Setting up custom Tachyon Instructions for the first time

Summary

A getting started guide to configuring and verifying your Tachyon system so that you can run customized Tachyon Instructions.

Aside from the Product Packs provided with Tachyon and the ones available from the Tachyon Exchange, Tachyon lets you add to its functionality by defining your own instructions, either by modifying existing ones or creating them from scratch.

This page describes how to prepare your Tachyon system to run your custom instructions; it does not provide a comprehensive reference for all the methods that you can use when defining your instructions, for that please refer to the online Tachyon SDK documentation.

The process requires a Tachyon administrator to use the Server installation account to install a copy of the Tachyon Instruction Management Studio (TIMS) editor on the server, and test the code signing certificate. The certificate thumbprint and your prefix can then be registered with 1E who will update the Tachyon license after which you can run your instructions.

Prefixes, code signing certificates and licensing

If you want to develop your own custom Tachyon instructions, or modify others, then you will need to sign them using your own code signing certificate so that they can be licensed, imported and run in your Tachyon system. You don't need to do this for instructions that are provided with the product or that have been downloaded from the Tachyon Exchange as they've already been code signed and licensed using the Platform and Exchange certificates from 1E.

Ideally all of your Tachyon instruction developers should share a single code signing certificate between them. Each code signing certificate must be registered in your Tachyon license and associated with a particular instruction name prefix. Ideally you would have one prefix to go with one signing certificate that could be used for all your custom instructions. When you have chosen your prefix and have your code signing certificate(s) you then need to send details of these to 1E, who will update your Tachyon license. This will then automatically activate on your Tachyon Server (assuming it has connection to the Internet).

The following points apply to the importing and running of custom Tachyon instructions:

- Tachyon will only allow instructions to be *imported* if they have been signed and the public key of the code-signing certificate exists in the Tachyon Server's Trusted Publishers certificate store.
- Tachyon will only allow instructions to be *run* if their prefix and the thumbprint of their code-signing certificate have been registered in the Tachyon Server's license file (even if instructions have been successfully imported they will be flagged as unlicensed if the license information is not there).

Registering a prefix and code signing certificate and updating the Tachyon license

The following steps may seem complex on initial viewing, but the process has been designed to verify that your code signing certificate can be used to sign instructions before you ask for it to be registered and added to the Tachyon License - as this may take several days to complete you don't want to have to wait for registration only to find that you want to use a different prefix or the signing certificate cannot be used. The general outline of the process is as follows:

- Decide what prefix you will use
- Obtain a code signing certificate, and export as a PFX for use on other computers
- Install the certificate on the Tachyon Server

Prerequisites

Before you start you will need the following:

- Tachyon Server is already installed and licensed in the lab, has been verified and is connected to the Internet
- TIMS installer MSI

Assumptions

There are many ways to define the code signing certificate and configure your Tachyon environment. Here we make some basic assumptions about the type of certificate and Tachyon environment to show the end-to-end process simply. If you want more details on other certification options please refer to the online Tachyon SDK documentation.

- Local user Personal store - for use by TIMS (optionally add to the Local computer store if multiple user accounts will use TIMS on the Server)
- Local computer Trusted Publishers store - for use by the Server
- Install TIMS and confirm it can see the code signing certificate
- Create a test instruction, sign and import it
- Before you can run the test instruction, you need to register your prefix and certificate thumbprint with 1E
- Once registration is complete you can run the test instruction
- Finally you should delete the test instruction to avoid any confusion

These steps are recommended for a lab environment with the following:

- A Microsoft CA has been installed
- A code signing template must be issued on the issuing CA. The default **Code Signing** template is sufficient
- All users will sign Tachyon Instructions on the Tachyon Server
- TIMS must be started as local administrator, so all users developing Tachyon Instructions must be AD domain user accounts that are also members of the Administrators local group on the Tachyon Server. This is one of the requirements for the Tachyon Server installation account anyway.

Steps to register a prefix and code signing certificate to obtain a Tachyon license

1. Decide your Instruction Name Prefix

a. You should choose a prefix that will be used to name all the instructions created by your TIMS developers
b. By default TIMS will use your logged-on account's domain name as your chosen prefix

2. Obtain a code signing certificate

Use this step if you and your fellow TIMS developers do not already have a code signing certificate.

Skip this step if you already have a PFX; the PFX is also useful way to share the certificate with each of your developers.

a. Log on to the Tachyon Server using the Tachyon Server installation account
b. Start Certificate Manager for Local User (CertMgr. msc) and request (enroll) a new code signing certificate, ensuring you set the option to allow the private key to be exported.

