System Galaxy Quick Guide

INSTALLATION AND CONFIGURATION

GCS Web API Server

FOR GALAXY MOBILE APP COMMUNICATION

GALAXY CONTROL SYSTEMS

SG 10.4.8
(or higher)
1ST EDITION
JAN 2016

Galaxy

Web API Service

for Mobile Apps

How to Install and Configure the GCS Web API Service

The information in this document is subject to change without notice.

No claims are made as to the accuracy or completeness of this document.

1st Edition, Revision B

Galaxy Control Systems

3 North Main Street

Walkersville MD 21793

301-845-6600

www.galaxysys.com

Table of Contents

1 Introduction to the Galaxy 'GCS Web API Service'

This guide is part of System Galaxy documentation suite. Consult appropriate documents when configuring your system.

The GCS Web API Service allows the Galaxy **DoorPoint** and **PersonPoint** Mobile Apps to connect to the *System Galaxy* database.

1. Introduction and Requirements.
2. Installing the GCS Web API Service
3. Changing the Port Number for the Web API Service
4. Testing Web API Connectivity
5. Obtaining and Importing the CSR Certificate.

Go to the DoorPoint or PersonPoint User Guides for information on using the mobile apps.

1.1 PLANNING & DEPLOYMENT

The GCS Web API Service should reside on the main *System Galaxy Communication Server* (recommended). The service has no dependencies. Therefore, it is not affected by (and does not affect) other GCS services. Take steps to protect your *Mobile Communications* in a live/production environment by using HTTPS secure socket with an SSL Certificate.

1.1.1 NETWORK & SECURITY CONSIDERATIONS & ASSUMPTIONS

Take appropriate steps to protect your Access Control System. Do not leave your system, services, or mobile apps exposed.

1. You should obtain in a ***CSR*** / ***SSL Certificate*** to encrypt your mobile communications. This is used in addition to the typical network security (i.e. firewalls, passwords, etc.) to protect the mobile data communications.
2. *Maintain the latest Windows updates on the main SG Communication Server, Database server, and client PCs.*
3. Galaxy only supports secure/encrypted connections. HTTPS secure socket connections with an SSL Certificate for your Mobile Apps is required in the live production environment.
   - » **Private Access:** Galaxy Apps to connect to a *private wireless router* when the smartphone is within range.
   - » **Public Access:** Galaxy Apps to connect to a *public network router* using a Public Cellular Provider.

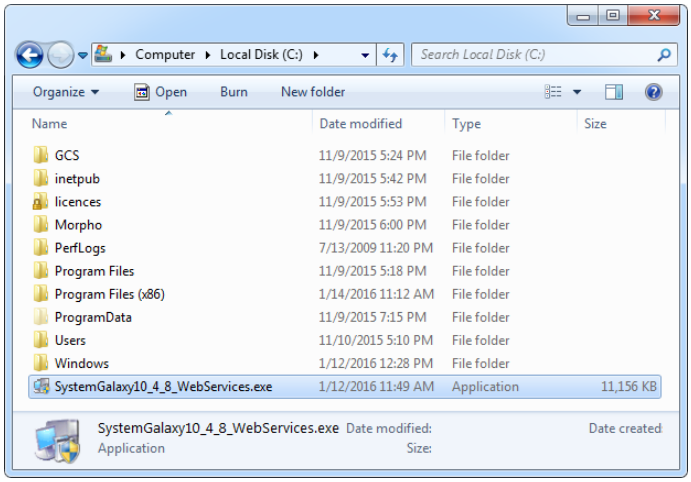
1.1.2 SYSTEM REQUIREMENTS & ASSUMPTIONS CONDENSED

1. Galaxy Mobile Apps require System Galaxy 10.4.8 (or higher).
2. System Galaxy database must already be installed and must be running before you install the Web API Service.
3. The GCS Web API Service must be able to connect to the System Galaxy database.
4. The GCS Web API Service is installed on the main *System Galaxy Communication Server*.
5. *GCS Web API Service* must be using a unique port number. **It cannot share port 80 or 443 with IIS or other apps**.
   - » 8000 is default HTTP port (configurable) – useful for testing environment only
   - » 8443 is default HTTPS port (configurable) – for live/production environment
6. The Mobile Communications should be protected by an SSL Certificate with privacy key in tact.
7. The GCS Web API Service and the SSL Certificate must reside on the same server.
8. Galaxy only supports secure/encrypted connections. HTTPS secure socket connections with an SSL Certificate for your Mobile Apps is required in the live production environment.
9. ***GCS Web API Service*** must provide (be configured with) a **valid SG login and password that exists in System Galaxy**. These SG credentials (username and password) must be active/valid in System Galaxy and must have the appropriate privileges that support the functions of service. The SG credentials must be configured into the service's 'exe.config' file. **This file can be encrypted** using the same method and tools you use to encrypt the SG Web Module – See the web module guide for details. *This **does not affect** the main GCS Communication, Event, Client Gateway and DB writer services.*

