



Windows agent admin manual

Contents

1. Introduction	2
2. Installation	3
2.1. Guided installation	3
2.2. Silent installation Windows end-user device	4
2.3. Silent installation Windows Servers for admin accounts	5
2.4. System level deployment of KeyTalk agent to Windows Servers	6
2.4.1 Installation.....	6
2.4.2 Configuration system level KeyTalk Windows agent	7
3. KeyTalk agent Configuration.....	10
4. Requesting a certificate (and key-pair).....	11
5. Reporting a problem : logfiles.....	11
6. Requesting and auto-renewing a certificate for IIS and other server applications	12
7. Auto configuring an S/MIME LDAP secure email address book for Outlook.....	13
8. Auto configuring S/MIME email signing and encryption for Outlook.....	13
9. Command line KeyTalk client.....	14
10. Remote Desktop / Citrix environment KeyTalk agent support.....	14
11. TPM 2.0 based virtual smartcard support	15
12. Renewal Windows Scheduled Tasks explained	15
13. KeyTalk support and contact details.....	16

Company	KeyTalk 1 BV
Author	MR van der Sman
Creation date	9 August 2015
Last updated	21 July 2025
Product	KeyTalk Windows agent
Data classification	Public
Software version	7.8.0
Manual version	7.8.0.1

1. Introduction

The KeyTalk Certificate and Key Management Solution supports various certificate automated enrollment protocols, such as ACME, SCEP, Native APIs, and custom REST API.

Our KeyTalk agent has been created around the KeyTalk Virtual Appliance REST API using TCP port 443 (TLS 1.3) and 80 (AIA downloads and CDP based CRL verification).

Its main advantage over ACME based agents, is that the KeyTalk agent supports private key rollover, and can collect existing certificate data related to already deployed certificates and keys.

The KeyTalk agent for Windows is used to seamlessly deploy and manage X.509 certificates for Windows based systems.

S/MIME certificates and private keys can be installed and configured for various regular email addresses, as well as shared mailboxes.

Network and VPN authentication certificates and private keys can be installed as both user and machine certificates in either the personal or system certificate store.

Server certificates and keys can be installed as is, or bound to an IIS or Websphere webserver, including support for Server Name Indication (SNI). Our custom PowerShell script supports allows you to configure any new or renewed certificate (and private key) and a preferred format for any application you can create a PowerShell script for.

These KeyTalk managed and deployed X.509 certificates are mostly used to:

- ✓ Enable email encryption and decryption
- ✓ Enable email digital signing to combat Business Email Compromise (BEC)
- ✓ Securely authenticate to Wifi, VPN and server applications using 802.1x or mTLS.
- ✓ Enable TLS on (web)servers and other applications.

The KeyTalk agent for Windows comes in 2 main flavors:

- 1) The generic enterprise KeyTalk agent: it supports various methods of authentication, supports the use of various certificate templates, and is compatible with Windows 10/11 and the Windows server range as of Server 2016 with latest updates and patches.
- 2) The Secure Email Service (SES) KeyTalk agent: It's a simplified version of the KeyTalk enterprise agent, focused solely on issuing S/MIME certificates using a One Time Password via email methodology. This version does not support multiple certificate templates and does not support the Windows server range.

Both the enterprise and the SES KeyTalk agent come in 2 variants:

- a) With certificate and key scraper function: Using the KeyTalk serverside configuration settings, a KeyTalk agent can attempt to scrape a single or multiple types of certificates and private keys from the Windows certificate store (personal and/or system). Primarily used to secure, make visible and make redeployment possible of known and unknown installed certificates to the KeyTalk management environment.
- b) Without certificate and key scraper function: These agent lack the entire codebase, to satisfy auditor and compliance officer needs where the scraping feature is deemed a risk.

2. Installation

To install the KeyTalk agent for Windows, administrator permissions are required.
Using the agent requires regular user permissions.

