SunGuide®:

Release 9.0 Installation Notes

SunGuide-IN-9.0

Prepared for:

Florida Department of Transportation
Traffic Engineering and Operations Office
605 Suwannee Street, M.S. 90
Tallahassee, Florida 32399-0450
(850) 410-5600

May 8, 2024

Document Control Panel			
File Name:	SunGuide-IN-9.0.docx		
File Location:	SunGuide CM Repository		
CDRL:	n/a		
Name		**Initial**	**Date**
Created By:	Adam Clauss, SwRI	ASC	09/04/08
Reviewed By:	Steve Dellenback, SwRI	SWD	10/24/08
	Steve Dellenback, SwRI	SWD	01/08/09
	Steve Dellenback, SwRI	SWD	03/06/09
	Steve Dellenback, SwRI	SWD	04/13/09
	Steve Dellenback, SwRI	SWD	05/15/09
	Robert Heller, SwRI	RWH	06/17/10
	Tucker Brown, SwRI	TJB	11/09/10
	Hector Iruegas, SwRI	HAI	11/18/10
	Tucker Brown, SwRI	TJB	02/11/11
	Hector Iruegas, SwRI	HAI	6/22/12
	Tucker Brown, SwRI	TJB	04/15/13
	Robert Heller, SwRI	RWH	05/15/13
	Roger Strain, SwRI	RLS	09/13/13
	Tucker Brown, SwRI	TJB	09/22/14
	AJ Skillern, SwRI	AJS	01/02/24
Modified By:	Adam Clauss, SwRI	ASC	10/24/08
	Adam Clauss, SwRI	ASC	11/17/08
	John Brisco, SwRI	JSB	01/08/09
	Adam Clauss, SwRI	ASC	03/06/09
	Adam Clauss, SwRI	ASC	04/13/09
	Adam Clauss, SwRI	ASC	05/15/09
	John Brisco, SwRI	JSB	06/22/09
	John Brisco, SwRI	JSB	02/11/10
	John Brisco, SwRI	JSB	03/25/10

	John Brisco, SwRI	JSB	05/07/10
	John Brisco, SwRI	JSB	05/10/10
	John Brisco, SwRI	JSB	05/25/10
	John Brisco, SwRI	JSB	06/15/10
	John Brisco, SwRI	JSB	11/04/10
	Tucker Brown, SwRI	TJB	11/18/10
	John Brisco, SwRI	JSB	02/11/11
	Roger Strain, SwRI	RLS	02/11/11
	Tucker Brown, SwRI	TJB	08/08/11
	Tucker Brown, SwRI	TJB	06/22/12
	Tucker Brown, SwRI	TJB	08/01/12
	Hector Iruegas, SwRI	HAI	04/11/13
	Ansley Skillern, SwRI	AJS	09/13/13
	Tucker Brown, SwRI	TJB	10/11/13
	Adam Hoffman, SwRI	AGH	7/11/14
	Tucker Brown, SwRI	TJB	07/30/15
	Ansley Skillern, SwRI	AJS	01/05/16
	Tucker Brown, SwRI	TJB	03/08/17
	Tucker Brown, SwRI	TJB	09/25/17
	Tucker Brown, SwRI	TJB	02/22/18
	Tucker Brown, SwRI	TJB	12/12/18
	Tucker Brown, SwRI	TJB	10/02/19
	Tucker Brown, SwRI	TJB	11/17/20
	Tucker Brown, SwRI	TJB	08/24/21
	Tucker Brown, SwRI	TJB	07/12/22
	Tucker Brown, SwRI	TJB	12/6/23
	Zackary Murphy, SwRI	ZBM	3/12/2024
Completed By:			

Table of Contents

List of Figures

List of Acronyms

CCTV.....Closed Circuit Television
COTS .....Commercial-Off-The-Shelf
DLL.....Dynamics Link Library
DMS.....Dynamic Message Sign
DOT .....Department of Transportation
FDOT .....Florida Department of Transportation
GUI .....Graphical User Interface
IN .....Installation Notes
ITN.....Invitation to Negotiate
ITS.....Intelligent Transportation Systems
SPARR.....Smart Phone Application for Road Rangers
SSL.....Secure Sockets Layer
SwRI .....Southwest Research Institute®
TSS.....Transportation Sensor Subsystem
VDD.....Version Description Document
XML.....Extensible Markup Language

Revision History

Revision	Date	Changes
4.0.0	September 10, 2008	Initial release
4.0.1	September 29, 2008	Updated based on IV&V results as well as new instructions for updating the event type table
4.0.2	October 3, 2008	Updated with CMB revised Event Lists, SAE codes and change of "Accident to Crash" terminology
4.1.0	October 24, 2008	Updated for release 4.1.0.
4.1.1	November 17, 2008	Updated for release 4.1.1.
4.1.2	January 8, 2009	Updated for release 4.1.2.
4.1.3	March 6, 2009	Updated for release 4.1.3.
4.2.0	May 15, 2009	Updated for release 4.2.0.
4.2.2	June 25, 2009	Updated for release 4.2.2.
4.3.0	February 11, 2010	Updated for release 4.3.0.
4.3.2	March 25, 2010	Updated for release 4.3.2.
4.3.3	May 7, 2010	Updated for release 4.3.3.
5.0.0	May 10, 2010	Updated for release 5.0.0.
5.0.1	May 25, 2010	Updated for release 5.0.1.
5.0.2	June 15, 2010	Updated for release 5.0.2.
5.0.3	June 21, 2010	Updated for release 5.0.3
5.0.4	November 4, 2010	Updated for release 5.0.4
5.0.5	February 11, 2010	Updated for SPARR enhancement (release 5.0.5).
5.1.0	August 9, 2011	Updated for release 5.1.0
5.1.1	June 22, 2012	Updated for release 5.1.1
6.0.0	April 11, 2013	Updated for release 6.0.0
6.0.0p1	September 13, 2013	Updated for release 6.0.0p1
6.0.0p2	October 11, 2013	Updated for release 6.0.0p2
6.1.0	July 11, 2014	Updated for release 6.1.0
6.1.0p1	July 30, 2015	Updated for release 6.1.0p1
6.2.0	January 5, 2016	Updated for release 6.2.0
7.0.0	March 8, 2017	Updated for release 7.0.0
7.1.0	September 25, 2017	Updated for release 7.1.0
7.1.1	February 22, 2018	Updated for release 7.1.1
7.1.2	December 12, 2018	Updated for release 7.1.2
7.2	October 2, 2019	Updated for release 7.2
8.0	November 17, 2020	Updated for release 8.0
8.1	August 24, 2021	Updated for release 8.1
8.2	July 12, 2022	Updated for release 8.2
9.0	December 6, 2023	Updated for release 9.0

1. Scope

1.1 Document Identification

This document serves as the Installation Notes (IN) for the SunGuide® Release 9.0 software.

