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: Installing Tachyon Server.

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 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.

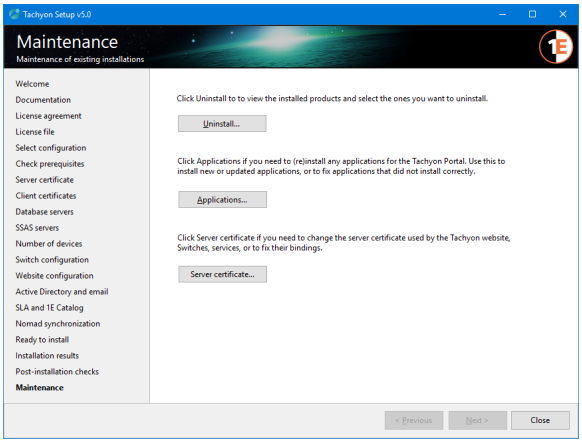
For clients, you can troubleshoot installation issues by reviewing its installation logfile. If you are having issues with 1E Client, please refer to 1E Client 5.0 - Troubleshooting.

Verify the Tachyon Server certificate bindings

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

To check the HTTPS binding of the Tachyon website use the following steps. These steps can also be used to change the certificate if it has expired, or a new certificate needs to be used.

1. Logon to the Tachyon Server using the Tachyon installation account, or user with local administrator rights.
2. Start Tachyon Setup and navigate directly to the Maintenance screen.
3. Click on **Server certificate...**



4. Review the **Certificate Bindings** screen.

   It shows the **thumbprint** of the certificate used by each of the bindings required by Tachyon, or the **Friendly name** if one has been used, as shown in the picture opposite.

   If the bindings are using different certificates then this may be deliberate, and you should find out why.

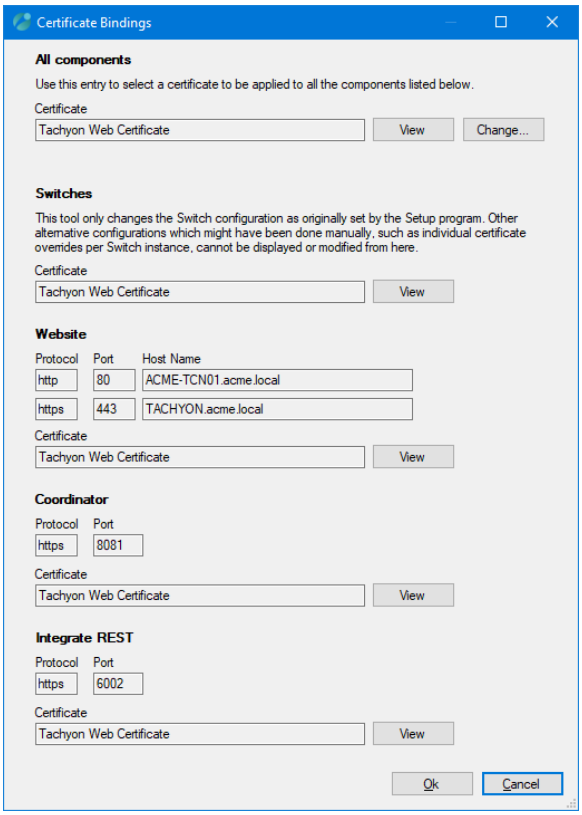
5. To view the details of a certificate, click **View**
6. To change the certificate, click **Change...**

   This will start the **Certificate Selector** similar to the Tachyon Setup: Server certificate screen.

   This will let you select a certificate and apply it to all the bindings.

If for any reason you need to apply a different certificate to each binding, then please contact 1E for details of how to

The Coordinator may be using port 8080 if you have upgraded from a Tachyon 3.3.

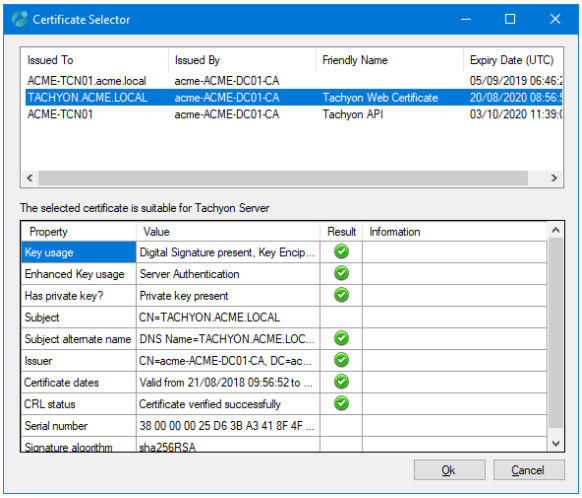


7. In the **Certificate Selector** screen, select a certificate, and the Selector will evaluate its suitability.

   Click **OK** when you have selected a suitable certificate.

   This will return you to the **Certificate Bindings** screen.
8. In the **Certificate Bindings** screen, click **OK** to save the new bindings configuration.

   You do not require an IIS reset.



