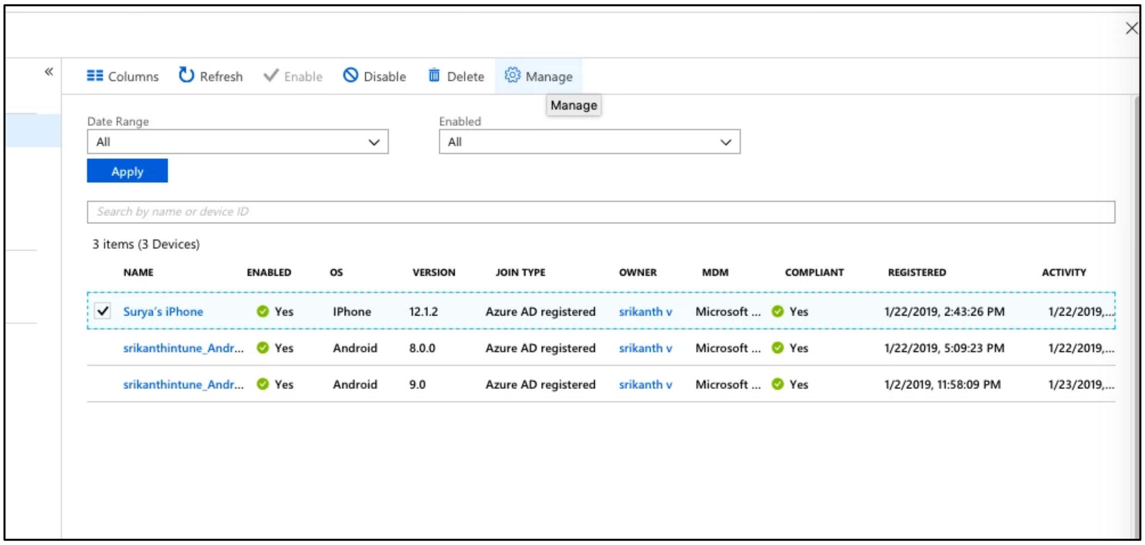
Date Range: All

Enabled: All

3 items (3 Devices)

| NAME | ENABLED | OS | VERSION | JOIN TYPE | OWNER | MDM | COMPLIANT | REGISTERED | ACTIVITY |
|---|---|---|---|---|---|---|---|---|---|
| Surya's iPhone | ✓ Yes | IPhone | 12.1.2 | Azure AD registered | srikanth v | Microsoft ... | ✓ Yes | 1/22/2019, 2:43:26 PM | 1/22/2019,... |
| srikanthintune_Andr... | ✓ Yes | Android | 8.0.0 | Azure AD registered | srikanth v | Microsoft ... | ✓ Yes | 1/22/2019, 5:09:23 PM | 1/22/2019,... |
| srikanthintune_Andr... | ✓ Yes | Android | 9.0 | Azure AD registered | srikanth v | Microsoft ... | ✓ Yes | 1/2/2019, 11:58:09 PM | 1/23/2019,... |

c) Select a device you would like to manage and click on "**Manage**".



