

# DigiCert® PKI Platform

Intune SCEP

June, 2022

## Legal Notice

Copyright© 2022 DigiCert, Inc. All rights reserved. DigiCert and its logo are registered trademarks of DigiCert, Inc. Other names may be trademarks of their respective owners.

The product described in this document is provided by DigiCert, Inc. and distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of DigiCert, Inc. and its licensors, if any.

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 .....	4
PREREQUISITES.....	5
INTEGRATION OVERVIEW.....	6
AZURE ACTIVE DIRECTORY APP REGISTRATION .....	7
INTUNE DEVICE PROFILE AND DIGICERT CERTIFICATE PROFILE CONFIGURATIONS FOR CERTIFICATE USE-CASES .....	20
<b>INTUNE TRUSTED CERTIFICATE PROFILE</b> .....	<b>20</b>
<b>SCEP CERTIFICATE CONFIGURATION</b> .....	<b>23</b>
DEVICE AUTHENTICATION .....	25
USER CLIENT AUTHENTICATION.....	37
S/MIME (DIGITAL SIGNATURE ONLY) FOR INTUNE .....	47
JOINING A DEVICE TO INTUNE MDM.....	57
VERIFY CERTIFICATE ISSUANCE DETAILS IN DIGICERT PKI PLATFORM .....	57
REVOCAION OF CERTIFICATES IN INTUNE.....	58

## 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.

The integration be accomplished using the Intune NDES connector (which implements DigiCert PKI Web Services APIs), and/or using Microsoft APIs.

The following tables shows the types of certificates that can be issued along with the integration method(s) for that type certificate.

*Table 1 Certificate Type Integration Method*

DigiCert Certificate Type	Microsoft Profile Type	Integration Method with DigiCert PKI Platform	Notes
Device Authentication	SCEP certificate	Microsoft API	This is a cloud-to-cloud integration.
	PKCS certificate	Microsoft NDES Connector	NDES connector runs on a Microsoft server machine that you host.
User Client Authentication	SCEP certificate	Microsoft API	This is a cloud-to-cloud integration.
	PKCS certificate	Microsoft NDES Connector	NDES connector runs on a Microsoft server machine that you host.
	SCEP certificate	Microsoft API	This is a cloud-to-cloud integration.

DigiCert Certificate Type	Microsoft Profile Type	Integration Method with DigiCert PKI Platform	Notes
S/MIME (Digital Signature only)			
	PKCS certificate	Microsoft NDES Connector	NDES connector runs on a Microsoft server machine that you host.
S/MIME (Encryption only)	PKCS imported certificate	Microsoft NDES (PFX) Connector	<p>Intune does not support new enrollments/renewals of S/MIME escrowed certificates.</p> <p>This solution feature recovers previously issued S/MIME key/certificate in PKCS12 format with associated password and imports into Intune for onward provisioning.</p>
Secure Email (S/MIME Signing and Encryption)	PKCS imported certificate	Microsoft NDES (PFX) Connector	<p>Intune does not support new enrollments/renewals of S/MIME escrowed certificates.</p> <p>This solution feature recovers previously issued S/MIME key/certificate in PKCS12 format with associated password and imports into Intune for onward provisioning.</p>

This document covers Microsoft Profile SCEP certificate types integrated using Microsoft APIs.

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

## Prerequisites

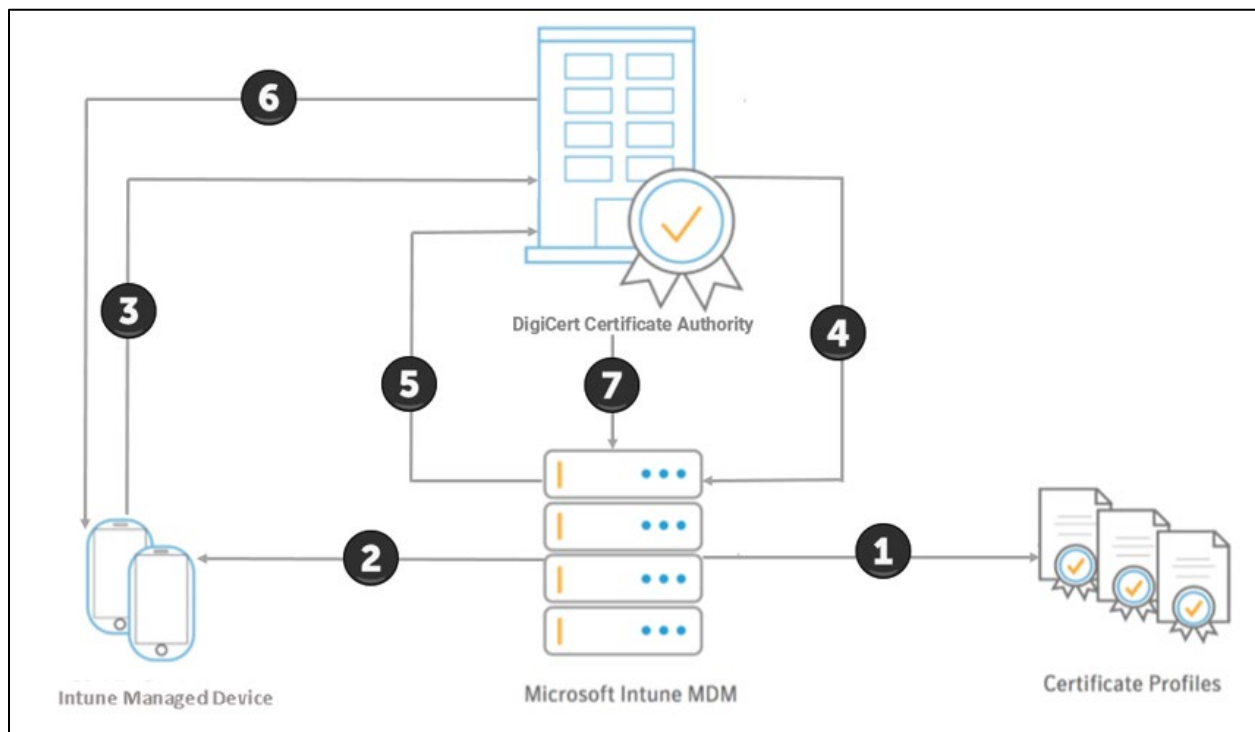
- Your Microsoft Azure tenant has Azure Active Directory services is enabled.
- Your Microsoft Intune account is configured for [Intune MDM Authority](#).
- Your Microsoft Intune account is configured with an [Apple MDM Push Certificate](#), if you will issue certificates to an Apple iOS device.

- Your DigiCert PKI Platform account is enabled with the following DigiCert Certificate Profile Templates and that you have at least one Seat allocated to the appropriate Seat Pool for the type of certificate you want to issue:

DigiCert certificate Profile Template	Seat Pool Type
Generic Device Authentication for Intune	Device
Client Authentication for Intune	User
S/MIME (Digital Signature only) for Intune	User

## Integration Overview

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



- The Intune Administrator creates certificate templates in Microsoft Intune corresponding to the profiles created in DigiCert PKI Platform.
- Microsoft Intune deploys the Device Configuration profiles (Trusted Certificate & SCEP types) to the specified group of endpoint devices.
- DigiCert Certificate Authority validates the request with Intune.

4. Microsoft Intune provides the validation response to DigiCert PKI Platform SCEP service.
5. DigiCert Certificate Authority issues the certificate to the requesting device.
6. Finally, DigiCert Certificate Authority provides the confirmation message to Intune.

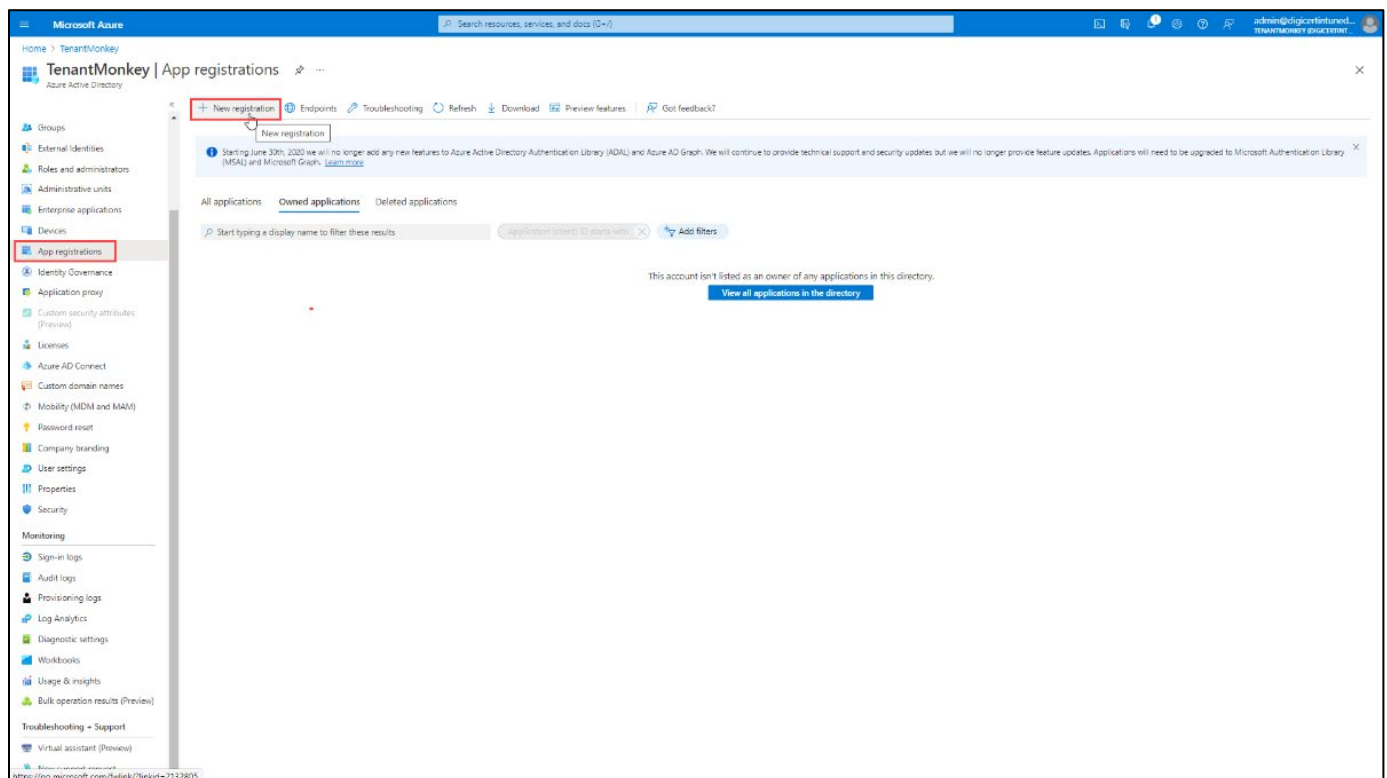
## Azure Active Directory App registration

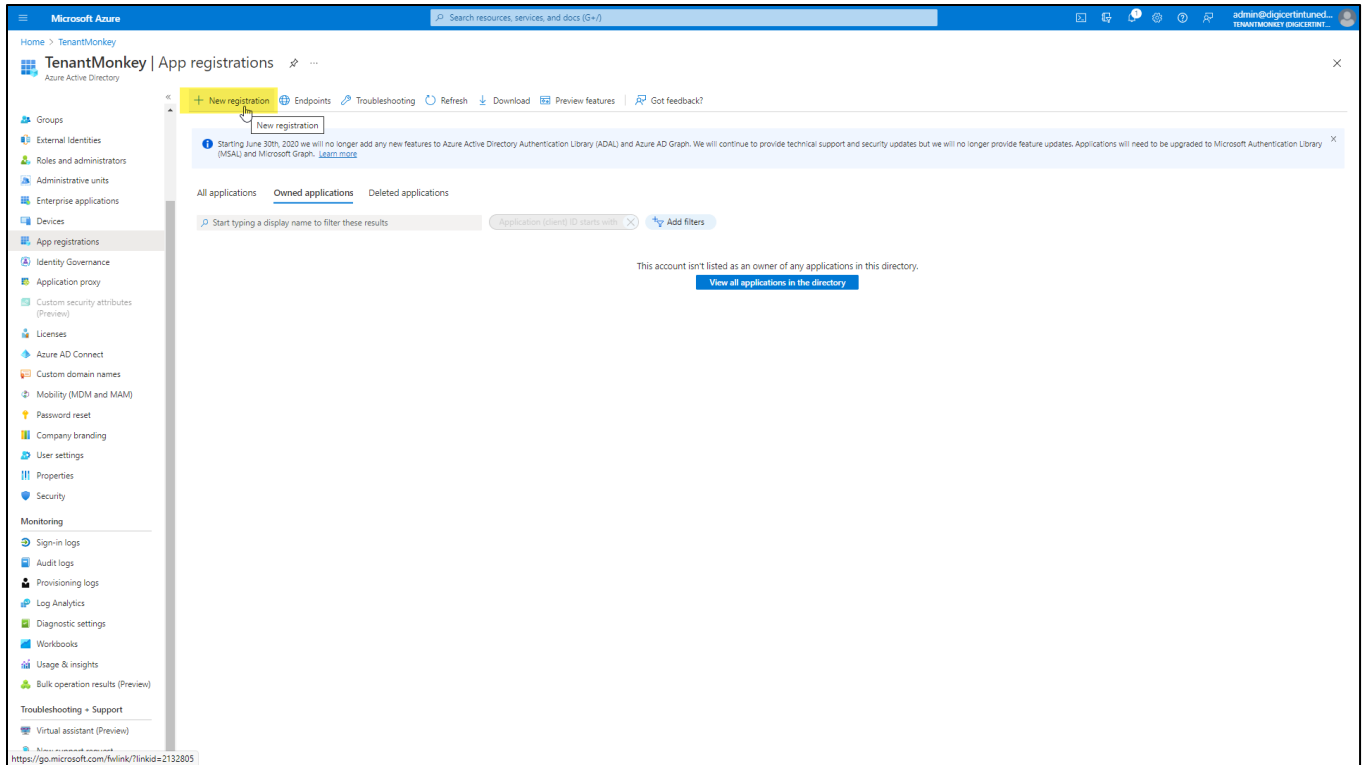
Create an application registration that DigiCert PKI Platform SCEP Service uses to communicate to Intune via APIs.

The goal of this procedure is to obtain **Application (client) ID**, **Client secret**, and **Tenant Name** which will be used to configure a DigiCert Certificate Profile in DigiCert PKI Manager.