1.2 Project Overview

The Florida Department of Transportation (FDOT) is conducting a program that is developing SunGuide software. The SunGuide software is a set of Intelligent Transportation System (ITS) software that allows the control of roadway devices as well as information exchange across a variety of transportation agencies. The goal of the SunGuide software is to have a common software base that can be deployed throughout the state of Florida. The SunGuide software development effort is based on ITS software available from the state of Texas; significant customization of the software is being performed as well as the development of new software modules. The following figure provides a graphical view of the software to be developed:

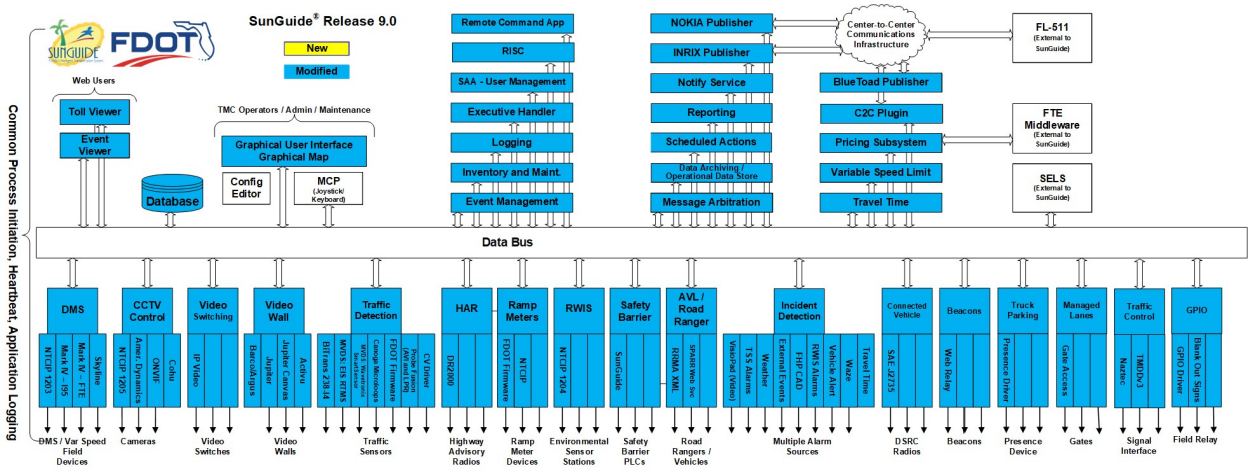


Figure 1 - High-Level Architectural Concept

1.3 Related Documents

Additional information regarding the SunGuide project can be found in the following documents and electronic publications:

- FDOT Scope of Services: *BEH21, Standard Written Agreement for SunGuide Software Support, Maintenance, and Development, Exhibit A: Scope of Services.* May 16, 2024.
- Notice to Proceed: Letter to Southwest Research Institute® (SwRI®) for BEH21, May 17, 2024
- Letter of Authorization 001: Letter to SwRI for BEH21, May 20, 2024.
- SunGuide Project website: http://sunguidesoftware.com.

1.4 Contacts

The following are contact persons for the SunGuide software project:

- Christine Shafik, Traffic Engineering and Operations Office, State Connected Mobility & Technologies Engineer, Central Office, Christine.Shafik@dot.state.fl.us, 850-410-5615
- JoAnna Hand, Traffic Engineering and Operations Office, State TSM&O Software Manager, Central Office, JoAnna.Hand@dot.state.fl.us, 850-410-5444
- Carla Holmes, Gresham Smith Project Manager, Carla.Holmes@dot.state.fl.us, 678-518-3654
- Tucker Brown, SwRI Project Manager, tbrown@swri.org, 210-522-3035
- AJ Skillern, SwRI Software Project Manager, askillern@swri.org, 210-522-6207

For current contact information please refer to this link: http://sunguidesoftware.com/contact-us

2. Installation Notes

This document is intended to be a "companion" document to the SunGuide Version Description Document (VDD). This document will provide detailed notes and tips on how to upgrade the SunGuide software to version 9.0 from version 8.2.

Prior to upgrading the database to version 9.0 PLEASE READ ALL INSTRUCTIONS and ensure that your system is up to date with v8.2, including all hotfixes. The 9.0 upgrade scripts will re-run any necessary 8.2 Hotfix scripts prior to running the 9.0 scripts.

This document contains numerous changes that have been highlighted in red. It also contains a section for "Installation Specific Instructions" that is not normally included. Please read through all sections before starting the installation.

NOTE: It is highly recommended that you test the database upgrade procedure before applying it to any Production database. If any errors are encountered, the database must be restored and the script attempted again after the failure is resolved. If you would like SwRI to perform a test, please make arrangements with SwRI and Central Office.

2.1 Upgrade Procedure

Please follow the steps below to complete the SunGuide installation. Please pay special attention to any notes in red as they are specific to this install.

1. Please close all active events prior to the upgrade.
2. Shut down all SunGuide process including Status Logger and Executive Handler.
3. Ensure .NET Framework v4.8 is installed on all application servers and any machine that will be used to run SunGuide processes or the upgrade scripts.
4. Upgrade config.xml file using the Configuration File Editor and the SunGuide Release 9.0 configuration schema. DO THIS STEP PROR TO RUNNING THE DATABASE SCRIPTS.
    a. NOTE: All passwords in the config file are updated and encrypted as part of this upgrade step.
5. SunGuide Database
    a. Backup the existing SunGuide database by using the SQL Server Import and Export Wizard.
        i. It is recommended that the script be run from the SunGuide database server but if not, please ensure you are able to access "sqlcmd" from the command line.
        ii. From the installation media, run the "runMe.bat" file from the "DatabaseScripts/9.0 Release" folder as an Administrator.
        iii. Enter the correct database information and config file path.
        iv. PLEASE NOTE: There is a prompt at the beginning of the scripts for the location of the SQL Server database files. This is an absolute, local path, from the database server (not where the scripts are being run).
        v. Review the log file for errors.
6. SunGuide Application Servers
    a. If using Windows Server 2016 or higher, ensure the following:
        i. Install IIS and IIS 6 Management Compatibility role and all Sub-Roles. Note that Windows Server 2008 and 2012 use a new version of IIS (7.0

and 7.5) which are not compatible with IIS 6 Applications. When installing IIS, install everything except "Server Side Includes" under the "Application Development" section.

b. Backup the various configuration files (plural) according to the list in the Backup List section below.
c. Uninstall SunGuide via the Control Panel -> Add/Remove Programs on all Application Servers. Reboot if prompted.
d. Ensure that the following folders were deleted on each SunGuide Application Server:
    i. C:\inetpub\wwwroot\OperatorMap (this path may be located on a shared location if running in a clustered environment)
    ii. C:\Program Files\Florida Department of Transportation
e. Install SunGuide via the installer on all application servers. Reboot if asked.
f. **Restore configuration. Please read through the entire step before continuing.**
    i. Restore the various configuration files according to the Backup List section below.
    ii. If restoring the backed up copy of your "OMInterface.dll.config.xml" verify the following entries to the file.

        <add key="deploymentName" value="**<NAME>**"
        <add key="deploymentPath"
        value="http://**<MAPHOST>**/OperatorMap/OperatorMap.application" />

        <NAME> in the first entry should be the unique deployment identifier for your installation, such as your center ID or location (e.g. 'District 9' or 'Broward County'). If installing multiple SunGuide deployments in the same center, each "deploymentName" will have to be unique in order to run each installation's Operator Map from a terminal.

        In the second entry, **<MAPHOST>** should be the network host name or IP address where the map can be reached. By default, the **<MAPHOST>** value in the URL is the hostname of the server the installer was run from. The URL may need to updated for a clustered environment to include the clustered host name.

        If you modify either of these two new values, you *must* sign the map again by running the sign.exe executable application in the Operator Map directory.

        The following tags should be added to your old OMInterface.dll.config.xml if you are restoring the backed up version.

