Server installation issues

Summary

Troubleshooting common issues that you may be having with implementation.

If your problem is not identified on this page, then please review Known issues: Installation issues. page.

Please ensure you have run through the steps in the Verifying page before making any configuration changes. Several verification steps refer back to this page.

If you need further help, please refer to the Troubleshooting page for how to contact 1E Support and the technical support process.

On this page:

Unable to install

If for any reason you are unable to install, then please review the Requirements.

When installing interactively, please confirm you are logged on using an account that has local Administrator rights.

For Agents, you can troubleshoot installation issues by reviewing the installation logfile. On Windows, start an Administrative command prompt and use an msiexec command line including a log file as described in Installing the Tachyon Agent by command-line

For Tachyon Servers, you can troubleshoot installation issues by reviewing the installation log file that is created in the same directory as **Tachyon.Setup.exe** after Tachyon Setup has run the Tachyon installer.

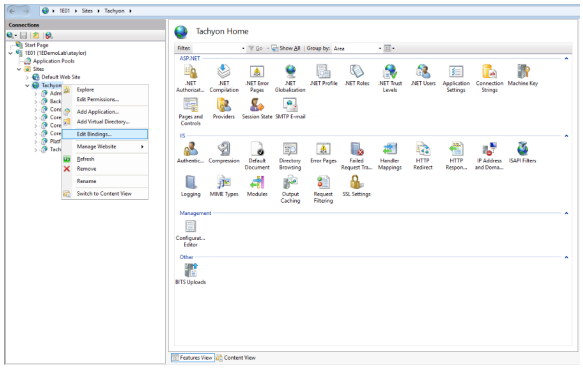
Verify the Tachyon website HTTPS binding

The Tachyon Server installer detects which Web Server certificate to use by matching the certificate's **Subject Name** (same as Issued To) with the **HTTPS Host header** supplied during installation. As discussed in Design considerations - Tachyon Server Certificates the **Subject Name** should be the DNS Alias FQDN of the server of type Common Name, for example **CN=TACHYON.ACME.LOCAL**

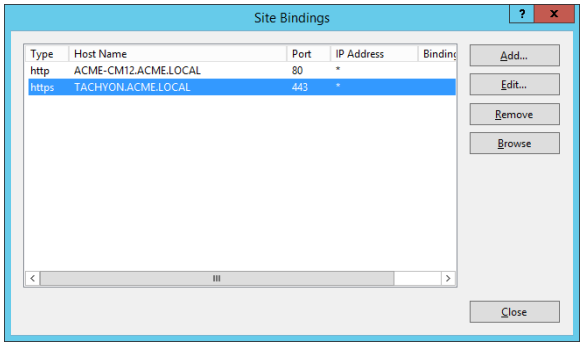
To check the HTTPS binding of the Tachyon website:

1. Open the Internet Information Services Manager on the machine where the Tachyon Server has been installed.

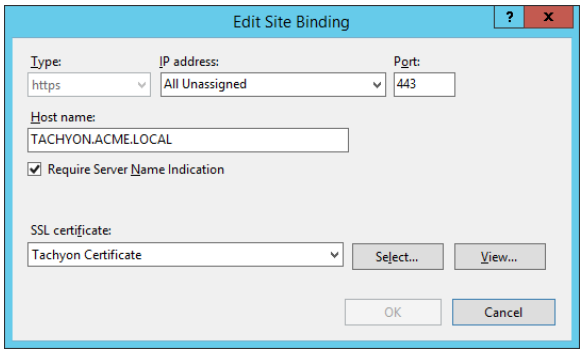
2. Navigate to the **Tachyon** website, right-click and select the **Edit Bindings...** menu item from the context menu, as shown in the picture opposite.



3. In the **Site Bindings** dialog select the HTTPS binding, as shown in the following picture, and click **Edit...**



4. Check that the **SSL certificate** is set to the correct certificate, for example **Tachyon Certificate**, as shown in the following picture.



We recommend that you review the HTTPS binding for the Tachyon web site created by the Tachyon Server installer, to ensure that the correct Web Server certificate has been selected.