> ⊘ Enrolling on the Server using the Server installer account means only that account will be able to access the certificate on the Server, and perform the remaining steps including signing instructions using TIMS. You will need to export the certificate with private key if you need to use the certificate elsewhere or others need access it.
>
> This is why you must enable the Export Private Key when you enroll. If you don't then you will have to start the entire process over again to enroll a new certificate and register it in Tachyon.
>
> See note on Certificate permissions for more details.

c. Make a backup copy of your certificate by exporting the code signing certificate as a PFX (including private key) and make the private key exportable. When exporting you must specify a password, which you must protect. If you do not specify a password, then the private key will be accessible only to the user accounts, AD groups and computers which you specified.

Certificate permissions

In some cases, the private key may only be accessible to specific users and not accessible to the installer account - in this case you will need to do the first steps (as well as the steps that involve TIMS) on a developer's PC using the developer's account. You may also be required to import into the Local User store instead of the Local Computer store.

When using Microsoft Certificate Manager to request a new certificate then you must request using Local User instead of Local Computer because this is a requirement of Microsoft's code signing template.

To share the certificate you will need to export it and then provide it to each user to import into their Local User store, or into their Local Computer store, where it will be accessible to all users of the computer.

⊘ The default template for enrolling a code signing certificate does not automatically have **Make private key exportable** enabled. When enrolling using the Microsoft wizard you must click on the Properties button and in Certificate Properties select the Private Key tab and enable the option.

3. Import the certificate to the local computer store

This step ensures the signing certificate is in a Personal store that is accessible by TIMS.

Exporting the Signing Certificate

a. Use the PFX to import the certificate into the Local Computer Personal certificate store on the Tachyon Server, ensure that the option to make the private key exportable is not set.

> ⚠ If you enrolled your own certificate, then exporting a PFX and then importing back into the Local Computer store allows everyone on the Server to access the certificate and use it to sign instructions in TIMS. By not allowing others to export the private key, you prevent them sharing it with others and you can decide who to give your PFX file to.
>
> If you were given a shared PFX and you are unable to import into the Local Computer store, then import to your Local User store. Each user that needs to use TIMS to sign instructions on the Server will also need to import the PFX into their own Local User store on the Server.

b. Start Certificate Manager and locate the certificate. Open the certificate and confirm you can see it "has a private key that corresponds to this certificate" (see screenshot below).

4. Copy the certificate to the Trusted Publishers store on the Tachyon Server

> This step is required to allow you to import instructions into Tachyon that have been signed using the certificate; if you prefer this step can wait until after the next step.

a. Copy the signing certificate from the Personal Store to the Trusted Publishers store
b. Reset IIS so that the Consumer API can cache the new certificate

5. Install TIMS onto the Tachyon Server

> This step confirms you can see the new signing certificate in TIMS. It also means that at least this certificate can be used to sign instructions using TIMS on the server. You may already have installed TIMS.

a. Logon to the Tachyon Server as the installer account
b. Install TIMS
c. Start TIMS using the installer account
d. Select the signing certificate (**Code Signing Select signing certificate**)
e. View the selected signing certificate (**Code Signing View selected signing certificate**)
f. Change to Always sign (**Code Signing Always sign**)
g. In the Instruction Definition pane, note the default name of the instruction. This will be **<YourDomainName>-NewInstruction-1**

6. Edit and Sign the HelloWorldTest instruction

> This step confirms you can create a sign an instruction in TIMS. Later, you will import this signed instruction into Tachyon.

a. Download or copy the test instruction XML to a folder on the Tachyon Server (this instruction is not already signed)
b. Start TIMS using the installer account

You can export the signing certificate with or without the private key. Exporting with a private key (as a PFX) is required only when sharing the certificate with other developers on their machines. You should save the export with a password, or ensure it is permissioned.

Your code signing certificate private key is a valuable secret. If an attacker were to get a copy of the certificate and its private key, they could sign their own instruction XML files. Of course, they would still need to compromise the Tachyon server in order to upload them, and the Tachyon Explorer in order to execute them, but nonetheless, you should treat code signing certificates as protected company assets.

The public key is required by the Tachyon Server. If the certificate is not already present in the Local Computer store, then you will need to export the public key (as a CER file) and import on the Tachyon Server.

1E requires only the thumbprint, or a CER file.

Download...

