XPressEntry / OnGuard Synchronization

Revision 9/16/2019

For use of the
XPressEntry Mobile Access Control System
with OnGuard

By

TELAERIS, **Inc.**

Important Notice

Trademark Acknowledgements

Telaeris, Inc.
9123 Chesapeake Drive
San Diego, California 92123
United States of America

(858) 627-9700

www.telaeris.com

Contents

Purpose

This document is intended to allow the user to synchronize an XPressEntry system with an OnGuard system.

Installation Pre-requisites

1) Onguard 7.0 or later Installed
2) XPressEntry Server 2.7+ Installed
3) OnGuard DataConduIT or OnGuard OpenAccess Enabled

License Requirement

1) DataConduIT/OpenAccess License for OnGuard – From Lenel
2) XPressEntry License with OnGuard Feature Enabled – From Telaeris

OnGuard Services

The following services should be enabled on the OnGuard Application Server or respective server:

DataConduIT:
LS DataConduIT Service
LS Communication Server
LS License Server
LS Linkage Server

OpenAccess:
OpenAccess Service
LS Communication Server
LS Web Service
LS Web Event Bridge
LS Event Context Provider Service
LS Message Broker Service

Setting Up OnGuard to Synchronize with XPressEntry

It is assumed OnGuard is installed with DataConduIT or Open Access enabled. If using DataConduIT a user with sufficient permissions for WMI to communicate is logged in.

Order of Operations

1) Set up OnGuard Data
2) Enable Synchronization from XPressEntry
3) Set up XPressEntry Data

Setup OnGuard Data and Settings

Handhelds

A XPressEntry handheld can act as any existing reader within Onguard, or as a dedicated entry and exit reader. For the latter, every physical XPressEntry handheld reader can have up to two logical readers in the OnGuard System. These should be distinguished with the words "Entry/Exit" or "IN/OUT" at the end of them. This will allow you to have one logical door for Entry and Exit readers per handheld. For example: Main Gate IN and Main Gate OUT. If only one direction will be tracked per handheld, you only need to create a single reader. For XPressEntry mustering, a reader can be added to exit the individual from the hazardous area.

XPressEntry Panel

Each reader created for XPressEntry will be added to an OnGuard Access Panel. You may create any type of access panel such as an LNL-2000 or LNL-2220. A physical access panel is not required. The "virtual panel" is required for handheld events to appear in Alarm Monitoring. It is suggested to use an easily distinguished name such as XPressEntry. *(Note that this can also be an actual panel.)* Optionally, if you are using the XPressEntry Device Translator Panel plugin, this may be used as the access panel.

XPressEntry Device Translator Panel (Optional)

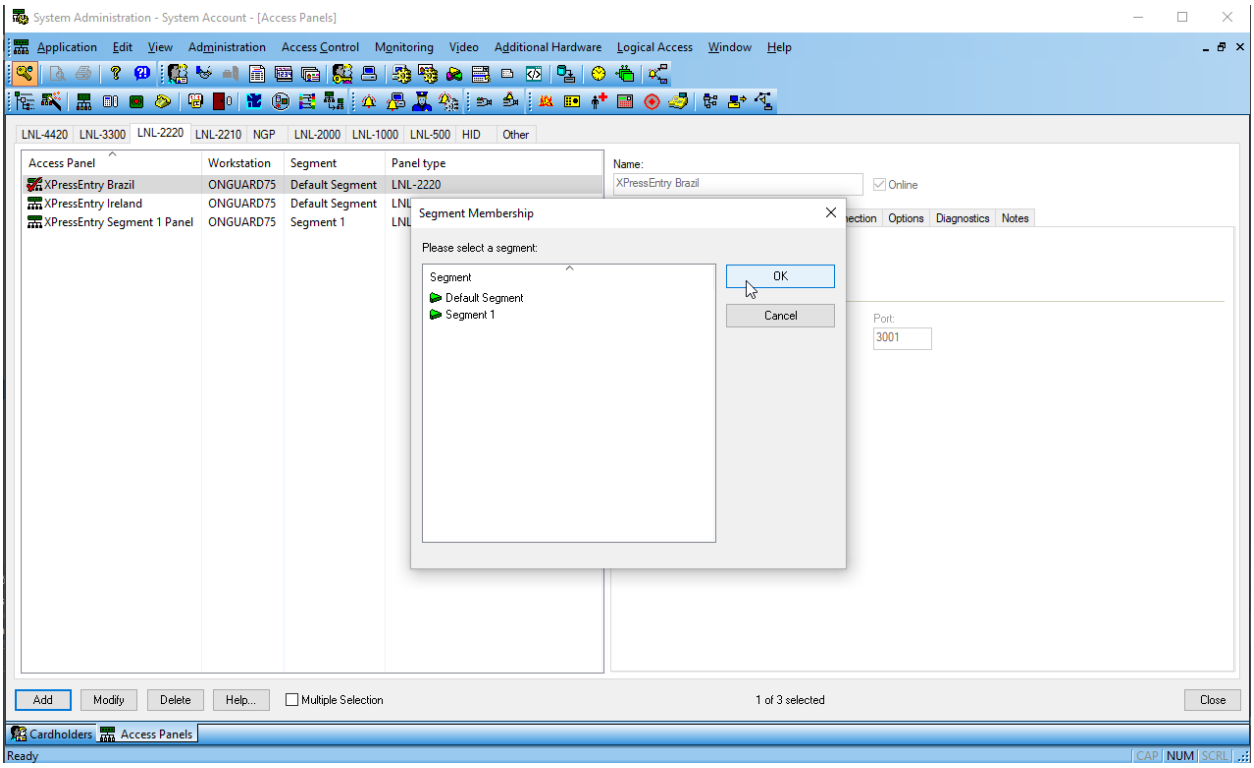
The XPressEntry Translator Panel is used to interface the XPressEntry system as a panel and the handhelds as live readers on the OnGuard System. With the Device Translator installed OnGuard can monitor the Online/Offline status of XPressEntry handhelds and server much like any OnGuard panel.

Device Translator Setup (Optional)

Download the XPressEntry Device Translator zip and extract the folder. Run the appropriate MSI installer for your version of OnGuard Under "Other" in Access Panels you should now have an XPressEntry Panel Type.

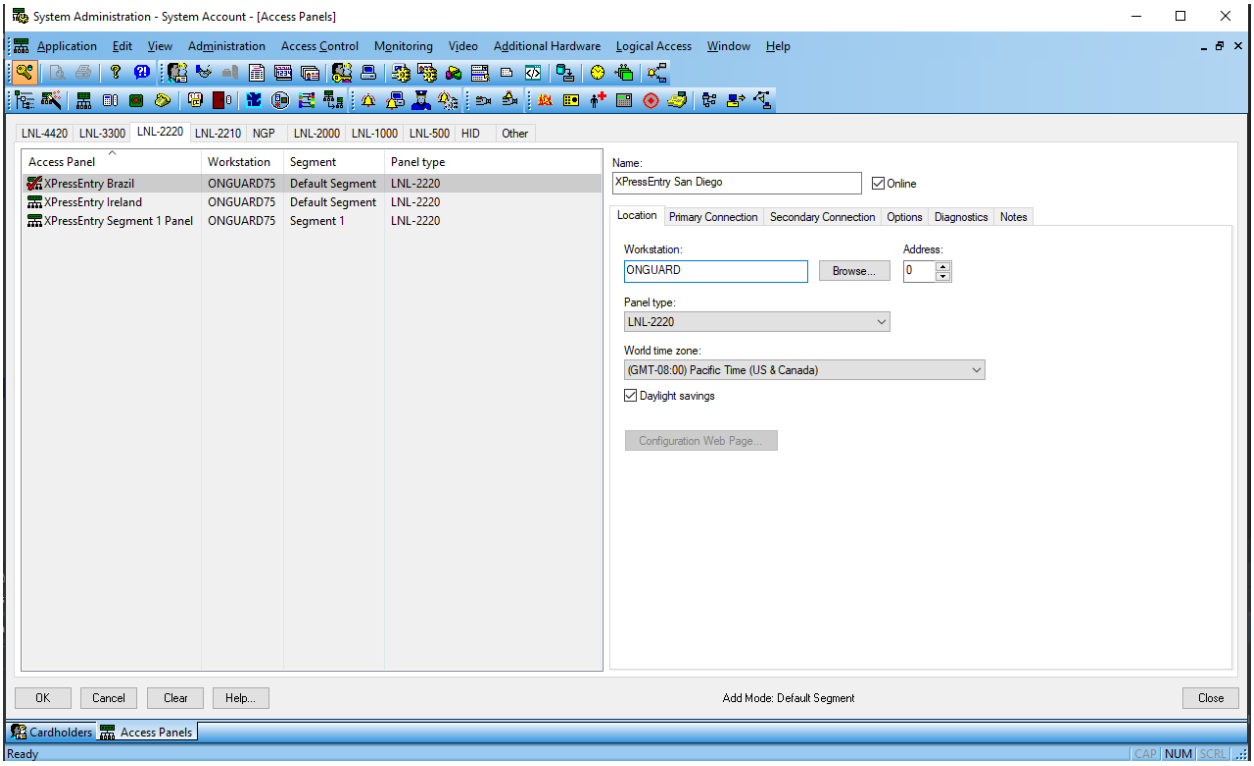
Panel Setup

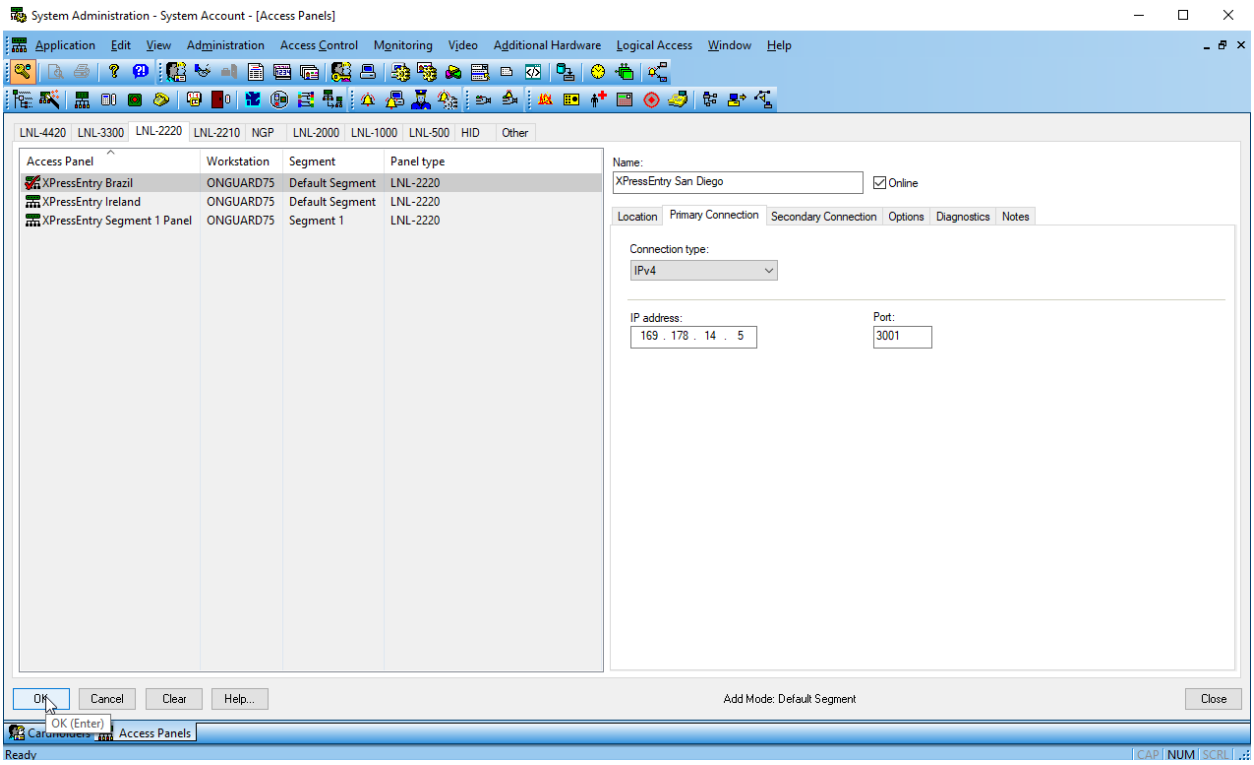
Create a new Access Panel. To create a new access panel in System Administration, select the Access Control Menu Option -> Access Panels. Select the LNL-2220 or any panel type you would like to add. If utilizing the Device Translator Panel, select the "Other" panel type. Click Add at the bottom left. Select a segment if required.



Although we are not connecting to a physical access panel, only three main settings are required.

1. Make sure the panel is set to “Online.”
2. In the location tab, set a workstation name. This can be the name of the application server for OnGuard.
3. Set the Primary Connection. OnGuard requires a default primary connection. Again, this is not connecting to a physical online panel. Select IPv4, and add invalid IP address into the IP Address box.





Click OK to add the new panel. Add the panel to the correct Monitor Zone. If you are not sure, select *Default Zone*.

