Release Note

Gallagher Command Centre 'Cardholder Web Service' feature

Gallagher Cardholder Interface Web Service v4.0.0
Gallagher Cardholder Diagnostic Client v7.30.08
Gallagher Command Centre vEL7.30.747
Gallagher Controller 6000 vGR7.30//b374
Gallagher legacy Controllers vBT7.30//b83

Table of Contents

Part 1 Introduction

This release note is for the ‘Cardholder Web Service’ feature of Gallagher Command Centre.

1.1 Purpose

The ‘Cardholder Web Service’ feature enables a third party system to create, remove and modify Cardholders within Command Centre.

Cardholder attributes that can be modified are:

- Cardholder details
- Cardholder authorisation
- Cardholder Personal Data Field values
- Cardholder cards
- Cardholder Competencies
- Cardholder access
- Cardholder user code

For a complete list of specific Cardholder attributes that can be modified, refer to the document *“CardholderWebService_docs.zip/index.html”* supplied with this release.

In addition, this release:

- enables the web service to communicate using the Transport Layer Security (TLS) protocol 1.1 or 1.2. SSL 2.0, SSL 3.0 and TLS 1.0 contain known vulnerabilities.
- enables the web service to detect if a client certificate has been used by more than one IP address and refuse a connection, if required.
- includes a diagnostic tool ‘Cardholder Diagnostic Client’ that enables a third party developer to diagnose connection and configuration issues, when connecting to the Cardholder Web Service.

1.2 Compatibility

The following versions of Gallagher code are required:

- v4.0.0 (or later release) of Gallagher Cardholder Interface Web Service
- v7.30.08 (or later v7.30 release) of Gallagher Cardholder Diagnostic Client
- vEL7.30.747 (or later vEL7.30 release) of Gallagher Command Centre

This feature has been tested using Microsoft Windows 7 (64-bit).

The Cardholder Web Service machine and the Cardholder Diagnostic Client machine require .NET 4.5

This feature has **not** been tested in a Command Centre multi-server environment.

1.3 Identifying Cardholders

It is recommended that Cardholders are identified in Command Centre by use of a unique ID PDF (unique values Personal Data Field). For a Cardholder to receive this PDF, the Cardholder must belong to an Access Group with this PDF assigned.

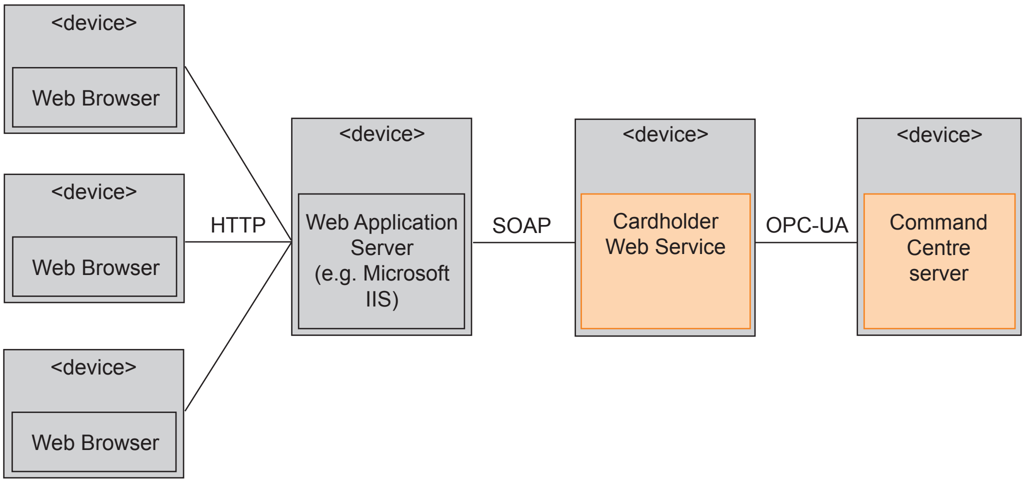
Therefore, it is advised that you create a master Access Group and assign the unique ID PDF to this group. All Cardholders imported using the Cardholder Web Service should be assigned to this group. As Cardholders are added and removed from other Access Groups, ensure the Cardholder always belongs to the master Access Group.

1.4 Deploying the Cardholder Web Service

The Cardholder Web Service can be deployed using one of the following methods.

Method one:
Web Application Server

This method uses a Web Application Server to communicate via SOAP to the Cardholder Web Service. Multiple Web Application Servers can be used, if required.

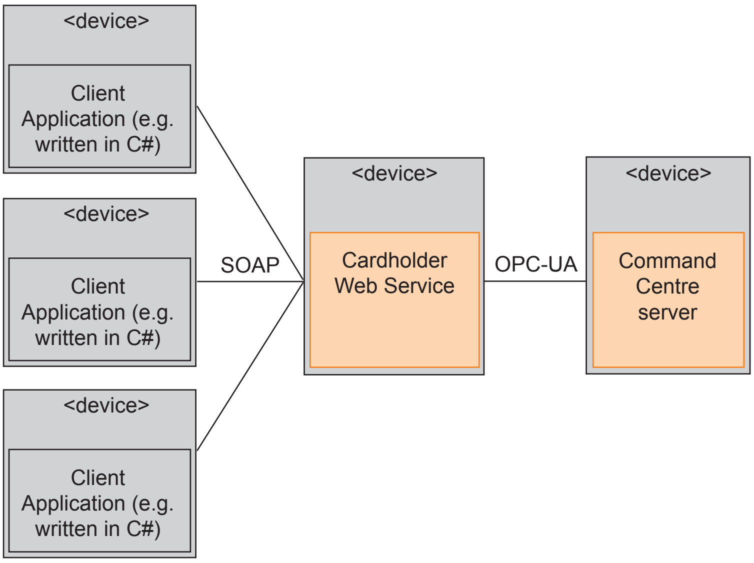


Notes:

- HTTP (Hyper Text Transfer Protocol). A protocol specification for transfering web pages.
- SOAP (Simple Object Access Protocol). A protocol specification for web services.
- IIS (Internet Information Service). Allows ASP.NET components to process SOAP messages.

Method two:
Client Application

This method uses a Client Application (written by the customer) to communicate via SOAP to the Cardholder Web Service. Multiple Client Applications can be used, if required.


<device>
Client Application (e.g. written in C#)
<device>
Client Application (e.g. written in C#)
<device>
Client Application (e.g. written in C#)
SOAP
<device>
Cardholder Web Service
OPC-UA
<device>
Command Centre server

Notes:

- SOAP (Simple Object Access Protocol). A protocol specification for web services.

1.5 OPC-UA connections

Command Centre supports a maximum of 100 simultaneous OPC-UA connections. This means the sum of:

- all running Command Centre Premier clients;
- all running Command Centre Visitor Management kiosks;
- all distinct operator credentials, recently in use with the Visitor Management Web Service, and
- all distinct operator credentials, recently in use with the Cardholder Web Service.

Note: Each web service (Visitor Management or Cardholder) is constrained to a pool of 50 OPC-UA connections. This value is controlled by the key ‘maxOpcuaConnections’ in the configuration file installed with the web service, (i.e. VmifService.exe.config or CifService.exe.config).

In addition, the key ‘opcuaIdleTimeoutMinutes’ is the number of minutes an OPC-UA connection can remain idle before the web service schedules it to shut down. The default value is 60 minutes. This value can be changed.