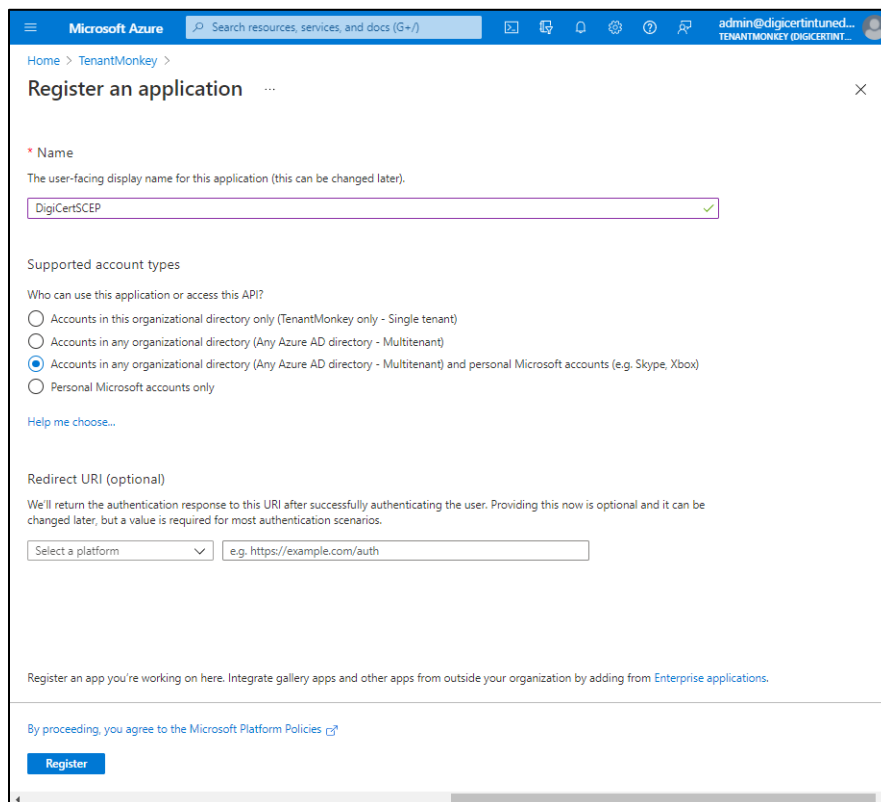
1. In the [Azure portal](#), search for or select **Azure Active Directory** from any page.
2. Select **App registrations**, and then select **New registration**.

Note: If you create many DigiCert Certificate Profiles using Azure Auth, you can reuse this app registration for each profile, or you can create and use separate app registrations for higher security and granular auditing and logging.





3. In the **Name** field, enter a meaningful display name for the application. Click **Register**.





4. Copy and save the **Application (client) ID** value in a secure file for later use.

**Application (client) ID** will be used later when configuring the DigiCert Certificate Profile in DigiCert PKI Manager.

The screenshot displays the Microsoft Azure portal interface for an application registration. The top navigation bar shows the user is logged in as 'admin@digicertintuned...' under the 'TENANTMONKEY (DIGICERTINT...)' subscription. The main content area is titled 'DigiCertSCEP' and includes a search bar and navigation options like 'Delete', 'Endpoints', and 'Preview features'. The 'Essentials' section is expanded, showing the following details:

- Display name: [DigiCertSCEP](#)
- Application (client) ID: **2662b113-de79-4da8-8bd7-d0d9e897e52f** (highlighted with a red box and a 'Copy to clipboard' tooltip)
- Object ID: 7aad55b3-952b-482e-bf66-36c554e62538
- Directory (tenant) ID: f0e414c1-27e6-435c-81b1-80f1177150f1
- Supported account types: [All Microsoft account users](#)

On the right side, there are links for 'Client credentials' ([Add a certificate or secret](#)), 'Redirect URIs' ([Add a Redirect URI](#)), 'Application ID URI' ([Add an Application ID URI](#)), and 'Managed application in local directory' ([DigiCertSCEP](#)).

Below the essentials section, there are three messages:

- Informational: Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)
- Informational: Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)
- Warning: Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant apps without verified publishers. [Add MPN ID to verify publisher](#)

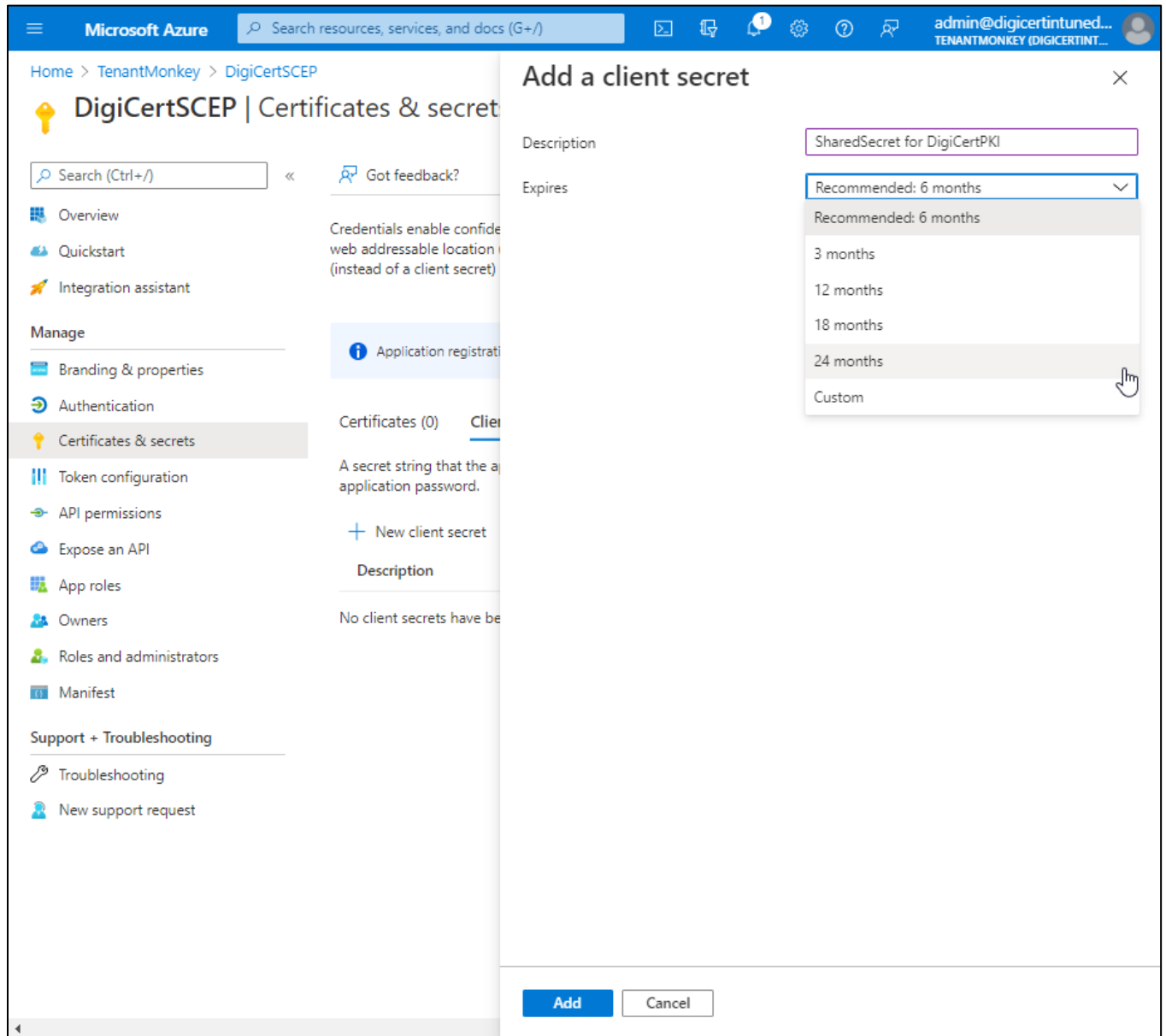
At the bottom, there are links for 'Get Started' and 'Documentation', followed by a large heading: 'Build your application with the Microsoft identity platform'. Below this heading is a short paragraph: 'The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-'

5. Select **Certificates & secrets**, and then select **New client secret**.

The screenshot shows the Microsoft Azure portal interface. At the top, the header includes the Microsoft Azure logo, a search bar, and the user profile 'admin@digicertintuned...'. The breadcrumb trail is 'Home > TenantMonkey > DigiCertSCEP'. The main heading is 'DigiCertSCEP | Certificates & secrets'. Below this is a search bar and a 'Got feedback?' link. The left-hand navigation pane is expanded to show 'Certificates & secrets', which is highlighted with a red box. The main content area shows a notification about application registration credentials, followed by three tabs: 'Certificates (0)', 'Client secrets (0)', and 'Federated credentials (0)'. The 'Client secrets (0)' tab is selected and highlighted with a red box. Below the tabs, there is a description of client secrets and a '+ New client secret' button, which is also highlighted with a red box and has a hand cursor pointing to it. Below the button is a table header with columns: 'Description', 'Expires', 'Value', and 'Secret ID'. The table content is empty, with the text 'No client secrets have been created for this application.' below it.

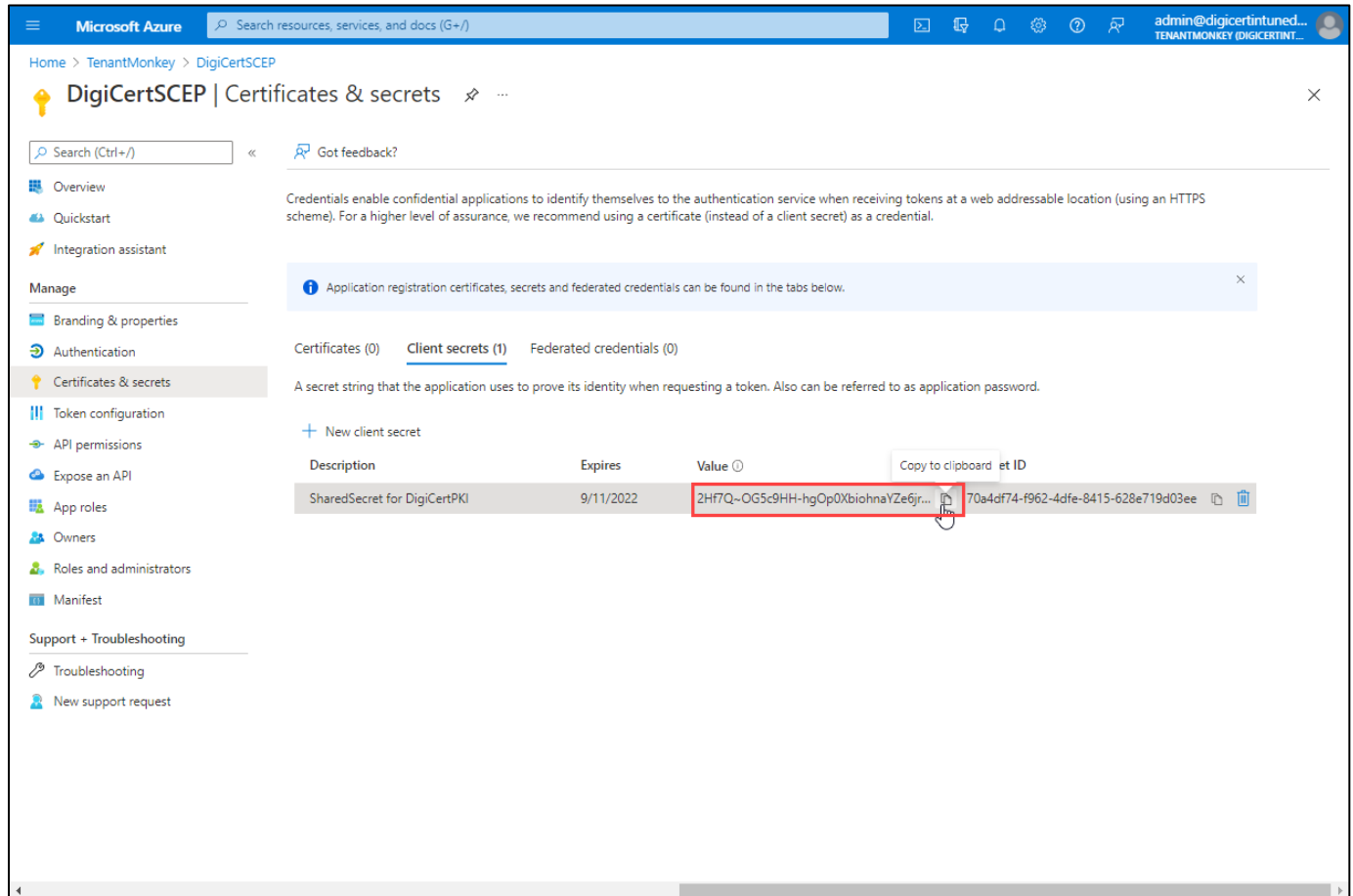
6. Enter a Description and select the desired expiration period for the client secret. Click **Add**.

Note: A new client secret will need to be created prior to expiration and updated in the DigiCert Certificate Profile in DigiCert PKI Manager portal to avoid service interruption.



- Copy and save the client secret Value in the same secure file as the previously saved Application (client) ID. **Client secret** will be used later when configuring the DigiCert Certificate Profile in DigiCert PKI Manager.

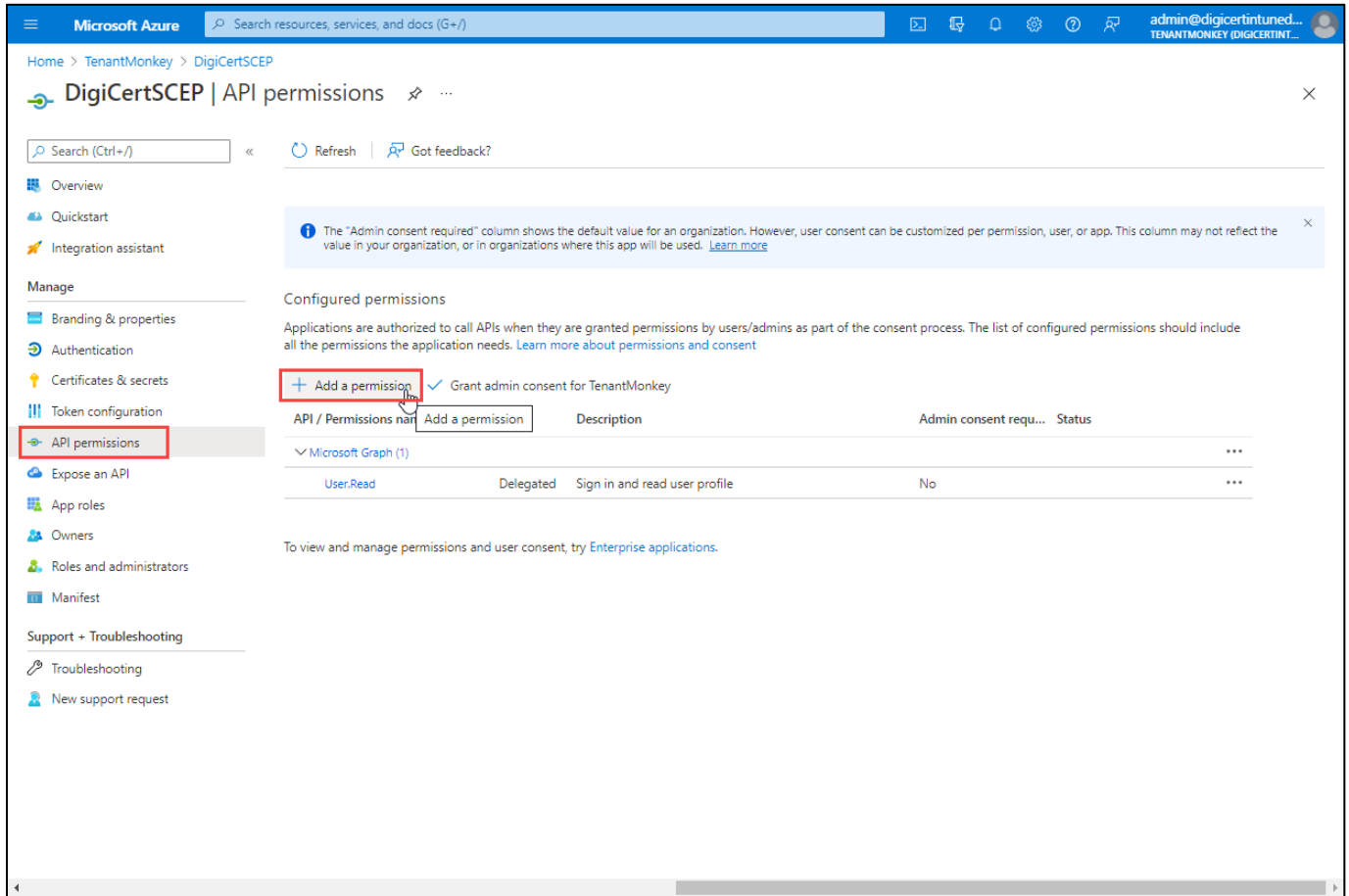
Note: The client secret Value cannot be viewed again once this view is closed. If you forget the value, you need to create a new client secret.



