

Walkthrough: Setting up Team Foundation Server 2008 to Require HTTPS and Secure Sockets Layer (SSL) for Windows Server 2008

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. Install and assign the certificate.
3. Configure the Team Foundation Server to require HTTPS and SSL.
4. Install the certificate (and certificate chain) on client computers.
5. 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 you already have a certification authority. 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 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.

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. Click on computer name (**Local Computer**) and then double-click **Server Certificates** in the IIS section of the center pane.
3. In **Server Certificates** under **Actions** choose **Create Certificate Request**.
4. On the **Distinguished Name Properties** page, enter the machine name/URL for the TFS application server in **Common name** box (this is very important - make sure common name matches with machine name/URL of the TFS app server; otherwise Team Explorer will **NOT** be able to connect to TFS), then specify values for **Organization**, **Organizational unit**, **City/locality**, **State/province**, and **Country/region**. Click **Next**.
5. On the **Cryptographic Service Provider Properties** page, click **Next**.

6. On the **File Name** page, specify the location where you want the certificate request file saved and the name of the file, and then click **Finish**.

 **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.

Issuing a Certificate Request and Creating a Binary Certificate File

After you have created a certificate request, you must have the CA issue a certificate based on the request. Once a certificate is created, you can assign it to the appropriate TFS web sites using IIS.

 **Note:**

The procedures for issuing a certificate will vary depending on the certificate authority that you use in your deployment.

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
- Reporting Service

Installing the Server Certificate

Follow these steps to install the server certificate on the IIS that hosts the Team Foundation Server website.

1. On the Team Foundation application-tier server, click **Start**, click **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. Click on computer name (**Local Computer**) and then double-click the **Server Certificates** item in the center pane.
3. In **Server Certificates** under **Actions** choose **Complete Certificate Request**.
4. On the **Specify Certificate Authority Response** page, under **File name containing the certification authority's response** column, browse to the directory containing the binary certificate you saved during the process of issuing the certificate in Certificate Server. Select the binary certificate file. Under Friendly name enter something so that you can recognize this is the certificate for TFS, such as "Team Foundation Server". Then click **OK**.

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 <computer name> (**local computer**) and then expand **Sites**.
3. Left-click **Default Web Site** to highlight it and then click **Bindings...** under the **Actions** window in the right hand side.
4. In **Site Bindings** screen, click **Add** button.
5. In **Add Site Binding** screen, choose "https" under **Type**. In **Port** input box, accept the default port or enter a new value. 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. In the **SSL certificate** drop down box, choose the server certificate installed in the previous step. Click **OK** to exit the screen.

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 default Web site, you must assign a different port value for the Team Foundation Server Web site and the SharePoint Central Administration Web site.

6. Click **Close** to exit the **Site Bindings** screen.
7. In the **Default Web Site Home** windows, double-click the **SSL Settings** item in the center pane. Select **Require SSL**. Make sure the **Ignore** option is selected under **client certificates**, and then click **Apply** in the **Actions** pane.
8. Click the **Default Web Site** node under Connections to return to the **Default Web Site Home** window. Double-click the **Authentication** item in the center pane and make sure that **Anonymous Authentication** is disabled. Enable **Windows Authentication** and either **Digest Authentication**, **Basic Authentication**, or both, as appropriate to your deployment. Disable other choices. For more information about authentication methods and Team Foundation Server, see [Team Foundation Server, Basic Authentication, and Digest Authentication](#).

Important Note:

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

Repeat steps 1-8 above for the **SharePoint Central Admin** and the **Team Foundation Server** websites. **Remember to specify a different port for each.**

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.

1. Launch the "SharePoint 3.0 Central Administration tool" by opening the **Administrative Tools**, and click on **SharePoint 3.0 Central Administration**.
2. Once the tool opens, click **Operations**.
3. Under **Global Configuration** click **Alternate Access Mappings**.
4. Click the internal URL for default web site.
5. In the text box titled **URL protocol, host and port** change the default website address from http to https and change the port number to the SSL port number for the default website. Click **OK**.
6. Under the **Alternative Access Mapping Collection** dropdown box, choose **Show All**.
7. Click the internal URL for SharePoint Central Administration.
8. In the text box titled **URL protocol, host and port** change the SharePoint Central Admin website address from http to https and change the port number to the SSL port number for the SharePoint Central Admin website. 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. (This should be already configured for TFS 2008, go through steps 1 to 5 if you need to make any updates)

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*;
 - 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*.
3. 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](#).

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

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

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

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

6. On the Team Foundation application-tier server, click **Start**, click **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
7. Expand <computer name> (**local computer**), expand **Sites**, left-click **Team Foundation Server**, and then go to **Server Components**, and double click on **ISAPI Filters**.
8. Under **ISAPI Filters**, click **Add** under **Actions**.
9. In **Add ISAPI Filter** screen, in **Filter name**, type **TFAuthenticationFilter**, in **Executable**, type or browse to *drive:\Program Files\Microsoft Visual Studio 2008 Team Foundation Server\Tools\AuthenticationFilter.dll*, and then click **OK**.

 **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 8081 for the Team Foundation Web SSL site port value, 443 for the default Web site SSL port value in IIS, and 17013 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://Contoso1:8081
/SharepointUri:https://Contoso1:443 **/SharepointSitesUri:**https://Contoso1:443/**Sites**
/SharepointAdminUri:https://Contoso1:17013
/ReportsUri:https://Contoso1:443/**Reports**
/ReportServerUri:https://Contoso1:443/**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 the first set steps if you are using Reporting Server 2005 and second set steps if you are using Reporting Server 2008.

To configure Report Server 2005 for SSL connections

1. On the Team Foundation application-tier server, click **Start**, click All Programs, click Microsoft SQL Server 2005, click Configuration Tools, and then click Reporting Services Configuration Manager.
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.

To configure Report Server 2008 for SSL connections

1. On the Team Foundation application-tier server, click **Start**, click All Programs, click Microsoft SQL Server 2008, click Configuration Tools, and then click Reporting Services Configuration Manager.
2. In the **Reporting Services Configuration Connection** dialog box, make sure that the computer and instance names are correct, and then click **Connect**.
3. In the Explorer pane, click **Web Service URL**.
4. In the **Report Server Web Service Site identification** section, use the SSL Certificate drop-down to select the server certificate you installed in IIS in the previous steps. Use the SSL Port box to specify the port number selected for the Default Web site, and then click **Apply**.
5. In the Explorer pane, click **Report Manager URL**.
6. In **Report Manager Site Identification**, click **Advanced**.
7. In **Multiple SSL Identities for Report Manager**, click **Add**. Select the certificate in the **Certificate** drop down box and click **OK**. Click **OK** to close **Advanced Multiple Web Site Configuration** screen.
8. Close Reporting Services Configuration Manager.

 **Note:**

Each Build Server, TFS Proxy Server 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.

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:

 [Copy Code](#)

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

4. 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 client authentication.

For more information, 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. The tool uses the thumbprint to identify the certificate, as shown in the following example:

 [Copy Code](#)

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

 [Copy Code](#)

```
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>).

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:

 [Copy Code](#)

```
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:

 [Copy Code](#)

```
wcfhttpconfig reserve Domain\Account  
https://+Computer:NewPortForHttps/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.
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.

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:

For Windows XP/Windows 2003:

Drive : **\Documents and Settings\username\Local Settings\Application Data\Microsoft\Team Foundation\2.0\Cache**

For Windows Vista/Windows 2008:

Drive: **\Users\username\AppData\Local\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.