Part 2 Installation

To install this feature, perform the following procedures:

2.1 Command Centre installation
2.2 Cardholder Web Service installation
2.3 Configure the Windows Firewall to allow OPC-UA access

2.1 Command Centre installation

1. Perform a backup of your Command Centre system.
2. Ensure your licence file contains the following option:

```
[Customisations]
CardholderWebService=1
```

3. Install vEL7.30.747 (or later vEL7.30 release) from the installation DVD, on the Command Centre server and all Command Centre workstations, if not already installed.
4. Ensure the Command Centre server is running. Ensure Command Centre has been configured with a valid system operator, (e.g. Cardholder Web Service Operator). This operator will be used by the Cardholder Web Service to modify Command Centre. Hence this operator must be configured with the appropriate privileges for the FT items being modified by the Cardholder Web Service.

2.2 Cardholder Web Service installation

The ‘Cardholder Web Service’ feature can be installed on the Command Centre server, but for increased security it is recommended that the Cardholder Web Service be installed on a separate server machine.

Note: The web service should not be installed on the same machine as the Gallagher Command Centre Visitor Management client. If you do attempt to run the web service on the same machine, you will be unable to log in to the Visitor Management client.

1. On the web server machine (server hosting the Cardholder Web Service - not the Command Centre server), unzip the customisation folder you have been provided, and run the customisation executable **CardholderInterfaceWebServiceSetup 4.0.0.msi**
   The ‘Welcome’ screen of the Gallagher Cardholder Interface Web Service Setup wizard displays.
2. Click the **Next** button.
   The ‘Gallagher Command Centre’ screen of the installation wizard displays.
3. Enter the Command Centre server name (or IP address) in the **IP or name of the Gallagher Command Centre server** field.

   Note: If you have chosen to install this feature on the Command Centre server machine, enter ‘localhost’.

4. Enter the OPC-UA port number in the **OPCUA Port** field. The default port used is 4840. Continue with the installation.
5. On the 'Installation Complete' screen of the installation wizard, ensure the **Launch Certificate Deployment tool** checkbox is checked, then click the **Finish** button.

2.3 Configure the Windows Firewall to allow OPC-UA access

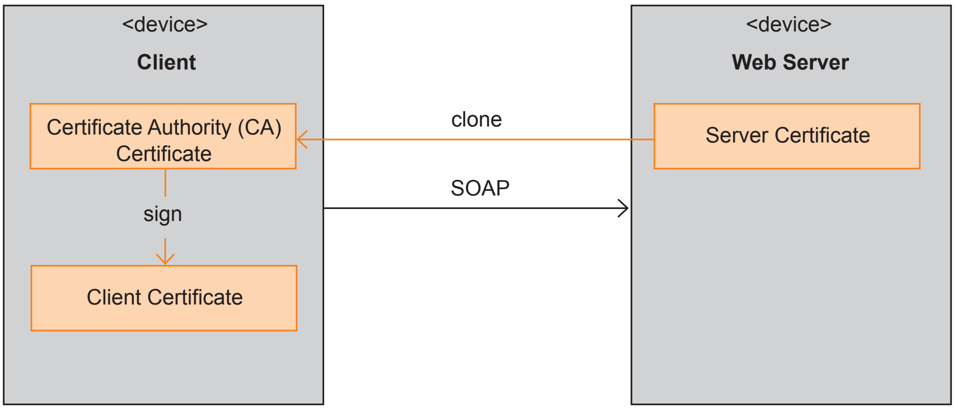
Configure both the Command Centre server and web server Windows Firewalls to allow traffic through the OPC-UA port.

Part 3 The Web Service Certificate Deployment utility

Note: The Web Service Certificate Deployment utility generates all certificates used by the Cardholder Web Service. No certificates are supplied by Gallagher Group Limited and no certificates are present in the installer. Gallagher has no more access to a customer's web service traffic than any other party, and no particular mechanism to recover or restore customer certificates.

3.1 Web server machine certificate

The Web Service Certificate Deployment utility is used to create the Server Certificate. It installs the Server Certificate (HTTPS Certificate) on the web server machine. This certificate is used for authenticating the web server and encrypting its traffic, and for verifying the Client Certificate.



3.2 Client machine certificates

The Web Service Certificate Deployment utility is used to create the Client Certificates. There are two methods available, as described below. It is recommended that you use method one, due to the inherent security of the Windows certificate store.

Method one:
Storing the client machine certificates in the Windows certificate store

The Web Service Certificate Deployment utility can be used to create a Windows certificate store executable. When run, the executable installs the following two certificates in the Windows certificate store:

- The Certificate Authority (CA) Certificate (a clone of the Server Certificate)
- The Client Certificate. This is signed by the Server Certificate (on the web server machine) and so can be used to authenticate the client machine to the web server machine.

Method two:
Exporting the raw certificate files

The Web Service Certificate Deployment utility can be used to export the client machine's raw certificate files. This method allows you to access the certificates without having to use the Windows certificate store. This method should only be used if you are unable to use the Windows certificate store, for example, if you wish to export the certificates to a Linux or other non-Microsoft platform.

Once exported, you can choose to import the certificates into another certificate store or convert them into another format. When converting the certificate, you may be required to enter the certificate's password. This password is automatically generated by the Web Service Certificate Deployment utility and is displayed in the third column of the utility grid.

For details on how to convert a certificate to PEM format, refer to the topic *"Converting an exported certificate to PEM format"* later in this note.

Part 4 Using the Web Service Certificate Deployment utility

To use the Web Service Certificate Deployment utility, perform the following procedures:

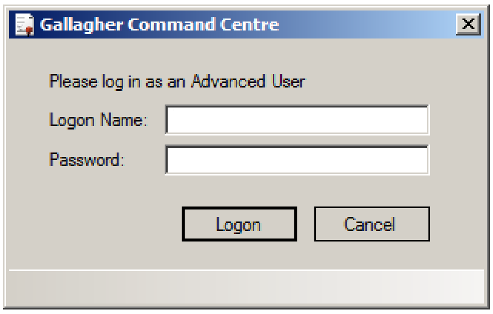
4.1 Configuring the Web Service
4.2 Creating a Client Certificate
4.3 Running the Client Certificate executable
4.4 Verifying the Client Certificate installation

4.1 Configuring the Web Service

1. If not already open, open the Web Service Certificate Deployment utility.

   The Web Service Certificate Deployment utility can be opened from the Windows **Start** menu (Start>All Programs>Gallagher>Web Service Certificate Deployment).

2. When the Web Service Certificate Deployment utility is opened, the Web Service Certificate Deployment utility logon screen displays.



