Cogito Group

DIGITAL IDENTITY AND SECURITY

# Azure Intune Client Configuration

## Cogito PKI Services

## 27 March 2023

## Version 3.4

| | |
|---|---|
| **Owner:** | Cameron Taylor |
| **Contact details:** | Email: Cameron.Taylor@cogitogroup.net<br>Security.Services@cogitogroup.net |
| **Program name:** | PKIaaS Services |
| **Division/Unit:** | Cogito Group |
| **Document status:** | Released and uploaded to Cogito Group web site |

# Revision history

| Revision date | Version No. | Author | Description of changes |
|---|---|---|---|
| 18/03/2019 | 0.1 | Rory Lindebaum | Initial draft. |
| 21/03/2019 | 1.0 | Cameron Miller | Final review. |
| 29/08/2019 | 1.1 | Ryan van den Eykel | Azure UI redesign update. |
| 19/03/2020 | 1.2 | Benjamin Hook | Formatting improvements. |
| 19/03/2020 | 1.3 | Ryan van den Eykel | Azure UI redesign update. |
| 04/06/2020 | 1.4 | Shane Little | Update and review. |
| 01/10/2020 | 1.5 | Cameron Taylor | Azure UI redesign update. |
| 01/12/2020 | 2.0 | Cameron Taylor | Updated for microservice implementation. |
| 16/12/2020 | 2.1 | Cameron Taylor | Updated instruction with additional clarity and specification. |
| 29/01/2021 | 2.2 | Cameron Taylor | Updated to include TLS cert config. |
| 12/05/2021 | 2.3 | Cameron Taylor | Updated to remove explicit references to CA names. |
| 17/05/2022 | 2.4 | Cameron Morris | Updated permissions to reflect change to Microsoft Graph API. |
| 05/12/2022 | 3.0 | Cameron Taylor | Updated Azure Intune Screenshots<br>Added security preface. |
| 07/03/2023 | 3.1 | Cameron Taylor | Inclusion of product information. |
| 16/03/2023 | 3.2 | Tony Martindale | Add Cogito Product Requirements section. |
| 21/03/2023 | 3.3 | Isobel Archer | Edited Cogito Product Requirements section. |
| 27/03/2023 | 3.4 | Tony Martindale | Further edit of Cogito Product Requirements section. |

# Contents

# 1 Overview

This document describes the procedure for adding the Cogito Jellyfish Intune SCEP Connector as a third party SCEP enrollment server.

The procedure can be summarized as a set of goals to accomplish within the Microsoft Azure Portal. These are:

- Create a Jellyfish SCEP *Application* within the Microsoft Azure *Azure Active Directory* service. Provision *API Permissions* and *Secrets* for the Jellyfish Intune SCEP Connector.
- Create a *Trusted certificate Configuration profile* within the Microsoft Azure *Microsoft Endpoint Manager admin center* deploying trust of the Jellyfish Certificate Authority trust chain.
- Create a *SCEP certificate Configuration Profile* within the Microsoft Azure *Microsoft Endpoint Manager admin center* deploying a 'policy' by which Intune may generate and validate Certificate Signing Requests.

**Disclaimer**

Document instructions and screenshots are valid as at ***05/12/2022***. Microsoft Azure Portal, Microsoft Azure Active Directory, and Microsoft Endpoint Manager admin center configuration is subject to change and has a history of modifying workflow, as such content of the document may not directly correlate to Microsoft web tooling appearance or functionality.

# 2 Cogito Product Requirements

Using the Cogito Jellyfish Intune SCEP Connector requires a subscription to one of Cogito's Jellyfish PKIaaS services (a Government service or https://securesme.com/) or a Jellyfish software license.

To arrange a subscription or license, please contact: sales@cogitogroup.net

# 3 Software Security

## 3.1 Preface

Cogito Jellyfish Intune SCEP Connector (usSCEP) provides the highest level of security possible within the Microsoft Intune implementation of the Simple Certificate Enrollment Protocol (SCEP).

Although usSCEP provides an implementation of the Simple SCEP Pre-shared Secret method of Certificate Signing Request (CSR) authentication method, the Microsoft Intune SCEP enrollment process does not use this method of authentication or validation.

usSCEP has a more secure method of authentication and validation than that provided by Microsoft's NDES service. usSCEP does not require the installation of any 'on-site' software such as Microsoft Intune Connector for the NDES service. usSCEP does not require Kerberos authentication and as such does not depend on an 'on-site' deployment of Active Directory.

## 3.2 Intune SCEP Request Flow

Cogito Jellyfish Intune SCEP Connector (usSCEP) conforms to the requirements of the Microsoft Intune SCEP request flow.

The authentication and validation procedure of this flow is implemented through an API request from usSCEP to the Microsoft Graph API. This request is a sequence of two subsequent requests, the first request reads the Service Principal Endpoints for the Intune 'Azure Application', this provides an address for which to submit a SCEP challenge request.

In the Microsoft Intune SCEP request flow, the validation procedure occurs after the CSR is generated, but before the CSR is signed.

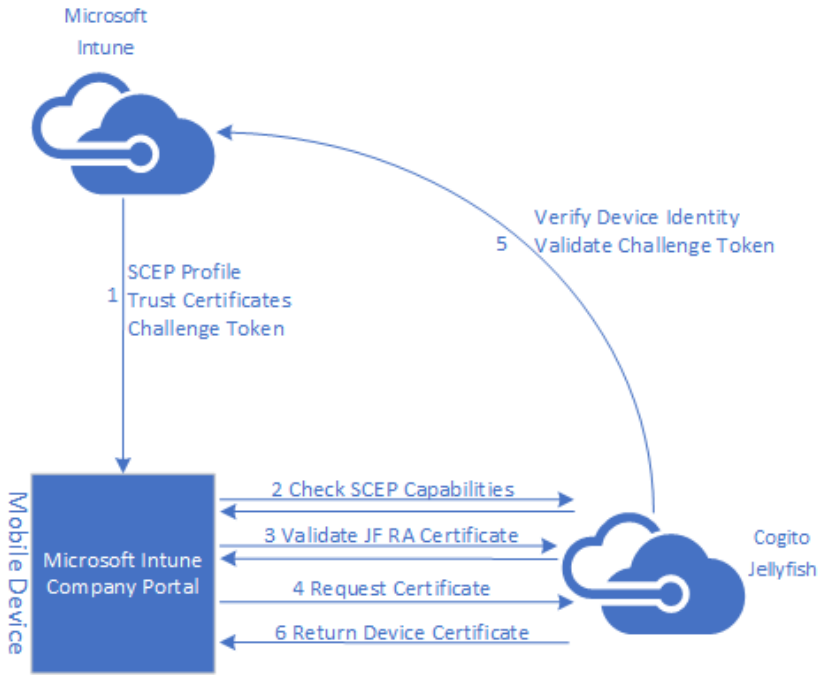


**Figure 1: In step 5 of the Microsoft Intune SCEP request flow, the CSR requested by the device is sent back to Azure Graph API to ensure it conforms to the profile by which it has been generated.**

Azure Intune uses the whole Certificate Signing Request (CSR) as the 'challenge'. This is a distinction from the Simple SCEP implementation in which a 'pre-shared secret' is used as validation.

The Azure Intune method of sending the whole CSR is a significant improvement to a 'pre-shared secret'. However, additional information is required to perform validation using a CSR. In the case of Azure Intune this additional information is already available and used to generate the CSR in the first place. The CSR generation and validation information is saved within the *SCEP certificate Device Configuration Profile* defined in the *Microsoft Endpoint Manager admin center*.

The *SCEP certificate Device Configuration Profile* (SCEP profile) takes the form of an exact match whitelist. The SCEP profile defines exactly which Subjects, Subject Alternatives Names, Key Usages, Extended Key Usages, Key Sizes, Hash Algorithms, and more **MUST** be included in a CSR intended for enrollment using this SCEP Profile. The SCEP Profile is permissioned against a set of Included and Excluded *Azure Active Directory Users or Groups*.

For the purposes of usSCEP validation: every CSR received by the services is sent to the Azure Graph API for validation. Azure Intune compares the contents of the CSR against the SCEP profile. Azure Intune verifies the Device ID contained within the CSR belongs to, or is assigned to a user that belongs to, one of the included Azure Users or Groups, and is **NOT** included in an excluded group. Azure Intune then verifies that all details within the CSR exactly match those of the SCEP profile, including any variable object identifiers exactly match those of the user or device the CSR has been determined to belong to.

Cogito and the Jellyfish Software including usSCEP are not involved in the validation procedure beyond requesting validation of a CSR.