- <add key=" enableEncryption" value="false"></add>
    - Whether or not to encrypt the data traffic from the map to the backend servers. Valid values are "true" to enable encryption, or "false" to disable it.
- <add key=" certificateHost" value=""></add>

- The certificate subject name to use when encryption is enabled.
- <add key=" compressionSize" value="20000000"></add>
  - The threshold (in bytes) after which messages will be compressed by the system when using Intelligent mode.
- <add key=" compressionMode" value="None"></add>
  - The compression mode used by the system to determine when to compress messages sent between different components of the system. Valid values are "Always", "Intelligent", or "None".

iii. The map tiles location in the "OMInterface.dll.config.xml" file must match the actual location of the map tile files. The default location is a folder named "Tiles" under the "OperatorMap" folder. To change the default location, edit the "value" attribute associated with the "key" attribute named "tilesets". The "value" attribute must contain pairs of strings that define the label of the tile set and the file system path of the tileset. The file path can be relative to the "OperatorMap" folder or it can be an absolute path. Note that neither the label nor the file path may contain any whitespace characters

7. SunGuide share data
   a. Report files:
      i. Verify the locations and user permissions of the report templates and exported reports folder as specified in the <RS> section of the config file.
      ii. Copy the newly installed reports to the configured location on the share (see <RS> section in config file). By default, these files are installed to C:\Report Templates.
      iii. If SunGuide is configured to run on an SQL Server database, use the SQL Server reports instead of the default Oracle reports. On the installation media, these are in the ReportTemplates\SQL Server Delivered folder. SwRI support staff will directly coordinate with the district system administrators to provide the updated reports that will be specific to the database from which they will extract data.
   b. Give NETWORK_SERVICE full access to the OperatorMap folder; use the Advanced Tab in the file security dialog to apply to all subfiles and subfolders.
8. IIS Configuration performed on each server hosting the web apps / S: drive:
   a. If using Windows Server 2016 or higher, do the following:
      i. Change the "Default Web Site" to an Application Pool with "Classic .NET AppPool" or an Application Pool set to Classic
      ii. Change the Application Pool for SunGuideAdmin to "Classic .NET AppPool" or an Application Pool set to Classic
      iii. Double click on "Authentication" located in the IIS section of "Default Web Site", select ASP .NET Impersonation and click "Enable" on the right hand side
      iv. Double click on "Directory Browsing" located in the IIS section of "Default Web Site" and click "Enable" on the right hand side (if disabled)

v. Navigate to "Request Filtering" located in the IIS section of "Default Web Site", once there highlight ".config", right click and remove it from list
vi. Turn off Windows Firewall using the Domain, Private and Public tab

b. MOVE the GROUP containing the network name used to access the operator map if in clustered configuration via cluster administrator to the appropriate server.
c. If using HTTPS for web services exposed by SunGuide, HTTPS bindings must be configured.
    i. You'll need the following on the host that you will be enabling HTTPS on:
        a. A valid SSL certificate.
        b. IIS installed on the host.
    ii. An SSL certificate needs to be imported onto the host system to bind it to a port. If you are certain that your certificate is installed properly on the host machine, you can skip this step. If you are not sure, follow these instructions to properly install the certificate.
        a. Navigate to IIS on the machine you want to allow HTTPS traffic on.
        b. In IIS right click on the Default Web Site and say "Edit Bindings..."
        c. From here click add, set the Type to https, leave the IP Address to all unassigned, set the port to the port you want to allow traffic on, finally choose the SSL certificate you want to use.
            - Ask FDOT IT support to obtain a trusted certificate.
            - If a self-signed certificate is sufficient follow the steps to make one in the encryption section.
    iii. For this release, this may specifically apply to the Generic Alert Driver. Be sure to add the binding to the port that was specified for the Generic Alert Driver in the config.xml.

9. Full System Test: Test the system in its entirety to verify that everything is functioning properly to identify and resolve any configuration/deployment issues.

2.2 Configuration Files Backup List

If the installation to be performed is on servers currently configured to execute SunGuide, the following files should be backed up prior to installation so that they can be reused once the new installation is performed.

- config.xml – primary configuration file that contains the settings for all the SunGuide subsystems and drivers
- FL-ATIS_FloodGate_Data.xml – contains the floodgate message "slot" configuration data used by the Floodgate GUI
- IpVideoDevices.xml – provides model specific settings for video devices
- SnapshotDevices.xml – defines video capture devices and corresponding IP video decoder devices
- OMInterface.dll.config.xml – Operator Map client configuration settings
- ProcessList.xml – Executive Handler Server's list of installed services

Note: This is only necessary if the system is not operating in a clustered environment. The Installer will auto-generate a ProcessList.xml for all installed SunGuide application processes.

- Web.config – If uninstalling and re-installing any C2C web services, each web service contains a web.config file for C2C configuration.

    1. If reusing the C2C Web.config files, there are two new values that need to be added.

```
<!-- A value that indicates whether to enable encryption when communicating with Executi
<add key="encryptionEnabled" value="false" />
<!-- The expected host to use when validating a certificate received from a server. -->
<add key="expectedServerName" value="sgapptest.d10.us.swri.org" />
```

