WinDSX Upgrade Instructions

Before Upgrading

1. Prior to Upgrading the Software, make a backup in the DataBase program under Setup. *Do not try to restore this backup into the upgraded software.* This is just a precautionary measure.

2. Next, select File and Exit in all programs on all PCs including the Comm Server. Stop any and all of these Service - DSXComm, DSXKey, and DSXDbas.

Order of Upgrade

3. If this system is using a Dedicated File Server for the database, the software must be un-installed and re-installed in that folder first. If the system is configured to use the Comm Server as the Shared folder containing the DataBase, this PC should be the first one updated. Once the File Server has been updated, the Comm Server is updated next, followed by all other Client Workstations.

Un-Installing WinDSX

4. Locate the appropriate Install folder on the new software distribution media and Open the Install folder and select Setup.exe, right click and select **"Run as Administrator"**. The installer will prompt you to either *Repair or Remove* the old version of software, select "Remove". When the process is finished the WinDSX folder and data will still be intact.

Re-installing WinDSX

5. Once the software is un-installed navigate to the appropriate Install folder on the new software distribution media, open it and locate the Setup.exe, right click and select **"Run as Administrator"**. Follow the prompts and be sure and install the software into the folder where it was just uninstalled from.

6. Once the software is loaded, locate the Db.exe program found in the program directory where the software was just installed. Right click on Db.exe and select **"Run as Administrator"**. Once the Db.exe program is finished updating the database it will leave you on the DataBase Login Screen. If this is a dedicated file server or file share select Cancel and upgrade the Comm Server next. If this is the Comm Server Login to finish the upgrade. When running (Db.exe) on the Comm Server, for the first time after the upgrade, the system may update the Access Levels (see Note /// below).

7. Repeat steps 4 - 7 for the Client PCs that run the WinDSX software. Regional Time Zones and Daylight Savings Options should be configured for each Workstation and each Location. These are found under *System Parameters* and under *Location*.

Note /// When upgrading from version 3.5.15 or lower to 3.5.16 and higher at the Comm Server, the program upgrades the access levels. When upgrading from 3.7.100 or lower to 3.7.101 and higher at the Comm Server or DailyOps PC, the access levels are upgraded to the current schema.

Moving the Comm Server to a Virtual Server or new PC

To migrate the Comm Server to a Virtual Server or new PC, follow these simple steps.

1. Uninstall the software on the existing Comm Server. This leaves the WinDSX folder and all data in place.

2. Copy the WinDSX folder on the Comm Server and Paste it to the target drive of the New PC or Virtual Server.

3. Install the WinDSX software into that same folder. It may be necessary to adjust IP Addresses under System Parameters and Comm Ports.

Permissions

Note /// The User of the system must have Full Control over the local WinDSX folder, the shared WinDSX folder and Read Only to the \Windows\System32\ folder.

Windows 7and 10 / Server 2008 and 2012

When installing DSX programs in these versions of Operating System it is important to right click on the setup.exe and select **"Run as Administrator"**.

The first time the program is started or any of the executables are launched the process should be to right click on the .exe or shortcut and select **"Run as Administrator"**.

This procedure should be performed on any of the following DSX programs when installed; Setup.exe, DB.exe, DbSql.exe, WS.exe if running without DB, PCM.exe, SIO.exe, and L85.exe.

Other Important Documents

DSX Softkey and DSX Key Monitor are now part of all DSX software installations. Locate the DSX Softkey instructions in the "Docs - Software" folder on the software distribution media (dsxsoftkey.pdf). Once you have installed or upgraded the WinDSX software you will need to create a DSX Softkey unless your system already has one. You can determine this by looking in the WinDSX folder on the Comm Server. If you find a DSXKeyData.xml file, your system has a key, and if you can edit a card holder, your key is functional.

Comm Server as a Service is a simple procedure outlined in the DSX Services.pdf. This document is found in the Utilities\CS as a Service\ folder on the software distribution media. All instructions and supporting files are found in this folder. The Comm Server when configured to run as a service will run the DSX Key Monitor program as a service. This negates the need to have the Key Monitor program configured as a service.

