

# MICROSOFT

## Walkthrough: Setting up Team Foundation Server to Require HTTPS and Secure Sockets Layer (SSL)

---

Compiled by Wendell Phillips and the Microsoft TFS CSS Team

2/19/2009

There has long been a walkthrough available on MSDN for accomplishing this task. We in support have found however that while this 'official' walkthrough is quite helpful, it is lacking in some areas and is missing some key items. Over the course of several support issues with customers who have tried to follow this walkthrough, we have updated it and made additions, creating what we feel is a more complete guide through the process. We are presenting it here for your viewing pleasure. This document may be updated from time to time as we need to make adjustments to the document. We also hope to have this document in its entirety up on MSDN as part of the official resources very soon. Enjoy, and please... let us know if you have any suggestions/additions/changes/etc. as you work through the process via comments to the BLOG at <http://blogs.msdn.com/dstfs>.

# Walkthrough: Setting up Team Foundation Server to Require HTTPS and Secure Sockets Layer (SSL)

The following walkthrough describes a process for requiring Team Foundation clients to use HTTPS and Secure Sockets Layer (SSL) connections to connect to Visual Studio Team System 2008 Team Foundation Server. In order to support external connections to your Team Foundation Server deployments, you must configure Internet Information Services (IIS) to enable Basic and/or Digest authentication. Additionally, you can configure an Internet Server Application Programming Interface (ISAPI) filter. See this article for an explanation of the Team Foundation Server ISAPI filter: [Team Foundation Server, Basic Authentication, and Digest Authentication](#).

Throughout this walkthrough, you will accomplish the following activities:

1. Create a certificate request for Team Foundation Server Web sites.
2. Issue the certificate request and create the binary certificate file.
3. Install and assign the certificate.
4. Configure the Team Foundation Server to require HTTPS and SSL.
5. Install the certificate (and certificate chain) on client computers.
6. Test the certificate.

## Prerequisites

To complete this walkthrough:

- The logical components that comprise the Team Foundation data tier and application tier of Team Foundation Server must be installed and operational. This walkthrough refers to the server or servers running the logical components that compose the Team Foundation application tier as the Team Foundation application-tier server. Also, it refers to the server or servers running the logical components that comprise the Team Foundation data tier as the Team Foundation data-tier server. Depending on your deployment configuration, the Team Foundation application-tier server and the Team Foundation data-tier server might be the same physical server or one or more different physical servers. For more information, see the Team Foundation Installation Guide. You can download the latest version of the Team Foundation Installation Guide from the Microsoft Download Center (<http://go.microsoft.com/fwlink/?linkid=79226>).
- You must have a certification authority (CA) available to issue certificates. This walkthrough assumes that you are using Microsoft Certificate Services as your CA. If you do not have a certification authority, you can install Microsoft Certificate Services and configure a certification authority. For more information, see the Microsoft Web site (<http://go.microsoft.com/fwlink/?LinkId=70929>).
- If you are using Fully Qualified Domain Names you will need to use one of the two solution methods proposed in this KB article: <http://support.microsoft.com/kb/926642>.

- If you configure a build agent for SSL connections:
  - Team Foundation Build and Team Explorer must be installed and operational.
  - A certificate must have been issued for the build agent.
  - Windows Support Tools must be installed on the build computer. These tools are required to associate a certificate with the IP address and port. For more information, see "Windows Support Tools" (<http://go.microsoft.com/fwlink/?LinkId=93827>).

### **Required Permissions**

You must be a member of the Administrators group on the Team Foundation application-tier and data-tier servers and a member of the Team Foundation Administrators group to complete this procedure. To configure a build agent for SSL connections, you must be a member of the Administrators group on the build computer. For more information about permissions, see [Team Foundation Server Permissions](#).

### **Assumptions**

This walkthrough assumes the following:

- The Team Foundation data-tier server and the Team Foundation application-tier server have been installed and deployed in a secure environment and configured according to security best practices.
- The administrator configuring Team Foundation Server with SSL is familiar with public key infrastructures (PKIs) and certificates, including familiarity with requesting, issuing, and assigning certificates. For more information about PKI and certificates, see the Microsoft Web site (<http://go.microsoft.com/fwlink/?LinkId=70930>).
- The administrator is familiar with configuring Internet Information Services (IIS), Microsoft SQL Server, and network settings, and has a working knowledge of the network topology of the development environment.

### **Installing Microsoft Certificate Services**

This walkthrough uses Microsoft Certificate Services as the certification authority (CA) for issuing certificates. For convenience in this walkthrough, Certificate Services is installed on the Team Foundation application-tier server, but you can choose your own certification authority software and deployment configuration as best suits your business needs. For security, you should consider isolating your root certification authority when you deploy Certificate Services in a production deployment. Physical isolation of the CA server, in a facility available only to security administrators, can significantly reduce the risk of tampering. For more information about Certificate Services features and best practices, see the Microsoft Web site (<http://go.microsoft.com/fwlink/?LinkId=70929>).

 **Caution:**

Once you have installed Certificate Services, you cannot change the name of the computer or the domain in which the computer is enlisted. If you change the computer name or domain, the certificate issued from the certification authority (CA) is invalidated.