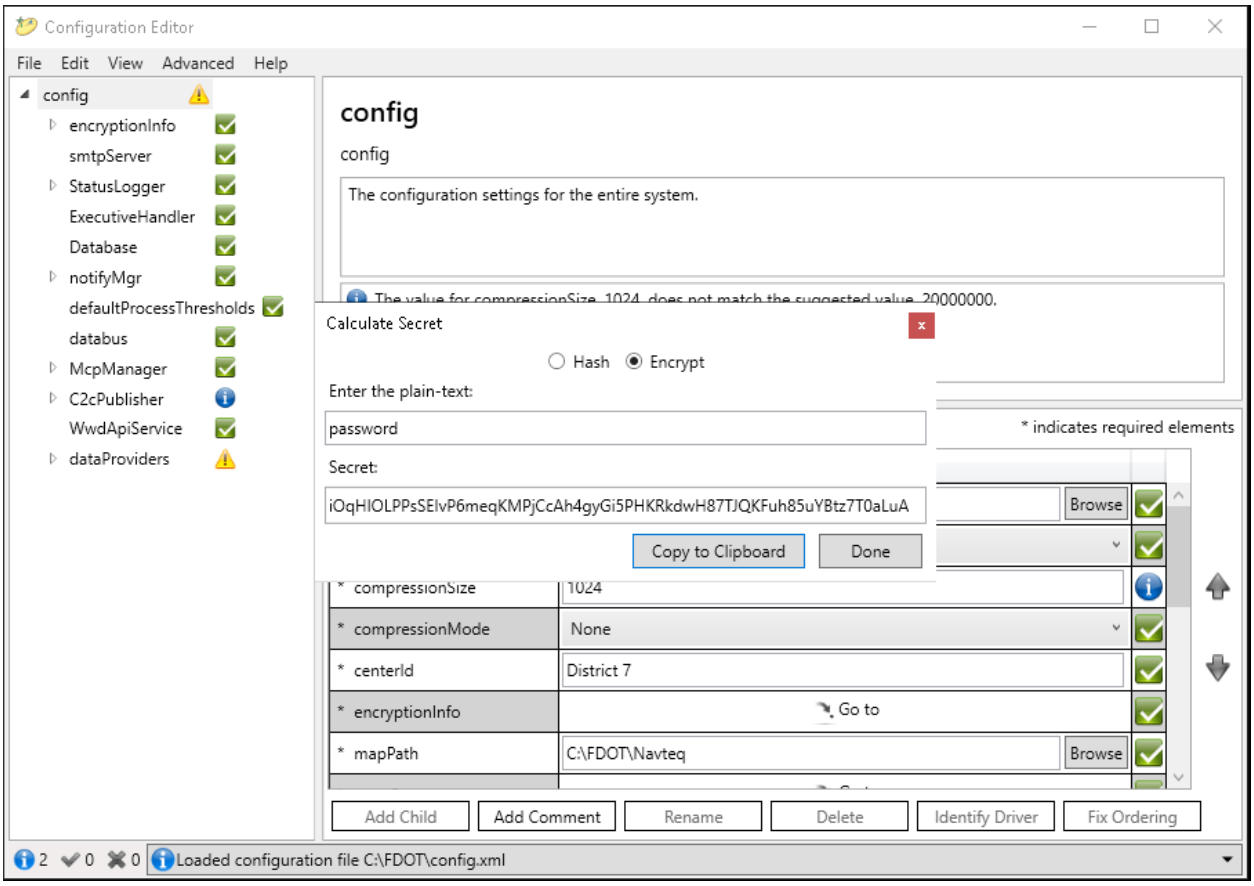
2.3 Post Installation Step

- Ensure 4.g.ii of the Upgrade Procedure was performed!

2.4 Installation Specific Instructions

2.4.1 Passwords

- ALL passwords in the configuration file and transmitted by SunGuide are encrypted.
- ALL passwords in the database are now hashed using the BCrypt hashing algorithm.
- ALL clients to the system (3rd party software) will need to get a new encrypted password to use when authenticating with the system.
    - To generate a new password, launch the Config Editor and, from the Advanced menu item, choose Calculate Secret. The tool allows the creation of a hashed or encrypted password. If a 3rd party will be using the password, select Encrypt and type the password for the user.
    - This tool should also be used to calculate values for use in the config file. This may include subsystem passwords or passwords to external clients (BlueToad, Waze, RITIS FTP, etc).



2.4.2 Encryption

Encryption should only be enabled after confirming all 3rd parties connecting to the system support handling encrypted communications.

NOTE: Encryption supports the highest TLS version supported by Windows. On most Windows OS versions, this is only TLSv1.2. As of Windows Server 2022 and Windows 11, TLSv1.3 is supported.

2.4.2.1 *How to Enable Encryption*

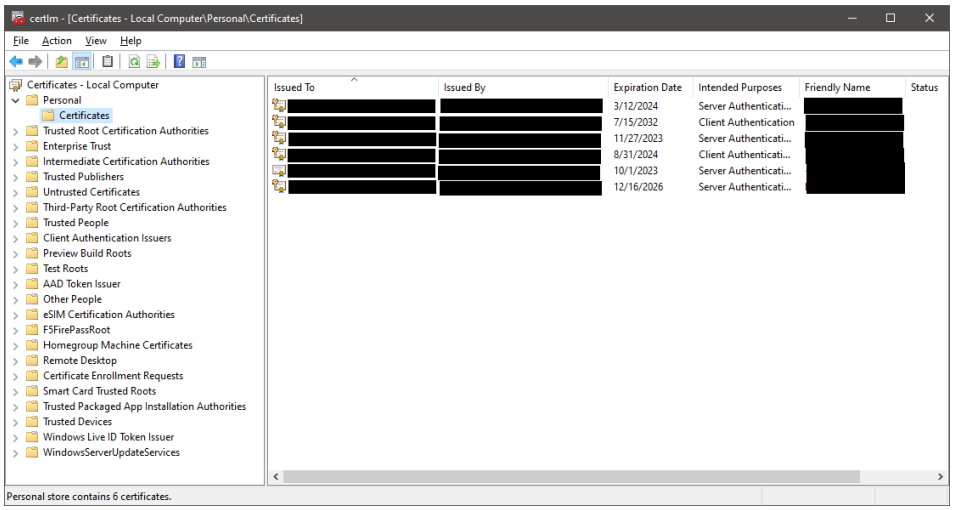
2.4.2.1.1 Stop ALL processes

This includes Status Log Service and Executive Handler Server Service.

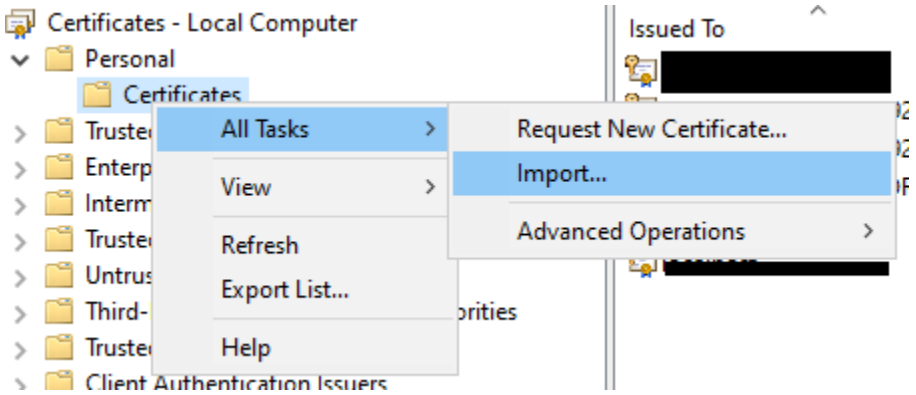
2.4.2.1.2 Install the certificate

Identify a certificate file to use for encrypting traffic. This may be a certificate file provided by a FDOT IT department, or a self-signed certificate made using the instructions below. **Install this certificate on the server, and any computer that will be communicating with this server,**

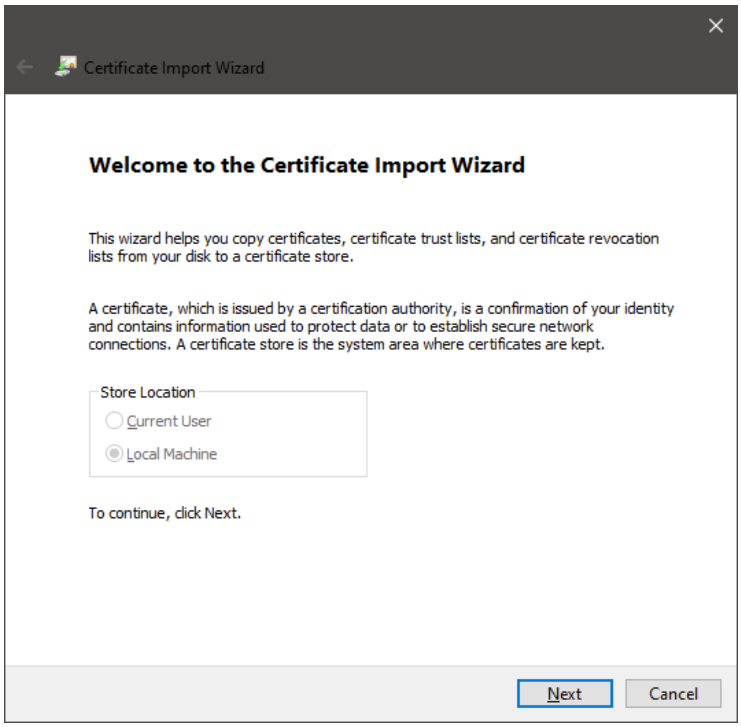
including those that will be running the Operator Map. To install the certificate, open the Computer Certificate Manager.



