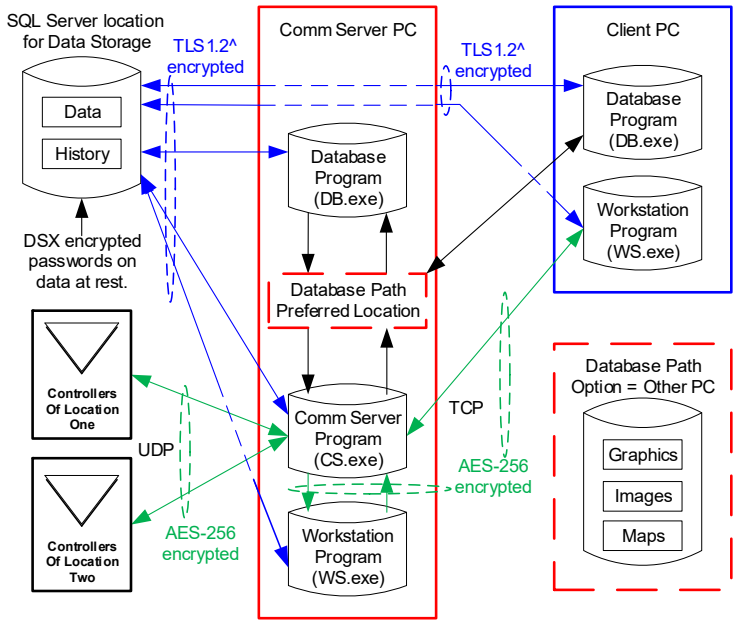
Application Security

Description

DSX has a multifaceted approach to Application Security including Encrypted Communication between the Comm Server PC, Client PCs, and the System Controllers. In addition, SQL Server may store the Database in larger more secure applications. The visual below illustrates application security options.



Comm Server to:	Configurable Ports:
Controllers	4000-5000
Client PCs	22223-22224
Mobile App	60001-60002
SQL Server	1433

AES-256 bit Communications Encryption

The cornerstone of secure communication, AES-256=bit encryption can be implemented between the Communication Server (Comm Server) and the field controllers as well as between the Comm Server and Workstations.
DSX recommends that all Encryption Keys be unique.

One Encryption Key per location for communication to Controllers
One Encryption Key for all Client Workstation communication.

Requirements

Firmware version 3181 or higher in all controllers
Feature be enabled in the USB Features Key.

Technical information about implementations that have been validated as conforming to the Advanced Encryption Standard (AES) Algorithm, as specified in the Federal Information Processing Standard Publication 197, Advanced Encryption Standard is available below.
https://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html
Validation Numbers, AES-1628, AES-1629

Active Directory Operator Authentication

WinDSX can utilize complex logins and passwords facilitated by Active Directory in Windows™ .
Operator Logins can be authenticated by Active Directory instead of WinDSX. This allows for complexity rules to be enforced along with expiration and age of password.

To configure:

1. WinDSX SQL Operators use the same Login Name as they do in Windows™.
2. Login name is entered like always under Operator Passwords in WinDSX SQL.
3. The Operator is assigned a Password Profile but is not assigned a Password.
4. When WinDSX receives a login from an operator that does not have a password in its database it sends the login request to Active Directory (AD) for authentication.
5. If AD authenticates the operator, they are given access to WinDSX SQL according to the Password Profile assigned to them.

DSX-LAN-D and DSX-IP-HUB

The DSX-LAN interface modules are an appliance and have no commercial operating system. They have no drive or memory that can be written to except for the configuration it requires such as IP address and Port number. Antivirus programs cannot be loaded on them or ran against them. They do not appear as a logical drive on the customer network. This appliance simply replies to the UDP packets that are sent to it, if they are properly formed packets coming from the expected source.

DSX Mobile Command App Security

DSX Mobile Command Server does not have an “open” port that can be perused for exploitation. The phone app Login messages are formatted according to a specific service contract and behavior/ It is transmitted with username, password, timestamp, and other phone app proprietary data. These parameters are encoded with a proprietary 256-bit key to provide different encoded data with each timestamp.