### To install Certificate Services

1. Click **Start**, click **Control Panel**, and then select **Add or Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. In the **Windows Components Wizard**, click **Certificate Services** in the **Components** list.
4. Review the text in the message box, and then click **Yes**.
5. Click **Next** to start the installation.
6. On the **CA Type** page, select **Stand-alone root CA**, and then click **Next**.
7. On the **CA Identifying Information** page, in **Common name for this CA**, type the name of the computer.
8. In **Validity period**, change the duration for the certificate to six (6) months, and then click **Next**.
9. On the **Certificate Database Settings** page, click **Next** without making any changes.  
A message box appears that shows that IIS must be stopped.
10. In the message box, click **Yes**.  
The **Configuring Components** page appears.
11. If a message box appears with information about Active Server Pages (ASP), click **Yes**.
12. Click **Finish**.
13. To support Vista Clients you will need to follow <http://support.microsoft.com/kb/922706>.

### Creating a Certificate Request for Team Foundation Server Web Sites

On the application-tier computer, you must create a certificate request for Team Foundation Server using Internet Information Services (IIS) Manager.

### To create a certificate request for Team Foundation Server Web sites

1. Click **Start**, click **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. Expand computername (**Local Computer**) and then expand **Web sites**.

3. Right-click **Team Foundation Server** and then click **Properties**.
4. In **Team Foundation Server Properties**, click the **Directory Security** tab.
5. Under **Secure Communications**, click **Server Certificate**.  
The **Web Server Certificate Wizard** appears. Click **Next**.
6. On the **Server Certificate** page, click **Create a new certificate**, and then click **Next**.
7. On the **Delayed or Immediate Request** page, click **Next**.
8. On the **Name and Security Settings** page, click **Next** without making any changes.
9. On the **Organization Information** page, specify values for **Organization** and **Organization unit**. For example, enter the name of your company as the **Organization** and your team or group name for **Organization unit**. Click **Next**.
10. On the **Your Site's Common Name** page, click **Next** without making any changes.
11. On the **Geographical Information** page, specify the appropriate information in the **Country/Region**, **State/province**, and **City/locality** boxes, and then click **Next**.
12. On the **Certificate Request File Name** page, under **File name**, specify the location where you want the certificate request file saved and the name of the file, and then click **Next**.

 **Note:**

Make sure that you save the certificate request file to a network share or other location that can be accessed from the CA computer.

13. Review the information listed on the **Request File Summary** page and then click **Next**.
14. Click **Finish**.
15. Click **OK** to exit the **Team Foundation Server Properties** dialog box.

### **Issuing a Certificate Request and Creating a Binary Certificate File**

After you have created a certificate request, you must have the CA, in this case Microsoft Certificate Services, issue a certificate based on the request. As soon as a certificate is created, you can assign the certificate to the appropriate Web sites using IIS.

#### **To issue a certificate request using Microsoft Certificate Services**

1. On the computer running Certificate Services, Click **Start**, click **Administrative Tools**, and then click **Certification Authority**.
2. In the Explorer pane, right-click the computer name, select **All Tasks**, and then click **Submit new request**.
3. In the **Open Request File** dialog box, locate the certificate request text file that you created in the previous procedure, and then click **Open**.
4. In the Explorer pane, expand the computer name, and then click **Pending Requests**.

5. Note the **Request ID** value for the pending request.
6. Right-click the request, select **All Tasks**, and then click **Issue**.
7. In the Explorer window, under the computer name, select **Issued Certificates** and review the listed certificates to verify that a certificate was issued that matches the **Request ID** value for your request.
8. In **Issued Certificates**, right-click the issued certificate, select **All Tasks**, and then click **Export Binary Data**.
9. In **Columns that contain binary data**, select **Binary Certificate**. Under **Export options**, select **Save binary data to a file**, and then click **OK**.
10. In **Save Binary Data**, save the file to a portable media device or network share that can be accessed by the Team Foundation application-tier computer.
11. Exit **Certification Authority**.

### **Installing and Assigning the Certificate**

Before you can use SSL with Team Foundation Server, you must install the server certificate on the Team Foundation Server Web site and then configure HTTPS on Team Foundation Server-related Web sites. These related Web sites include the following:

- Default Web site
- SharePoint Central Administration
- Report Server

### **Installing the Server Certificate**

Follow these steps to install the server certificate on Team Foundation Server.

#### **To install the server certificate on the Team Foundation Server Web site**

1. On the Team Foundation application-tier server, click **Start**, click **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. Expand <computername> (**local computer**) and then expand **Web sites**.
3. Right-click **Team Foundation Server** and then click **Properties**.
4. In **Team Foundation Server Properties**, click the **Directory Security** tab.
5. Under **Secure Communications**, click **Server Certificate**.  
The **Web Server Certificate Wizard** appears. Click **Next**.
6. On the **Pending Certificate Request** page, select **Process the pending request and install the certificate**, and then click **Next**.
7. On the **Process a Pending Request** page, click **Browse**.