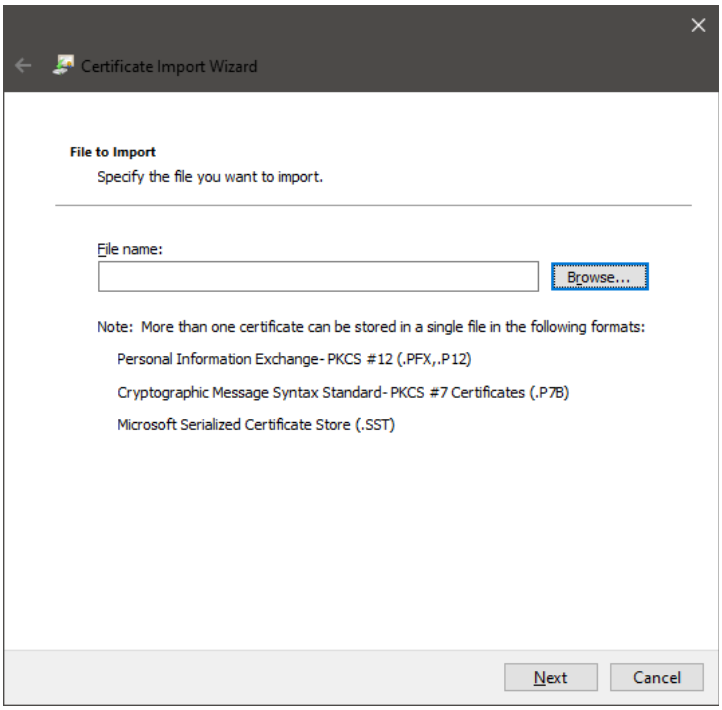
Right click on the folder structure for Personal → Certificates on the left hand side and select the context menu option for All Tasks → Import.



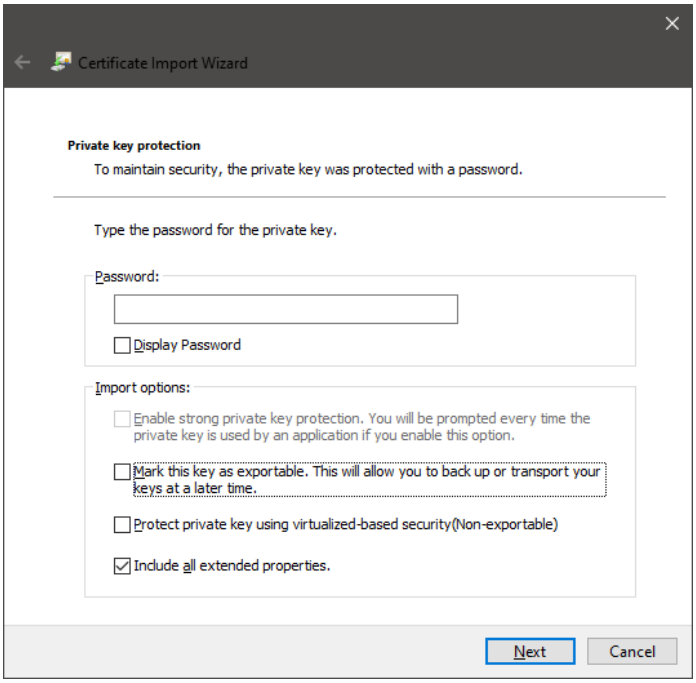
Follow the wizard to import the certificate. On the first screen, be sure the certificate is being imported to the "Local Machine" store. Click Next to continue.



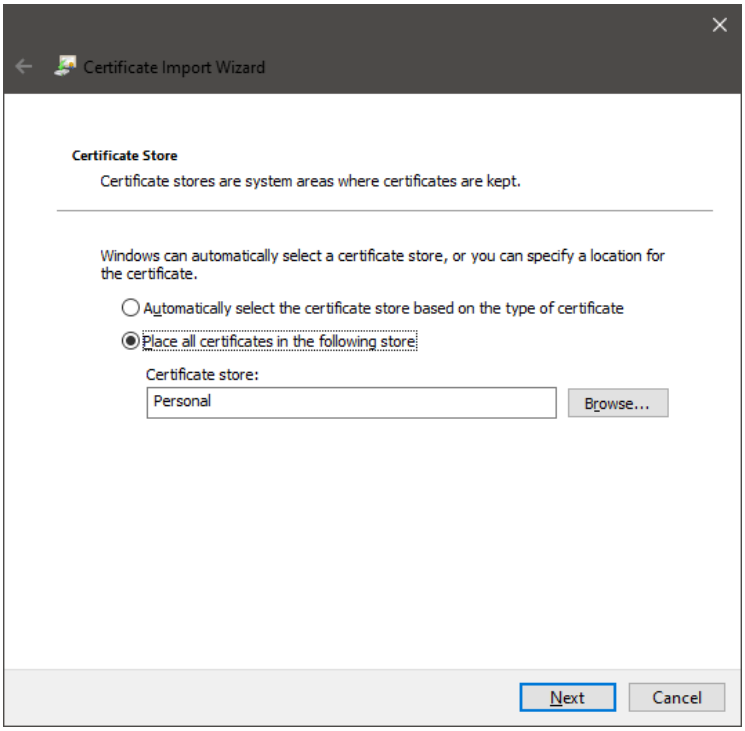
On the next screen, select the certificate file to import. If you do not see the certificate file, check the file extension filter. After specifying the file, click Next to continue.



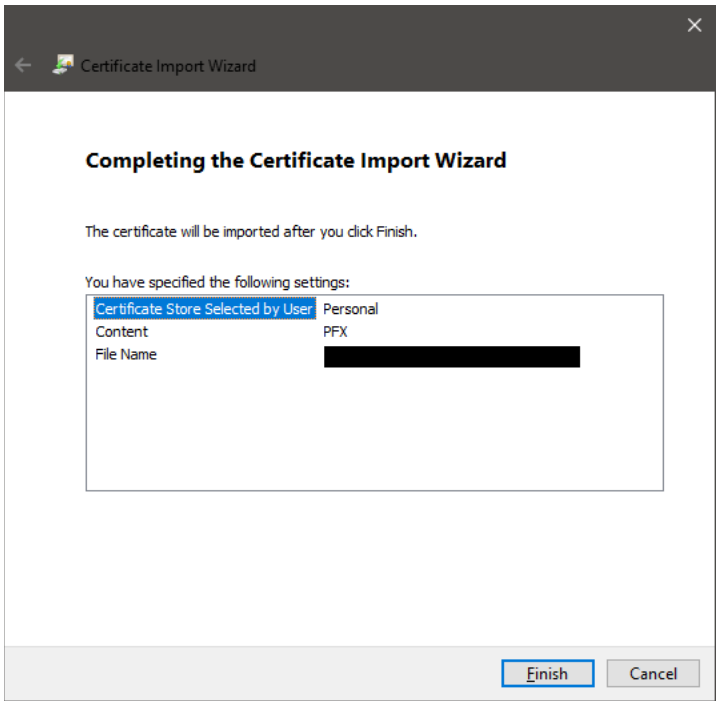
On the next screen, if needed, enter the password for the certificate file. After it has been entered, click Next to continue.



On the next screen, if the selection is anything other than the Personal store, update the store to be the Personal store. Click Next to continue.