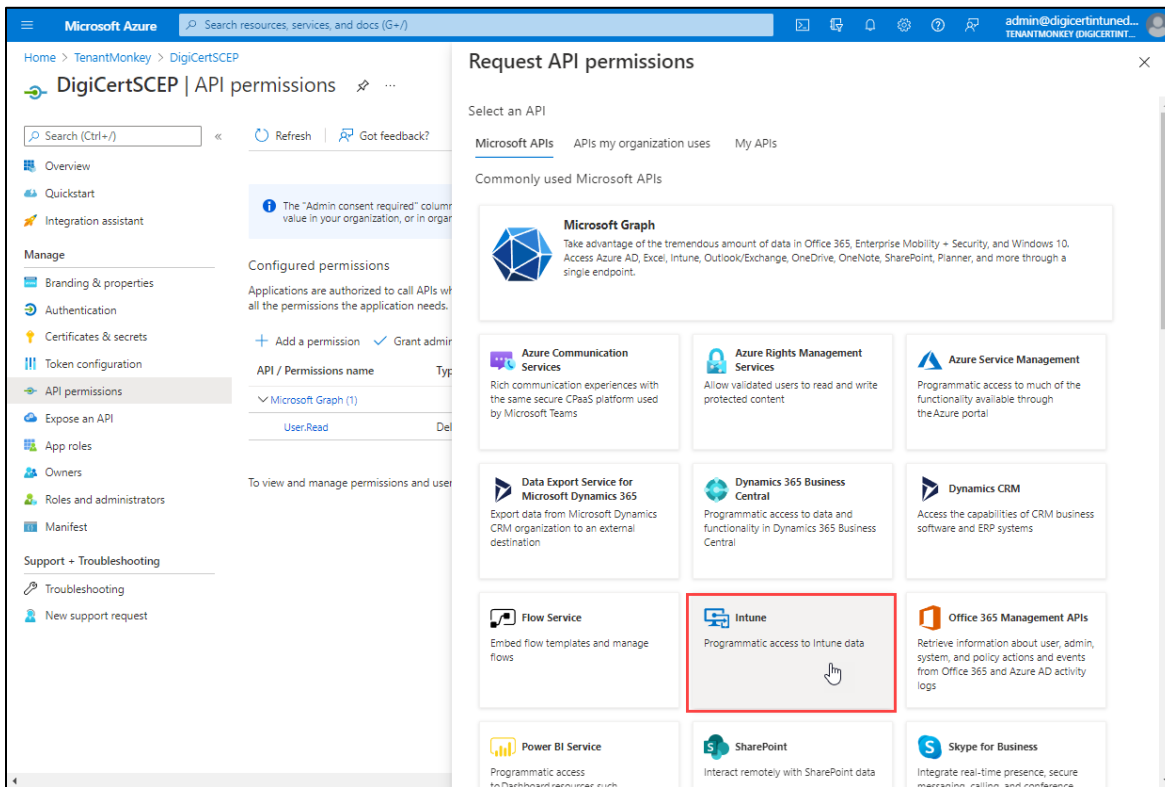
The screenshot shows the Microsoft Azure portal interface for managing application secrets. The page title is "DigiCertSCEP | Certificates & secrets". The left-hand navigation pane includes sections for "Manage" (Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, Manifest) and "Support + Troubleshooting" (Troubleshooting, New support request). The main content area shows a notification about application registration credentials, tabs for "Certificates (0)", "Client secrets (1)", and "Federated credentials (0)", and a "New client secret" button. A table displays the existing client secret:

Description	Expires	Value	Copy to clipboard	et ID
SharedSecret for DigiCertPKI	9/11/2022	2Hf7Q~OG5c9HH-hgOp0XbiohnaYZe6jr...		70a4df74-f962-4dfe-8415-628e719d03ee

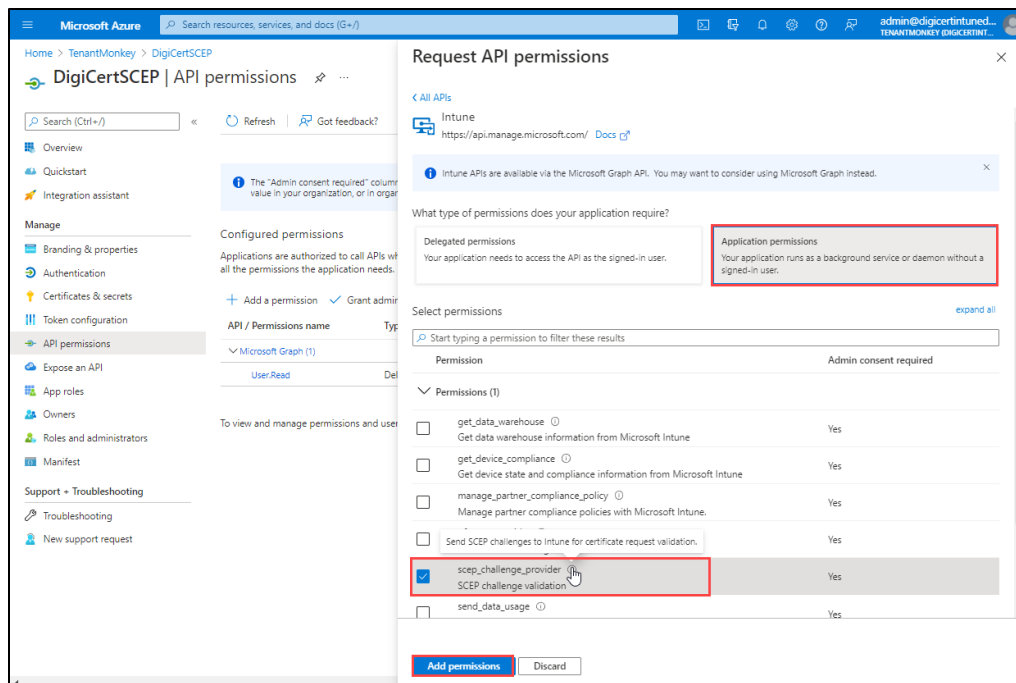
8. Select **API Permissions**, and then select **Add a permission**.



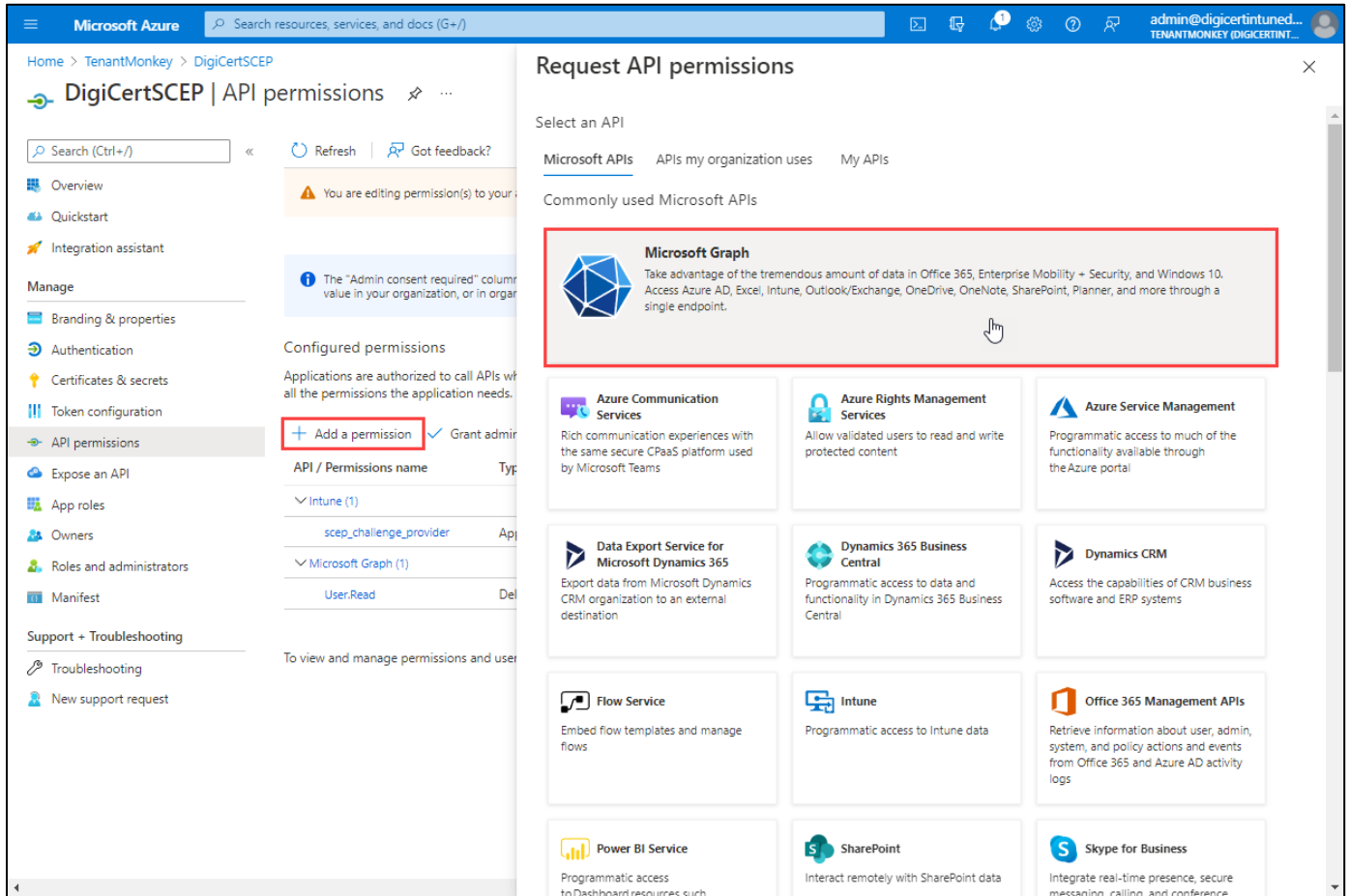
## 9. Select Intune.



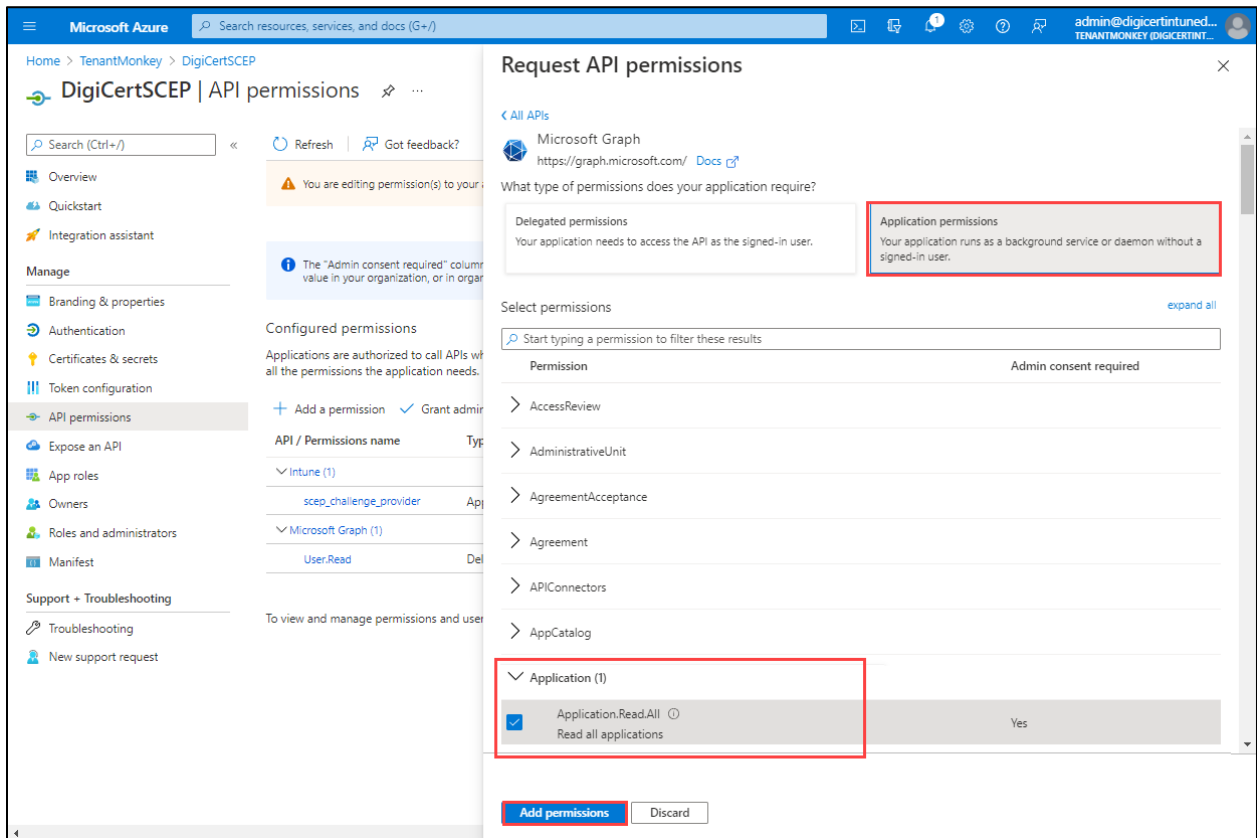
## 10. Select Application permissions, then select scep\_challenge\_provider. Select Add permissions.



