KeyTalk automated IIS certificate renewal

Serving HTTPS traffic via the Microsoft Internet Information Services (*IIS*) server requires assigning a server SSL certificate for each HTTPS binding[1] defined in your IIS server. Typically, these certificates have a long lifetime. Decreasing certificate lifetime improves security, but increases maintenance work to generate and assign new certificates.

This document shows how the *IIS HTTPS certificate renewal* feature of the KeyTalk windows client can be used to automate the retrieval and installation of new IIS HTTPS binding certificates on Windows 2012 server systems.

After configuration, KeyTalk will do the following periodically for each IIS HTTPS binding you have configured for automated certificate retrieval:

1. Check the lifetime of the currently installed certificate
2. If the certificate is about to expire (typically less than 25% lifetime):
   a. Retrieve a new SSL certificate from your KeyTalk server
   b. Apply the retrieved certificate to the configured IIS HTTPS binding

The following sections describe how to configure your KeyTalk client and server.

System Requirements

Before configuring the *IIS HTTPS certificate renewal* feature, please make sure that the server running IIS meets the following requirements:

1. Windows Server 2012 installed
2. Microsoft IIS version 7.5 or higher with properly configured *https* binding
3. Windows Management Framework version 3 or higher installed
4. Powershell v3 installed
   - normally installed automatically by Windows Management Framework 3
   - check by typing `$PSVersionTable` in powershell command line
5. Powershell has *WebAdministration* module installed
   - check by typing `Get-Module -ListAvailable -Name WebAdministration` in powershell command line
6. User installing and running the KeyTalk Client has administrator rights

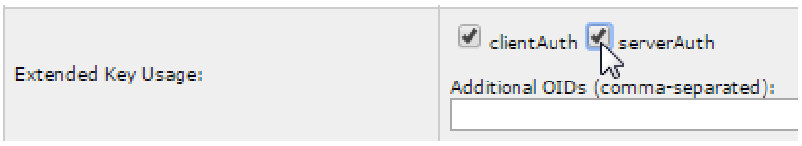
[1] An IIS HTTPS binding is a combination of IP and port number used for serving HTTPS traffic. E.g., a typical HTTPS binding runs on port 443 and listens on all IPs (*).

KeyTalk server configuration

1. Log into your KeyTalk server web interface.

2. Click *Services* → *Add*

3. Fill in the values for your new service that will be used to provide the IIS SSL certificates.
   In the Extended Key Usage section, enable the *serverAuth* setting.

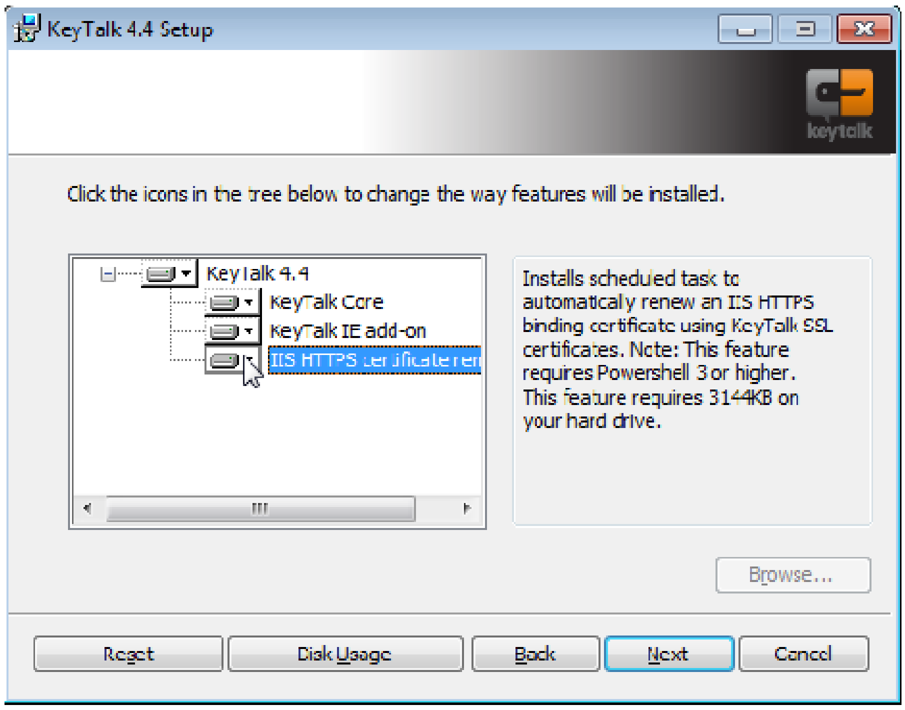


Extended Key Usage: ✓ clientAuth ✓ serverAuth
Additional OIDs (comma-separated):

4. On your authentication module backend bound to this service, create a user with the same name as your domain name (e.g. *example.com*).
   This name will be used to fill in the X.509 *Common Name* field of the generated certificates.

