Deploying 1E Client on Linux

Summary

Guidance for deploying the 1E Client onto Red Hat Enterprise Linux devices, including installation and uninstallation. Only the Tachyon features of 1E Client are available on Linux and other non-Windows OS.

On this page:

Requirements

Please review Design Considerations and Requirements pages. After installation please review the Verifying page.

For details of supported OS platforms please refer to Supported Platforms reference page.

Guidance provided below is for installation on Red Hat Enterprise.

Please contact 1E if guidance is required for installation on other non-Windows OS and for Android.

1E Client does not have a license key. Even so, you must adhere to the terms of your license agreement.

Deployment choices

You must decide how you will configure the 1E Client and deploy to devices. For more information about configuring the 1E Client properties during and after installation, please refer to 1E Client configuration settings and installer properties.

Deploying the 1E Client is normally achieved using your existing software deployment tool.

Non-Windows installation account

To install the 1E Client on a non-Windows client the installation account must have privileges to run the **sudo** command.

Certificate files

Each Tachyon client device requires a **.pfx** certificate file. Please refer to Client certificates below, for steps to create and use the **.pfx** file.

For Linux devices, 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.

If you have configured Tachyon Server to require client certificates, then each device requires a certificate with the following properties so the Tachyon client can be authenticated by the Tachyon Switch.

Client certificates must meet the following requirements:

- 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.
- Has at least the following Enhanced Key Usage
  - Client Authentication
- Revocation information is included.
  - References at least one CRL Distribution point that uses HTTP.

- Has a Subject Name of type Common Name (**CN=<hostname>**) or Subject Alternative Name (**DNS Name=<hostname>**) where <hostname> depends on the type of device:
  - On domain-joined Windows PCs this must be the **hostname FQDN** of the computer, for example **W701.ACME.LOCAL**
  - On workgroup Windows PCs and non-Windows devices, this must be the hostname 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**
- Has a private key
  - For workgroup Windows and non-Windows devices, this must be exportable

Preparation

The Windows and non-Windows versions of the 1E Client are available for download from the 1E Support Portal.

Installation source files for 1E Client for non-Windows are available in a zip file called **1EClient-Non-Windows.v5.0.x.x.zip**

Within the zip, the Linux 1E Client is provided as the following **.rpm** files:

- 1e.client-CentOS_7_x64_v5.0.0.xxx.rpm
- 1e.client-Fedora_21_x64_v5.0.0.xxx.rpm
- 1e.client-openSUSE_42.1_x64_v5.0.0.xxx.rpm
- 1e.client-RHEL_6.2_x64_v5.0.0.xxx.rpm
- 1e.client-RHEL_6.2_x86_v5.0.0.xxx.rpm
- 1e.client-RHEL_7.1_x64_v5.0.0.xxx.rpm
- 1e.client-RHEL_8.1_x64_v5.0.0.xxx.rpm
- 1e.client-SLES_12.2_x64_v5.0.0.xxx.rpm

Installation

The basic command to install an RPM package is **rpm -i <package_file>**. Although RPM, by design, does not support configuration during installation (with the Linux recommended approach being to configure after installation) - the 1E Client does in fact support configuration through the use of environment variables. These can be easily set in a bash command line by one or more space-separated name=value pairs preceding the install command. So, if the RPM package file name is **1e.client-RHEL_7.1_x64_v5.0.0.745.rpm** and the Tachyon Server (assuming that the switch and the background channel are both installed on the Tachyon Server) has the DNS Name FQDN tachyon.acme.local then the command to run would be:

```
sudo SWITCH=tachyon.acme.local:4000 BACKGROUNDCHANNELURL=https://tachyon.acme.local:443/Background/ rpm -i
1e.client-RHEL_7.1_x64_v5.0.0.745.rpm
```

Please refer to 1E Client configuration settings and installer properties for a list of other configuration properties that can be configured in the same way.

The correct case for each property must be used when entering the Linux installer command.

When the package starts to install you may notice that the **ldconfig** command generates a warning saying that a **.py file is not an ELF file - it has the wrong magic bytes at the start**.

This is because **ldconfig** assumes all files in **/usr/lib** are ELF files, and that file is a python file.

You can safely ignore this warning.

After the package is installed the application configuration files will be installed to the following directory:

```
/etc/1E/Client
```

After running the Linux RPM package the client is installed and started as a daemon (service).