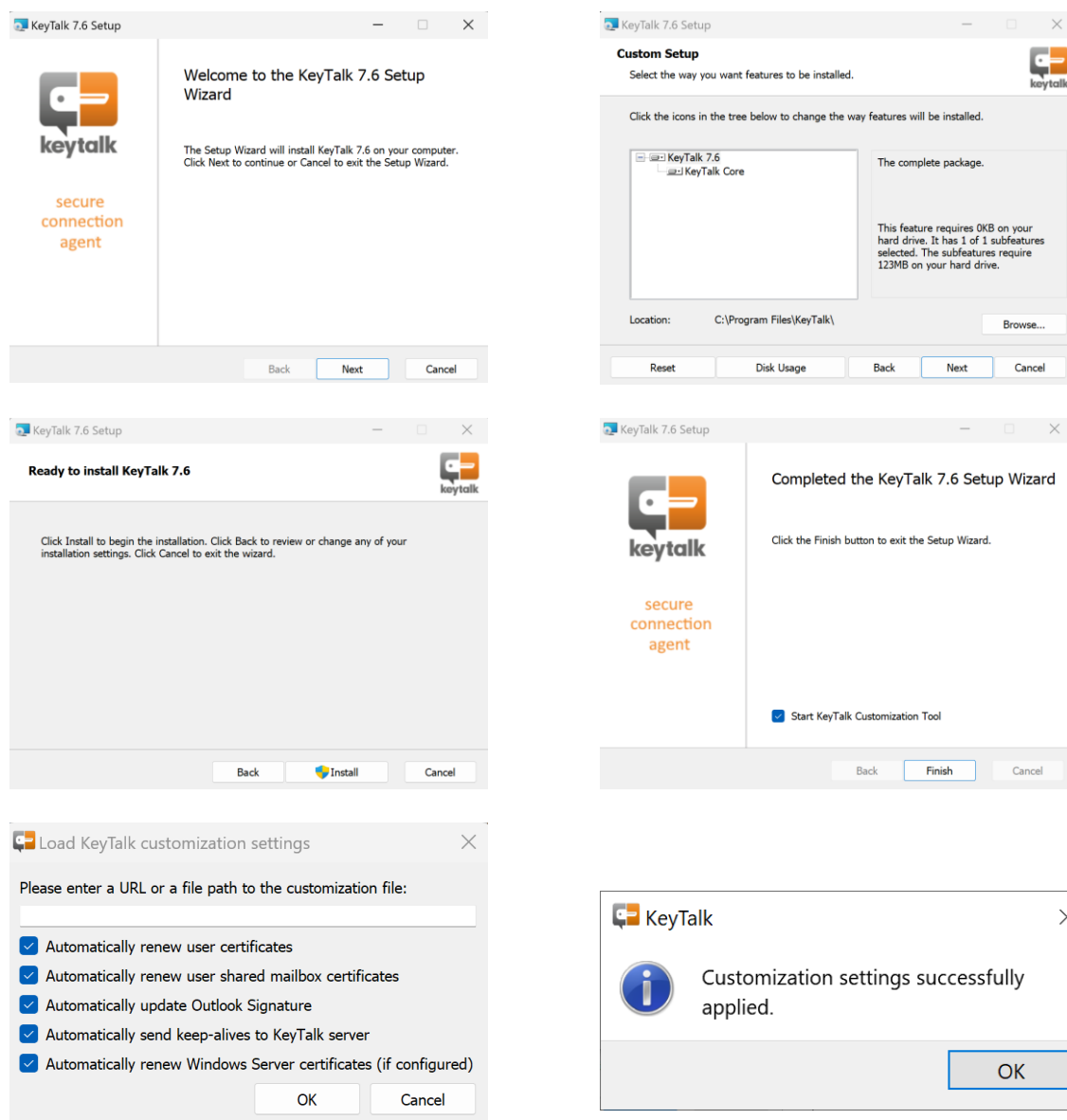
Note: depending on whether you are installing the Secure Email Agent or the KeyTalk Enterprise agent, the installation screens may differ from those documented below.

For use of S/MIME automated Classic Outlook configuration ensure your user's Outlook is already configured for the relevant email addresses.

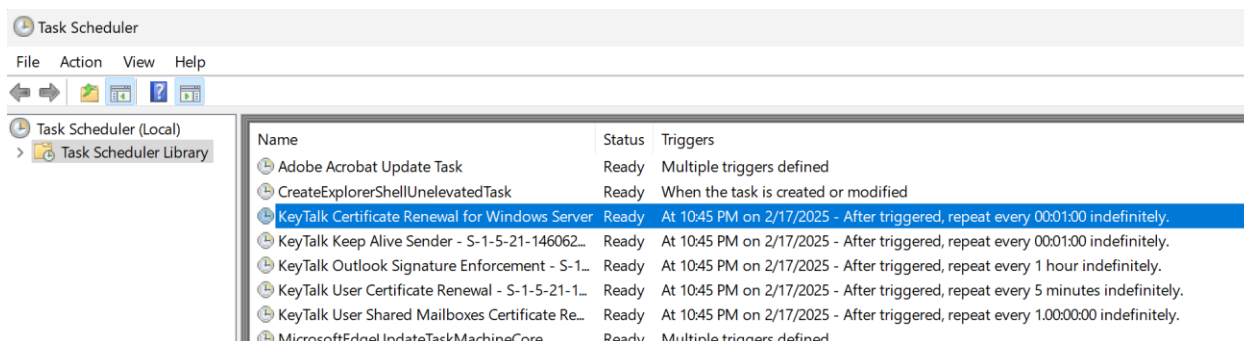
New Outlook is as of 17-Feb-2025 still in beta for S/MIME support according to Microsoft. New Outlook currently only supports S/MIME on a primary email address but not on any other configured email addresses.

2.1. Guided installation

Install the KeyTalk agent as found here: <https://www.keytalk.com/download#clients>



The KeyTalk agent installer adds tasks to the Windows Task Scheduler. These tasks when enabled, regularly check if the installed certificates are about to expire, have been revoked, have expired or have been removed. When so the KeyTalk agent will be invoked for renewal, either in the background (Windows Servers, or Users having a Kerberos token) or in plain sight requiring active interaction with the user. These tasks also guard for updated/changed Outlook textual disclaimers (when set KeyTalk server side), and support regular KeyTalk agent to KeyTalk server keep-alive messages ensuring the admins know which endpoints still have an active KeyTalk agent running.



2.2 Silent installation Windows end-user device

Most administrators will prefer a silent installation to multiple laptops/desktops so these can easily be deployed via script or GPO or through Intune.

With the KeyTalk agent for Windows being an MSI the administrator can easily repackage his own installer. To (mass) deploy using CLI, administrators can use the following command:

```
cscript /nologo MsiSilentInstall.vbs path\\to\\msi [ full-path\\to\\rccd [rccd-proxy-user rccd-proxy-password] ]
```

Example: msiexec /i KeyTalk.msi /qn RCCDPATH=https://downloads.keytalk.com/test.rccd

The RCCD (Real Client Configuration Data) file url most likely points to the KeyTalk virtual appliance-side stored configuration file (as found under the relevant Certificate Template), in which case the url will look something like:

<https://keytalk.keytalk.com:443/public/1.6.8/rccd?uid=9b922ce879ec4845b7bb6cd44b1f9ae9>

When it's not possible to deploy the KeyTalk agent via the provided sample VBS script, simply use a 2-step deployment.

