Design Considerations

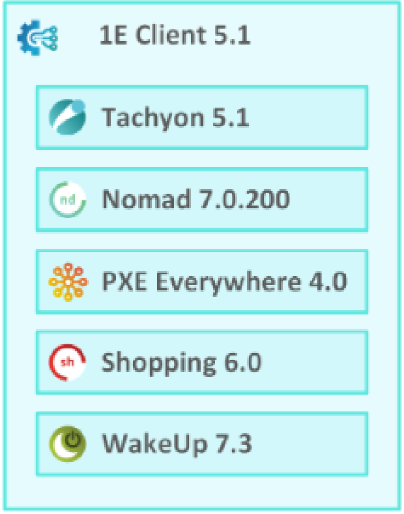
Summary

Information that will help you design and plan deployment of **1E Client** in your organization. Includes infrastructure dependencies for each 1E product supported by the 1E Client.

Please refer to the relevant 1E product documentation for more detail, links are provided below to relevant documentation spaces.

This page is part of the design phase of implementation.

1E Client is deployed as part of one or more 1E Solutions. You should review documentation for whichever 1E Solutions you are licensed to use, to help you decide which 1E Client features to configure, determined by which server systems are used.



1E Client deployment

You will need to plan the deployment of 1E Client using whichever software deployment tools you have. For more detail, please refer to:

- Deploying 1E Client on Windows which shows a manual interactive installation, with screenshots and descriptions of configurable settings
- 1E Client Deployment Assistant (CDA) which is used with Microsoft System Center Configuration Manager to deploy 1E Client, and also 1E NightWatchman Agent.

> CDA is the recommended method of deploying 1E Client on Windows if your organization uses Configuration Manager. It is a wizard that guides you through common settings for clients and deployments, and provides additional options that the installers do not. It creates the following:
>
> - a MST transform file for each MSI containing your chosen settings
> - optionally creates applications and packages in Configuration Manager - although this is optional you must have a connection to a Configuration Manager site
> - optionally creates deployments and collections for the applications
> - optionally distributes source files to Distribution Points
> - an answer file which records the chosen settings (the wizard uses a template answer file which controls the default settings seen in the wizard).
>
> 1E Client Deployment Assistant (CDA) is provided as a zip which you extract on a computer that has the Configuration Manager console installed. Windows ADK (with WinPE add-on) is also required locally if CDA is used to configure a deployment of PXE Everywhere.

> ⚠ You must use CDA if you are deploying 1E Client with PXE Everywhere and you want to deploy it with the boot image at the same time.

1E Client features and modules

You will need to decide which client features and modules to enable and configure. Unless otherwise stated, modules are only available on Windows computers. Please refer to Supported Platforms for details of supported OS platforms.

All modules including the Tachyon client feature can be optionally enabled during deployment of the 1E Client or after deployment by enabling features in its configuration file.

Feature /module	Description	Infrastructure dependencies
1E Client	This is the main service that determines which features and modules are enabled, including uninstallation of legacy versions of the 1E clients listed below. Please refer to 1E Client settings for details of configurable options.	
Tachyon client	1E Client feature which replaces Tachyon Agent to support Tachyon 4.1 and later but will work with earlier versions of Tachyon Server. Must be enabled on each end-user device to provide Real-time and Inventory features to support the following Tachyon applications: Explorer, Experience, Guaranteed State, Patch Success, Application Migration, and AppClarity. Also required to support Tachyon integration with NightWatchman and Nomad. Supports Windows and non-Windows devices. Please refer to Tachyon client settings for details of configurable options.	Full Tachyon infrastructure including Master and Response Stacks. See Tachyon infrastructure dependencies below.
Nomad client	1E Client module which replaces the NomadBranch client to support Nomad 7.0 and later, as well as Tachyon clients use of the Nomad content download feature. Must be enabled on each end-user device to provide bandwidth efficient download of content for Tachyon clients, as well as Configuration Manager clients. It is optionally used by PXE Everywhere. Please refer to Nomad client settings for details of configurable options.	ActiveEfficiency Server is required for several Nomad features, as described in Nomad infrastructure dependencies below.
PXE Everywhere Agent	1E Client module which replaces the PXE Everywhere Agent to support PXE Everywhere 4.0 and later. Enabled on as may end-user devices as possible to provide a lightweight PXE service that responds to PXE requests on their local subnet. Please refer to PXE Everywhere Agent settings for details of configurable options.	PXE Everywhere Central must be installed, as described in PXE Everywhere infrastructure dependencies below. You can also configure PXE Everywhere to support environments that use DHCP Snooping.
Shopping client	Must be enabled on each end-user device to support access to the Shopping web portal, and WSA features to support OS rebuilds and upgrades. Please refer to Shopping client settings for details of configurable options.	Shopping Central website and Shopping Receiver services are required, as described in Shopping infrastructure dependencies below.
WakeUp client	1E Client module which replaces WakeUp Agent to support WakeUp Server 7.2.500 and later. This version contains hotfixes. Must be enabled on each end-user device to support Wake-on-LAN and Configuration Manager policy refresh. Also integrates with the 1E NightWatchman Agent. Please refer to WakeUp client settings for details of configurable options.	WakeUp Servers are required, as described in Night Watchman and WakeUp infrastructure dependencies below.

