System Galaxy Addendum

GCS Web API Setup Guide

- Configuring the GCS Web API Settings for encrypted communication.
- Creating Web API Connection credentials.
- Adding a signed SSL Certificate to the Web Server.

SG 11.8.6 (or newer)

AUGUST 2024

Contents

Introduction to the GCS Web API

This guide covers how to install and set up the Web API for System Galaxy.

System Galaxy's **Web API Interface** supports both *System Galaxy API Applications* and *3rd-Party API Apps. This support* includes *Active Directory, LaunchPoint Web Client*, *Galaxy Mobile Apps*, and *idProducer Badging solution, 3rd-Party Video Plug-in apps*, *3rd-Party Elevator apps, and other 3rd-Party solutions*.

During the installation, System Galaxy (v11.8.6 or higher) automatically creates a reserved ***Web API Login,*** that is only used for fundamental API operations that are exclusive to the System Galaxy software. This reserved *Web API User Login* should not be shared or used by any API apps or by 3rd-Party User Logins.

All Galaxy API Apps and 3rd-Party API Apps must create their own *SG Operator Login* that is configured with the appropriate settings and permissions needed to support the operation of their application.

FEATURED TOPICS …

- Configure Web Services during the SG Software Installation
- Creating a custom Web API User Account in SG Operator screen (if needed).
- *Configure Web API AppSettings file.*
- *Configure SQL Server ConnectionStringsPDSA file*
- *Configure SQL Server ConnectionStrings file*
- Obtaining a Certificate
- Importing a Signed Certificate
- Verifying the Certificate Key
- Repairing a Missing Certificate Key
- Capturing the Certificate Thumbprint
- Adding the Certificate Thumbprint to the Batch File
- Editing the Delete Certificate Batch file
- Adding the Certificate to the Web API Service (SSL Setup batch file)

  (including Deleting an Expired Certificate)

Configuring Web Services Settings during SG Installation

During Part-3 of the System Galaxy software installation, the dealer can configure the port number(s) and Session Timeout for the *Web Services*. If SG is already installed, these values can be changed in the appSettings config file.

In SG 11.8.6 (or higher), SG Installer will silently create a ***reserved Web API User*** ("SGApiUser" & random password). The Web API User Login account is silently added to the SG database (operators table) and to appSettings config file.

NOTICE: SG 11.8.5 (or older), the dealer could see and change the Web API User Login (name/password) in Web Services window.

PREREQUISITES

- You must have installed Steps 1 and 2 of the System Galaxy installation.
- You should know the HTTP/HTTPS Port Number the customer wants to use for Web API connections.
- Notice that an *HTTPS Secure Socket* requires the end-user to purchase/install an authentic Signed Certificate for the Web API Service. Galaxy recommends getting the longest certificate possible to avoid it expiring in only one year. *Later sections of this guide cover how to obtain and install a signed certificate*.

STEPS

1. During Part-3 of the System Galaxy software install, you will encounter the ***Web Services Settings screen***.

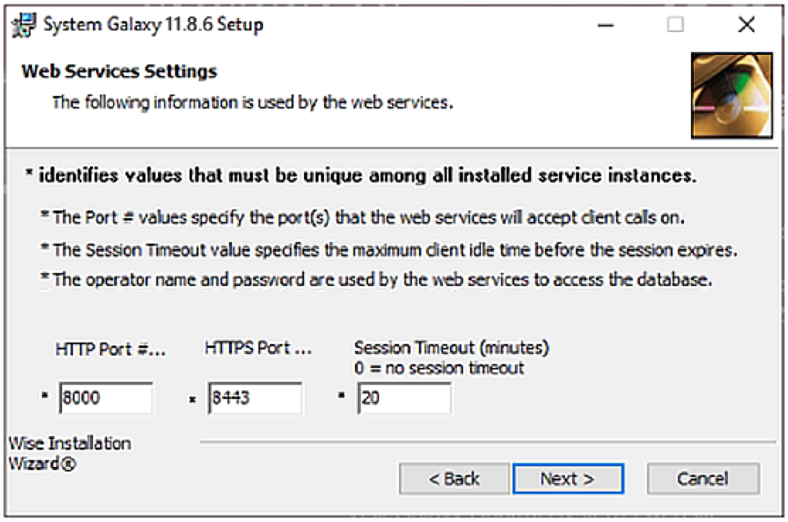
2. If you want to change the Web Settings, edit the following fields as needed …

   a) Set the appropriate **Port Number** in the HTTP or HTTPS field, as needed.

   b) Recommended to set the **Session Timeout** to "20" (default). Setting a "0" means no timeout.

   c) The reserved *Web API User Login* is no longer visible or programmable in this screen as of v11.8.6.

   NOTICE: SG 11.8.6 (or higher), the **Web API User** ("SGApiUser" & random password) is silently created and added to the SG database (system operator table). In SG 11.8.5 or below, you must enter the username and password in this screen and then create the system operator account in System Galaxy software after the installation is completed. The username and password are case-sensitive and must match exactly.



System Galaxy 11.8.6 Setup

Web Services Settings

The following information is used by the web services.

* identifies values that must be unique among all installed service instances.

* The Port # values specify the port(s) that the web services will accept client calls on.

* The Session Timeout value specifies the maximum client idle time before the session expires.

* The operator name and password are used by the web services to access the database.

HTTP Port #... : * 8000

HTTPS Port ... : * 8443

Session Timeout (minutes) 0 = no session timeout : * 20

3. Click **Next** to accept changes (or to keep the default settings) as desired.

4. Click **Finish** to complete the installation.

Adding a *API User Login* (System Operator) for API-based Apps

This topic describes how to add an *API User Login* for any 3rd-Party or proprietary API-based App (application).

Do <u>not</u> use the reserved *SGApiUser login* to operate your 3rd-Party or proprietary API Apps. The SGApiUser login is exclusively reserved for System Galaxy internal operations. In SG 11.8.6 or higher the SGApiUser login and operator account are automatically created. In SG 11.8.5 or lower the installer must set the Username and Password during the installation and must manually create the User Account in the system operator screen.