If the correct certificate is not shown, you will need to:

- create a certificate if none already exist - please refer to Requirements: Tachyon Server Certificates
- ensure the certificate exists in the **Local Computer Personal Certificates** store of the server
- give the certificate a friendly name
- run the **SetSSLCerts.ps1** script decribed below using the certificate's friendly name

There are several reasons why the installer may pick the wrong Web server certificate or fail to find a suitable certificate:

- There are no certificates - you will need to create one - please refer to Requirements: Tachyon Server Certificates
- The correct certificate does not exist in the **Local Computer Personal Certificates** store of the server
    - The correct certificate may have been added to the wrong store
    - The certificate has not been added to any store
    - The certificate is not correctly configured, for example, the certificate does not have a **Subject Name** the same as the DNS Alias FQDN of the server of type Common Name, for example **CN=TACHYON.ACME.LOCAL**
- If there are multiple certificates with the same **Subject Name** in the **Local Computer Personal Certificates** store of the server, and the wrong one is selected

SetSSLCerts.ps1

A script is written to disk during install in **%programfiles%\1E\Tachyon\TachyonExternal** called **SetSSLCerts.ps1**. This can be used to set up IIS bindings and to bind the certificate used for the Coordinator. It takes three parameters, and four if a specific certificate is to be selected. The parameter order is not important if you specify the parameter names.

- **SecureSiteName** (mandatory)
    - The https host header for the ssl website. For example, **tachyon.acme.local**
- **SecurePort** (optional)
    - The port used for the ssl website. The default is **443**.
- **WorkflowWebPort** (optional)
    - The port used for the ssl binding for the coordinator service. The default is **8080**.
- A method of identifying a suitable certificate (optional) associated with a certificate in the personal folder of the local machine store.
    - **CertificateFriendlyName** - the friendly name is not part of a certificate and can be changed by modifying the certificate's properties in the certificate snap-in in mmc. You should ensure the friendly name is used for only one certificate.
    - **CertificateThumbprint** - this is unique for every certificate.

Example usage:

```
./SetSSLCerts.ps1 -SecureSiteName tachyon.acme.local -SecurePort 10443 -WorkflowWebPort 18080 -
CertificateFriendlyName "tachyon"
```

or

```
./SetSSLCerts.ps1 -SecureSiteName tachyon.acme.local -SecurePort 10443 -WorkflowWebPort 18080 -
CertificateThumbprint "3d699d8f28c2d7e0514cb0e047a1fd2f9db9bf4f"
```

SetSSLCerts.ps1 can be used to set up SSL bindings post-installation if the installer fails to select a certificate, or if a certificate has expired and needs to be be replaced. You should ensure that the same certificate is also used to create Switch certificate files.

Verify IIS Configuration

For minimum requirements for IIS see Preparation: Windows Server roles and features.

To review the configuration:

1. Start PowerShell with Admin privileges.

2. Type **Get-WindowsFeature** and wait for the listing to complete. It can be useful to pipe this output to a file.
3. Check the results and confirm that each of the minimum requirements is listed with an [X].

The below table provides a summary of the key IIS features used by Tachyon, and how they are used by the Tachyon website and its web applications.

	Stack	Authentication Enabled	SSL Settings	IP Address and Domain Restrictions
Tachyon (website)	Both	Anonymous and Windows	Not configured	Not configured
Admin	Master	Windows	Not configured	Not configured
Background	Response	Anonymous and Windows	Require SSL (ignore)	Not configured
Consumer	Master	Windows	Require SSL (ignore)	Not configured
Core	Response	Anonymous	Require SSL (ignore)	Local IP addresses (plus remote DMZ Server added manually)
CoreExternal	Master	Anonymous	Not configured	Not configured
CoreInternal	Response	Anonymous	Not configured	Local IP addresses
Platform	Master	Windows	Not configured	Not configured
Tachyon	Master	Windows	Require SSL (ignore)	Not configured

The **IP Address and Domain Restrictions** feature is described in more detail below. Steps for verifying its configuration are provided in Verify IIS Security of the Tachyon Website .