8. In the **Open** dialog box, under **Files of type**, select **All files (\*.\*)** from the drop-down list, and then locate the directory where you saved the binary certificate in the previous procedure. Select the binary certificate file and then click **Open**.
9. On the **Process a Pending Request** page, click **Next**.
10. On the **SSL Port** page, accept the default value or enter a new value, and then click **Next**. The default port for SSL connections is 443, but you must assign a unique port value for each of the following three sites: the Team Foundation Server Web site, the default Web site, and the SharePoint Central Administration Web site.

 **Important Note:**

Consider using a port number other than the default, as using a default port number can reduce the security of your deployment. Make a note of the SSL port value that you assign. Before you accept the default value, make sure that the port is not being used by another server certificate. SSL port values must be different for each server certificate you install. For example, if the default port of 443 is not already being used and you accept the default port value of 443 for the Team Foundation Server Web site, you must assign a different port value for the default Web site and the SharePoint Central Administration Web site. If you choose to use a different port, make sure this port is not in use by another server or reserved for a common application. Make a note of the port you use. The certificate is bound to the port number when installed in a web site. If you change the port number, you must remove and re-add the certificate.

11. Review the information about the **Certificate Summary** page, and then click **Next**.
12. Click **Finish**.
13. On the **Directory Security** tab, under **Authentication and access control**, click **Edit**.
14. In **Authentication Methods**, make sure that the **Enable anonymous access** box is cleared. In **Authenticated access**, select **Integrated Windows authentication** and either **Basic Authentication** or **Digest authentication for Windows domain servers** or both, depending on your deployment. Clear any other selections, and then click **OK**.

 **Note:**

After clicking **Digest authentication for Windows domain servers**, you might be prompted to confirm your choice. Read the text and then click **Yes**.

15. Click **OK** to close the **Team Foundation Server Properties** dialog box.

 **Note:**

If an **Inheritance Overrides** dialog box appears after clicking **OK**, click **Select All**, and then click **OK**.

## Assigning the Certificate to Default Web Site

Follow these steps to set up HTTPS on the default Web site in IIS.

### **Note:**

Depending on your certification hierarchy and public key infrastructure, you might also want to also configure IIS for client certificate authentication. For more information, see [Certificates \(IIS 6.0\)](#), [Certificate Services](#), and [Certificates](#) on the Microsoft Web site. See additional information located here (ConfigTeamBlogURLPlaceholder) for information specific to Team Foundation Server.

## To set up HTTPS on the Default Web site and require SSL

1. On the Team Foundation application-tier server, click **Start**, click **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. Expand <computername> (**local computer**) and then expand **Web Sites**.
3. Right-click **Default Web Site** and then click **Properties**.
4. In **Default Web Site Properties**, click the **Directory Security** tab.
5. Under **Secure Communications**, click **Server Certificate**.  
The **Web Server Certificate Wizard** appears. Click **Next**.
6. On the **Server Certificate** page, select **Assign an existing certificate**, and then click **Next**.
7. On the **Available Certificates** page, select the certificate whose **Friendly Name** value is **Team Foundation Server**. You might have to scroll to see the **Friendly Name** column in the list. Click **Next**.
8. On the **SSL Port** page, accept the default value or enter a new value, and then click **Next**.  
The default port for SSL connections is 443, but you must assign a unique port value for each of the following three sites: the Team Foundation Server Web site, the default Web site, and the SharePoint Central Administration Web site.

### **Important Note:**

Consider using a port number other than the default, as using a default port number can reduce the security of your deployment. Make a note of the SSL port value. SSL port values must be different for each server certificate you install. For example, if you accept the default port value of 443 for the Team Foundation Server Web site, you must assign a different port value for the default Web site and the SharePoint Central Administration Web site.

9. Review the information about the **Certificate Summary** page and then click **Next**.
10. Click **Finish**. The wizard will close.
11. On the **Directory Security** tab, under **Secure Communications**, click **Edit**.
12. In **Secure Communications**, select **Require secure channel (SSL)**. Make sure that **Ignore client certificates** is selected, and then click **OK**.

13. On the **Directory Security** tab, under **Authentication and access control**, click **Edit**.
14. In **Authentication Methods**, make sure that the **Enable anonymous access** box is cleared. In **Authenticated access**, select **Integrated Windows authentication** and either **Digest authentication for Windows domain servers**, **Basic authentication**, or both, as appropriate to your deployment. Clear any other selections, and then click **OK**. For more information about authentication methods and Team Foundation Server, see [Team Foundation Server, Basic Authentication, and Digest Authentication](#).

 **Note:**

After clicking **Digest authentication for Windows domain servers**, you might be prompted to confirm your choice. Read the text and then click **Yes**.

 **Important Note:**

You must configure Digest authentication correctly. Otherwise, attempts to access Team Foundation Server will fail. Do not choose Digest authentication unless your deployments meets all the requirements for Digest authentication. For more information about Digest authentication, see the Microsoft Web site (<http://go.microsoft.com/fwlink/?LinkId=89709>).

15. Click **OK** to close the **Default Web Site Properties** dialog box.

 **Note:**

If an **Inheritance Overrides** dialog box appears after clicking **OK**, click **Select All**, and then click **OK**.