## 3.3 Microsoft Graph API

Cogito Jellyfish Intune SCEP Connector (usSCEP) uses the OAuth authentication procedure for establishing a connection to Microsoft Graph API. The establishment of the OAuth connection requires the usSCEP to store two Object Identifiers associated with a customer's Azure Active Directory environment, and one 'pre-shared secret' in the form of an *App Registration Secret*.

The three stored values can be described in more detail as:

- *Directory (tenant) ID*: Used by usSCEP as part of the OAuth authentication procedure prior to transmitting validation requests.
- *Application (client) ID:* Used by usSCEP in the first stage of the validation process to identify which *Service Principal* to enquire for a service provider for the second stage of the validation process.
- *App Registration Secret:* Used by usSCEP as part of the OAuth authentication procedure prior to transmitting validation requests. Directly associated with the permissions we are granted for the purpose of request validation. Revocation of this token effectively disables all SCEP enrollments, and our access to your Azure tenancy and services.

An OAuth session is created each time a usSCEP certificate enrollment is triggered. The OAuth session is reused for both the first and second stage of the validation process. Subsequent enrolments will use distinct sessions.

SCEP enrolments for other Azure tenancies may occur on the same service. Each validation procedure is handled in a silo, and there is no 'cross-pollination' of customer Object Identifiers or secrets.

# 4 Prerequisites

Before configuration of Azure Intune may be performed the following requirements must be provisioned and available.

## 4.1 Jellyfish Product Prerequisites

The following Jellyfish Products are required before Jellyfish SCEP can be provisioned:

- Optional: Issuing Certificate Authority - base service (a shared Certificate Authority may be used in the case where one is already available to the service).
- Required: Certificate Template under management - uplift. For the purposes of issuing SCEP certificates.
- Required: Autoenrollment services server - uplift.

## 4.2 Technical Prerequisites

The following accounts, credentials and keys must be available to complete this configuration:

- Administrative access to the following Microsoft Azure platform services
    - Microsoft Azure Portal
    - Microsoft Azure Active Directory
    - Microsoft Endpoint manager admin center (in some instances this may simply be referred to as *Intune* with the *Microsoft Azure Portal*)
- Provision of the Cogito Jellyfish Intune SCEP Connector service by Cogito Group Operators. This must be confirmed through the following email inbox:
    - Security.Services@cogitogroup.net
- Your unique customer SCEP Server URL. This is sent to you by Cogito Group Operators as part of the Provisioning of the Cogito Jellyfish Intune SCEP Connector.
    - Example Server URL: https://jellyfish.securesme.com/intune/a5e8ee4c-eed9-4a7b-be8e-a97a875cdcf5/OperationsCA302/scep
- The Certificate Authority certificates required for establishing trust for your device configuration. This is at least the Root Certificate Authority, and at most the Root, Intermediate, and Issuing Certificate Authority certificates.
    - For NZTaaS customers, certificates can be downloaded from: http://pki.govt.nz
    - Cogito Group Operators are available for assistance with which Certificates you require and may be contacted through the following email inbox:
        - Security.Services@cogitogroup.net

# 5 Configuring Azure Intune

This document describes the most common configuration for the Cogito Jellyfish SCEP Intune Connector. If you organisation requires deviations from the below configuration, and the setup does not result in successfully issued SCEP certificates, please contact:

Security.Services@cogitogroup.net

For further assistance. Standard Professional Services charges may be incurred in some cases.

## 5.1 Microsoft Azure Portal

This document describes procedures for configuring within the *Azure Active Directory* service as well as from the *Microsoft Endpoint Manager admin center* server. Both services are accessible through the *Microsoft Azure Portal* website. Access to the *Microsoft Azure Portal* website is a prerequisite requirement to the Configuring Azure Intune section of this document.

It is recommended to search for the following services through the *Search resources, services, and docs* toolbar at the top of the *Microsoft Azure Portal*.