2 Installing the GCS Web API Service

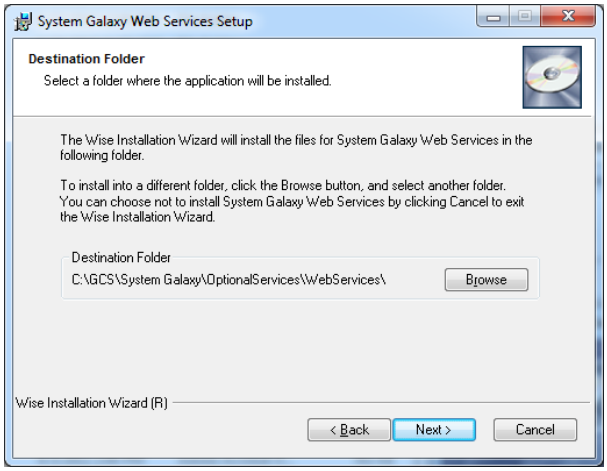
This section covers how to install the GCS Web API Service on the main SG Communication Server.

IMPORTANT: The System Galaxy Database and core GCS Services must be up and running.

Steps to Install the Web API Service:	***Screenshots***
1. **Insert the Galaxy Install CD.** Or copy the GCS Web Services Installer file to the server (pictured). 2. Double-click the install executable "SystemGalaxy10_4_8_WebServices.exe" *The Installer will launch.*	
3. When Welcome screen displays, click [NEXT] to continue.	

The SG Web Services installer displays the Destination Folder.

4. Click [NEXT] to accept the default folder path and continue with installation.



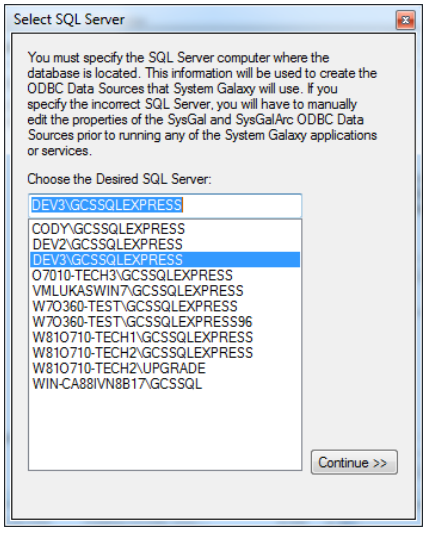
5. Click the [Choose Available SQL Server] button.

The Select SQL Server dialog displays the list of *SQL Server instances* that are currently running on the network. By default this is named GCSSQLEXPRESS.

In some cases the network admin or database administrator may have installed the database in a SQL Server that has a different name than the default name.

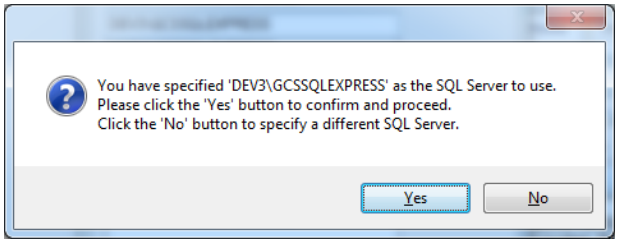
You must choose the correct *SQL Server Instance* that is running the System Galaxy 10.4.8 database.

6. Select (highlight) the appropriate instance name.
7. Click [Continue >>] button.

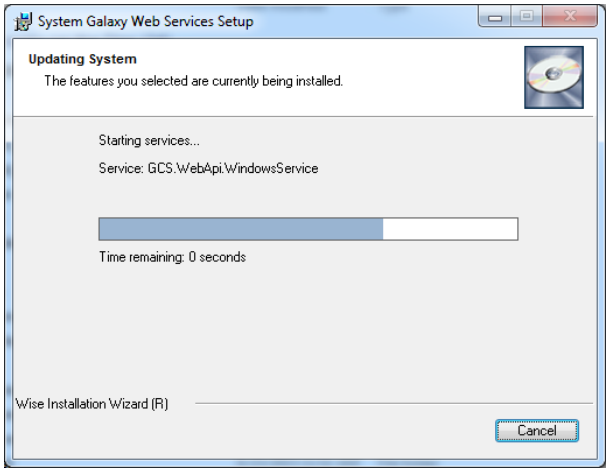


8. Click [Yes] to accept the selected instance.

   *Clicking **No** will allow you to return to the list and select a different instance name.*



The System Update dialog displays a progress bar to indicate the percentage of installation accomplished.



