System Galaxy Quick Guide INSTALLATION AND CONFIGURATION



GCS Web API Server

FOR GALAXY MOBILE APP COMMUNICATION

SG 10.4.8 (or higher) 1ST EDITION JAN 2016



Table of Contents

1	Inti	oduc	tion to the Galaxy 'GCS Web API Service'5
	1.1	PLAN	NING & DEPLOYMENT
		1.1.1	NETWORK & SECURITY CONSIDERATIONS & ASSUMPTIONS
		1.1.2	SYSTEM REQUIREMENTS & ASSUMPTIONS CONDENSED
2	Ins	talling	g the GCS Web API Service6
3	Cha	angin	g the Port Number for the GCS Web API Service9
4	Tes	sting (he Web API Connectivity10
5	Ob	tainin	g & Importing the CSR Certificate11
	5.1	OBTA	NING A CSR CERTIFICATE 11
		5.1.1	PURCHASING AN SSL CERTIFICATE 11
	5.2	IMPO	RTING THE SSL CERTIFICATE INTO THE CERTIFICATE STORE
		5.2.1	VERIFYING A PRIVACY KEY 12
	5.3	ASSIG	NING THE SSL CERTIFICATE TO THE WEB API SERVER
		5.3.1	CAPTURING THE CERTHASH (CERTIFICATE THUMBPRINT)14
		5.3.2	ADDING THE CERTHASH (CERTIFICATE THUMBPRINT) TO THE SSL SETUP BATCH 17
		5.3.3	RUNNING THE SSL SETUP BATCH FILE (Adding the Certificate to the Service)

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. <u>It cannot share port 80 or 443 with IIS or other apps</u>. » 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:

1. Insert the Galaxy Install CD.

Or copy the GCS Web Services Installer file to the server (pictured).

 Double-click the install executable "SystemGalaxy10_4_8_WebServices.exe"

The Installer will launch.

Computer 🕨 Local Disk (C:)	🕨 🕶 😽 Sea	rch Local Disk ((C:) 🔎
Organize 🔻 📷 Open Burn Nev	v folder		
Name	Date modified	Туре	Size
🐌 GCS	11/9/2015 5:24 PM	File folder	
퉬 inetpub	11/9/2015 5:42 PM	File folder	
🎒 licences	11/9/2015 5:53 PM	File folder	
퉬 Morpho	11/9/2015 6:00 PM	File folder	
PerfLogs	7/13/2009 11:20 PM	File folder	
🌗 Program Files	11/9/2015 5:18 PM	File folder	
🌗 Program Files (x86)	1/14/2016 11:12 AM	File folder	
🕛 ProgramData	11/9/2015 7:15 PM	File folder	
🐌 Users	11/10/2015 5:10 PM	File folder	
🐌 Windows	1/12/2016 12:28 PM	File folder	
SystemGalaxy10_4_8_WebServices.exe	1/12/2016 11:49 AM	Application	11,156 KB
SystemGalaxy10_4_8_WebService Application	es.exe Date modified: Size:		Date created

Screenshots

3. When Welcome screen displays,

click [NEXT] to continue.



ø

Welcome to the System Galaxy Web Services Installation Wizard

It is strongly recommended that you exit all Windows programs before running this setup program.