Feature Information and Configuration

AES 256bit Encryption

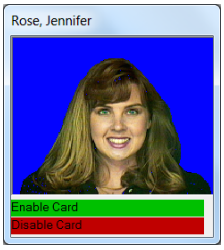
DSX communications can now be secured using AES 256-bit Encryption. The encryption can be implemented between the Communication Server and the field controllers and between Communication Server and Workstations. This feature requires firmware version 3181 or higher in all controllers and that the feature be purchased and enabled in the DSX SoftKey. Each Location can have an Encryption Key entered to encrypt the communications between the Comm Server and that Location's controllers. The AES 256-bit Encryption propagates itself from the Master Controller to all subsequent controllers. Each Location can optionally be given up to 32 keyboard characters as an Encryption Key. The key cannot be viewed once entered. Controllers will only switch in and out of encryption at power up. The Comm Server can be given a separate key to encrypt communications to all Workstations. Enter the Passwords and restart the program. Power the controllers down and up starting at the Master Controller.

Card Enable/Disable from Image Recall Window

There is a new feature that will allow a card to be enabled or disabled from the Image Recall Window in Workstation. When the picture is displayed in response to a card read the operator can double click on the text at the bottom of the window and Enable/Disable buttons will appear.

The operator can click on a button to enable or disable the card that was just read. The feature uses the Database API to send text files that change the stop date of the card. The database program must be running on the Comm Server PC or the Daily Ops PC. Disable will set the stop date to the present time. Enable defaults to setting the stop date to the next day.

See the Software Installation Manual for details. The Enable/Disable setting can be overridden using the C:\WinDSX\RunData\DB_Settings.txt.



Locate the keys below in that file and set how many days the card should be enabled for or what time it is to be deactivated.
Name: CeOffSet
Value: 0 <set this to # of days or to 0 to disable
Default: 0
Desc: DispMug Card Enable date offset. 1=card will be enabled for 1 day. Set to 9999 to enable card forever. **Set to 0 to disable feature.**

Name: CeStopTime
Value: 00:00:00
Default: 00:00:00
Desc: DispMug Card Enable Stop Time. Adds a specific time to the stop date. 13:15:00 would equal 1:15 PM. Set for minutes of 00, 15, 30, 45.

Startup Map

There is a new feature that allows Workstation to display a Map at startup. This can be used where the Map is to always be displayed such as on large monitors in a security office.

To configure this feature, close the program on the PC where it is to be used. Browse to the WinDSX\ RunData\ folder. Locate the WS_Settings.txt file and open. Scroll to the bottom where you will find the entries regarding the Startup Map.

Startup Map Name - name of map within software.
Startup Map Is Maximized - full size of map
Startup Map X Position - starting position
Startup Map Y Position - starting position
Startup Map Save Changes - can be set to YES so that once the program is running and the Map is displayed you can move it to where you want it to be. Once closed, it will start back up in that same position. You can enable Save Changes, start the program, position the map, close the program, set the Save Changes back to No and it will always come up in the place you specified.

Email Notification

Email Groups are groups of people that will be sent an email or text message due to a Location, Device, or Input Alarm. Email Groups consist of a single or multiple Card Holders that each have a Time Zone assigned in the group. The Time Zone selected for each Card Holder determines when that person will receive the email notification for the alarm to which the Email Group is assigned.

Card Holders that are to receive an Email Notification must have an Email Address in a UDF field that is configured as an Email Address. Email Groups can be assigned to a Location, to each Device and to each Input as desired. Those that have an Email Group assigned will send an email or text message upon alarm. See the Help on Email Groups and UDFs.

Before Starting:

1. You need an exchange server or an ISP such as ComCast or RoadRunner. Alternatively, you can use web based email such as Gmail or Yahoo as your email server if you know what ports are required and your fire wall allows access through these ports. For Gmail: Change your settings > Go to the "Less secure apps" section in My Account. Next to "Access for less secure apps," select Turn on. (Note to Google Apps users: This setting is hidden if your administrator has locked less secure app account access.)

2. Test to make sure that you can send an email to yourself. Then try to send an email to one of the desired target email addresses from this email client program.

3. Make sure that the Windows User has full control over the local WinDSX Folder on the Comm Server PC where the software is installed.