11. Select Add a permission, and then select Microsoft Graph.



12. Select **Application permissions**, expand **Application**, check **Application.Read.All**, and then **Add permissions**.



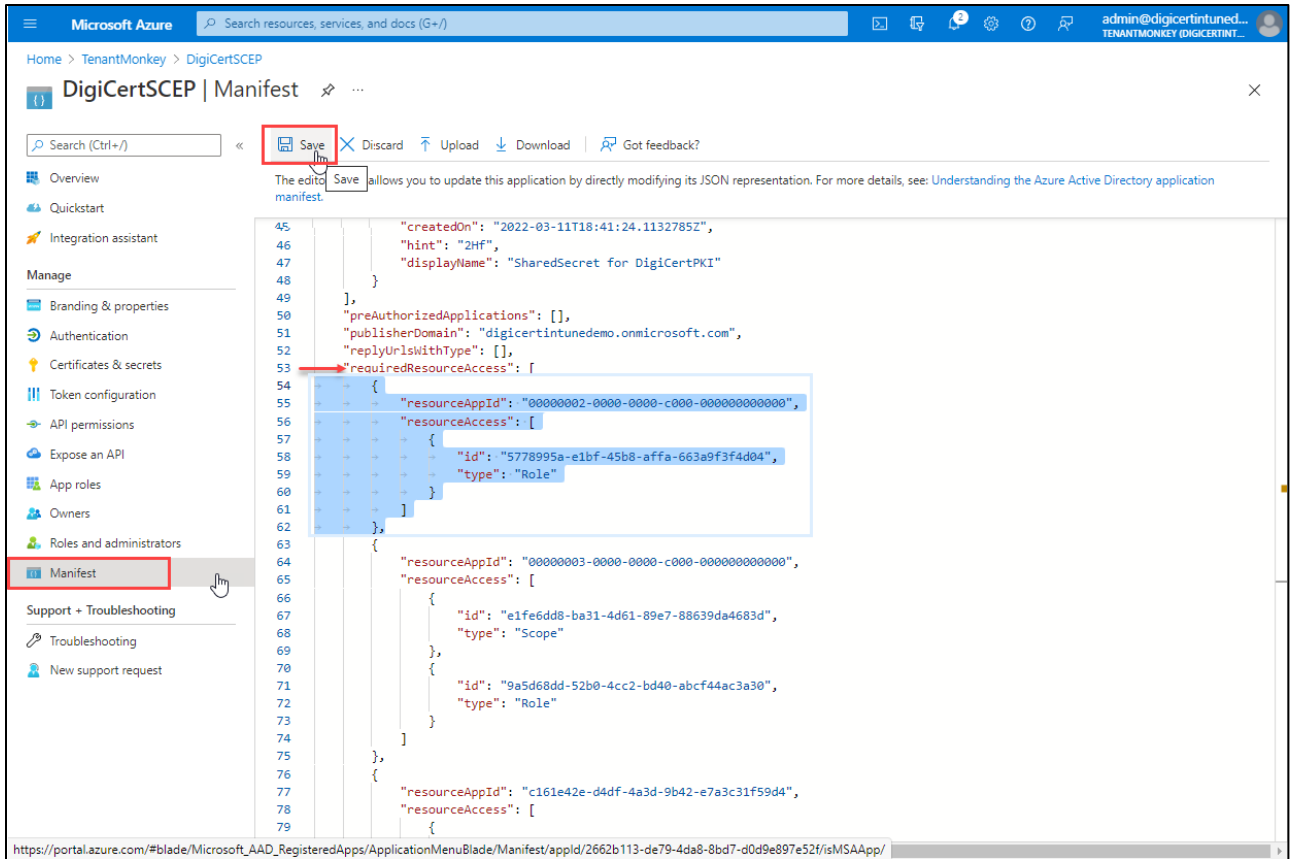


13. Select **Manifest** to modify and directly update the application JSON representation to enable **Azure AD Graph** API.

Note: Currently this integration also depends on the **Azure AD Graph** API, which is on a deprecation path and cannot be configured using the "Request API permission" GUI workflow. *It is recommended that you download and save a backup of the Manifest JSON file prior to making any changes.*

In the application manifest locate the "requiredResourceAccess" array and insert the following object as-is (which represents the Azure AD Graph API application role permissions), as shown in the screenshot and **Save**.

```
{
  "resourceAppId": "00000002-0000-0000-c000-000000000000",
  "resourceAccess": [
    {
      "id": "5778995a-e1bf-45b8-affa-663a9f3f4d04",
      "type": "Role"
    }
  ]
},
```



14. Select API permissions, and then select Grant admin consent for <TenantName>.

Microsoft Azure | Search resources, services, and docs (G+)

Home > TenantMonkey > DigiCertSCEP

### DigiCertSCEP | API permissions

Search (Ctrl+/) Refresh Got feedback?

Successfully granted admin consent for the requested permissions.

This application is using Azure AD Graph API, which is on a deprecation path. Starting June 30th, 2020 we will no longer add any new features to Azure AD Graph API. We strongly recommend that you upgrade your application to use Microsoft Graph API instead of Azure AD Graph API to access Azure Active Directory resources. [Learn more](#)

Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant apps without verified publishers. [Add MPN ID to verify publisher](#)

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

#### Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission  Grant admin consent for TenantMonkey

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

To view and manage permissions and user consent, try [Enterprise applications](#).

The app registration process in Azure AD is complete.

15. In the Azure Portal, in the upper right-hand corner, hovering over your user account displays the account details.

Note the **Azure account Domain** and save this as your *Tenant Name* along with the *Application (client) ID* and *Client secret*, as they will be used later when configuring the DigiCert Certificate Profile in DigiCert PKI Manager.

The screenshot shows the Azure portal interface. In the top right corner, the user account dropdown menu is open, displaying the following details:

- Name: Tenant
- Email: [redacted]
- Directory: T
- Domain: digicertintunedemo.onmicrosoft.com

The main content area shows the 'API permissions' page for 'DigiCertSCEP'. It includes a search bar, a refresh button, and a 'Got feedback?' link. Below this, there are several informational and warning messages. The 'Configured permissions' section shows a table of permissions:

API / Permissions name	Type	Description	Admin consent requ...	Status
Azure Active Directory Graph (1)				
Directory.Read.All	Application	Read directory data	Yes	Granted for TenantMon...

## Intune Device Profile and DigiCert Certificate Profile configurations for certificate use-cases

### Intune Trusted Certificate profile

The goal of this procedure is to provide the entire CA certificate chain to the targeted device platform(s).

When configuring a certificate profile in DigiCert PKI Manager, you will configure the issuer certificate authority (CA) that issues the end entity (EE) certificate to your target device or user. In addition to configuring the Intune Device Configuration profile for the SCEP certificate type, you will need to create one or more Trusted Certificate profiles for each certificate in the CA hierarchy that you are using. If you use an Online Root Issuing CA, then you will only need to create a Trusted Certificate Profile for that Root CA. If you have a multi-tier CA hierarchy, then you will also create a Trusted Certificate profile for each intermediate CA in the certificate hierarchy. Common CA hierarchies consist of a Root CA and a subordinate Intermediate Issuer CA.

Download the CA certificates from **DigiCert PKI Manager**.

The DigiCert certificate profile configuration determines what CA you are using to issue the EE certificate.

The screenshot shows the DigiCert PKI Platform interface. The main window is titled "Manage certificate profiles" and includes navigation buttons: "Add certificate profiles", "Manage custom scripts", "Clone certificate profiles", and "Download AE Config". The "Create profile" workflow is shown with steps: "Select mode", "Select template", "Customize options" (highlighted), and "Customize services".

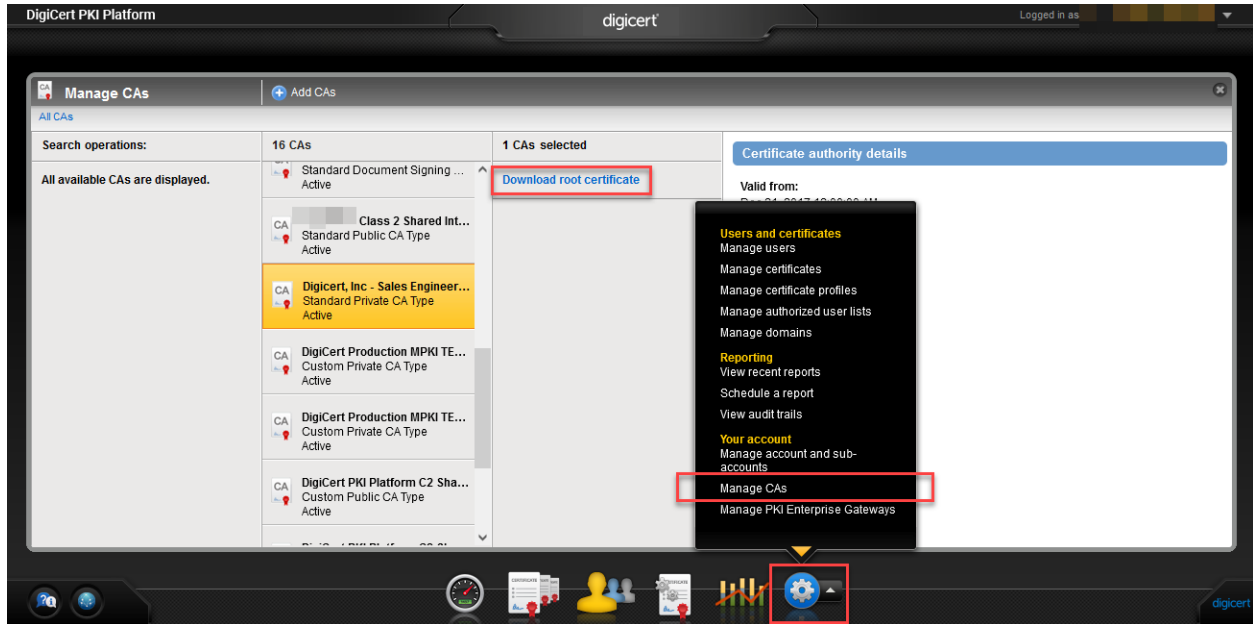
The "Customize certificate options" section is active, displaying the following configuration:

- Certificate friendly name:** (empty text field)
- Primary certificate options:**
  - Certificate authority:** DigiCert Production MPKI TEST Issuing CA (dropdown menu, highlighted with a red box)
  - Enrollment method:** SCEP
  - Authentication method:** Azure Auth (with a lock icon)
  - Certificate store:** Not applicable
  - Private key security level:** Not applicable
- CA name:** DigiCert Production MPKI TEST Issuing CA
- CA type:** Private
- Signing algorithms:** SHA256 with RSA encryption

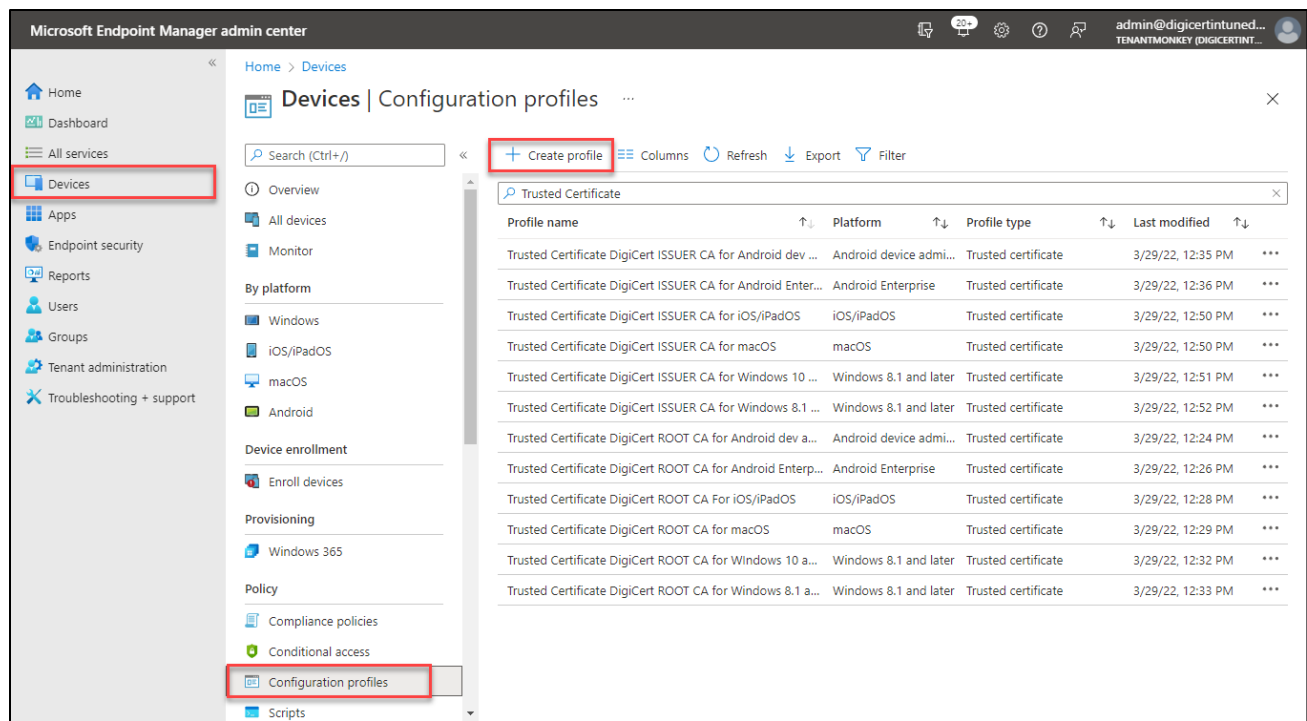
At the bottom, there are buttons for "Back", "Cancel", "Preview", and "Save". The Windows taskbar is visible at the bottom of the screen.

Download CA certificate files from DigiCert PKI Manager **Manage CAs**.

Note: The example shows **Download root certificate**. You should also **Download intermediate certificates** as appropriate to your specific CA hierarchy.



1. In [Microsoft Endpoint Manager admin center](#), select **Devices**, and then select **Configuration profiles**, and then **Create profile**



2. Configure the desired platform of the devices that will receive the profile and select Trusted Certificate from the drop-down or from the Templates list. For detailed steps refer to [Create trusted certificate profiles in Microsoft Intune | Microsoft Docs](#).

Note: When configuring **Windows** platform devices **Destination Store**, select **Root store for Root CA** and **Intermediate store for Intermediate/Issuer CA**.

## SCEP Certificate Configuration

The goal of this procedure is to configure a **DigiCert Certificate Profile** which will work in conjunction with an **Intune Device configuration profile**.

