Configuring HTTP and HTTPS

.NET Framework (current version)

WCF services and clients can communicate over HTTP and HTTPS. The HTTP/HTTPS settings are configured by using Internet Information Services (IIS) or through the use of a command-line tool. When a WCF service is hosted under IIS HTTP or HTTPS settings can be configured within IIS (using the inetmgr.exe tool). If a WCF service is self-hosted, HTTP or HTTPS settings are configured by using a command-line tool.

At the minimum you will want to configure a URL registration, and add a Firewall exception for the URL your service will be using.

The tool used to configure HTTP settings depends on the operating system the computer is running.

When running Windows Server 2003 or Windows XP, use the HttpCfg.exe tool. Windows Server 2003 automatically installs this tool. When running Windows XP, you can download the tool at Windows XP Service Pack 2 Support Tools. For more information, see Httpcfg Overview.

When running Windows Vistaor Windows 7, you configure these settings with the Netsh.exe tool.

Configuring Namespace Reservations

Namespace reservation assigns the rights for a portion of the HTTP URL namespace to a particular group of users. A reservation gives those users the right to create services that listen on that portion of the namespace. Reservations are URL prefixes, meaning that the reservation covers all sub-paths of the reservation path. Namespace reservations permit two ways to use wildcards. The HTTP Server API documentation describes the order of resolution between namespace claims that involve wildcards.

A running application can create a similar request to add namespace registrations. Registrations and reservations compete for portions of the namespace. A reservation may have precedence over a registration according to the order of resolution given in the order of resolution between namespace claims that involve wildcards. In this case, the reservation blocks the running application from receiving requests.

Running Windows XP or Server 2003

Use the **httpcfg.exe set urlacl** command to change namespace reservations. The Windows Support Tools documentation explains the syntax for the Httpcfg.exe tool. Modifying the reservation rights for a portion of the namespace requires either administrative privileges or ownership of that portion of the namespace. Initially, the entire HTTP namespace belongs to the local administrator.

The following shows the syntax of the Httpcfg command with the **set urlacl** option

```
httpcfg set urlacl /u {http://URL:Port/ | https://URL:Port/} /aACL
```

The **/u** parameter is required when using **set urlacl**. It takes a string that contains a fully-qualified URL that serves as the record key for the reservation being made.

The **/a** parameter is also required when using **set urlacl**. It takes a string that contains an Access Control List (ACL) in the

form of a Security Descriptor Definition Language (SDDL) string.

The following shows an example of using this command.

```
httpcfg.exe set urlacl /u http://myhost:8000/ /a "O:AOG:DAD:(A;;RPWPCCDCLCSWRCWDWOGA;;;S-1-
0-0)"
```

Running Windows Vista, Windows Server 2008 R2 or Windows 7

If you are running on Windows Vista, Windows Server 2008 R2 or Windows 7, use the Netsh.exe tool. The following shows an example of using this command.

```
netsh http add urlacl url=http://+:80/MyUri user=DOMAIN\user
```

This command adds an URL reservation for the specified URL namespace for the DOMAIN\user account. For more information on using the netsh command type “netsh http add urlacl” in a command-prompt and press enter.

Configuring a Firewall Exception

When self-hosting a WCF service that communicates over HTTP, an exception must be added to the firewall configuration to allow inbound connections using a particular URL. For more information, see Open a port in Windows Firewall (Windows 7)

Configuring SSL Certificates

The Secure Sockets Layer (SSL) protocol uses certificates on the client and server to store encryption keys. The server provides its SSL certificate when a connection is made so that the client can verify the server identity. The server can also request a certificate from the client to provide mutual authentication of both sides of the connection.

Certificates are stored in a centralized store according to the IP address and port number of the connection. The special IP address 0.0.0.0 matches any IP address for the local machine. Note that the certificate store does not distinguish URLs based on the path. Services with the same IP address and port combination must share certificates even if the path in the URL for the services is different.

For step-by-step instructions, see How to: Configure a Port with an SSL Certificate.

Configuring the IP Listen List

The HTTP Server API only binds to an IP address and port once a user registers a URL. By default, the HTTP Server API binds to the port in the URL for all of the IP addresses of the machine. A conflict arises if an application that does not use the HTTP Server API has previously bound to that combination of IP address and port. The IP Listen List allows WCF services to coexist with applications that use a port for some of the IP addresses of the machine. If the IP Listen List contains any entries, the

HTTP Server API only binds to those IP addresses that the list specifies. Modifying the IP Listen List requires administrative privileges.

Running Windows XP or Server 2003

Use the httpcfg tool to modify the IP Listen List, as shown in the following example. The Windows Support Tools documentation explains the syntax for the httpcfg.exe tool.

```
httpcfg.exe set iplisten -i 0.0.0.0:8000
```

Running Windows Vista or Windows 7

Use the netsh tool to modify the IP Listen List, as shown in the following example.

```
netsh http add iplisten ipaddress=0.0.0.0:8000
```

Other Configuration Settings

When using T:System.ServiceModel.WsDualHttpBinding, the client connection uses defaults that are compatible with namespace reservations and the Windows firewall. If you choose to customize the client base address of a dual connection, then you also must configure these HTTP settings on the client to match the new address.

The HTTP Server API has some advanced configuration settings that are not available through HttpCfg. These settings are maintained in the registry and apply to all applications running on the systems that use the HTTP Server APIs. For information about these settings, see Http.sys registry settings for IIS. Most users should not need to change these settings.

Issues Specific to Windows XP

IIS does not support port sharing on Windows XP. If IIS is running and a WCF service attempts to use a namespace with the same port, the WCF service fails to start. IIS and WCF both default to using port 80. Either change the port assignment for one of the services or use the IP Listen List to assign the WCF service to a network adapter not used by IIS. IIS 6.0 and later have been redesigned to use the HTTP Server APIs.

See Also

T:System.ServiceModel.WsDualHttpBinding
How to: Configure a Port with an SSL Certificate

;

© 2016 Microsoft