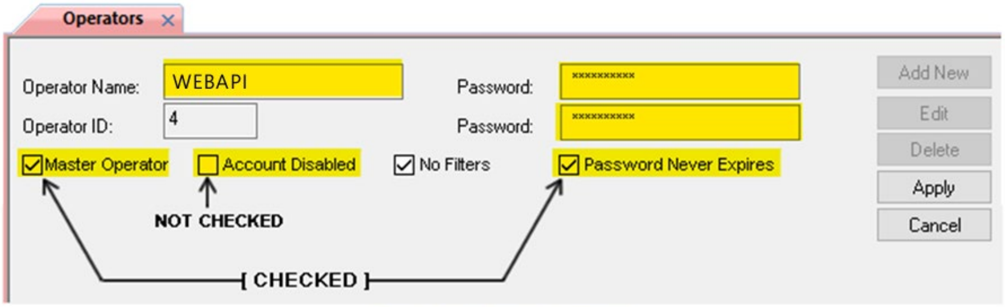
REQUIREMENTS

- An SG system admin (master operator) is required to create User Logins (system operator accounts).
- You must create a User Login (system operator) for your 3rd-Party or Proprietary API-Apps.
- All **User Logins** (system operators) must have the correct ***operator permissions*** (privileges/filters) to support the features of the *Proprietary* and *3rd-Party API Apps* ~ such as idProducer, LaunchPoint Client, LaunchPoint Mobile App, Active Directory, etc.

STEPS

To create a *User Login account* for your API-based application (app), you must create a *system operator*.

1. From the SG Menu, click **Configuration** > **System** > **System Operators**
2. Enter the **Operator Name** (case-sensitive)**:** must be a *valid email address* in SG11.8.6 or higher.
3. Enter a strong **Password** that contains each the following …
   - 8 characters long (minimum length)
   - Uppercase character
   - Lowercase character
   - Number character
   - **Do not use any special characters!**
4. The '**Master Operator**' checkbox does not need to be on for a User Login.
5. The '**Account Disabled**' checkbox should be unchecked. User Login must be active.
6. The '**No Filters**' checkbox should be unchecked if you are customizing the user permissions.
   - Checked = user permissions (operator privileges/filters) will be ignored. User will have permission to all.
   - Unchecked = user permissions (privileges and filter settings) will be applied.
7. Set the '**Password Never Expires**' checkbox as needed.
   - Checked = password will never expire
   - Unchecked = password will expire at midnight on the chosen date.
8. Click **Apply** to save the operator account (click Yes to accept "no filters" if prompted).



Operator Name: WEBAPI

Operator ID: 4

Password: xxxxxxxxxx

Password: xxxxxxxxxx

☑ Master Operator ☐ Account Disabled ☑ No Filters ☑ Password Never Expires

System Operator screen is cropped

Configure AppSettings Keys the GCS Web API

The GCS Web API uses an **appSettings config file** to define the configurable keys for the Web API. Several of the API-Based Applications rely on settings in this file that will permit or prevent their interoperation with the API.

PREREQUISITES

- If you are changing the name or password of the default *Web API User login*, then you will need to create a new SG Operator account (matching same username and password) in System Galaxy Operator screen.
- (Best Practice) Before you make changes, make a backup copy of the appSettings file.

STEPS

1. In Windows Explorer, browse the GCS\System Galaxy\OptionalServices\WebServices folder.
2. (Best Practice) Before you make changes, make a copy of the appSettings file for a backup copy. This way you have an unedited original copy that …
   - you can roll back to, if you need to undo changes …
   - you can review as an example, if you need to verify your syntax or correct mistakes made when you edited your working copy …
3. Right-click the **appSettings config file** and choose to Edit in Notepad app.
4. Edit only the **value** between the quotation marks (bold text)…

<add key=”SGUserName” value=”**SGApiUser**” /> (the default API Username is shown)	← Where ”**SGApiUser**” is shown, you enter the exact same Operator Username you created for the WEB API operator.
<add key=”SGPassword” value=”***Password1***” />	← Where ”**Password1**” is shown, you must enter the exact same password you made when you created the WEB API operator.
<add key=”UserSessionTimeout” value=”**20**” />	← The default value is **20 minutes**. ”0” means no timeout. You may increase this value as needed.
<add key=”HTTPPort” value=”**8000**” />	← The default value is **8000**. ”0” (zero) will disable the HTTP port for the API. You can disable the HTTP port if you are using HTTPS.
<add key=”HTTPSPort” value=”**8443**” />	← The default value is **0** (means port is disabled) ”0” (zero) disables the HTTPS port for the API. You must set this to the HTTPS port number you will use. NOTICE: Using this port requires a signed certificate**.**

Continue on the next page.

5. (conditional) *IF you are using ASSA-DSR Readers*, edit the following keys as shown (bold text)…

<add key="AssaDsrEnabled" value="**true**" />	← must be set to "true" to enable DSR operation ("false" is the default value)
<add key="AssaDsrCallbackServiceEnabled" value="**true**" />	← must be set to "true" to enable DSR callback operation ("false" is the default value)
<add key=" AssaDsrCallbackOnHttps " value="**false**" />	← should be set to "false" (default)
<add key=" AssaDsrCallbackOnPort " value="**9090**" />	← should set to desired port number ("9090" is the default value)
<add key=" AssaDsrSyncUsersUseProxRawWherePossible " value="**false**" />	← should be set to "false" (default)
<add key=" AssaDsrCheckOnlineStatusIntervalMinutes " value="**1**" />	← should be set to "1" (default)
<add key=" AssaDsrPollLogEventsIntervalMinutes " value="**1**" />	← should be set to "1" (default)
<add key=" AssaDsrSyncUsersSchedulesAuthorizationsMinutes " value="**1**" />	← should be set to "1" (default)

6. (optional) You can edit the following keys as shown (bold text)…

<add key="ThrottleLimit" value="**0**" />	← default is 0 = no throttle limit (number of requests)
<add key="ThrottleSwaggerLimit" value="**100**" />	← default is 100
<add key="ThrottleTimeIntervalSeconds" value="**0**" />	← default is 0 = time interval in seconds between requests.