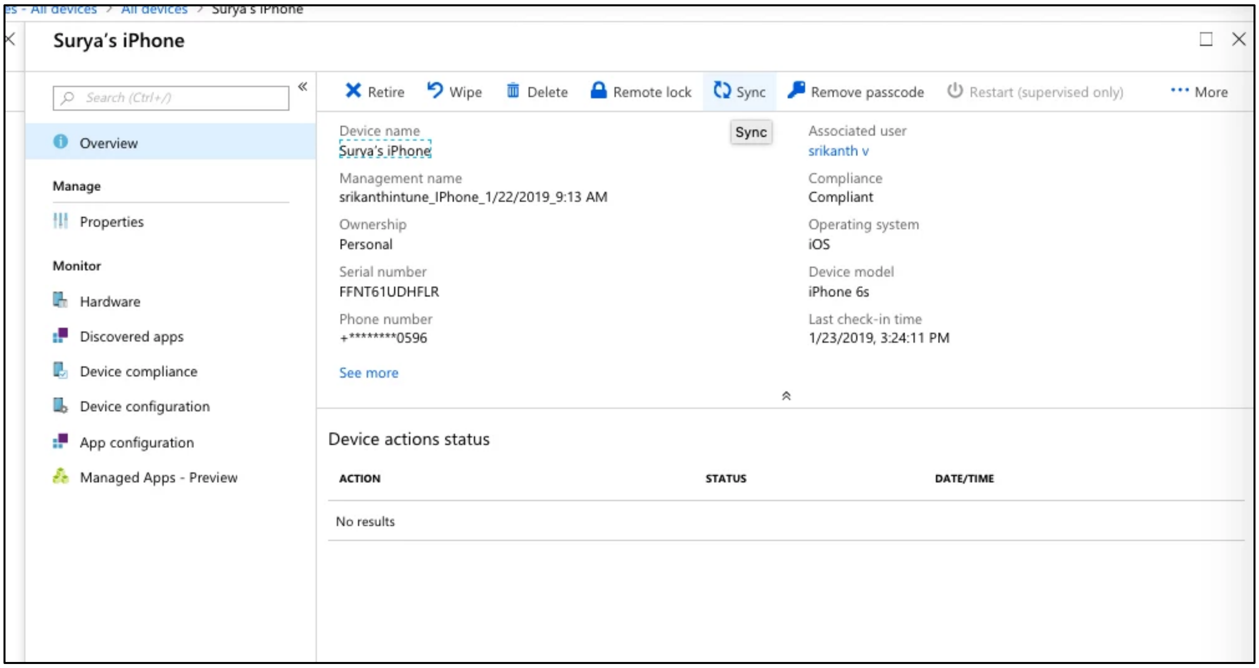
Date Range: All

Enabled: All

3 items (3 Devices)

| | NAME | ENABLED | OS | VERSION | JOIN TYPE | OWNER | MDM | COMPLIANT | REGISTERED | ACTIVITY |
|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | Surya's iPhone | ✓ Yes | IPhone | 12.1.2 | Azure AD registered | srikanth v | Microsoft ... | ✓ Yes | 1/22/2019, 2:43:26 PM | 1/22/2019,... |
| | srikanthintune_Andr... | ✓ Yes | Android | 8.0.0 | Azure AD registered | srikanth v | Microsoft ... | ✓ Yes | 1/22/2019, 5:09:23 PM | 1/22/2019,... |
| | srikanthintune_Andr... | ✓ Yes | Android | 9.0 | Azure AD registered | srikanth v | Microsoft ... | ✓ Yes | 1/2/2019, 11:58:09 PM | 1/23/2019,... |

d) Click on "**Sync**" and this will Sync the device with the settings configured.



Device name
Surya's iPhone

Management name
srikanthintune_IPhone_1/22/2019_9:13 AM

Ownership
Personal

Serial number
FFNT61UDHFLR

Phone number
+********0596

Associated user
srikanth v

Compliance
Compliant

Operating system
iOS

Device model
iPhone 6s

Last check-in time
1/23/2019, 3:24:11 PM

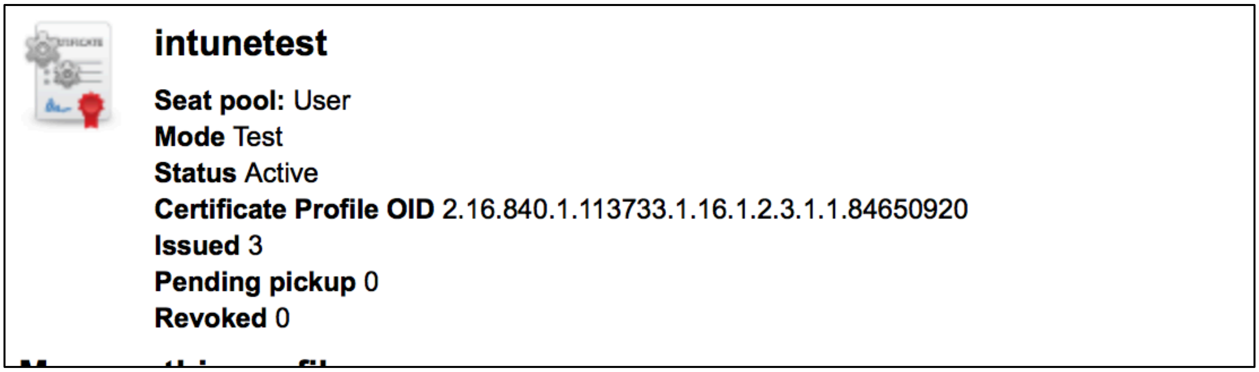
Device actions status

| ACTION | STATUS | DATE/TIME |
|---|---|---|
| No results | | |

e) Once the Sync is initiated, certificate profile settings will be installed to the device, the device will call out to the SCEP CA for certificate issuance, and a certificate will be installed on the device.