Upgrading the 1E Client

Upgrading from 1E Client 4.1 or 1E Client 5.0 to 1E Client 5.1 simply requires deploying the new version, using the same or different configuration settings.

If you are upgrading from Tachyon Agent, Shopping Agent, NomadBranch and/or 1E Agent (for NightWatchman and WakeUp) then please refer to Upgrading to 1E Client.

Supported Platforms

All 1E Client features are supported on the following Windows OS:

Windows

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows 10 CB 21H2
- Windows 11 CB 21H2
- Windows 10 CB 21H1
- Windows 10 CB 20H2
- Windows 10 CB 2004
- Windows 10 CB 1909
- Windows 10 CB 1903
- Windows 8.1

The zip for 1E Client for Windows is available for download from the 1E Support Portal .

Professional and Enterprise editions of Windows 10 are supported.

All versions are provided with 32-bit & 64-installers, and can be installed on physical and virtual computers.

This list is automatically updated to show only those OS versions in mainstream support by Microsoft, and therefore supported by 1E, and by 1E Client 5.1. However the following OS continue to be supported as exceptions to help customers during their migration to the latest OS:

- Windows Server 2012 R2
- Windows 7 SP1

Please refer to Constraints of Legacy OS regarding end of mainstream support.

For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search.

Please refer to https://1eportal.force.com/s/support-for-msft-rapid-release-cycle for details of which Current Branch versions are supported by 1E products, and known issues regarding specific versions.

The Tachyon client features of 1E Client are supported on the following non-Windows OS:

macOS

- macOS Catalina 10.15
- macOS Mojave 10.14
- macOS High Sierra 10.13

Linux

- CentOS 8.1
- Debian 10.4
- Fedora 32
- openSUSE Leap 15.1
- Red Hat Enterprise Linux 7.1
- Red Hat Enterprise Linux 8.1
- SUSE Linux Enterprise 15.1
- Ubuntu 18.04

Solaris

- Solaris 11.4
- Solaris 11.3

1E Client supports only Tachyon features on non-Windows devices.

Other versions of these non-Windows OS should work but have not been tested by 1E.

The 1E Client for non-Windows zip is available for download from the 1E Support Portal, and includes 1E Client packages for the following architectures:

- Linux variations on Intel 64-bit platforms
- Solaris on Intel 64-bit and SPARC platforms

Also included in the download are 1E Client packages for the following legacy Linux distributions:

- Fedora 21
- openSUSE Leap 42.1

1E Client packages for other Linux distributions can be requested, including Raspbian for Raspberry Pi.

Tachyon infrastructure dependencies

Please refer to Tachyon 5.1 documentation for more details.

If you intend using Tachyon for its Real-time, Inventory, Patch Success, or Guaranteed State features, then you require at least one Tachyon Server and a Tachyon license.

Organizations with less than 50000 devices will typically have a single-server system with one Tachyon Switch, but there may be reasons why a more complex configuration would be required. Key factors are the location of servers and how devices and users will connect to them.

Every Tachyon system has a single **Master Stack**, which provides web services for Tachyon applications. Master Stack components are typically all installed on a single **Master Server**.