Please log in as an Advanced User

Logon Name:

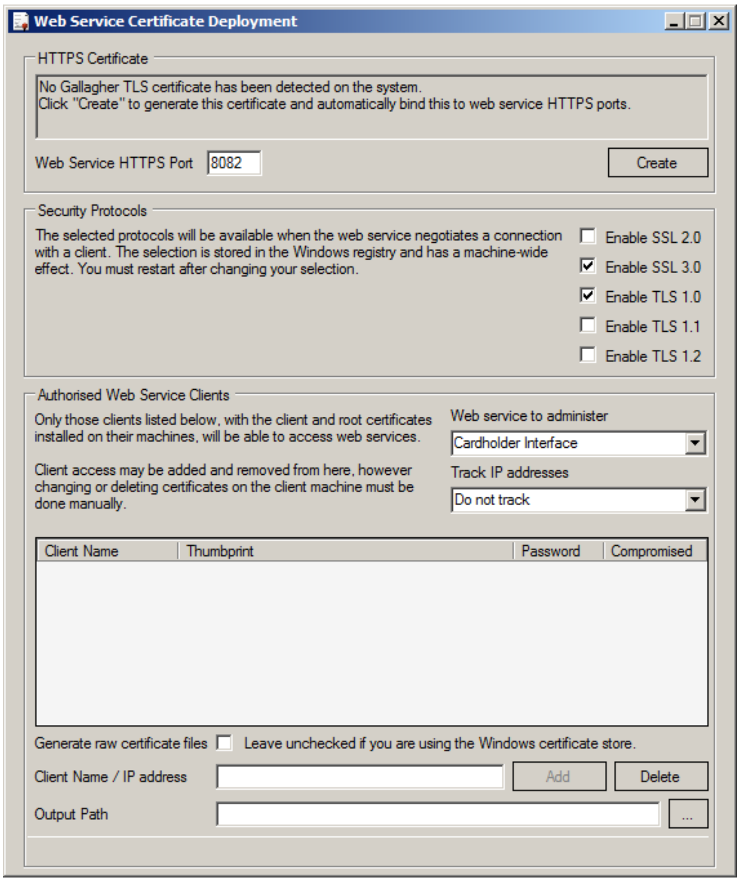
Password:

Note: The purpose of the logon screen is to verify the person using the utility. There is no technical reason for the utility to talk to Command Centre.

3. Ensure the FT Services (for the Command Centre server) are running, then enter a valid Command Centre operator username and password and click the **Logon** button.

   Note: This operator will be used by the Cardholder Web Service to modify Command Centre. Hence this operator must be configured with the appropriate privileges for the FT items being modified by the Cardholder Web Service.

   The Web Service Certificate Deployment utility window opens.



Web Service Certificate Deployment
HTTPS Certificate
Create
Security Protocols
Authorised Web Service Clients
Add
Delete
...

No Gallagher TLS certificate has been detected on the system.
Click "Create" to generate this certificate and automatically bind this to web service HTTPS ports.

Web Service HTTPS Port 8082

The selected protocols will be available when the web service negotiates a connection with a client. The selection is stored in the Windows registry and has a machine-wide effect. You must restart after changing your selection.

☐ Enable SSL 2.0
☑ Enable SSL 3.0
☑ Enable TLS 1.0
☐ Enable TLS 1.1
☐ Enable TLS 1.2

Only those clients listed below, with the client and root certificates installed on their machines, will be able to access web services.

Client access may be added and removed from here, however changing or deleting certificates on the client machine must be done manually.

Web service to administer: Cardholder Interface

Track IP addresses: Do not track

Client Name	Thumbprint	Password	Compromised

Generate raw certificate files ☐ Leave unchecked if you are using the Windows certificate store.

Client Name / IP address

Output Path

4. Select **Cardholder Interface** from the Web service to administer drop-down list.

   Note: The entries shown in this list are controlled by your Command Centre licence file (CommandCentre.lic) and the web interface customisation you have installed.

5. Verify the port you wish to use for the Cardholder Interface in the **Web Service HTTPS Port** field. The HTTPS Certificate will be bound to this port.

   Note: If the Web Service Certificate Deployment utility is run a subsequent time and the certificate already exists then you will be able to bind the certificate to another port.

6. Select the appropriate Security Protocol(s) that will be accepted by the web service. The selection(s) will modify the registry `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols` and has a machine-wide effect.

   Notes:

   - SSL 2.0, SSL 3.0 and TLS 1.0 contain known vulnerabilities.
   - If you have modified the Security Protocol selections, when closing the Web Service Certificate Deployment utility, the utility will restart the machine. A restart is required, in order for the registry modifications to take effect.
   - If you wish to use versions of TLS higher than 1.0, you need to ensure that the web service accepts these protocols by using the Certificate Deployment tool. You may also need to change registry settings under HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols on the client machine and restart it. See http://support.microsoft.com/kb/245030. Depending on the version of Windows, other software running on the machine and other unknowns, this may be unnecessary. These registry changes will affect other software running on the machine.

7. Select the appropriate IP address tracking option, from the **Track IP addresses** drop-down list.

Option	**Description**
Do not track	This is the default option. The client certificate will **not** be bound to the IP address of the client machine. This option should be used for client machines that use dynamic IP addressing (DHCP).
Display compromised certificates	The web service tracks the IP address that the client machine claims to be using. If one certificate is used by more than one IP address, the **Compromised** checkbox is checked and the row is coloured red.
Refuse new clients	In addition to the above display functionality, only the first IP address identified by the web service can be used. Connection attempts by subsequent IP addresses will fail.
Refuse compromised certificates	In addition to the above display functionality, if the web service detects that the certificate has been used by more than one IP address, all connection attempts from any IP address will fail.

8. Click the **Create** button, to create and bind the HTTPS Certificate to the port. If the certificate is successfully created, a confirmation window displays.

   Note: Only the configuration for the web service, (i.e. Cardholder Interface) chosen in the drop-down box will be updated.

9. Click the **OK** button. You can now use the Web Service Certificate Deployment utility to create the Client Certificates.

4.2 Creating a Client Certificate

You will need to create a Client Certificate file for each machine (client machine) that will be using the Cardholder Web Service. The Web Service Certificate Deployment utility can be used to manage the certificates created, however you will need to either manually run the Client Certificate executable (.exe file) or install the raw certificate files on the client machine in order to add the certificates to the client machine. If a machine stops being used as a client, these certificates should be removed manually.

To create a Client Certificate, perform the following procedure:

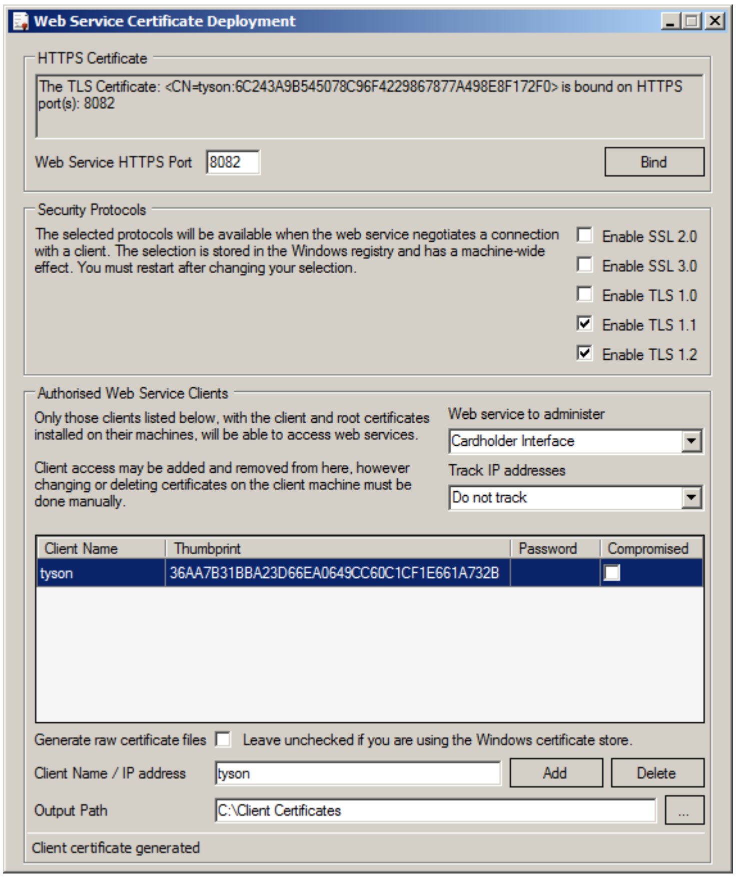
1. Open the Web Service Certificate Deployment utility.
2. If not already done, create an HTTPS Certificate and bind it to the port that will be used by the Cardholder Web Service. Refer to the topic *“Configuring the Web Service”* for details.
3. Select **Cardholder Interface** from the Web service to administer drop-down list.
4. It is advised that you store the Client Certificate in the Windows certificate store. If doing so, go to Step 5. If you will not be using the Windows certificate store, check the **Generate raw certificate files** checkbox, then go to Step 5.
5. Enter the client machine name (or IP address) in the **Client Name / IP address** field.