On the final screen, click Finish to complete the import.



When using a self-signed certificate, it must also be added to the Trusted Root Certification Authorities list to trust it.

2.4.2.1.3 Generating a self-signed certificate

Open an Administrator session PowerShell terminal window and execute the following sequence of commands, replacing the text that says “ReplaceMe” in the above lines with appropriate values as described below:

```
$cert = New-SelfSignedCertificate -DnsName "ReplaceMe"
$pwd = ConvertTo-SecureString -String "ReplaceMe" -Force -AsPlainText
Export-PfxCertificate -Cert $cert -FilePath "ReplaceMe" -Password $pwd
```

The text to replace in the first line is the DNS name, which is typically DNS name associated with the server(s) where the processes will be running and can be a wild card. The text to replace in the second line is a password to restrict access to the certificate. The text to replace in the third line is the path to write the certificate file to on disk for use in exporting to other machines. It should be the full file path, including file name and extension “.pfx” where the file will be located.

2.4.2.1.4 Update the config.xml file

Open the config file using the Config Editor, Notepad++, or another text editor. Update the encryptionInfo section at the top of the config file to have the following settings:

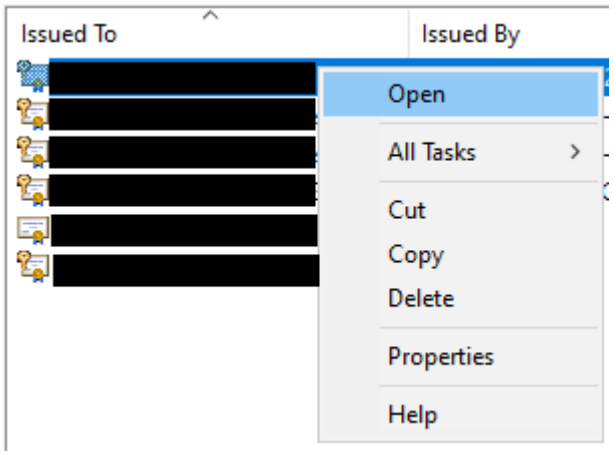
- *enabled* - Set this to true.
- *certThumbprint* - This is the certificate thumbprint as a hexadecimal string. It can be identified using the method described below.

- *expectedServerName* - This must be either the primary or an alternative subject name of the certificate. These can be identified using the method described below.
- *java*
    - *certificatePath* - A path to the certificate file that was imported in the previous step.
    - *certificatePassword* - The encrypted password for the certificate file.
    - *TLSVersion* - Options are TLSv1.2 or TLSv1.3. TLSv1.3 is only supported on Windows Server 2022.

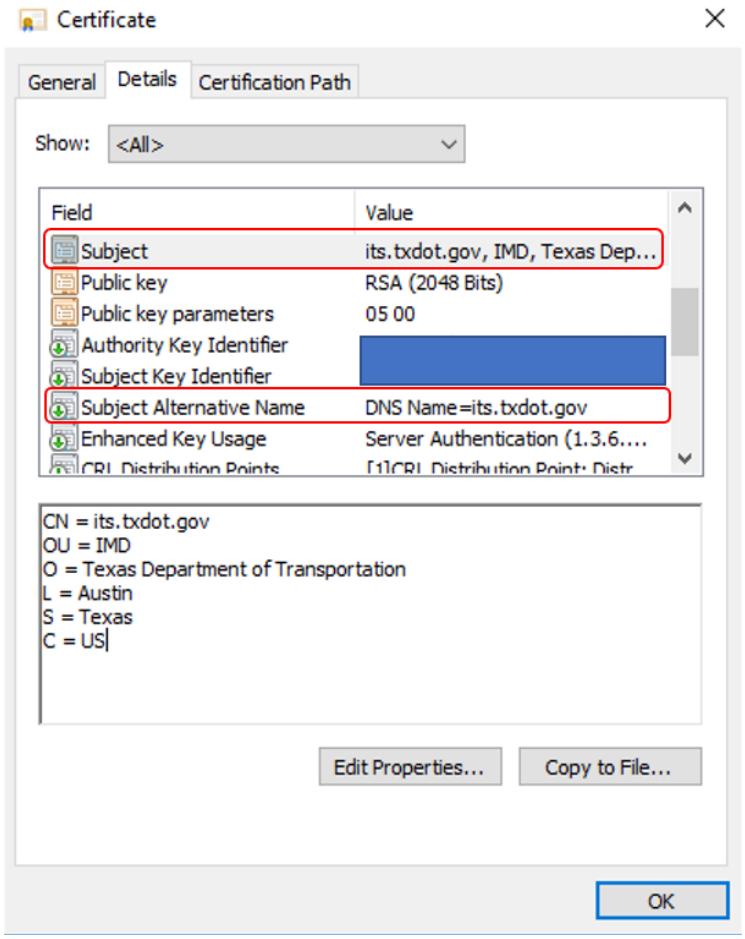
```
<encryptionInfo>
    <enable>true</enable>
    <certThumbprint>[redacted]</certThumbprint>
    <expectedServerName>sgapptest.d10.us.swri.org</expectedServerName>
    <java>
        <certificatePath>\\sgapptest.d10.us.swri.org\FDOT\d10.us.swri.org.pfx</certificatePath>
        <certificatePassword>[redacted]</certificatePassword>
        <TLSVersion>TLSv1.3</TLSVersion>
    </java>
</encryptionInfo>
```

Identifying properties of a certificate

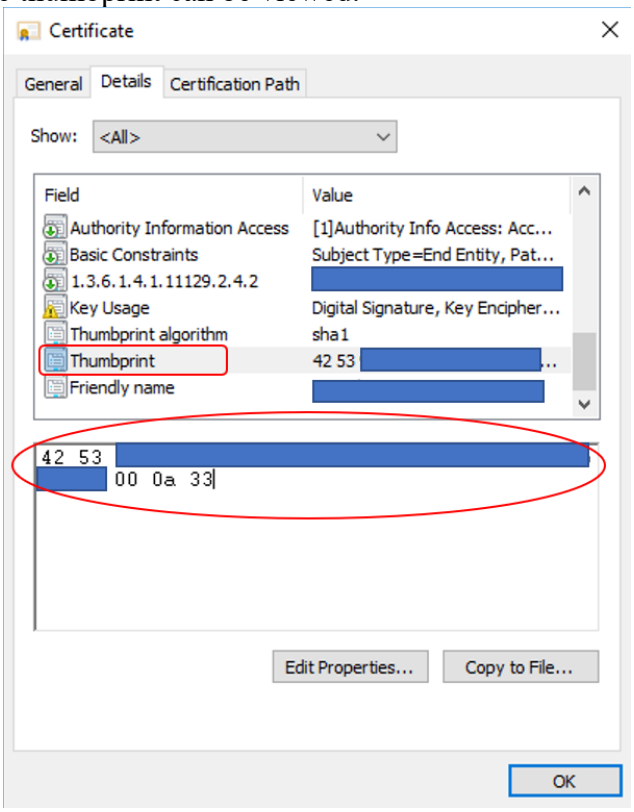
To get the thumbprint or server name(s) of a certificate that has been imported into the computer's store, right click on the certificate and select the option to "Open" the certificate details or just double click it.



Navigate to the "Details" tab and view the properties of the certificate as shown below.