IP Address and Domain Restrictions

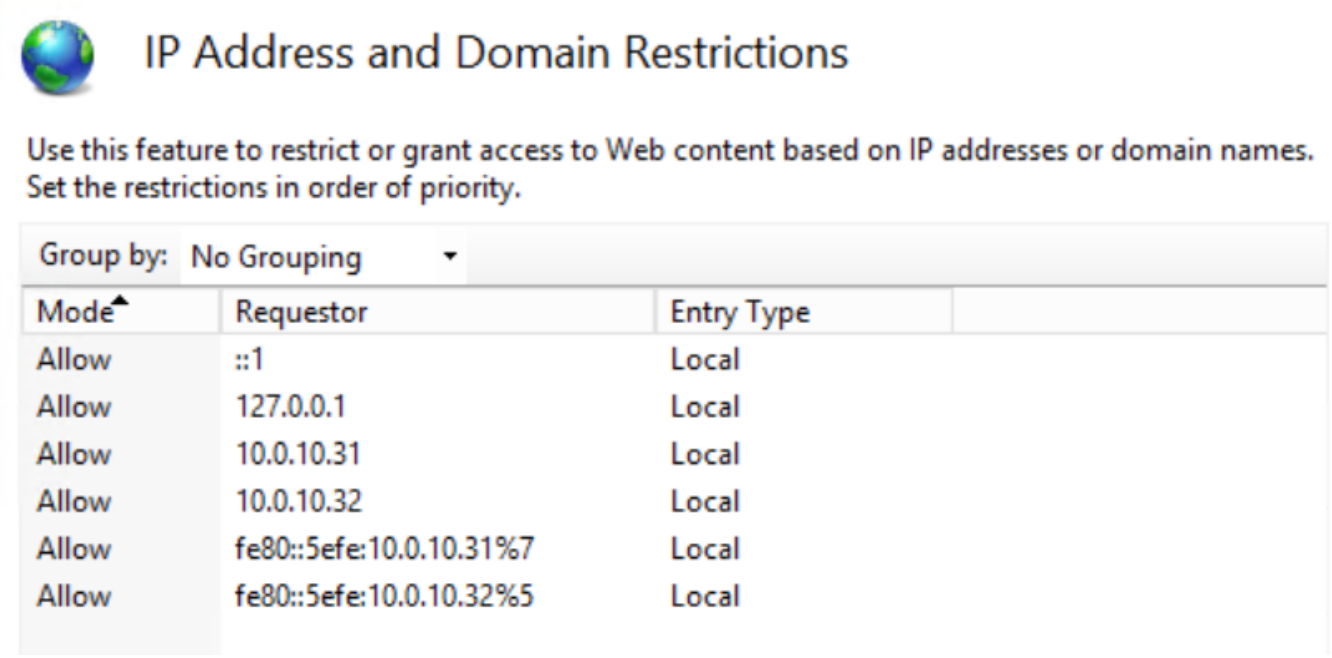
The Tachyon website uses the IIS feature **IP Address and Domain Restrictions** to restrict access to Tachyon Server web applications. The following web applications are configured during installation (and upgrade), so that only local connections are allowed, and remote connections are denied.

- Core (Response Stack)
- CoreInternal (Response Stack)

Other web applications, including Tachyon and Background, are not configured and therefore they allow all local and remote connections.

Below is an example of what the configuration looks like for a Tachyon Server which has a two network adapters, one for a Switch, the other for SQL traffic, with IPv4 enabled and IPv6 disabled on each interface. The IPv6 addresses shown are isatap addresses, which is enabled by default on the server.

- **::1** is the IPv6 loopback address
- **127.0.0.1** is the IPv4 loopback address
- **10.0.10.31** is the IPv4 address for network interface #7
- **10.0.10.32** is the IPv4 address for network interface #5
- **fe80::5efe:10.0.10.31%7** is the isatap address for network interface #7
- **fe80::5efe:10.0.10.32%5** is the isatap address for network interface #5



When to modify IP Address and Domain Restrictions

The Tachyon installer uses the PowerShell cmdlet **Get-NetIPAddress** to list all the IPv4 and IPv6 Addresses and adds them all to the restricted web applications during installation or upgrade. You must modify the configuration of **IP Address and Domain Restrictions** if the network interface configuration has changed on a Tachyon Server, for example if an IP Address is changed, or a new network interface is installed.

You will also need to modify the configuration of the Response Stack's Core web application to manually add the internal-facing IP Address of a DMZ Server.

Changing the configuration of Network Adapters

If the configuration of any network adapters is changed then the Tachyon website configuration for **IP Address and Domain Restrictions** may need to be updated with the server's new IPv4 and IPv6 addresses. Failure to update the configuration after a network change will cause issues between the Switch and the Core and prevent the Tachyon Server from functioning.

Use the PowerShell cmdlet **Get-NetIPAddress** to determine the current IP Addresses, and if necessary update the configuration for the three web applications (Authentication, Core and CoreInternal).

The following **AddIpSec.ps1** script can be used to refresh local IP Addresses. It does not remove old, unwanted, or remote IP Addresses.