Tachyon real-time features require **Response Stacks**, which are made up of one or more **Response Servers**. A **DMZ Server** is an example of a Response Server. Each Response Stack has at least one **Background Channel** for sharing resources, and a single **Core** component that supports an associated set of up to five **Switches**. Switches are the primary mechanism for rapidly requesting and retrieving responses from the **Tachyon clients**. As each Switch can handle up to 50,000 devices there is a limit of 250,000 devices per Response Stack. Switches may be local or remote to the other components in the Response Stack.

Databases for Tachyon, Catalog, Experience, SLA and BI, are installed on SQL Server database instance(s) that may also be local or remote to their respective Master and Response servers. It is also possible for multiple Response Stacks to share the same Responses database. **Cubes** used by Experience and BI are installed on a local or remote SQL Server Analysis Services (SSAS) instance.

PKI and certificates

Client-Switch communication uses **WebSocket Secure** protocol, whereby each Tachyon client establishes a secure link to the Switch which is then used by the Switch to send instructions to the Tachyon client. This is shown as a dotted line in the pictures in the Communication Ports page.

All other communications from external devices use **HTTPS**, including Tachyon client connecting to the Background Channel in order to download resources that may be required by instructions, and using the Tachyon Portal to administer and use the system.

All communication is encrypted, which requires a **Public Key Infrastructure** (PKI). More specifically, PKI is required for:

- **Tachyon web server certificate** - prerequisite for each Tachyon Server website, must contain all the DNS Names used for the server
- **Tachyon Server certificate** - usually an exported version of the website certificate
- **Tachyon client certificates** - each Tachyon client uses the device's client certificate to authenticate itself to Tachyon Switches
- **Certificate Revocation Lists (CRLs)** - Tachyon clients and Switches use HTTP-based CRL Distribution Points to validate certificates
- **Code signing certificates** - used for signing custom and modified instructions, so they can be imported into Tachyon and then run
- **Digital signing certificates** - used for signing 1E software

✓ You can use Tachyon Setup to install Tachyon Server so it does not require Tachyon clients to present certificates to the Tachyon Switch. The Platform can be reconfigured later to re-enable use of client certificates when your environment is ready. The Tachyon Server requires a Web Server certificate. If this is an issue for you then please contact 1E.

Miscellaneous

In addition to PKI and network requirements, other infrastructure dependencies are:

- **DNS** - each Tachyon Server requires a DNS Name, this is also useful for ActiveEfficiency Server if it is installed
- **Active Directory** - for installation and user accounts and groups; Tachyon supports multi-domain, multi-forest environments that have two-way trusts
- **IIS** - a standard configuration required on each Tachyon Server
- **SQL Server** - for Tachyon Master and Response Stack databases, Catalog SLA and BI databases, and ActiveEfficiency if installed
- **SQL Analysis Services** - must be installed in multi-dimensional mode, for Business Intelligence (SLA BI cube) required by Patch Success
- **Email** - optional for approval and notification emails, but required if using two-factor authentication (2FA)
- **Internet access** - the Master Stack requires access to the 1E license service via the Internet in order to keep the Tachyon license activated, and 1E Catalog requires access to the 1E Catalog Cloud service to download Catalog updates

For more detail about client certificates, please refer to Tachyon client requirements: Client Certificates.

Downloading Tachyon client content and Nomad integration

Tachyon client downloads content from the Tachyon Background Channel. Content is mainly scripts and other files required by Tachyon instructions. It also includes client resources such as extensible modules, providers, and other dependencies to maintain the 1E Client. In most cases, client resources are version controlled to prevent repeated downloads. Tachyon instructions always request a download even if they have run an instruction before, unless the content for that instruction has been cached in memory.

You may need to consider the impact on the network if there is a large amount of content included in an instruction. This is more of an operational consideration instead of a design consideration.

1E Nomad is an optionally licensed component of the 1E Client. It makes software deployment, patching and downloading content more efficient and reduces the impact on the network. It removes the need for remote Distribution Point servers in Microsoft System Center Configuration Manager systems. When Nomad is installed on computers it automatically elects a peer to download content from a server over the WAN and then peer-shares the content with other PCs at the same location. The downloaded content is cached locally on each PC in case it is needed again.

Tachyon can optionally use Nomad to download content from servers irrespective of whether Nomad is integrated with Configuration Manager or not, and also uses advanced Nomad features which use ActiveEfficiency.