7. Note that there are additional keys for LaunchPoint, idProducer, and ASSA-DSR which are not covered in this section.

8. Save the file after changes are made and restart the GCS Web API Service to initiate new values.

Configure the ConnectionStringsPDSA file (for Web Service)

The GCS Web API uses the **ConnectionStringsPDSA config file** to set the configurable connection string for the Web Service. This allows the Web Service to connect to the System Galaxy database.

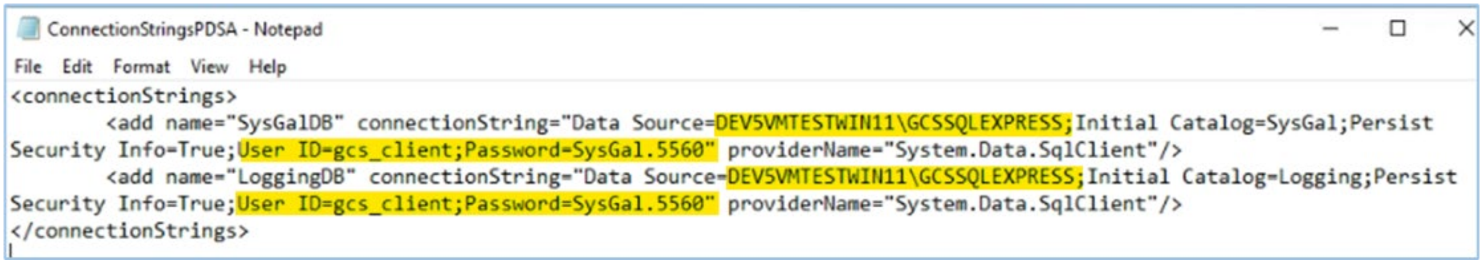
> IMPORTANT: If the database is moved or running on a different computer, you will need to edit the connection string (machine name) to match the true location. Also, if the database instance name was changed, you must also edit the instance name to match the new name. And if the client login credentials have been changed, you must update the User ID and Password to match the new login credentials.

PREREQUISITES

- You must have installed all 3 Steps of the System Galaxy software.
- (Best Practice) Before you make changes, make a backup copy of the connectionSettingsPDSA file.

STEPS

1. Open the computer Services Window and stop the GCS WebAPI Service before editing the config file.
2. On the computer where the GCS Web API Service is running, open the Windows Explorer and browse to the **GCS\System Galaxy\OptionalServices\WebServices** folder.
3. Open and edit the **connectionSettingsPDSA config file** in Notepad app using Run as Administrator.
4. In Notepad, you can turn on Word Wrap from the Format menu.
5. Locate the ***connectionString field*** in the config file.
   - (if needed) Enter the **machine name** of the database server (i.e., the computer the database is running on).
   - (if needed) Enter the **database instance name** if the database instance name has been changed.
6. (if needed) Enter the **User ID** and **Password** only if the client login credentials have been changed.
7. Save your file changes and restart the Galaxy services.



```
<connectionStrings>
	<add name="SysGalDB" connectionString="Data Source=DEV5VMTESTWIN11\GCSSQLEXPRESS;Initial Catalog=SysGal;Persist Security Info=True;User ID=gcs_client;Password=SysGal.5560" providerName="System.Data.SqlClient"/>
	<add name="LoggingDB" connectionString="Data Source=DEV5VMTESTWIN11\GCSSQLEXPRESS;Initial Catalog=Logging;Persist Security Info=True;User ID=gcs_client;Password=SysGal.5560" providerName="System.Data.SqlClient"/>
</connectionStrings>
```

Configure the ConnectionStrings file (for Web Service)

The GCS Web API uses the **ConnectionStrings file** to set the configurable connection string for the Web Service. This allows the Web Service to connect to the System Galaxy database.

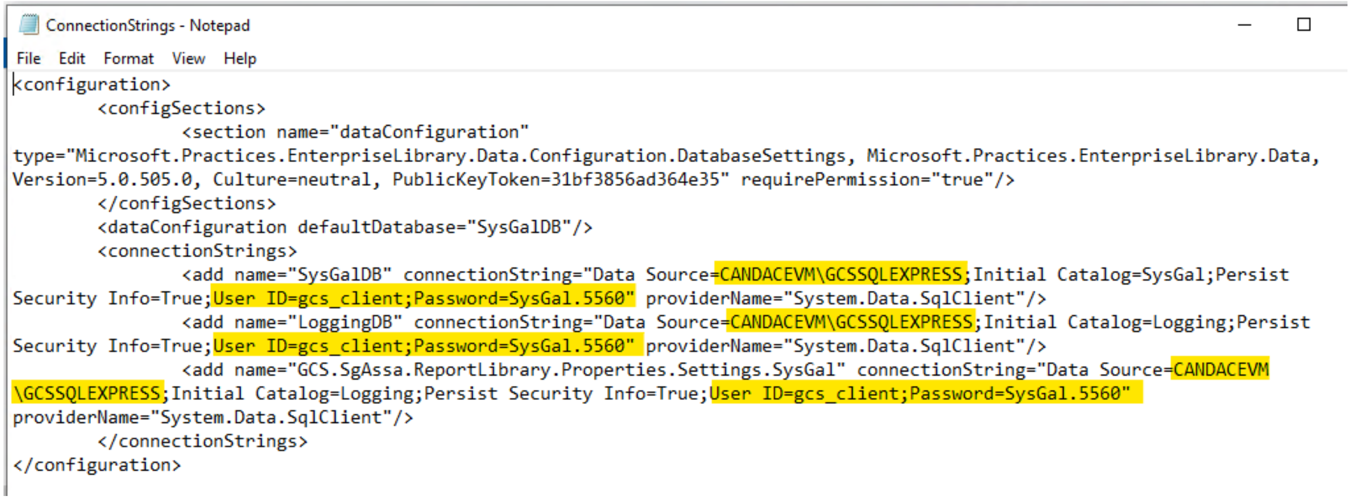
> IMPORTANT: If the database is moved or running on a different computer, you will need to edit the connection string (machine name) to match the true location. Also, if the database instance name was changed, you must also edit the instance name to match the new name. And if the client login credentials have been changed, you must update the User ID and Password to match the new login credentials.