DigiCert Certificate Profile Template	Seat Pool Type
Generic Device Authentication for Intune	Device
Client Authentication for Intune	User
S/MIME (Digital Signature only) for Intune	User

In all cases configure the **DigiCert Certificate Profile** with:

- **Enrollment Method: SCEP**
- **Authentication Method: Azure Auth**

For **Azure Auth** settings, use the values obtained in Azure Active Directory App registration for:

- **Application (client) ID**
- **Client secret**
- **Tenant Domain Name**

Once the DigiCert Certificate Profile is created, you will configure a corresponding Intune Device configuration profile with the required values, settings, and the **DigiCert SCEP URL** for the specific certificate profile.

Note: The format of the SCEP URL that is consumed by the targeted device platforms varies.

The following table describes the form of the SCEP URL to be used by Intune supported device platforms:

Table 2 SCEP URL Form

Target Device Platform	DigiCert SCEP Service Endpoint URL Form	Example
iOS/iPadOS Android macOS	Use the default SCEP service endpoint as displayed in the DigiCert Certificate Profile  http://<HOST>/scep/<Certificate Profile OID>/cgi-bin/pkiclient.exe	http://pki-scep.symauth.com/scep/2.16.840.1.113733.1.16.1.4.nn.n.n.nnnnnnnnn/cgi-bin/pkiclient.exe
Windows (User Store)	<ul style="list-style-type: none"> <li>• HTTPS required</li> <li>• Do not include "/pkiclient.exe" in URL</li> </ul> https://<HOST>/scep/<Certificate.Profile.OID>/cgi-bin	https://pki-scep.symauth.com/scep/2.16.840.1.113733.1.16.1.4.nn.n.n.nnnnnnnnn/cgi-bin
Windows (Computer Store)	<ul style="list-style-type: none"> <li>• HTTPS supported but not required</li> <li>• Do not include "/pkiclient.exe" in URL</li> </ul> http://<HOST>/scep/<Certificate.Profile.OID>/cgi-bin or https://<HOST>/scep/<Certificate.Profile.OID>/cgi-bin	http://pki-scep.symauth.com/scep/2.16.840.1.113733.1.16.1.4.nn.n.n.nnnnnnnnn/cgi-bin  Or https://pki-scep.symauth.com/scep/2.16.840.1.113733.1.16.1.4.nn.n.n.nnnnnnnnn/cgi-bin

Other DigiCert PKI use-case specific information can be found in the following sections and should be used in conjunction with Microsoft docs [Use SCEP certificate profiles with Microsoft Intune | Microsoft Docs](#).

The general workflow for creating an Intune Device configuration profile consists of the following sections:

1. Basics
2. Configuration settings
3. Assignments
4. Applicability Rules (*Applies to Windows 10/11 only*)



The following sections in this guide focus on the **Configuration settings** which determine the certificate details that work in conjunction with the corresponding DigiCert Certificate Profile

For other non-certificate related aspects, refer to Microsoft Documentation.

- [Configure device settings | Microsoft Docs](#)
- [Create and assign SCEP certificate profiles in Intune | Microsoft Docs](#)
- [Assign user and device profiles in Microsoft Intune | Microsoft Docs](#)
- [Applicability Rules | Microsoft Docs](#)

## Device Authentication

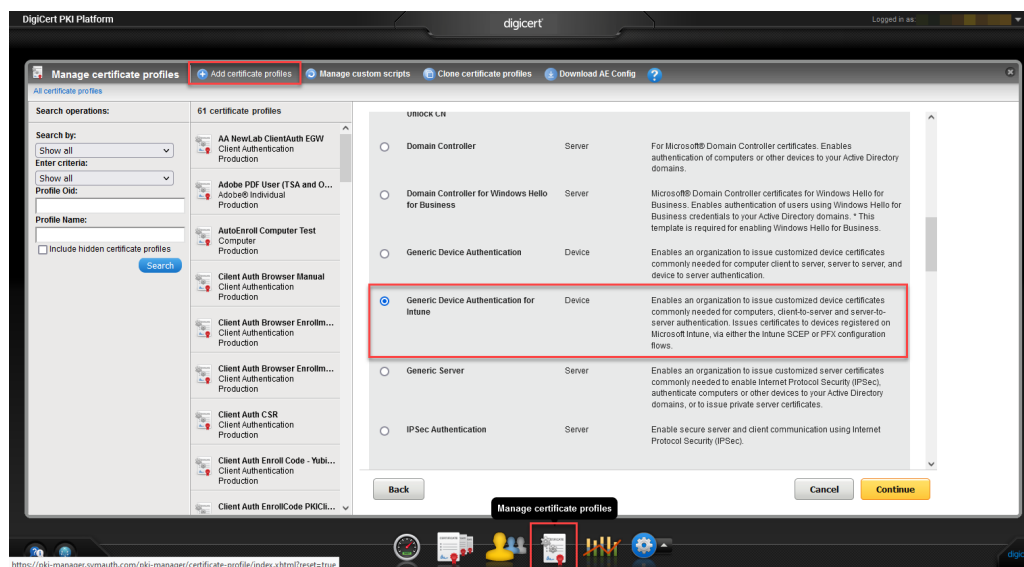
Device certificates contain identity information commonly needed for computer client to server, server to server, and device to server authentication. This type of certificate is issued from DigiCert PKI Platform using the Certificate Profile Template **Generic Device Authentication for Intune** which consumes Seats from your accounts Device Seat Pool.

The following is just an example of a typical certificate configuration and may not meet your specific application requirements.

You should configure the profiles to meet the technical x.509 certificate profile requirements of your 3<sup>rd</sup>-party relying PKI application as well as abiding by any other IT practices, conventions, and certificate policies.

## DigiCert Certificate Profile

1. In DigiCert PKI Manager select **Manage certificate templates**, then **Add certificate profiles**, and select **Generic Device Authentication for Intune** template.



2. Enter a **Certificate friendly name**. In **Primary certificate options**, select the **Certificate authority**.

Note: The **CA Name** is the Issuer CA you download when configuring **Intune Trusted Certificate profile**.

**Create profile:** Select mode Select template **Customize options** Customize services

**Customize certificate options**

Review and change the template options for this profile.

Certificate friendly name:

**Primary certificate options**

Certificate authority: DigiCert Production MPKI TE...	Certificate authority: DigiCert Production MPKI TEST Issuing CA
Enrollment method: SCEP	CA name: DigiCert Production MPKI TEST Issuing CA
Authentication method: Azure Auth	CA type: Private
Certificate store: Not applicable	Signing algorithms: SHA256 with RSA encryption
Private key security level: Not applicable	

3. Select **Enrollment method: SCEP**.

**Create profile:** Select mode Select template **Customize options** Customize services

**Customize certificate options**

Review and change the template options for this profile.

**Certificate friendly name:**

?**Primary certificate options**

Certificate authority:  
DigiCert Production MPKI TE...

Enrollment method:  
**SCEP**

Authentication method:  
**Azure Auth**

Certificate store:  
Not applicable

Private key security level:  
Not applicable

**Enrollment method:**

SCEP

Use SCEP if you will enroll for user certificates using the Simple Certificate Enrollment Protocol.

4. Select **Authentication method: Azure Auth**, and then enter the values you obtained in Azure Active Directory App registration.


**Customize certificate options**


Review and change the template options for this profile.

**Certificate friendly name:**

 ?

**Primary certificate options**

Certificate authority:  
**Intune QA TEST CA** 

Enrollment method:  
**SCEP** 

**Authentication method:  
Azure Auth**

Certificate store:  
**Not applicable**

Private key security level:  
**Not applicable**

This option was set when the certificate profile was created. It can no longer be modified.

**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.

This MPKI account has already got a Microsoft Intune connection configuration associated with it.

**Application (client) ID:**

**Client Secret (the value, not the ID):**

**Tenant Name :**

(usually something ending with onmicrosoft.com)

5. In **Certificate fields**, configure the **Subject DN** to meet your application and policy requirements.

Note that for any value source which is set for SCEP request, the value will need to be configured to be populated in the Intune Device configuration profile.

In this example the Common Name (CN) component will be submitted in the SCEP request as a unique device identifier value as configured in the corresponding Intune Device configuration profile.

Advanced options

Certificate fields

Subject DN + Add field

- Common Name (CN) Source: Scep Request Required: Yes
- Organizational Unit (OU) Source: Entered by admin Required: No
- Organization (O) Source: Account Value: DigiCert, Inc.

Certificate field:  
Common Name (CN)

Source for the field's value:  
Scep Request

Required ?  
 Yes  
 No

6. Including a **SubjectAltName** (SAN) is optional, although many relying PKI applications can make use of a SAN value.

Note that for any value source which is set for SCEP request, the value will need to be configured to be populated in the Intune Device configuration profile.

**SubjectAltName** + Add field

**DNS Name**  
Source: Scep Request  
Required: Yes

**Add certificate field**  
Select a field to add to the certificate and define the value for the new field.

Certificate field:  
DNS Name

Source for the field's value:  
Scep Request

Required ?  
 Yes  
 No

7. Configure the **Key Usage (KU)** to meet your application and policy requirements. This example shows the typical settings for client device authentication.

**Key Usage (KU)**

Key Usage values

The Key Usage extension defines the security services for which a certificate can be used. The options can be used in any combination.

**Criticality**  
 True  False

Digital Signature  
 Key Encipherment  
 Non Repudiation  
 Data Encipherment  
 Key Agreement

8. Configure the **Extended Key Usage (EKU)** to meet your application and policy requirements.

This example shows the typical settings for client device authentication.

**Extended Key Usage (EKU)**

Extended Key Usage values

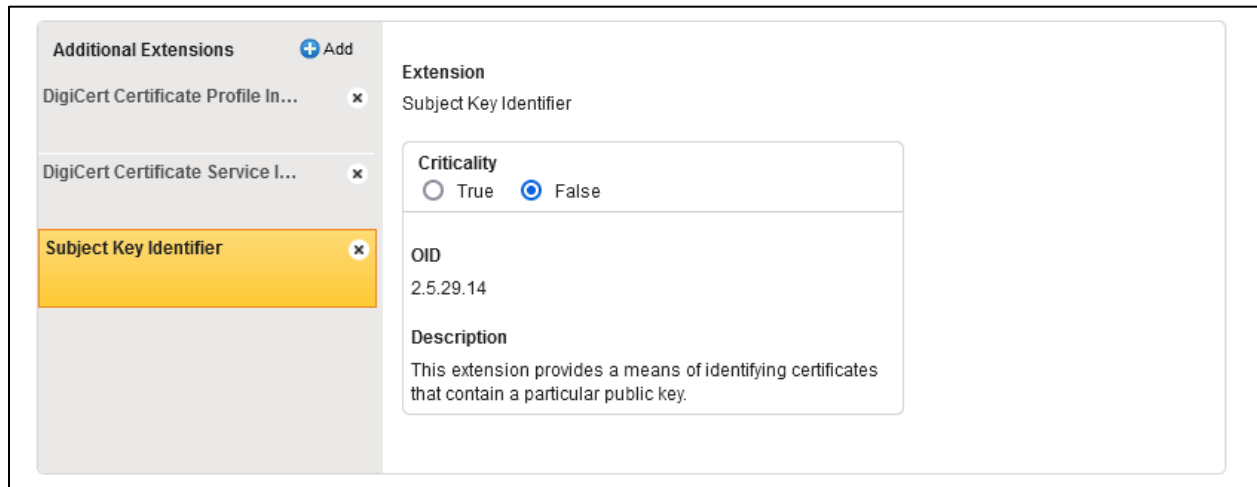
The Extended Key Usage extension indicates how a certificate's public key can be used.

**EKU Criticality**

True  False

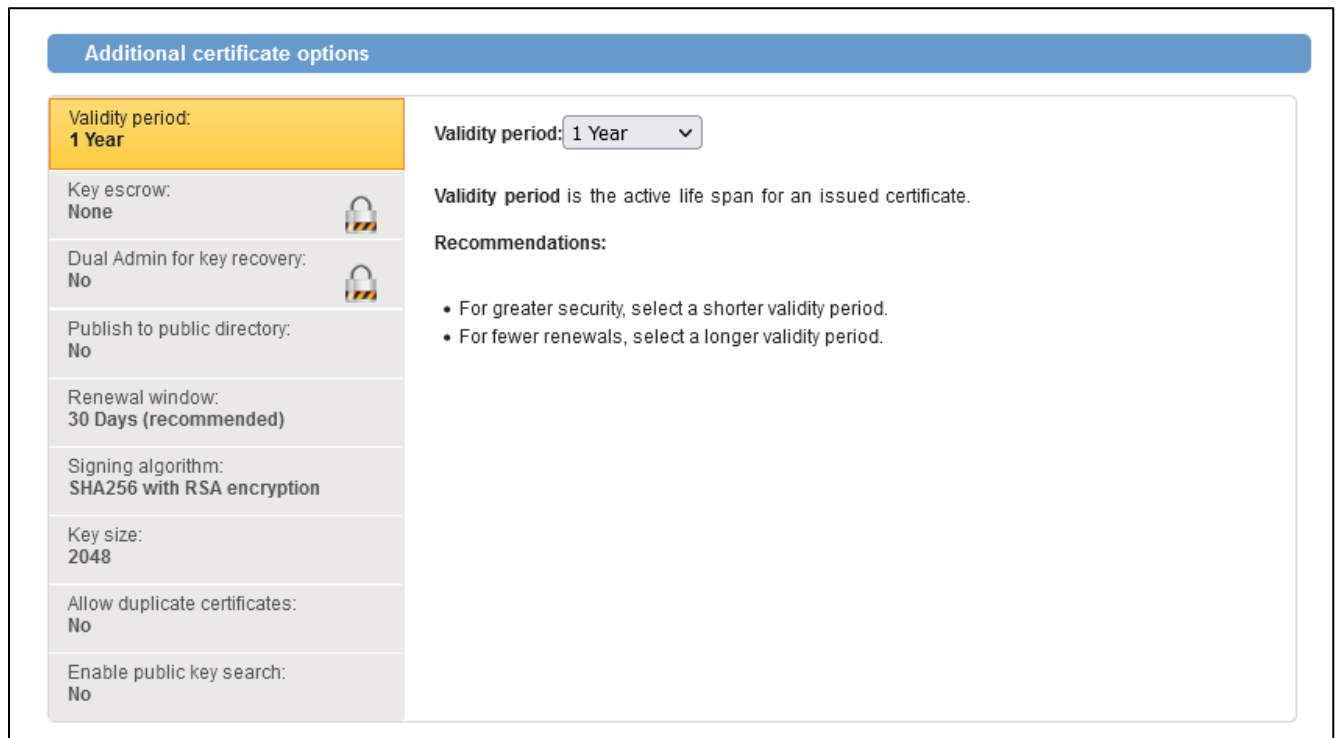
- Client Authentication (1.3.6.1.5.5.7.3.2)
- IPSec IKE-Intermediate (1.3.6.1.5.5.8.2.2)
- IPSec IKE (1.3.6.1.5.5.7.3.17)
- Signing KDC Responses (1.3.6.1.5.2.3.5)

9. Configure the **Additional Extensions** to meet your application and policy requirements. Subject Key Identifier is a standard certificate extension that can be useful to your relying application use-case. The DigiCert extensions while useful are not required.