Requirements:

- Password and proprietary app data must pass the server’s expectations and the timestamp must be within a small window or the server will reject and terminate communication on that IP port.
- If the login is successful, a randomly generated session key is returned, 256 bit encoded as well, to the phone app. All subsequent messages from the phone app must contain this session key or the server will terminate communication. All parameters and response data are 256 bit encoded with the expected 256 bit key or the server will terminate communication immediately.

Permissions

All Users require Full Control over their Local WinDSX folder and the Shared WinDSX folder (typically the Comm Server). The Shared Folder is Shared to Everyone with Full Control. Each User needs full control over their Temp on the PC they are logged into Windows on. \User\AppData\Temp\DsxTmp

Mixed or SQL Server Authentication: Select SQL Server Authentication and enter a Login and Password. When setting up the Client PCs the first time DBSQL.exe is started it will launch SQLSetup. Enter the Name of the SQL Server and the Username and Password you entered in the SQL Server. This will be done on all PCs the first time the program is run.

Windows Authentication or Named Pipes: Select Windows Authentication. When setting up the Client PCs, the first time DBSQL.exe is started, it will launch SQLSetup.exe. Enter the Name of the SQL Server. Do not enter a Username or Password. This will be done on all PCs the first time the program is run. Rights and permissions must be given to the user in the SQL Management Studio and AD.

Systems on a Domain: Requires a Domain User Account with Local Administrative Rights to the Local folder, the Comm Server PC folder or Shared database folder if different and both SQL databases.

System in a WorkGroup: Comm Server is also the SQL Server, create the Users for each Client and Comm Server in Computer Management\Local Users and Groups\Users. In the SQL Management Studio \Security\Logins add these same accounts from the local Comm Server and set them to Windows Authentication and give them Data_Reader, Data_Writer, and Public rights to AcsData and AcsLog.

SQL 2012 and up Additional Configuration In SQL 2012 and up the TCP/IP protocol and Named Pipes must be enabled. Start the SQL Server Configuration Manager, navigate to Protocols for MSSQL Server. Enable Named Pipes & TCP/IP. Double click on the TCP/IP protocol name. On the TCP/IP Properties window, Click the IP Addresses tab. Scroll all the way down to the bottom. Make sure the TCP Port is set to 1433.

In SQL Server 2012 and up you must manually turn on the SQL Server Browser Service. Go to Services and find **SQL Server Browser**. Double click the Service. Change the startup type from **Disabled** to **Automatic** and Start the service.

Testing Services

Determine what works as an application and what works as a Service:

Workstation should show Primary OnLine in the bottom right corner in Green before setting Comm Server to run as a Service. Before the DSXComm Service is started, the Workstation program should show Comm Loss in the Bottom right corner. When the DSXComm Service is started, it should change to Primary online. If not, the Permissions assigned to the Service will not be sufficient.

Once Comm Server is a Service, DataBase must be a Service also for it to import API files on the same PC. When both are running as a program, DataBase should process API files from the Root of the WinDSX folder C:\WinDSX or the API subfolder C:\WinDSX\API\

Permissions tests for DSX and System Folders

In the DSX DataBase program add and delete a Company and a Comm Port.

Outside of the program open the WinDSX folder and delete the Alarm.mdb
Edit Update.txt and see if you can change the 0 to a 1 and save and close.
Open the Errors folder and create a subfolder called OLD and grab all files in Errors and move them to it.
C:\WinDSX\Errors\OLD
In the C: drive Go to \User\AppData\Temp\DsxTmp and create a folder and a file and delete them both.

Note: These actions should be possible without the operator having to enter a password to complete them.

Moving Folders from old PCs to new such as coming from a Windows 2016 or older Server or Windows 10 and older to a new PC or Server requires that you replace the owner and child permissions for the new server and user(s).

If these tests do not return the proper results, see the Permissions required on the previous pages.