### To configure the Team Foundation Server Web site to require SSL

1. On the Team Foundation application-tier server, click **Start**, click **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. Expand <computername> **(local computer)** and then expand **Web sites**.
3. Right-click **Team Foundation Server** and then click **Properties**.
4. In **Team Foundation Server Properties**, click the **Directory Security** tab.
5. On the **Directory Security** tab, under **Secure Communications**, click **Edit**.
6. In **Secure Communications**, select **Require secure channel (SSL)**. Make sure that **Ignore client certificates** is selected, and then click **OK**.
7. Click **OK** to close the **Team Foundation Server Properties** dialog box.

 **Note:**

If an **Inheritance Overrides** dialog box appears after clicking **OK**, click **Select All**, and then click **OK**.

 **Important Note:**

If you are using a Wildcard Server Certificate, you must also install the certificate in the Personal Store of the Team Foundation Server Service Account.

### Assigning the Certificate to SharePoint Central Administration

Follow these steps to set up HTTPS for SharePoint Central Administration.

#### To set up HTTPS for SharePoint Central Administration and require SSL

1. On the Team Foundation application-tier server, click **Start**, click **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. Expand <computername> (**local computer**) and then expand **Web Sites**.
3. Right-click **SharePoint Central Administration** and then click **Properties**.
4. In **SharePoint Central Administration Properties**, click the **Directory Security** tab.
5. Under **Secure Communications**, click **Server Certificate**.  
The **Web Server Certificate Wizard** appears. Click **Next**.
6. On the **Server Certificate** page, select **Assign an existing certificate**, and then click **Next**.
7. On the **Available Certificates** page, select the certificate whose **Friendly Name** value is **Team Foundation Server**. You might have to scroll to see the **Friendly Name** column in the list.
8. Click **Next**.
9. On the **SSL Port** page, accept the default value or enter a new value, and then click **Next**.  
The default port for SSL connections is 443, but you must assign a unique port value for each of the following three sites: the Team Foundation Server Web site, the default Web site, and the SharePoint Central Administration Web site.

 **Important Note:**

Consider using a port number other than the default, as using a default port number can reduce the security of your deployment. Make a note of the SSL port value. SSL port values must be different for each server certificate you install. For example, if you accept the default port value of 443 for the Team Foundation Server Web site, you must assign a different port value for the default Web site and the SharePoint Central Administration Web site.

 **Note:**

Make a note of this value, as you will need it in order to assign the certificate to the SQL Report Server.

10. Review the information about the **Certificate Summary** page and then click **Next**.
11. Click **Finish**.
12. On the **Directory Security** tab, under **Secure Communications**, click **Edit**.
13. In **Secure Communications**, select **Require secure channel (SSL)**. Make sure that **Ignore client certificates** is selected, and then click **OK**.
14. Click **OK** to close the **SharePoint Central Administration Properties** dialog box.

## Configure Alternate Access Mappings in SharePoint

The default installation settings for Alternate Access Mappings in SharePoint will have entries for the default site and for the Central Administration Site set as non-SSL values. You will need to update the existing values or add new values as appropriate for your installation. In this example, a mapping of: <https://Contoso1:1443> (Internal URL) to <https://Contoso1:1443> (Public URL) must exist for the Default Web Site and a mapping of <https://Contoso1:2443> to <https://Contoso1:2443> for the Central Administration Site.

1. Start **SharePoint Central Administration**, select **Operations** and then select **Alternate Access Mappings**.
2. Select the Listing for <http://Contoso1> in the Internal URL column.
3. Edit this value to reflect the SSL URL value for the Default Web Site – <https://Contoso1:1443> and click **OK**.
4. Return to the Alternate Access Mappings page and select the Central Administration URL – <http://Contoso1:17012>.
5. Edit the value to the appropriate setting for secure access to the Central Administration Site – <https://Contoso1:2443> and click **OK**.

## Configuring the ISAPI Filter

To use the ISAPI filter, you must create an ISAPI initialization file in the same directory as the AuthenticationFilter.dll file that is part of Team Foundation Server. You must also add the ISAPI filter to the registry.

### To configure the ISAPI Filter

1. On the Team Foundation application-tier server, click **Start**, click **Programs**, click **Accessories**, and click **Notepad**.
2. In Notepad, create the following file, where *ProxyAddress* is the IP address where external network traffic to Team Foundation Server will appear to originate from (usually a router) for which you want to require HTTPS/SSL and Basic and/or Digest authentication, and *SubnetMask* is the IP address/subnet mask pair or pairs for which you do not want to enforce Digest or Basic authentication.

 **Important Note:**

If you add the ProxyIPList key to the file, the SubnetList key and its values will be ignored. For more information, see [Team Foundation Server, Basic Authentication, and Digest Authentication](#).

 **Note:**

You can have more than one value for either ProxyAddress or SubnetMask. Separate ProxyAddress or SubnetMask values with a semicolon.

```
[config]
RequireSecurePort=true
ProxyIPList=ProxyAddress;
SubnetList=SubnetMask;
```

3. Save this file as **AuthenticationFilter.ini** in the same directory as AuthenticationFilter.dll. This directory is *drive:\Program Files\Microsoft Visual Studio 2008 Team Foundation Server\Tools*.
4. Open a Command Prompt window. To open a Command Prompt, click **Start**, click **Run**, type **cmd**, and then click **OK**.