KeyTalk client configuration (client running on your IIS Server)

1. Set up the KeyTalk client on your server running IIS.
   During setup, enable the *IIS HTTPS certificate renewal* feature.



KeyTalk 4.4 Setup

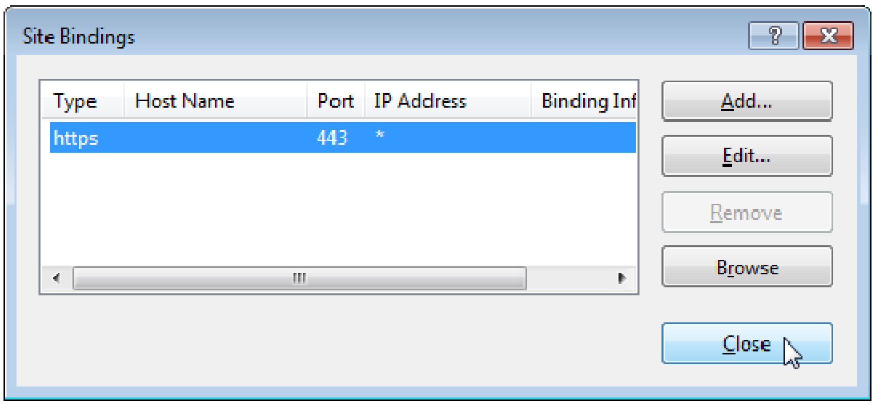
Click the icons in the tree below to change the way features will be installed.

- KeyTalk 4.4
  - KeyTalk Core
  - KeyTalk IE add-on
  - IIS HTTPS certificate ren

Installs scheduled task to automatically renew an IIS HTTPS binding certificate using KeyTalk SSL certificates. Note: This feature requires Powershell 3 or higher. This feature requires 314KB on your hard drive.

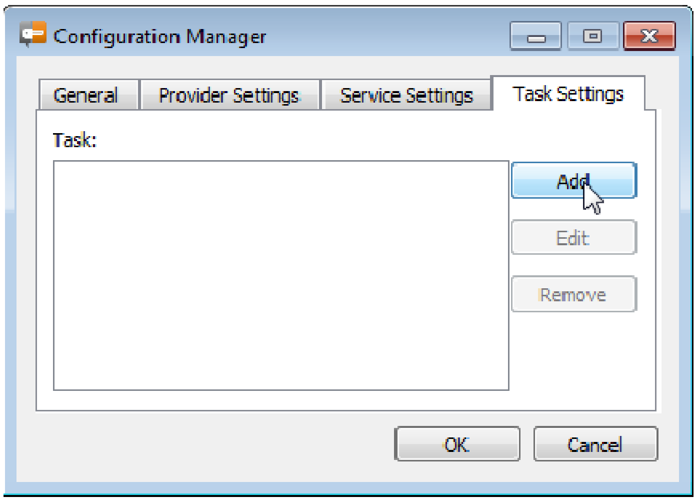
2. Load the RCCD configuration file containing the service used to provide IIS HTTPS binding certificates.

3. Look up your IIS HTTPS binding information:
    a. Start the *IIS Manager*
    b. Right click your site
    c. Select *Edit Bindings*
    d. Take note of the *Port* and *IP Address* values of your https binding:

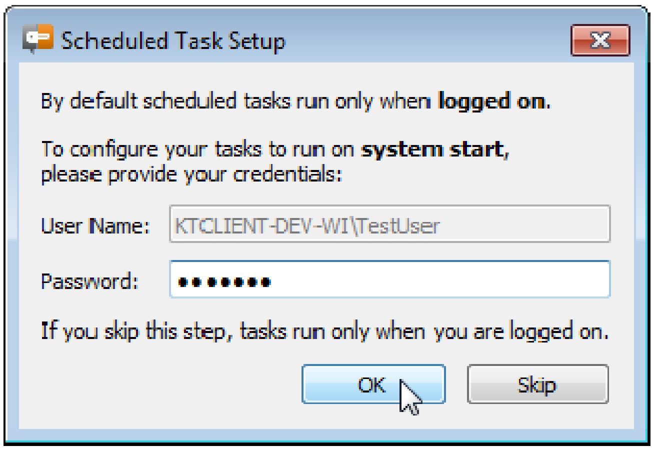


Type	Host Name	Port	IP Address	Binding Inf
https		443	*	

4. Start the *KeyTalk Configuration Manager*, select the *Task Settings* tab and click *Add*.



5. Upon adding the first task the following dialog is displayed:


Scheduled Task Setup

By default scheduled tasks run only when **logged on**.