- 1) Deploy the KeyTalk agent msi
- 2) Configure the installed KeyTalk agent using the command:
 "C:\Program Files\KeyTalk\ReseptConfigManager.exe" --rccd-path=https://downloads.keytalk.com/test.rccd

2.3 Silent installation Windows Servers for admin accounts

Most administrators will prefer a silent installation to multiple servers, whereby the server configuration task (task.ini) is also included in the silent installation.

The below is an example on the task.ini file to configure a target Windows server with IIS using a default IIS binding IP (0.0.0.0):

```
ConfigVersion = "2.0";
TaskList = (
{
    Name = "Task_Server";
    TaskType = "Regular Task";
    UseISBinding = false;
    UseWebSphereBinding = false;
    KeyTalkProvider = "MyCompany";
    KeyTalkService = "Server_Internal-KeyTalkCA";
    KeyTalkUser = "__KT_HOST_FQDN__";
    KeyTalkPassword = "";
    CertificateStore = "My";
    CertApproverEmail = "";
    TrackComputerName = "Do not track";
    HttpsBindingIp = "0.0.0.0";
    HttpsBindingDomain = "";
    HttpsBindingPort = 443;
    WebSphereKeyDbTypeParam = "pkcs12";
    WebSphereKeyDbPath = "";
    WebSphereKeyDbPwd = "";
    WebSphereHttpServerPath = "";
    WebSphereCertLabel = "";
    ScriptLogFilePath = "C:\\Users\\test \\AppData\\Local\\Temp\\keytalk_task_Task.log";
    EmailReporting = false;
} );
```

NOTE!: “__KT_HOST_FQDN__” is a parameter value and automatically selects the servername as the username in the task.ini once its opened and resaved.

With the KeyTalk app for Windows being an MSI the administrator can easily repack his own installer, or the administrator can use the following command:

```
cscript /nologo MsiSilentInstall.vbs \path\to\msi \path\to\rccd --tasks-ini \path\to\tasks.ini
```

2.4 System level deployment of KeyTalk agent to Windows Servers

Where chapter 2.3 assumes installation on an Administrator account level on the Windows Server, this is not always preferred as admin accounts can come and go. Thus requiring the KeyTalk agent to perpetually run on system level.

These steps outline the flow to install and configure KeyTalk Windows agent in order to obtain certificates as Local System account on Windows Server 2016 and beyond (incl optionally IIS)

2.4.1 Installation

1. Download psexec.exe from Sysinternals
2. Start command prompt as admin
3. Start command prompt as Local System account
> psexec -i -s cmd.exe
4. Install KeyTalk agent as Local System

```
> msixec /i KeyTalkAgent-<version>.msi
```

Or if you choose to both install and customize KeyTalk in a single command:

```
> msixec /i KeyTalkAgent-<version>.msi /qb RCCDPATH=rccd-path-or-url
```

You can optionally prevent KeyTalk Windows Scheduled tasks from been created during installation by specifying CREATE_SCHTASKS=No argument:

```
> msixec /i KeyTalkAgent-<version>.msi /qb RCCDPATH=rccd-path-or-url  
CREATE_SCHTASKS=No
```

You can also install KeyTalk Windows server task configuration:

```
> msixec /i KeyTalkAgent-<version>.msi /qb RCCDPATH=rccd-path-or-url  
CREATE_SCHTASKS=No WSVR_TASKS_CONFPATH=\path\to\tasks.ini
```

2.4.2 Configuration system level KeyTalk Windows agent

Once installed, KeyTalk agent for Windows can be configured as Local System either from CLI or using UI tooling. Below we outline both options.

2.4.1 Configuration using CLI

UI-less configuration could be useful for further automating KeyTalk agent deployments.

From the Local System CLI

```
> pushd C:\Program Files\KeyTalk
```

Use *ReseptConfigManager* utility to (re)load RCCD, optionally without creating KeyTalk Scheduled tasks and to deploy Windows Server scheduled tasks configuration from tasks.ini.

```
> ReseptConfigManager.exe [--rccd-path rccd-path-or-url  
[--create-schtasks Yes|No]] [--tasks-ini-path \path\to\tasks.ini]
```

Use *ConfigUpdater* utility to create and remove KeyTalk Windows Scheduled tasks. If the task already exists, it is kept intact.

```
> ConfigUpdater.exe [--install-scheduled-tasks] [--remove-scheduled-tasks]
```

To create only KeyTalk Windows Server Scheduled task:

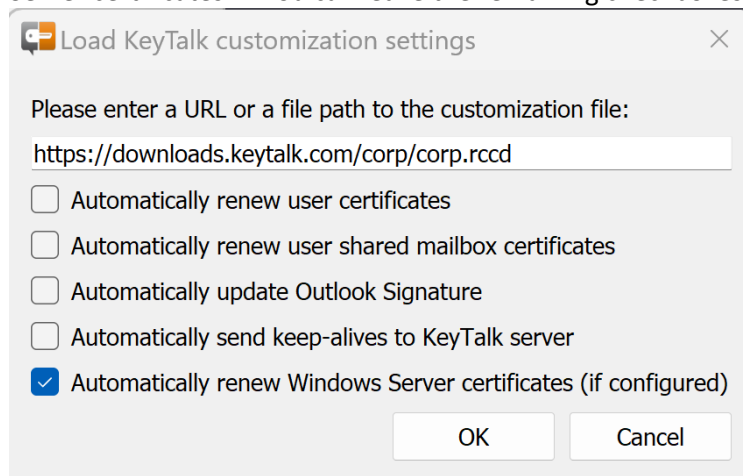
```
> ConfigUpdater.exe --install-winsvr-cert-renewal-scheduled-task
```