 **Note:**

Even if you are logged on with administrative credentials, you must open an elevated Command Prompt to perform this function on a server that is running Windows Server 2008. To open an elevated Command Prompt, click **Start**, right-click **Command Prompt**, and click **Run as Administrator**. For more information, see the [Microsoft Web site](#).

5. At the command prompt, type the following command:

```
reg.exe add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Applcat
ion\TFS ISAPI Filter" /v ErrorMessageFile /t REG_SZ /d
%windir%\Microsoft.NET\Framework\v2.0.50727\EventLogMessages.dll /f
```

6. At the command prompt, type the following command:

```
reg.exe add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Applcat
ion\TFS ISAPI Filter" /v TypesSupported /t REG_DWORD /d 7 /f
```

7. On the Team Foundation application-tier server, click **Start**, click **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
8. Expand <computername> (**local computer**), expand **Web Sites**, right-click **Team Foundation Server**, and then click **Properties**.
9. In **Team Foundation Server Properties**, click the **ISAPI Filters** tab.

10. Under **ISAPI Filters**, click **Add**.
11. In **Add/Edit Filter Properties**, in **Filter name**, type **TFAuthenticationFilter**, in **Executable**, type *drive:\Program Files\Microsoft Visual Studio 2008 Team Foundation Server\Tools\AuthenticationFilter.dll*, and then click **OK**.

### **Configuring Your Firewall to Allow SSL Traffic**

You must configure your firewall to allow for traffic on the SSL ports you specified in IIS for the default Web site, the Team Foundation Server Web site, and the SharePoint Central Administration Web site.

#### **Note:**

The procedures for configuring your firewall to allow for SSL traffic will vary depending on the firewall software and hardware that you use in your deployment.

### **To configure a firewall to allow for network traffic on the SSL ports that are used by Team Foundation Server**

- See your firewall product documentation to determine the steps that are required to allow for network traffic on the SSL ports you specified for the default Web site, the Team Foundation Server Web site, and the SharePoint Central Administration Web site.

### **Updating Team Projects for SQL Report Server by Using the TfsConfigWss command-line tool**

Follow these steps to update the team project Web sites for SQL Report Server so that reports appear correctly on the team project portal sites.

### **To update team project sites for SQL Report Server**

1. On the application-tier server for Team Foundation, open a Command Prompt window, and change directories to *Drive:\%ProgramFiles%\Microsoft Visual Studio 2008 Team Foundation Server\Tools*.
2. At the command prompt, type the following command, and replace these strings:
  - SharePointSite is the new uniform resource indicator (URI) of the site collection for SharePoint Products and Technologies.
  - Reports is the new URI for SQL Server Reporting Services.
  - ReportServer is the new URI for the ReportsService.asmx Web service.

**TfsConfigWss ConfigureReporting /SharepointSitesUri: SharePointSite  
/ReportsUri:Reports /ReportServerUri:ReportServer**

## Updating Team Foundation Server Configuration Information

Follow these steps to update configuration information with the https URL values for the Windows SharePoint Services and Reporting Services Web sites.

### To update configuration information for Team Foundation Server

1. On the Team Foundation application-tier server, open a Command Prompt window, and change directories to Drive:\%ProgramFiles%\Microsoft Visual Studio 2008 Team Foundation Server\Tools.
2. Type the following command, and replace these strings:
  - BaseServerURL is the new URI for the Web server for the Team Foundation application-tier server.
  - BaseSiteURL is the new URI for the default Web site for the application-tier server.
  - SharePointSite is the new URI for the SharePoint Products and Technologies site collection.
  - SharePointAdministration is the new URI for the SharePoint Central Administration Web site.
  - Reports is the new URI for SQL Server Reporting Services.
  - ReportServer is the new URI for the ReportsService.asmx Web service.

```
TfsAdminUtil ConfigureConnections /ATUri:BaseServerURL  
/SharepointUri:BaseSiteURL /SharepointSitesUri:SharePointSite  
/SharepointAdminUri:SharePointAdministration /ReportsUri:Reports  
/ReportServerUri:ReportServer
```

#### **Note:**

If you are using a named instance, you will need to specify the named instance as part of the values for Reports and ReportServer. Do not eliminate or change the name of the named instance.

For example, if you specified port 443 for the Team Foundation Web SSL site port value, 1443 for the default Web site SSL port value in IIS, and 2443 for the SharePoint Central Administration port value, and your application-tier server was named Contoso1, you would modify the values as follows:

```
TfsAdminUtil ConfigureConnections /ATUri:https://Contoso1:443  
/SharepointUri:https://Contoso1:1443  
/SharepointSitesUri:https://Contoso1:1443/Sites  
/SharepointAdminUri:https://Contoso1:2443  
/ReportsUri:https://Contoso1:1443/Reports  
/ReportServerUri:https://Contoso1:1443/ReportServer
```

 **Note:**

The ConfigureConnections command has several additional options, such as updating the public Web address used in e-mail alerts. For more information, see [ConfigureConnections Command](#).

## Configuring Reporting Services for SSL Connections

Follow these steps to configure Reporting Services to require SSL.

