Tachyon client requirements

Summary

Information that will help you design and plan the implementation of **Tachyon** in your organization. This includes all the prerequisites and dependencies, which are necessary to install 1E Client with Tachyon client enabled.

For a full understanding of Tachyon features and their configuration please refer to Tachyon 5.2 documentation.

Tachyon client features are not required if the 1E Client is being installed only to support PXE Everywhere, Shopping, or WakeUp.

Tachyon client features are required if you are using any of the following:

- Tachyon Experience
- Tachyon Explorer
- Guaranteed State
- Patch Success
- Nomad - if using Nomad Content Distribution features of the Tachyon Platform. Also requires Nomad client to be enabled
- AppClarity - if using Tachyon as an inventory data source
- Application Migration - if using Tachyon as an inventory data source

On this page:

Public Key Infrastructure

Tachyon features require a PKI and certificates on client devices and servers. Please see below for client requirements, and Tachyon 5.2 - Requirements: Certificates for server requirements.

You need to have a PKI in your environment with at least one Issuing CA.

Tachyon requires each Issuing CA has:

- a **Certificate Revocation List** (CRL) **Distribution Point** (CDP) that uses HTTP/S
- this HTTP/S CDP information is included in certificates issued to Tachyon Server and client devices

PKI notes

If you have an existing PKI and have just added a new CDP to support HTTP/S then you will need to re-issue certificates to your servers and devices.

Tachyon deliberately does not work with self-signed certificates for security reasons. Therefore Tachyon client or Server cannot be installed on the same server as a Root CA, because its certificate is self-signed.

Tachyon uses TLSv1.2. If your PKI is using SHA512 then please ensure that your environment has relevant updates applied, as described in KB2973337. See Client issues: Enabling SHA-512 to work with TLSv1.2.

If you want Tachyon to manage legacy OS that Microsoft no longer supports there may be issues with encrypted certificates described in Requirements: Constraints of Legacy OS.

Client Certificates

If you have configured Tachyon Server to require client certificates (Tachyon Setup: Client certificates) then each device requires a certificate with the following properties so the Tachyon client be authenticated by the Tachyon Switch.

1. Issued by a trusted Certificate Authority (CA)
   - The certificate for the Root CA in the Certification Path must exist in the Trusted Root CA store of the client
   - If the issuing CA is not the Root CA then the certificate for the issuing CA and any intermediate CA in the Certification Path must exist in the Intermediate CA store of the client
   - If either of these CA certificates are different to those used by the Tachyon Web Server, they will need to be exported and imported on the Tachyon Web Server
   - Most organizations have automated distribution of these CA certificates to clients and servers, using Group Policy for example.
2. Has at least the following Enhanced Key Usage

        - Client Authentication
3. Has at least the following Key Usage
    - Digital Signature
    - Key encipherment
4. Has a private key
    - For workgroup and non-Windows devices, the **private key must be exportable**
5. Revocation information is included.
    - References at least one CRL Distribution point that uses HTTP.
6. Has a Subject Name of type Common Name (**CN=<computername>**) or Subject Alternative Name (**DNS Name=<computername>**) where <computername> depends on the type of device:
    - On domain-joined Windows PCs this must be the **computername FQDN** of the computer, for example **W701.ACME.LOCAL**
    - On workgroup Windows PCs and non-Windows devices, this must be the computername of the computer - as returned by the **hostname** command, for example on Windows PC this could be **W701**, and on a Mac this could be **MAC01.local**

> Tachyon clients and Switches use OpenSSL and its validation process to verify certificates.

The client device's certificate is stored differently depending on the type of OS.

- For Windows devices, the certificate is stored in the Windows Local Computer personal certificates store.
- For non-Windows devices, except for the Mac, the Tachyon client does not use proprietary certificate stores. Instead, the client requires the certificate exists as a **.pfx** file in the client installation folder structure:
    - Deploying 1E Client on Linux: Client certificates
- For macOS, you have a choice of storing the client certificate in the macOS Key Store or using the **.pfx** file approach required by other non-Windows devices.
    - Please refer to Deploying 1E Client on macOS: Client certificates

The following need to be considered when requesting this type of certificate.

- The certificate can be used only on the server it was intended, that has the correct computername FQDN and DNS Alias FQDN.
- It is not possible to use the **Create Certificate Request** method in IIS Manager Server Certificates, because it does not support all the above requirements.
- If you have a Microsoft CA, and a suitable **Web Server** template has been issued and enabled in the **Active Directory Enrollment Policy**, then it is possible to **Request New Certificate** in the **Certificates (Local Computer)** mmc snap-in and use the **Certificate Enrollment wizard**.
- Many organizations have their own process for submitting a Certificate Signing Request (CSR). Please ensure all the above requirements are specified. Security administrators sometimes have difficulty providing a certificate with one or more Subject Alternative Names (SAN), and it helps to explain these are type DNS.