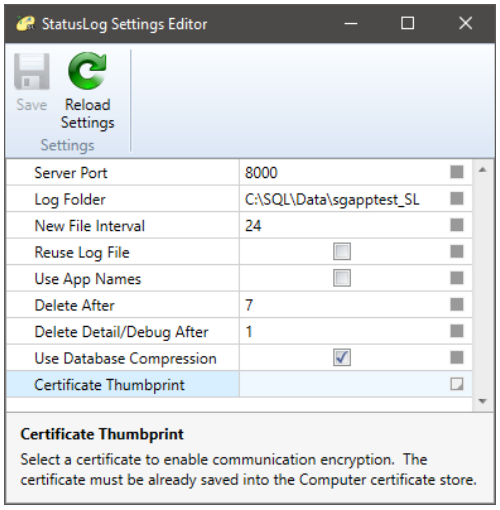

Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Subject
its.txdot.gov, IMD, Texas Dep...
Public key
RSA (2048 Bits)
Public key parameters
05 00
Authority Key Identifier
Subject Key Identifier
Subject Alternative Name
DNS Name=its.txdot.gov
Enhanced Key Usage
Server Authentication (1.3.6....
CN = its.txdot.gov
OU = IMD
O = Texas Department of Transportation
L = Austin
S = Texas
C = US
Edit Properties...
Copy to File...
OK

Within the “Details”, the thumbprint can be viewed.

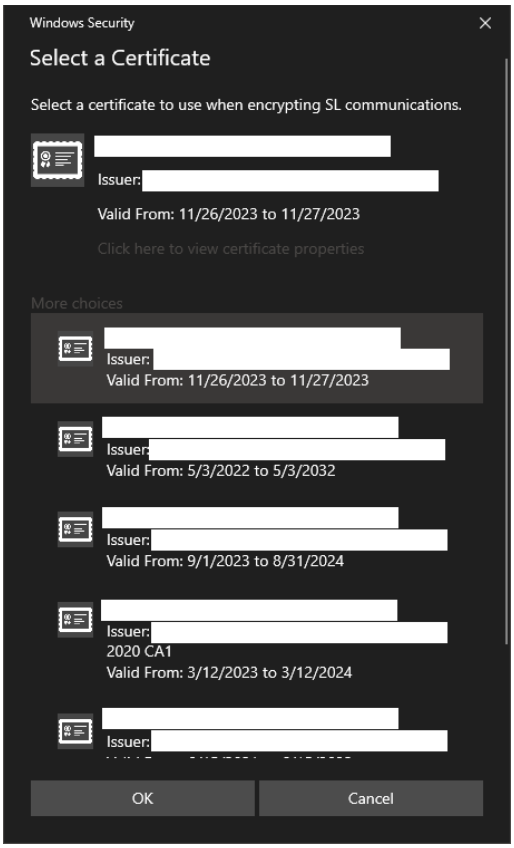


2.4.2.1.5 Status Logger

Open Status Log Settings. Click the blank space for the value into the Certificate Thumbprint row.



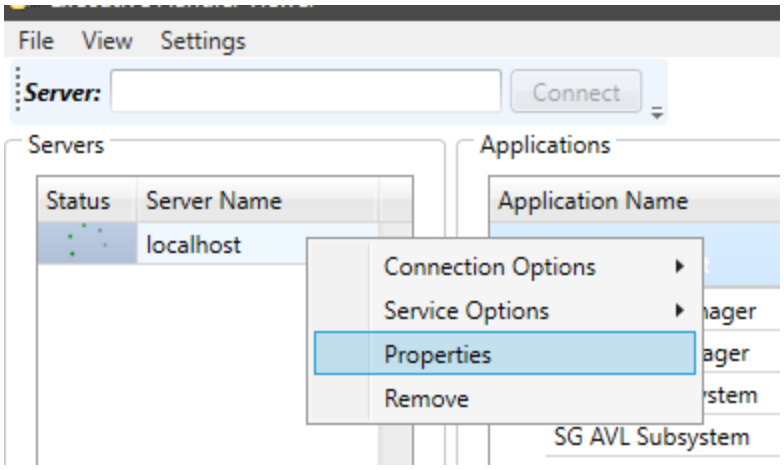
In the window that opens, pick the certificate that you imported in the first step. If you don't see your certificate as the initial choice, select the option for "More Choices" right above the "OK" button.



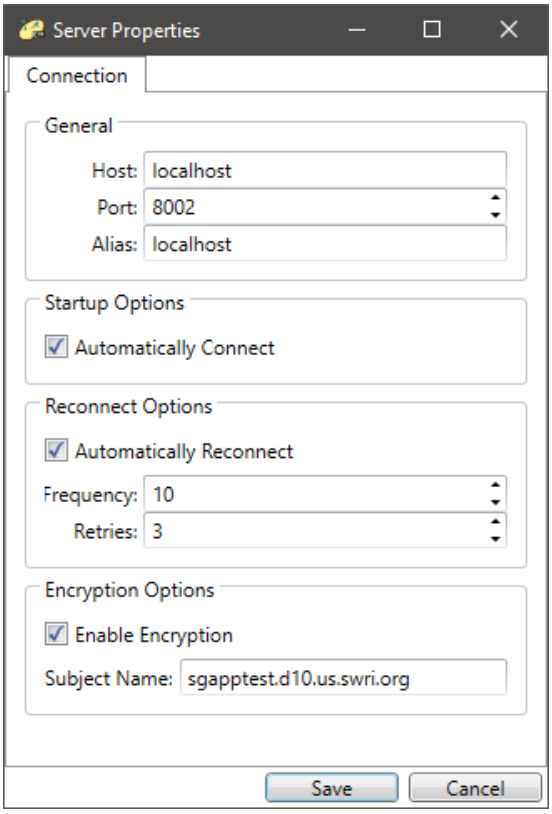
After selecting the certificate, click the "Save" button in the top left of the window.
Start Status Log Service.

2.4.2.1.6 Executive Handler

Start Executive Handler Server Service.
Open Executive Handler Viewer. If you have an already unencrypted connection to the server, you can add a new, encrypted configuration or modify the existing. Once the entry has been added to the server list, right click it and select the Properties context menu option.



In the window that opens, check the box to enable encrypted communications. Type the expected subject name for the connection. After editing the settings, click Save at the bottom.



If EH Viewer does not automatically connect to the server, you can force it to connect by right clicking and selecting the Connection Option to Connect to the server. If you successfully connect to Executive Handler Server, you may begin starting services on the server.

2.4.2.1.7 Operator Map/Event Viewer

Open the OMInterface.dll.config.xml for the Map and Event Viewer. In each file, edit the following settings using Notepad++ or another text editor:

- enableEncryption - Set the value attribute to true.
- certificateHost - Set the value attribute to be a valid subject name of the certificate.

```
<add key="enableEncryption" value="true"></add>
<add key="certificateHost" value="sgapptest.d10.us.swri.org"></add>
```

If modifying the OMInterface.dll.config.xml file of Event Viewer, you will need to manually recycle the associated IIS app pool for the settings to take effect.

2.4.2.1.8 C2C Web Services

Open the Web.config file for all C2C Collector, Command Receiver, Extractor, and Provider web services on the server. Modify the following settings using Notepad++ or another text editor:

- encryptionEnabled - Set the value attribute to true.
- expectedServerName - Set the value attribute to be a valid subject name of the certificate.

```
<!-- A value that indicates whether to enable encryption when communicating with Executive Ha
<add key="encryptionEnabled" value="true" />
<!-- The expected host to use when validating a certificate received from a server. -->
<add key="expectedServerName" value="sgapptest.d10.us.swri.org" />
```

Restart the IIS application pool for any web service that was modified.