10. Configure the **Additional certificate options** to meet your application and policy requirements.

Note the Validity period and Key size as you will configure these settings in the Intune Device configuration profile.







11. Upon saving the profile, copy the **SCEP service endpoint URL**.

The SCEP URL will be used later when configuring the Intune Device configuration profile.

Note: Intune Device configuration profiles for Windows platform devices require translation of the SCEP URL. Refer to **Table 2 SCEP URL Form**.

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



### Intune\_SCEP\_device

**Seat pool:** Device  
**Mode:** Production  
**Status:** Active  
**Certificate template name:** Generic Device Authentication for Intune  
**Certificate Profile OID:** 2.16.840.1.113733.1.16.1. [redacted]  
**CA name:** DigiCert Production MPKI TEST Issuing CA  
**Issued:** 0  
**Pending pickup:** 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://pki-scep.symauth.com/scep/2.16.840.1.113733.1.16.1.\[redacted\]62/cgi-bin/pkiclient.exe](http://pki-scep.symauth.com/scep/2.16.840.1.113733.1.16.1.[redacted]62/cgi-bin/pkiclient.exe)

NOTE: Some services like Microsoft Endpoint Manager (formerly Microsoft Intune) use 'https', others such as Cisco routers 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

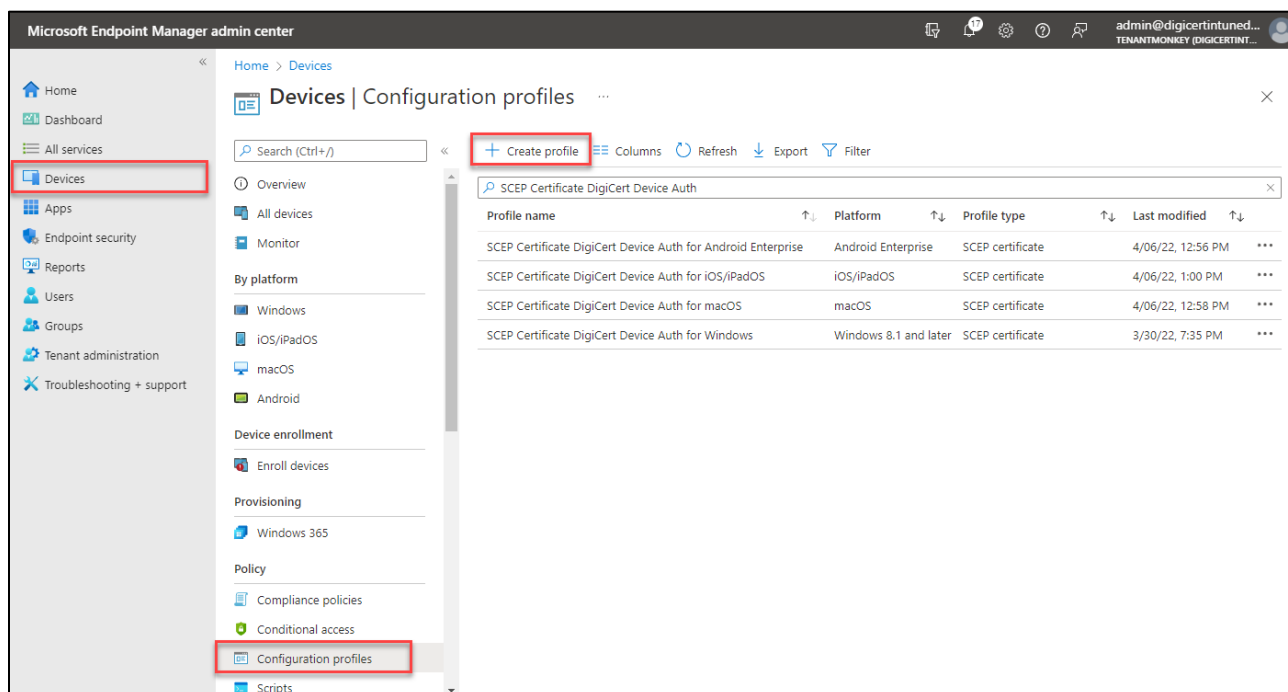
 Select where PKI Manager obtains identifiers for the user. Seat ID is used to uniquely identify the user to PKI Manager. User email is required for user searches and, if configured, to send notifications to the user.

Seat ID:	Common name
User email:	Email

Edit

## Microsoft Device Configuration Profile

1. In [Microsoft Endpoint Manager admin center](#), select **Devices**, and then select **Configuration profiles**, and then **Create profile**.



2. Configure the desired platform of the devices that will receive the profile and select **SCEP Certificate** from the drop-down or from the Templates list.
3. For **Configuration Settings**, configure settings and values to match your corresponding DigiCert Certificate Profile.

Setting	Comments
Certificate type: Device	Corresponds to the DigiCert Profile Type and Seat Pool Type of "Device". Depending on the platform OS behavior, determines the storage location of the key/certificate on the target device platform.
Subject name format	Include attributes/values that are will be sourced in the SCEP request by the DigiCert Certificate Profile.
Subject alternative name	Include attributes/values that are will be sourced in the SCEP request by the DigiCert Certificate Profile.
Certificate validity period	Match with the DigiCert Certificate Profile configuration.
Key storage provider (KSP)	Only determines the target platform behavior.

Setting	Comments
Key usage	<p>The certificate issued by DigiCert will contain the Key usage (typically, Digital Signature, Key Encipherment) as set in the DigiCert Certificate Profile regardless of the Microsoft configuration setting.</p> <p>However, this setting may also influence how the target platform OS enforces key flags settings and usages on that device and therefore it is recommended that the setting match the intended purpose in the DigiCert Certificate Profile configuration.</p>
Key size	Match with the DigiCert Certificate Profile configuration.
Hash algorithm	Select the strongest level of security that the connecting devices support.
Root certificate	<p>This should be the CA Certificate that issues the end-entity as configured in the DigiCert Certificate Profile.</p> <p>If you are using a multi-tier CA certificate hierarchy then you should select the Issuer CA certificate file.</p> <p>See Intune Trusted Certificate profile.</p>
Extended key usage	<p>The certificate issued by DigiCert will contain the Extended key usage as set in the DigiCert Certificate Profile regardless of Microsoft configuration setting.</p> <p>However, this setting may also influence how the target platform OS enforces key flags settings and usages on that device and therefore it is recommended that the setting match the intended purpose in the DigiCert Certificate Profile configuration.</p>
Renewal threshold (%)	This value should be tuned to match the Renewal window setting in the DigiCert Certificate Profile.
SCEP Server URL	For proper formatting refer to Table 2 SCEP URL Form.

Home > Devices > SCEP Certificate DigiCert Device Auth >

## SCEP certificate

Windows 8.1 and later

1 Configuration settings 2 Review + save

Certificate type

Subject name format \*

Subject alternative name

Attribute	Value
DNS	{{AzureADDeviceId}},onmicrosoft.com
	Not configured

Certificate validity period \*

Key storage provider (KSP) \*

Key usage \*

Key size (bits) \*

Hash algorithm \*

Root Certificate \*

+ Root Certificate

Extended key usage \*

Name	Object Identifier	Predefined values
Client Authentication	1.3.6.1.5.5.7.3.2	Client Authentication (1.3.6.1...
Not configured	Not configured	Not configured

Enrollment Settings

Renewal threshold (%) \*

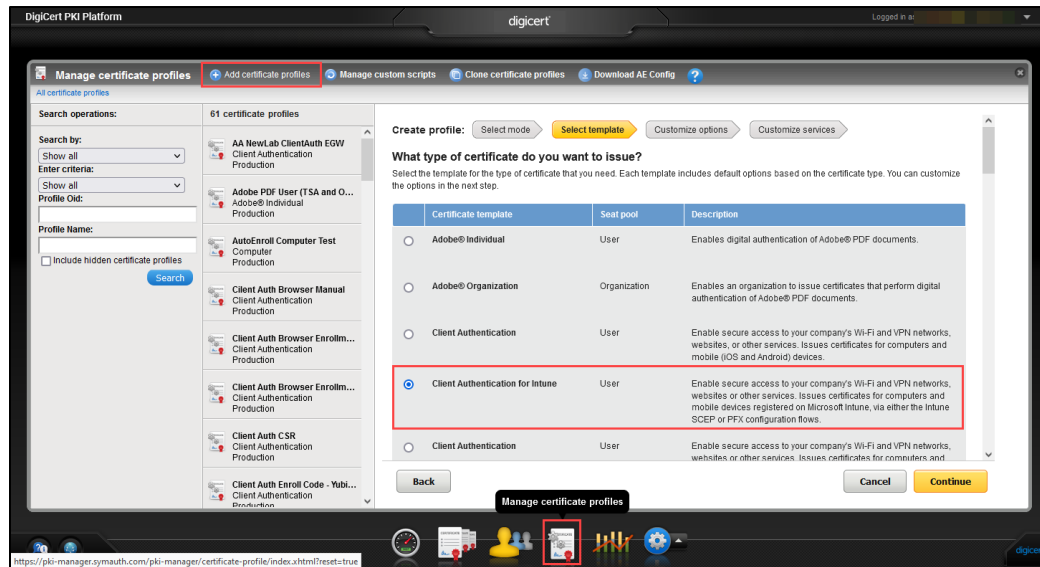
SCEP Server URLs \*

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

## User Client Authentication

### DigiCert Certificate Profile

1. In DigiCert PKI Manager select **Manage certificate Templates**, then **Add certificate profiles**, and select **Client Authentication** for Intune template.



2. Enter a **Certificate friendly name**, and in **Primary certificate options** select the **Certificate authority**.

Note: The **CA Name** is the Issuer CA you download when configuring **Intune Trusted Certificate profile**.

**Create profile:** Select mode Select template **Customize options** Customize services

**Customize certificate options**

Review and change the template options for this profile.

Certificate friendly name:

 ?

#### Primary certificate options

Certificate authority:  
DigiCert Production MPKI TE...

Enrollment method:  
SCEP

Authentication method:  
Azure Auth

Certificate store:  
Not applicable

Private key security level:  
Not applicable

Certificate authority:

DigiCert Production MPKI TEST Issuing CA ?

CA name:

DigiCert Production MPKI TEST Issuing CA

CA type:

Private

Signing algorithms:

SHA256 with RSA encryption

### 3. Select Enrollment method: SCEP

**Create profile:** Select mode Select template **Customize options** Customize services

**Customize certificate options**

Review and change the template options for this profile.

Certificate friendly name:

 ?

#### Primary certificate options

Certificate authority:  
DigiCert Production MPKI TE...

Enrollment method:  
SCEP

Authentication method:  
Azure Auth

Certificate store:  
Not applicable

Private key security level:  
Not applicable

Enrollment method:

SCEP

Use SCEP if you will enroll for user certificates using the Simple Certificate Enrollment Protocol.

### 4. Select Authentication method: Azure Auth, and then enter the values you obtained in Azure Active Directory App registration.


**Customize certificate options**


Review and change the template options for this profile.

**Certificate friendly name:**

 ?

**Primary certificate options**

Certificate authority:  
**Intune QA TEST CA** 

Enrollment method:  
**SCEP** 

Authentication method:  
**Azure Auth**

Certificate store:  
**Not applicable**

Private key security level:  
**Not applicable**

This option was set when the certificate profile was created. It can no longer be modified.

**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.

This MPKI account has already got a Microsoft Intune connection configuration associated with it.

**Application (client) ID:**

**Client Secret (the value, not the ID):**

**Tenant Name :**

(usually something ending with onmicrosoft.com)

5. In **Certificate fields**, configure the **Subject DN** to meet your application and policy requirements.

Note that for any value source which is set for SCEP request, the value will need to be configured to be populated in the Intune Device configuration profile.

In this example the Common Name (CN) component will be submitted in the SCEP request as a unique device identifier value as configured in the corresponding Intune Device configuration profile.

**Certificate fields**

**Subject DN** + Add field

- Common Name (CN)** (Selected)
  - Source: Scep Request
  - Required: Yes
- Organizational Unit (OU)
  - Source: Fixed value
  - Value: VPN-WEB
- Organizational Unit (OU)
  - Source: Fixed value
  - Value: MULTI-ALLOWED

**Edit certificate field**

Certificate field: Common Name (CN)

Source for the field's value: Scep Request

Required ?

Yes

No

6. Including a **SubjectAltName** (SAN) is optional, although many relying PKI applications can make use of a SAN value.

Note that for any value source which is set for SCEP request, the value will need to be configured to be populated in the Intune Device configuration profile.

**SubjectAltName** + Add field

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

**Edit certificate field**

Certificate field: Other Name (UPN)

Source for the field's value: Scep Request

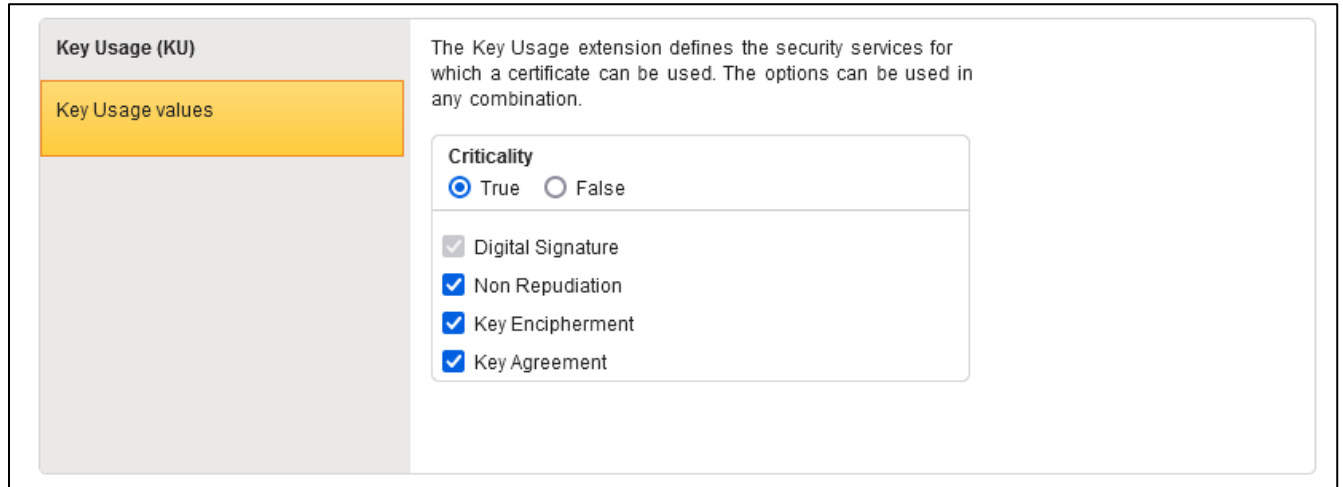
Required ?

Yes

No



7. Configure the **Key Usage (KU)** to meet your application and policy requirements.  
This example shows the typical settings for user client authentication.