### 5.1.1 Azure Active Directory

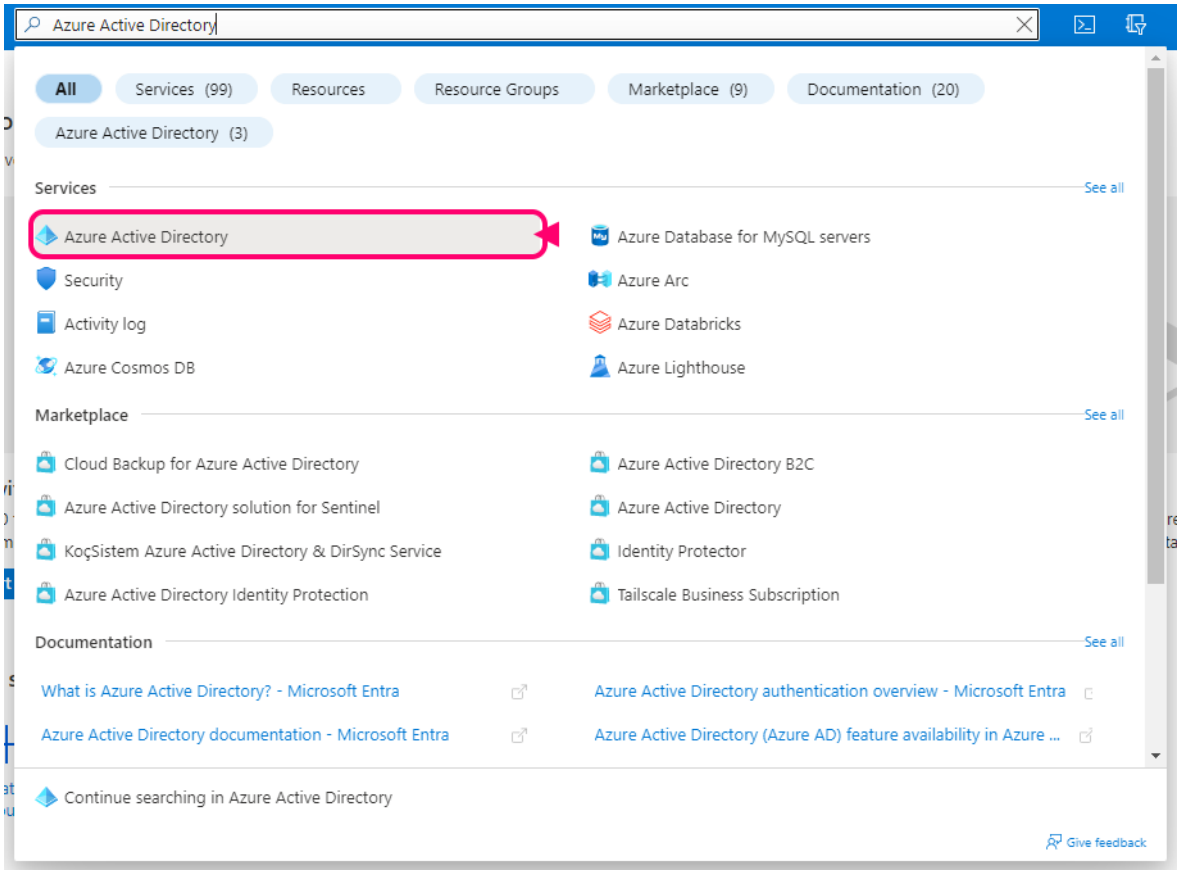


**Figure 2: When searching for "Azure Active Directory" the service appears as the first result.**

### 5.1.2 Microsoft Endpoint Manager admin center (Intune)

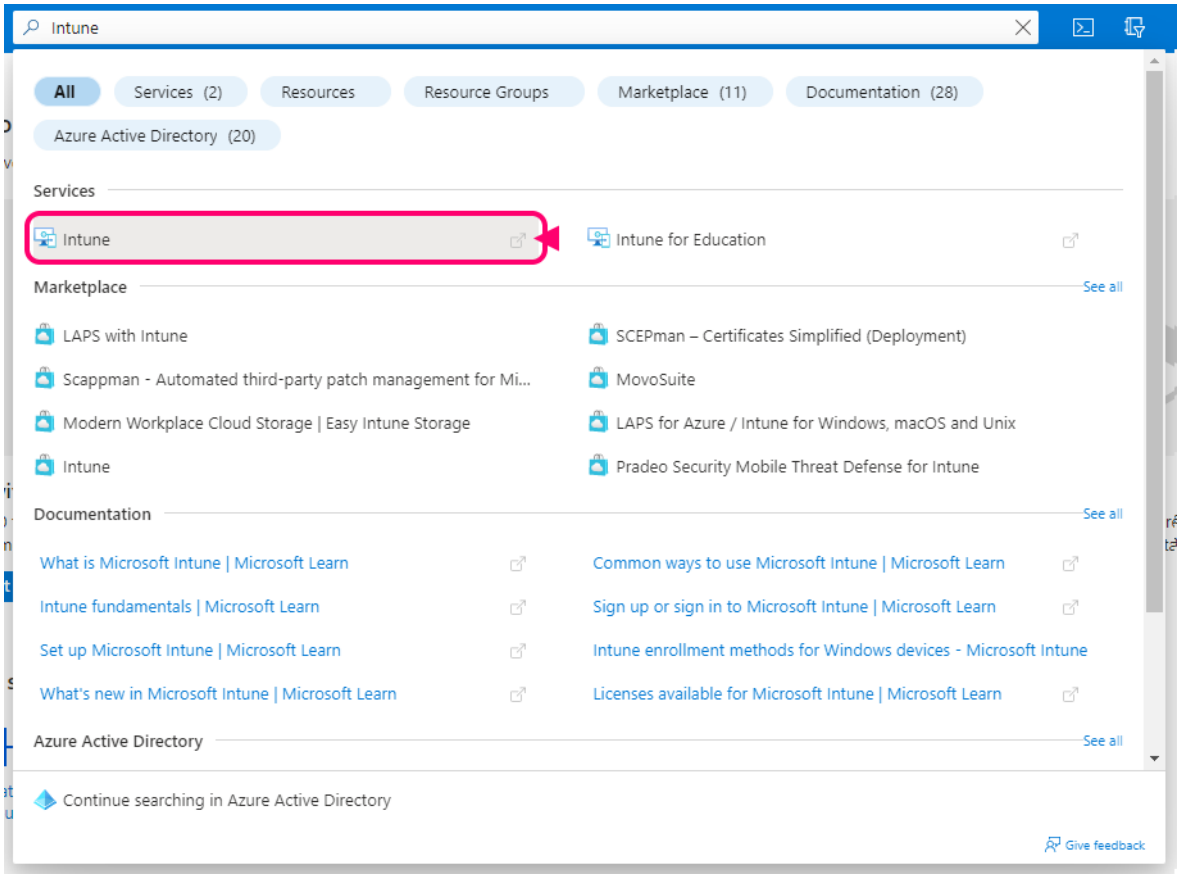


**Figure 3: When searching for "Intune" the service appears as the first result. Note that despite the service name, the Intune service directs to the Microsoft Endpoint Manager admin center.**

## 5.2 App Registrations

Application registration occurs in the *Azure Active Directory* service.

1. In the left menu bar, under the *Manage* heading: select *App Registrations*.
2. In the top of the *App Registrations* blade click the + *New registrations* button.

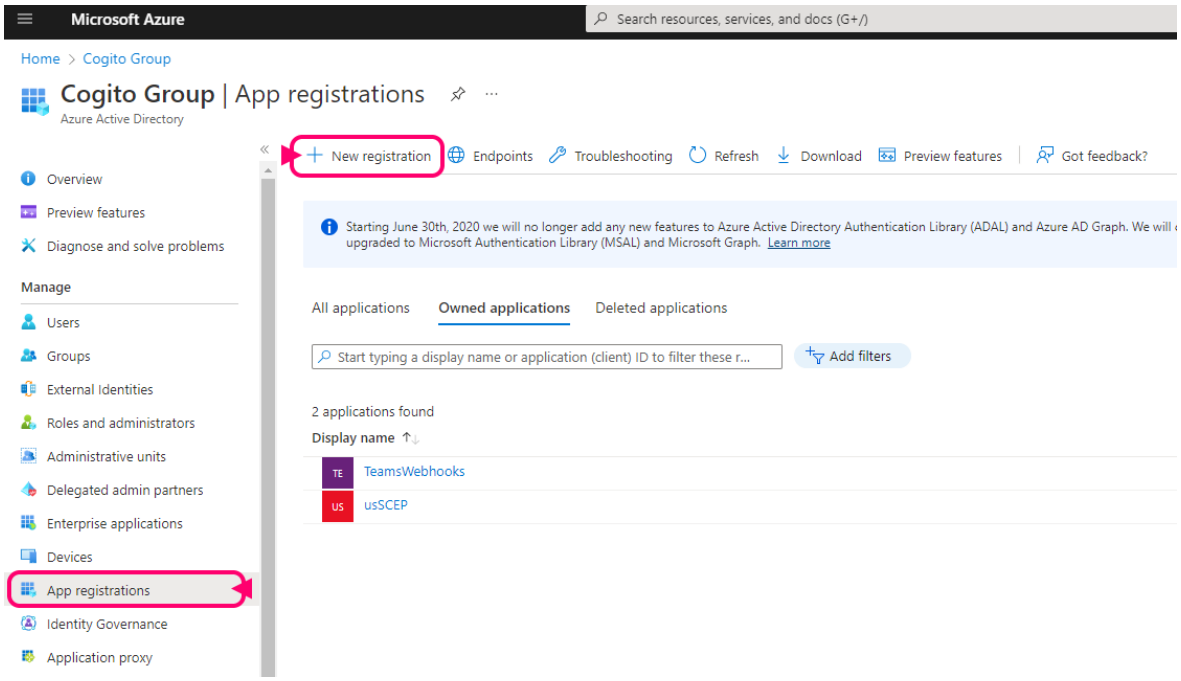


**Figure 4: Within Microsoft Azure Active Directory Service, App registrations appears in the left menu. Within the App registrations blade, + New registrations appears at the top.**

3. Fill out the details on the fist page of the *Register an application* page:
    a. Enter the Name of the application. We recommend this includes the words: *Cogito Jellyfish SCEP Intune Connector.* We additionally recommend you include any identifying information your organization will require to identify this application in the future.
    b. Select *Accounts in this organizational directory only (Single tenant)*.
    c. Do not specify a *Redirect URI*
    d. Click *Register.* You will be redirected to the application summary for the application just created.
4. Record the Two Object Identifiers required by Cogito Group Operators to later complete your onboarding procedure.
    a. *Application (client) ID:* A Globally Unique Object Identifier unique to this application.
    b. *Directory (tenant) ID*: A Globally Unique Object Identifier used to identify your tenancy within Azure.

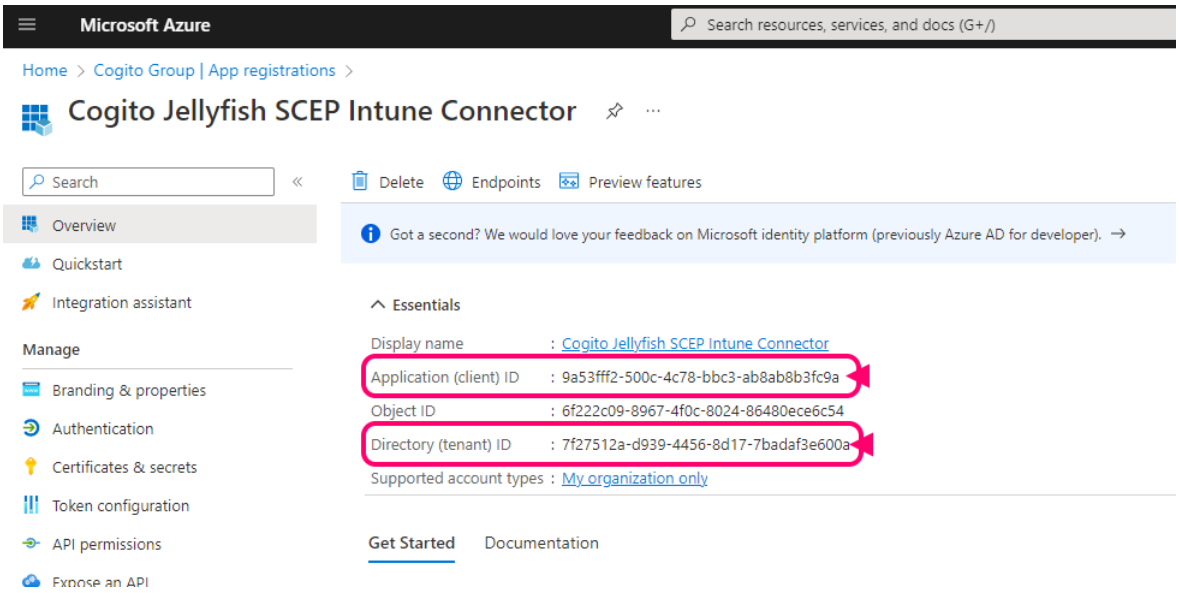


**Figure 5: Application ID appears second in the list of *Essentials*. Directory ID appears fourth in the list of *Essentials*. Both GUIDs will have a copy button appears on the right-hand side when hovered.**

5. In the left menu bar select *API Permissions.*
6. Remove all existing permissions, the default permissions are not required by the Cogito Jellyfish SCEP Intune Connector. This is done using the ellipsis to the right on the Microsoft Graph heading. After clicking the ellipsis select *Remove all permissions.*