Tachyon Switch certificate issues

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

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

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].
4. Alternatively, run Tachyon Setup and run the Post-installation check.

The table below shows the IIS web applications used by Tachyon, and the IIS features that affect how users and clients connect. For more detail about these IIS web applications, please refer to Tachyon Architecture: Tachyon Single-Server system.

IIS web application	Stack	Authentication Enabled	SSL Settings	IP Address and Domain Restrictions
Website	Master, Response & DMZ	Anonymous and Windows	Not configured	Not configured
ActiveEfficiency	Master	Anonymous and Windows	Not configured	Not configured
Admin	Master	Windows	Not configured	Not configured
Background	Response & DMZ	Anonymous and Windows Anonymous is used by clients, Windows is used by Consumer API	Require SSL (ignore)	Not configured
CatalogWeb	Master	Anonymous and Windows	Not configured	Not configured
Consumer	Master	Windows Basic Authentication is also enabled if using 1E Core 1.0 (f or ServiceNow integration)	Require SSL (ignore)	Not configured
Core	Response & DMZ	Anonymous	Require SSL (ignore)	Local IP addresses (plus remote DMZ Server added manually)
CoreExternal	Master	Anonymous	Not configured	Not configured
CoreInternal	Response & DMZ	Anonymous	Not configured	Local IP addresses
Experience	Master	Windows	Require SSL (ignore)	Not configured
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

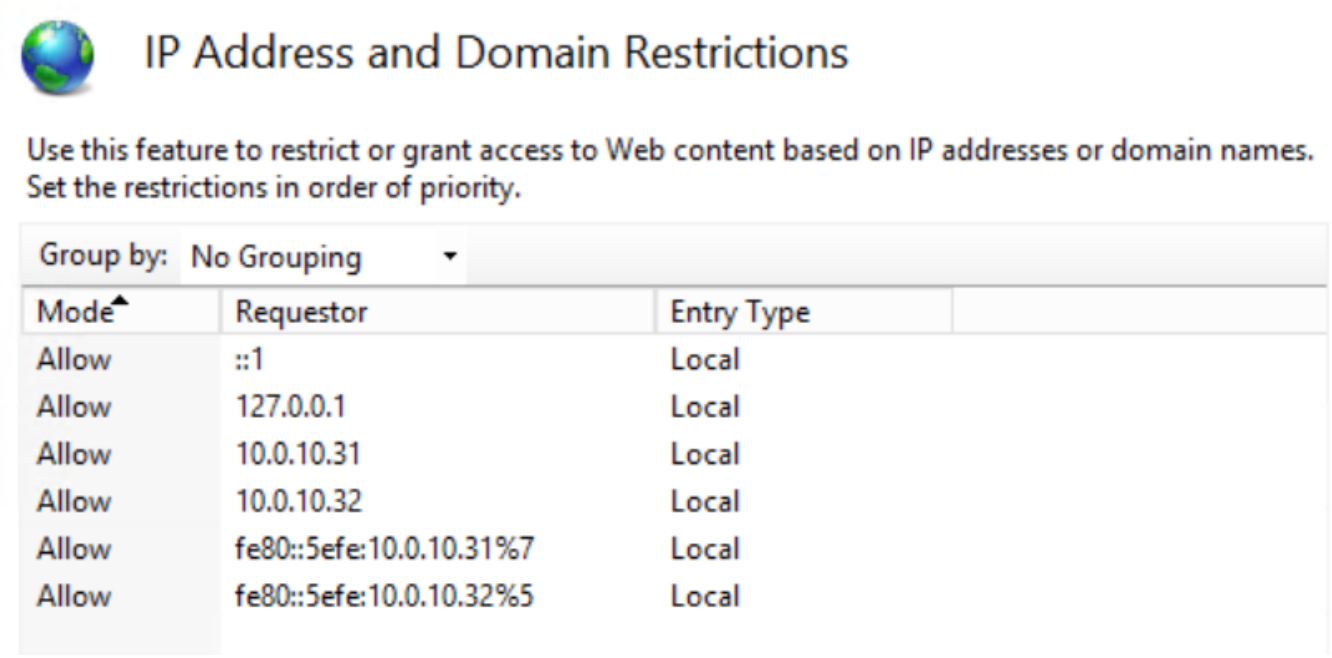
The Tachyon website uses the IIS feature **IP Address and Domain Restrictions** to restrict access to Tachyon Server web applications. The following web applications are configured during installation (and upgrade), so that only local connections are allowed, and remote connections are denied.

- 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 following SETSPN commands, 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$
```

Use each command as follows:

1. List 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. Use this if **tachyon.acme.local** is a CNAME record and its (A) Host record is **acme-tcn01.acme.local**
3. Use this if **tachyon.acme.local** is a (A) Host record.

The above example assumes:

- The service account for all Tachyon web application pools is 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, it does no harm to create an SPN for each DNS Name used to access the Tachyon Server, including its CNAMEs and (A) Host records using: `setspn -s http/<DNS Name> ACME\ACME-TCN01$`

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.acme.local** 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 the internal account used by the Application Pool 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.