   Note: The value entered is used to name the Client Certificate, and logged by the Cardholder Web Service during connect and disconnect attempts. It is recommended that you use a unique name for each Client Certificate, for ease of troubleshooting.

6. Enter the output location for the Client Certificate executable or raw certificate files in the **Output Path** field, (e.g. C:\Client Certificates).
7. Click the **Add** button.

   - If using the Windows certificate store, the client machine name and certificate thumbprint is listed in the Web Service Certificate Deployment utility list. The Client Certificate executable ‘GallagherWebServiceClientCertificate[*ClientName*].exe’ is created in the nominated directory.
   - If using raw certificate files, the client machine name, certificate

thumbprint and certificate password is listed in the Web Service Certificate Deployment utility list. The raw certificate files ‘GallagherWebServicesClientCertificate[*ClientName*].pfx’ and ‘GallagherWebServicesRootCertificate[*ClientName*].cer’ are created in the nominated directory.



Web Service Certificate Deployment

HTTPS Certificate

The TLS Certificate: <CN=tyson:6C243A9B545078C96F4229867877A498E8F172F0> is bound on HTTPS port(s): 8082

Web Service HTTPS Port: 8082

Security Protocols

The selected protocols will be available when the web service negotiates a connection with a client. The selection is stored in the Windows registry and has a machine-wide effect. You must restart after changing your selection.

☐ Enable SSL 2.0
☐ Enable SSL 3.0
☐ Enable TLS 1.0
☑ Enable TLS 1.1
☑ Enable TLS 1.2

Authorised Web Service Clients

Only those clients listed below, with the client and root certificates installed on their machines, will be able to access web services.

Client access may be added and removed from here, however changing or deleting certificates on the client machine must be done manually.

Web service to administer: Cardholder Interface

Track IP addresses: Do not track

Client Name	Thumbprint	Password	Compromised
tyson	36AA7B31BBA23D66EA0649CC60C1CF1E661A732B		☐

Generate raw certificate files ☐ Leave unchecked if you are using the Windows certificate store.

Client Name / IP address: tyson

Output Path: C:\Client Certificates

Client certificate generated

4.3 Running the Client Certificate executable

Note: This procedure is only applicable if using the Windows certificate store.

You will need to run the generated Client Certificate executable ‘GallagherWebServiceClientCertificate[*ClientName*].exe’ on the client machine. When the executable is run, the Client Certificate will be added to the client machine’s Windows certificate store.

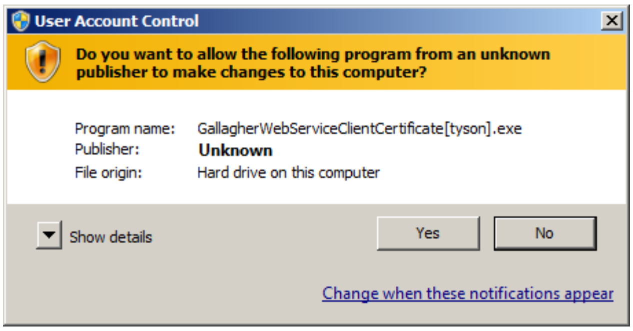
To install the Client Certificate, perform the following procedure:

Important: The Security Protocols selected when the certificate executable was generated will modify the registry `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols` on the client machine. The client installer will prompt you to restart the client machine. A restart is required, in order for the registry modifications to take effect.

1. Double click the generated Client Certificate executable.

   Ensure you have the appropriate privileges required to update the client machine’s Windows certificate store. If run without the appropriate privileges, you may be presented with the following User Account Control warning. Alternatively, you may be required to enter the appropriate Windows credentials.

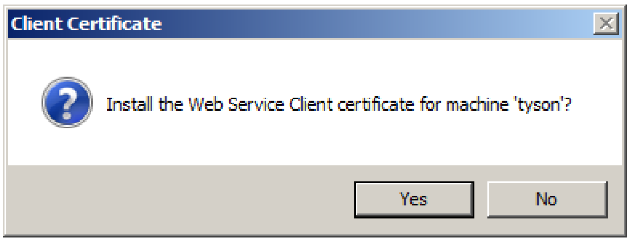
Note: The publisher is unknown because the executable is generated dynamically (not statically predefined) by the Web Service Certificate Deployment utility.



Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: GallagherWebServiceClientCertificate[tyson].exe
Publisher: **Unknown**
File origin: Hard drive on this computer

2. Click the **Yes** button to continue.
   The Client Certificate window displays.



Install the Web Service Client certificate for machine 'tyson'?

3. Check to ensure the correct Client Certificate is being installed on the correct client machine, then click the **Yes** button.
   A confirmation window displays.

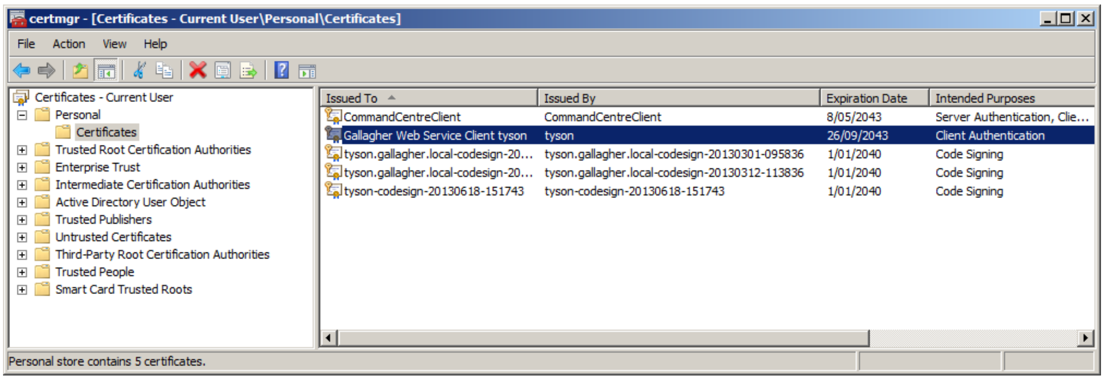
4. Click the **OK** button.

4.4 Verifying the Client Certificate installation

Note: This procedure is only applicable if using the Windows certificate store.

To verify the Client Certificate installation, open the Microsoft Certificate Manager. To open the Microsoft Certificate Manager, enter **certmgr.msc** into the Windows run field.

The Client Certificate is located in the ‘Certificates - Current User\Personal\Certificates’ store. All certificates generated by the Certificate Deployment utility use “Gallagher Web Service” in their Friendly Name field.