 \mbox{Click} Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

< Back Next > Cancel

The SG Web Services installer displays the Destination Folder.	Jgr system calaxy web services setup Destination Folder
· ·	Select a folder where the application will be installed.
 Click [NEXT] to accept the default folder path and continue with installation. 	The Wise Installation Wizard will install the files for System Galaxy Web Services in the following folder. To install into a different folder, click the Browse button, and select another folder. You can choose not to install System Galaxy Web Services by clicking Cancel to exit the Wise Installation Wizard. Destination Folder
	C:\GCS\System Galaxy\DptionalServices\WebServices\ Browse Wise Installation Wizard (R) < <u>Back</u> Next> Cancel
	방 System Galaxy Web Services Setup
5 Click the [Choose Available SOL Server] button	SQL Server Connection Select the SQL server and security credentials to be used for SQL script execution during installation.
5. Click the [Choose Available SQL Server] button.	A SQL Server must be selected. The selected SQL Server Instance will be used to create System ODBC Data Sources for the Systal and SystalAirc databases. Galaxy service and client software applications will use these ODBC Data Sources to connect to the databases. Click and Choose an Available SQL Server Instance Selected SQL Server Instance: *
	Use Integrated Windows Authentication
	Vise Installation Wizard®
The <u>Select SQL Server</u> dialog displays the list of <i>SQL Server</i> <i>instances</i> that are currently running on the network. By default this is named GCSSQLEXPRESS.	You must specify the SQL Server computer where the database is located. This information will be used to create the ODBC Data Sources that System Galaxy will use. If you specify the incorrect SQL Server, you will have to manually edit the properties of the SysGal and SysGalArc ODBC Data Sources prior to running any of the System Galaxy applications or services.
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.	Choose the Desired SQL Server: DEV3XGCSSQLEXPRESS CODYXGCSSQLEXPRESS DEV2XGCSSQLEXPRESS
You must choose the <u>correct</u> <i>SQL Server Instance</i> that is running the System Galaxy 10.4.8 database.	IDEVXstQSSQLEXPRESS O7010-TECH3VGCSSQLEXPRESS VMLUKASWIN7/GCSSQLEXPRESS W70360-TESTVGCSSQLEXPRESS W70360-TESTVGCSSQLEXPRESS W810710-TECH1VGCSSQLEXPRESS W810710-TECH2VGCSSQLEXPRESS W810710-TECH2VGCSSQLEXPRESS W810710-TECH2VGCSSQLEXPRESS W810710-TECH2VGCSSQLEXPRESS W810710-TECH2VGCSSQLEXPRESS W910710-TECH2VGCSSQLEXPRESS W910710-TECH2VGCSQLEXPRESS W910710-TECH2VGCSQLEXPRESS W910710-TECH2VGCSQLEXPRESS W910710-TECH2VGCSQLEXPRESS W910710-TECH2VGCSQLEXPRESS W910710-TECH2VGCSQLEXPRESS W91070-TECH2VGCSQLEXPRESS W910-TECH2VGCSQLEXPRESS W910-TECH2VGCSQLEXPRESS
6. Select (highlight) the appropriate instance name.	
7. Click [Continue >>] button.	Continue >>
	X
8. Click [Yes] to accept the selected instance. Clicking No will allow you to return to the list and select a	You have specified 'DEV3\GCSSQLEXPRESS' as the SQL Server to use. Please click the 'Yes' button to confirm and proceed. Click the 'No' button to specify a different SQL Server.
different instance name.	<u>Y</u> es <u>N</u> o

The <u>System Update</u> 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.

Updating System	
The features you selected are currently being installed.	
Starting services	
Service: GCS.WebApi.WindowsService	
Time remaining: 0 seconds	
Wise Installation Wizard (B)	
The mean of the area (in)	Canad

10. Click [FINISH] to close the installer.



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

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

😋 🔍 🕶 📔 « Local Disk (C:) 🕨 GCS 🕨 Sy	rstem Galaxy 🕨 Option	alServices > WebServices	s þ - •	Search WebServices		Q
Organize 🔻 💔 Open 🔻 Burn I	New folder				811 -	0
Name	Date modified	Туре	Size	File version		^
GCS.WebApi.SysGal.Controllers.xml	12/21/2015 9:24 AM	XML Document	55 KB			
GCS.WebApi.SysGal.Entities.dll	1/12/2016 10:30 AM	Application extension	175 KB	1.0.0.0		
GCS.WebApi.SysGal.Entities.xml	12/21/2015 9:24 AM	XML Document	395 KB			E
GCS.WebApi.WindowsService.exe	1/12/2016 11:46 AM	Application	448 KB	1.0.0.0		
GCS.WebApi.WindowsService.exe.config	1/13/2016 11:18 AM	XML Configuration File	12 KB			
GCSActiveDirectory.dll	12/21/2015 9:24 AM	Application extension	51 KB	10.4.2.0		
GCSCompute.dll	12/16/2015 1:45 PM	Application extension	6 KB	1.0.0.0		
GCSSchindlerElevatorSDK.dll	12/21/2015 9:24 AM	Application extension	35 KB	1.0.0.0		
GCSUtilities.dll	12/21/2015 9:24 AM	Application extension	29 KB	1.0.0.0		-
GCS.WebApi.WindowsService.ex XML Configuration File	e.config Date modified Size	: 1/13/2016 11:18 AM : 11.7 KB	Date created:	1/12/2016 10:58 AM		