To configure your tasks to run on **system start**, please provide your credentials:

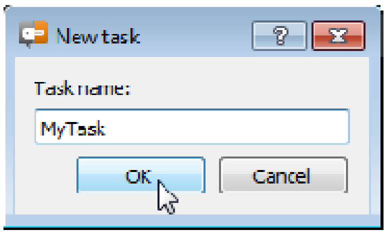
User Name: KTCLIENT-DEV-WI\TestUser

Password: ●●●●●●●

If you skip this step, tasks run only when you are logged on.

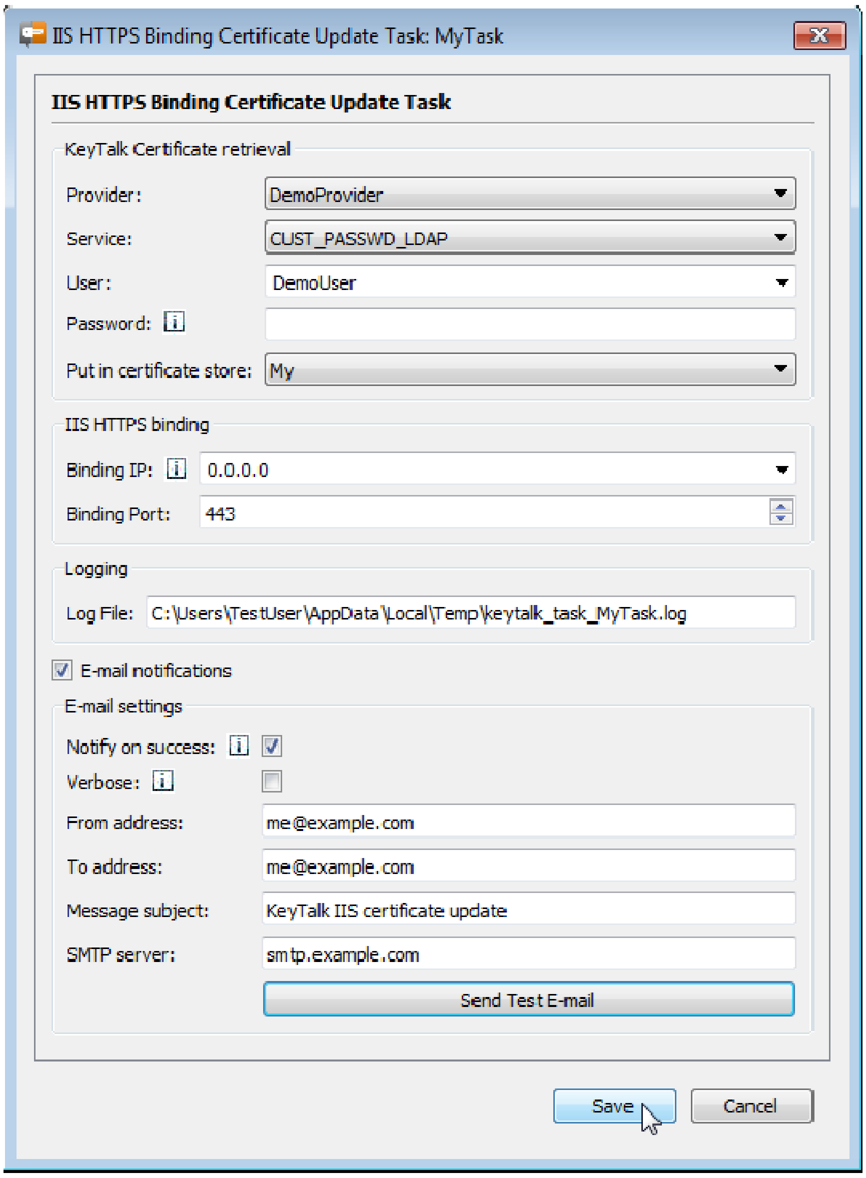
If you want tasks to run regardless whether you are not logged on or not, fill in the password and click *OK*. To keep on running tasks only when logged in, you can select *Skip*.
Note: This setting is global for all tasks.