Tachyon client integration with Nomad

Tachyon client integration with Nomad allows Tachyon clients to make use of Nomad features for more efficient downloading of content from different HTTP sources including the Tachyon Background Channel. Using this feature needs the following settings enabled, you can do this during the 1E Client installation:

- Nomad client module - enabled (off by default)
- Tachyon integration with Nomad - enabled (on by default)

With the Tachyon integration setting enabled, the Tachyon client will automatically detect if the Nomad client module is enabled and use it to download content from HTTP sources when requested.

Tachyon's use of Nomad works irrespective of whether Nomad is integrated with Microsoft Configuration Manager, or using 1E ActiveEfficiency or Content Distribution features.

The Nomad client included in 1E Client 5.2 and later requires Tachyon Platform with Content Distribution features enabled. Content Distribution is the replacement for ActiveEfficiency.

Configuration Manager is not a prerequisite for Tachyon integration with Nomad, but you will need to consider the following:

Configuration Manager client present	You do not need to make any configuration changes to Nomad for it to integrate with Tachyon, other than enable the Nomad client module in the 1E Client, or have a legacy version of the Nomad client installed. Please refer to Nomad 7.1 documentation for guidance on designing and deploying Nomad.
Configuration Manager client not present	You must ensure the following bits are enabled in the relevant Nomad installer properties and their corresponding registry values. These are enabled by default in the Nomad client module of the 1E Client, but if you modify the following properties for any other purposes then you must ensure these bits are set: • CompatibilityFlags bit 1 - enable long hashes • SpecialNetShare bit 13 - enable HTTP(S)

> If you have any configuration baselines or other policies that control Nomad settings then these will need to be reviewed. Review is especially important if you have upgraded from legacy Nomad Branch 6.x where these bits were disabled by default.

Tachyon scripting requirements

Tachyon real-time instructions are written in the Tachyon native language SCALE, which is very like SQL but with additional logic, functions and methods. Scripts can be downloaded when an instruction runs, or actual command text embedded in the instruction. You will very probably want to use scripts in the instructions you download from 1E or instructions you write yourself. Therefore, you must ensure the appropriate scripting environment is present on Agent devices.

Windows Tachyon clients can use PowerShell scripts. Ensure your Tachyon client devices have an appropriate version of PowerShell installed to support any custom scripts you may develop. See PowerShell on Windows OS.

Non-Windows Tachyon clients can use bash as their scripting medium. This should be present on all non-Windows Tachyon client devices.

For more information about SCALE and writing your own instructions, please refer to:

- Tachyon 5.2 - Installing TIMS
- Tachyon 5.2 - Setting up custom Tachyon Instructions for the first time
- Tachyon SDK - Writing Tachyon Instructions

PowerShell

PowerShell is used by some Tachyon instructions (that have PowerShell commands embedded or scripts that are downloaded) and some of these require PowerShell 3.0 or later, although some scripts will support PowerShell 2.0. PowerShell scripts are supported only on Windows OS.

If installing or upgrading PowerShell, it is best to install the latest version available. However, do not expect full forward or backward compatibility between PowerShell versions.

> To determine the version of PowerShell on a computer, start PowerShell (command prompt or ISE) and enter one of the following commands: **$PSVersionTable.PSVersion** or **$PSVersionTable** for more detail.

The table below shows which versions of PowerShell are supported on each OS version and Service Pack, and if it is built-in or needs to be installed.

OS Version	PowerShell Version						Notes
	1.0	2.0 (Note 3)	3.0	4.0	5.0	5.1	
Windows Server 2016, 2019					RTM (Note 9)	RTM (Notes 12, 13)	Note 4
Windows 10					RTM (built-in)	Anniversary Update (built-in)	
Windows Server 2012 R2				RTM (built-in)	RTM (Note 9)	RTM (Note 12)	Note 4
Windows 8.1				RTM (built-in)	RTM (Note 9)	RTM (Note 12)	
Windows Server 2012 *			RTM (built-in)	RTM (Note 7)	RTM (Note 9)	RTM (Note 12)	Note 4
Windows 8 *			RTM (built-in)				
Windows Server 2008 R2 *		RTM (built-in)	SP1 (Note 6)	SP1 (Note 7)	SP1 (Note 8)	SP1 (Note 10)	Note 4
Windows 7		RTM (built-in)	SP1 (Note 6)	SP1 (Note 7)	SP1 (Note 8)	SP1 (Note 10)	
Windows Server 2008 *	RTM (built-in)		SP1 & SP2 (Note 2)				
Windows Server 2003 *	RTM & SP1	R2 & SP2					Notes 1, 2
Windows Vista *	RTM	SP1 & SP2					Notes 1, 2
Windows XP *	RTM, SP1 & SP2	SP3					Notes 1, 2