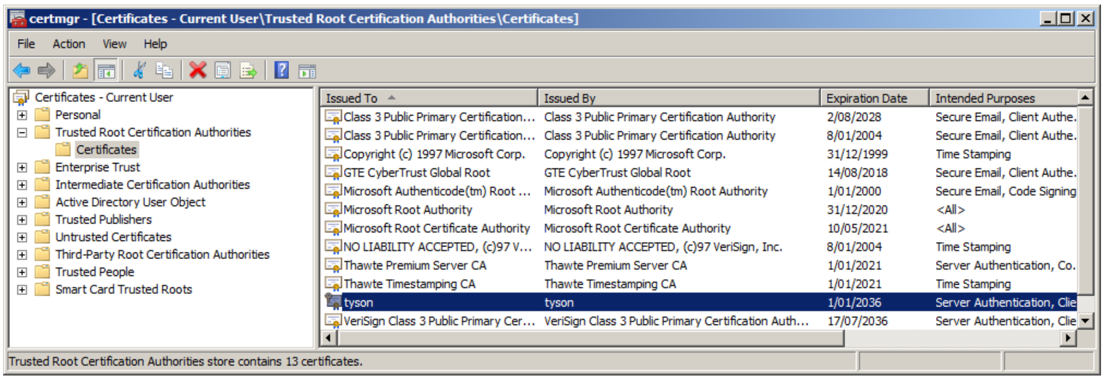
certmgr - [Certificates - Current User\Personal\Certificates]

- Certificates - Current User
  - Personal
    - Certificates
  - Trusted Root Certification Authorities
  - Enterprise Trust
  - Intermediate Certification Authorities
  - Active Directory User Object
  - Trusted Publishers
  - Untrusted Certificates
  - Third-Party Root Certification Authorities
  - Trusted People
  - Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes
CommandCentreClient	CommandCentreClient	8/05/2043	Server Authentication, Clie...
Gallagher Web Service Client tyson	tyson	26/09/2043	Client Authentication
tyson.gallagher.local-codesign-20...	tyson.gallagher.local-codesign-20130301-095836	1/01/2040	Code Signing
tyson.gallagher.local-codesign-20...	tyson.gallagher.local-codesign-20130312-113836	1/01/2040	Code Signing
tyson-codesign-20130618-151743	tyson-codesign-20130618-151743	1/01/2040	Code Signing

Personal store contains 5 certificates.

The Certificate Authority (CA) Certificate is located in the ‘Certificates\Trusted Root Certificate Authorities\Certificates’ store. All certificates generated by the Certificate Deployment utility use “Gallagher Web Service” in their Friendly Name field.



certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]

- Certificates - Current User
  - Personal
  - Trusted Root Certification Authorities
    - Certificates
  - Enterprise Trust
  - Intermediate Certification Authorities
  - Active Directory User Object
  - Trusted Publishers
  - Untrusted Certificates
  - Third-Party Root Certification Authorities
  - Trusted People
  - Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes
Class 3 Public Primary Certification...	Class 3 Public Primary Certification Authority	2/08/2028	Secure Email, Client Authe.
Class 3 Public Primary Certification...	Class 3 Public Primary Certification Authority	8/01/2004	Secure Email, Client Authe.
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	31/12/1999	Time Stamping
GTE CyberTrust Global Root	GTE CyberTrust Global Root	14/08/2018	Secure Email, Client Authe.
Microsoft Authenticode(tm) Root ...	Microsoft Authenticode(tm) Root Authority	1/01/2000	Secure Email, Code Signing
Microsoft Root Authority	Microsoft Root Authority	31/12/2020	<All>
Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	10/05/2021	<All>
NO LIABILITY ACCEPTED, (c)97 V...	NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.	8/01/2004	Time Stamping
Thawte Premium Server CA	Thawte Premium Server CA	1/01/2021	Server Authentication, Co.
Thawte Timestamping CA	Thawte Timestamping CA	1/01/2021	Time Stamping
tyson	tyson	1/01/2036	Server Authentication, Clie
VeriSign Class 3 Public Primary Cer...	VeriSign Class 3 Public Primary Certification Auth...	17/07/2036	Server Authentication, Clie

Trusted Root Certification Authorities store contains 13 certificates.

Part 5 Converting an exported certificate to PEM format

To convert a PFX certificate to PEM format, perform the following procedure using OpenSSL:

Note: This step is not applicable if using the Windows certificate store. This method enables you to use the Cardholder Web Service with the scripting language PHP, refer to the Appendix for further details.

1. Openssl pkcs12 -in “C:\Certificates\GallagherWebServicesClientCertificate[10.60.70.10].pfx” -out “C:\Certificates\GallagherWebServicesClientCertificate[10.60.70.10].pem” –clcerts

2. Enter the Import Password (password from the Web Service Certificate Deployment utility), for example: QSVvILQQjFEaGg

3. MAC verified OK

4. Enter PEM pass phrase (your own pass phrase), for example: sn00py

5. Verifying - Enter PEM pass phrase (your own pass phrase), for example: sn00py

To convert a PFX certificate to CA PEM format, perform the following procedure using OpenSSL:

1. openssl pkcs12 -in “C:\Certificates\GallagherWebServicesClientCertificate[10.60.70.10].pfx” -out “C:\Certificates\GallagherWebServicesRootCertificate[10.60.70.10].pem” –cacerts
2. Enter the Import Password (password from the Web Service Certificate Deployment utility), for example: QSVvILQQjFEaGg
3. MAC verified OK
4. Enter PEM pass phrase (your own pass phrase), for example: sn00py
5. Verifying - Enter PEM pass phrase (your own pass phrase), for example: sn00py

Part 6 Notes for administrators

The following points are relevant for administrators who will administer the running software for the ‘Cardholder Web Service’ feature:

- Administrators are largely responsible for securing the ‘Cardholder Web Service’ feature. During startup, the web service reads the available ciphers from the registry of the server on which it is running. If the registry lists ciphers the web service thinks are obsolete or insecure, the web service will log warnings. For example:

  “The following cipher appears to be available in Windows but is not sufficiently secure. If it has been disabled by a group security policy, this message can be ignored. SSL_CK_DES_192_EDE3_CBC_WITH_MD5”.

  It is up to the system administrator to decide what to do about them, they can only be disabled on a machine-wide basis by registry key or group security policy. This may affect other software on the machine. A system administrator may choose group security policy as the safer alternative to editing the registry, but the web service does not notice and will continue to issue warnings.

  Note: The web service will run correctly in spite of these warnings, but it may not be as secure as required.

- Any changes made using the Web Service Certificate Deployment utility will not be noticed by the web service until the web service is restarted. Binding the Server Certificate to a port happens immediately, as that’s an operating system execution, but the web service only reads its configuration at startup.
- The web service machine’s registry and certificate stores must be kept secure as unauthorised access could impact security. Likewise, the following files must also be kept secure:
  - the exes and dlls
  - the config file **CifService.exe.config**
  - any raw certificate files or executables generated by the Web Service Deployment utility. These files are particularly important, as they are

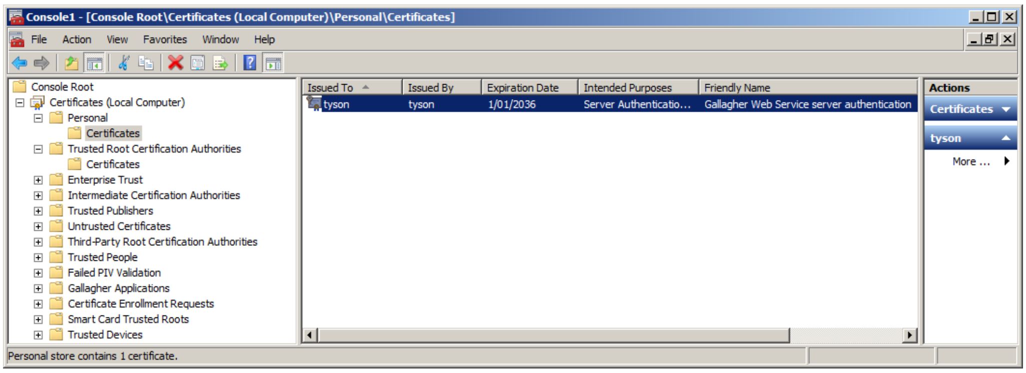
intended to be created on the web server machine, taken to the client machine(s) and installed there. They must be transported in a secure fashion, installed, and securely deleted from the client(s). They should be either destroyed entirely or archived securely for their lifetime. If a copy was installed on a rogue machine, that machine would be able to authenticate itself with the web server. A rogue client would still need a Command Centre username and password to successfully make web service calls.