Adding Entry/Exit/Muster Readers

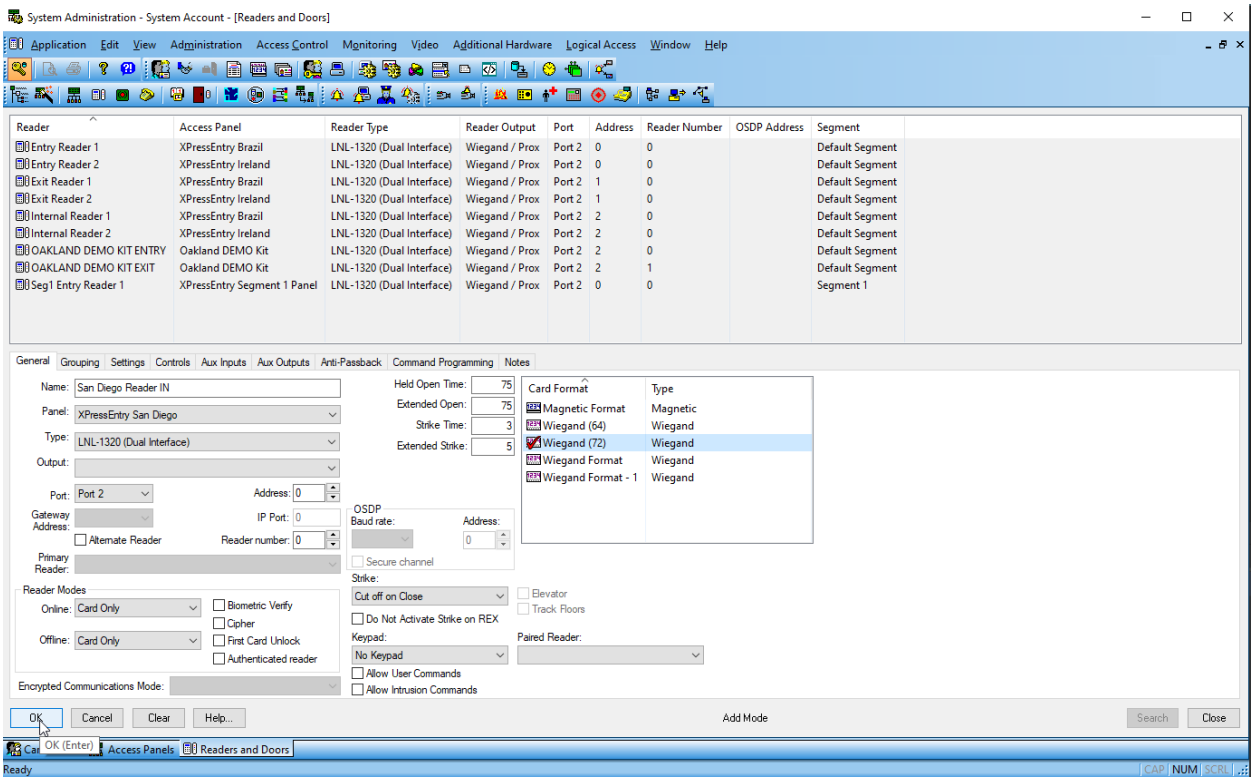
Each Entry/Exit handheld will require two readers. If the handheld is used mainly for mustering, one reader is only required per handheld. To create a new reader in System Administration, select the Access Control Menu Option -> Readers and Doors. Select Add in the bottom left.

Required Fields:

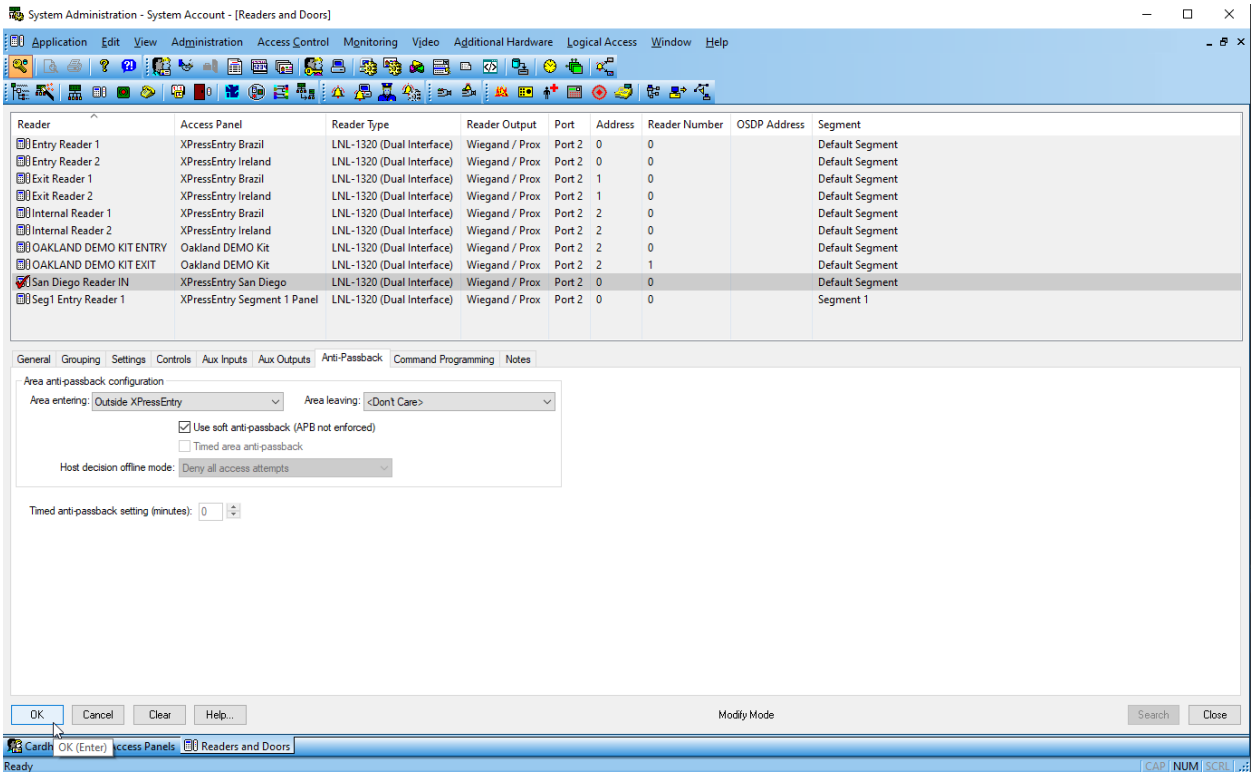
1. Name – Set the name of the reader.
2. Panel – Select the XPressEntry Panel created.
3. Type – Type is required by default. Select LNL-1320 (Dual Interface)
4. Output – Select Wiegand/Prox
5. Port/Address/Reader Number – Set the port, address, and reader number. The address and reader number will increment for each additional reader added.
6. Online/Offline – Set to Card Only.
7. Card Format – Select any card format. This is an OnGuard requirement to have a card format selected, but card formats will be configured separately in XPressEntry.

Click OK.

Repeat and create as many readers as necessary.



If the reader is being added as a muster reader, select Anti-Passback tab, and set Area Entering as an Outside, or Muster point area. Set Area Leaving as <Don't Care>. In this scenario, you will want to check "use soft anti-passback."

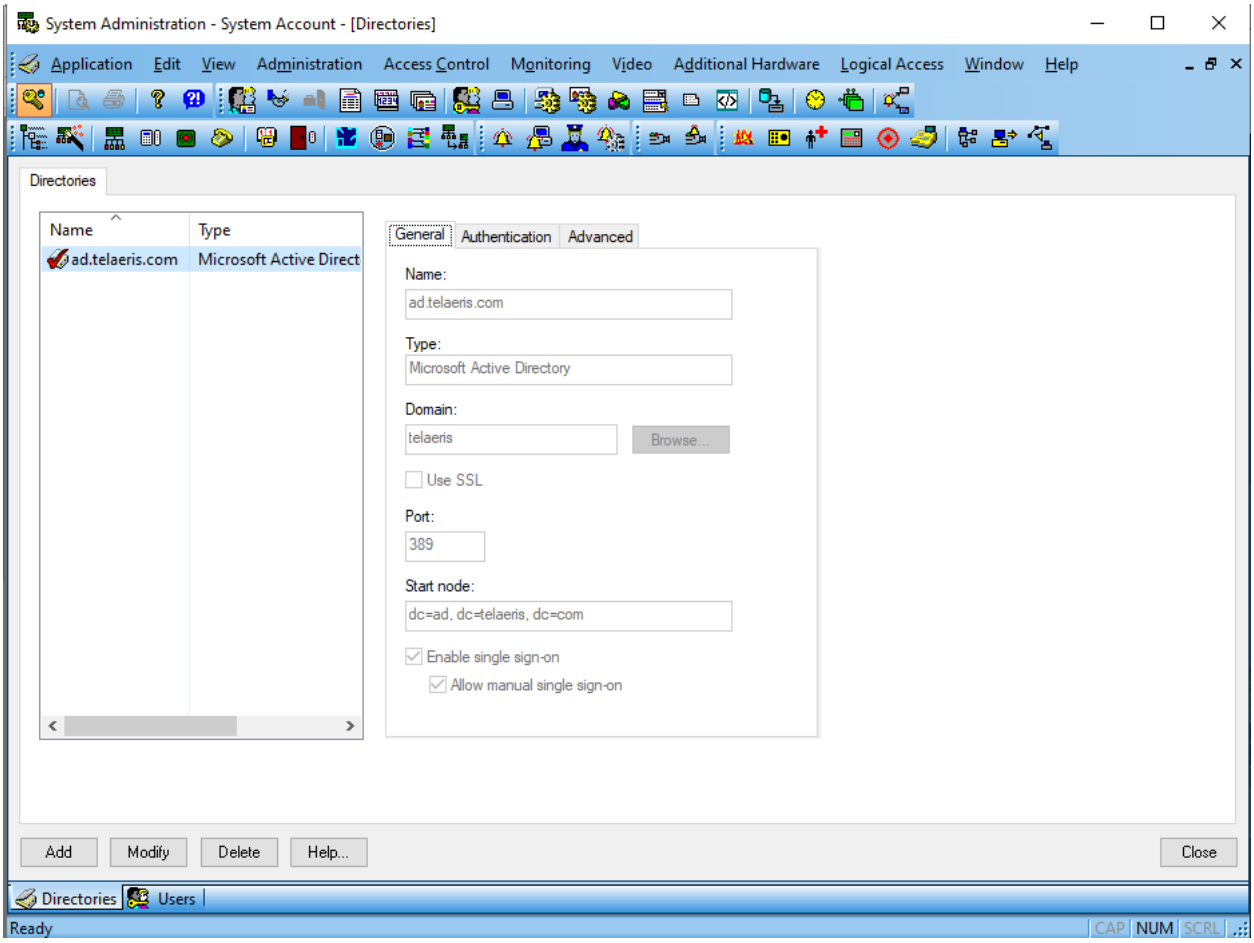


Note that these are setup similar to physical readers in the system, even though the panel may never physically be online. These are just placeholders for events that come in from XPressEntry.

OnGuard DataConduIT Setup

Single Sign-On Directory

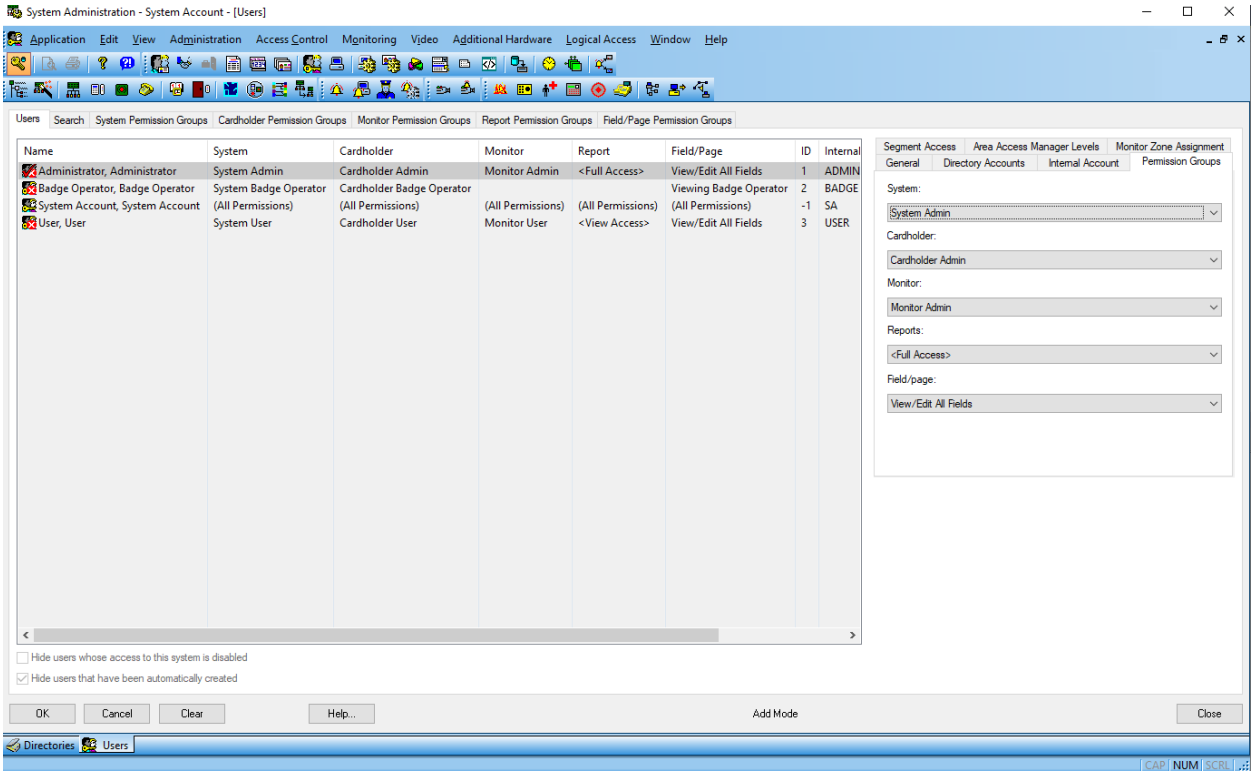
When using DataConduIT Single Sign-On is required. In general, this will involve using an existing directory or setting up a new directory (Administration -> Directories) to enable Single Sign-On (SSO). SSO is required for DataConduIT to function properly.