## Appendix-E. Verify Certificate Issuance details in DigiCert PKI Platform

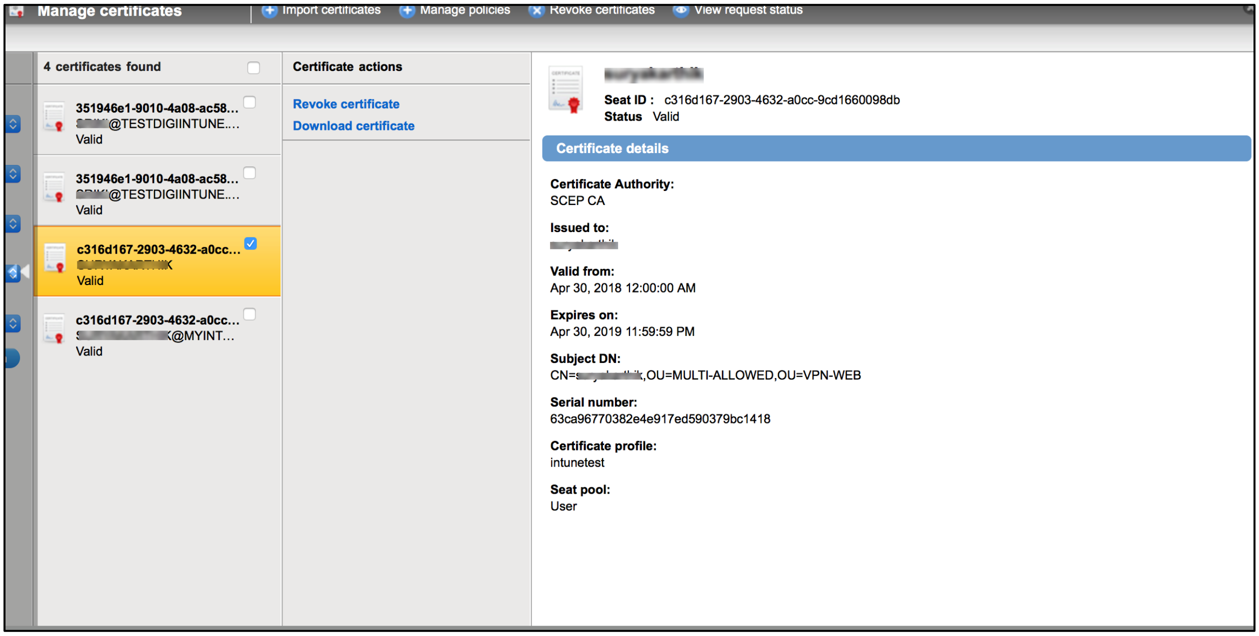
The certificate issuance can also be verified from the DigiCert PKI Platform. If you go to the" Manage **Certificate profile**" section and select the profile that you created, you can see the total number of certificates issued for that profile.



**intunetest**

**Seat pool:** User
**Mode** Test
**Status** Active
**Certificate Profile OID** 2.16.840.1.113733.1.16.1.2.3.1.1.84650920
**Issued** 3
**Pending pickup** 0
**Revoked** 0

You can also go to the “**Certificate Management**” section on the PKI manager and search for that profile to see the certificate details as follows:



4 certificates found

351946e1-9010-4a08-ac58…
[redacted]@TESTDIGIINTUNE.…
Valid

351946e1-9010-4a08-ac58…
[redacted]@TESTDIGIINTUNE.…
Valid

c316d167-2903-4632-a0cc… ☑
[redacted]
Valid

c316d167-2903-4632-a0cc…
[redacted]@MYINT…
Valid

[redacted]
**Seat ID :** c316d167-2903-4632-a0cc-9cd1660098db
**Status** Valid

**Certificate Authority:**
SCEP CA

**Issued to:**
[redacted]

**Valid from:**
Apr 30, 2018 12:00:00 AM

**Expires on:**
Apr 30, 2019 11:59:59 PM

**Subject DN:**
CN=[redacted],OU=MULTI-ALLOWED,OU=VPN-WEB

**Serial number:**
63ca96770382e4e917ed590379bc1418

**Certificate profile:**
intunetest

**Seat pool:**
User