2.4.2 Configuration using UI

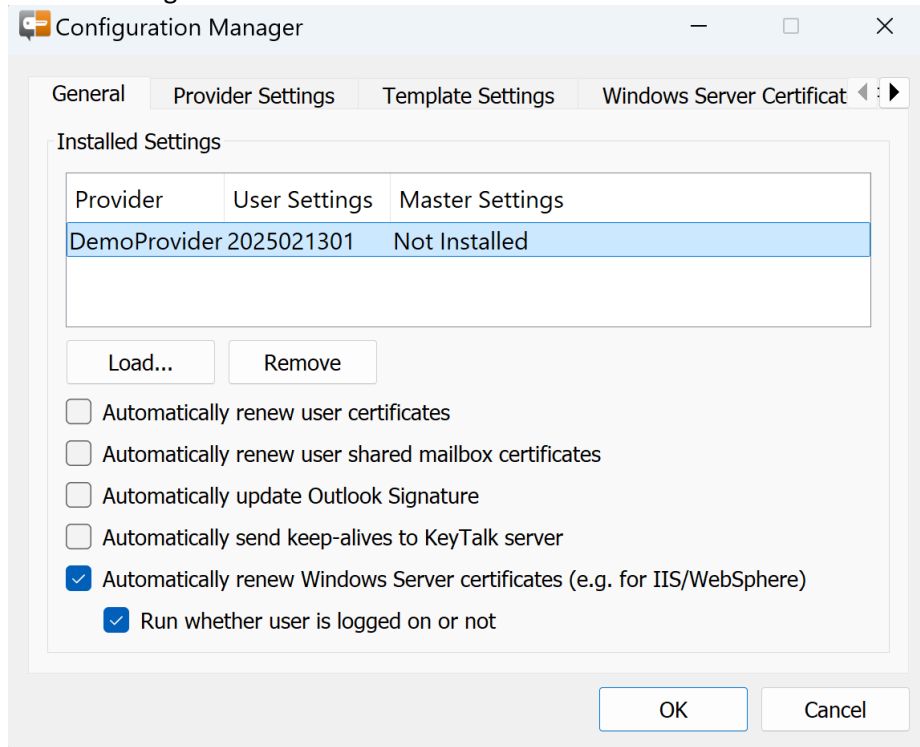
From the Local System CLI

```
> pushd C:\Program Files\KeyTalk  
> ReseptConfigManager.exe
```

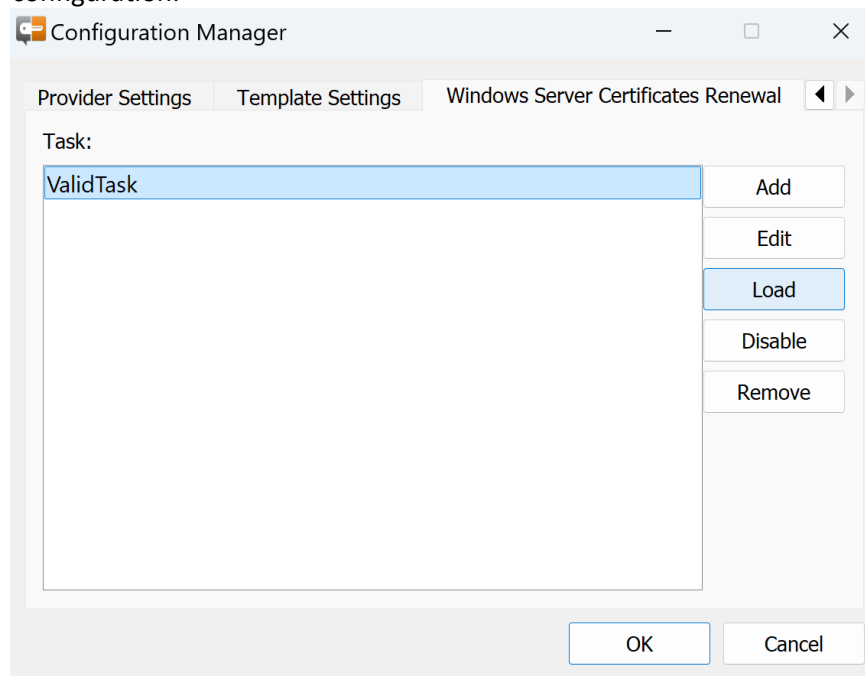
- A) If your KeyTalk agent is not yet customized with a configuration file (RCCD file), you will see the following screen. Enter the location of RCCD file and select “Automatically renew Windows Server certificates”. You can leave the remaining checkboxes unselected.



- B) When you your KeyTalk agent has already been customized with a configuration file, you will see the following screen. Select “Automatically renew Windows Server certificates”. You can leave the remaining checkboxes unselected.



Go to “Windows Server Certificate Renewal tab” and create tasks from “Windows Server Certificates” tab. Optionally, you can load the tasks configuration from the previously created configuration.