PREREQUISITES

- You must have installed all 3 Steps of the System Galaxy software.
- (Best Practice) Before you make changes, make a backup copy of the connectionStrings file.

STEPS

1. Open the computer Services Window and stop the GCS WebAPI Service before editing the config file.
2. On the computer where the GCS Web API Service is running, open the Windows Explorer and browse to the **GCS\System Galaxy\Configuration** folder.
3. Open and edit the **connectionStrings file** in Notepad app using Run as Administrator.
4. In Notepad, you can turn on Word Wrap from the Format menu.
5. Locate the ***connectionString field*** in the config file.
   - (if needed) Enter the **machine name** of the database server (i.e., the computer the database is running on).
   - (if needed) Enter the **database instance name** if the database instance name has been changed.
6. (if needed) Enter the **User ID** and **Password** only if the client login credentials have been changed.
7. Save your file changes and restart the Galaxy services.



```
<configuration>
        <configSections>
                <section name="dataConfiguration"
type="Microsoft.Practices.EnterpriseLibrary.Data.Configuration.DatabaseSettings, Microsoft.Practices.EnterpriseLibrary.Data,
Version=5.0.505.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" requirePermission="true"/>
        </configSections>
        <dataConfiguration defaultDatabase="SysGalDB"/>
        <connectionStrings>
                <add name="SysGalDB" connectionString="Data Source=CANDACEVM\GCSSQLEXPRESS;Initial Catalog=SysGal;Persist
Security Info=True;User ID=gcs_client;Password=SysGal.5560" providerName="System.Data.SqlClient"/>
                <add name="LoggingDB" connectionString="Data Source=CANDACEVM\GCSSQLEXPRESS;Initial Catalog=Logging;Persist
Security Info=True;User ID=gcs_client;Password=SysGal.5560" providerName="System.Data.SqlClient"/>
                <add name="GCS.SgAssa.ReportLibrary.Properties.Settings.SysGal" connectionString="Data Source=CANDACEVM
\GCSSQLEXPRESS;Initial Catalog=Logging;Persist Security Info=True;User ID=gcs_client;Password=SysGal.5560"
providerName="System.Data.SqlClient"/>
        </connectionStrings>
</configuration>
```

Obtain & Import an SSL Certificate

This section covers how to obtain, import, configure, and test the CSR Certificate.

Obtaining an SSL Certificate

The end-user should purchase an **SSL Certificate** as a part of the security measures in a live/production environment.

- An SSL Certificate will encrypt the communications between the API-Based Apps and Web API Server.
- The SSL Certificate will reside on the same computer where the GCS Web API Service is running.

IMPORTANT NOTICES

- Galaxy recommends you purchase the longest certificate lifespan possible. The API-Based Applications will stop working when the Certificate expires.
- Self-signed certificates will not work in a live/production environment.
- Galaxy makes no recommendations as to which brand will provide the best security or best value.

PURCHASE AN SSL CERTIFICATE

1. Identify Certificate Authority (CA), such as GoDaddy, Verisign, etc. to purchase a *Signed SSL Certificate*. The Certificate Authority will assist you in generating a Certificate Request CSR
2. You must create the CSR Request on the same computer where the web services are installed/running.
3. When the SSL Certificate is created, you will install it on the Web Server computer using the instructions in the following sections.

IMPORTANT: Contact the Certificate Authority for technical support when submitting information to obtain the CSR and purchase an SSL certificate.

Import an SSL Certificate into the Certificate Store

You must import the Signed SSL Certificate into the Certificate Store on the computer where the ***GCS Web API Service*** is running/residing.

IMPORTANT NOTICES

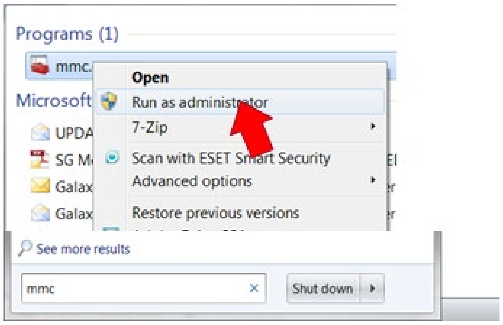
- **Remember which branch/folder the SSL Certificate is imported into.**
- Galaxy recommends placing the Certificate in the Personal branch of the Certificate Store.
- The **SSL Setup Batch file** will fail if there is not a private key on the Certificate.

VERIFY THE PRIVACY KEY

You must verify that a **privacy "key" symbol** is visible on the Certificate after the Certificate has been imported into the Certificate Store.

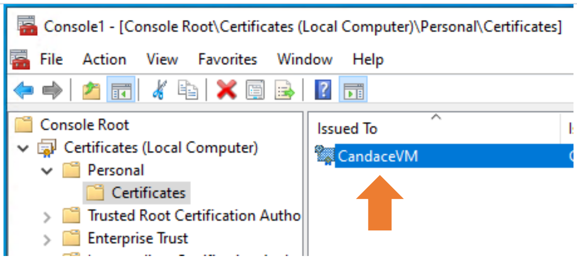
Run the certs.mmc file as an admin using the following steps.

1. Click on the Windows Start button.
2. In the Run field, type "mmc" and press <enter>.
3. Right-click the **mmc.exe** file.
4. Select ***Run as administrator***.

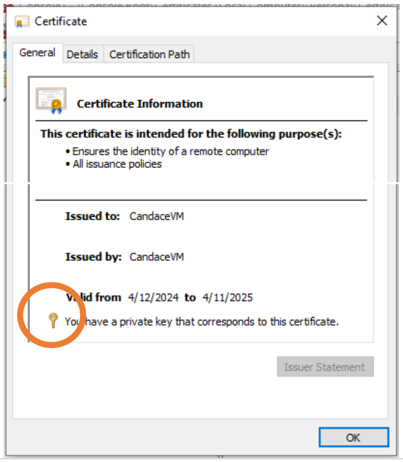


5. Under the Certificates branch, and open the folder where you imported the Certificate. Galaxy recommends the Personal folder.
6. Double-click on the *Certificate Name* or icon

   The Certificate details window will open.