* These OS are regarded as legacy OS:

1. PowerShell is not built-in for these OS. These OS do not support 3.0 or later. See 166988236
2. If PowerShell 1.0 is installed it must be removed in order to install a later version.
3. Support for PowerShell 2.0 is included in PowerShell 3.0 and later.
4. PowerShell is not installed by default on these OS but is an optional feature that should be enabled using Server Manager.
5. PowerShell 2.0 is part of WMF Core package (KB968930) with prerequisite of .NET Framework 3.51 (which includes .NET 2.0 SP1).
6. PowerShell 3.0 is part of WMF 3.0 with prerequisite of .NET Framework 4.0 or later. Refer https://www.microsoft.com/en-us/download/details.aspx?id=34595
7. PowerShell 4.0 is part of WMF 4.0 with prerequisite of .NET Framework 4.5 or later. Refer https://www.microsoft.com/en-us/download/details.aspx?id=40855
8. PowerShell 5.0 is part of WMF 5.0 with prerequisites of .NET Framework 4.5 or later and WMF 4.0. Refer https://www.microsoft.com/en-us/download/details.aspx?id=50395
9. PowerShell 5.0 is part of WMF 5.0 without any other prerequisites. Refer https://www.microsoft.com/en-us/download/details.aspx?id=50395
10. PowerShell 5.1 is part of WMF 5.1 with prerequisites of .NET Framework 4.6 or later, WMF 4.0 and SHA-2 Code Signing. Refer https://msdn.microsoft.com/en-us/powershell/wmf/5.1/install-configure
11. PowerShell 5.1 is part of WMF 5.1 with prerequisites of .NET Framework 4.6 or later and WMF 4.0. Refer https://msdn.microsoft.com/en-us/powershell/wmf/5.1/install-configure
12. PowerShell 5.1 is part of WMF 5.1 with prerequisite of .NET Framework 4.6 or later. Refer https://msdn.microsoft.com/en-us/powershell/wmf/5.1/install-configure
13. In these Server OS, PowerShell 5.1 is referred to as the Desktop Experience. You can use the PowerShell Core version if you prefer.

Microsoft ended support for .NET Framework 4, 4.5, and 4.5.1 on January 12, 2016. Please refer to https://support.microsoft.com/en-gb/help/17455/lifecycle-faq-net-framework.

Bash and Perl

Bash and perl are required for installation of all non-Windows 1E Clients, with the exception of the 1E Client for Android which is installed through the Google Play Store and configured using UI screens.

Tachyon instructions support the use of Bash scripts on all supported non-Windows OS.

To see if an Instruction requires a Bash script, look in its Instruction Definition XML file for the Scripting.Run method. Bash is the preferred choice when developing custom Instructions for non-Windows OS.

There are slight differences between OS implementations of Bash, particularly on the Mac. Therefore, 1E recommends testing custom Bash scripts on each supported OS.

Requirements for verifying the Tachyon installation

The Verifying page provides detailed steps for verifying a new or upgraded infrastructure, including firsts steps for uploading and running instructions. Below is a list of requirements to perform verification testing.

1. Tachyon Server installed
2. Remote workstation with a supported browser
3. The name and password for the **server installation account**
    a. the AD account must be enabled
    b. the account may already be assigned to other Tachyon roles either directly or via membership of an AD group role.
4. Two AD User accounts, **Test User 1** and **2**
    a. must not be existing Tachyon users because they will be assigned specific roles for the purpose of these tests
    b. must have email addresses and be able to read emails.
5. The **1E Tachyon Platform** instruction set with two Verification instructions
    a. the verification steps describe how to create this instruction set by uploading the 1E Tachyon Platform Product Pack
    b. you may have already uploaded this Product Pack using the Product Pack Deployment Tool, either during Setup or after
    c. the 1E Tachyon Platform Product Pack is included in the **TachyonPlatform zip** file that you can download from the 1E Support Portal (1eportal.force.com/s/tachyontopicdetail).
6. At least one test device on which the 1E Client will be installed
7. 1E Client installation source files and configuration details required by your Tachyon implementation.

Firewall ports

Please refer to Tachyon communication ports.