Tachyon Server post-installation tasks

Summary

Post-installation tasks, which include verification checks and mandatory and optional configuration tasks.

Required tasks

The following tasks must be performed post-installation. You may have already performed some of these tasks as part of following the instructions on the Quick Start.

The Tachyon Portal website will be available after installation via the Tachyon DNS Alias FQDN. For example:

> https://tachyon.acme.local/Tachyon

Verify installation

> ⚠️ You must perform the verification tests provided on the Verifying page. Those tests reference each of the required tasks below.

Confirming the Tachyon website HTTPS binding

If you have implemented Tachyon Server on an IIS server that has previously been or is currently used by other applications then there may be other Web Server certificates in the **Local Computer's Personal Certificates store** in addition to the Tachyon Web Server certificate. In earlier versions of Tachyon it was possible under these circumstances for the Tachyon Server installer to bind to the wrong certificate. The current version contains improved logic for avoiding this problem, but it is still good practice to verify that the configuration is indeed as expected.

To select the correct certificate for the HTTPS binding see the troubleshooting steps for Server installation issues.

Configure permissions

Immediately after installation you can only access the **Tachyon Portal** and the **Settings** application using the installation account, until additional users have been added and assigned to their roles.

The installation account is assigned the following roles and cannot be modified because it is a System Principal.

- Permissions Administrators
- Instruction Set Administrators
- Consumer Administrators
- Applications Administrators

This means that one of your first steps after installation is to connect to the Portal using the installation account and add other Tachyon users with necessary roles as described in the Users page and the Roles page.

> ⚠️ After the initial configuration of Tachyon users and groups has been performed we recommend that the above roles are applied to one or more other Tachyon users and that the installation account is disabled in Active Directory. It can be enabled later for installation of updates and upgrades.
>
> This approach of having a dedicated installation account ensures the same account is used for all installation activities and has relevant rights on the Tachyon server and in SQL Server. Disabling it makes it more secure than a normal user account. If an ordinary user account is used for installation tasks there is a risk the account may be deleted, causing difficulties for future upgrades or re-installations.

Add Product Packs and configure Instruction Sets

Tachyon functionality is based around Instructions, until these are added to the system you will not be able to ask questions or perform actions. 1E provides instructions in zip files called Product Packs. A collection of Product Packs necessary for for zip files available in the **Tachyon Platform** zip (available on the 1E Support Portal) and from the Tachyon Exchange (tachyonexchange.1e.com). Each Product Pack contains a related collection of Instruction Definitions. Product Packs and Instruction Definitions can be added to Tachyon by **Instruction Set Administrators**.

When added into Tachyon, Instructions are immediately allocated to the built-in **Unassigned** Instruction set. Instruction sets provide a way of determining the permissions for the Instructions they contain, but the **Unassigned** Instruction set is only intended as a staging area for newly loaded Instructions - and Instructions in this set cannot be used directly. An Instruction can only belong to a single Instruction set, so after loading it into Tachyon, and before it can be used, it must be moved to another Instruction set - one created by an **Instruction Set Administrator**.

Instruction sets created by **Instruction Set Administrators** can be used as the basis for custom roles created by **Permissions Administrators**. These custom roles determine the permissions for the Instruction sets and all the Instructions they contain. This enables the **Permissions Administrators** to complete the assignment of specific Instruction set roles to users and determine which Instructions they can action, approve, question or view.

You can either load instructions into Tachyon and create Instruction Sets for them automatically from Tachyon Setup, please refer to Quick Start: Uploading Product Packs using the Tachyon Product Pack deployment tool for more details, or you can load the product packs and create their associated instruction sets by hand.