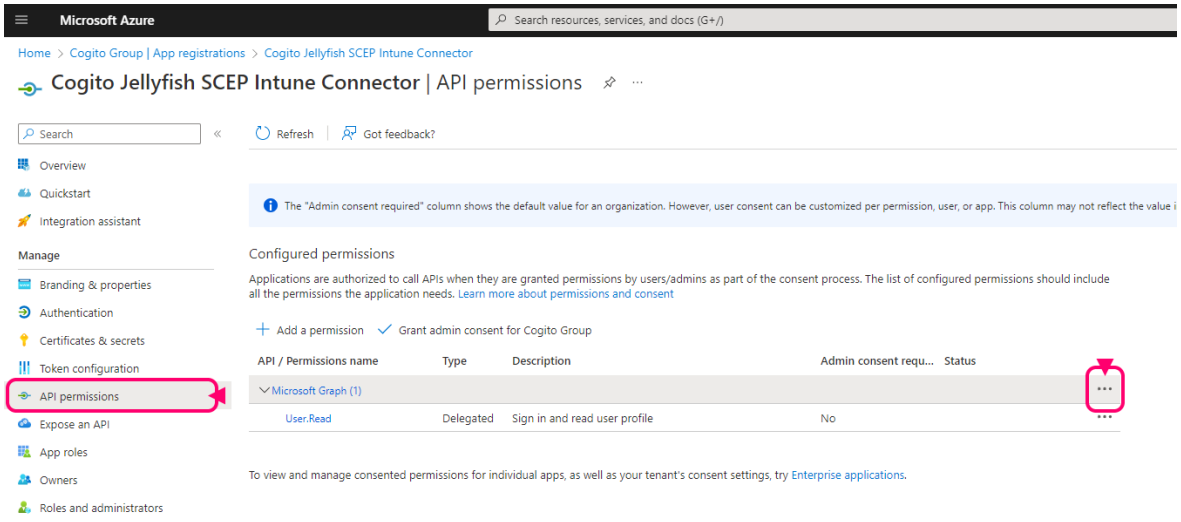


**Figure 6: The *API permissions* menu item is on the left. All default permissions are removed using the ellipsis on the right under the Microsoft Graph heading.**

7. Click *+ Add a permission* near the top of the *API permissions* blade.
    a. In the *Request API permissions* tab select *Microsoft Graph*
    b. Click *Application permissions*.

c. Search for: *ServicePrincipalEndpoint.Read.All*

d. Expand *ServicePrincipalEndpoint* and tick *ServicePrincipalEndpoint.Read.All*

e. Click *Add permissions* at the bottom.

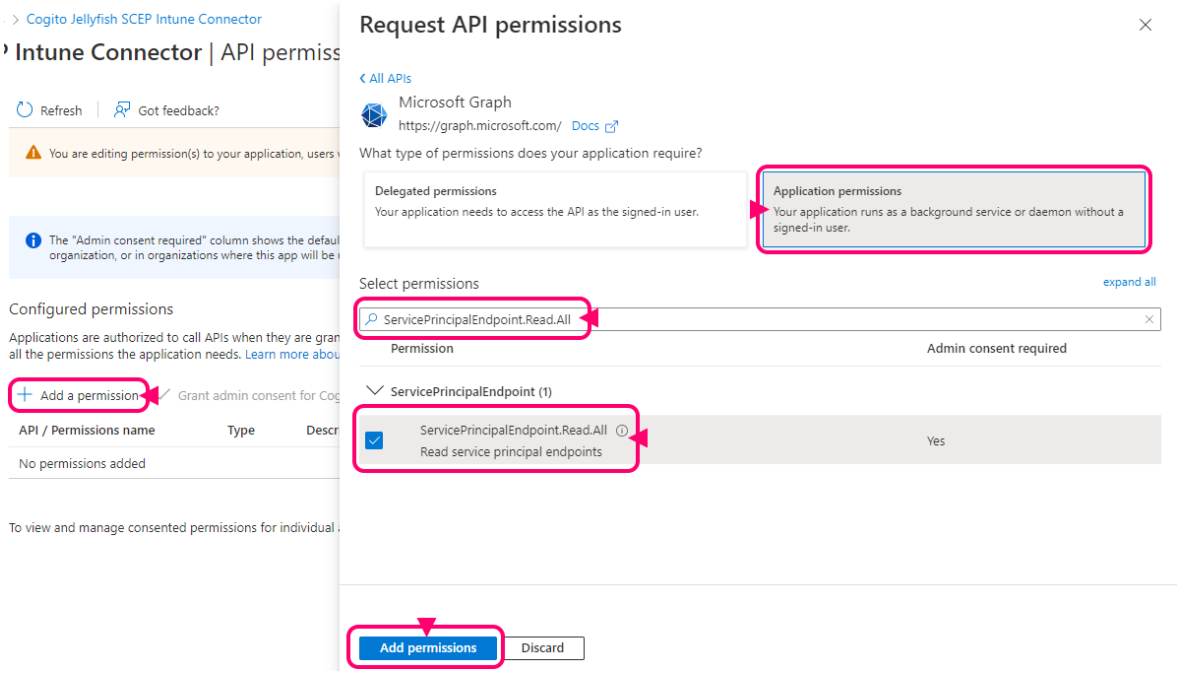


**Figure 7: Click + *Add a permission* on the left. Choose *Microsoft Graph*. Then in order from top to bottom: select *Application permissions*, search for *ServicePrincipalEndpoint* tick *ServicePrincipalEndpoint.Read.All*, click *Add permissions*.**

8. Click + *Add a permission* near the top of the *API permissions blade.*

   a. In the *Request API permissions tab* select *Intune*, it is mid-way down the list of service permissions.

   b. Click *Application permissions*.

   c. Search for *scep_challenge_provider*.

   d. Expand *Permissions* and tick *scep_challenge_provider*

   e. Click *Add permissions* at the bottom.

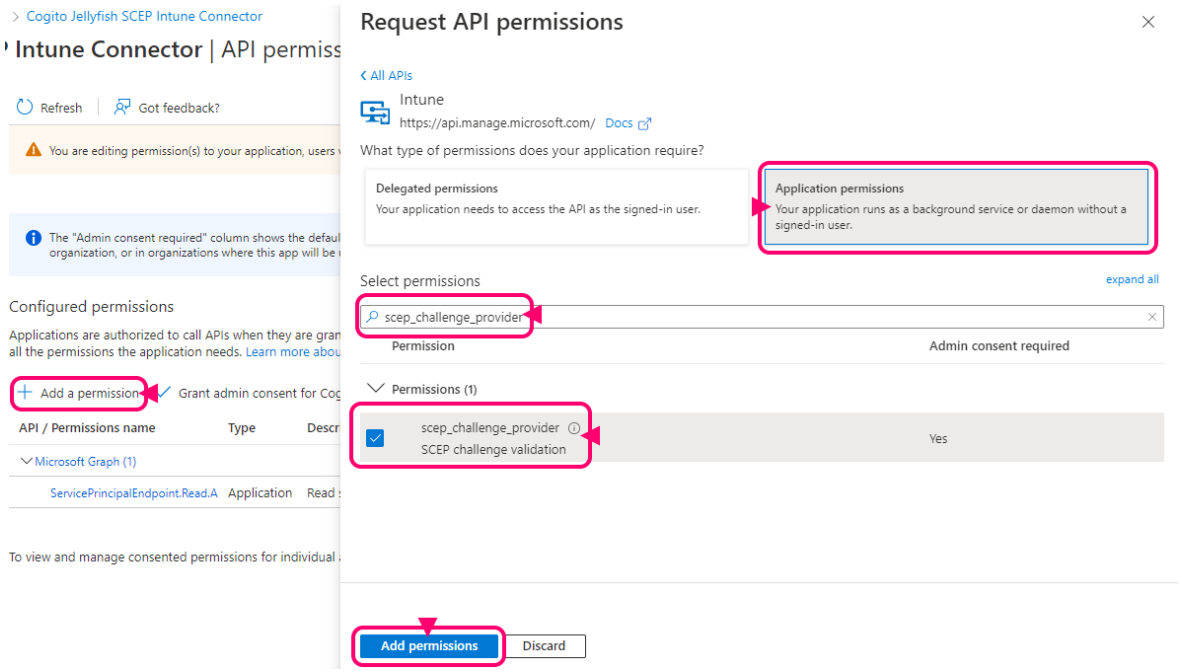


**Figure 8: Click + *Add a permission* on the left. Choose *Intune*. Then in the order from top to bottom: select *Application permissions*, search for *scep_challenge_provider*, tick *scep_challenge_provider*, click *Add permissions.***

9. Click ✓ *Grant admin consent for*. This confirms the permissions changes. This requires administrative privileges for the Azure Active Directory tenancy.