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Autho
Enterprise Trust
Issued To
CandaceVM

7. On the bottom of the General tab, look for the *private key* symbol.
   a. If you have a privacy key, then go to the section to [Capture the Cert Hash](#).
   b. If the is privacy key is missing, then you must generate the key. Go to the section to [Repair the Certificate Key](#).



Certificate Information

This certificate is intended for the following purpose(s):
- Ensures the identity of a remote computer
- All issuance policies

Issued to: CandaceVM

Issued by: CandaceVM

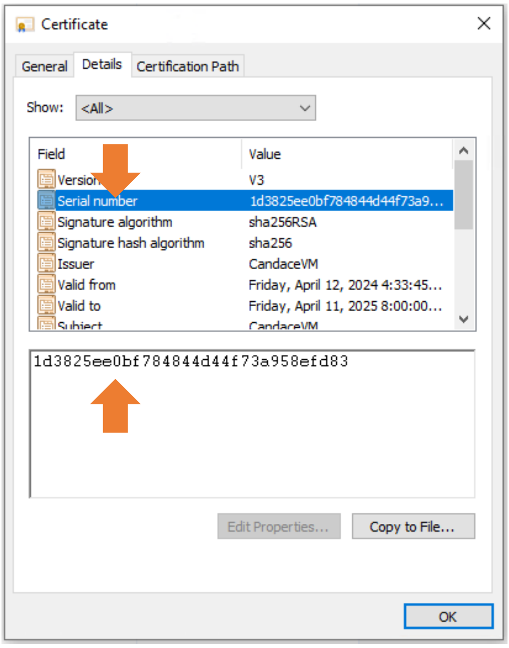
Valid from 4/12/2024 to 4/11/2025

You have a private key that corresponds to this certificate.

REPAIR THE MISSING CERTIFICATE KEY

If there is not a key, then you must generate one.

1. Select (click) the Details tab.
2. Select (highlight) the ***Serial Number*** field in the upper List View.
3. In the lower window, select (highlight) the number and copy it (Ctl+C) - or write it down.



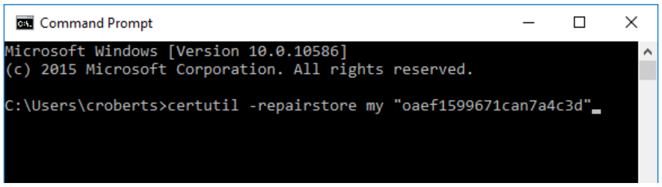
Show: <All>

Field	Value
Version	V3
Serial number	1d3825ee0bf784844d44f73a9...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	CandaceVM
Valid from	Friday, April 12, 2024 4:33:45...
Valid to	Friday, April 11, 2025 8:00:00...
Subject	CandaceVM

```
1d3825ee0bf784844d44f73a958efd83
```

4. Click on the windows Start button.
5. Type **cmd** into the Run field.
6. When a Windows Command Shell opens, type the following instruction, **include the quotemarks (" ")** at the command prompt:

   certutil -repairstore my "*SerialNumber*"



```
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\croberts>certutil -repairstore my "oaef1599671can7a4c3d"
```

> WHERE "SerialNumber" REPRESENTS THE ENTIRE HEX NUMBER (INCLUDING THE QUOTE MARKS) THAT YOU OBTAINED FROM THE CERTIFICATE DETAILS IN THE PREVIOUS STEPS. DO NOT INCLUDE ANY SPACES IN THE SERIAL NUMBER OR BETWEEN THE QUOTEMARKS.

END OF REPAIRING A CERTIFICATE KEY

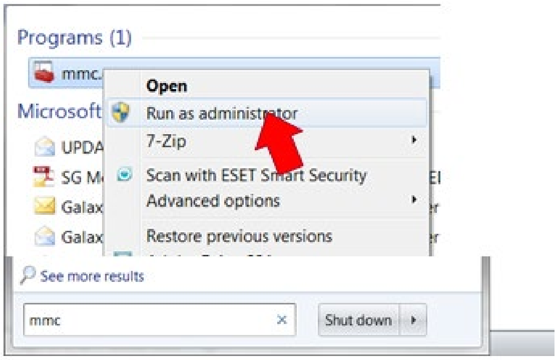
Assigning the SSL Certificate to the Web API Server

After the Signed SSL Certificate has been imported, you must assign the Certificate to the GCS Web API Service by running the SSL Setup batch file. The batch file must be edited and configured with the Certificate ***Thumbprint string***.

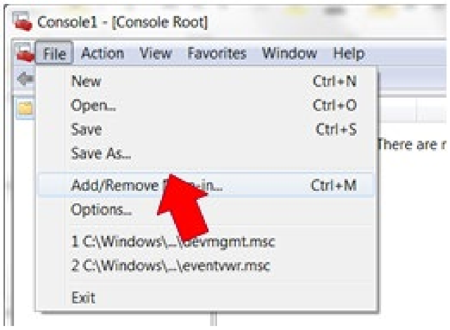
CAPTURE THE CERTHASH (i.e., Thumbprint string)

Run the certs.mmc file as an admin using the following steps.

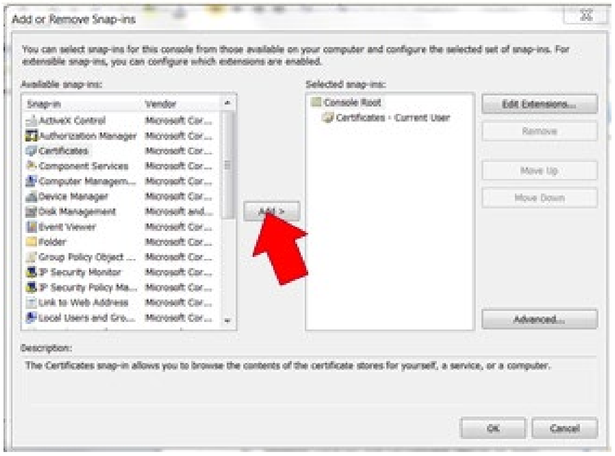
1. Click on the Windows Start button.
2. In the Run field, type “mmc” and press <enter>.
3. Right-click the **mmc.exe** file.
4. Select ***Run as administrator***.



