

KeyTalk SCEP server for Intune guide

This guide will explain the steps required to configure KeyTalk server as a SCEP provider for Microsoft Intune device certificates.

For the security, the following page shows how KeyTalk server validates SCEP requests: [Use third-party certification authorities \(CA\) with SCEP in Microsoft Intune - Azure | Microsoft Docs](#)

Requirements

- KeyTalk server version 6.2.0 and up
- Azure Active Directory
- Microsoft Intune
- Client devices need access to KeyTalk server via port 80 for SCEP HTTP and port 443 for HTTPS (incoming server-side)

Overview of the SCEP configuration

SCEP is used to issue device certificates for Intune enrolled devices. SCEP-specific configuration is required for KeyTalk server to act as a trusted SCEP intermediary. This guide will show the steps needed to configure both KeyTalk Server as well as Microsoft Endpoint Manager for Intune.

Besides the usual Template for device certificates, KeyTalk server also requires Communication Certificates to ensure the devices can trust KeyTalk server. You can find more information on these Communication Certificates in section 'Communication certificates explained'.

Device certificate Template requirements

The Device certificate Template should match the SCEP Profile as configured in Intune to avoid unexpected certificate attributes. KeyTalk server cannot validate whether the Template matches the SCEP profile.

Communication certificate Template requirements

SCEP is currently supported for the following Signer products:

- KeyTalk
- GlobalSign Atlas

SCEP devices consider the following attributes:

- Validity, as expired certificates are not accepted
- Key Usage, KeyTalk server overrides the Template to set the correct Key Usage for both Communication certificates
- Issuer, the SCEP Issuing CA must have issued/signed both Communication certificates

KeyTalk

As SCEP devices do not consider most certificate attributes you are free to set most Certificate Settings to your taste. Note that Subject CN will be generated based on the KeyTalk SCEP configuration.

- Basic Constraints must be set to CA:FALSE
- Key Usage will be ignored

- Extended Key Usage is not considered by SCEP devices

GlobalSign Atlas

A separate GlobalSign Atlas account needs to be configured for KeyTalk to generate the required Communication certificates. This account should allow KeyTalk server to set the keyEncipherment & digitalSignature Key Usages.

- Add this account at 'Certificates and Keys' -> 'Third Party Signers'.
- Create a Template with 'Signer' set to "GlobalSign Atlas" & 'GlobalSign Atlas Product' set to "Generic".
- Match the Key Size (bits), Validity (months), and other required Certificate settings to the GlobalSign account profile.

Communication certificates explained

The Communication Certificates are necessary for SCEP client devices to be able to trust that KeyTalk Server can indeed issue certificates for the intended CA. Besides issuing/signing the device certificates, the Issuing CA must also issue two certificates with very specific Key Usages. These are:

- Certificate (and key) for Encryption, called Recipient
- Certificate (and key) for Signing, called Signer

The Recipient is used for devices to encrypt the CSR object. KeyTalk Server signs the Certificate response with Signer.

Requirements for these certificates:

- Both certificates need to be valid and not revoked
- Both certificates need to be signed by the same Issuing CA that issues/signs the device certificates
- Recipient must have Key Usage set to either 'keyEncipherment' or 'digitalSignature'. Not both and no other Key Usages.
- Signer must have Key Usage set to 'digitalSignature', no other Key Usages.

Configure KeyTalk server

Note: Only a single KeyTalk Template can be configured for use with SCEP. Once configured for SCEP, this Template will no longer be available for regular client authentication. SCEP is only available for Templates with an Azure Module.

- Configure a KeyTalk Template for the device certificates.
- In the Registration Authority tab, configure Azure Module for the device certificate Template. Make sure to fill out the 'Tenant Domain' field and set 'Additional options for CN and SAN' to None
- Navigate to Templates->SCEP to set the SCEP configuration.

The SCEP configuration requires Communication Certificates to be configured. This can either be achieved by configuring a Template to generate the Communication Certificates (choose 'Let KeyTalk generate Communication Certificates' for this option) or by uploading them manually. For more information about the Communication Certificates see section 'Communication certificates explained'.

Note: When updating the settings they will be applied within 30 minutes. If the update needs to be applied immediately, please go to System -> Daemons and restarts 'SCEP Daemon'.

SCEP configuration Field explanation:

“Device certificate Template”: Choose the correct Azure Module-enabled Template.

If “Let KeyTalk generate Communication Certificate” is checked:

- “Communication Certificate Template”: Choose the Template created to provide Communication Certificates. Ensure that the CA for this Template matches the Device certificate Template CA.
- “Communication Certificate Subject CN Base”: Base for the Communication certificate Subject CN names. Recipient and Signer will be added to this name. Example for template **YourCompany Comm**: *CN=YourCompany Comm Recipient* & *CN=YourCompany Comm Signer*

If “Let KeyTalk generate Communication Certificate” is not checked:

- “Communication Recipient Certificate”: Upload a PFX or PEM file with certificate and key for the Communication Certificate with Key Usage ‘keyEncipherment’
- “Communication Signing Certificate”: Upload a PFX or PEM file with certificate and key for the Communication Certificate with Key Usage ‘digitalSignature’

“SCEP Issuing CA Certificates”: Upload the SCEP Issuing CA certificate as PEM. This can either be a single certificate (the certificate directly issuing/signing the Communication & device certificates) or the full certificate chain. To reiterate: the Device Certificates and the Communication Certificates need to be issued/signed by the same Issuing CA Certificate.