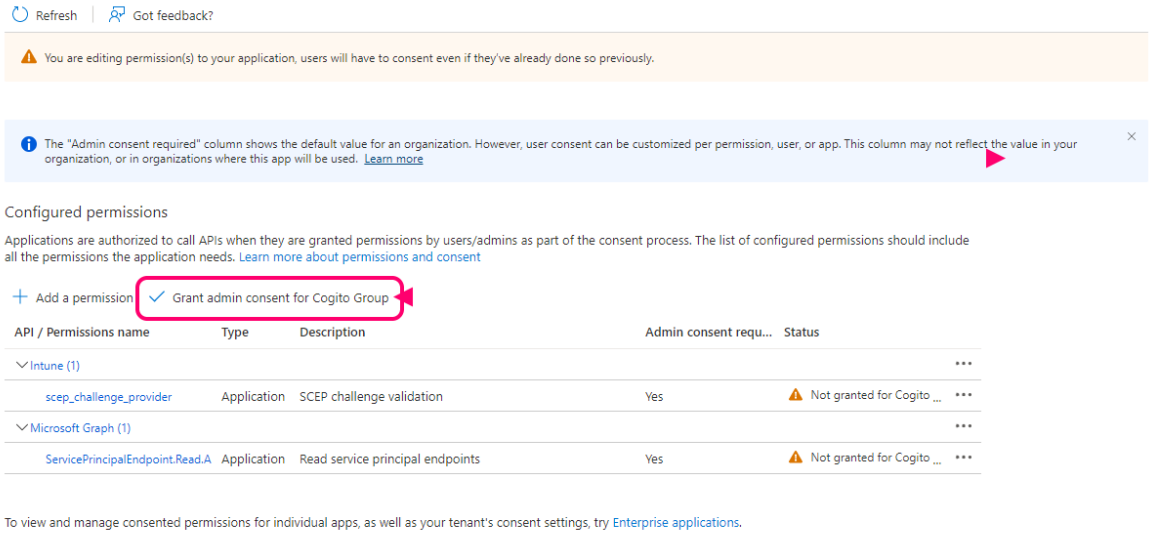


**Figure 9: Grant admin consent applies the API permission changes.**

10. Click *Certificates & secrets* in the left menu.
    a. Click + *New client secret* near the top of the page.

b. In the *Add a client secret* tab, enter a description that identifies this client secret. We recommend a description that contains the word: "Cogito Jellyfish Intune SCEP Connector Access".

c. Set an expiry compliant with your security policies. We recommend 24 moths, as rotation of this token will require co-ordination with Cogito Group Operators, and must be arranged through: Security.Services@cogitogroup.net

d. Click *Add* at the bottom

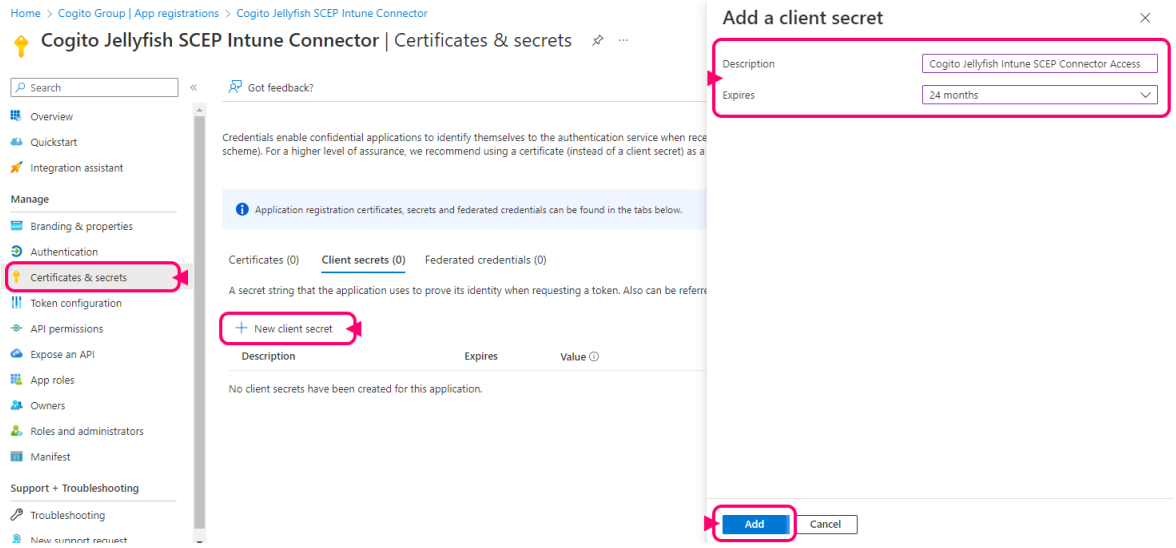


**Figure 10: Certificates & secrets appears in the left menu bar. + *New client secret* near the top of the *Certificates & secrets blade*. Fill out the details in the *Add a client secret* tab, and click *Add.***

11. Immediately copy and record the *Value* of the secret that been created. The secret value will only appear this one time, after leaving this page the secret is lost forever and must be re-created. Note: the *Secret ID* is not required.

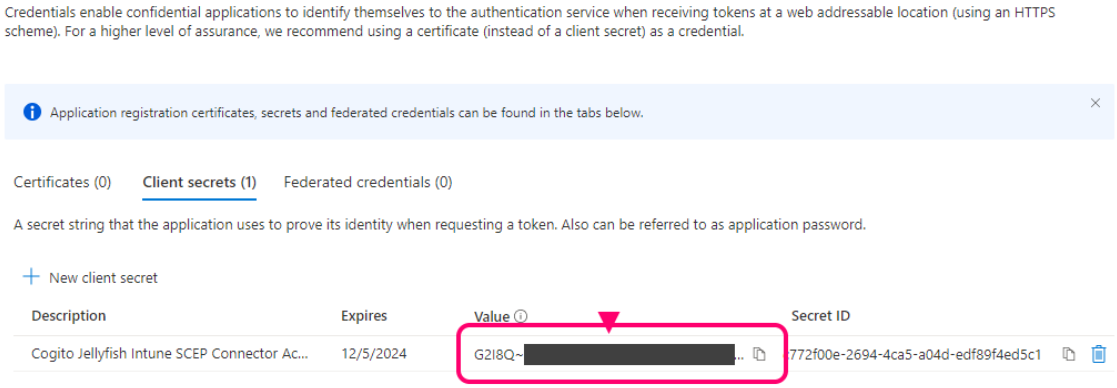


**Figure 11: A copy button appears next to the *Value*. Note: the *Value* in this figure has been redacted, and will appear without censor during configuration.**

12. Send the three values recorded earlier (and described below) to Cogito Operators. These values must be tested and deployed to the service prior to service operation. For a smooth deployment, please allow some time at this stage to work with your Cogito Operator to successfully test and verify functionality of your provided information.

    a. *Application (client) ID*

    b. *Customer (tenant) ID*

    c. *App Registrations Client Secret Value*

## 5.3 Trusted Certificate

Trusted Certificate configuration occurs in the *Microsoft Endpoint Manager admin center* service.

Prior to completing the following steps, ensure you have the Root Certificate Authority Certificate accessible. For more information on how to retrieve this certificate consult the *Prerequisites* section of this documentation.

1. In the far-left menu select *Devices*.
2. In the left sub menu select *Configuration profiles*. This may be searched for or found under the *Policy* section.
3. Near the top of the page click + *Create profile*.
4. In the *Create a profile* tab, select the platform you are configuring (in the example case *Windows 10 and later*)
5. Select the Profile type of *Templates*.
6. Search for *Trusted Certificate* and select it.
7. Click the *Create* button at the bottom.