The client certificate **Tachyon.pfx** and a **cacert.pem** file are required in the hidden directory: */etc/1E/Client/.sslcerts*

If **Tachyon.pfx** contains the same certificate trust chain as the Tachyon Switch, then **cacert.pem** is optional. This is because the client will have already cached the public certificates when it parses **Tachyon.pfx** and **cacert.pem** will be duplicating the public certificate information. If **Tachyon.pfx** is using a different certificate trust chain from the Tachyon Switch, then **cacert.pem** is always required.

Reconfiguration

Please refer to 1E Client command-line parameters if you would like to see details of other CLI commands.

This method is suitable for reconfiguring all 1E Client settings on non-Windows devices because only Tachyon client features are available and all settings are stored in the 1E Client configuration file.

Example:

```
/usr/sbin/1E.Client -reconfigure Switch=ACME-DMZ01.ACME.LOCAL:4000 BackgroundChannelUrl=https://ACME-DMZ01.
ACME.LOCAL:443/Background/ -restart
```

Client certificates

Each client device requires its own certificate, which must be created as a **.pfx** file.

Using OpenSSL to create the .pfx file

Each non-Windows devices requires its own certificate. Below is a guide for using a Microsoft CA to issue a certificate (which is the same for Windows computers), then exporting it and using OpenSSL to prepare it before installing it on the non-Windows device.

First, you will need to have created a new Certificate template on your Certificate Authority by making a duplicate of either the Computer or Workstation template and configuring it with at least the following properties:

- **General** - use a suitable name such as **Tachyon Devices** and validity period
- **Request Handling** - Allow private keys to be exported
- **Subject Name** - Allow information to be supplied in the certificate request, rather than being built from Active Directory information
- **Extensions** - Application Policies should contain only Client Authentication
- **Security** - ensure relevant users and computers will be able to request certificates.

Once the new template is created on the CA, issue it.

Using the issued template, request a certificate for a target device, and export it in **.pfx** form and remember the password.

The target device requires a copy of the basic **cacert.pem** and the **.pfx** file with its password removed. You can do this using the following steps. Use the relevant OpenSSL version for the OS. OpenSSL is normally available by default on Linux and Mac devices. If you want to follow these steps on Windows you will need to download the open source version appropriate to your OS.

1. First, extract the certificate:

   ```
   openssl pkcs12 -clcerts -nokeys -in <YourPKCSFile>.pfx -out certificate.crt
   ```

2. Second, the CA key:

   ```
   openssl pkcs12 -cacerts -nokeys -in <YourPKCSFile>.pfx -out ca-cert.ca
   ```

3. Now, the private key:

   ```
   openssl pkcs12 -nocerts -in <YourPKCSFile>.pfx -out private.key -passout pass:TemporaryPassword
   ```

4. Remove the passphrase:

   ```
   openssl rsa -in private.key -out new.key -passin pass:TemporaryPassword
   ```

5. Put things together for the new PKCS-File (on Windows, **type** can be used instead of **cat**):

   ```
   cat new.key > PEM.pem
   cat certificate.crt >> PEM.pem
   cat ca-cert.ca >> PEM.pem
   ```

6. And create the new **.pfx** file, when prompted for a password ensure that you enter an empty password (that is press enter when prompted for the password and confirmation without entering any text):

   ```
   openssl pkcs12 -export -nodes -CAfile ca-cert.ca -in PEM.pem -out Tachyon.pfx
   ```

Now you have a new PKCS12 key file without passphrase on the private key part. This **Tachyon.pfx** file and the **cacert.pem** file, must be placed in one of the following locations - depending on the OS. These are hidden folders.

Storing the .pfx on the client

The client certificate file (**Tachyon.pfx**), and Certificate Authority (CA) certificate(s) for the Switch certificate (**cacert.pem** file) are stored in the hidden directory: **/Library/Application Support/1E/Client/.sslcerts**

If the client certificate (**Tachyon.pfx**) uses the same certificate trust chain as the Tachyon Switch, then **cacert.pem** is optional. This is because the client will have already cached the public certificates when it parses **Tachyon.pfx**.

If the client certificate (**Tachyon.pfx**) uses a different certificate trust chain from the Tachyon Switch, then **cacert.pem** is always required.

Uninstallation

The following command-line can be used to uninstall the 1E Client on Linux:

```
sudo rpm -e 1e.client
```

Uninstallation will leave behind files, folders and registry entries that were created after installation:

Location	Artifacts	Recommendation
Installation folder	None.	
Logs folder	Log files remain.	The log files can be deleted or renamed. If not deleted, then a new installation that uses the same logs folder will continue to use the old log file.
	Client\Persist folder remains.	You should keep the **Persist** folder, which contains status information about current instructions, only if you intend to re-install the 1E Client.