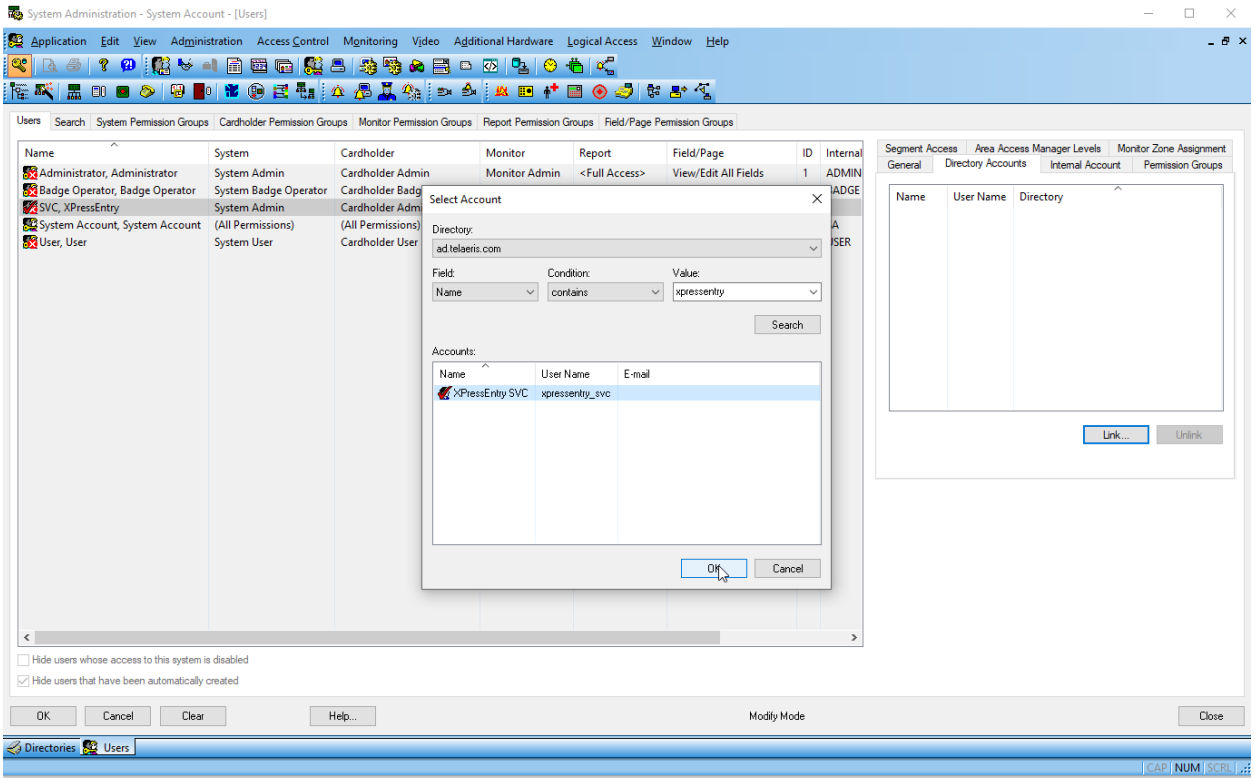
Single Sign-On User

An OnGuard User account is required which DataConduIT can access. (Administration -> Users). This should be linked to a Windows Service account for SSO through the Directory Accounts tab. The SSO Windows Service account will be used to connect the XPressEntry service with DataConduIT.

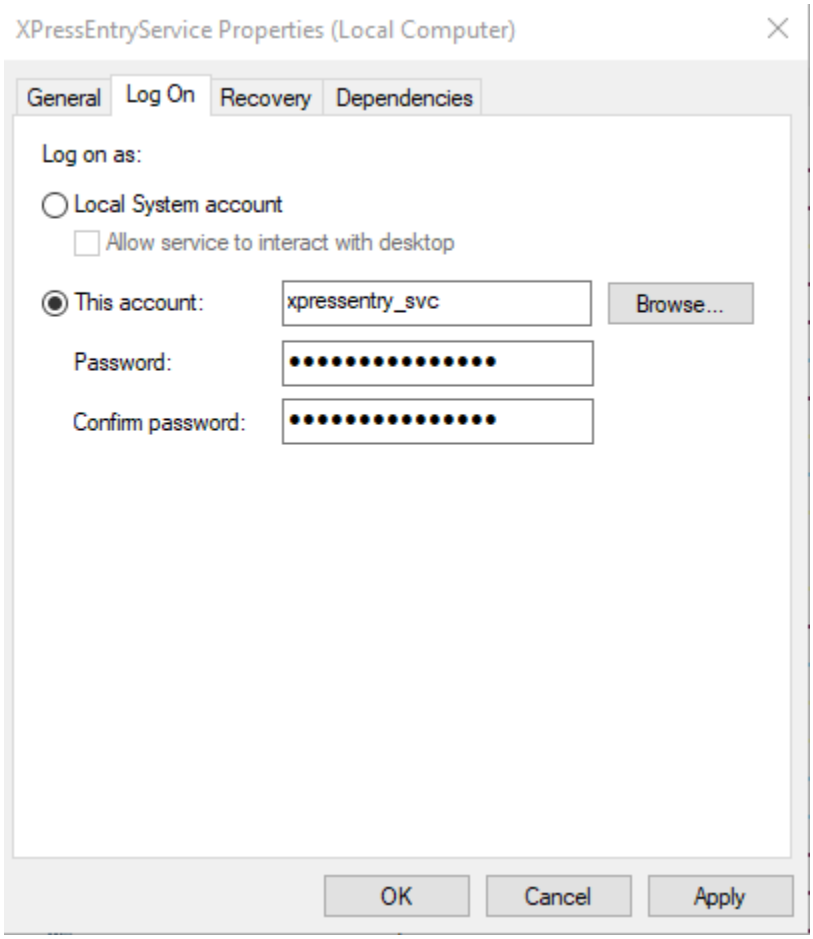
1. Create a Windows Service Account. Ex: username XPressEntry_SVC.
2. Create an OnGuard User. The OnGuard User will require System, cardholder, and monitor Admin access levels under Permission Groups.



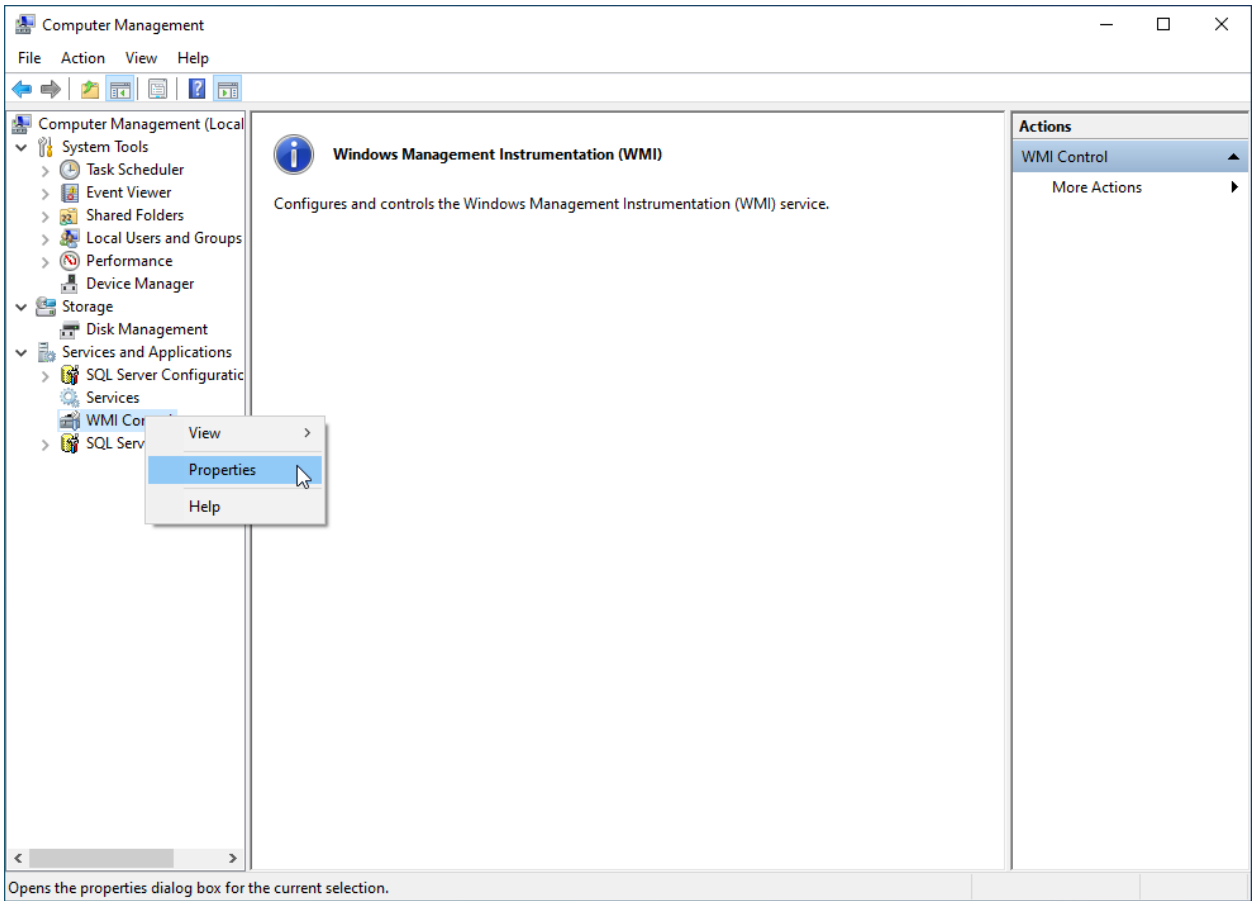
3. Link the Windows Service account to the new user



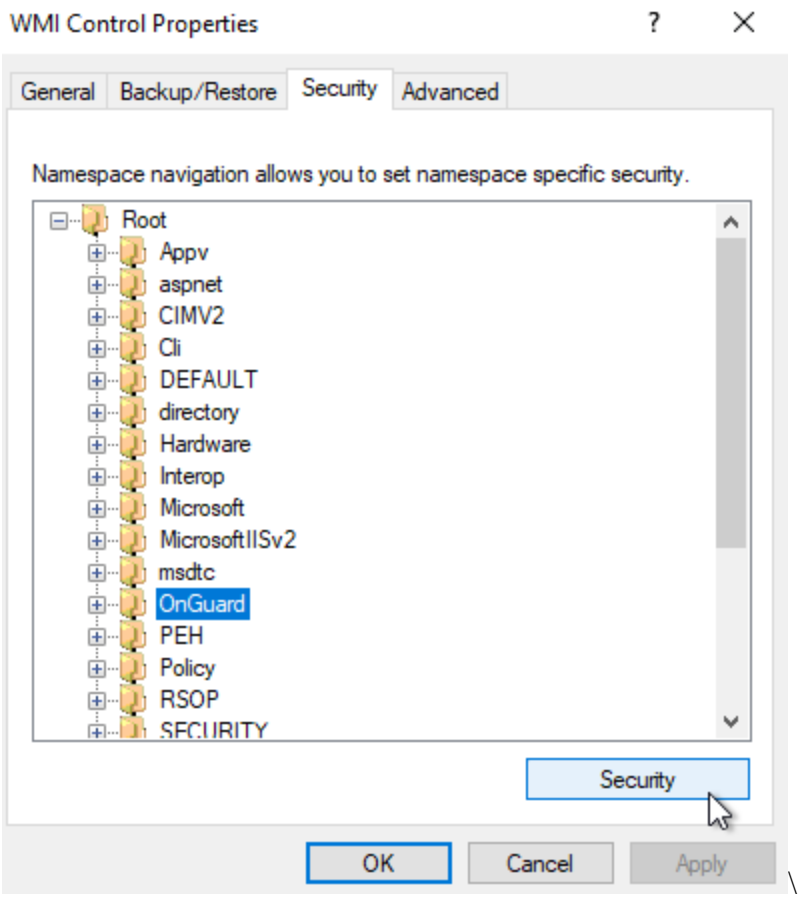
4. On the machine that XPressEntry Server is installed, go to Windows Services. Find the XPressEntryService, right-click and click on Properties. Select Log On. Select This account, and sign in with the Windows Service account.



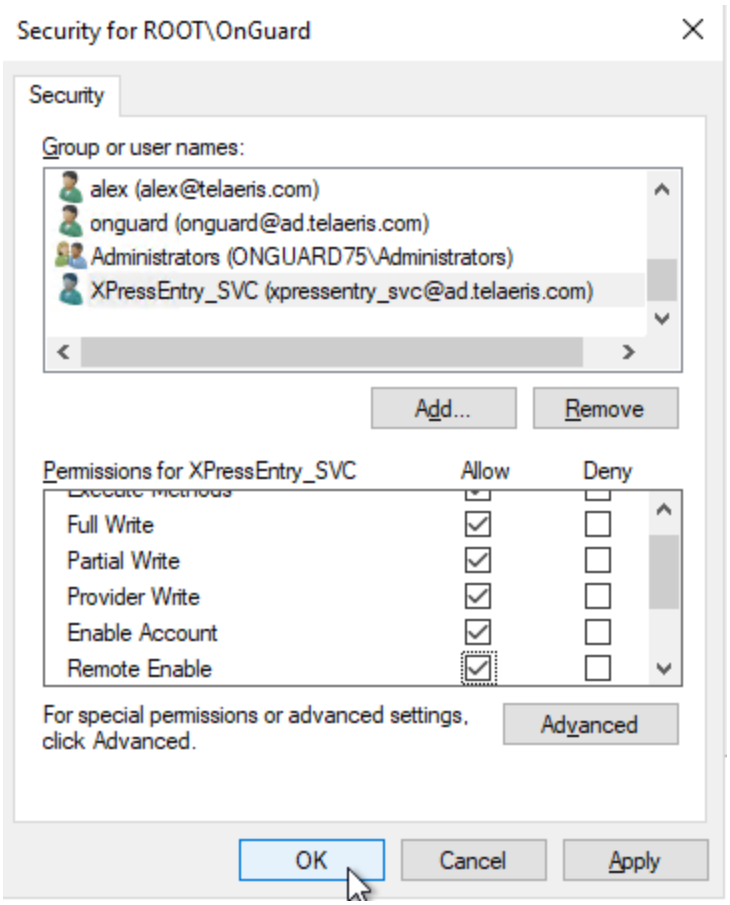
5. Open Run with **Windows+R** hotkeys, type **compmgmt.msc** and tap **OK**. Expand Services and Applications and right click WMI Control and select Properties. If using SQL Server as the XPressEntry database, The Windows service account will require db.owner permissions to XPressEntry database.