Nomad integration disabled

If Nomad integration is not used, the following apply:

- Tachyon client waits a randomized stagger period defined by its DefaultStaggerRangeSeconds setting, and then downloads content from the specified **Background Channel**.
- Tachyon client retains modules and extensibles that it has downloaded, but does not retain instruction scripts after they have been run. Any instruction that requires a script or other file will download the latest version each time the instruction is run.

Nomad integration enabled

Nomad integration is available on Windows PC devices and is enabled by default, but can be disabled during installation of the 1E Client.

With the Nomad integration feature enabled, Tachyon client will detect if a supported version of Nomad is running on the device.

- Tachyon client immediately requests Nomad to download content from the specified HTTP source such as the **Background Channel**. Nomad behaves in the same way as it does with Configuration Manager by ensuring the latest version of content is obtained and electing a master to perform the actual download.
- Nomad maintains its own cache of downloaded content which avoids the need for repeat downloads over the WAN, and provides content to peers that require the same resources which avoids peer devices having to download over the WAN.
- If the Nomad integration feature is enabled, and requested content is not provided within the timeout period, the Tachyon client will fall back to downloading directly from the HTTP source. The most likely reason for a timeout is if Nomad is busy downloading other content.

To use Nomad, there is no special configuration of Tachyon Servers. The Background Channel is a web application on the Tachyon Server which uses HTTPS and default port is 443. The URL for the Background Channel is defined in the 1E Client configuration file and is specified during installation of the 1E Client if Tachyon features are enabled. The Tachyon client passes this URL to Nomad when it requests content to be downloaded. Instructions can also specify other HTTP sources.

Nomad does not need to be configured to use certificates in order to communicate with the Background Channel (the Nomad CertIssuer and CertSubject settings are used only with Configuration Manager Distribution Points that are configured to validate device certificates).

Nomad Single-Site Download (SSD) feature uses ActiveEfficiency Server to further reduce the impact downloading content over the WAN.

Nomad infrastructure dependencies

Please refer to Nomad 7.0.200 documentation for more details.

In addition to deploying 1E Client (with Nomad client module enabled) on all computers and on Configuration Manager Distribution Points, the following are also required:

- Nomad tools installed on Configuration Manager sites and SMS Providers
- Nomad Configuration Manager Console extensions on Configuration Manager site servers any other computer that has the Configuration Manager Console installed

As explained above, Nomad can be used for downloading content for Tachyon clients, as well as Configuration Manager clients.

Although not a requirement for generally using Nomad, ActiveEfficiency Server must be installed and available before you can use certain Nomad features.

The following Nomad features require ActiveEfficiency:

- Single-site download (SSD)
- Single-site Peer Backup Assistant (SSPBA)
- High Availability Peer Backup Assistant (HAPBA)
- Get migration settings task sequence action used to manage computer associations
- Nomad Pre-caching
- Nomad Dashboard
- WakeUp integration (also requires NightWatchman Management Center server, WakeUp Servers installed on Configuration Manager sites, and Single-site download)
- Nomad Download Pause (also requires Tachyon infrastructure)

Hotfix requirement

If you will be using any of these features with Nomad 7.0 you must install ActiveEfficiency 1.10 with the latest accumulated hotfix available on the 1E Support Portal (https://1eportal.force.com/s/article/LatestHotfixes).

PXE Everywhere infrastructure dependencies

PXE Everywhere helps with OS Deployment. The PXE Everywhere Agent is a lightweight PXE service deployed throughout the network, responding to PXE requests on local subnets. Local Agents elect which one will respond to the original PXE request, and communicate with PXE Everywhere Central to determine what to do next, by asking Configuration Manager. If the original PXE client has been assigned a Task Sequence, then the Agent provides the associated boot image to the local PXE client, which can then start the Task Sequence. Boot images will have been previously deployed to Agents, providing the reassurance there will always be a local Agent capable of quickly responding with the relevant boot image. It also means you can deploy a PXE solution without needing to configure routers to support DHCP forwarding to a central PXE server. Please refer to PXE Everywhere 4.0 documentation for more details.

PXE Everywhere does not depend on Nomad but is often used with Nomad, which helps with distribution of PXE boot images via Configuration Manager, which further reduces the impact of network traffic on the WAN.