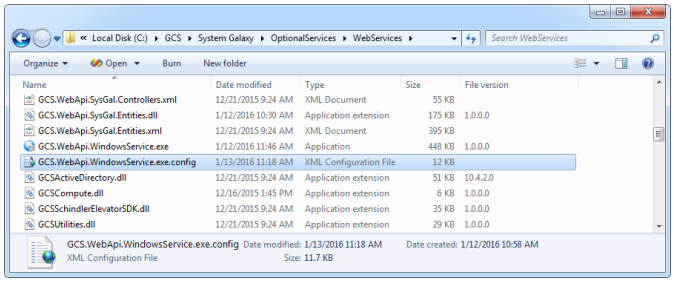
9. Allow the files to extract and complete the installation.

   Clicking [Cancel] will abort the installation.
   A confirmation to stop the installer is also displayed.

10. Click [FINISH] to close the installer.

Notice that the files are installed in the WebServices folder under the normal *System Galaxy* folder.

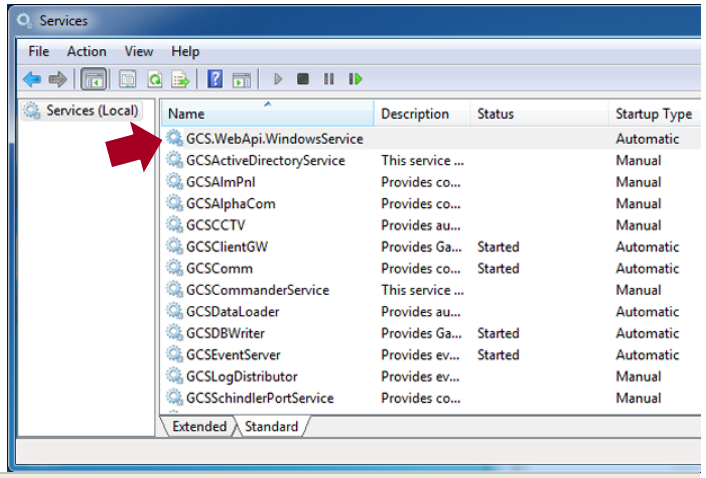
GCS.WebApi.WindowsService.exe.config XML file is located in the WebServices folder. This file is where the default port number is configured. The default port is 8000.



Notice the GCS.WebApi.WindowsService is now present in the *Services Explorer Window*. By default the service is configured to run/start automatically.

The *GCS.WebApi.WindowsService* has no dependencies. Starting and stopping the service will not affect other services.

11. Right-clicking the *service name* and choosing "Start" from the context menu to start the service.



END OF INSTALLATION INSTRUCTIONS

3 Changing the Port Number for the GCS Web API Service

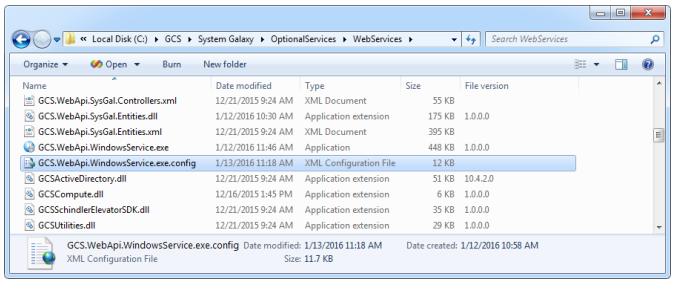
This section covers how to change the port number used to connect with the DoorPoint and PersonPoint Apps.

The default live/production port is HTTPS Port 8443. The default testing port is HTTP Port 8000 (testing only).

IMPORTANT: You must restart your service after changing the port number.

Steps to Configure the XML file's Port Number : ***Screenshots***

Always make a backup copy of your xml config file BEFORE you make any changes to it. Preserve the backup as a way to restore your working file in the event you mistakenly change or step on the surrounding code / commands.

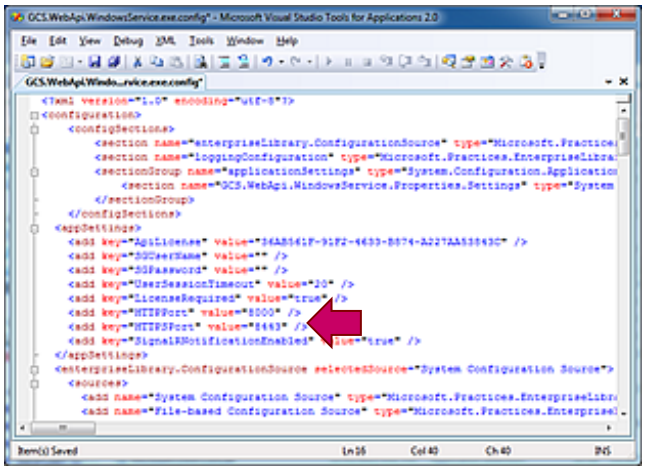


1. **Make a backup of your GCS.WebApi.WindowsService XML config file.**

2. Open the GCS.WebApi.WindowsService XML file.

   THE FILE IS LOCATED IN …
   (C:)GCS\System Galaxy\OptionalServices\WebServices

   The Microsoft Visual Studio will launch.