6. Select the Security Tab. Expand the Root folder, highlight the OnGuard folder, then click Security Button.

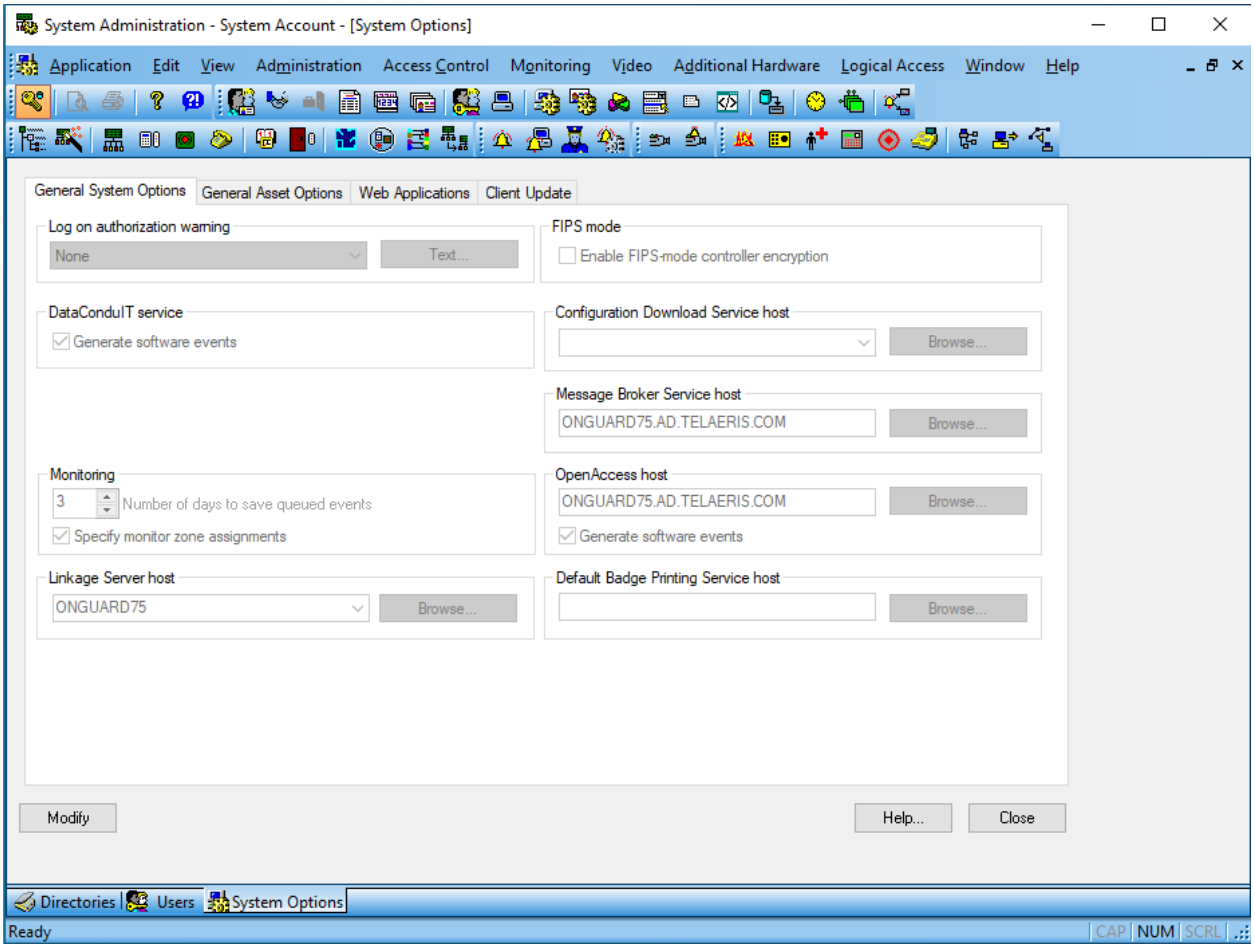


7. Click Add, and browse for the xpressentry_svc windows service account. Click OK. Under the permissions for xpressentry_svc, Allow Execute Method, Full Write, Partial Write, Provider Write, Enable Account, and Remote Enable. Click OK.



Software Events / Linkage Server

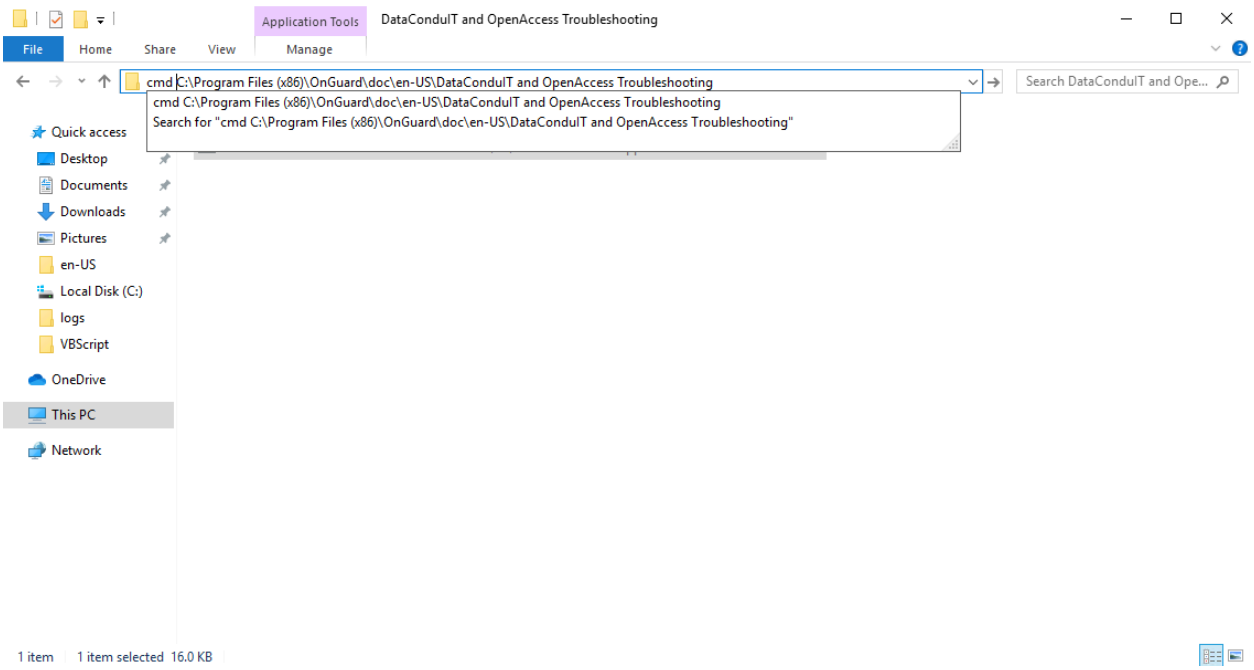
OnGuard Software Events in the system options page must be enabled for XPressEntry to pull occupancy data for mustering, and cardholder and badge changes instantly. This will allow XPressEntry to get user updates from OnGuard via Software Events instead of only during a scheduled synchronization. This is done from the Administration -> System Options page. Enable Software Events for the respective sync method for DataConduIT or OpenAccess. The Linkage server also needs to be set for software events to function properly. Add the Machine name of where the Linkage Service is running.



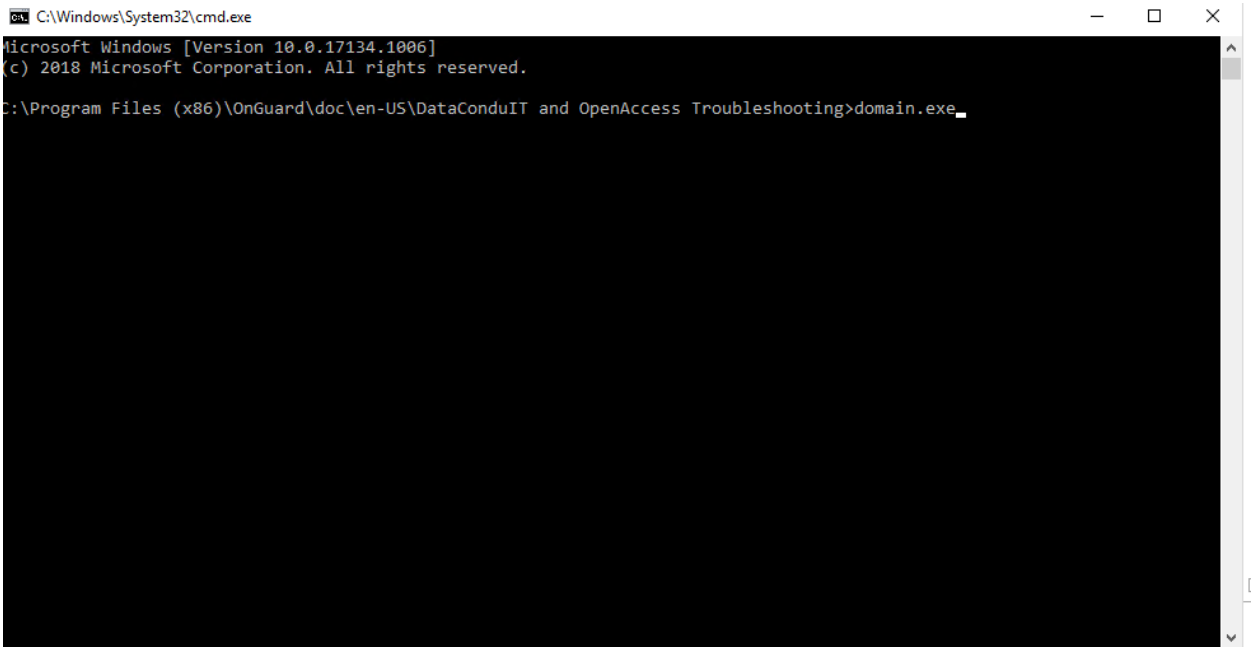
Next, to give proper permissions for Software Events the following will be required from the following excerpt in the OnGuard DataConduit.pdf.

> "Use **domain.exe** located in the **TroubleShooting** directory of the DataConduIT documentation file structure to determine if this may be the problem. If the NT4Domain is different from the W2KDomain, then you will need to update the LNL_DIRECTORY.DIR_HOSTNAME to match the NT4Domain. In case this is Oracle, please use all upper case. A sample SQL query to do this is below; it assumes the NT4Domain name is "Lenel" from **domain.exe** and that the directory to be updated is LNL_DIRECTORYID = 1.
> update lnl_directory set dir_hostname = 'LENEL' where lnl_directoryid=1"

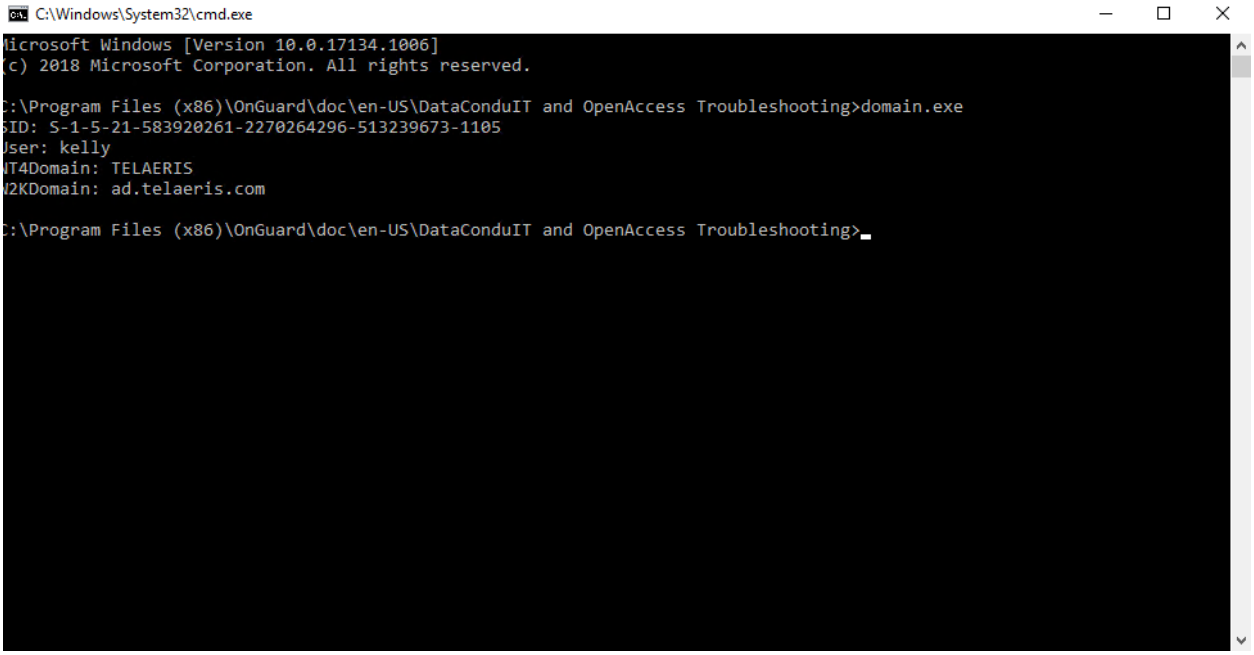
1. On the Onguard Application Server, open the following folder location: *C:\Program Files (x86)\OnGuard\doc\en-US\DataConduIT and OpenAccess Troubleshooting*
2. Click on the path location, and type *"CMD"* with the space in front of the path. Press Enter.



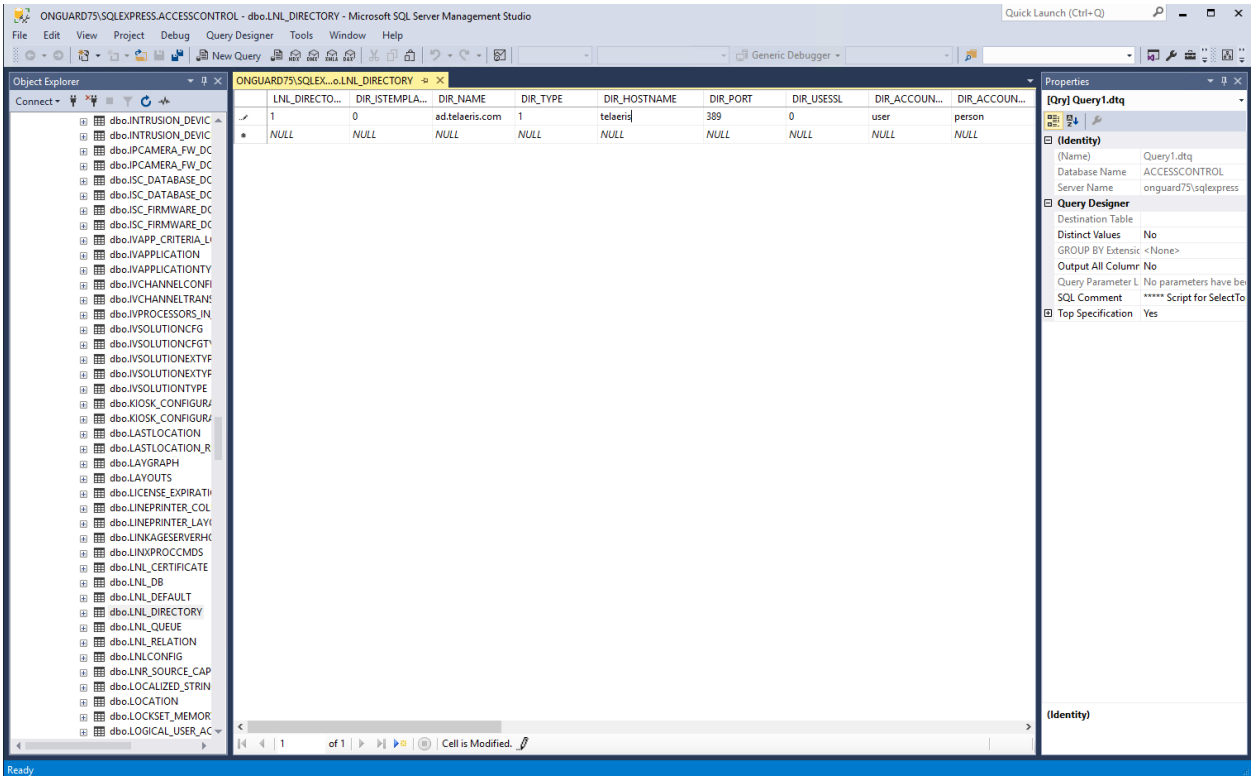
3. The following Command Line window will appear. Type in domain.exe and press enter.