1E Client Deployment Assistant (CDA) is the recommended method of using Configuration Manager to deploy 1E Client to client computers. CDA is necessary if you want to include a boot image in the same deployment as the 1E Client.

PXE Everywhere also works in environments that use DHCP Snooping, as described in PXE Everywhere 4.0 - Design Considerations: DHCP Snooping. This requires the following configuration changes:

- install of one or more PXE Everywhere Responders, typically on server OS in the central network - Responders only communicate with Agents, they do not communicate with the PXE Everywhere Central server or with Configuration Manager
- authorize the Responders to respond to PXE requests
- configure DHCP Relays (IP helpers) on routers to forward DHCP/PXE request packets to the PXE Everywhere Responder(s) in addition to any DHCP Relays you already have configured for the DHCP server(s)
- configure PXE Everywhere Agents to listen on port 2067 (default) instead of port 67.

Shopping infrastructure dependencies

Please refer to Shopping 6.0 documentation for more details.

Shopping requires an ActiveEfficiency Server, and ActiveEfficiency Scout to import data from Configuration Manager into ActiveEfficiency.

A Shopping solution requires a Shopping Central server on a web server, and a Shopping Receiver installed on each Configuration Manager Site server that has client reporting to it, and on a CAS if using Shopping for OS Deployment.

If users are using Edge or Metro browsers then you must enable the loopback feature. This feature implements a mechanism for passing information between the Shopping client, the browser's secure sandboxed environment and the local machine. This mechanism affects these browsers as a whole and is not just restricted for use by Shopping.

> ⚠ Before enabling the loopback feature, check your security policy on enabling loopback and be aware of the implications of allowing access between browsers and the local machine.

NightWatchman and WakeUp infrastructure dependencies

Please refer to NightWatchman Enterprise 7.3 documentation for more details.

A NightWatchman Management Center server is required if implementing NightWatchman or WakeUp solutions.

If implementing WakeUp, or Nomad integration with WakeUp, then you require at least one WakeUp Server. If you have Configuration Manager you require a WakeUp Server on each Site server that has clients reporting into it. If you do not have Configuration Manager you require one or more independent WakeUp Servers.

1E NightWatchman Agent is a separately installed client agent, that can optionally be used to help with power management of computers. It is not included in 1E Client, but is included in the 1E Client Deployment Assistant (CDA) which assists with deploying Windows versions of 1E clients via Configuration Manager. When 1E NightWatchman Agent is installed alongside the WakeUp client it will optionally manage the computer returning to its original power state after being woken using 1E WakeUp and the computer is not busy, for example installing patches.

Web WakeUp is an optional server component that is typically installed on the NightWatchman Management Center server. It is a web portal for users and administrators to search for computers to wake. It optionally provides a remote desktop link to the woken computer.

Constraints of Legacy OS

In this documentation, the following are referred to as legacy OS. Below are described some known issues for these OS.

1E does not provide support for 1E products on the following OS unless the OS is explicitly listed as being supported for a specific 1E product or product feature. This is because Microsoft has ended mainstream support for these OS or they are not significantly used by business organizations.

• **Windows XP** • **Windows Vista** • **Windows 7** • **Windows 8.0**	• **Windows Server 2003** • **Windows Server 2008** • **Windows Server 2008 R2** • **Windows Server 2012** • **Windows Server 2012 R2**

Please contact 1E if you require support for these legacy OS. If you experience an issue on these OS, then please try replicating the issue on a supported OS.

For Microsoft product lifecycle details, please refer to https://support.microsoft.com/en-us/lifecycle/search.

PowerShell limitations

PowerShell version 3.0 (required by some Tachyon instructions) is not supported on Windows XP, Vista and Server 2003. However, PowerShell 2.0 is supported on the following OS versions:

- Windows XP SP3
- Vista SP1 & SP2
- Windows Server 2003 R2 & SP2

Certificate limitations - SHA2

Like most software vendors, 1E software requires the OS to support SHA2. If your organization has a PKI configured to use SHA2 256 or higher encryption, then your legacy OS may have already been updated to support it.

Windows XP and Server 2003 require an update as described in **KB968730.** Microsoft no longer provides this hotfix as a download. You must contact Microsoft Support if you need it.