3. Press **< Ctl+F > keyboard keys** to open search box.

4. Enter the *default port number* you wish to find.
   i.e. enter **HTTPPort** *or* **HTTPSPort**
   Visual Studio will highlight the appropriate row.

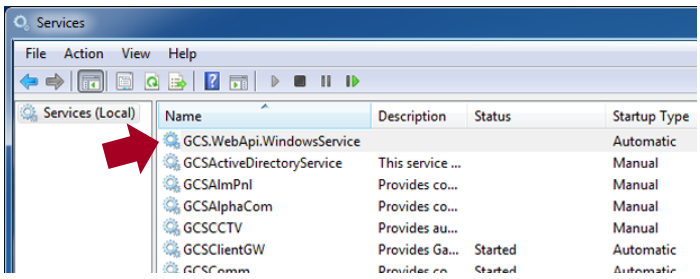
5. **CAREFULLY** replace the existing port number with your desired port number. DO NOT OVERWRITE OR DELETE ANY QUOTE (" ") MARKS OR ANY OTHER CHARACTERS!

6. Click [Save] icon on the toolbar to save changes.

7. Close the file and *Visual Studio* window.

Important: **GCS Web API Service** must be configured with a ***valid SG login and password*** that exists in System Galaxy. These credentials must be active/valid in System Galaxy and must have the appropriate privileges that support the functions of service. The SG credentials must be configured into the service's 'exe.config' file. **This file can be encrypted** using the same method and tools you use to encrypt the SG Web Module – See the Web Module Guide for encryption details. *This **does not affect** the main GCS Communication, Event, Client Gateway and DB writer services.*

Restart the GCS.WebApi.WindowsService in the Services window.



8. Open the Services window.

9. Right-click the *service name* to get a context menu.

10. Choosing "Restart" from the context menu to restart the GCS.WebApi.WindowsService.

END OF INSTRUCTIONS

4 Testing the Web API Connectivity

This section covers how to TEST the Web API Service connectivity.

After you change the port number in the XML Config file you must test your local PC connectivity.

Steps to Test the Web API Service:	***Screenshots***

1. Open a Browser on the same PC as the machine that the Web API Service is running.

   This should be main SG Communication server.

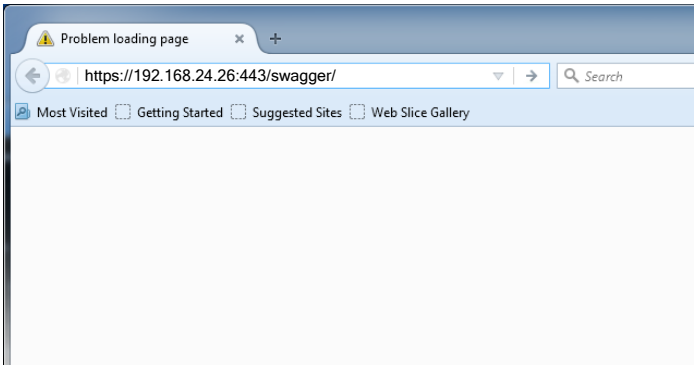
2. Enter the Test IP Address as follows:

   http://Server-IP-Address:Port/swagger/

   – OR –

   https://Server-IP-Address:Port/swagger/

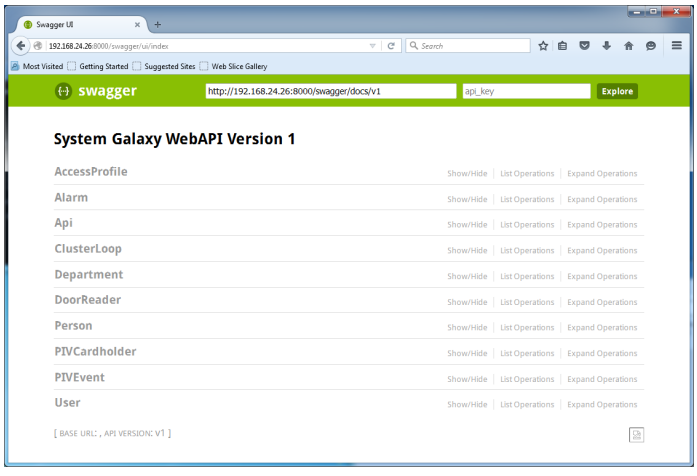
   WHERE Server-IP-Address:Port REPRESENTS YOUR COMM. SERVER'S IP ADDRESS AND THE PORT # THAT YOU CHANGED IN STEP-2 OF THE PREVIOUS SECTION.