ⓘ   The **ProductPacks** folder in the Tachyon Platform zip file contains a number of **Classic** and **Integrated** product pack zip files:

- 1E ConfigMgrConsoleExtensions Product Pack — Classic Product Pack used to create the 1E ConfigMgrConsoleExtensions instruction set required by the Tachyon Configuration Manager console extensions.
- 1E Explorer TachyonAgent Product Pack — Classic Product Pack used to create the 1E Explorer TachyonAgent instruction set that can be used to configure and query Tachyon clients.
- 1E Explorer TachyonCore Product Pack — Classic Product Pack used to create the 1E Explorer TachyonCore instruction set that includes instructions for Tagging and Quarantine.
- 1E Inventory Product Pack — Classic Product Pack used to create the 1E Inventory instruction set required by the Tachyon Powered Inventory feature.
- 1E Patch Success Product Pack — Classic Product Pack used to create the 1E Patch Success instruction set required by the Patch Success application.
- 1E Tachyon Platform Product Pack — Classic Product Pack used to create the 1E Tachyon Platform instruction set required by the Tachyon Platform verification process.
- Microsoft SCCM Client Health Integrated Product Pack — Integrated Product Pack used to create the MS SCCM Client Health instruction set and Microsoft SCCM Client Health policy.
- Nomad Client Health Integrated Product Pack — Integrated Product Pack used to create the Nomad Client Health instruction set and Nomad Client Health policy.
- Windows Client Health Integrated Product Pack — Integrated Product Pack used to create the Windows Client Health instruction set and Windows Client Health policy.
- Tachyon Core Integrated Product Pack — Reference for the policy objects contained in the Integrated Product Pack: Tachyon Core.
- Trigger templates and preconditions reference — Reference for all the precondition fragments and trigger templates available in Integrated Product Packs included in the Tachyon Platform zip. These can be used to create your own custom rules and policies.

Deploy Tachyon clients

You will need to deploy the Tachyon client to at least one device in order to use any instructions.

Please refer to Deploying Tachyon clients for guidance on deploying clients to Windows and non-Windows devices.

Configure the Tachyon Server to support the Export all responses feature

The **Export all** feature is displayed on the responses page for a question once it has finished retrieving all its responses. To enable this to work you need to configure the following:

1. **Configure BCP**:

   The **Export all** feature is described in Exporting data from Tachyon Explorer. To enable Tachyon users with the appropriate permissions to use the **Export all** feature you must ensure that **Microsoft Bulk Copy Program (BCP)** is installed on each **Tachyon Response Stack** server, specifically where the Core component is hosted.

   - If Microsoft SQL Server is installed on the same server as the Tachyon Response Stack then BCP will normally be present.
   - If the TachyonResponses database is remote to the Tachyon Response Stack and there is no local copy of Microsoft SQL Server then you will need to install BCP.

   You can confirm BCP is installed by starting a command prompt and typing **bcp** and usage information is displayed. The command **bcp -v** displays the version.

   ⚠   The information here applies regardless of which version of SQL Server is being used. This does not imply that Tachyon itself is supported under every possible version of SQL Server that falls within those ranges. See Requirements for the supported versions and required Service Packs.

⚠️

Install the following components to get BCP working:

Installer file name	Product Name	Where to get it from
vc_redist.x64.exe	Visual C++ 2017 Redistributable	https://support.microsoft.com/en-gb/help/2977003/the-latest-supported-visual-c-downloads
msodbcsql.msi	Microsoft® ODBC Driver 13.1 for SQL Server®	https://www.microsoft.com/en-us/download/details.aspx?id=53339 This needs to be installed because of a known issue in the Microsoft Command Line Utilities 15 for SQL Server.
msodbcsql.msi	Microsoft® ODBC Driver 17 for SQL Server®	https://www.microsoft.com/en-us/download/details.aspx?id=56567
MsSqlCmdLnUtils.msi	Microsoft Command Line Utilities 15 for SQL Server	https://docs.microsoft.com/en-us/sql/tools/bcp-utility

To verify the components have been installed you can use **AppWiz.cpl** and check for the **Product Name**.

2. **Configure the share**:

The **Export all** feature enables the bulk copying of the entire completed responses for a Tachyon question to a specified **network share**.

⚠️ As this may potentially be a very large data set the location must have sufficient disk-space to store the exported data.

To use this feature you must create one or more network shares on the Tachyon Server or other location, and configure NTFS and share permissions as follows. If desired, it can be hidden using a $ at the end of the share name.

Share permissions

Configure the share with Everyone modify access, or the same as the NTFS security.