2.4.3 Enrolling the certificate (and private key)

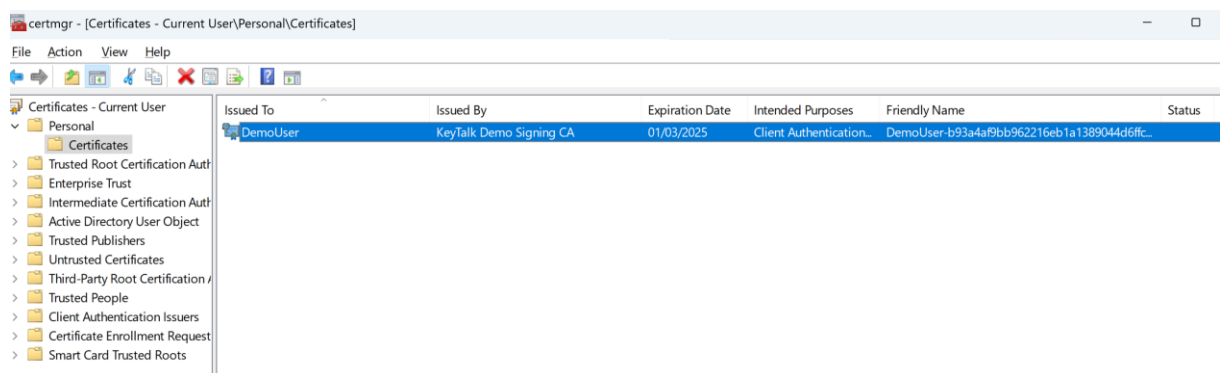
Once KeyTalk Windows Server Certificate tasks are configured, the Windows server certificate is automatically requested from KeyTalk server every minute. You can watch the progress in %WINDIR%\Temp\keytalk_task_<task-name>.log

You can choose to force requesting a certificate from Windows Task Scheduler.

DropboxUpdateTaskMachineCore	Running	Multiple triggers defined
DropboxUpdateTaskMachineUA	Ready	At 8:35 every day - After triggered, repeat every 1 hour for a duration of 1 day.
iGoAudioTask	Running	At log on of any user
iGoAudioTaskSession	Running	At log on of any user
KeyTalk Certificate Renewal for Windows Server	Ready	At 18:11 on 09-Dec-24 - After triggered, repeat every 00:01:00 indefinitely.
MicrosoftEdgeUpdateTaskMachineCore	Ready	Multiple triggers defined
MicrosoftEdgeUpdateTaskMachineUA	Ready	At 8:28 every day - After triggered, repeat every 1 hour for a duration of 1 day.
NvDriverUpdateCheckDaily_{B2FE1952-0186-46C3-BAEC-A8...	Ready	At 12:25 every day
NVIDIA GeForce Experience SelfUpdate_{B2FE1952-0186-46...	Ready	On event - Log: Application, Source: NVIDIA GeForce Experience SelfUpdate Sourc
NvNodeLauncher_{B2FE1952-0186-46C3-BAEC-A80AA35AC5...	Ready	At log on of any user - After triggered, repeat every 1.00:00:00 indefinitely.
NvTmRep_CrashReport1_{B2FE1952-0186-46C3-BAEC-A80A...	Ready	At 12:25 every day
NvTmRep_CrashReport2_{B2FE1952-0186-46C3-BAEC-A80A...	Ready	At 18:25 every day

Locate the obtained certificate by starting Windows Certificate Manager from the Local System CLI:

```
> certmgr.msc or MMC
```



2.4.4 Troubleshooting

Configuration logs:

```
%WINDIR%\Temp\ktconfig.log  
%WINDIR%\Temp\ktconfigupdater.log  
%WINDIR%\Temp\ktconfigtool.log  
%allusersprofile%\keytalk\ktbrokerservice.log
```

Certificate retrieval logs:

```
%WINDIR%\Temp\keytalk_task_<task-name>.log  
%WINDIR%\system32\config\systemprofile\AppData\Roaming\KeyTalk\ktclient.log
```

3. KeyTalk agent Configuration

Each KeyTalk agent requires a configuration file. Without it the KeyTalk agent doesn't know where to contact the KeyTalk virtual appliance to request a certificate.

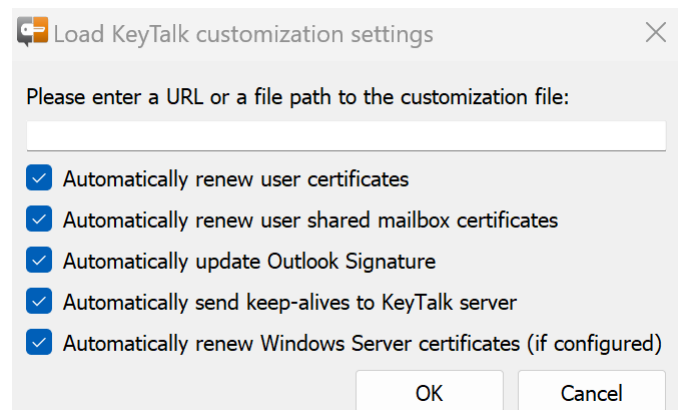
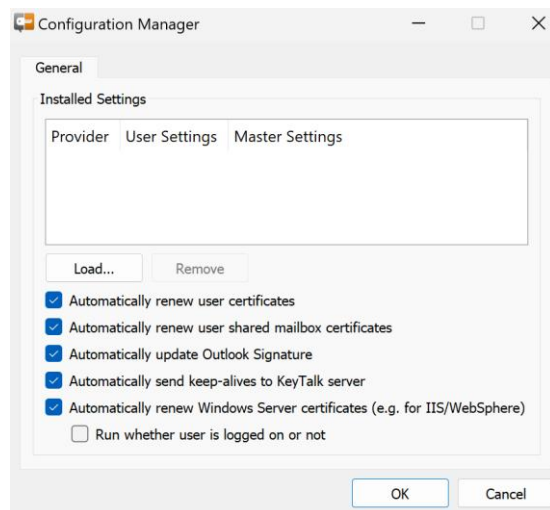
Additionally, the configuration file enables the KeyTalk agent to set the private CA running on your KeyTalk virtual appliance as trusted on the Windows environment the agent gets deployed to. As of version 7.6.x the KeyTalk agent can also use port 80 to fetch the CA trust of the private CA from the KeyTalk virtual appliance.