XXXX-HelloWorldTest.xml

```xml
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<InstructionDefinition
Author="1E"
```

c. Open the test instruction (File Open select **XXXX-HelloWorldTest.xml**)
d. Click Run, to show the Message Hello World in the Results pane
e. In the Instruction Definition pane, change the instruction name so that XXXX is changed to your chosen prefix
f. Save the updated test instruction (File Save As) and confirm the XML file name uses your chosen prefix
g. At the top of the instruction pane, confirm you can see the 'This instruction definition was signed by <your certificate>'

> ⓘ If you gave your signing certificate a friendly name, you will see that here, otherwise you will see the subject name of the certificate.

> ⚠ If you are testing multiple prefixes or signing certificates then you must make the instruction unique and recognisable, by changing the Instruction Name and ReadablePayload.

```
Name="XXXX-HelloWorldTest"
ReadablePayload="Get Hello World Test Message"
Description="Reply Hello World"
InstructionType="Question"
InstructionTtlMinutes="10"
ResponseTtlMinutes="10"
Version="1.0"
xmlns="http://schemas.1e.com/Tachyon
/InstructionDefinition/1.0">
  <Payload><![CDATA[SELECT "Hello World" AS
Message;]]></Payload>
  <SchemaJson><![CDATA[[
  {
    "Name": "Message",
    "Type": "string",
    "Length": 32
  }
]]]></SchemaJson>
</InstructionDefinition>
```

7. Import the HelloWorldTest instruction into Tachyon

> This step confirms you can import signed instructions. More specifically, that the Tachyon Server is able to see the certificate in the Trusted Publishers store (and the updated Consumer Web. Config file has taken effect).

a. Using the the installer account, start a browser, connect to Tachyon Explorer and navigate to the **Instruction Sets** admin page
b. Locate the XML file in the folder where you saved the instruction, and drag it onto the drop zone of the Instruction Sets admin page
c. Confirm the instruction uploaded without error
d. Confirm the instruction is not licensed

8. Get the Thumbprint of the code signing certificate and send the Thumbprint and Prefix details to 1E

> By this point we know the certificate can be used by TIMS, and will allow your own signed instructions to be imported into Tachyon; the remaining steps will update your license with your prefix and code signing thumbprint so that you can run your signed instructions. In the meantime you can carry on using TIMS to develop and test other instructions.

a. Get the thumbprint of your signing certificate
   i. Look at the properties of the code signing certificate, Details tab, and find the Thumbprint (see screenshot)
   ii. Copy this to notepad, remove the spaces and convert to UPPERCASE
b. Get your chosen prefix
c. Email them to SalesOps@1e.com
d. Currently the licensing process takes around 3 days. You will receive an email notification that your license has been updated

> ⚠ The application of the license will only work automatically if your Tachyon Server is

> connected to the Internet, so that it can re-activate its updated license directly with the 1E License server.

9. Confirm your Tachyon Server License has been updated

> This step confirms the server has had its license automatically updated.

    a. After you have received the license email notification
    b. Using the the installer account, start a browser, connect to Tachyon Explorer and navigate to the **License Info** admin page

> ⚠ The License Info page will auto-refresh every 10 minutes so you may have to wait for the information to update.

    c. Check that the new license has been applied, these instructions will work if you have only registered one Prefix with 1E:

        i. Under the **Products** heading expand **Item 2** the **Name** will be **TachyonExplorer**
        ii. Under **Item 2** expand **Instructions** then expand **Item 3**
        iii. Confirm that the Thumbprint and Pattern (Prefix) that you sent in the email to 1E have been added to the license

> ⓘ The License info page (and the LIC file it is based on) uses the term pattern to mean the same thing as prefix.

10. Confirm the HelloWorldTest instruction is licensed

> This step confirms you can run signed instructions. More specifically, that the Tachyon Server license has been updated to include the thumbprint of your signing certificate, and your chosen prefix.

    a. Using the the installer account, start a browser, connect to Tachyon Explorer and navigate to the **Instruction Sets** admin page
    b. Locate the instruction you imported earlier and confirm it is now licensed
    c. Optionally navigate to the Tachyon Explorer home page, and run the instruction. Type **Hello** and select the **Hello World** instruction; set coverage to a specific test machine

11. Delete the HelloWorldTest instruction

> This step avoids issues that may occur if you re-import the same instruction at a later date using the same ReadablePayload but a different prefix and signing certificate; if you did not delete then importing the same instruction with a different name will result in two instructions with the same ReadablePayload, rather than updating the instruction.

    a. Connect to Tachyon Explorer and navigate to the Instruction Sets admin page
    b. Delete the instruction you imported earlier