4. Make note of the NT4 Domain Name.



5. Connect to SQL Server Management Studio that hosts the OnGuard Database.
6. Under Database -> AccessControl -> Tables -> dbo.LNL_DIRECTORY, right click the table, and select *Edit Top 200 Rows.* Find the directory row of the current domain. Change the Dir_hostname to the NT4 Domain from the command line

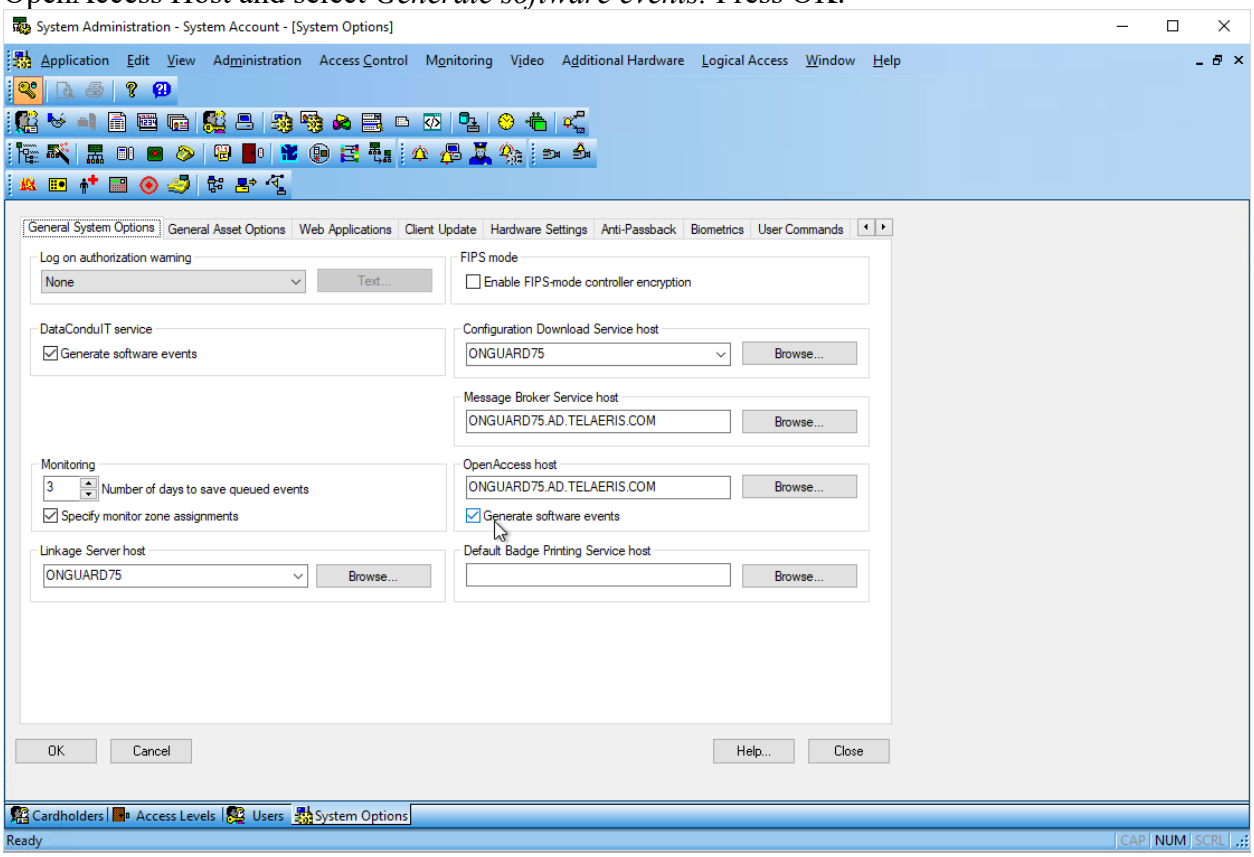


OnGuard OpenAccess Setup

Available with OnGuard 7.4 and newer.

Enable OpenAccess

To enable OpenAccess, from System Administration, Administration -> System Options. Set the OpenAccess Host and select *Generate software events.* Press OK.

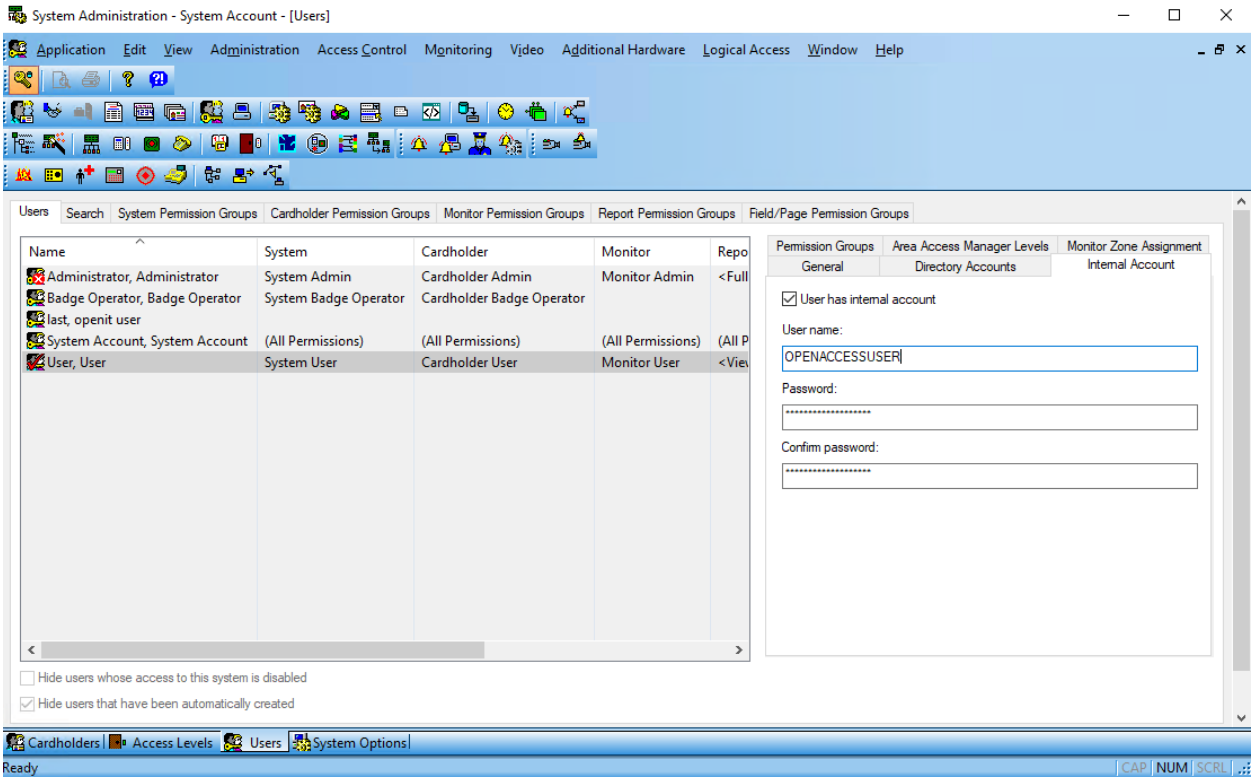


The required running OnGuard Services to run OpenAccess include:

LS OpenAccess
LS Communication Server
LS Web Event Bridge
LS Event Context Provider Service
LS Message Broker Service

Create OnGuard User

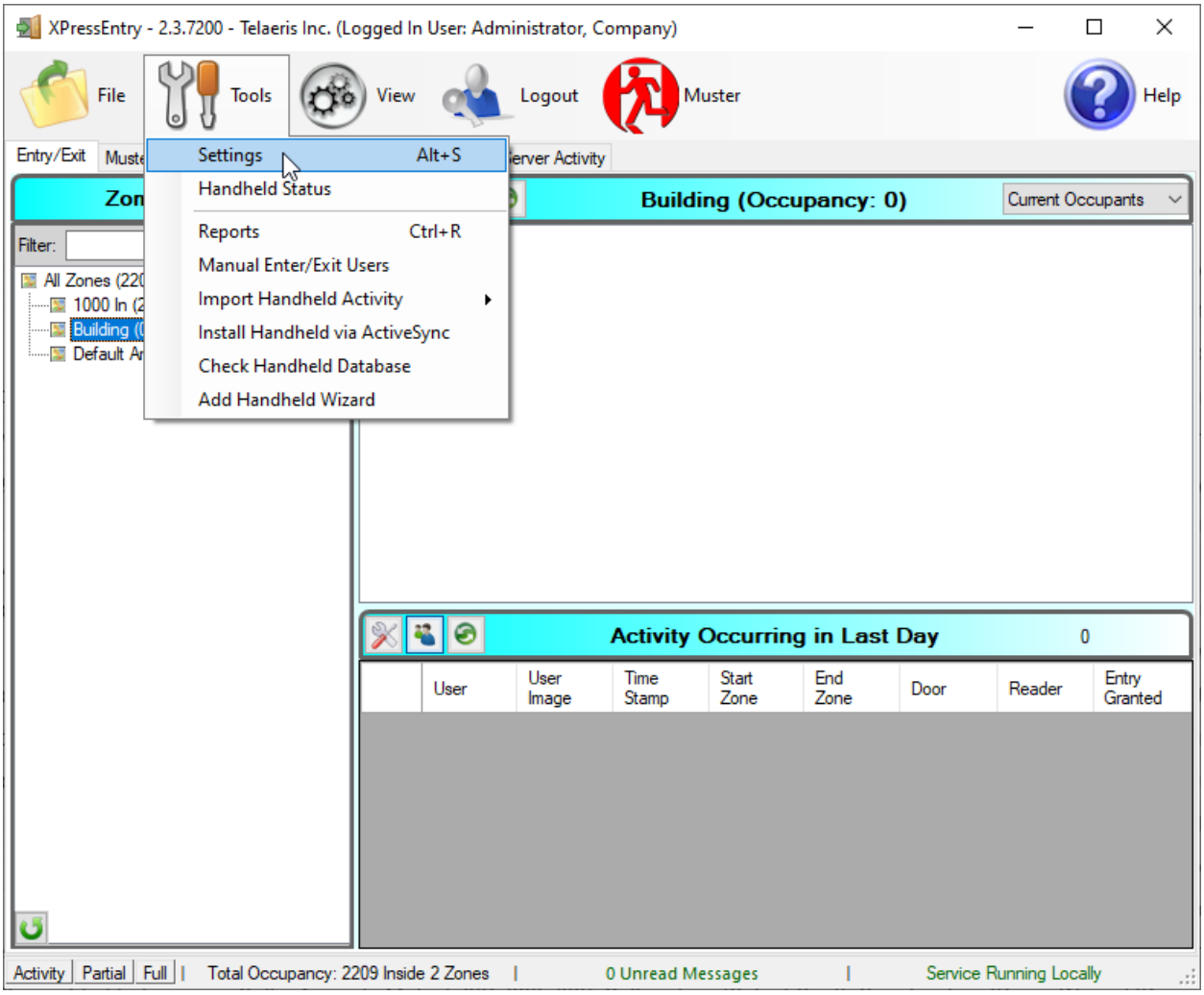
An OnGuard User account is required which OpenAccess can access. (Administration -> Users). Create a new User with an internal account. You can also choose to utilize a Directory account.



Enable Synchronization

XPressEntry uses a module called “Data Manager” to synchronize Cardholders/Cards with OnGuard.