The needed configuration file is a Real Client Configuration Data file, or RCCD. It only contains public information so can be distributed on the open internet when need be.

Most companies will distribute it by means of a url whereby the RCCD is by default hosted on the KeyTalk virtual appliance (full url found in the KeyTalk Certificate Template)

To import this configuration file into the KeyTalk agent, the app will automatically ask for it when a configuration file is missing.

Or you can manually load it by starting the "KeyTalk Configuration Manager" as found under installed programs.

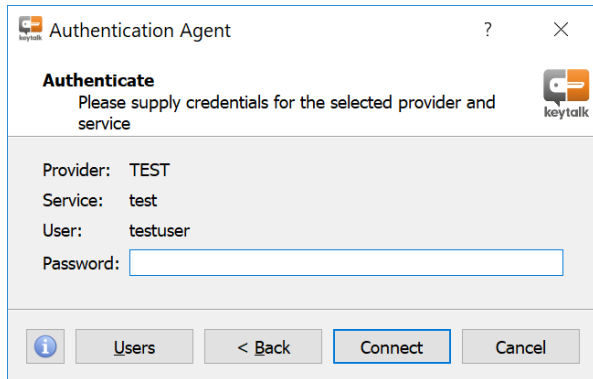


The actual config settings can be found under: `\AppData\Roaming\KeyTalk\user.ini`

4. Requesting a certificate (and key-pair)

Once the configuration file has been loaded, the KeyTalk agent will be able to fetch a certificate for the user (or the server or the machine)

Depending on the KeyTalk virtual appliance administrator enforced configuration settings, the user may be requested to type the corporate authentication credentials, such as username/password or token based One Time Password:



Alternatively, no username/password or other credentials might be asked, as Kerberos based silent authentication is also supported. When using Kerberos, a username/password will only be requested if the Kerberos token is found not be valid or usable.

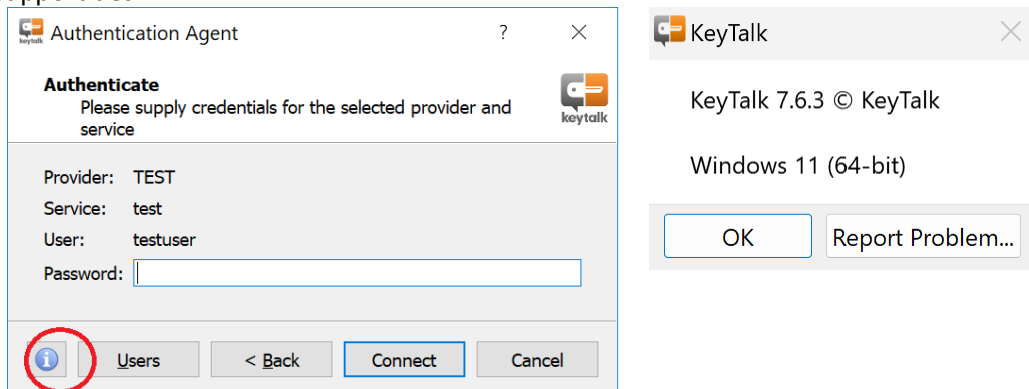
A message will appear when a certificate was successfully obtained and automatically installed.

Should you wish to inspect the installed certificate, open CMD or Powershell and type: certmgr or mmc

5. Reporting a problem : logfiles

The KeyTalk app keeps a local logfile for trouble shooting purposes.

Should a user encounter any issues, the user can generate a problem report and send it by email to his support desk:



Users and support staff can easily open the generated Problem Report, by renaming the created DAT file to ZIP and opening it. The container contains several relevant logfiles, whereby the most notable log is the ktclient.log file.

This logfile can also be directly found under the current user's %AppData%\Roaming\KeyTalk

6. Requesting and auto-renewing a certificate for IIS and other server applications

Following the KeyTalk agent installation process and configuration, an administrator can finalize the configuration to automatically fetch, renew, and bind certificates to IIS or Websphere HTTP.

