AES-256 Encryption

AES-256 Bit Communications Encryption

Communication encryption is available with both WinDSX and WinDSX-SQL

-Between Communication Server and Field Controllers

-Between Communication Server and Workstations.

Requirements

Firmware version 3181 or higher in all controllers

Communication Encryption feature be enabled in the USB Features Key.

Each Location can have an Encryption Key for communications between the Comm Server and Controllers

A separate Key can be entered for encryption between the Comm Server and all Client Workstations.

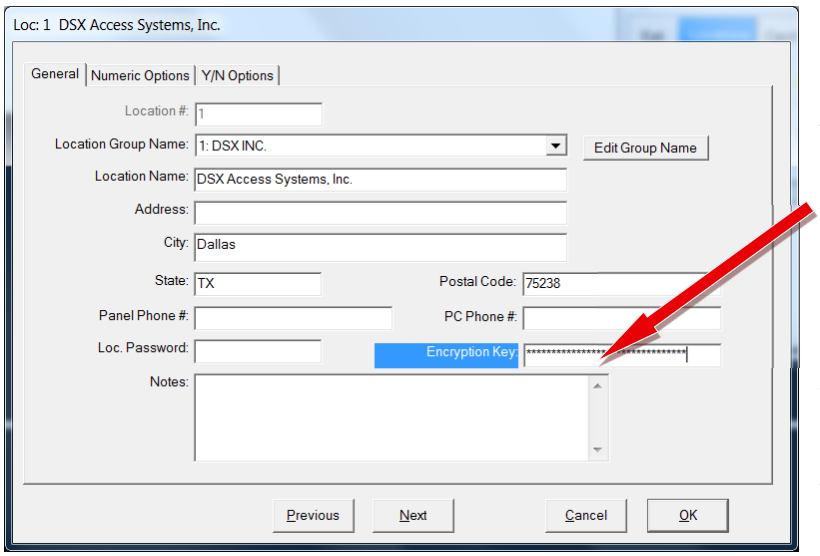
Comm Server to Location Controllers

Encryption Key is entered under each Location – General – Numeric Options – Y/N Options.

This communication includes information between the Comm Server and the Location Master Controller and all Sub Controllers in that Location. Each Location can be given its own key.

The Controllers will accept the Key on a power up. To move a controller in and/or out of encrypted communications requires a reboot of the controller. Enter up to 32 Keyboard characters as the encryption key.

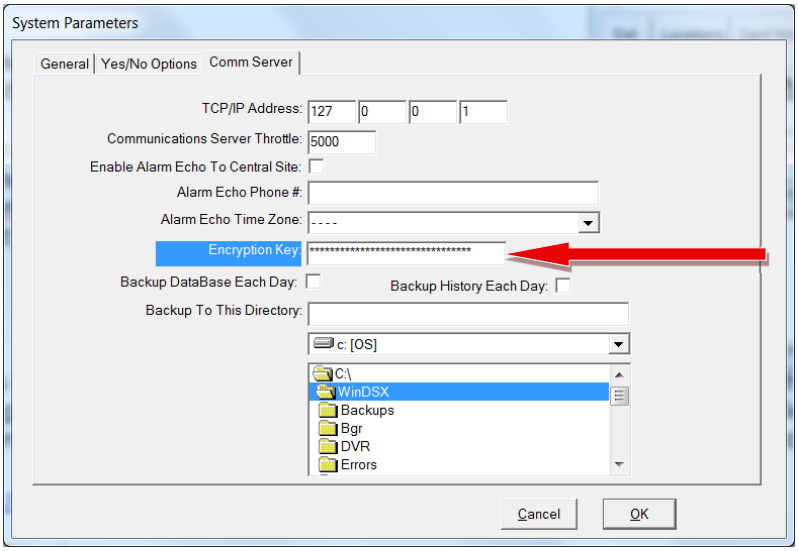
To Implement Communications Encryption to a Location



1. AES-256 must be enabled in the DSX SoftKey and DSX_Key_Monitor must be running and recognizing the key.
2. Enter up to 32 Keyboard Characters in this field and click OK to save.
3. Close the program (File/Exit) and restart. If the Comm Server is running as a Service (DSXComm), stop the service and restart it.
4. Reboot the Master Controller First, followed by All Sub Controllers.

{To remove Encryption would require the same four steps above except in step 2 you would clear out the encryption field.}

To Implement Communications Encryption to the Client Workstations



1. AES-256 must be enabled in the DSX SoftKey and DSX_Key_Monitor must be running and recognizing the key.
2. Enter up to 32 Keyboard Characters in this field and click OK to save.
3. Close the program (File/Exit) on all Client PCs and restart. If the Comm Server is running as a Service (DSXComm), stop the service and restart it.
4. Re Start the Comm Server First, followed by All Client PCs.

The link below provides 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.*

http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html

Validation Numbers
1628
1629