IBM

SupportPac CA76

CICS TG V9: SSL connectivity for .NET applications

Installation and User Guide
Version 1.0 – Dec 2012

Authors

Paul Crockett, Alex Woodgate, Sue Bayliss
IBM United Kingdom Limited
Hursley Park, Winchester, SO21 2JN

Description

SupportPac CA76 enables the development of .NET Framework applications that can connect to CICS Transaction Gateway (CICS TG) using Secure Sockets Layer (SSL) protocols. The use of SSL provides authentication and encryption capabilities for secure communication between the application and CICS TG.

This SupportPac provides an updated version of the CICS TG V9.0 Application Programming Interface (API) for .NET. The updated API provides a new `SslGatewayConnection` class that can be used in place of the existing `GatewayConnection` class and provides SSL connectivity into CICS TG. Documentation for the API is provided.

There is no support for mapping an X.509 certificate to a RACF user ID when using .NET applications.

System requirements

One of:
–   CICS Transaction Gateway for z/OS V9.0 or later
–   CICS Transaction Gateway for Multiplatforms V9.0 or later
–   CICS Transaction Gateway Desktop Edition V9.0 or later

Any Microsoft Windows operating system supported by CICS TG V9.0 with .NET Framework V3.5 or later.

Skill level required

Application developers must be familiar with developing applications in C#, VB.NET, or other .NET languages. An understanding of SSL technology is preferable.

Supplied files

`IBM.CTG.Client.dll`	.NET assembly containing the SupportPac API
`Samples/`	Sample programs written in C# and VB.NET
`Documentation/`	HTML documentation for the SupportPac API
`License/`	SupportPac license files
`ca76.pdf`	This readme file

Installation

Copy the file `ca76.zip` to a directory on your system. Extract the file contents using a utility that supports the zip format.

Do not extract this SupportPac into the CICS TG installation directory.

Configuring your system environment for SSL

The .NET Framework loads X.509 certificates for SSL authentication from the current user's certificate store and the computer certificate store. If the Gateway daemon is configured to use a self-signed certificate, the certificate must be available in the certificate store used by the client application.

When connecting to a Gateway daemon SSL handler which is configured with client authentication enabled, a certificate for client authentication must be available in the certificate store used by the application. If the client application uses a self-signed certificate, the certificate must be available in the key ring used by the Gateway daemon.

User, service, and computer certificate stores can be managed using the Certificates snap-in for the Microsoft Management Console utility (mmc.exe).

Compiling and using the sample programs

The SupportPac includes ECI and ESI sample programs written in C# and VB.NET. These are updated versions of the sample programs provided with CICS TG that demonstrate the use of the `SslGatewayConnection` class. The ECI sample programs require server programs to be installed on your CICS server. These server programs are provided with CICS TG.

The samples can be compiled using Microsoft Visual Studio 2010 or 2012 using the included Visual Studio project files, or from the command line using the included command files. The command files require the C# compiler (`csc.exe`) or the VB.NET compiler (`vbc.exe`), to be available on the PATH. The C# and VB.NET compilers are included in the .NET Framework.

Application development

To use the SupportPac API in your .NET applications, add a reference to the file
`IBM.CTG.Client.dll`. In Visual Studio, go to **Project → Add Reference... → Browse**, then
select the `IBM.CTG.Client.dll` from the SupportPac and click OK. When compiling from
the command line, use the `/reference` compiler option, as shown in the following examples.

```
csc.exe /reference:<supportpac_path>/IBM.CTG.Client.dll ^
   /target:exe /out:AppName.exe AppName.cs

vbc.exe /reference:<supportpac_path>/IBM.CTG.Client.dll ^
   /target:exe /out:AppName.exe AppName.vb
```

The API provides an `SslGatewayConnection` class that can be used in place of the existing
`GatewayConnection` class for communicating with the Gateway daemon. The
`SslGatewayConnection` class provides different constructors that allow the application to
specify properties for the SSL connection. The properties that can be specified are:
- The SSL and TLS protocols that are allowed for the connection
- One or more client certificates for use when client authentication is enabled
- A callback delegate that selects a specific client certificate to be sent
- A callback delegate that validates the certificate provided by the Gateway daemon

The default properties specify that both Secure Sockets Layer (SSL) 3.0 and Transport
Layer Security (TLS) 1.0 are acceptable for secure communications. Refer to the CICS TG
Information Center for details of the supported versions of the SSL and TLS protocols.

When connecting to a Gateway daemon SSL handler which is configured with client
authentication enabled, one or more client certificates must be specified in the
`SslProperties` object passed to the `SslGatewayConnection` constructor. Client certificates
can be obtained by creating an `X509Store` object, and querying the `Certificates` property.

Documentation for the API is provided in HTML format and can be viewed by opening the
file `<supportpac_path>/Documentation/index.html` in a web browser.

Application deployment

When deploying an application onto another system, the assembly file `IBM.CTG.Client.dll`
must be deployed with the application. The assembly file can be deployed into the same
directory as the application executable, or into the Global Assembly Cache (GAC).

Further details

More information, see the CICS TG V9.0 Information Center:

http://www.ibm.com/software/htp/cics/ctg/library/index.html

Support information can be found on the SupportPac download page:

http://www.ibm.com/support/docview.wss?uid=swg24034001