Important: in a live production environment you should use the ***machine name*** instead of the IP address because the machine could move or be subject to network changes. Using a machine name means any changes to the network addresses will be transparent to the Mobile App / Web API Service.

3. You should see this page if you are correctly configured.

   IMPORTANT: YOU MUST ALSO TEST THAT YOU CAN REACH THIS PAGE FROM A BROWSER ON YOUR SMARTPHONE.



END OF INSTRUCTIONS

5 Obtaining & Importing the CSR Certificate

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

5.1 OBTAINING A CSR 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 Mobile Apps and the Web API Server.
- The SSL Certificate will reside on the same *communication server* where the GCS Web API Service is running.

You must submit a **Certificate Signing Request (CSR)** to a *Certificate Authority* who will issue an SSL Certificate back to you for a cost.

5.1.1 PURCHASING AN SSL CERTIFICATE

When purchasing an SSL Certificate, the integrator or user must create a CSR or *Certificate Signing Request.* The Certificate Authority (CA) of your choosing (such as Comodo, GoDaddy, Semantic, Verisign, etc.) will typically assist you in generating a CSR on the local machine/server where the web services are installed/running.

The integrator or end-user will provide the appropriate information to the Certificate Authority (CA) and will cover any associated costs.

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

IMPORTANT: Galaxy recommends you purchase the longest certificate lifespan possible. The mobile apps will stop working when the Certificate expires.

IMPORTANT: Self-signed certificates will not work in a live/production environment.

NOTICE: Galaxy Control Systems makes no recommendations as to which brand will provide the best security or best value.

5.2 IMPORTING THE SSL CERTIFICATE INTO THE CERTIFICATE STORE

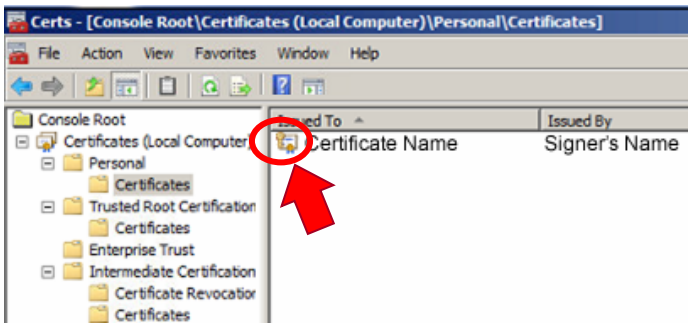
Once the Certificate has been purchased, the integrator or end-user will import the Certificate onto the *GCS Communication Server* where the GCS Web API Service resides.

IMPORTANT: PAY ATTENTION/REMEMBER where the Certificate is imported (which branch in the Certificate Store it is located). Contact the *Certificate Authority* for technical assistance with importing their certificate.

5.2.1 VERIFYING A PRIVACY KEY

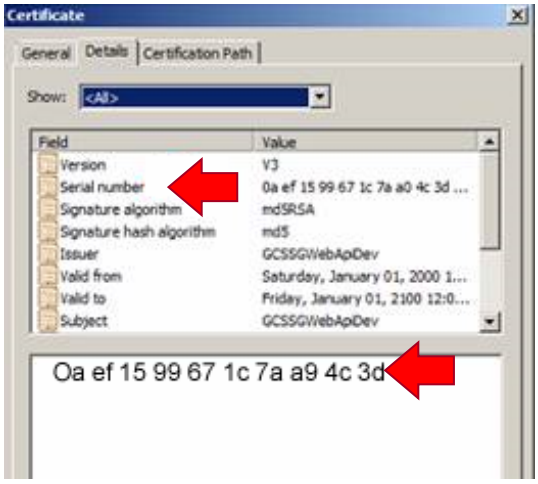
Once the Certificate has been imported into the certificate store, user must verify that a "key" symbol is visible on the Certificate icon. If it is the first attempt at importing it should have the key. If you are re-importing it for some reason, you may need to generate the privacy key. The SSL Setup Batch file will fail if there is not a private key on the Certificate.

- » ***If a key is already present, the user can skip to next section 5.2.3.***
- » **If a key is NOT present, the user must generate a privacy key – see below.**

Steps to Repair a Privacy Key:	***Screenshots***
1. **Open the Certificate Store and open the branch where you imported the Certificate.** *See the steps to open your Certificate Store in the following section 5.3.1 for details.* 2. Double-click on the *Certificate Name* or icon *The Certificate details window will open.*	
3. On the bottom of the General tab, look for the *private key* symbol. 4. If you have a privacy key, then skip to the next chapter. 5. If there is NOT privacy key, then you must generate the key. Go to the next step.	