### To configure Report Server for SSL connections

1. On the Team Foundation application-tier server, click **Start**, click Programs, click Microsoft SQL Server 2005, click Configuration Tools, and then click Reporting Services Configuration.
2. In the **Report Server Installation Instance Selection** dialog box, make sure that the computer and instance names are correct, and then click **Connect**.
3. In the Explorer pane, click Report Server Virtual Directory.
4. In **Report Server Virtual Directory Settings**, select **Require Secure Socket Layer (SSL) connections**. In **Require For**, select **1 - Connections**. In **Certificate Name**, type ApplicationTierServerName:ReportSiteSSLPort, and then click **Apply**.
5. Close Reporting Services Configuration Manager.

 **Note:**

Each Build Server, ProxyServer and Client Computer that will be connecting to TFS must trust the Certificate Authority that has issued the certificate(s) that identify the Team Foundation Server websites. This is done by browsing to the Certificate Authority website and installing the Certificate Chain for the CA server.

### Establishing trust to the Certificate Authority

1. From the computer that will need to trust the Certificate Authority browse to the CertSrv virtual directory on the Certificate Authority server.
2. Click "Download a CA Certificate, Certificate chain or CRL."
3. Click "Download CA Certificate Chain"
4. Click Open, and navigate to the Certificates item in the left pane of Certificate Manager.
5. In the right-hand pane, right click on the Certificate and select All Tasks – Open.
6. In the Certificate Import Wizard, click Next.
7. Select "Place all Certificates in the following store" and click Browse.

8. On the Select Certificate Store page, select "Show Physical Stores", expand Trusted Root Certification Authorities, select Local Computer and click OK.
9. Click Next and Finish.

### Installing the Certificate on Build Computers

If you installed Build Services on one or more servers, you must install the certificate on each of those servers.

#### **Note:**

In order to perform builds over SSL, the certificate must be installed in the trusted root store on both the build computer for the account on which the build service is running and the computer that initiates the build.

### To install the certificate on build computers

1. Log on to the build computer by using an account that is a member of the Administrators group on that computer.
2. Open a browser and open the following Web site, where TeamFoundationAT is the name of your Application Tier Server, and port is the SSL port number you assigned to the Team Foundation Server web site:  
  
**`https://TeamFoundationAT:port/services/v1.0/serverstatus.asmx`**
3. A security message dialog box appears. On **Security Alert**, click **View Certificate**.
4. On the **Certificate** dialog box, click the **Certification Path** tab.
5. In **Certification path**, click the certification authority. This should be the top node of the certification hierarchy, and there should be a red **X** next to the name. This indicates that the certification authority is not trusted because it is not in the Trusted Root Certification Authorities store. Click **View Certificate**.
6. On the **Certificate** dialog box, click **Install Certificate**.  
  
The Certificate Import Wizard opens. Click **Next**.
7. On the **Certificate Store** page, select **Place all certificates in the following store**, and then click **Browse**.
8. In **Select Certificate Store**, select **Show physical stores**. In **Select the certificate store you want to use**, expand **Trusted Root Certification Authorities**, select **Local Computer**, and then click **OK**.
9. On the **Certificate Store** page, click **Next**.
10. On the **Completing the Certificate Import Wizard** page, click **Finish**.
11. A **Certificate Import Wizard** dialog box might appear confirming that the import was successful. If the dialog box appears, click **OK**.

12. On the **Certificate** dialog box, click **OK**. The Certificate dialog box for the top node certification hierarchy will close.
13. On the **Certificate** dialog box, click **OK**. The Certificate dialog box for the subservient certificate will close.
14. On **Security Alert**, click **No**.
15. Open a browser and open the following Web site, where TeamFoundationAT is the name of your Application Tier Server, and port is the SSL port number you assigned to the Team Foundation Server web site:  
  
**`https://TeamFoundationAT:port/services/v1.0/serverstatus.asmx`**
16. The **ServerStatus Web Service** page should open. This confirms that you have installed the certificate and the certification authority correctly. Close the browser.

### **Configuring a Build Agent for SSL Connections**

To configure a build agent for SSL connections, you must configure an HTTPS certificate for each combination of IP address and port. If all build agents share the same port on the build computer, you must configure only a single certificate. If you run more than one build agent on more than one port, you must configure a certificate for each port.

You configure a build agent to require SSL by performing the following tasks in sequence:

1. Create and configure the build agent to require HTTPS.
2. Stop the Visual Studio Team Foundation Build service.
3. Modify the build service configuration to require HTTPS.
4. Associate a certificate with the IP address and port.
5. Configure the port and protocol for the build agent.
6. Restart the Visual Studio Team Foundation Build service.
7. Verify the SSL configuration.

### **To configure the build agent to require HTTPS**

1. Open the **Manage Build Agents** dialog box, and select the **Require Secure Channel (HTTPS)** check box.

For more information, see [How to: Create and Manage Build Agents](#).

2. Click **Edit**. The **Build Agent Properties** dialog box appears.
3. In the **Agent status** list, click **Disabled**.