5. Click the File menu when the console window opens.
6. Select Add/Remove Snap-in


Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Windows\...\devmgmt.msc
2 C:\Windows\...\eventvwr.msc
Exit
There are r

7. Select (highlight) the Certificates snap-in in the Available column on the left side.
8. Click the [Add >] button to move it to the right.



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy Ma...	Microsoft Cor...
Link to Web Address	Microsoft Cor...
Local Users and Gro...	Microsoft Cor...

Selected snap-ins:

Console Root
Certificates - Current User

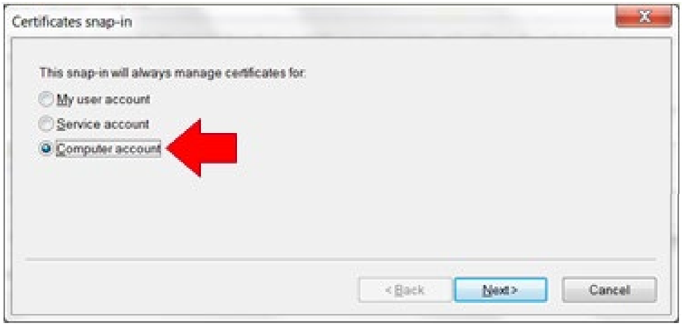
Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Continue on the next page.

9. Choose Computer account option.

10. Click [Next >] button.

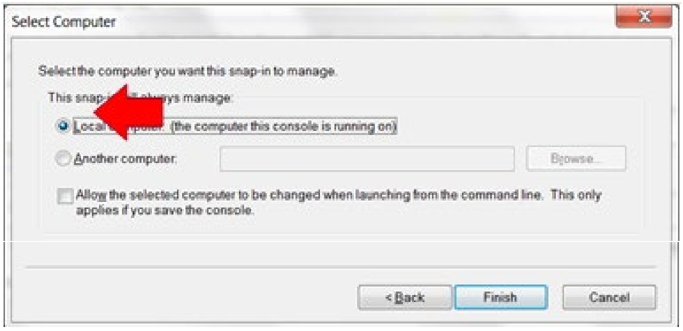


Certificates snap-in

This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account

11. Click [Finish] button to accept *local computer*.



Select Computer

Select the computer you want this snap-in to manage.

This snap-in will always manage:

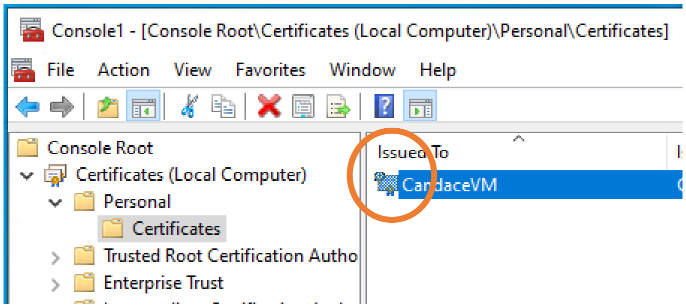
● Local computer: (the computer this console is running on)
○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

12. Double-click on the *Certificate Name* or icon.

13. Select (click) the Details tab.

The Certificate details window will open.



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

14. On the Details list, look for the *Thumbprint* field.

The entire *hex string* will be displayed in the bottom window.

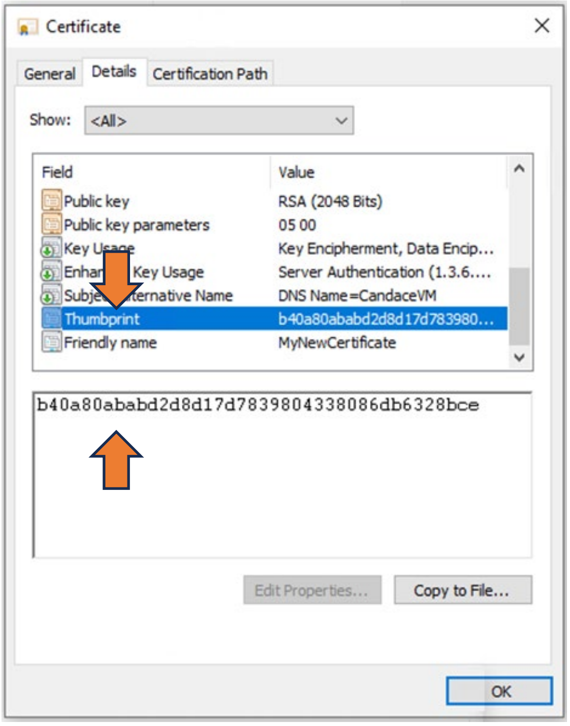
15. Carefully write down the ***hex string***.

- DO NOT copy the leading space character.
- Start with the first non-space character.
- <u>Do not include any spaces between the alpha-numeric characters</u>.

It is possible to copy the string to clipboard, but it may or may not be deemed secure to do so.