AddIpSec.ps1

```
# extracted from Tachyon Server SetSSLCerts.ps1 script

Import-Module "WebAdministration"

Function AddIpSec() {
    param(
        [Parameter(Mandatory=$true)][string]$SiteName,
        [Parameter(Mandatory=$true)][string]$AppName
    )

    Write-Output "Adding IP restrictions to $AppName"

    $fullAppPath = "IIS:\Sites\" + $SiteName + "\" + $AppName

    if (Test-Path -Path $fullAppPath) {
        $appPath = $SiteName + "/" + $AppName
        $ipAddreses = Get-NetIPAddress | sort IpAddress | foreach { $_.IPAddress }
        Set-WebConfigurationProperty /system.webserver/security/ipsecurity -Name allowUnlisted -Value
"false" -Location $appPath -PSPath IIS:\
        foreach ($ipAddress in $ipAddreses)
        {
            $existingRestriction = Get-WebConfiguration system.webServer/Security/ipSecurity/add -
Location $appPath -PSPath IIS:\ | where { $_.ipAddress -eq $ipAddress }
            if (-not ($existingRestriction)) {
                Add-WebConfiguration system.webServer/security/ipSecurity -Location $appPath -Value @
{ipAddress="$ipAddress";allowed="true"} -PSPath IIS:\
                Write-Output "Allowed restriction on IP $ipAddress added to $AppName"
            }
            else {
                Write-Output "Restriction on IP $ipAddress already exists in $AppName. So skipping."
            }
        }
    }
    else {
        Write-Output "$AppName web application does not exist"
    }
}

$siteName = "Tachyon"

AddIpSec -SiteName $siteName -AppName "Core"
AddIpSec -SiteName $siteName -AppName "CoreInternal"
AddIpSec -SiteName $siteName -AppName "Authentication"
```

Remote Access to the Core

A post-installation verification test is to confirm web browsers do not have remote access to the Core. A remote web browser is not expected to be able to access the Core or CoreInternal web applications, which should return a 'Server Error 403 - Forbidden: Access is denied'. If you are able to access these web applications from a remote computer then it is probable that the **IP Address and Domain Restrictions** feature is not installed.

Use the following steps to check if the **IP Address and Domain Restrictions** feature is installed and to install it.

1. Logon to the Tachyon Server using an account that has administrator privileges.
2. Start Powershell with Admin privileges.
3. Type **Get-WindowsFeature** and wait for the listing to complete.
4. Check to see if Web Server Security feature **IP Address and Domain Restrictions** is installed or not.
5. If installed, then Verify IIS Configuration to determine if there may be another reason for the issue.
6. If not installed, then:
    a. type **Install-WindowsFeature Web-IP-Security** and wait for the feature installation to complete (a reboot or IIS restart is not required).
    b. after the feature installation, the Core and CoreInternal web applications will have their configuration settings restored to the settings configured at the time that Tachyon was installed.
7. Use the PowerShell cmdlet **Get-NetIPAddress** to determine the current IP Addresses, and if necessary update the configuration for the Core and CoreInternal web applications.
8. Repeat the verification steps.

401 Not Authorized

There are a number of reasons why you may see this error when you browse to the Tachyon Portal for the first time. You may also see errors saying Not Authorized or Unauthorized in server log files.

The usual reason for this is the SPN is not registered in AD for the DNS Name used to access the server.

Service Principal Names (SPN) are attributes of AD accounts. A domain administrator will need to create an HTTP class SPN for the Tachyon web server service account, by using one of the following methods:

- by editing the ServicePrincipalName attribute of the web server's computer account
- using the SETSPN commands below substituting your DNS Name, server and service account

```
setspn -l ACME\ACME-TCN01$
setspn -s http/acme-tcn01.acme.local ACME\ACME-TCN01$
setspn -s http/tachyon.acme.local ACME\ACME-TCN01$
```

The above example assumes :

- Tachyon web application pools are using Network Service
- The Tachyon server name is **ACME-TCN01** with a computer account in the **ACME** domain, which means the service account is **ACME\ACME-TCN01$**
- The DNS Name for the server is **tachyon.acme.local**

If in doubt, create both SPNs.

The above commands achieve the following:

1. Lists existing SPNs for the service account. Run this to record details before you request for any new SPN(s) to be created. Re-run this after creation, ensuring you wait sufficient time for AD replication to occur.
2. Creates an SPN for a CNAME record.
3. Creates an SPN for a (A) Host record.

To determine which type of record a DNS Name is, run the following command:

```
nslookup tachyon.acme.local
```

- If the command returns Name: **acme-tcn01.acmelocal** and alias **tachyon.acme.local** then tachyon.acme.local is a CNAME record.
- If the command returns Name: **tachyon.acme.local** and no aliases then tachyon.acme.local is a (A) Host record.

More complex scenarios can be configured which requires in-depth knowledge of IIS, SPN and DNS configuration and are beyond the scope of this documentation.

403 Access Denied

You may see this error when doing post-installation verification tests.When you use a browser to open an application in the Tachyon Portal, you will see **Server Error 403 - Forbidden: 'Access denied'** if your AD account does not have read access to the Tachyon web application folders. This can happen if Tachyon is installed in a non-default location and the NTFS permissions on the installation folder are not correct. To remedy the issue, you should review and correct NTFS permissions as described in Services and NTFS Security.