Notice the <u>GCS.WebApi.WindowsService</u> 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 :

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 <u>GCS.WebApi.WindowsService</u> XML config file.
- 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.
- Enter the *default port number* you wish to find.
 i.e. enter HTTPPort or HTTPSPort
 Visual Studio will highlight the appropriate row.
- 5. <u>CAREFULLY</u> replace the existing port number with your desired port number. <u>DO NOT OVERWRITE OR</u> <u>DELETE ANY QUOTE ("") MARKS OR ANY OTHER CHARACTERS!</u>
- 6. Click [Save] icon on the toolbar to save changes.
- 7. Close the file and Visual Studio window.

🗲 🕞 🗣 🕌 🔍 Local Disk (C:) 🕨 GCS 🕨 Sy	rstem Galaxy 🕨 Option	alServices WebServices	() v	Search WebServices		_
Organize 🔻 🚧 Open 👻 Burn I	New folder				800 -	
Name	Date modified	Туре	Size	File version		
GCS.WebApi.SysGal.Controllers.xml	12/21/2015 9:24 AM	XML Document	55 KB			
GCS.WebApi.SysGal.Entities.dll	1/12/2016 10:30 AM	Application extension	175 KB	1.0.0.0		
GCS.WebApi.SysGal.Entities.xml	12/21/2015 9:24 AM	XML Document	395 KB			
GCS.WebApi.WindowsService.exe	1/12/2016 11:46 AM	Application	448 KB	1.0.0.0		
GCS.WebApi.WindowsService.exe.config	1/13/2016 11:18 AM	XML Configuration File	12 KB			
GCSActiveDirectory.dll	12/21/2015 9:24 AM	Application extension	51 KB	10.4.2.0		
GCSCompute.dll	12/16/2015 1:45 PM	Application extension	6 KB	1.0.0.0		
GCSSchindlerElevatorSDK.dll	12/21/2015 9:24 AM	Application extension	35 KB	1.0.0.0		
GCSUtilities.dll	12/21/2015 9:24 AM	Application extension	29 KB	1.0.0.0		
GCS.WebApi.WindowsService.ex	e.config Date modified	: 1/13/2016 11:18 AM	Date created:	1/12/2016 10:58 AM		



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 <u>GCS.WebApi.WindowsService</u> 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 <u>GCS.WebApi.WindowsService</u>.

O ₀ Services		
File Action View Help		
	II IÞ	
Services (Local) Name	Description Status Startup	Туре
GCS.WebApi.Windov	vsService Automa	atic
GCSActiveDirectoryS	ervice This service Manual	1
GCSAImPnI	Provides co Manual	1
GCSAlphaCom	Provides co Manual	1
GCSCCTV	Provides au Manual	1
GCSClientGW	Provides Ga Started Automa	atic
GCSComm	Provides co. Started Automa	atic

END OF INSTRUCTIONS

Screenshots

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 <u>Server-IP-Address:Port</u> 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.