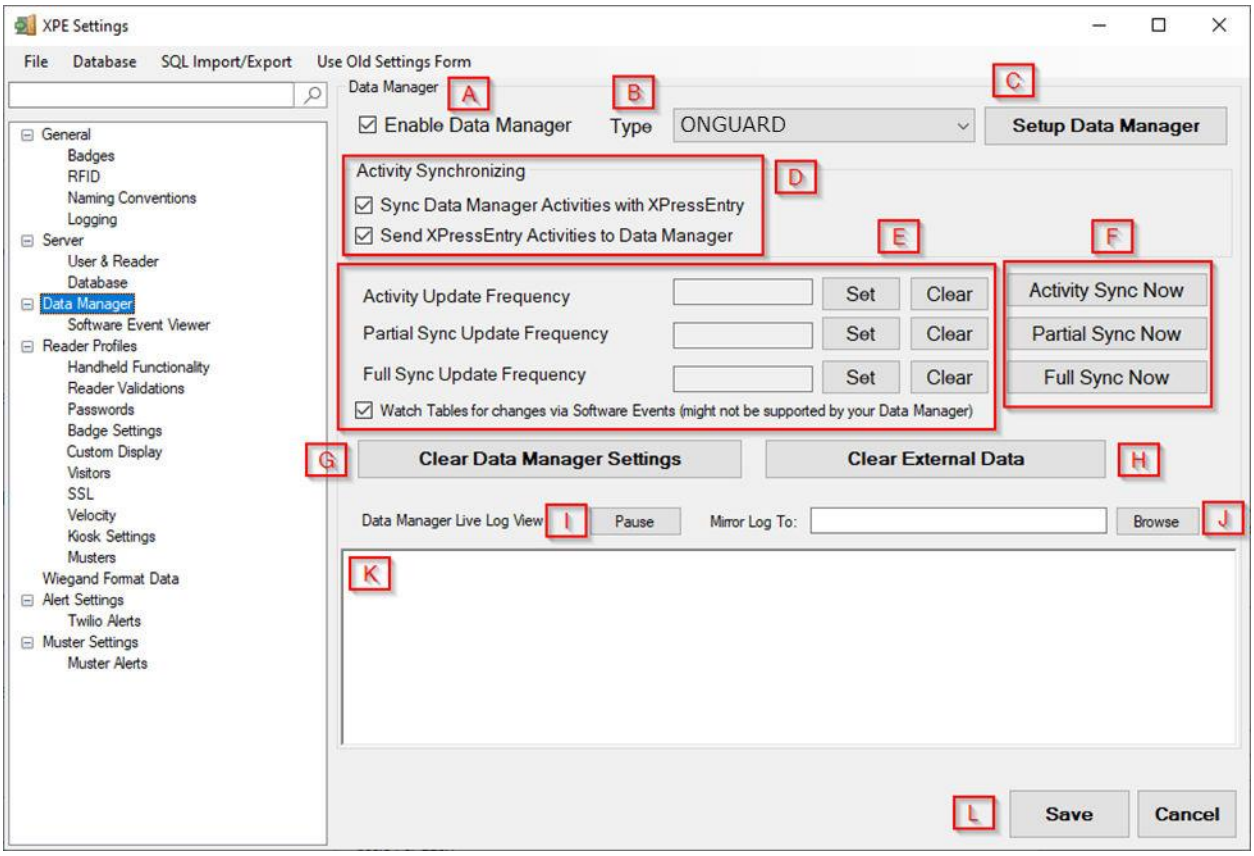
From the main page of XPressEntry, go to XPressEntry / Settings (CTRL+S)



Data Manager Overview

From the Settings page select the Data Manager Tab

Figure 9- Data Manager



a. Enable Data Manager – This must be checked to enable the OnGuard Synchronization
b. Type – Select OnGuard as the Data Manager type
c. Setup Data Manager – Opens the OnGuard Data Manager Settings
d. Activity Synchronizing – Controls the bi-directional communication between XPressEntry and OnGuard.
    1. Sync Data Manager Activities with XPressEntry – Pull data from OnGuard. Mainly used for occupancy tracking.
    2. Send XPressEntry Activities to Data Manager – Send handheld or server activities back to OnGuard as an event.
e. Update Frequency – Set the update frequency for each sync
    1. Activity Update – Push and pull OnGuard activities
    2. Partial Sync Update – Pulls all data excluding cardholder data, including readers, areas, access levels.
    3. Full Sync Update – Pulls all data from OnGuard. Depending on the size of the OnGuard system, this sync can take a while. Recommended to sync overnight, once a night.
f. Send XPressEntry Activities to Data Manager – Send handheld or server activities back to OnGuard as an event.
g. Clear Data Manager Settings – Clears All settings on this form.
h. Clear External Data – Clears all data that was synced from OnGuard, including cardholders, badges, reader etc.
i. Pause/Unpause – Can pause or unpause the logs as it populates.

j. Mirror Log – Outputs a secondary log file at the chosen location
k. Log – Displays all Data Manager Logs
l. Save – After any changes, press Save to apply changes to any sync. If settings are not saved, the next sync will NOT use the new changes.

Set the Update Frequency to as often as you want the system to update. Note that only one update can run at a time and if this value is very low the system will constantly try to update (this is not always a problem

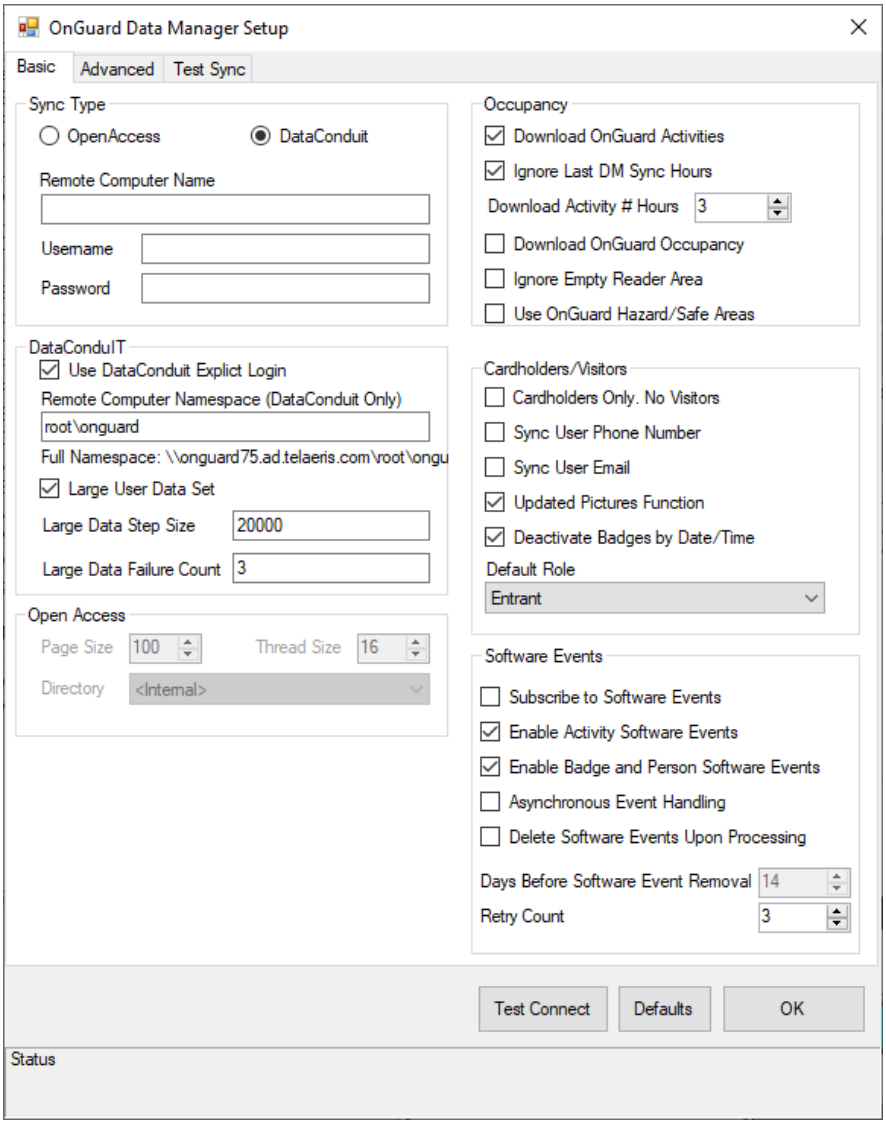
OnGuard Setup Page Overview

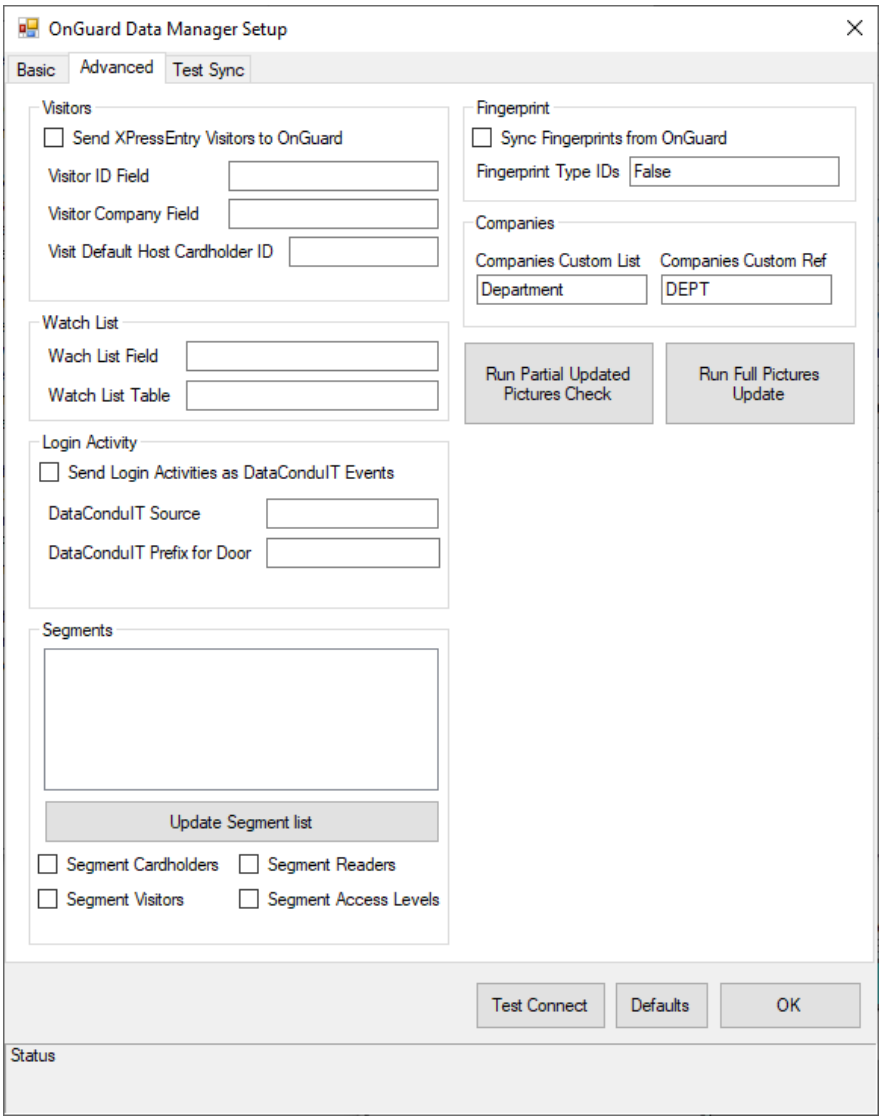
Press the "Setup Data Manager" button to get the OnGuard specific setup screen.

Basic Settings

1. Sync Type – Select which method will be used to connect to Onguard: OpenAccess or DataConduIT.
    a. OpenAccess – Select if using OpenAccess
    b. DataConduIT – Select if using DataConduIT
    c. Remote Computer Name – IP or Hostname of the machine hosting DataConduIT Service or OpenAccess Service. Typical setup has these services running on the main Onguard application server.
    d. Username – Username for OpenAccess or DataConduIT Single Sign On. (Required for DataConduIT Only if "Use DataConduIT Explicit Login is checked)
    e. Password – Password for OpenAccess or DataConduIT Single Sign On. (Required for DataConduIT Only if "Use DataConduIT Explicit Login is checked)
2. DataConduIT – Settings specific to using DataConduIT
    a. Use DataConduIT Explicit Login – In some scenarios, using explicit login for Single Sign-On is required for DataConduIT SSO to grant access. Use this if SSO via the XPressEntry Service Log On user does not work.
    b. Remote Computer Namespace – Namespace for DataConduIT WMI settings. Default location namespace is root\onguard, and is rarely different.
    c. Large User Data Set – For large cardholder systems, breaks down the DataConduIT syncs into smaller batches. Syncs pull records based on cardholder and badge ID's in order. For instance, the first pull will pull all ID's between 1 and 20000. The second pull will pull all ID's between 20001 and 40000. If there are major gap's between table ID ranges, increate the data step size or failure count.
        i. Large Data Step Size – Number of records pulled on each instance.
        ii. Large Data Failure Count – Number of pulls with zero records returned, signaling there are potentially no more records to pull.
3. OpenAccess – Settings specific to using OpenAccess
    a. Page Size – Max number of records pulled per request. OpenAccess max is 100.
    b. Thread Size – Max number of threads that run concurrently pulling data via OpenAccess. Max 16.

    c. Directory – Select the directory for Single Sign On via OpenAccess. Requires connection the Remote Computer Name.
4. Occupancy – Settings for occupancy tracking. Used with mustering and anti-passback mainly.
    a. Download OnGuard Activities – Downloads cardholder activities from either the last sync, or last # of hours from OnGuard, and inserts as badge activities into XPressEntry.
    b. Ignore Last DM Sync Hours – If checked, will ignore the last sync complete time, and pull all activities from Download Activity # of Hours.
    c. Download Activity # Hours – Number of hours to pull records from.
    d. Ignore Empty Reader Area – If readers within OnGuard do not utilize Anti-passback areas, selecting this will not move the cardholder into an empty area and potentially keep them in the marked hazard area.
    e. Use OnGuard Hazard/Safe Areas – When syncing areas, if an area is marked as a hazardous or safe area, XPressEntry will pull the info and preset the areas accordingly.
5. Cardholder/Visitors – Settings for syncing Cardholders and visitors
    a. Cardholder only. No Visitors – If checked, will sync only cardholders.
    b. Sync User Phone Number – if checked, will sync cardholder phone number field.
    c. Sync User Email – If checked, will sync cardholder email field.
    d. Update Pictures Function – Uses the updated pictures functions. Check by default in most scenarios.
    e. Deactivate Badges by Date/Time – Respect badge expirations by date and time.
    f. Default Role – Default XPressEntry role assigned to cardholders when synced. Typically, Entrant will be set as the default.
6. Software Events – Settings for OnGuard Software Events
    a. Subscribe to Software Events – Enables software events
    b. Enable Activity Software Events – Enables software events for all cardholder badge activities. Required for monitoring activities for mustering and anti-passback setup.
    c. Enable Badge and Person Software Events – Enables software events for any cardholder and badge changes to a cardholder in System Administration. These changes will populate with a few seconds into XPressEntry without requiring a partial or full sync.
    d. Asynchronous Event Handling – Used for Asynchronous software events. Used in special cases. Ask Telaeris Support for more details.
    e. Delete Software Events Upon Processing – Software events enter a database queue when added to XPressEntry. Check this to delete the event from the queue once it has created a badge activity.
    f. Days Before Software Event Removal – Days to hold onto software event queued data.
    g. Retry Count – Number of attempts to process a software activity in the queue.