- The KeyTalk app/Configuration Manager must be run with **administrator** rights
- The IIS server must already have been configured for SSL/TLS on port 443
- IIS version must be minimally 10
- The Windows server must be minimally 2016
- The KeyTalk virtual appliance Certificate Template must be set to issue server certificate (Extended Key Usage = Server Auth, or DV/ OV/EV public CA certs)

From the KeyTalk Configuration Manager, create a certificate task as administrator of the Windows server:

Certificate Update Task

KeyTalk Certificate retrieval

Provider: DemoProvider
Template: CUST_ANO_INTERNAL
User: DemoUser
Password:
Import Certificate To Store: My
Track Computer Name: Do not track
Certificate Approver Email:
Domains for SAN DNS: www.test2.keytalk.com

☐ Use IIS HTTPS binding

IIS HTTPS binding

☒ Binding IP: 0.0.0.0
☐ Binding Domain:
Binding Port: 443

☐ Use IBM WebSphere Binding

IBM WebSphere

Key Database Type: pkcs12
Key Database Path:
Key Database Password:
HTTP Server Install Path:
Certificate Label:

☒ Run Command on successful certificate retrieval

Settings

Command: powershell.exe -ExecutionPolicy ByPass -File "C:\Program Files\KeyTalk\scripts\Sample_ApplyCertificateToIIS.ps1"
Argument 1: <path to PKCS#12 certificate package>
Argument 2: <password for PKCS#12 certificate package>
Argument 3: <certificate SHA1 fingerprint>

Logging

Log File: C:\Users\andre\AppData\Local\Temp\keytalk_task_andy.log

☐ E-mail notifications

E-mail settings

Notify on success: ☒

Save Cancel

To mass deploy your server certificate management template you can use:

```
> cscript /nologo MsiSilentInstall.vbs "c:\KeyTalkClient-5.X.X.msi"  
"c:\MyProvider.rccd" --tasks-ini "C:\tasks.ini"
```

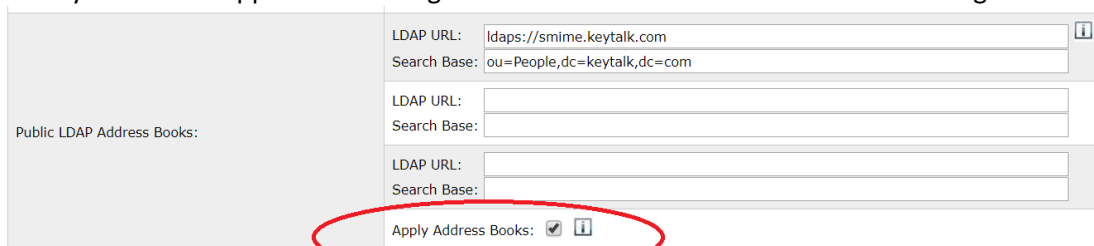
In order to support SNI hosts, 1 task needs to be created per SNI host.

7. Auto configuring an S/MIME LDAP secure email address book for Outlook

When the KeyTalk virtual appliance has been configured to configure client side an LDAP address book, containing email address public keys to support S/MIME email encryption, the KeyTalk agent will facilitate this configuration provided local user right allow for this.

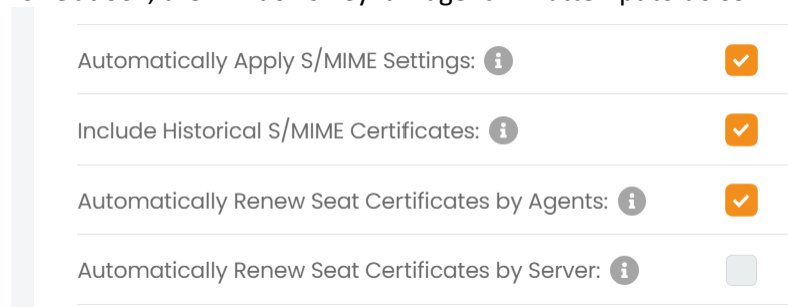
The automated configuration will only happen when:

- Classic Outlook is set as the default mail client
- The KeyTalk virtual appliance is configured to enforce the LDAP address book configuration



8. Auto configuring S/MIME email signing and encryption for Outlook

When the KeyTalk virtual appliance has been configured to configure client side email encryption and signing for Outlook, the Windows KeyTalk agent will attempt to do so:



Clientside the Outlook default email address is expected to the main email address the certificate is issued to.

If the main email address does not match with the S/MIME certificate's email address, a best match email address is configured Outlook side for the S/MIME email certificate as obtained by the KeyTalk client.

The KeyTalk client will enforce SHA256 as the hashing algo and set AES256 as the encryption algo. Additionally it will set email signing to always on. Email encryption is not set automatically.

Note: The KeyTalk agent for Windows will not publish the configured certificate to GAL. Reason being that publish to GAL only exists in single email configurations on Outlook, and AD or EntraID syncs periodically with Exchange (Online) for GAL purposes, whereby KeyTalk virtual appliance already publishes the certificate to AD, and EntraID, and Exchange Online and optionally to a configured LDAP Address book (such as OpenLDAP)

9. Command line KeyTalk client

Command line users, or those who wish to script their processes, can also use the KeyTalk agent from the command line.

The command prompt client can be found in the KeyTalk program installation directory, usually:
"C:\Program Files\KeyTalk\ReseptConsoleClient.exe"

Resept is an ode and reference to the 2003 original internal project name for the product now known as KeyTalk.

To see all possible commands, type: **reseptconsoleclient -help**

A sample command could be:

reseptconsoleclient --user test --password test --save-pfx

In this example we assume a single KeyTalk service RCCD config file was loaded into the KeyTalk client, and as a result the reseptconsoleclient will automatically assume that the only available KeyTalk provider and only available service needs to be addresses, using the username test and password test with the certificate output in PFX format (and a separate private-key password file).

The saved PFX and passwordfile can be found in: \AppData\Local\Temp\keytalk.pfx and
\Local\Temp\keytalk.pfx.pass

A sample command could also be:

**reseptconsoleclient --provider PROVIDERNAME --service SERVICENAME --user test
--password test --save-pfx**

Similar to the first example, in this case a more elaborate KeyTalk configuration likely applies, whereby multiple KeyTalk providers (ie KeyTalk clusters) are available to choose from, and multiple KeyTalk services are available to choose from, therefor requiring the KeyTalk provider and service to be specified.