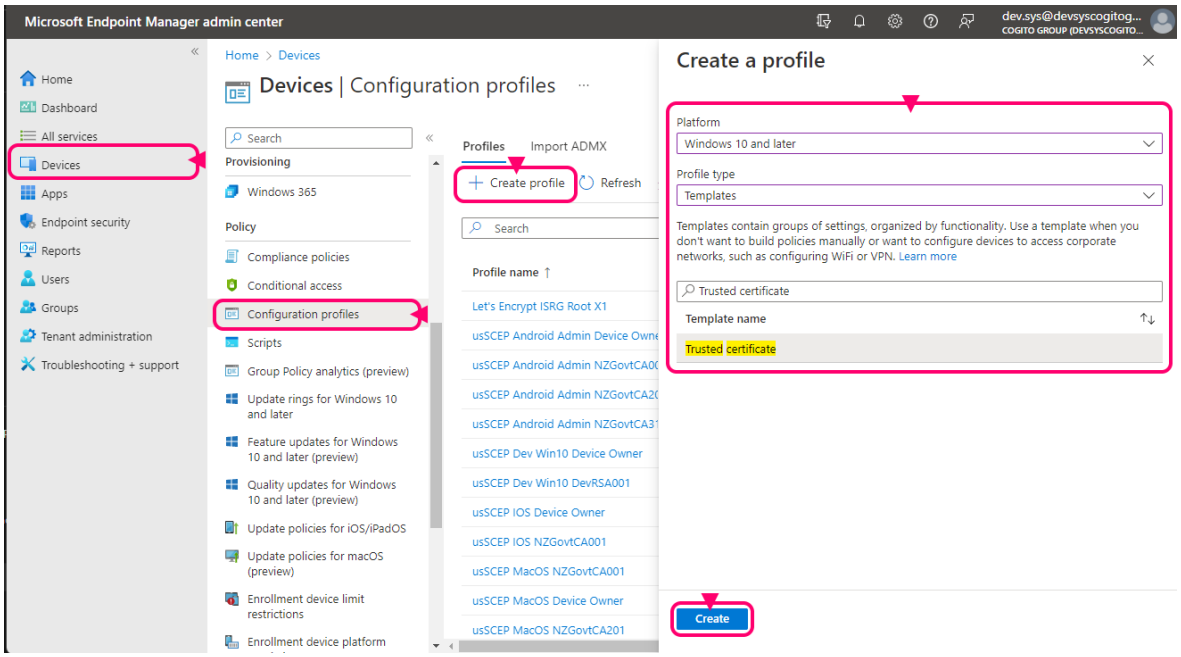


**Figure 12: From left to right: Select *Devices*, select *Configuration profiles*, click + *Create profile*, enter the details as per the configuration documentation, click *Create*.**

8. On the *Basics* tab of the *Trusted certificate* page, enter a Name to describe the profile both applied to Jellyfish SCEP and the Certificate Authority it represents. We recommend including the words: "Jellyfish SCEP - Trusted Certificate <CA-Name>" where CA Name is the name of the root certificate authority being deployed.
9. Optionally fill in a description. This is useful only for your organizations operational team.
10. Click *Next*.

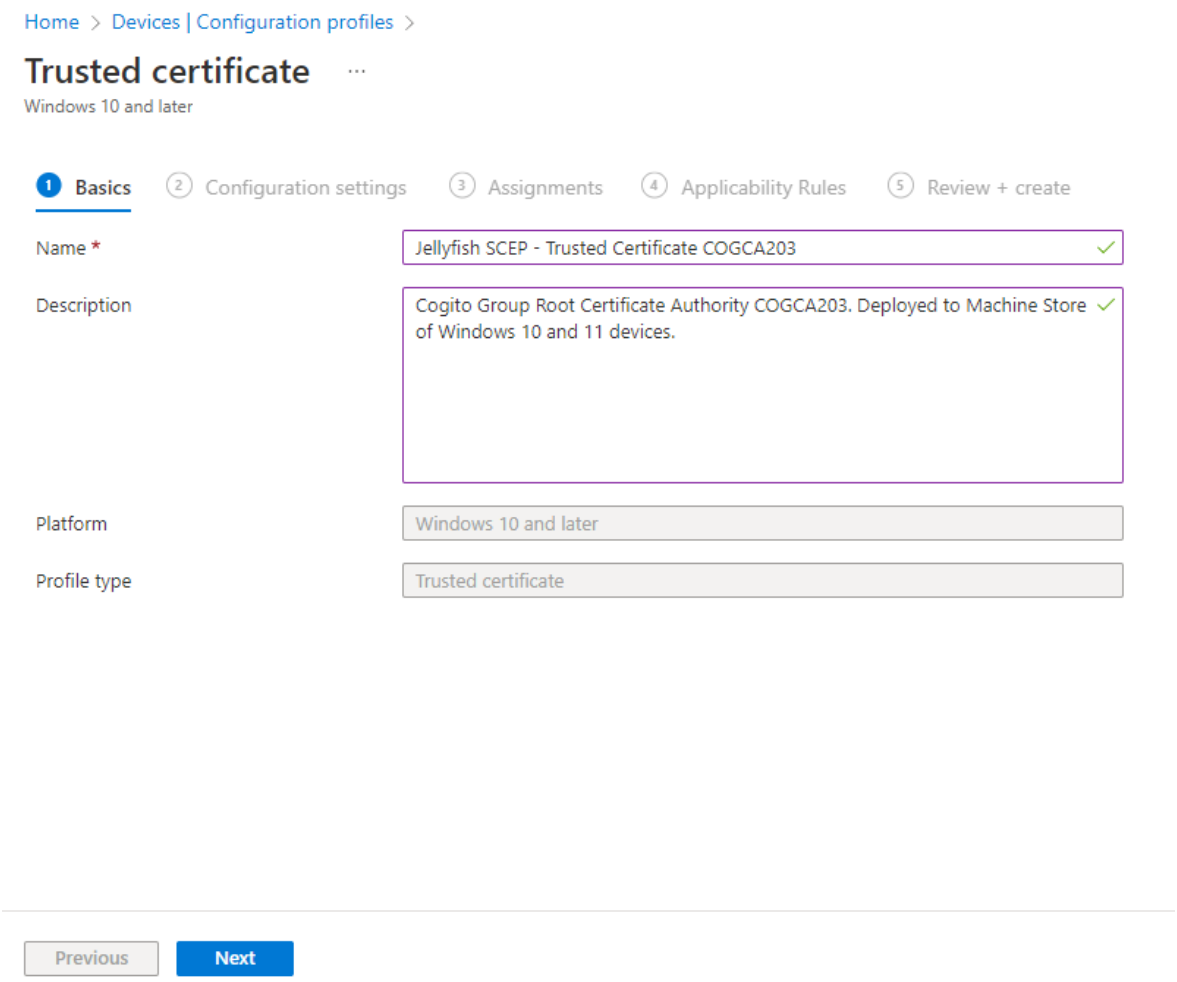


**Figure 13: An example of a Name and Description that describes the COGCA203 Certificate Authority *Trusted Certificate Configuration profile.***

11. On the *Configuration settings* tab, upload the Root Certificate Authority Certificate collected earlier.
12. Choose the appropriate Destination Store, this is usually *Computer certificate Store - Root*.
13. Click *Next* near the bottom.
14. On the *Assignments* tab, under *Included groups* add the groups appropriate for your organization.
    a. When deploying Cogito Jellyfish SCEP Intune Connector for the first time, we recommend creating a Staged Rollout group, which may initially include only one user, additional users may be added to this group as confidence in the deployment grows.
    b. We do **NOT** recommend using the *Add all users* or *Add all devices* options for tenancies with a large number of users or devices.
    c. The larger the number of users or devices are configured simultaneously, the greater the load on our services to facilitate enrollment requests. If requesting a large number of enrollments: be aware of some time delay between deploying the

*Configuration profile* and all members of the associated groups completing their enrollment.

15. Click *Next* at the bottom.
16. Leave the *Applicability Rules* tab empty and click *Next* at the bottom.
17. Review the details of the *Trusted certificate Configuration profile.*
    a. We recommend ensuring the *Configuration settings* and *Assignment* sections are correct before continuing, a fault in this information may result in erroneous deployment of trusted certificates.
18. Click *Create* at the bottom.

## 5.4 Trusted Certificate - Android Specific

Android requires not only the Root Certificate Authority Certificate to be deployed as a *Trusted certificate Configuration profile*, but all element of the Certificate Authority Chain.

The number of entities may differ depending on the Certificate Authority that your Cogito Jellyfish SCEP Intune Connector's Registration Authority certificate was issued from.

- For NZTaaS customers using a Cogito hosted Certificate Authority, you will be using a Three Tier PKI including a Root, Intermediate, and Issuing Certificate Authority. E.g.:
  - NZGovtCA001 => NZGovtCA201 => NZGovtCA312

If you are unsure about which Certificate Authority Certificate must be deployed in your environment specifically for Android, contact your Cogito Operator at: Security.Services@cogitogroup.net

Ensure you mention you are configuring Android Trusted Certificates.

1. Follow the instructions in section: *Configuring Azure Intune - Trusted Certificate* for any subsequent Certificate Authority Certificates.

## 5.5 SCEP Certificate

SCEP Certificate configuration occurs in the *Microsoft Endpoint Manager admin center* service

1. In the far-left menu select *Devices*.
2. In the left sub menu select *Configuration profiles*. This may be searched for or found under the *Policy* section.
3. Near the top of the page click + *Create profile*.
4. In the *Create a profile* tab, select the platform you are configuring (in the example case *Windows 10 and later*)
5. Select the Profile type of *Templates*.
6. Search for *SCEP certificate* and select it.
7. Click the *Create* button at the bottom.