OnGuard Data Manager Setup
Basic
Advanced
Test Sync
Sync Type
OpenAccess
DataConduit
Remote Computer Name
Username
Password
DataConduIT
Use DataConduit Explict Login
Remote Computer Namespace (DataConduit Only)
root\onguard
Full Namespace: \\onguard75.ad.telaeris.com\root\ongu
Large User Data Set
Large Data Step Size
20000
Large Data Failure Count
3
Open Access
Page Size
100
Thread Size
16
Directory
<Internal>
Occupancy
Download OnGuard Activities
Ignore Last DM Sync Hours
Download Activity # Hours
3
Download OnGuard Occupancy
Ignore Empty Reader Area
Use OnGuard Hazard/Safe Areas
Cardholders/Visitors
Cardholders Only. No Visitors
Sync User Phone Number
Sync User Email
Updated Pictures Function
Deactivate Badges by Date/Time
Default Role
Entrant
Software Events
Subscribe to Software Events
Enable Activity Software Events
Enable Badge and Person Software Events
Asynchronous Event Handling
Delete Software Events Upon Processing
Days Before Software Event Removal
14
Retry Count
3
Test Connect
Defaults
OK
Status



Advanced Settings

1. Visitors – Advance Visitor Settings
    a. Send XpressEntry Visitors to OnGuard – Add enrolled visitors from XPressEntry to OnGuard.
    b. Visitor ID Field –
    c. Visitor Company Field –
    d. Visit Default Host Cardholder ID –
2. Watch List – Set a watch list customer field for cardholders
    a. Watch List Field – Field name
    b. Watch List Table – Table Name
3. Login Activity – Send XPressEntry handheld login activity to OnGuard as an alarm.
    a. Send Login Activities as DataConduIT Events – check to send login activities.
    b. DataConduIT Source – Set the logical source device name from OnGuard
    c. DataConduIT Prefix for Door –

4. Segments – Pull specific segments if segments are utilized in OnGuard
    a. Segments – Displays a list of segments from OnGuard
    b. Segment Cardholders – Segment Cardholders pulled from OnGuard
    c. Segment Visitors – Segment Visitors pulled from OnGuard
    d. Segment Readers– Segment Readers pulled from OnGuard
    e. Segment Access Levels – Segment Access Levels pulled from OnGuard
5. Fingerprint – Pull Fingerprint templates from OnGuard.
    a. Sync Fingerprints from OnGuard – Enables fingerprint sync
    b. Fingerprint Type ID –
6. Companies – Pull custom fields to populate companies field in XPressEntry
    a. Companies Custom List –
    b. Companies Custom Ref -

The permissions for the user running XPressEntry are assumed to be sufficient to access DataConduIT via WMI. The configuration of the PC with these permissions is assumed to be outside the scope of this document. XPressEntry uses the System.Management.Impersonation level to access DataConduIT via WMI.

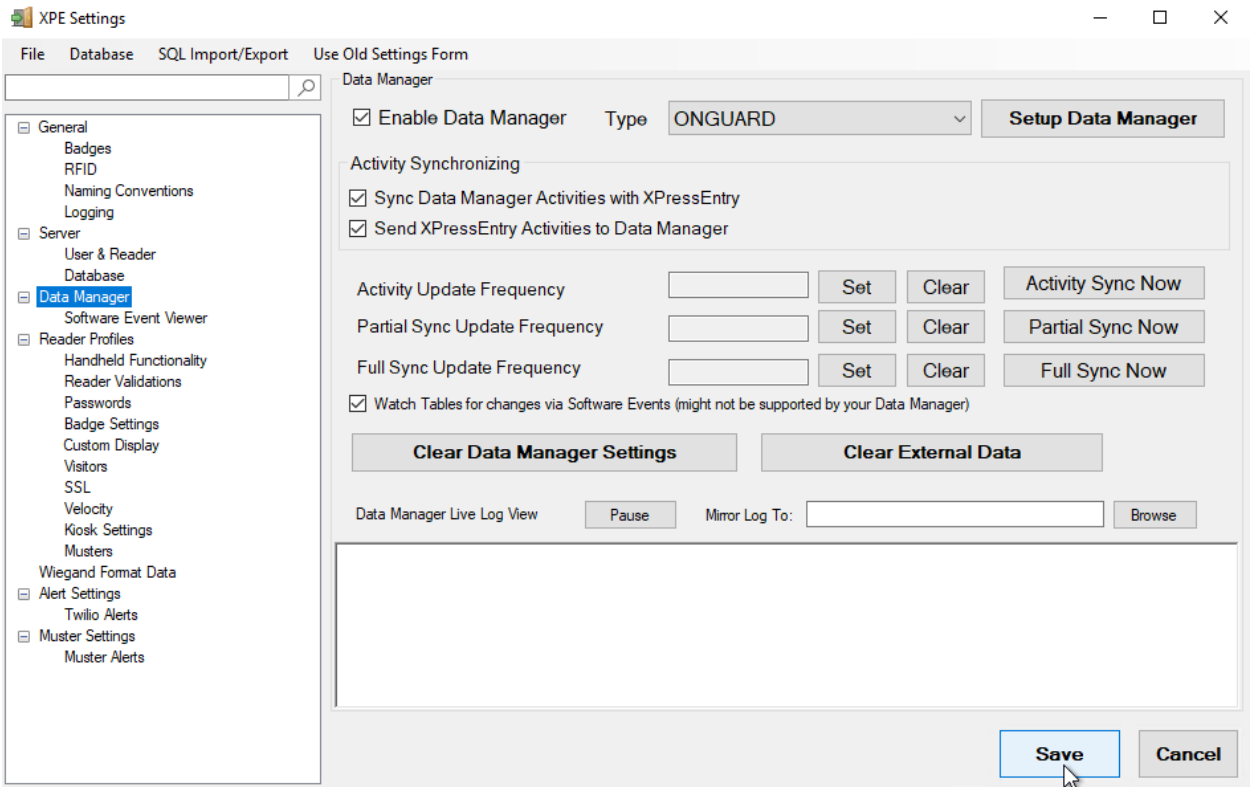
DataConduIT and OpenAccess is used for all data transfers between XPressEntry and OnGuard. As a result, you must setup DataConduIT and OpenAccess to use DataConduIT appropriately. This is assumed to be outside the scope of this document.

After any changes to the Data Manager Settings, click OK, and click Save on the Settings Window.

OnGuard Data Manager Suggested Configuration Steps

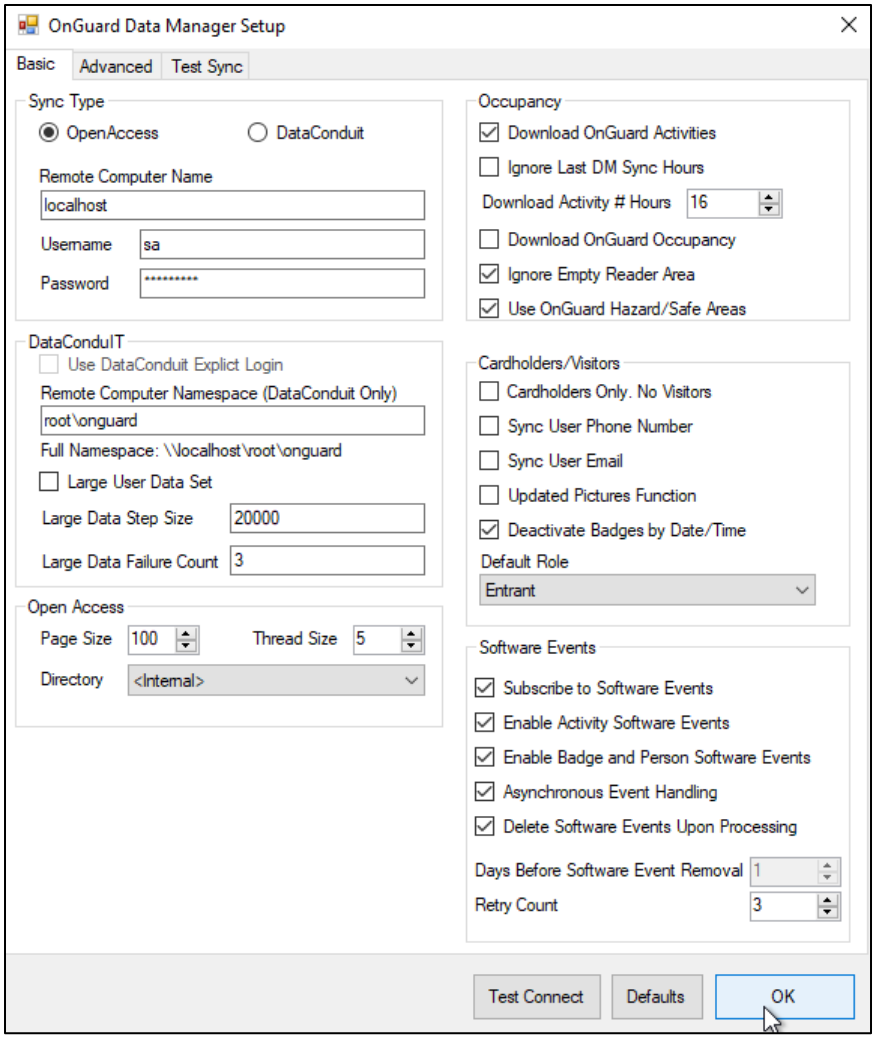
Below are instructions for a basic setup outside of the default settings. Proper settings may vary and depend upon environment setup and requirements. Please read the Overview sections above for further information on any settings not mentioned in the steps below.

1. Select *Enable Data Manager* in the Data Manager Tab.
2. Select the *Type* drop down, and select *Onguard*
3. Click Save. This will enable the *Setup Data Manager* button to be enabled.
4. If using XPressEntry for Entry/Exit Mode, typical setup would require *Send XpressEntry Activities to Data Manager* checked.
5. If using XPressEntry for Entry/Exit Mode with Anti-passback or Muster Mode, typical setup would require *Sync Data Manager Activities with XpressEntry* checked.



6. Click *Setup Data Manager*
7. Select the sync type we will use to connect to OnGuard, OpenAccess or DataConduIT.
8. Set the remote computer name of the OnGuard application server.
9. Login parameters differ between DataConduIT and OpenAccess
    a. For DataConduIT, it is important that the XPressEntry service is using the LogOn user that has User permissions for DataConduIT. In some instances, such as if the XPressEntry machine is on a separate domain from the OnGuard Application Server, you may be able to check the *Use DataConduIT Explicit Login*, and add the username and password of the OnGuard user with permissions.
    b. For OpenAccess, first select the directory that you will be using to signing into OpenAccess. For local OnGuard accounts, select <Internal>. Log in with the proper username and password.

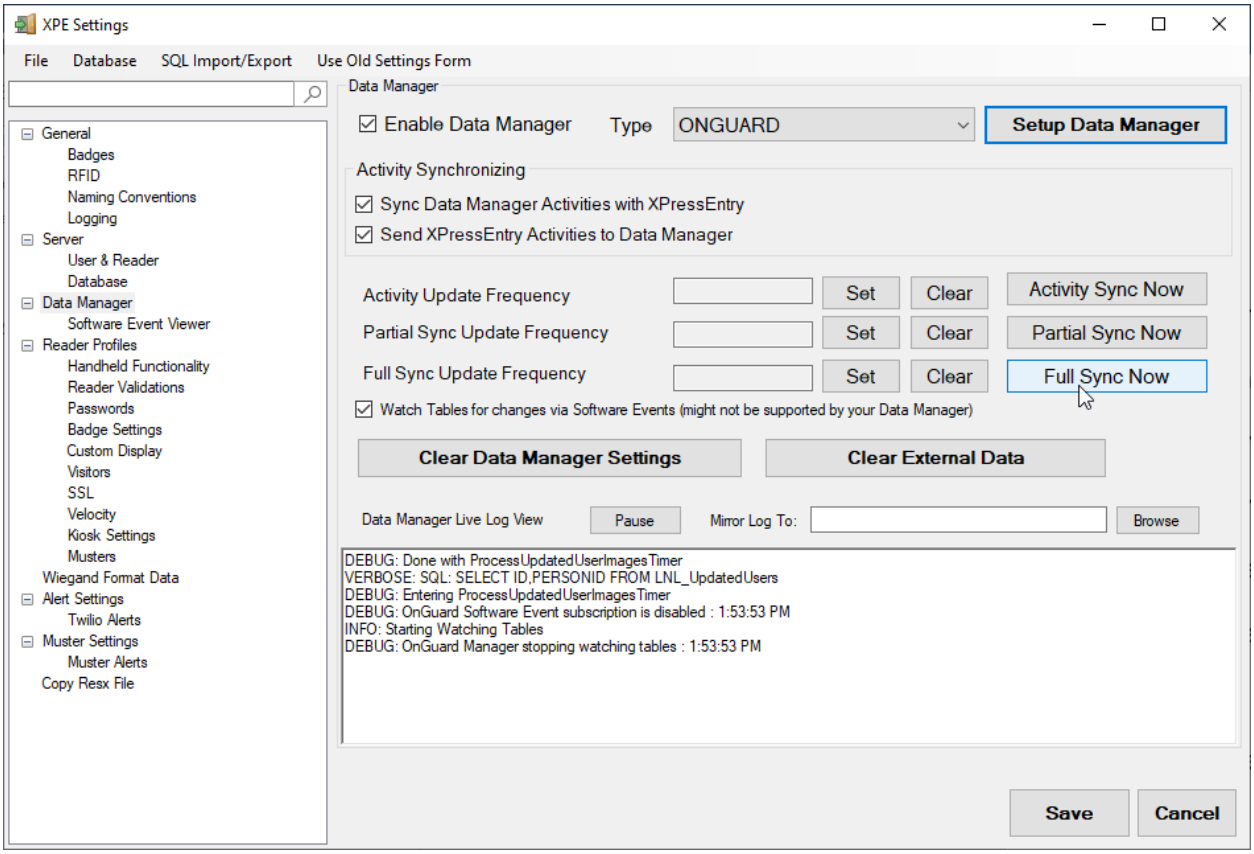
    Click *Test Connect* to see if the connection is successful.
10. If DataConduIT is selected as the sync type and OnGuard Cardholder count is greater than 30,000, Select the *Large User Data Set* checkbox.
11. Check *Update Pictures Function*
12. Check *Subscribe to Software Events*
13. If utilizing Muster Mode or anti-passback, check *Enable Activity Software Events.*
14. Check *Enable Badge and Person Software Events*
15. Uncheck the Asynchronous Event Handling.
16. Click OK.
17. Click Save on the Data Manager Tab.