### To stop the Visual Studio Team Foundation Build service

1. Log on to the build computer by using an account that is a member of the Administrators group on that computer.
2. On the build computer, click **Start**, click **Control Panel**, click **Administrative Tools**, and then click **Services**.
3. In the **Services (Local)** pane, right-click **Visual Studio Team Foundation Build**, and click **Properties**.

The **Visual Studio Team Foundation Build Properties (Local Computer)** dialog box opens.

4. Under **Service Status**, click **Stop**.

### To modify the build service configuration to require HTTPS

1. Log on to the build computer by using an account that is a member of the Administrators group on that computer.
2. Open Drive:\Program Files\Microsoft Visual Studio 2008\Common7\IDE\PrivateAssemblies, right-click TfsBuildservice.config.exe, and click **Open**.

The file opens in the XML editor for Visual Studio.

3. In the <appSettings> section, change the value of the RequireSecureChannel key to "true". For example, change the key definition to the following string:

```
<add key="RequireSecureChannel" value="true" />
```

4. Make sure the port setting matches your desired Build port.
5. Save your changes, and close the file.

### To associate an SSL certificate to an IP address and port number

1. Log on to the build computer by using an account that is a member of the Administrators group on that computer.
2. Use the Certificates snap-in to find an X.509 certificate that has an intended purpose of **Server** authentication for the Build Server. If you are installing on the Application Tier and it has a Server Authentication certificate you can use the same certificate.

Note, for more information on the following steps, see "How To: Retrieve the Thumbprint of a Certificate" (<http://go.microsoft.com/fwlink/?LinkId=93828>).

3. Copy the thumbprint of the certificate into a text editor, such as Notepad.
4. Remove all spaces between the hexadecimal characters.

You can perform this task by using the text editor's find-and-replace feature to replace each space with a null character.

5. On the build computer, click **Start**, click **All Programs**, click **Windows Support Tools**, and then click **Command Prompt**.
6. Run the **HttpCfg.exe** tool in "set" mode on the SSL store to bind the certificate to a port number. (HttpCfg.exe is available as a part of the Support Tools installation on the Windows Server 2003 CD.) The tool uses the thumbprint to identify the certificate, as shown in the following example:

```
httpcfg set ssl /i 0.0.0.0:9191 /h ThumbprintwithNoSpaces
```

The /i parameter has the syntax of IPAddress:Port and instructs the tool to set the certificate to port 9191 of the build computer. The IP address 0.0.0.0 reserves all computer addresses for simplicity. If you need additional precision, specify the exact IP address on which the agent service is published. The /h parameter specifies the thumbprint of the certificate.

If client certificates must be negotiated, add the parameter/f 2 as shown in the following example:

```
httpcfg set ssl /i 0.0.0.0:9191 /h ThumbprintwithNoSpaces /f 2
```

For more information about the syntax of the **HttpCfg.exe** command, see "How To: Configure a Port with An SSL Certificate" (<http://go.microsoft.com/fwlink/?LinkId=93829>).

Note: This article mentions using a Client Authentication

## To configure the build agent port and protocol

1. At the command prompt, run **wcfhttpconfig free** PortNumber. The command statement should resemble the following string:

```
wcfhttpconfig free OldPortForHttp
```

For more information, see [wcfhttpconfig \(Team Foundation Build\)](#).

2. At the command prompt, run **wcfhttpconfig reserve** UserAccount URL. The command statement should resemble the following:

```
wcfhttpconfig reserve Domain\Account  
https://+Computer:NewPortForHttps/Build/v2.0/AgentService.asmx
```

Where Computer is blank and the Domain\Account in the Build Service Account. For Example:

```
wcfhttpconfig reserve contoso\TfsBuild
https://+:9191/Build/v2.0/AgentService.asmx
```

3. Add the port to the exceptions list for Windows Firewall.

### To restart the Visual Studio Team Foundation Build service

1. Log on to the build computer by using an account that is a member of the Administrators group on that computer.
2. On the build computer, click **Start**, click **Control Panel**, click **Administrative Tools**, and then click **Services**.
3. In the **Services (Local)** pane, right-click **Visual Studio Team Foundation Build**, and click **Properties**.

The **Visual Studio Team Foundation Build Properties (Local Computer)** dialog box opens.

4. Under **Service Status**, click **Start**.

### To verify the SSL configuration

1. Open the **Manage Build Agents** dialog box.

For more information, see [How to: Create and Manage Build Agents](#).

2. Click **Edit**.

The **Build Agent Properties** dialog box appears.

3. In the **Agent status** list, click **Enabled**.

4. Verify whether communication is occurring by running a build using the build agent.

For more information, see [How to: Queue or Start a Build Definition](#).

## Installing the Certificate on Team Foundation Server Proxy Computers

If you installed Team Foundation Server Proxy on one or more computers, you must install the certificate on each of those computers.

### Note:

In addition to the procedure below, you must configure any firewalls for the proxy computer to allow for traffic on the SSL ports that you specified for Team Foundation Server. The procedures for configuring your firewall in this way will vary depending on the firewall software and hardware that you use in your deployment.