🚯 Swagger Ul 🛛 🗙 🕂			
	v C	k, Search	
Most Visited 🗍 Getting Started 🗍 Suggested Sites	Web Slice Gallery		
💮 swagger	http://192.168.24.26:8000/swagger/docs/v1	api_key	Explore
System Galaxy Web	API Version 1		
AccessProfile		Show/Hide List Operation	s Expand Operations
Alarm		Show/Hide List Operation	s Expand Operations
Api		Show/Hide List Operation	s Expand Operations
ClusterLoop		Show/Hide List Operation	s Expand Operations
Department		Show/Hide List Operation	s Expand Operations
DoorReader		Show/Hide List Operation	s Expand Operations
Person		Show/Hide List Operation	s Expand Operations
PIVCardholder		Show/Hide List Operation	s Expand Operations
PIVEvent		Show/Hide List Operation	s Expand Operations
User		Show/Hide List Operation	s Expand Operations
[BASE URL: , API VERSION: V1]			21

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 <u>GCS Web API Service</u> 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 ^{\$24} 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. <u>The SSL Setup Batch file will fail if there is not a</u> <u>private key on the Certificate</u>.

- » 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:

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.

👎 🖤 🔼 🗊 🖬 💁 🗣 👎		
Console Root Certificates (Local Computer Personal Trusted Root Certification Certificates Enterprise Trust Intermediate Certification Certificate Revocation Certificate Revocation	ced To A Certificate Name	Issued By Signer's
General Details Certification Path		×
Certificate Information		
instal this certificate in the Trust Authorities store.	sice, io enable trust, and Root Certification	
Issued to: GCSSGWebApDev		
Issued by: GCSSGWebApDev		
Valid from 1/ 1/ 2000 to 1/	/ 1/ 2100 sponds to this certificate.	

Screenshots

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 <u>GCS Web API Service</u> 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*.

Select Computer	X
Select the computer you want this snap-in to manage. This snap-in yill always manage:	Browse
< <u>B</u> ack	Finish Cancel

- 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.

eneral Details Certification Path	1
Show: <all></all>	•
Field	Value
Authority Information Access Authority Key Identifier Subject Alternative Name Subject Key Identifier Basic Constraints Key Usage	 [1]Authority Info Access: Acc KeyID=40 c2 bd 27 8e cc 34 8 DNS Name=mobiledev.galaxys 60 dc 16 7b e1 46 5a 1b f9 4d Subject Type=End Entity, Pat Digital Signature, Key Encipher
Thumbprint algorithm	sha1
🧱 Thumbprint	ed 13 8b af 8a 1a 22 6a 07 4b 🔽
ed 13 8b af 8 Oc 02 71 61 30 e.	? 6a 07 4b 1a 7c 33 38
earn more about <u>certificate details</u>	dit Properties Copy to File

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. 🔒 SSL Secu JO) 🌡 • SSL 🔹 த Search SSL Se Organize 💌 📷 Open Share with 💌 THE SETUP SSL BATCH FILE IS LOCATED IN ... Print 🙀 Favorites Name Date modified Type (C:)GCS\System Galaxy\OptionalServices\WebServices\ E Desktop Certs.msc 10/6/2015 9:05 AM Microsoft Comm Downloads create_ssl_cert.bat 10/2/2015 2:43 PM Windows Batch F Recent Place 🚳 delete_ssl.bat 10/5/2015 2:22 PM Windows Batch F makecert.exe 11/21/2014 9:04 AM Application 詞 Libraries 10/2/2015 3:19 PM Documer NOTES.txt Text Docu setup_ssl.ba 2015 9-18 AM Pictures

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

NOTES.txt 10/2/2015 3:19 PM Te Setup_ssl.bat 10/6/2015 9:18 AM W Open Edit Print

- 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 *if you are not using the default 8443* 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

- 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.

 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\

- 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*.

C:\Users\Public\Desktop\SSL Security>netsh http add urlacl url=https://+:443/ us r=Everyone JRL reservation successfully added

L reservation successfully added

Users\Public\Desktop\SSL Security>ren GCS.WebApi.WindowsService APPID Users\Public\Desktop\SSL Security>netsh http add sslcert ipport=0.0.0.0:443 o hash=ed138baf8a1a226a074b1a7c33380c02716130Z9 appid=(a94469c6-alc1-4c07-93f0pe7871d723) parameter is incorrect.

Nsers\Public\Desktop\SSL Security>echo off

Failed because a character is wrong



END OF INSTRUCTIONS