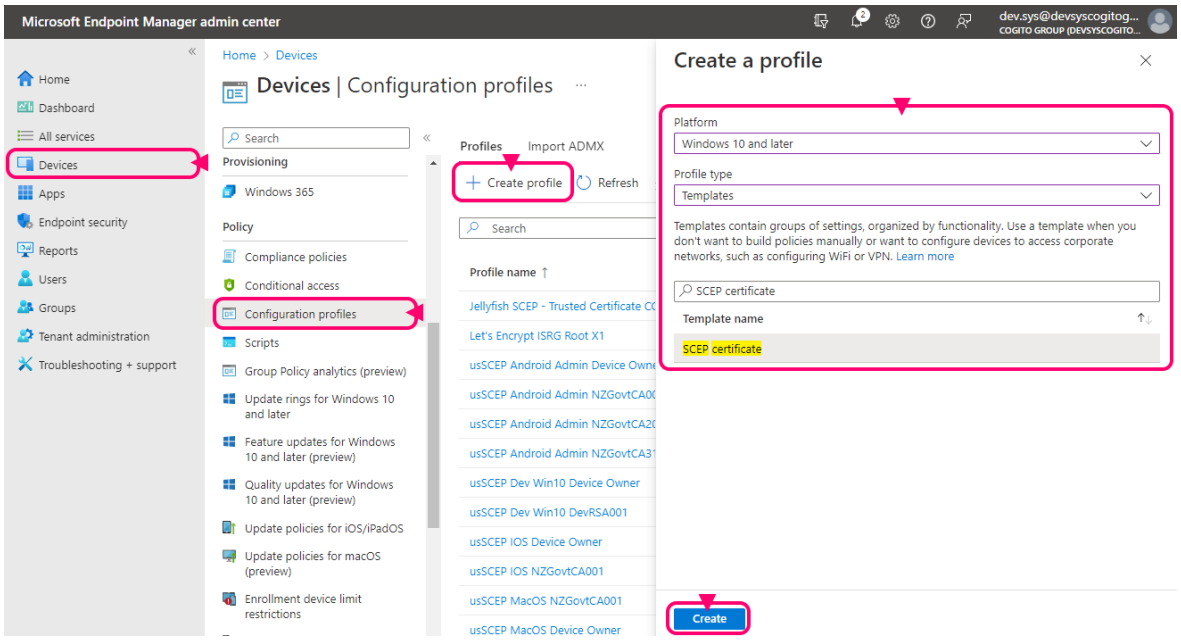


**Figure 14: From left to right: Select *Devices*, select *Configuration profiles*, click + *Create profile*, enter the details as per the configuration documentation, click Create.**

8. On the *Basics* tab of the *SCEP certificate* page, enter a Name to describe the profile both applied to Jellyfish SCEP and that this is a SCEP certificate profile, when deploying more than one certificate profile, ensure the names can be distinguished. We recommend including the words: "Jellyfish SCEP - SCEP Certificate".
9. Optionally fill in a description. This is useful only for your organizations operational team.
10. Click *Next*.

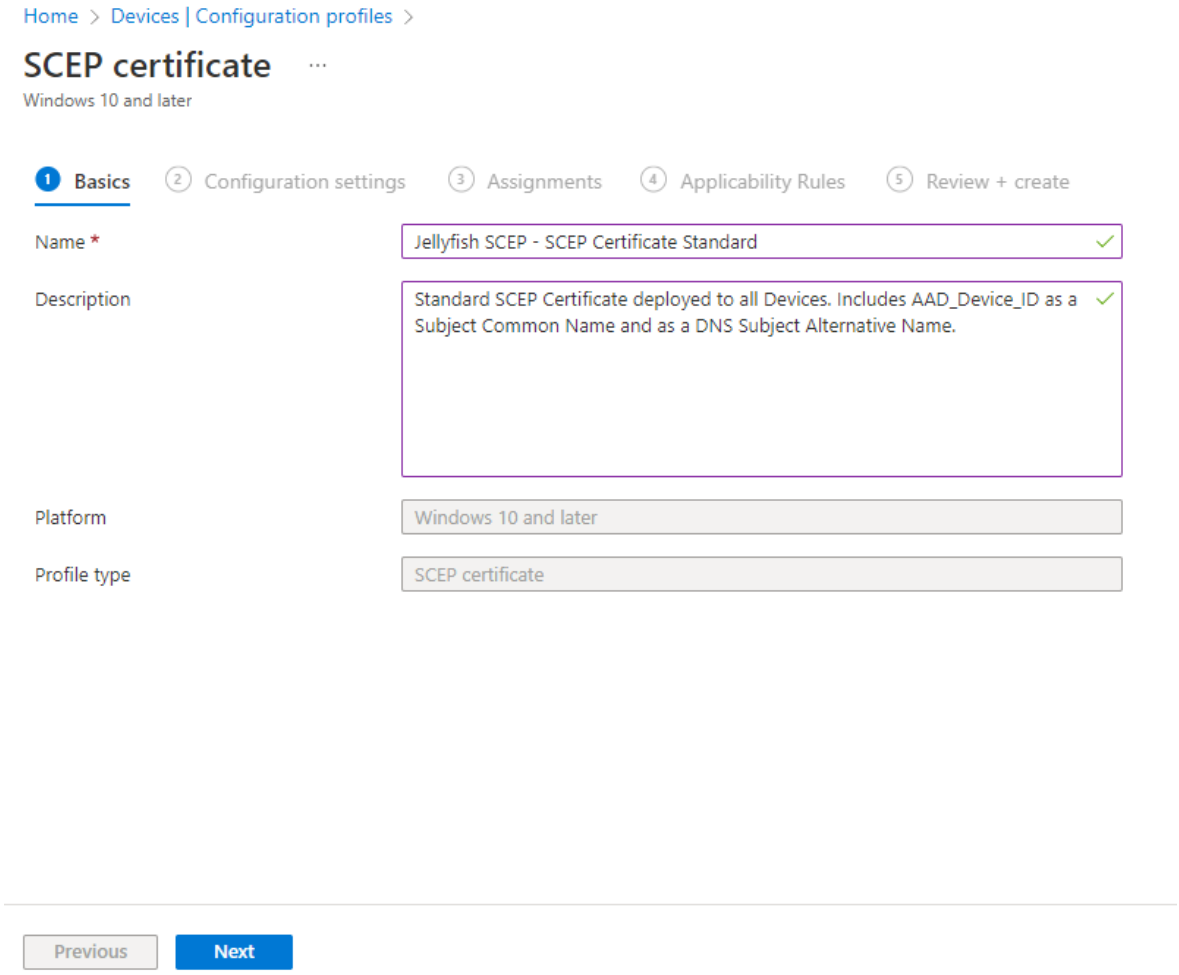


**Figure 15: An example of a name and description of a Standard SCEP Certificate, configured as per the steps in this documentation.**

11. On the *Configuration settings* tab, the following details are recommended. More specific details can be configured if required:
    a. Certificate type: *User,* or *Device* depending on your organization requirements, and which certificate profile is current being configured.
    b. Subject name format: *CN={{AAD_DEVICE_ID}}*, additional Subject Names may be configured as required.
    c. Subject alternative name:
        i. Attribute: DNS
        ii. Value: {{AAD_DEVICE_ID}}
    d. Certificate validity period: Years 1
    e. Key storage provider (KSP): Enroll to Trusted Platform Module (TPM) KSP if present, otherwise Software KSP.
    f. Key usage: Digital signature and Key encipherment
    g. Key Size (bits): 2048

h. Hash algorithm: SHA-2

i. Root Certificate: The *Trusted certificate Configuration profile* as configured in the above section *Trusted Certificate*. In the case of an Android configuration, ensure all Root Certificates created are selected here.

j. Extended Key Usage:

   i. Name: Client Authentication

   ii. Object Identifier: 1.3.6.1.5.5.7.3.2

   iii. Predefined Values: Client Authentication

k. Renewal threshold (%): 20

l. SCEP Server URLs: The URL provided by your Cogito Operator as part of your onboarding procedure. For more details refer to the Prerequisites section of this document.