6. Select a name for your task and confirm with *OK*.


New task

Task name: MyTask

7. Fill in the details about your KeyTalk service and IIS binding:



IIS HTTPS Binding Certificate Update Task: MyTask

IIS HTTPS Binding Certificate Update Task

KeyTalk Certificate retrieval

Provider:	DemoProvider
Service:	CUST_PASSWD_LDAP
User:	DemoUser
Password:	
Put in certificate store:	My

IIS HTTPS binding

Binding IP:	0.0.0.0
Binding Port:	443

Logging

Log File:	C:\Users\TestUser\AppData\Local\Temp\keytalk_task_MyTask.log

☑ E-mail notifications

E-mail settings

Notify on success:	☑
Verbose:	☐
From address:	me@example.com
To address:	me@example.com
Message subject:	KeyTalk IIS certificate update
SMTP server:	smtp.example.com

In the IIS server *Binding IP,* fill in the value you looked up from your IIS HTTPS binding. If the value in IIS was * you can use either 0.0.0.0 or * here.
The logging of the last run will be written to the location specified in the Log *File field*.
It is recommended to configure E-mail notifications so an e-mail is sent when certificate update fails. Currently only an SMTP server without authentication is supported. To test your notification settings use the *Send Test E-Mail* button.
More information about the fields can be found by hovering over the ⓘ icons.

After the task definition is saved, KeyTalk will check if a certificate update is due and perform an update if the certificate is about to expire.

Advanced usage

Unattended installation and configuration

The MsiSilentInstall.vbs script can be used for automating KeyTalk client installation and customization without user intervention.

The following example shows how to perform an installation of the KeyTalk client, installing an RCCD file containing provider definitions, and installing a task configuration in one go:

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

The command arguments can be read as follows:

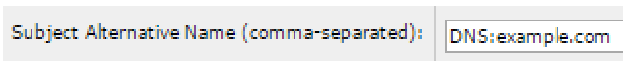
1. `"c:\KeyTalkClient-5.X.X.msi"`: use this installer file
2. `"c:\MyProvider.rccd"`: After installation, install this RCCD file containing the required providers and services to obtain certificates
3. `--with-iis` : Select the IIS Certificate renewal feature during installation
4. `--tasks-ini "C:\tasks.ini"`: After installation, install this task configuration file.
   This file is created in the steps found in section *KeyTalk client configuration (client running on your IIS Server*).
   The configuration file can be found in `%allusersprofile%\KeyTalk\tasks.ini`.

Note that installing a task configuration (the `--tasks-ini` option) requires the `--with-iis` option, which enables the scheduled tasks and an RCCD file which contains the providers and services used in your task configuration.

Subject Alternative Name vs Common Name

Web browsers are allowed to identify servers by *Subject Alternative Name* as well as by *Common Name*. Modern browsers should prefer the *Subject Alternative Name* over the *Common Name.*
See RFC 5280 and RFC 6125 for more information.

The *Common Name* in the certificate is filled by the KeyTalk username used to retrieve the certificate. The *Subject Alternative Name* can be set in your KeyTalk service as follows:


Subject Alternative Name (comma-separated): DNS:example.com

Using OID instead of serverAuth option

Instead of using the *serverAuth* checkbox in the service definition you can add OID *1.3.6.1.5.5.7.3.1*. The effect of these settings is the same.

Running all tasks manually

To run all tasks manually from the command line you can use the following command:

```
> cd "C:\Program Files\KeyTalk\Scripts\"
> powershell -ExecutionPolicy Bypass -File RunScheduledScripts.ps1
```

Forcing a certificate renewal manually

By default a new certificate is only requested when it is close to expiration. Typically a certificate is renewed when 25% or less of the certificate life time is remaining.

When reducing the TTL (Time To Live) setting of your certificates, you may not want to wait for an expiration, but force a certificate to be renewed immediately instead. This can be done with the following command:

```
> cd "C:\Program Files\KeyTalk\Scripts\"
> powershell -ExecutionPolicy Bypass -File UpdateIISCertificate.ps1 -taskName
MyTask
```

IPv6 binding IPs

To use an IPv6 binding IP address, simply type it into the Binding IP field on the task configuration user interface.

Troubleshooting

PowerShell performance issues

PowerShell is used for various parts of the system. Below fix may help if you are experiencing slow performance while:

1. Running the certificate update script
2. Checking dependencies (this is done before adding or editing tasks)
3. Sending a test-email (in task configuration)

Running the following command on a *PowerShell* prompt can decrease PowerShell startup time overhead significantly:

```
> $env:path = [Runtime.InteropServices.RuntimeEnvironment]::GetRuntimeDirectory()
> cd $pshome ; dir *.dll|foreach {Write-Host "Generating image for: $_"; ngen
install /nologo $_.FullName}
```