- To revoke a Client Certificate, you can use the Web Service Certificate Deployment utility. This utility can also be used to revoke the Server Certificate, which would have the effect of revoking all the Client Certificates, as they were all signed by it.
- A web-service client establishes a session by supplying a Command Centre operator login and password to a “connect” method. Upon successful log in a session token is returned. The session token must be supplied in subsequent calls to the other web-service methods.

  The session will have a restricted life-span. The life-span is configurable by the administrator of the web-service machine (see **CifService.exe.config**). By default, session life-span is 15 minutes. There are two session timeout keys, “sessionRetireTimeoutMinutes” and “sessionDestroyTimeoutDays”, both are commented with their purpose and valid values.
- If you restart the Command Centre services, you will also need to restart the ‘FT Gallagher Cardholder Web Service’. This will not happen automatically, as it may not be on the same machine.
- The web service logs information in the file: C:\ProgramData\Gallagher\Command Centre\CifWebServiceLog.txt
- The ‘Cardholder Web Service’ feature can become unresponsive due to information being deleted in Command Centre, with the Web Service not receiving/acknowledging the notification.

  If this occurs, restarting the Web Service will fix the problem, as long as the two workarounds described above are in place then no other ill effects should be apparent.
- If the web service or a client of the web service has been installed on a Command Centre workstation and the log file *“CifWebServiceLog.txt”* has logged the error *“Logon error Opc.Ua.ServiceResultException: BadIdentityTokenRejected”*, ensure all unused web service certificates have been removed from the certificate store and restart both Command Centre and the web service.
- Only one server certificate should be present on the server machine. The certmgr.msc allows you to view the certificates installed in the current user store but not the local machine store.

  To view the certificates in the local machine store run mmc.exe (as admin) and add the snapin named “Certificates” and point it to your local machine (server machine). All certificates generated by the Certificate Deployment utility use “Gallagher Web Service” in their Friendly Name field.



Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

- Console Root
  - Certificates (Local Computer)
    - Personal
      - Certificates
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Failed PIV Validation
    - Gallagher Applications
    - Certificate Enrollment Requests
    - Smart Card Trusted Roots
    - Trusted Devices

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
tyson	tyson	1/01/2036	Server Authenticatio...	Gallagher Web Service server authentication

Personal store contains 1 certificate.

- If a web service operator on a client machine attempts to connect to the web service using an incorrect/invalid login and a second web service operator on a second client machine attempts to connect to the web service using a correct/valid login, the second operator will receive the message *"Could not establish a session with Command Centre using the web service. Unable to log into Command Centre: UserAccessDenied"*. The second operator will need to wait approximately 3 minutes for the incorrect/invalid login to timeout.
- If the web service detects a compromised certificate, the IP address tracking functionality chosen in the Web Service Certificate Deployment utility is actioned immediately. However, the display grid in the utility is updated when restarted.

Part 7 Notes for developers

The following points are relevant for developers who will write client software for the 'Cardholder Web Service' feature:

- The 'Cardholder Web Service' feature uses SOAP v1.1 and is written in WCF and .NET. It uses Microsoft's `basicHttpBinding`.
- If you are writing client software in WCF and .NET, you may find `CardholderInterface.dll` and `CommonContract.dll` useful to include in your project. It contains the interface and classes from which the web service's WSDL was generated, and can be re-used on the client for slightly cleaner code than what Visual Studio generates from the WSDL.
- A separate document *"CardholderWebService_docs_v7_30_xx.zip/index.html"* is available as a guide to help developers design and write software that interfaces with the 'Cardholder Web Service' feature.

Part 8 Limitations

- The web service will consume a Command Centre Premier client licence.
- The web service should not be installed on the same machine as the Gallagher Command Centre Visitor Management client. If you do attempt to run the web service on the same machine, you will be unable to log in to the Visitor Management client.

- If the web service is installed on the Command Centre server and if you uncheck SSL 3.0 or TLS 1.0, SQL Server will no longer start. Hence Command Centre will be unusable.

Part 9 Uninstallation

To permanently uninstall this feature, perform the following procedure:

1. Stop the FT Gallagher Cardholder Web Service.
2. Perform a backup of your Command Centre system.
3. Exit Command Centre and stop the FT Services.
4. Remove the Server Certificate (HTTPS Certificate) from both the Current User and Local Computer certificate stores on the server machine:
   - Certificates - Current User\Trusted Root Certification Authorities\Certificates
   - Certificates - Local Computer\Trusted Root Certification Authorities\Certificates

   Remove the all Client Certificates from both the Current User and Local Computer certificate stores on all client machines:
   - Certificates - Current User\Personal\Certificates
   - Certificates - Local Computer\Personal\Certificates

   Note: For details on how to remove a certificate from the Local Computer certificate store, refer to the section *"Notes for administrators*".
5. Using the Windows **Programs and Features** utility, remove the program 'Gallagher Cardholder Interface Web Service' from the web server machine.
6. Restart the FT Services.

Part 10 Upgrading

To upgrade the 'Cardholder Web Service' feature, perform one of the following procedures:

10.1 Upgrade procedure (removes all previously generated certificates)
10.2 Upgrade procedure (preserves all previously generated certificates)

10.1 Upgrade procedure (removes all previously generated certificates)

This upgrade procedure requires you to remove all previously generated certificates.

1. Stop the FT Gallagher Cardholder Web Service.
2. Perform a backup of your Command Centre system.
3. Exit Command Centre and stop the FT Services.
4. Remove the Server Certificate (HTTPS Certificate) from both the Current User

and Local Computer certificate stores on the server machine:

- Certificates - Current User\Trusted Root Certification Authorities\Certificates
- Certificates - Local Computer\Trusted Root Certification Authorities\Certificates

Remove the all Client Certificates from both the Current User and Local Computer certificate stores on all client machines:

- Certificates - Current User\Personal\Certificates
- Certificates - Local Computer\Personal\Certificates

Note: For details on how to remove a certificate from the Local Computer certificate store, refer to the section *“Notes for administrators*”.

5. Using the Windows **Programs and Features** utility, remove the program ‘Gallagher Cardholder Interface Web Service’ from the web server machine.
6. Restart the FT Services.
7. On the web server machine (server hosting the Cardholder Web Service - not the Command Centre server), unzip the customisation folder you have been provided, and run the customisation executable **CardholderInterfaceWebServiceSetup.msi**
   The ‘Welcome’ screen of the Gallagher Cardholder Interface Web Service Setup wizard displays.
8. Click the **Next** button.
   The ‘Gallagher Command Centre’ screen of the installation wizard displays.
9. Enter the Command Centre server name (or IP address) in the **IP or name of the Gallagher Command Centre server** field.