16. Click OK to close this window.

17. Go to the next section to add the cert hash.



Certificate

Show: <All>

Field	Value
Public key	RSA (2048 Bits)
Public key parameters	05 00
Key Usage	Key Encipherment, Data Encip...
Enhanced Key Usage	Server Authentication (1.3.6....
Subject Alternative Name	DNS Name=CandaceVM
Thumbprint	b40a80ababd2d8d17d783980...
Friendly name	MyNewCertificate

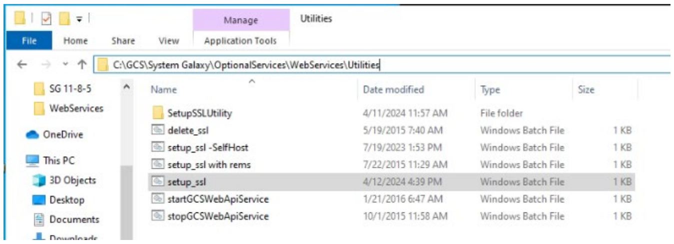
```
b40a80ababd2d8d17d7839804338086db6328bce
```

COPY CERTHASH (Thumbprint) TO THE 'SETUP_SSL' BATCH FILE

1. Locate the "**setup_ssl.bat**" batch file.

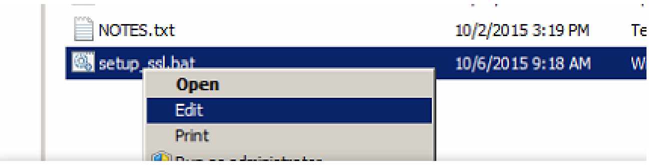
THE SETUP SSL BATCH FILE IS LOCATED IN …

(C:)GCS\System Galaxy\OptionalServices\WebServices\Utilities



Name	Date modified	Type	Size
SetupSSLUtility	4/11/2024 11:57 AM	File folder	
delete_ssl	5/19/2015 7:40 AM	Windows Batch File	1 KB
setup_ssl -SelfHost	7/19/2023 1:53 PM	Windows Batch File	1 KB
setup_ssl with rems	7/22/2015 11:29 AM	Windows Batch File	1 KB
setup_ssl	4/12/2024 4:39 PM	Windows Batch File	1 KB
startGCSWebApiService	1/21/2016 6:47 AM	Windows Batch File	1 KB
stopGCSWebApiService	10/1/2015 11:58 AM	Windows Batch File	1 KB

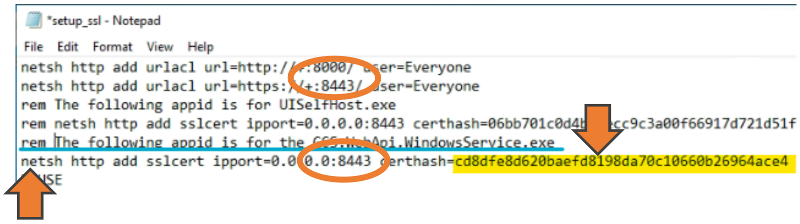
2. Right-click the **setup_ssl.bat** filename and select EDIT from the context menu. Open in Notepad.



3. Locate the "certhash" string in the batch file below the GCS.WebApi.WindowsService.
4. Select (highlight) the existing *hash string* and replace it with the *thumbprint string* you copied from the Certificate Details tab.

   Do not include any spaces!

5. Remove the "rem" command on the line where the netsh command adds the cert hash.
6. Also, *if you are not using the default 8443* you must update/change the port number to the port you will use.
7. Save the file and close it.



```
netsh http add urlacl url=http://+:8000/ user=Everyone
netsh http add urlacl url=https://+:8443/ user=Everyone
rem The following appid is for UISelfHost.exe
rem netsh http add sslcert ipport=0.0.0.0:8443 certhash=06bb701c0d4b[illegible]cc9c3a00f66917d721d51f
rem The following appid is for the GCS.WebApi.WindowsService.exe
netsh http add sslcert ipport=0.0.0.0:8443 certhash=cd8dfe8d620baefd8198da70c10660b26964ace4
PAUSE
```

In the example above the port number '8443' has not been replaced.

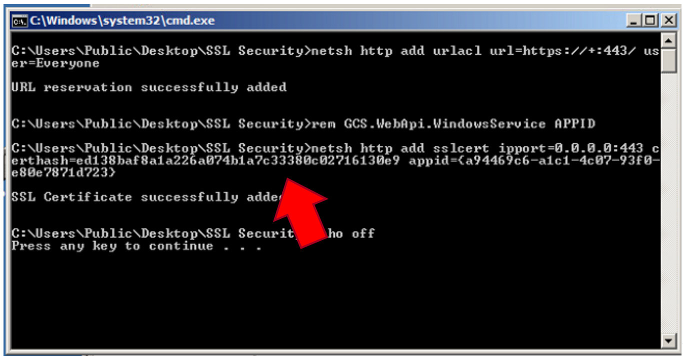
RUN THE SSL SETUP BATCH FILE (Add the Certificate to the Web Service)

IMPORTANT: if your prior Certificate expired, you must delete it before you add the new certificate to the Web Services. The [delete_ssl batch file](#) can be used to delete the old certificate. Run as Administrator.

1. Run the SSL Setup batch file by double-clicking it.

   A Windows command shell will open.

2. Close the command window after you see the prompt "SSL Certificate successfully added".

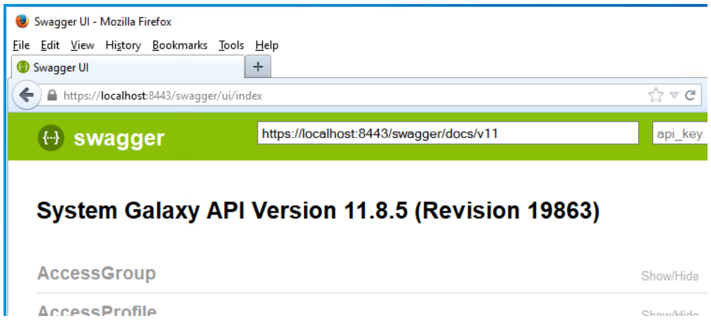


```
C:\Windows\system32\cmd.exe

C:\Users\Public\Desktop\SSL Security>netsh http add urlacl url=https://+:443/ us
er=Everyone

URL reservation successfully added


C:\Users\Public\Desktop\SSL Security>rem GCS.WebApi.WindowsService APPID

C:\Users\Public\Desktop\SSL Security>netsh http add sslcert ipport=0.0.0.0:443 c
erthash=ed138baf8a1a226a074b1a7c33380c02716130e9 appid={a94469c6-a1c1-4c07-93f0-
e80e7871d723}

SSL Certificate successfully adde


C:\Users\Public\Desktop\SSL Securit      ho off
Press any key to continue . . .
```