**Key Usage (KU)**

Key Usage values

The Key Usage extension defines the security services for which a certificate can be used. The options can be used in any combination.

**Criticality**

True  False

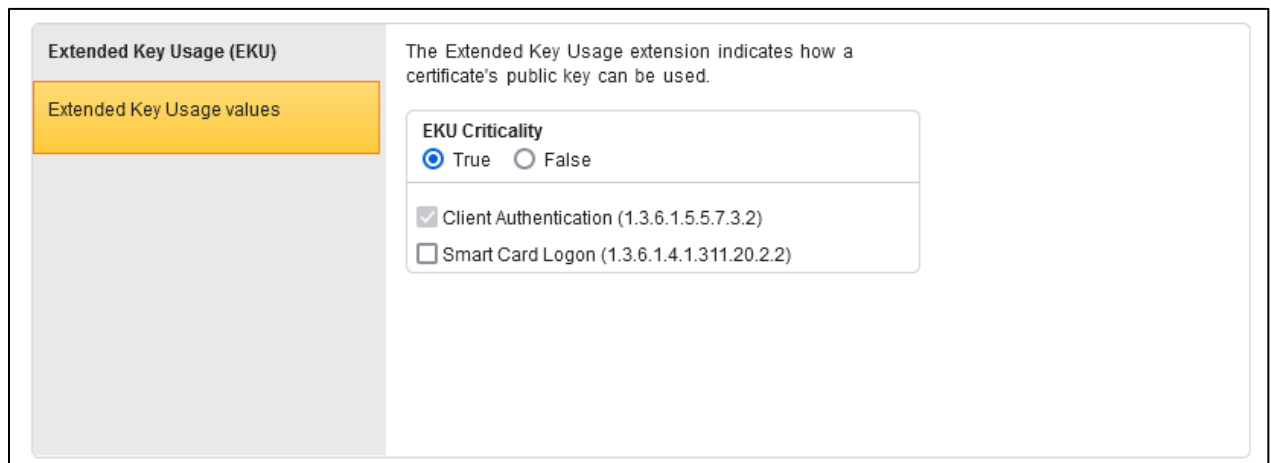
Digital Signature

Non Repudiation

Key Encipherment

Key Agreement

8. Configure the **Extended Key Usage (EKU)** to meet your application and policy requirements.  
This example shows the typical settings for user client authentication.



**Extended Key Usage (EKU)**

Extended Key Usage values

The Extended Key Usage extension indicates how a certificate's public key can be used.

**EKU Criticality**

True  False



Client Authentication (1.3.6.1.5.5.7.3.2)

Smart Card Logon (1.3.6.1.4.1.311.20.2.2)

9. Configure the **Additional certificate options** to meet your application and policy requirements.

Note the Validity period and Key size as you will configure these settings in the Intune Device configuration profile.

Additional certificate options

<b>Validity period:</b> <b>1 Year</b>	<b>Validity period:</b> 1 Year <input type="button" value="v"/>
<b>Key escrow:</b> None 	<p><b>Validity period</b> is the active life span for an issued certificate.</p> <p><b>Recommendations:</b></p> <ul style="list-style-type: none"> <li>For greater security, select a shorter validity period.</li> <li>For fewer renewals, select a longer validity period.</li> </ul>
<b>Dual Admin for key recovery:</b> No 	
<b>Publish to public directory:</b> No	
<b>Renewal window:</b> 30 Days (recommended)	
<b>Signing algorithm:</b> SHA256 with RSA encryption	
<b>Key size:</b> 2048	
<b>Allow duplicate certificates:</b> Yes	
<b>Enable public key search:</b> No	

10. Upon saving the profile, copy the **SCEP service endpoint URL**.

The SCEP URL will be used later when configuring the Intune Device configuration profile.

Note: Intune Device configuration profiles for Windows platform devices require translation of the SCEP URL. Refer to **Table 2 SCEP URL Form**.



### Intune\_SCEP\_user

**Seat pool:** User  
**Mode:** Production  
**Status:** Active  
**Certificate template name:** Client Authentication for Intune  
**Certificate Profile OID:** 2.16.840.1.113733.1.16.1.██████████  
**CA name:** DigiCert Production MPKI TEST Issuing CA  
**Issued:** 0  
**Pending pickup:** 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://pki-scep.symauth.com/scep/2.16.840.1.113733.1.16.1.██████████0/cgi-bin/pkiclient.exe>

NOTE: Some services like Microsoft Endpoint Manager (formerly Microsoft Intune) use 'https', others such as Cisco routers 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)

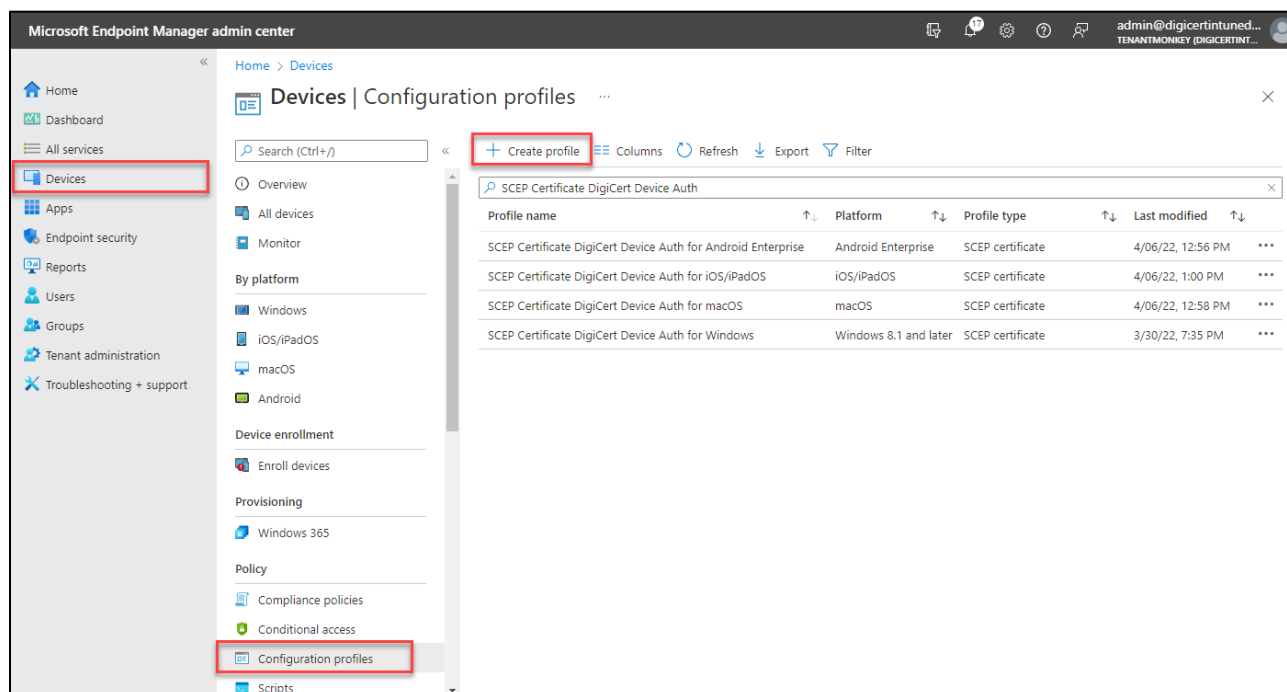
**Customize user identification**



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.

## Microsoft Device Configuration Profile

1. In [Microsoft Endpoint Manager admin center](#), select **Devices**, and then select **Configuration profiles**, and then **Create profile**.



2. Configure the desired platform of the devices that will receive the profile and select **SCEP Certificate** from the drop-down or from the Templates list.
3. For **Configuration Settings**, configure settings and values to match your corresponding DigiCert Certificate Profile.

Setting	Comments
Certificate type: User	Corresponds to the DigiCert Profile Type and Seat Pool Type of "User". Depending on the platform OS behavior, determines the storage location of the key/certificate on the target device platform.
Subject name format	Include attributes/values that are will be sourced in the SCEP request by the DigiCert Certificate Profile.
Subject alternative name	Include attributes/values that are will be sourced in the SCEP request by the DigiCert Certificate Profile.
Certificate validity period	Match with the DigiCert Certificate Profile configuration.
Key storage provider (KSP)	Only determines the target platform behavior.

Setting	Comments
Key usage	<p>The certificate issued by DigiCert will contain the Key usage (typically, Digital Signature, Non Repudiation, Key Encipherment, Key Agreement) as set in the DigiCert Certificate Profile regardless of the Microsoft configuration setting.</p> <p>However, this setting may also influence how the target platform OS enforces key flags settings and usages on that device and therefore it is recommended that the setting match the intended purpose in the DigiCert Certificate Profile configuration.</p>
Key size	Match with the DigiCert Certificate Profile configuration.
Hash algorithm	Select the strongest level of security that the connecting devices support.
Root certificate	<p>This should be the CA Certificate that issues the end-entity as configured in the DigiCert Certificate Profile.</p> <p>If you are using a multi-tier CA certificate hierarchy then you should select the Issuer CA certificate file.</p> <p>See Intune Trusted Certificate profile.</p>
Extended key usage	<p>The certificate issued by DigiCert will contain the Extended key usage as set in the DigiCert Certificate Profile regardless of Microsoft configuration setting.</p> <p>However, this setting may also influence how the target platform OS enforces key flags settings and usages on that device and therefore it is recommended that the setting match the intended purpose in the DigiCert Certificate Profile configuration.</p>
Renewal threshold (%)	This value should be tuned to match the Renewal window setting in the DigiCert Certificate Profile.
SCEP Server URL	For proper formatting refer to Table 2 SCEP URL Form

Home > Devices > SCEP Certificate DigiCert User Client Authentication >

## SCEP certificate

Windows 8.1 and later

**1** Configuration settings **2** Review + save

Certificate type: User

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

Subject alternative name ⓘ

Attribute	Value
User principal name (UPN)	{{UserPrincipalName}}
	Not configured

Certificate validity period \* ⓘ: Years 1

Key storage provider (KSP) \* ⓘ: Enroll to Trusted Platform Module (TPM) KSP if present, otherwise Software K...

Key usage \* ⓘ: 2 selected

Key size (bits) \* ⓘ: 2048

Hash algorithm \* ⓘ: SHA-2

Root Certificate \* ⓘ: Trusted Certificate DigiCert ISSUER CA for Windows 10 and later

+ 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.../cgi-bin

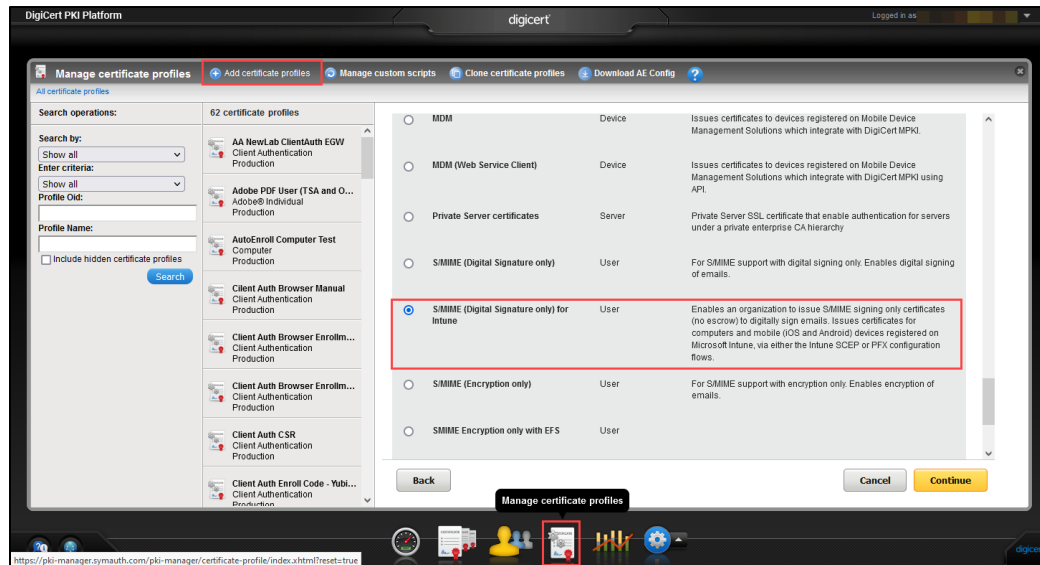
e.g. https://contoso.com/certsrv/mscep/mscep.dll

Previous Next

## S/MIME (Digital Signature only) for Intune

### DigiCert Certificate Profile

1. In DigiCert PKI Manager select **Manage certificate Templates**, then **Add certificate profiles**, and select **S/MIME (Digital Signature only) for Intune** template.



2. Enter a **Certificate friendly name**.  
Note: The **CA Name** is the Issuer CA you download when configuring Intune Trusted Certificate profile.

**Create profile:** Select mode → Select template → **Customize options** → Customize services

**Customize certificate options**

Review and change the template options for this profile.

**Certificate friendly name:**

 ?

**Primary certificate options**

<b>Certificate authority:</b> DigiCert PKI Platform C2 Sha...	<b>CA name:</b> DigiCert PKI Platform C2 Shared SMIME Individual Subscriber CA
<b>Enrollment method:</b> PKI Web Services	<b>CA type:</b> Public
<b>Authentication method:</b> 3rd party application	<b>Signing algorithms:</b> SHA256 with RSA encryption
<b>Certificate store:</b> Not applicable	
<b>Private key security level:</b> Not applicable	

3. Select **Enrollment method: SCEP**.

**Create profile:** Select mode Select template **Customize options** Customize services

**Customize certificate options**

Review and change the template options for this profile.

Certificate friendly name:  ?

**Primary certificate options**

Certificate authority: DigiCert PKI Platform C2 Sha...	<b>Enrollment method:</b> SCEP
<b>Enrollment method:</b> SCEP	Use SCEP if you will enroll for user certificates using the Simple Certificate Enrollment Protocol.
Authentication method: <b>Azure Auth</b>	
Certificate store: Not applicable	
Private key security level: Not applicable	

4. Select **Authentication method: Azure Auth**, and then enter the values you obtained in Azure Active Directory App registration.



### Customize certificate options

Review and change the template options for this profile.


Certificate friendly name:

#### Primary certificate options

Certificate authority:  
**Intune QA TEST CA** 

This option was set when the certificate profile was created. It can no longer be modified.

Enrollment method:  
**SCEP** 

Authentication method:  
**Azure Auth**

**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.

Certificate store:  
**Not applicable**

Private key security level:  
**Not applicable**

This MPKI account has already got a Microsoft Intune connection configuration associated with it.

**Application (client) ID:**

**Client Secret (the value, not the ID):**

**Tenant Name :**

(usually something ending with onmicrosoft.com)

- In **Certificate fields**, configure the **Subject DN** to meet your application and policy requirements.

Note that for any value source which is set for SCEP request, the value will need to be configured to be populated in the Intune Device configuration profile.