### To install the certificate on Team Foundation Server Proxy computers

1. Log on to the Team Foundation Server Proxy server by using an account that is a member of the Administrators group on that computer.
2. Open a browser and open the following Web site, where TeamFoundationAT is the name of your Application Tier Server, and port is the SSL port number you assigned to the Team Foundation Server web site:

**<https://TeamFoundationAT:port/services/v1.0/serverstatus.asmx>**

3. A security message dialog box appears. On **Security Alert**, click **View Certificate**.
4. On the **Certificate** dialog box, click the **Certification Path** tab.
5. In **Certification path**, click the certification authority. This should be the top node of the certification hierarchy, and there should be a red **X** next to the name. This indicates that the certification authority is not trusted because it is not in the Trusted Root Certification Authorities store. Click **View Certificate**.
6. On the **Certificate** dialog box, click **Install Certificate**.  
The Certificate Import Wizard opens. Click **Next**.
7. On the **Certificate Store** page, select **Place all certificates in the following store**, and then click **Browse**.
8. In **Select Certificate Store**, select **Show physical stores**. In **Select the certificate store you want to use**, expand **Trusted Root Certification Authorities**, select **Local Computer**, and then click **OK**.
9. On the **Certificate Store** page, click **Next**.
10. On the **Completing the Certificate Import Wizard** page, click **Finish**.
11. A **Certificate Import Wizard** dialog box might appear confirming that the import was successful. If this dialog box appears, click **OK**.
12. On the **Certificate** dialog box, click **OK**. The Certificate dialog box for the top node certification hierarchy will close.
13. On the **Certificate** dialog box, click **OK**. The Certificate dialog box for the subservient certificate will close. On **Security Alert**, click **No**.
14. Open a browser and open the following Web site, where TeamFoundationAT is the name of your Application Tier Server, and port is the SSL port number you assigned to the Team Foundation Server web site:

**<https://TeamFoundationAT:port/services/v1.0/serverstatus.asmx>**

15. The **ServerStatus Web Service** page should open. This confirms that you have installed the certificate and the certification authority correctly. Close the browser.

## Installing the Certificate on Client Computers

Every client computer that accesses Team Foundation Server must have the certificate installed locally. Additionally, if the client computer has previously accessed a Team Foundation Server team project, you must clear the client cache for every user who uses the computer to connect to Team Foundation Server before that user will be able to connect to Team Foundation Server.

### Important Note:

Do not follow this procedure for Team Foundation clients that are installed on the server that is running Team Foundation Server.

## To install the certificate on Team Foundation client computers

1. Log on to the Team Foundation client computer by using an account that is a member of the **Administrators** group on that computer.
2. Open a browser and open the following Web site, where TeamFoundationAT is the name of your Application Tier Server, and port is the SSL port number you assigned to the Team Foundation Server web site:

**<https://TeamFoundationAT:port/services/v1.0/serverstatus.asmx>**

3. A security message dialog box appears. On **Security Alert**, click **View Certificate**.
4. On the **Certificate** dialog box, click the **Certification Path** tab.
5. In **Certification path**, click the certification authority. This should be the top node of the certification hierarchy, and there should be a red **X** next to the name. This indicates that the certification authority is not trusted because it is not in the Trusted Root Certification Authorities store. Click **View Certificate**.
6. On the **Certificate** dialog box, click **Install Certificate**.  
The Certificate Import Wizard opens. Click **Next**.
7. On the **Certificate Store** page, select **Place all certificates in the following store**, and then click **Browse**.
8. In **Select Certificate Store**, select **Show physical stores**. In **Select the certificate store you want to use**, expand **Trusted Root Certification Authorities**, select **Local Computer**, and then click **OK**.
9. On the **Certificate Store** page, click **Next**.
10. On the **Completing the Certificate Import Wizard** page, click **Finish**.
11. A **Certificate Import Wizard** dialog box might appear confirming that the import was successful. If the dialog box appears, click **OK**.
12. On the **Certificate** dialog box, click **OK**. The Certificate dialog box for the top node certification hierarchy will close.

13. On the **Certificate** dialog box, click **OK**. The Certificate dialog box for the subservient certificate will close.
14. On **Security Alert**, click **No**.
15. Open a browser and open the following Web site, where TeamFoundationAT is the name of your Application Tier Server, and port is the SSL port number you assigned to the Team Foundation Server web site:  
  
**`https://TeamFoundationAT:port/services/v1.0/serverstatus.asmx`**
16. The **ServerStatus Web Service** page should open. This confirms that you have installed the certificate and the certification authority correctly. Close the browser.

### **To clear the cache on Team Foundation client computers**

1. Log on to the Team Foundation client computer by using the user credentials of the user you want to update.
2. On the Team Foundation client computer, close all open instances of Visual Studio.
3. Open a browser and open the following folder:  
  
**`\Documents and Settings\<username>\Local Settings\Application Data\Microsoft\Team Foundation\2.0\Cache`**
4. Delete the contents of the Cache directory. Make sure that you delete all subfolders.
5. Click **Start**, click **Run**, type **`devenv /resetuserdata`**, and then click **OK**.
6. Repeat these steps for every user account on the computer that accesses Team Foundation Server.

 **Note:**

You might want to consider distributing instructions on how to clear the cache to all of your Team Foundation Server users so that they can clear the cache for themselves.