4. To setup up the Email client, this PC must have the .NET Framework 4.0 or higher installed.

OlMail.exe configuration:

5. In the WinDSX folder on the Comm Server PC there is a file called OlMail.exe. This program has to be run once and initialized: Double Click on OlMail.exe.
A.) Enter the Name of the “SMTP Server” to send the email through.
B.) Enter the “Port Number”. The default is 25. You may have to get this information from your IT department or from your email provider.
C.) Enter the “From Email Address” that will be used on all email's sent. This is the User Name from the email provider.
D.) Select “Server Requires Authentication” if the SMTP Server requires a password. Enter the Password in the "Password" field.
E.) Select "Server Requires Secure Sockets Layer" if SSL is required.
F.) Select “Log Command Lines” for trouble shooting purposes only. This will cause OlMail to create an OlMail.txt file to be written into the c:\WinDSX\Errors folder on the Comm Server PC.

WinDSX Configuration:

6. Once the above has been configured it is time to configure the WinDSX Database program.

A.) Define a UDFName and configure it as *“Data is Email Address”.*

B.) Edit or Add a cardholder and assign an email address to the UDF designated as an Email Address field.

C.) Create an Email Group and assign it to those Locations, Devices, and Inputs that you want to initiate an Email Notification.

For more information go to Email Groups in the DSX software and Press F1. Then select "Click here for step by step instructions".

DataBase Configuration Settings

Starting with Version 3.10.1 - all database configuration settings are now in the RunData folder. This includes all text file and registry settings. The gDb_settings.txt contains global settings and will reside in the RunData subfolder of the shared DSX directory. The Db_settings.txt file contains local settings and will reside in the RunData folder of the local DSX directory. For more information see the Software Installation Manual.

To make changes to these configuration files the program must be exited. Once closed edit the file and set the appropriate entries under Value: Save the file and restart WinDSX.

gBD_Settings.txt < located in the WinDSX\RunData\ folder of the shared directory.

Name: DailyOps
Desc: If you do not want the comm server to run daily ops enter the workstation number that will run daily ops. CS as a Service.exe will modify this file.

Name: HsAISql
Desc: Name of SQL Server for High Security Area Log

Name: HsAIDb
Desc: Name of Database on SQL Server for High Security Area Log
---
Name: HsAIUdf
Desc: UDF number stored with High Security Area Log. Unique ID.

Name: HideLgIn
Desc: 0 = Off, 1 = On. Set to 1 to hide the last login name at startup.

Name: IssueLev
Desc: 0 = Off, 1 = On. Set to 1 to change the Card Number field to work as an issue level
---
Name: PwLength
Desc: Minimum length accepted for operator password

Name: InRptByLoc
Desc: Print the Who Is In report by location. Use a start { and a stop } to contain each loc that should be included. {0,6,1,2,;\\myserver\waybackprinter}{1} This is two groupings print Locs 6,1,2 and send to waybackprinter. Second grouping will print Loc 1 and send to default printer. See the help system for more details.

DB_Settings.txt - only partially displayed here. < located in the local WinDSX\RunData\ folder of each PC where the software is installed.

Name: InOutTimer
Desc: How often In/Out Screen Refreshes In Seconds. Limit is 99.

Name: BcNB
Desc: Barcode: Width of Narrow Bar in inches

Name: BcRatio
Desc: Barcode: Ratio of Wide Bar to Narrow Bar

Name: BcBB
Desc: Barcode: 0 = Off, 1 = On. Set to 1 to enable Bearer Bars (Horizontal lines at top/bottom of barcode)

Name: BcAA
Desc: Barcode: 0 = Off, 1 = On. Set to 1 to enable auto alignment of barcode to edge of card
---
Name: TaRpt
Desc: Name of the custom Time and Attendance report to use.

Name: DelHist
Desc: How many days of history are stored before auto delete. Only valid on non SQL systems at the DailyOps PC. Zero = no delete
---
Name: IbCardType
Desc: Change the Card type for Integrated Biometrics integration. 1 = 26 bit, 2 = DSX 33 bit
---
Name: IbFacCode
Desc: Change the facility code for Integrated Biometrics

Name: AuxEx
Desc: Text to display in the Aux Export button of Card Holder General Tab
---
Name: AuxExExe
Desc: Name of exe to call from Aux Export button

Name: DoTime
Desc: When will DailyOps occur. Default is Midnight.

Name: DoDate
Desc: Last date DailyOps occurred.

Name: BuRoll
Desc: How many auto backups before roll over.

Name: AuBakNum
Desc: Current auto backup number.

Name: HidePIN
Desc: Set to any character to hide the PIN entry on Card form. Will display that character instead of PIN