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

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



9. Click on the windows Start button.
10. Type **cmd** into the Run field.
11. When a Windows Command Shell opens, type the following instruction **including quotemarks (" ")** at the command prompt:

    certutil -repairstore my "*SerialNumber*"

    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 INSTRUCTIONS

5.3 ASSIGNING THE SSL CERTIFICATE TO THE WEB API SERVER

After the private Certificate has been imported, the integrator or end-user must assign the Certificate onto the GCS Web API Service by running the SSL Setup batch file. The batch file must be edited and configured with the Thumbprint string from the Certificate.

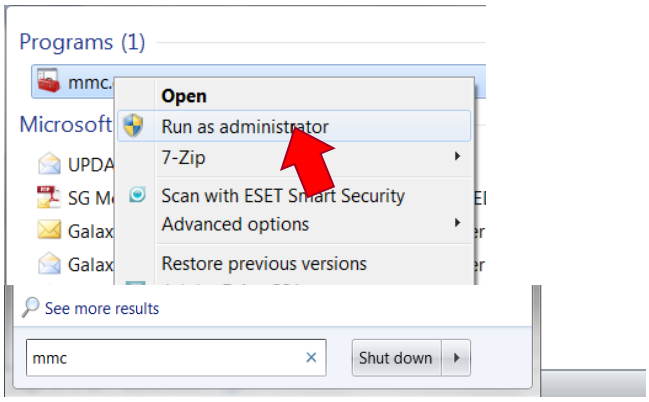
Contact the Certificate Authority for technical assistance with importing the certificate.

5.3.1 CAPTURING THE CERTHASH (CERTIFICATE THUMBPRINT)

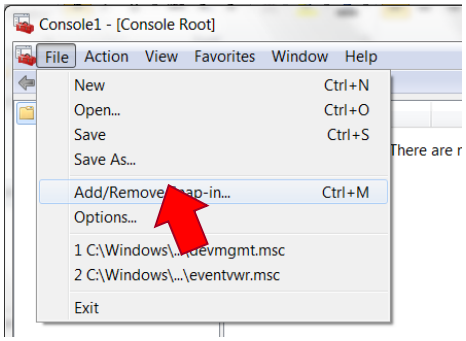
Steps to Capture the Certificate Thumbprint:	***Screenshots***

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

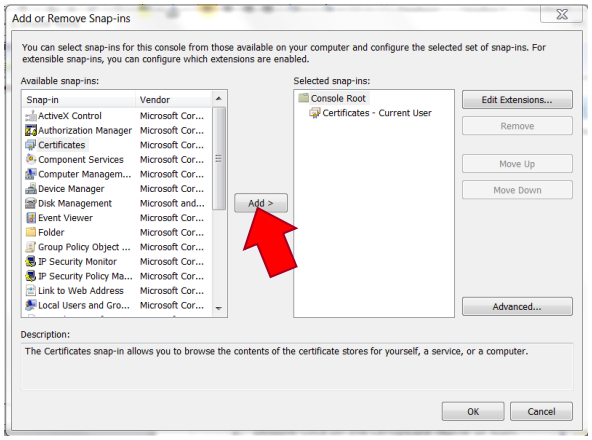
1. Click on the Windows Start button.
2. In the Run field, type “mmc” and press <enter>.
3. Right-click the **mmc.exe** file.
4. Select ***Run as administrator***.



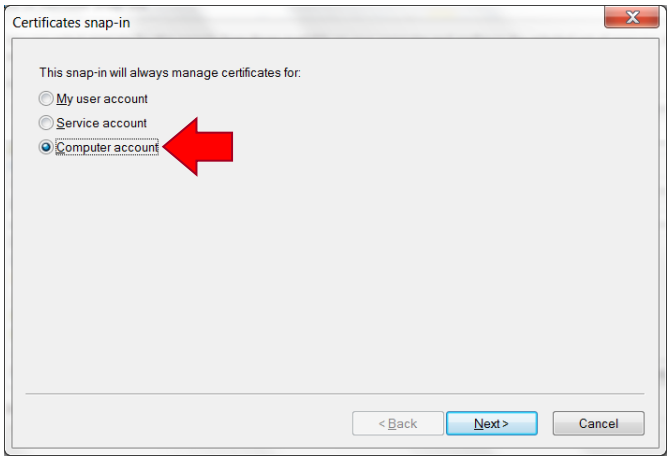
5. Click the File menu when the console window opens.
6. Select Add/Remove Snap-in