> Do not enable Anonymous authentication to fix this type of issue.

404 File not found

You may see this error when doing post-installation verification tests.

When you use a browser to open an application in the Tachyon Portal, and you see **Server Error 404 - 'File not found'** the reason is probably because you have not installed the IIS features **Web-ASP** and/or **Web-Asp-Net45**.

Use the following steps to check if the **Web-ASP** and/or **Web-Asp-Net45** features are installed and to install them.

1. Logon to the Tachyon Server using an account that has server administrator privileges.
2. Start Powershell with Admin privileges.
3. Type **Get-WindowsFeature** and wait for the listing to complete.
4. Check to see if Web Server Application Development feature **Web-ASP** and/or **Web-Asp-Net45** is installed or not.
5. If not installed
    a. type **Install-WindowsFeature Web-ASP, Web-Asp-Net45** and wait for the feature installation to complete (a reboot or IIS restart is not required).
    b. perform an IIS Reset
6. If installed, then Verify IIS Configuration to determine if there may be another reason for the issue.

7. Repeat the verification steps.

Tachyon Switch certificate issues

The Switch will start and then stop if there is an issue with its certificate files.

Check the following log files for errors. The default location for Tachyon Server logs is the **%AllUsersProfile%\1E\Tachyon** folder on the server where Tachyon Server is installed.

- Tachyon.Switch.Host.log
- Tachyon.Switch.log

Check to see if the following files exist in **%ProgramFiles%\1E\Tachyon\Switch\SSL** directory.

- **<computername>.cer**
- **<computername>.key**
- **cacert.pem**

If you forget to put the Tachyon Switch certificate files in the same directory as the Tachyon Server installer when installing Tachyon Server the Tachyon Switch Host Service will be unable to start and you will see errors similar to the following in the **Tachyon.Switch.Host.log** file:

```
2017-02-23 15:04:53,942 ERROR Tachyon.Switch.Host.SwitchProcess - Switch #1 Standard error out: ERROR:
0xD0006003 Cannot Continue - Machine Certificate validation failed
2017-02-23 15:04:53,942 ERROR Tachyon.Switch.Host.SwitchProcess - Switch #1 Standard error out:
2017-02-23 15:04:54,458 INFO  Tachyon.Switch.Host.SwitchProcess - Switch #1 has stopped running. It will not
be restarted.
```

In the **Tachyon.Switch.log** file, you will see something similar to the following:

```
15:04:53.411 CheckMyCertificate: TMNT2.tmnt.local "C:\Program Files\1E\Tachyon\Switch\SSL\TMNT2.cer"
15:04:53.411 Failed to Open "C:\Program Files\1E\Tachyon\Switch\SSL\TMNT2.cer"
15:04:53.411 ERROR: 0xD0006003 Cannot Continue - Machine Certificate validation failed
```

The Switch certificate files should should have been copied to the installation source folder prior to installation, for the installer to copy them to the SSL directory. You can copy any missing file into the Switch SSL folder, and then restart the Switch Host service and re-check the logs.

The Switch certificate files should have been created using the CertPrep tool as described in Preparation: Switch certificate files. In addition, the **cacert .pem** file may have been manually updated. If it has been updated incorrectly, replace it with the basic PEM file as created by the CertPrep tool, and restart the Switch Host service and re-check the logs. If the Switch starts OK using the basic pem, then review the bad pem file to look for editing mistakes.

Port 8080 issues

On a Tachyon reinstallation it is possible that port 8080 on the Tachyon Server becomes unusable. Typically this issue occur if the tachyon Server has been installed directly from the msi installer, rather than installation from the Tachyon Server Setup utility. This issue would manifest in the Tachyon Coordinator log as:

> INFO <OnStart>b__0 - Starting web Server at 'https://+:8080' ...
>
> ERROR <OnStart>b__0 - Starting web Server Exception has been thrown by the target of an invocation.

Also it may appear in the Tachyon Consumer log as:

> System.AggregateException: One or more errors occurred. ---> System.Net.Http.HttpRequestException: An error occurred while sending the request. ---> System.Net.WebException: Unable to connect to the remote server ---> System.Net.Sockets.SocketException: No connection could be made because the target machine actively refused it 10.10.99.38:8080

The solution is to clear the port:

> netsh http delete sslcert ipport=0.0.0.0:8080
>
> netsh http delete urlacl url=https://+:8080/

Followed by a reinstallation of the Tachyon Server.