Windows 7 and Server 2008 R2 require an update as described in **KB3033929**. This update is not available for Vista and Server 2008.

Windows 8, 8.1, Server 2012, Server 2012 R2 and later OS already support SHA2.

Certificate limitations - encrypted certificate requests

Windows XP and Server 2003 are unable to encrypt certificate requests, whereas later OS are able to support higher more secure RPC authentication levels. If you are using a Microsoft CA and expect these clients to request (enrol) certificates then the CA must have its IF_ENFORCEENCRYPTICERTREQUEST flag disabled. It is disabled by default on Windows 2003 and 2008 CA, but is enabled by default on Windows 2012 CA.

To determine which InterfaceFlags are set, execute the following command on the CA server:

```
certutil -getreg CA\InterfaceFlags
```

If the following is specified then it means the flag is enabled.

```
IF_ENFORCEENCRYPTICERTREQUEST -- 200 (512)
```

To disable the encrypt certificate requests flag, execute the following commands on the CA server:

```
certutil -setreg CA\InterfaceFlags -IF_ENFORCEENCRYPTICERTREQUEST
sc stop certsvc
sc start certsvc
```

Certificate limitations - signing certificates missing

On Windows computers, the installation MSI files, and binary executable and DLL files of 1E software are digitally signed. The 1E code signing certificate uses a timestamping certificate as its countersignature. 1E occasionally changes its code signing certificate, and uses it for new releases and patches for older versions, as shown in the table(s) below.

Root Certificate Authorities are implicitly trusted to validate certificates, and their certificates must be correctly installed to do this. Your computers should already have the necessary **root CA** certificates installed, however this may have been prevented by your organization's security policies, or inability to connect to the Internet, or they are legacy OS. In general this is not an issue because by default Windows allows software to be installed and run without validation, although you may see a warning or experience a delay. However, you *must* have relevant CA certificates installed if you are using 1E Client (which self-validates its own files), or your organization has applied more secure polices (for example UAC, AppLocker or SmartScreen).

Typical reasons for issues with signing certificate are:

- If your organization has disabled **Automatic Root Certificates Update** then you must ensure the relevant **root CA** certificates are correctly installed on each computer
- If computers do not have access to the Internet then you must ensure the relevant **root and issuing CA** certificates are correctly installed on each computer, numbered in the table(s) below.

The signature algorithm of the 1E code signing certificate is SHA256RSA. In most cases the file digest algorithm of an authenticode signature is SHA256, and the countersignature is a RFC3161 compliant timestamp. The exception is on legacy OS (Windows XP, Vista, Server 2003 and Server 2008) which require the file digest algorithm of an authenticode signature to be SHA1, and a legacy countersignature.

The table below applies to software and hotfixes released in 2020.

2020	Signing certificate	Timestamping certificates
Certificate	1E Limited	TIMESTAMP-SHA256-2019-10-15 ***and*** DigiCert Timestamp Responder
Issuing CA	**DigiCert EV Code Signing CA (SHA2)** Thumbprint: 60ee3fc53d4bdfd1697ae5beae1cab1c0f3ad4e3	**DigiCert SHA2 Assured ID Timestamping CA** Thumbprint: 3ba63a6e4841355772debef9cdcf4d5af353a297 ***and*** **DigiCert Assured ID CA-1** Thumbprint: 19a09b5a36f4dd99727df783c17a51231a56c117
Root CA	**DigiCert High Assurance EV Root CA** Thumbprint: 5fb7ee0633e259dbad0c4c9ae6d38f1a61c7dc25	**DigiCert Assured ID Root CA** Thumbprint: 0563b8630d62d75abbc8ab1e4bdfb5a899b24d43

This is described in Common client requirements: Digital signing certificates. To verify if you affected by this issue see Client issues: 1E Digital Signing Certificates.

Certificate limitations - expired root certificates

Ensure that your Root CA Certificates are up-to-date on clients and servers. The **Automatic Root Certificates Update** feature is enabled by default on these legacy OS but its configuration may have been changed or restricted by Group Policy **Turn off Automatic Root Certificates Update**.

If this GPO is enabled then you will see `DisableRootAutoUpdate = 1 (dword)` in `HKLM\Software\Policies\Microsoft\SystemCertificates\AuthRoot.`