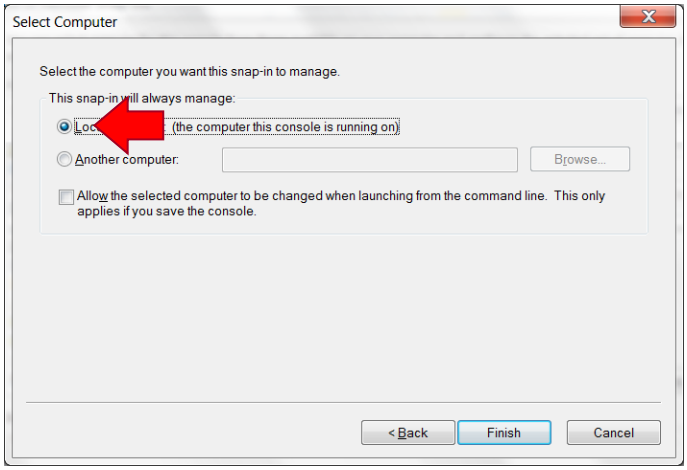
7. Select (highlight) the Certificates snap-in in the Available column on the left side.
8. Click the [Add >] button to move it to the right.



9. Choose Computer account option.
10. Click [Next >] button.

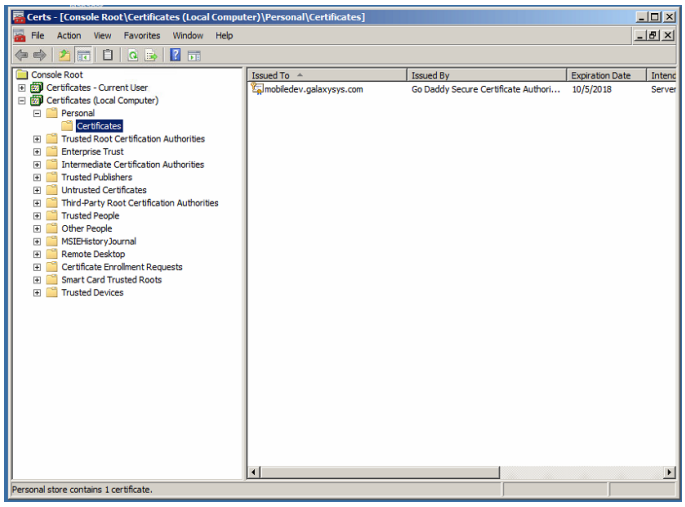


11. Click [Finish] button to accept *local computer*.



12. Double-click on the *Certificate Name* or icon.
13. Select (click) the Details tab.

The Certificate details window will open.



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

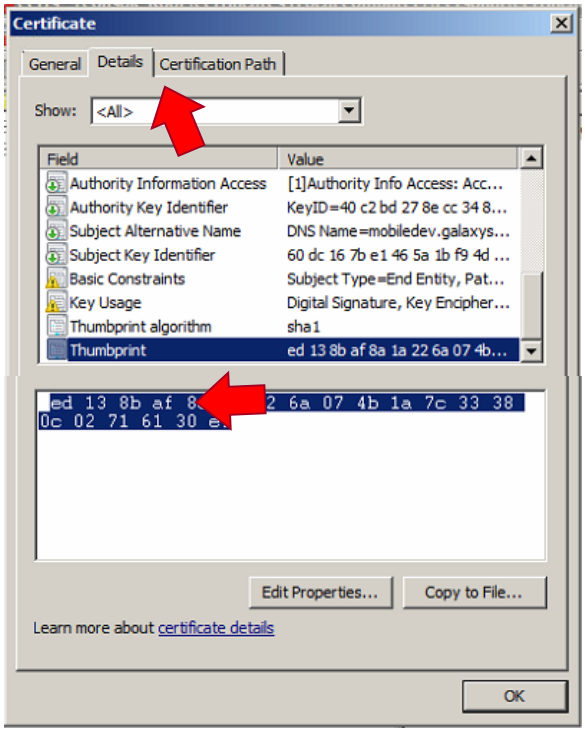
    The entire *hex string* will be displayed in the bottom window.

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

    - **DO NOT copy the leading space character.**
    - **Start with the first non-space character.**
    - **Do not include the spaces between the alpha-numeric characters.**

    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.



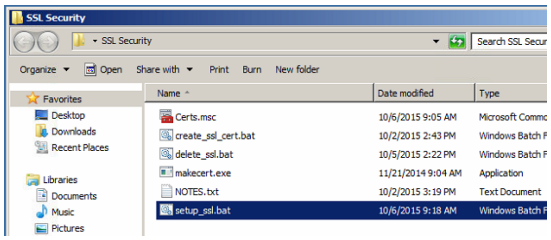
CONTINUE TO NEXT SECTION

5.3.2 ADDING THE CERTHASH (CERTIFICATE THUMBPRINT) TO THE SSL SETUP BATCH

Steps to Add Certhash to SSL Setup file:	*Screenshots*

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

THE SETUP SSL BATCH FILE IS LOCATED IN …
(C:)GCS\System Galaxy\OptionalServices\WebServices