NTFS Security

The share folder needs **modify** access configured for the service account(s) used by the Tachyon Core application pool on *each* Response Stack server and the service account used by the Tachyon Consumer application pool on the Master Stack server. By default this account is NT AUTHORITY\NETWORK SERVICE (if the share folder is located on a Tachyon 'all-in-one' server where both the Tachyon Consumer and Core components are installed e.g. Master Stack and Response stack). However, there is another scenario where the share folder is neither located on the same server as the Tachyon Consumer or Tachyon Core components, but on a remote fileserver (like a NAS device, DFS share, etc). In this case, the Tachyon Consumer AND Tachyon Core components will attempt to connect to the share folder as their respective computer accounts, for example <domain>\<computer$>.

Therefore, depending on where the share folder is located, you will need to configuring NTFS permissions for the following:

- If the share is on the same server as the Tachyon Core application pool, the share must have NTFS **Modify** permissions added for the built-in **NT AUTHORITY\NETWORK SERVICE** account local to the server.
- If the share is remote from the server used by a Tachyon Core application pool, the share must have NTFS **Modify** permissions added for the **server$ account**. For example, if the Tachyon Core application pool is running on a server called **ACME-TCN01** the server account **ACME-TCN01$** would need to be added to the remote share with NTFS **Modify** permissions.
- If you have installed multiple Response Stacks, then repeat the preceding step, adding permissions on the share for each of the computers that are running a Tachyon Core. For instance, if you have deployed Response Stacks on two computers called **ACME-TCN01** and **ACME-TCN02**, then the server accounts **ACME-TCN01$** and **ACME-TCN02$** would need to be added to the share with NTFS **Modify** permissions.
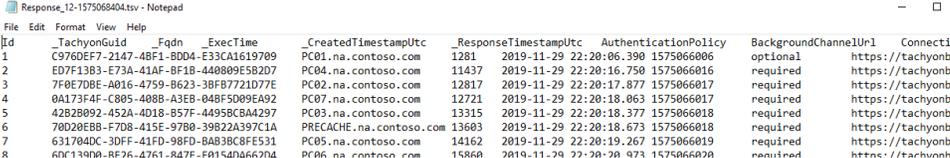
✓ Alternatively, you can use an AD security group that contains the computer$ account of all your Tachyon Servers.

ⓘ Include any user accounts or AD groups that would require access to the share.

The preceding are the *minimum* permissions required. Of course, if your share has *more* permissions it will also work for **Export All**. For example, if your share inherits from its parent the **Modify** permission for **Authenticated Users**, then this will automatically include permission for local and remote computer$ accounts, so you will not need to explicitly grant the permissions mentioned above.

Error: Header-row missing in .tsv file export	Tachyon Consumer has no access to share folder	
Error: Contents missing in .tsv file export	Tachyon Core (s) has no access to share folder	
Successful: Both header-row and contents correctly included in .tsv file export	Tachyon Consumer and Tachyon Core(s) have access to share folder	

Optional tasks

The following tasks are not essential but may enhance the performance and use of Tachyon in your environment.

Add an inventory connector

You can add an inventory connector to Tachyon that will sync data from a data source to an inventory repository. Typically this connector would be to another system such as Configuration Manager or to Tachyon itself. For more details please refer to the Connectors page. At least one configured inventory connector is required to support management groups.

Create management groups

You can create Management groups to partition your estate into groups of devices that can be managed separately. This is done by creating a management group in the Settings application, please refer to Management groups page and Management groups - tutorial for more details. To synchronize the management groups with Explorer you'll need to add a Tachyon connector, please refer to Tachyon connector for more details.

Change Tachyon database owner to 'sa'

After the databases have been created, best practice is to change the **owner** of each database to **sa**, to avoid issues if the owner's Windows account is deleted in future.

The following script can be used to change the **owner** of each Tachyon database to **sa**. This will work even if the **sa** login has been disabled, which is also best practice.