When instead of a PFX a PEM file is preferred, use --save-pfx , AND change the user.ini (see chapter 3) to include:

CertFormat="PEM";

NOTE: Kerberos based authentication is currently reserved only for GUI based client use.

10. Remote Desktop / Citrix environment KeyTalk agent support

Remote Desktop and Citrix environments are hardly ever single server based.

When deploying a KeyTalk agent for a user, the KeyTalk RCCD configuration file needs to be available on every server instance the cluster.

The KeyTalk agent supports a master config file which can be embedded in any KeyTalk RCCD file upon creation in the KeyTalk virtual appliance with a value set to "do not allow overwrite"

This config file is installed in the /Users/Public and will be automatically copied to a User, when a KeyTalk config file is missing, or is deemed corrupt.

11. TPM 2.0 based virtual smartcard support

The KeyTalk agent for Windows supports TPM 2.0 based virtual smartcards.

As a result a private key is generated on the TPM, based on the Certificate Signing Request meta data as defined in the KeyTalk certificate template, provided that TPM Virtual Smart Card support is selected.

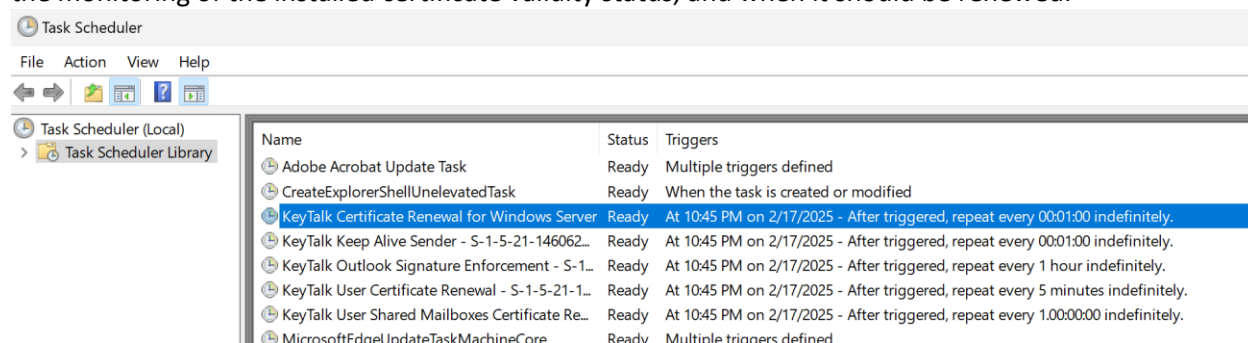
When the agent sends back the CSR to the KeyTalk virtual appliance to have it signed, the meta data as part of the CSR is verified against the enforced KeyTalk certificate template configured required CSR matching data. If it doesn't match, the certificate will not be issued. This feature has been implemented to prevent skilled users from manipulating the data generated by the KeyTalk agent.

The KeyTalk agent for Windows does not activate and configure a virtual smart card as of yet. It currently assumes the Admin has already done so.

NOTE: Key roll over is not supported when using TPM based virtual smart cards.

12. Renewal Windows Scheduled Tasks explained

Upon installing the KeyTalk agent, various scheduled tasks can be added to the Windows instance, aiding in the monitoring of the installed certificate validity status, and when it should be renewed.



KeyTalk IIS and IBM WebSphere SSL Certificate Renewal

This script runs checks on all the tasks as setup in the KeyTalk Configuration Manager.

By default the script runs every single minute, checking whether the certificates related to the task are still valid.

When a new/renewed certificate is required it automatically requests this certificate from the KeyTalk server using the KeyTalk agent, and stores it to the relevant certificate store.

It also updates the IIS binding to the new certificate if the task requires it.

KeyTalk Keep Alive Sender

Sends a message to the KeyTalk virtual appliance to prove the agent is active on the enrolled end-point.

KeyTalk Outlook Signature Enforcement

When the KeyTalk virtual appliance contains a configuration to enforce specific Disclaimer texts under a given Outlook configured corporate email, this task ensures any user made changes are undone.

KeyTalk User Certificate Renewal

This script checks with the KeyTalk agent if the certificate for the latest provider/service is still valid. By default the script runs every 5 minutes. If a new/renewed certificate is required it attempts to quietly refresh using Kerberos if the Service allows this. Otherwise it will open the KeyTalk agent for the user to authenticate.

KeyTalk User Shared Mailboxes Renewal

This script checks if a given user is a member of 1 or more shared mailboxes on Exchange Online. When so, and the KeyTalk virtual appliance EntraID is configured for this purpose, the Shared Mailbox S/MIME certificate and private key is fetched and installed/configured for the user's Outlook.

13. KeyTalk support and contact details

KeyTalk provides third line support to its commercial partners.

For 1st and 2nd line support kindly contact your IT department or your KeyTalk supplier, and include a description of your problem together with a generated agent Problem Report.

Should you feel there is a need to directly contact KeyTalk for technical support or technical questions, kindly raise a ticket using: <https://support.keytalk.com> or email us at: support@keytalk.com

Should you have commercial related questions, kindly email us at: sales@keytalk.com

Our office details:

Company name:	KeyTalk I BV
Dutch Chamber of Commerce registration:	59072555
VAT number:	NL853305766B01
KeyTalk HQ address:	Maanlander 47 3824MN Amersfoort The Netherlands