2. Edit the batch file by right-clicking the filename and selecting EDIT from the context menu.

3. Locate the "certhash" string in the batch file.

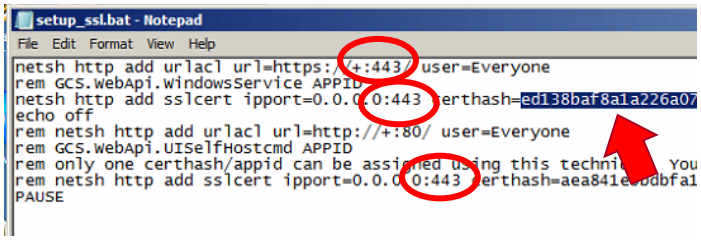
4. Select (highlight) the existing *hex string* and replace it with the *thumbprint hex string* you copied from the Certificate Details.

   Do not include any spaces!

5. Also *<u>if you are not using the default 8443</u>* you must update/change the port number.

   This must be done in every location that the port number 8443 appears in the file. It must match the same port number used for the Web API Service.

6. Save the file and close it.



CONTINUE TO NEXT SECTION

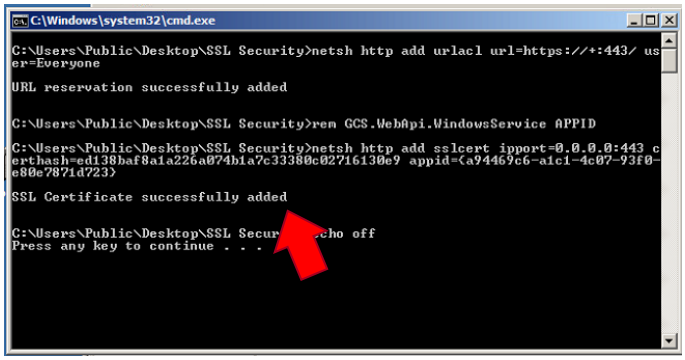
5.3.3 RUNNING THE SSL SETUP BATCH FILE (Adding the Certificate to the Service)

Steps to Assign the Certificate to the Service:	*Screenshots*

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

   A Windows command shell will open.

2. Press *any key* to close the command window after you see the prompt "SSL Certificate successfully added".



Now you should log into one of the Galaxy Mobile Apps using a valid System Galaxy login and verify you can connect to the Web API Service without any problems.

3. Tap the Mobile App and provide the appropriate http connection string which should include your IP and Port number.

IF FOR ANY REASON you get an error >>>
running the SSL Setup batch file, you can remove the thumbprint by running the delete_ssl.bat

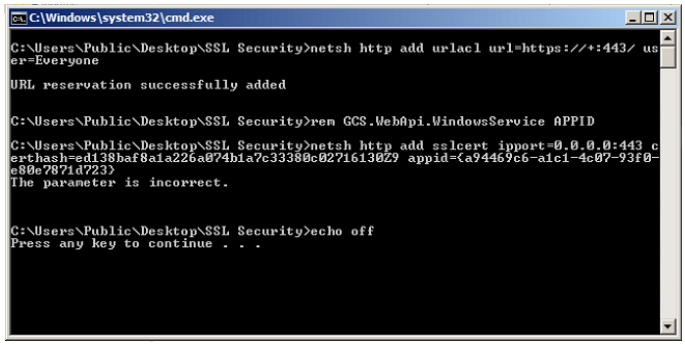
THE DELETE SSL BATCH FILE IS LOCATED IN …
(C:)GCS\System Galaxy\OptionalServices\WebServices

4. Double-click the **delete_ssl.bat** file to delete your SSL certificate thumbprint.

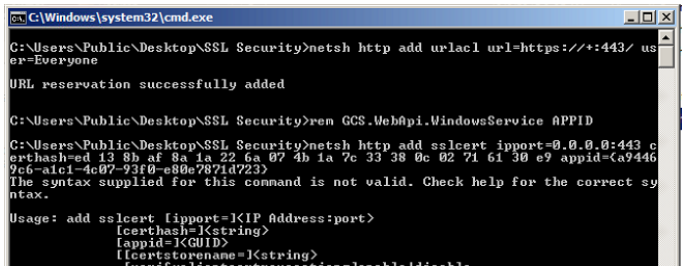
   a) Now you must rerun part 5.3.1 to verify your **thumbprint hex string** is accurate.

   b) Rerun part 5.3.2 to edit the **SSL Setup batch** file correcting any errors to the port numbers or certhash.

   c) Rerun this part 5.3.3 to ***add your SSL Certificate successfully***.



Failed because a character is wrong



Failed because you included spaces

END OF INSTRUCTIONS