   Note: If you have chosen to install this feature on the Command Centre server machine, enter ‘localhost’.
10. Enter the OPC-UA port number in the **OPCUA Port** field. The default port used is 4840. Continue with the installation.
11. On the ‘Installation Complete’ screen of the installation wizard, ensure the **Launch Certificate Deployment tool** checkbox is checked, then click the **Finish** button.
12. Log on to the Web Service Certificate Deployment utility.
13. Re-create the Server Certificate (HTTPS Certificate), refer to the topic *“Creating a Server Certificate (HTTPS Certificate)”* earlier in this release note.
14. Re-create all Client Certificates, refer to the topic *“Creating a Client Certificate“* earlier in this release note.
15. Re-deploy all Client Certificates.
16. Start the ‘FT Gallagher Cardholder Web Service’.

    Note: This service has a delayed startup.

10.2 Upgrade procedure (preserves all previously generated certificates)

Pros and cons of this upgrade are:

Pro: You don't need to generate new certificates during the upgrade or distribute them to client machines.

Pro: If you do it enough times, its actually quicker.

Con: Its more complex.

Con: Its more prone to error. Errors may leave the web service unable to start or clients unable to connect or both.

Con: Certificates from previous versions of the Certificate Deployment utility will not work with TLS 1.2. The web service will fall back to an older protocol if one is available, otherwise fail to negotiate a connection.

1. Stop the FT Gallagher Cardholder Web Service. Do not stop the FT Services.
2. Perform a backup of your Command Centre system.
3. Copy of the web service's XML configuration file, normally located at: C:\Program Files (x86)\Gallagher\Cardholder Web Service**CifService.exe.config.** Treat this copy securely.
4. Using the Windows **Programs and Features** utility, remove the program 'Gallagher Cardholder Interface Web Service' from the web server machine.
5. On the web server machine (server hosting the Cardholder Web Service - not the Command Centre server), unzip the customisation folder you have been provided, and run the customisation executable **CardholderInterfaceWebServiceSetup.msi**
   The 'Welcome' screen of the Gallagher Cardholder Interface Web Service Setup wizard displays.
6. Click the **Next** button.
   The 'Gallagher Command Centre' screen of the installation wizard displays.
7. Enter the Command Centre server name (or IP address) in the **IP or name of the Gallagher Command Centre server** field.

   Note: If you have chosen to install this feature on the Command Centre server machine, enter 'localhost'.
8. Enter the OPC-UA port number in the **OPCUA Port** field. The default port used is 4840. Continue with the installation.
9. On the 'Installation Complete' screen of the installation wizard, ensure the **Launch Certificate Deployment tool** checkbox is **unchecked**, then click the **Finish** button. You do not need to use the Certificate Deployment utility.
10. Copy the file **CifService.exe.config** back into its proper location, overwriting the default file just installed. This should require elevated permissions.
11. Start the FT Gallagher Cardholder Web Service.

    Note: This service has a delayed startup.

Part 11 The Cardholder Diagnostic Client

This section of the release note is for the Cardholder Diagnostic Client.

11.1 Purpose

The Cardholder Diagnostic Client is a connection status tool, that enables a third party developer to diagnose connection and configuration issues, when connecting to the Cardholder Web Service.

The Cardholder Diagnostic Client installs sample code in C# and Java.

11.2 Compatibility

The Cardholder Diagnostic Client is compatible with the Gallagher Cardholder Interface Web Service v4.0.0 (or later release).

11.3 Installation

Note: You will need to configure the Cardholder Web Service prior to using the Cardholder Diagnostic Client.

1. On the client machine that will be using the Cardholder Web Service, unzip the customisation folder you have been provided, and run the executable **Gallagher Cardholder Diagnostic Client Setup 7.30.08.msi**

   The 'Welcome' screen of the Gallagher Cardholder Diagnostic Client Setup Wizard displays.

2. Click the **Next** button.

   The 'Destination Folder' screen of the installation wizard displays.

3. Enter the installation destination folder, or alternatively select an installation destination folder, by selecting the **Change...** button.

4. Click the **Next** button.

   The 'Ready to install Gallagher Cardholder Diagnostic Client' screen of the installation wizard displays.

5. Click the **Install** button. The Cardholder Diagnostic Client will install. Once installed, the 'Installation Complete' screen of the installation wizard displays.

6. Click the **Finish** button.

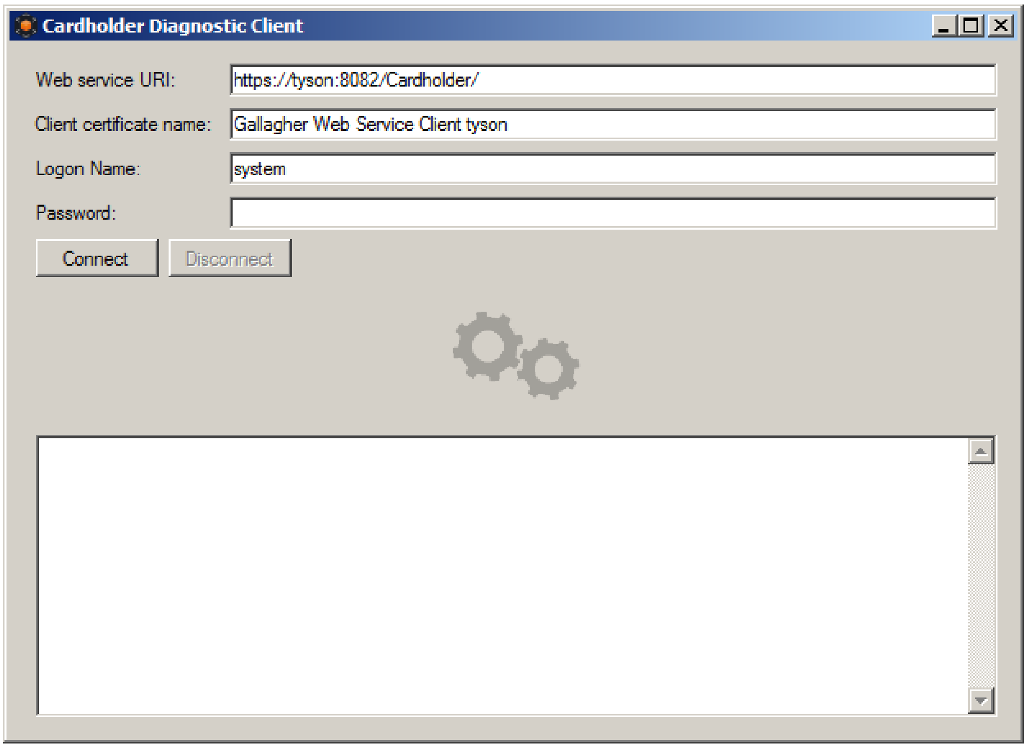
7. To ensure that the Cardholder Diagnostic Client has installed correctly, select the **Programs and Features** utility from the Windows/Control Panel on the client machine. The program 'Gallagher Cardholder Diagnostic Client' should be listed as currently installed.

11.4 Using the Cardholder Diagnostic Client

To use the Cardholder Diagnostic Client, perform the following procedure:

1. Open the Cardholder Diagnostic Client.

   The Cardholder Diagnostic Client can be opened from the Windows **Start** menu (Start>All Programs>Gallagher>Cardholder Web Service Diagnostic Client). The Cardholder Diagnostic Client displays.