In this example the Common Name (CN) component will be submitted in the SCEP request as a unique device identifier value as configured in the corresponding Intune Device configuration profile.

The screenshot shows the 'Advanced options' section for 'Certificate fields'. On the left, under 'Subject DN', there is a list of fields: 'Common Name (CN)' (Source: Scep Request, Required: Yes), 'Organizational Unit (OU)' (Source: Fixed value, Value: S/MIME Signing), 'Organizational Unit (OU)' (Source: Fixed value, Value: MULTI-ALLOWED), 'Organizational Unit (OU)' (Source: Fixed value, Value: For Test/Demo ...), and 'Organization (O)' (Source: Fixed value, Value: DigiCert, Inc.). The 'Common Name (CN)' field is selected. On the right, the 'Edit certificate field' pane shows the configuration for the 'Common Name (CN)' field. The 'Certificate field' is 'Common Name (CN)', the 'Source for the field's value' is 'Scep Request', and the 'Required?' checkbox is checked.

- Including a **SubjectAltName** (SAN) is optional, although many relying PKI applications can make use of a SAN value.

Note that for any value source which is set for SCEP request, the value will need to be configured to be populated in the Intune Device configuration profile.

The screenshot shows the 'SubjectAltName' configuration interface. On the left, under 'SubjectAltName', there is a list of fields: 'RFC822 Name' (Source: Scep Request, Required: Yes). The 'RFC822 Name' field is selected. On the right, the 'Edit certificate field' pane shows the configuration for the 'RFC822 Name' field. The 'Certificate field' is 'RFC822 Name', the 'Source for the field's value' is 'Scep Request', and the 'Required?' checkbox is checked. A note above the configuration pane states: 'Note: This certificate field is required for this template. The field cannot be deleted.'

7. Configure the **Key Usage (KU)** to meet your application and policy requirements.  
This example shows the typical settings for user S/MIME digital signature.

The screenshot shows the 'Key Usage (KU)' configuration page. On the left, there is a sidebar with 'Key Usage (KU)' at the top and 'Key Usage values' highlighted in orange. The main content area has a title 'Key Usage (KU)' and a descriptive paragraph: 'The Key Usage extension defines the security services for which a certificate can be used. The options can be used in any combination.' Below this, there are two sections: 'Criticality' with radio buttons for 'True' (selected) and 'False', and a list of services with checkboxes: 'Digital Signature' (checked) and 'Non Repudiation' (checked).

8. Configure the **Extended Key Usage (EKU)** to meet your application and policy requirements.  
This example shows the typical settings for user S/MIME digital signature.

The screenshot shows the 'Extended Key Usage (EKU)' configuration page. On the left, there is a sidebar with 'Extended Key Usage (EKU)' at the top and 'Extended Key Usage values' highlighted in orange. The main content area has a title 'Extended Key Usage (EKU)' and a descriptive paragraph: 'The Extended Key Usage extension indicates how a certificate's public key can be used.' Below this, there are two sections: 'EKU Criticality' with radio buttons for 'True' (selected) and 'False', and a list of services with checkboxes: 'Email Protection (1.3.6.1.5.5.7.3.4)' (checked).

9. Configure the **Additional certificate options** to meet your application and policy requirements.

Note the Validity period and Key size as you will configure these settings in the Intune Device configuration profile.

Additional certificate options

<b>Validity period:</b> 1 Year	<b>Validity period:</b> 1 Year <input type="button" value="v"/>
<b>Key escrow:</b> None	<b>Validity period</b> is the active life span for an issued certificate.
<b>Dual Admin for key recovery:</b> No	<b>Recommendations:</b>
<b>Publish to public directory:</b> Yes	<ul style="list-style-type: none"> <li>For greater security, select a shorter validity period.</li> <li>For fewer renewals, select a longer validity period.</li> </ul>
<b>Renewal window:</b> 30 Days (recommended)	
<b>Signing algorithm:</b> SHA256 with RSA encryption	
<b>Key size:</b> 2048	
<b>Allow duplicate certificates:</b> Yes	
<b>Enable public key search:</b> No	

10. Upon saving the profile, copy the **SCEP service endpoint URL**.

The SCEP URL will be used later when configuring the Intune Device configuration profile.

Note: Intune Device configuration profiles for Windows platform devices require translation of the SCEP URL. Refer to **Table 2 SCEP URL Form**.



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



### Intune\_SCEP\_SMIME\_DigitalSignature

**Seat pool:** User

**Mode:** Production

**Status:** Active

**Certificate template name:** S/MIME (Digital Signature only) for Intune

**Certificate Profile OID:** 2.16.840.1.113733.1.16.1

**CA name:** DigiCert PKI Platform C2 Shared SMIME Individual Subscriber CA

**Issued:** 0

**Pending pickup:** 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://pki-scep.symauth.com/scep/2.16.840.1.113733.1.16.1.0/cgi-bin/pkiclient.exe`

NOTE: Some services like Microsoft Endpoint Manager (formerly Microsoft Intune) use 'https', others such as Cisco routers use 'http'.

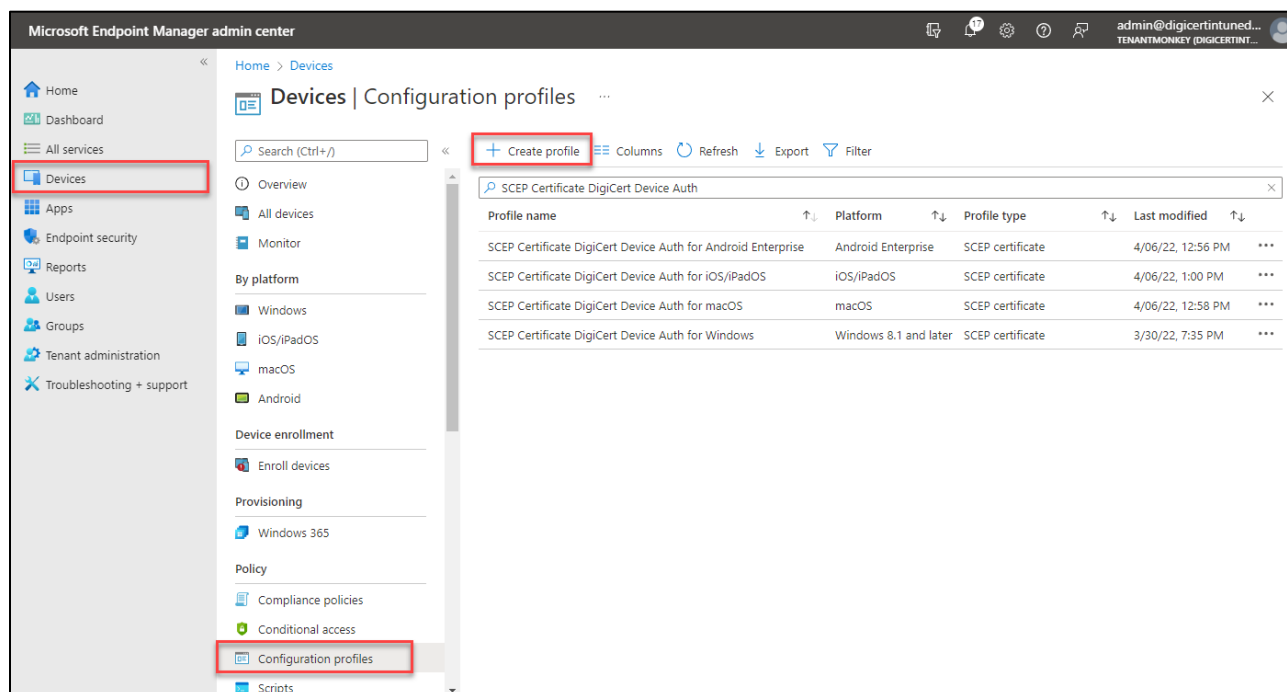
Your user device CSRs may include:

- 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](#)

## Microsoft Device Configuration Profile

1. In [Microsoft Endpoint Manager admin center](#), select **Devices**, and then select **Configuration profiles**, and then **Create profile**.



2. Configure the desired platform of the devices that will receive the profile and select **SCEP Certificate** from the drop-down or from the Templates list.
3. For **Configuration Settings**, configure settings and values to match your corresponding DigiCert Certificate Profile.

Setting	Comments
Certificate type: User	Corresponds to the DigiCert Profile Type and Seat Pool Type of "User". Depending on the platform OS behavior, determines the storage location of the key/certificate on the target device platform.
Subject name format	Include attributes/values that are will be sourced in the SCEP request by the DigiCert Certificate Profile.
Subject alternative name	Include attributes/values that are will be sourced in the SCEP request by the DigiCert Certificate Profile.
Certificate validity period	Match with the DigiCert Certificate Profile configuration.
Key storage provider (KSP)	Only determines the target platform behavior.

Setting	Comments
Key usage	<p>The certificate issued by DigiCert will contain the Key usage (typically, Digital Signature, Non Repudiation) as set in the DigiCert Certificate Profile regardless of the Microsoft configuration setting.</p> <p>However, this setting may also influence how the target platform OS enforces key flags settings and usages on that device and therefore it is recommended that the setting match the intended purpose in the DigiCert Certificate Profile configuration.</p>
Key size	Match with the DigiCert Certificate Profile configuration.
Hash algorithm	Select the strongest level of security that the connecting devices support.
Root certificate	<p>This should be the CA Certificate that issues the end-entity as configured in the DigiCert Certificate Profile.</p> <p>If you are using a multi-tier CA certificate hierarchy then you should select the Issuer CA certificate file.</p> <p>See Intune Trusted Certificate profile.</p>
Extended key usage	<p>The certificate issued by DigiCert will contain the Extended key usage as set in the DigiCert Certificate Profile regardless of Microsoft configuration setting.</p> <p>However, this setting may also influence how the target platform OS enforces key flags settings and usages on that device and therefore it is recommended that the setting match the intended purpose in the DigiCert Certificate Profile configuration.</p>
Renewal threshold (%)	This value should be tuned to match the Renewal window setting in the DigiCert Certificate Profile.
SCEP Server URL	For proper formatting refer to Table 2 SCEP URL Form

Home > Devices > SCEP Certificate DigiCert User SMIME Digital Signature Only >

## SCEP certificate

Windows 8.1 and later

1 Configuration settings 2 Review + save

Certificate type: User

Subject name format: CN={{UserName}},E={{EmailAddress}}

Subject alternative name

Attribute	Value
Email address	{{EmailAddress}}
	Not configured

Certificate validity period: 1 Years

Key storage provider (KSP): Enroll to Trusted Platform Module (TPM) KSP if present, otherwise Software K...

Key usage: 2 selected

Key size (bits): 2048

Hash algorithm: SHA-2

Root Certificate: Trusted Certificate DigiCert ISSUER CA for Windows 10 and later

+ Root Certificate

Extended key usage

Name	Object Identifier	Predefined values
Secure Email	1.3.6.1.5.5.7.3.4	Secure Email (1.3.6.1.5.5.7.3.4)
Not configured	Not configured	Not configured

Enrollment Settings

Renewal threshold (%): 20

SCEP Server URLs

https://pki-scep.symauth.com/scep/2.16.840.1.113733.1.16.1.4.27.1.8.1412550860/cgi-bin

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

Previous Next



## Joining a Device to Intune MDM

- [Enroll devices in Microsoft Intune | Microsoft Docs](#)
  - [Enroll Android devices | Microsoft Docs](#)
  - [Set up enrollment for macOS devices in Intune | Microsoft Docs](#)
  - [MDM enrollment of Windows 10-based devices | Microsoft Docs](#)

## Verify Certificate Issuance details in DigiCert PKI Platform

Issued certificates can be verified in **DigiCert PKI Manager** by viewing the certificate profile in **Manage certificate profiles** or by using search certificates in **Manage certificates**.

### Manage certificate profiles

The screenshot shows the DigiCert PKI Platform interface. The main window is titled "Manage certificate profiles" and contains a search sidebar on the left, a list of certificate profiles in the center, and a detailed view of the selected profile on the right.

**Search operations:**

- Search by: Show all
- Enter criteria: Active
- Profile Oid: [Empty field]
- Profile Name: [Empty field]
- Include hidden certificate profiles
- Search button

**61 certificate profiles**

- IOS Client Auth - Client Authentication - Production
- LH\_Intune\_demo-NDES - Client Authentication for Intune - Production
- LH\_Intune\_demo-SMIME - Secure Email - Production
- LH\_Intune\_demo\_SCEP - Client Authentication for Intune - Production** (Selected)
- LH\_Intune\_SCEP\_device - Generic Device Authentication... - Production

**1 certificate profiles selected**

- Customize options
- Hide profile
- Suspend profile
- Move profile to test
- Enroll user for a certificate
- Delete profile

**LH\_Intune\_demo\_SCEP**

- Seat pool: User
- Mode: Production
- Status: Active
- Certificate template name: Client Authentication for Intune
- Certificate Profile OID: 2.16.840.1.113733.1.16.1.4
- CA name: DigiCert Production MPKI TEST Issuing CA
- Issued: 17
- Pending pickup: 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://pki-scep.symauth.com/scep/2.16.840.1.113733.1.16.1.4. /cgi-bin/pkiclient.exe`

NOTE: Some services like Microsoft Endpoint Manager (formerly Microsoft Intune) use 'https', others such as Cisco routers use 'http'.

Your user device CSRs may include:

## Manage certificates

The screenshot displays the DigiCert PKI Platform interface for managing certificates. The main area shows a search for certificates, with 17 results found. The search filters include 'Certificate profile' set to 'LH\_Intune\_demo\_SCEP'. The results list shows certificates with various statuses: Valid, Expired, and Revoked. A detailed view of a selected certificate is shown on the right, including the following information:

- Seat ID:** [redacted]@digicertintunedemo.onmicrosoft.com
- Status:** Valid
- Certificate Authority:** DigiCert Production MPKI TEST Issuing CA
- Issued to:** [redacted]
- Valid from:** Nov 16, 2021 12:00:00 AM
- Expires on:** Nov 16, 2022 11:59:59 PM
- Subject DN:** CN=[redacted], OU=LH\_Intune\_demo, OU=VPN-WEB, OU=MULTI-ALLOWED
- Issuer DN:** CN=DigiCert Production MPKI TEST Issuing CA, OU=FOR TEST PURPOSES ONLY, O=DigiCert Inc, C=US
- Serial number:** 739b9d33657291f53fc1cd40547eb659
- Certificate profile:** LH\_Intune\_demo\_SCEP
- Seat pool:** User

## Revocation of Certificates in Intune

There are many scenarios where certificates that were provisioned by Intune are then removed and revoked.

See [Remove SCEP and PKCS certificates in Microsoft Intune | Microsoft Docs](#)

With DigiCert/Intune SCEP integrations which communicate via the Azure Active Directory App registration, Intune maintains a list of certificates to be revoked. The DigiCert PKI Platform fetches 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 revoked status of the certificate is then available via DigiCert Validation Services (CRL/OCSP), once the revocation process is complete.