Change owner to 'sa'

```
ALTER AUTHORIZATION ON DATABASE::TachyonMaster To "sa"
GO
ALTER AUTHORIZATION ON DATABASE::TachyonResponses To "sa"
GO
```

⚠️ Ensure the Server Installation Account retains the **db_owner** role on the database to support re-configuration and upgrades. If the account is removed from being **owner**, then it will also be removed from the **db_owner** role and will need to be re-assigned, for example by using the **Grant db_owner** SQL script.

The **owner** user and **db_owner** role are both mapped to the database **dbo** user. It is preferable for the account to be a member of the **db_owner** role, instead of being the **owner** user.

Grant db_owner

```
USE [TachyonMaster]
GO
CREATE USER [ACME\TCNinstaller01] FOR LOGIN [ACME\TCNinstaller01];
ALTER ROLE [db_owner] ADD member [ACME\TCNinstaller01];
GO
USE [TachyonResponses]
GO
CREATE USER [ACME\TCNinstaller01] FOR LOGIN [ACME\TCNinstaller01];
ALTER ROLE [db_owner] ADD member [ACME\TCNinstaller01];
GO
```

Lock down the Switch SSL Certificate folder

If you want additional protection for the Switch's certificate then you can change the NTFS security on the Switch's SSL folder as described in Services and NTFS Security.

You should also remove the original copies of the certificate files from the installation files.

Changing the SMTP Host configuration

The Tachyon Server installer does not support configuration of SMTP credentials, but these can be configured post-installation. By default, Tachyon assumes port 25 and anonymous authentication.

Tachyon stores its SMTP configuration in

- **<INSTALLDIR>\Tachyon\Coordinator\Tachyon.Server.Coordinator.exe.config** (workflow emails)

After any changes reboot the server or restart the **1E Tachyon Coordinator** service.

```
<configuration>
  ...
  <appSettings>
    ...
    <add key="smtpHost" value="ACME-EXC01.acme.local"/>
    <add key="TachyonEmail" value="Tachyon@acme.local"/>
    ...
    <add key="2FAEnabled" value="true" />
    ...
  </appSettings>
  ...
  </entityFramework>
  <!-- The settings in the following section can be modified to provide custom port and authentication
options for SMTP -->
  <system.net>
    <mailSettings>
      <smtp deliveryMethod="Network">
        <network
          port="25"
          defaultCredentials="true"
          userName=""
          password=""
        />
      </smtp>
    </mailSettings>
  </system.net>
</configuration>
```

⚠

⚠️ Microsoft's documentation for the SMTP network section can be found here: https://msdn.microsoft.com/en-us/library/ms164242(v=vs.110).aspx.

When **defaultCredentials** is set to true, the mail subsystem uses the Windows credentials from the process under which the coordinator service is running to connect to the mail server. In general, this will only work with Microsoft servers, or servers that allow anonymous connections. To use different credentials, set defaultCredentials="false" and add values for **username** and **password** (and, optionally, **clientDomain**).

To use an encrypted connection, if the server supports it, add **enableSsl**="true". Change the **port** as needed, for example, port="465" or port="587".

Microsoft supports parameters named **host** and **From**, but these are ignored by Tachyon because the **smtpHost** and **TachyonEmail** keys in the <appSettings> section take precedence.

⚠️ If **smtpHost** is set to empty (blank) in a config file then email is disabled for the corresponding feature.

The Two-factor Authentication feature requires email. Therefore if **smtpHost** is set to empty, then the 2FA feature must be disabled by setting **<add key="2FAEnabled" value="false" />** in the **<INSTALLDIR>\Tachyon\Coordinator\Tachyon.Server.Coordinator.exe.config** file.

Finally, reboot the server or restart the **1E Tachyon Coordinator** service.

Enabling or disabling Two-factor Authentication

2FA is optionally disabled (enabled by default) in Tachyon Setup: Active Directory and email screen. If you need to change this after installation, then you need to edit the setting **<add key="2FAEnabled" value="true" />** in the **<INSTALLDIR>\Tachyon\Coordinator\Tachyon.Server.Coordinator.exe.config** file.

If enabling 2FA, please refer to Requirements: Two-factor Authentication Requirements and Requirements: Email Requirements.