Web service URI: https://tyson:8082/Cardholder/

Client certificate name: Gallagher Web Service Client tyson

Logon Name: system

Password:

2. Complete the fields as described in the following table.

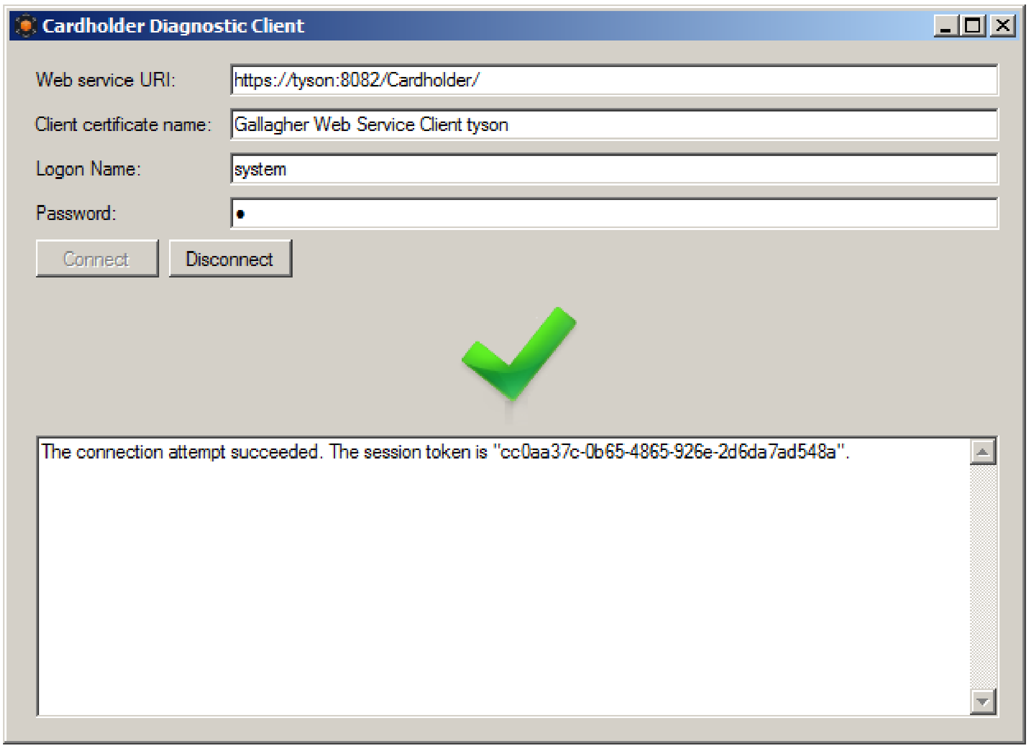
Field	Description
Web service URI	Enter the web service Uniform Resource Identifier (URI). **Note:** The web service URI is logged during web service start-up to the file *C:\ProgramData\Gallagher\Command Centre\CifWebServiceLog.txt*
Client certificate name	Enter the client certificate name. To locate the name of the client certificate, refer to the topic *"Verifying the Client Certificate installation"* earlier in this release note. **Note:** If you leave the client certificate name as the default, it will work if only one client certificate is installed.
Logon name	Enter the username of the Command Centre operator used to run the web service.
Password	Enter the password of the Command Centre operator used to run the web service.

3. Ensure the ‘FT Services’ (on the Command Centre server) are running.

4. Ensure the ‘FT Gallagher Cardholder Web Service’ is running.
   Note: This service has a delayed startup.

5. Click the **Connect** button. Wait as the diagnostic tool attempts a connection.

   If the connection is successful, a green tick and session token is displayed.



Web service URI: https://tyson:8082/Cardholder/

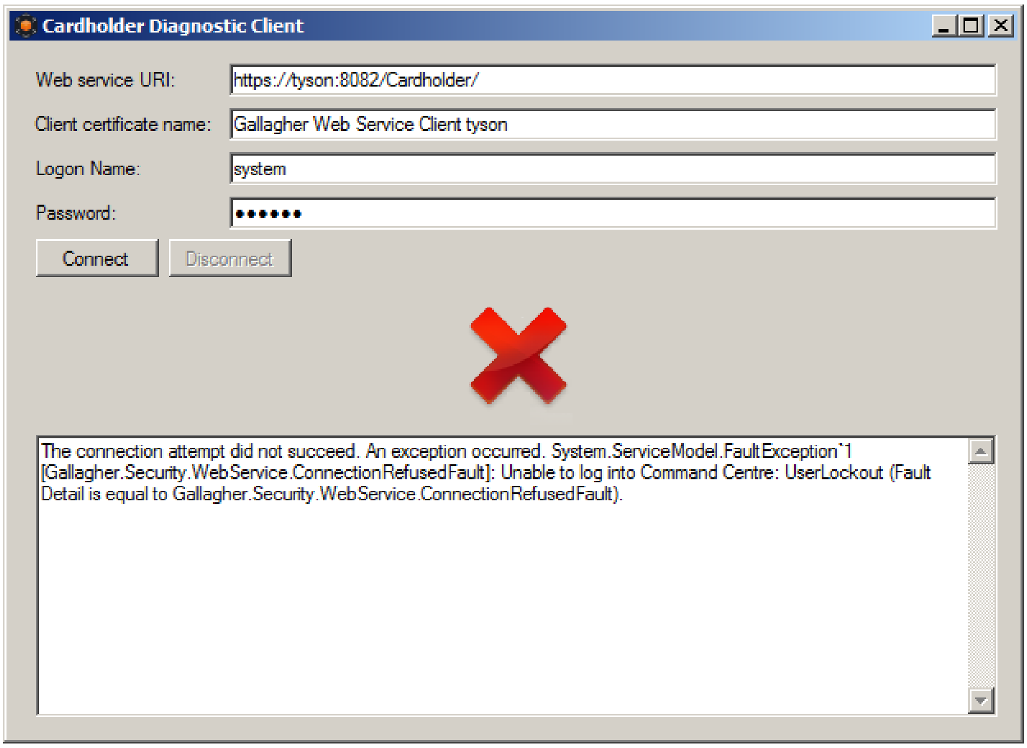
Client certificate name: Gallagher Web Service Client tyson

Logon Name: system

Password: •

```
The connection attempt succeeded. The session token is "cc0aa37c-0b65-4865-926e-2d6da7ad548a".
```

If the connection is unsuccessful, a red cross and error diagnostics are displayed.



Web service URI: https://tyson:8082/Cardholder/

Client certificate name: Gallagher Web Service Client tyson

Logon Name: system

Password: ••••••

```
The connection attempt did not succeed. An exception occurred. System.ServiceModel.FaultException`1
[Gallagher.Security.WebService.ConnectionRefusedFault]: Unable to log into Command Centre: UserLockout (Fault
Detail is equal to Gallagher.Security.WebService.ConnectionRefusedFault).
```

Note: Resize the application to view the error diagnostics in a cleaner format.

11.5 Logging

The Cardholder Diagnostic Client logs information in the file:
C:\Users\<Username>\AppData\Local\Gallagher\Command Centre\
CifDiagnosticClient.log

11.6 Uninstallation

To uninstall the Cardholder Diagnostic Client, using the Windows **Programs and Features** utility, remove the program ‘Gallagher Cardholder Diagnostic Client’ from the client machine.