"

3. Use the Swagger page to test the SSL Certificate.

   https://localhost:8443/swagger


Swagger UI - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Swagger UI
+
https://localhost:8443/swagger/ui/index
swagger
https://localhost:8443/swagger/docs/v11
api_key
Show/Hide
Show/Hide

System Galaxy API Version 11.8.5 (Revision 19863)

AccessGroup

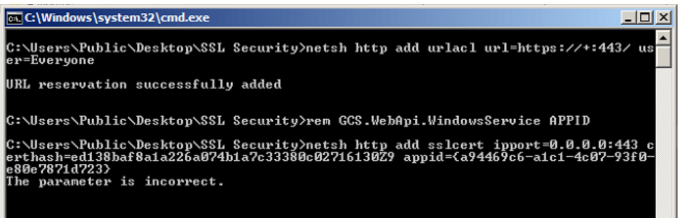
AccessProfile

IF Operating System returns an error in the CMD Shell …

IMPORTANT: If running the *SSL Setup batch file* returns an error, then you must remove the thumbprint by running the **delete_ssl.bat** file. Then rerun the SSL Setup file correctly.

THE BATCH FILE IS LOCATED IN …

(C:)GCS\System Galaxy\OptionalServices\WebServices\Utilities



```
C:\Windows\system32\cmd.exe

C:\Users\Public\Desktop\SSL Security>netsh http add urlacl url=https://+:443/ us
er=Everyone

URL reservation successfully added


C:\Users\Public\Desktop\SSL Security>rem GCS.WebApi.WindowsService APPID

C:\Users\Public\Desktop\SSL Security>netsh http add sslcert ipport=0.0.0.0:443 c
erthash=ed138baf8a1a226a074b1a7c33380c027161302Z9 appid={a94469c6-a1c1-4c07-93f0-
e80e7871d723}
The parameter is incorrect.
```

"The parameter is incorrect."

Failed due to incorrect character in certhash in the SSL Setup file.

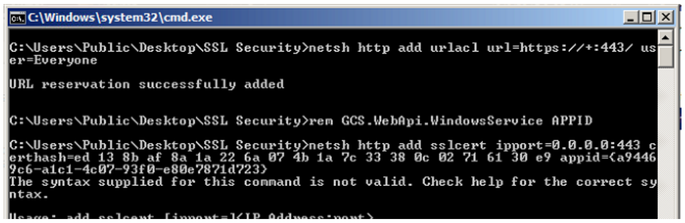
4. To delete and re-run the SSL Setup do the following…

   a) Double-click the **delete_ssl.bat** file to run it - this deletes your SSL certificate thumbprint. See Appendix for [Editing the *delete_ssl.*](#)*bat* before continuing to next step.

   b) Re-do Part 5.3.1: to verify your **thumbprint hex string** is accurate.

   c) Re-do Part 5.3.2: to edit the **SSL Setup batch** file, correct any errors to the port numbers or certhash.

   d) Re-do this Part 5.3.3 to ***add your SSL Certificate***.



```
C:\Windows\system32\cmd.exe

C:\Users\Public\Desktop\SSL Security>netsh http add urlacl url=https://+:443/ us
er=Everyone

URL reservation successfully added


C:\Users\Public\Desktop\SSL Security>rem GCS.WebApi.WindowsService APPID

C:\Users\Public\Desktop\SSL Security>netsh http add sslcert ipport=0.0.0.0:443 c
erthash=ed 13 8b af 8a 1a 22 6a 07 4b 1a 7c 33 38 0c 02 71 61 30 e9 appid={a9446
9c6-a1c1-4c07-93f0-e80e7871d723}
The syntax supplied for this command is not valid. Check help for the correct sy
ntax.

Usage: add sslcert [ipport=]<IP Address:port>
```

"The syntax supplied for this command is not valid."

Failed due to spaces included in the certhash in SSL Setup file.

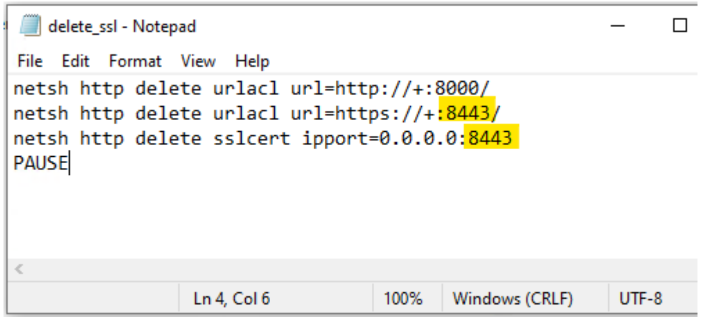
Appendix

EDIT AND RUN THE DELETE_SSL BATCH FILE (for Expired Certificates, etc.)

If you have one of the following issues, you may need to edit and run the delete_ssl.bat file …

- you have an expired certificate
- you encountered and Operating System error when running the ssl_setup-bat file in prior section

Edit the delete_ssl.bat file ONLY IF you are using custom ports for the Web API connections. (8443 is the default HTTPS Port)



```
netsh http delete urlacl url=http://+:8000/
netsh http delete urlacl url=https://+:8443/
netsh http delete sslcert ipport=0.0.0.0:8443
PAUSE
```

1. **To edit the delete_ssl.bat file**: navigate to the Web Services Utilities folder.
   (C:)GCS\System Galaxy\OptionalServices\WebServices\Utilities

2. Right-click the filename of the **delete_ssl.bat file** and choose ***Edit*** from the shortcut menu.

3. Open the **delete_ssl.bat** in Notepad.

4. Where you see the HTTPS Ports (highlighted), carefully change the port to the port number the end-user has designated for the Web API.

5. Select File and Save to save your changes.

Run the delete_ssl.bat file as follows …

6. Right-click the **delete_ssl.bat** file to run it as Administrator.

7. The batch file will run in a Windows Command Shell- this deletes your SSL certificate thumbprint.

8. Return to the appropriate section to finish running the ssl_setup.bat (run as Administrator).