2.4.2.2 *How to Disable Encryption*

2.4.2.2.1 Stop ALL processes

This includes Status Log Service and Executive Handler Server Service.

2.4.2.2.2 Update the config.xml file

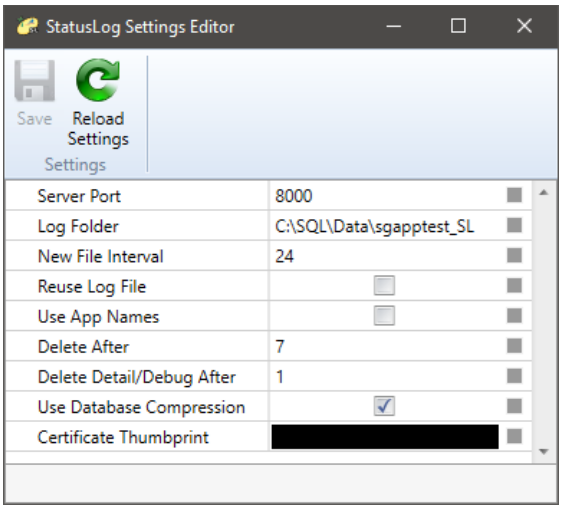
Open the config file using the Config Editor, Notepad++, or another text editor. Update the encryptionInfo section at the top of the config file to have the following settings:

- *enabled* - Set this to false.

```
<encryptionInfo>
    <enable>false</enable>
    <certThumbprint>[redacted]</certThumbprint>
    <expectedServerName>sgapptest.d10.us.swri.org</expectedServerName>
    <java>
        <certificatePath>\\sgapptest.d10.us.swri.org\FDOT\d10.us.swri.org.pfx</certificatePath>
        <certificatePassword>[redacted]</certificatePassword>
        <TLSVersion>TLSv1.3</TLSVersion>
    </java>
</encryptionInfo>
```

2.4.2.2.3 Status Logger

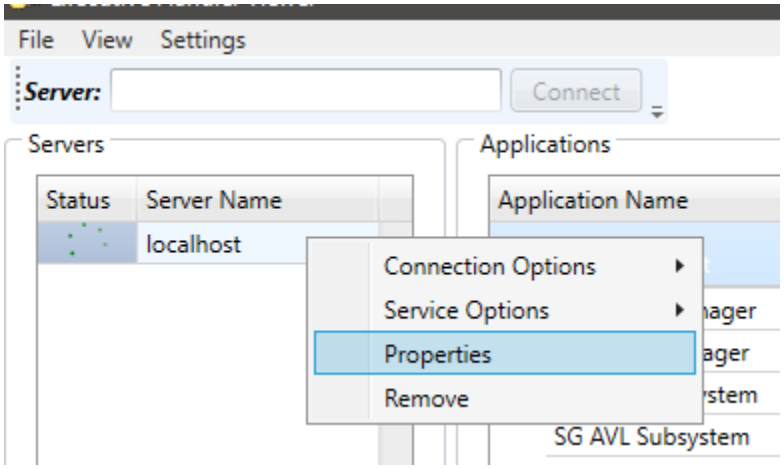
Open Status Log Settings. Click the little grey box to the right of the server certificate thumbprint and click the option to remove the entry.



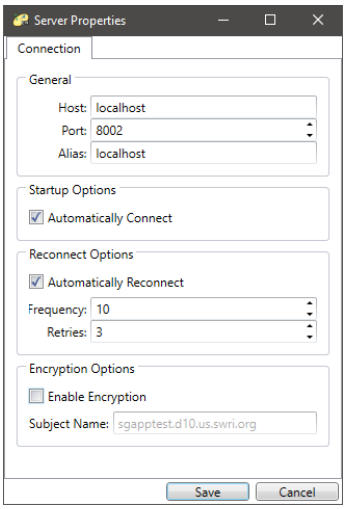
After removing the thumbprint, click the "Save" button in the top left of the window.
Start Status Log Service.

2.4.2.2.4 Executive Handler

Start Executive Handler Server Service.
Open Executive Handler Viewer. If you have an already encrypted connection to the server, you can add a new, unencrypted configuration or modify the existing. Once the entry has been added to the server list, right click it and select the Properties context menu option.



In the window that opens, uncheck the box to enable encrypted communications. After editing the settings, click Save at the bottom.



If EH Viewer does not automatically connect to the server, you can force it to connect by right clicking and selecting the Connection Option to Connect to the server.
If you successfully connect to Executive Handler Server, you may begin starting services on the server.

2.4.2.2.5 Operator Map/Event Viewer

Open the OMInterface.dll.config.xml for the Map and Event Viewer. In each file, edit the following settings using Notepad++ or another text editor:

- enableEncryption - Set the value attribute to false.

```
<add key="enableEncryption" value="false"></add>
<add key="certificateHost" value="sgapptest.d10.us.swri.org"></add>
```

If modifying the OMInterface.dll.config.xml file of Event Viewer, you will need to manually recycle the associated IIS app pool for the settings to take effect.

2.4.2.2.6 C2C Web Services

Open the Web.config file for all C2C Collector, Command Receiver, Extractor, and Provider web services on the server. Modify the following settings using Notepad++ or another text editor:

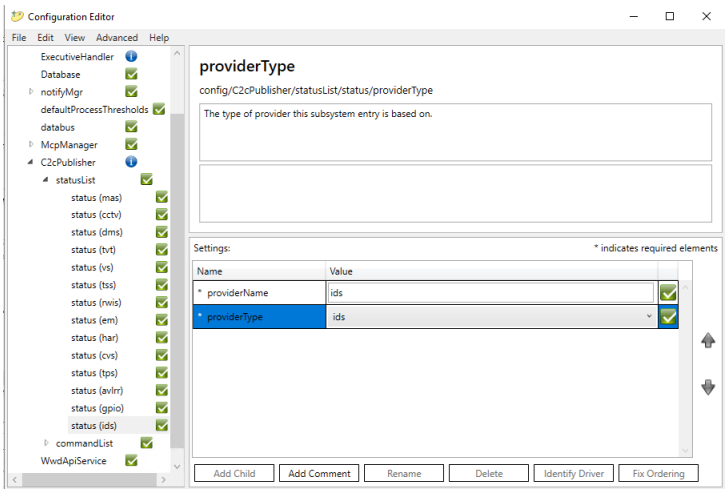
- encryptionEnabled - Set the value attribute to false.

```
<!-- A value that indicates whether to enable encryption when communicating with Executi
<add key="encryptionEnabled" value="false" />
<!-- The expected host to use when validating a certificate received from a server. -->
<add key="expectedServerName" value="sgapptest.d10.us.swri.org" />
```

Restart the IIS application pool for any web service that was modified.

2.4.3 C2C Vehicle Alert Device Data

Vehicle alert device data can now be published via C2C web services.
To do so, add ids as a provider type in the status list section of the C2cPublisher configuration.



Additionally, verify that vehicleAlertStatusData is in the subscriptionDataTypes section of each relevant C2C component's (Collector, Extractor, Provider) Web.config file.

2.5 Operator Map Troubleshooting

- Try uninstalling Operator Map from the list of Add or Remove Programs in the Control Panel and then reinstall from the web site.

2.6 Release Notes

- None