12. For more details regarding configuring SCEP certificate details, consult the Microsoft SCEP Certificate configuration documentation available here: https://learn.microsoft.com/en-us/mem/intune/protect/certificates-profile-scep

13. Click *Next* at the bottom.

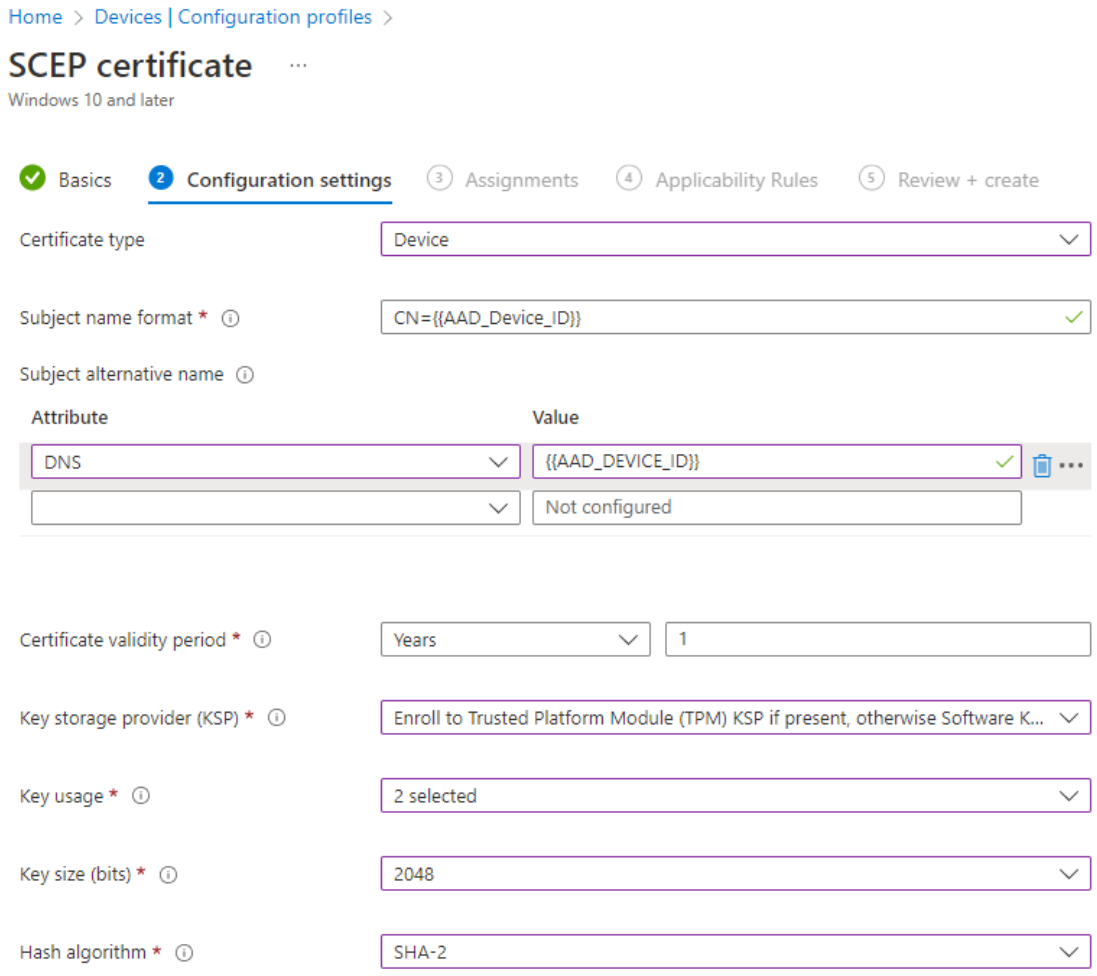


**Figure 16: Example details of recommended SCEP certificate settings Part 1.**

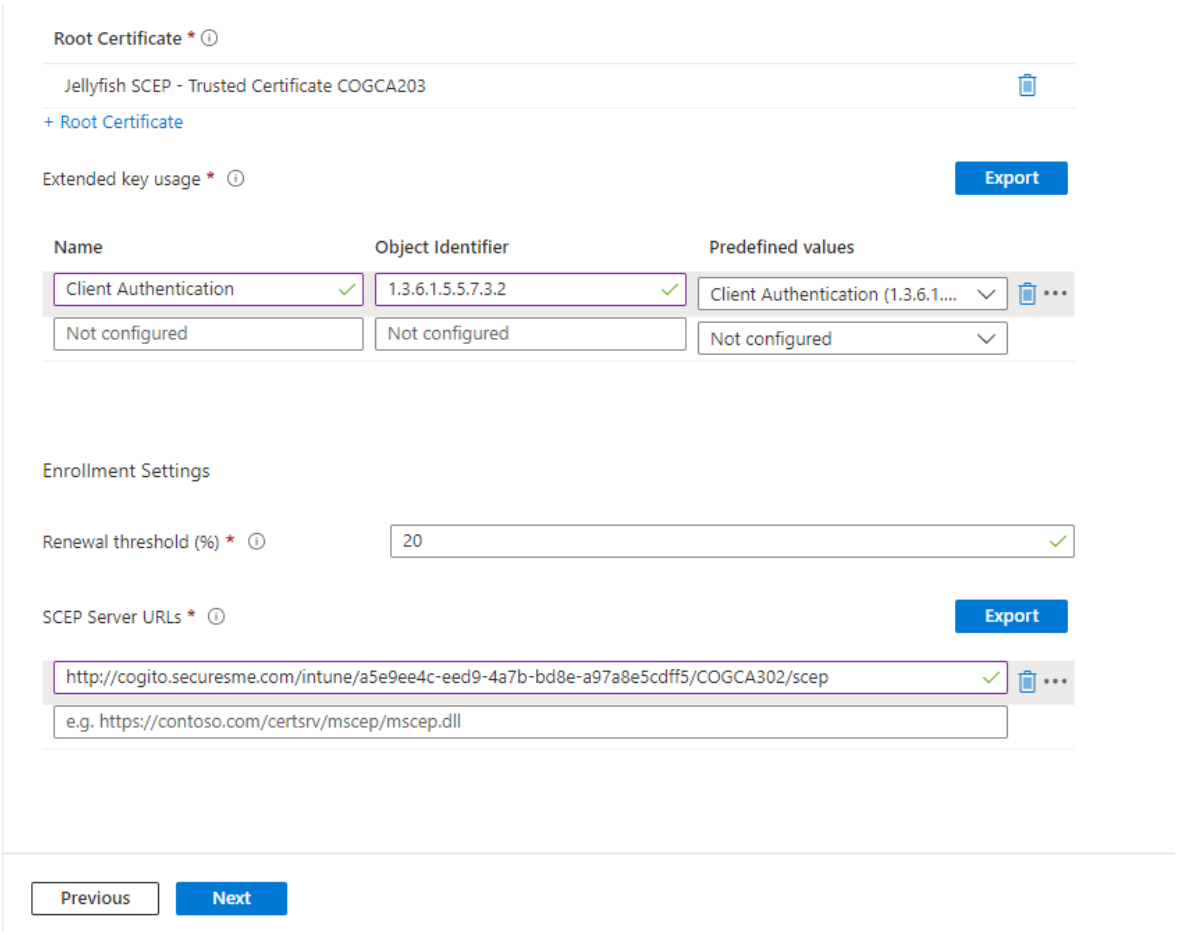


**Figure 17: Example details of recommended SCEP certificate settings Part 2.**

14. On the *Assignments* tab, under *Included groups* add the groups appropriate for your organization.
    a. When deploying Cogito Jellyfish SCEP Intune Connector for the first time, we recommend creating a Staged Rollout group, which may initially include only one user, additional users may be added to this group as confidence in the deployment grows.
    b. We do **NOT** recommend using the *Add all users* or *Add all devices* options for tenancies with a large number of users or devices.
    c. The larger the number of users or devices are configured simultaneously, the greater the load on our services to facilitate enrollment requests. If requesting a large number of enrollments: be aware of some time delay between deploying the *Configuration profile* and all members of the associated groups completing their enrollment.
15. Click *Next* at the bottom.
16. Leave the *Applicability Rules* tab empty and click *Next* at the bottom.
17. Review the details of the *SCEP certificate Configuration profile.*

a. We recommend ensuring the *Configuration settings* and *Assignment* sections are correct before continuing, a fault in this information may result in erroneous enrollment of SCEP certificate, or more likely a failure to issue any certificates.

b. We recommend triple checking the SCEP Server URLs at this point, comparing against the URL provided in the SCEP onboarding process. Ensure devices can hit this URL and that there is no restriction within your network on this URL.

c. Network connectivity to this URL can be tested by suffixing the URL with the following query parameters:
*?operation=getcacaps*

E.g.: https://jellyfish.securesme.com/intune/0/0/scep?operation=getcacaps

The expected results in a plain text list of Cogito Jellyfish Intune SCEP Connector capabilities. If this webpage fails to load, the device will not be able to complete a SCEP enrollment.

18. Click *Create* at the bottom.