Configure SCEP to provision certificates for Intune-enabled devices

Enable SCEP: ☒

Device certificate Template: CUST_PASSWD_SCEP

Let KeyTalk generate Comm Certificates: ☒

Comm Certificate Template: * CUST_ANO_SCEP_RA

Comm Certificate Subject CN Base: * KeyTalk Demo Comm

Comm Recipient Certificate Info: Subject: /CN=KeyTalk Demo Comm Recipient
Serial: 44:7b:f5:b0:04:b2:4d:c0:92:0c:ba:6f:c3:f4:a3:4b

Comm Signing Certificate Info: Subject: /CN=KeyTalk Demo Comm Signer
Serial: eb:4a:f5:70:73:fd:48:2d:ab:fa:d4:b2:b7:c7:d5:b9

SCEP Issuing CA Certificates: *
Subject: /emailAddress=info@keytalk.com/C=NL/O=KeyTalk IT Security/OU=Factory Default/CN=KeyTalk Demo PCA
Serial: 01:c2
Choose File No file chosen

Ok

The SCEP server should be running after the configuration is complete. This can be tested by filling out and entering the following URL (preferably on a client device):

[https://\[Your IP address\]/intunescep/pkiclient.exe?operation=GetCACaps](https://[Your IP address]/intunescep/pkiclient.exe?operation=GetCACaps)

Example: <https://demo.keytalkdemo.com/intunescep/pkiclient.exe?operation=GetCACaps>

If the server is configured correctly you should see a list of 3 items:

AES
POSTPKIOperation
SHA-256

If you cannot reach the page and/or you get a timeout, please ensure you have access to port 443 of your KeyTalk server. If you see an error page like ‘HTTP Status 500 – Internal Server Error’, please ensure you have taken every numbered step in this section correctly.

Configure Intune: App permissions

The Enterprise Application requires additional permissions.

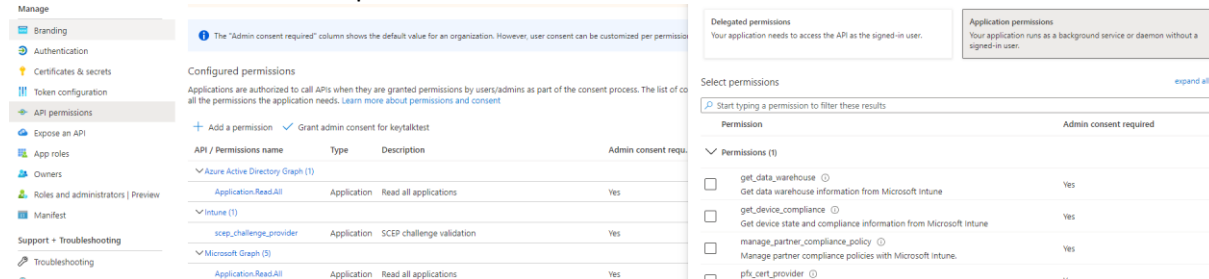
Go to the Azure Portal -> Azure AD -> App registrations and select the Enterprise Application that is used to configure user authentication with KeyTalk and go to API Permissions.

Add permission for Intune -> Application permissions -> scep_challenge_provider.

Add permission for Microsoft Graph -> Application permissions -> Application.Read.All.

If still available, add permission for Azure Active Directory Graph -> Application permissions -> Application.Read.All.

Grant admin consent for the permissions.



Configure Intune: Configuration profiles

Configuration Profiles must be configured to allow devices to request and install SCEP certificates. Generally, this involves 3 types of configuration profiles: Trusted Certificate, SCEP certificate and a usage profile, for example Wi-Fi or VPN Authentication. These profiles should be created in that order.

Go to the Endpoint Manager admin center -> Devices -> Configuration profiles.

Configure Intune: Trusted certificate profile

First create a Trusted certificate profile. This profile will install the trusted certificate for each platform* you support.

**Note: For Windows choose the platform "Windows 8.1 and later".*

- Select Create profile, choosing the platform and Profile type 'Trusted certificate'.
- 'Step 2. Configuration setting' upload the same SCEP Issuing CA Certificates you uploaded to KeyTalk SCEP Configuration (rename the .pem file to .cer if necessary).
- Upload the .cer file you have prepared in the 'Configure Intune: Prepare the Trusted certificate' step.
- *Windows only:* For SCEP Issuing CA Certificates (as uploaded in KeyTalk) with Issuing CA chain, choose Destination Store 'Computer certificate store – Root'. For a single Issuing CA cert only, choose 'Computer certificate store – Intermediate'
- Step 3: Assign to/exclude specific Device groups and/or choose 'Add all devices'.

Trusted certificate ...

Windows 8.1 and later

✓ Basics ⓘ Configuration settings ③ Assignments ④ Review + create

Certificate file * Not configured

Select a valid .cer file

✗ The value must not be empty.

Destination store ⓘ

Computer certificate store - Intermediate

Configure Intune: SCEP profile

Second create a SCEP profile.

- Select Create profile, choosing the desired platform and Profile type 'SCEP certificate'.
- Configure the certificate settings so they correctly match your device certificate profile settings where possible.
- Select the Trusted certificate profile you configured as the 'Root certificate'
- Add your available SCEP Server URLs in the following pattern
https://[IP or address]:/intunescep
Examples: <https://demo.keytalkdemo.com/intunescep>
- Assign to/exclude specific Device groups and/or choose 'Add all devices'.

Configure Intune: Remaining profiles

Create a profile for which the certificate should be used.

Windows Wi-Fi example, when setting the Configuration settings:

- Choose 'SCEP certificate' as the Authentication method.
- Select the correct SCEP profile under "Client certificate for client authentication (Identity certificate)"

Root certificates for server validation

KeyTalkDemoPCATrust



+ [Select one or more certificate profiles](#)

Client Authentication

Authentication method * ⓘ

SCEP certificate

Client certificate for client authentication (Identity certificate) *

SCEP for Win10



+ [Select a certificate profile](#)

Maintenance

Please ensure to keep the RA certificates up-to-date.