Setup XPressEntry Data

After all settings have been configured, click Full Sync Now on the Settings Data Manager page. This sync may take a while, depending on the number of cardholders. 30k cardholder system can take around 20 minutes.

Note: If utilizing DataConduIT and full sync displays receiving 0/0 data on each table, and no data is being synced into XPressEntry, please check the previous steps for WMI/DataConduIT permission issues.



Once the OnGuard System is set up and synchronizing, you will see all of this data represented in XPressEntry under the Add/Edit Info tab. Data which is imported from OnGuard cannot be changed and is Grayed out.

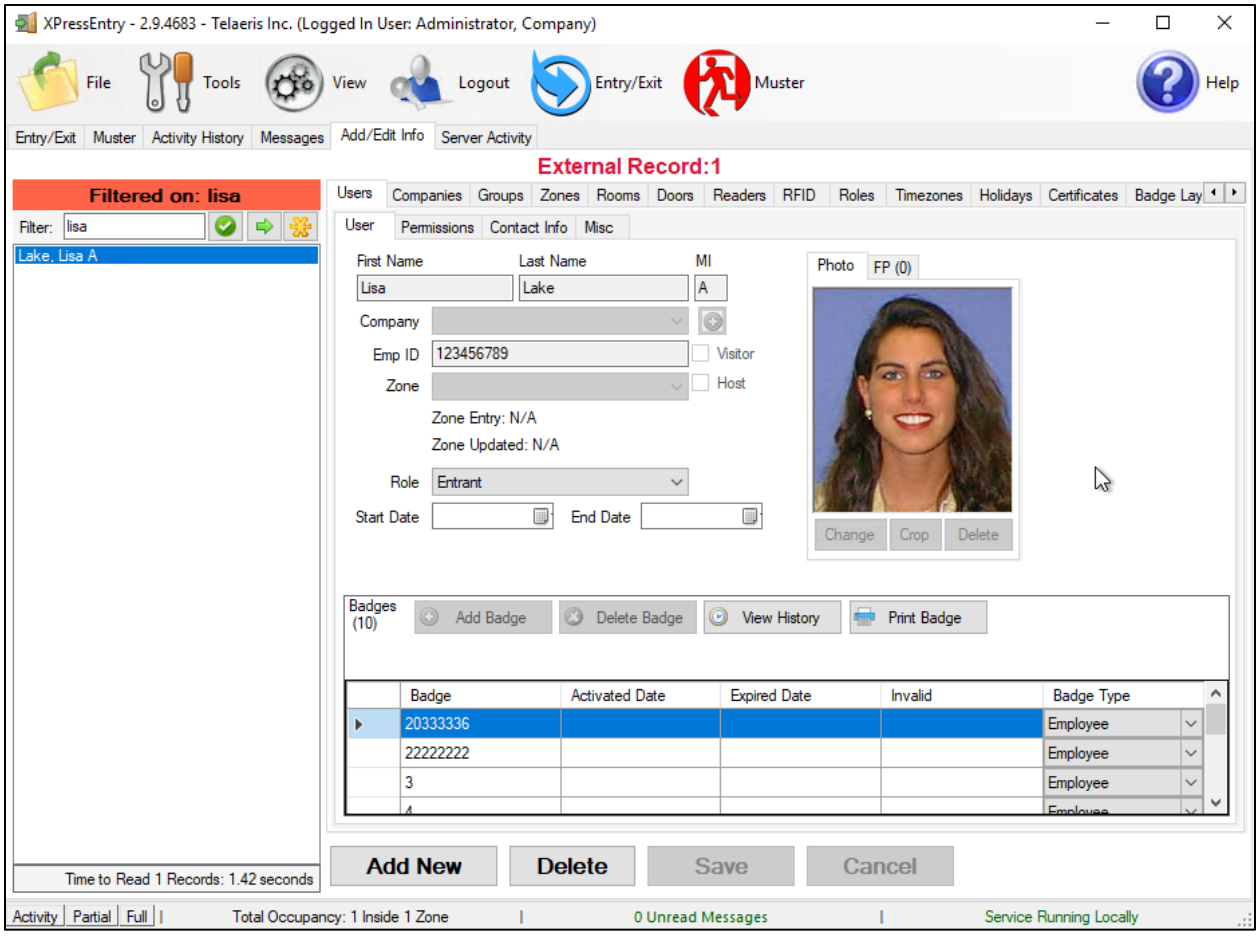
Priority of Data Synchronization

Any changes made in OnGuard should be shown in XPressEntry in the following order:
Highest Priority: Badge/User/Zone Occupancy changes are updated immediately when software events are enabled.

Lower Priority: Door/Reader/Area/XPressEntry Activities/User Permissions will be updated whenever the Data Manager Synchronizer runs. This can be run manually from the Settings page -> Data Manager tab by pressing “Partial Sync Now”.

Users

Here is a sample of a properly synchronized user:

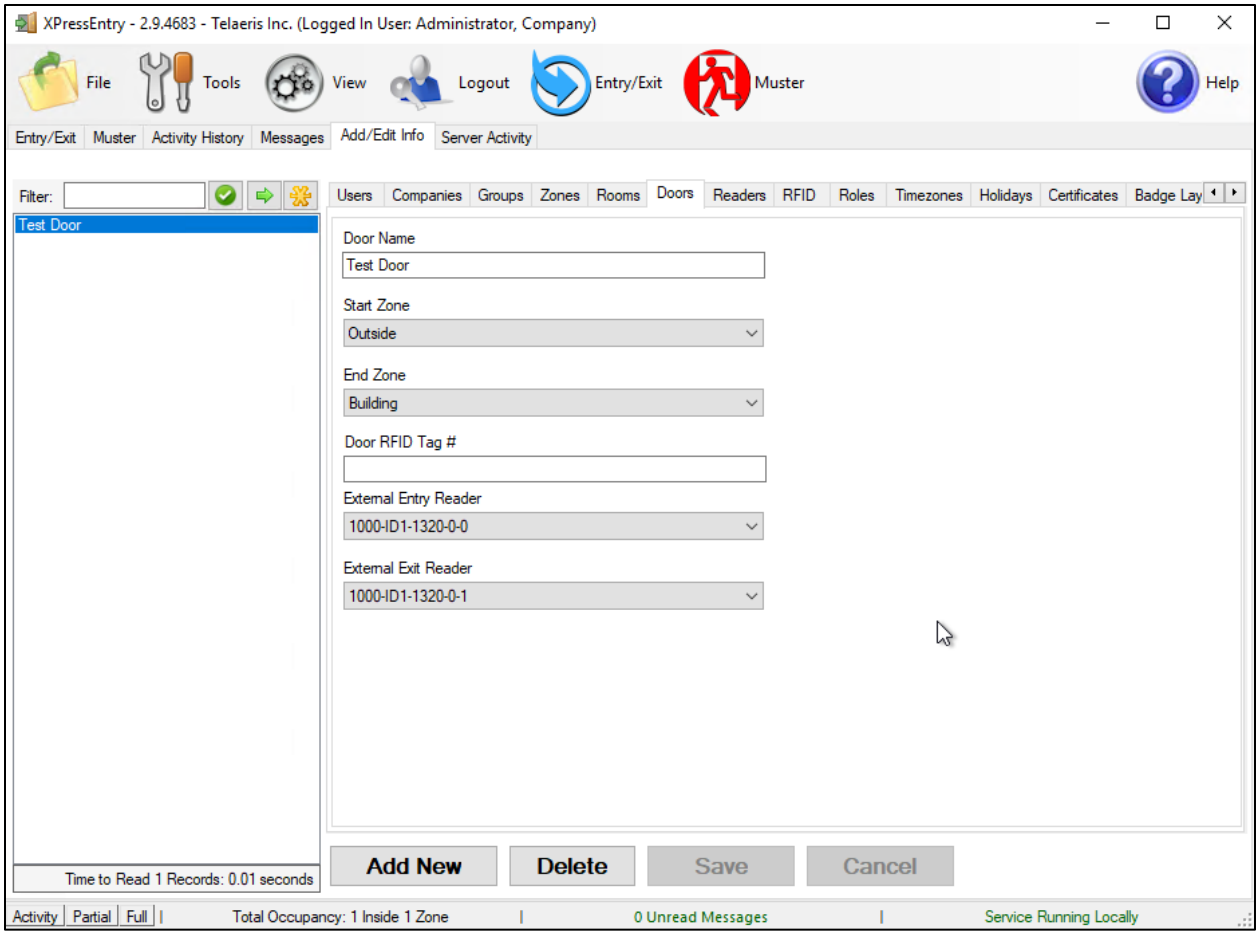


Those users have the same AccessLevel Permissions from OnGuard:

Doors

Entry/Exit permissions in XPressEntry are set by doors. Doors are portals between two zones and can be “Entered” or “Exited”. The permissions for a door are determined by the External Entry Reader and External Exit reader. Users will have permission to Enter or Exit a door based on their OnGuard permissions for the selected readers. These are also the readers in OnGuard an Entry or Exit will be assigned to. For Muster Mode, the handhelds default Door External Exit Reader will be used to move the mustered user to the correct area in OnGuard, and will create an exit read that will show up in Alarm Monitor.

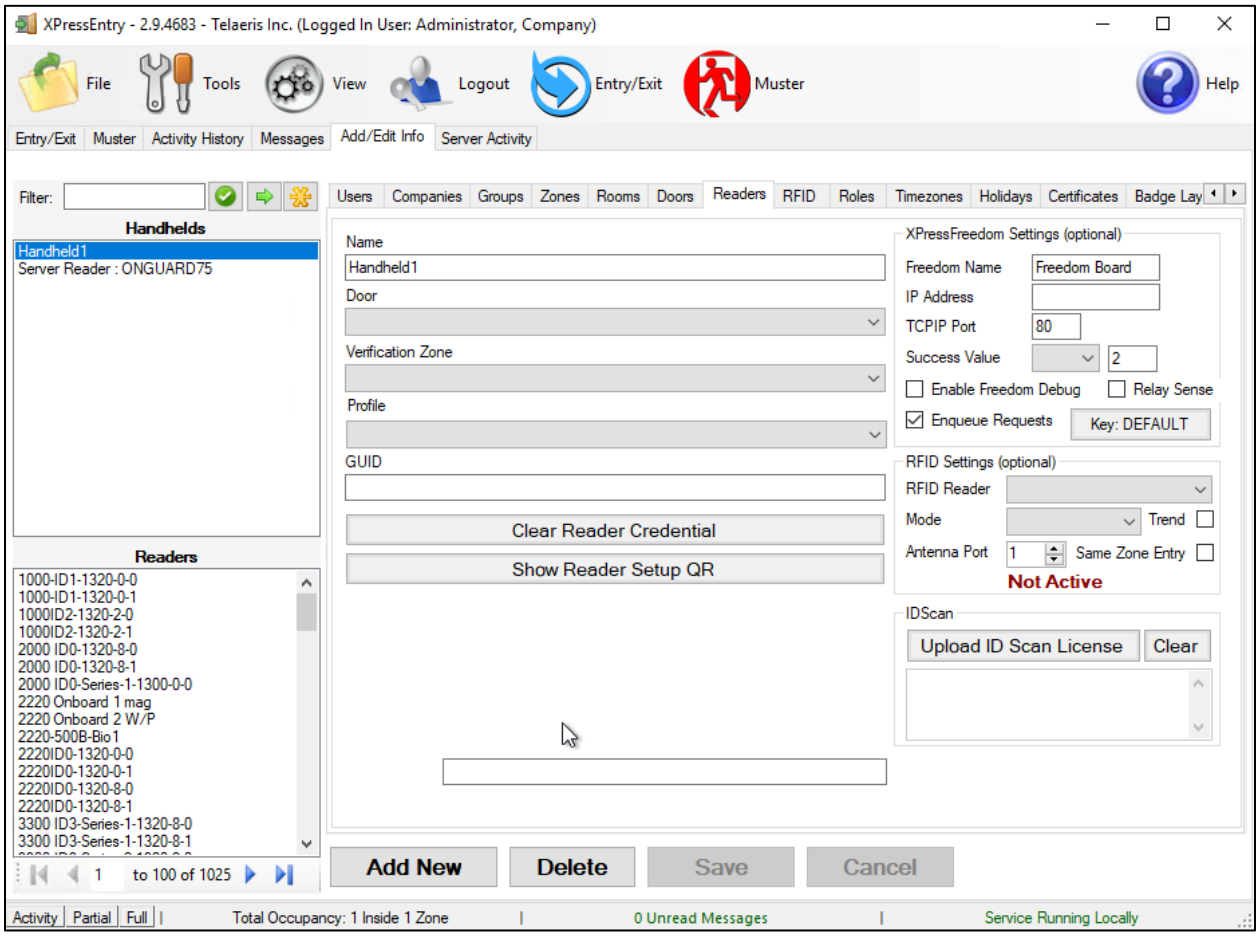
Doors should be set by the user for each Handheld Reader in XPressEntry.


XPressEntry - 2.9.4683 - Telaeris Inc. (Logged In User: Administrator, Company)
File
Tools
View
Logout
Entry/Exit
Muster
Help
Entry/Exit
Muster
Activity History
Messages
Add/Edit Info
Server Activity
Filter:
Users
Companies
Groups
Zones
Rooms
Doors
Readers
RFID
Roles
Timezones
Holidays
Certificates
Badge Lay
Test Door
Door Name
Test Door
Start Zone
Outside
End Zone
Building
Door RFID Tag #
External Entry Reader
1000-ID1-1320-0-0
External Exit Reader
1000-ID1-1320-0-1
Time to Read 1 Records: 0.01 seconds
Add New
Delete
Save
Cancel
Activity
Partial
Full
Total Occupancy: 1 Inside 1 Zone
0 Unread Messages
Service Running Locally

Readers

XPressEntry divides readers up into two categories: “Handhelds” and “Readers”

Handhelds refer to physical readers in the system. All handhelds have a GUID which identifies the hardware. There are currently three types:
The Server Reader – used to assign badge activities from the server. This will likely be named “Server Reader: COMPUTER NAME” and have a 20-22 character GUID
Physical Handheld devices. These are typically either an Android or Windows CE Embedded device. These have a long GUID.

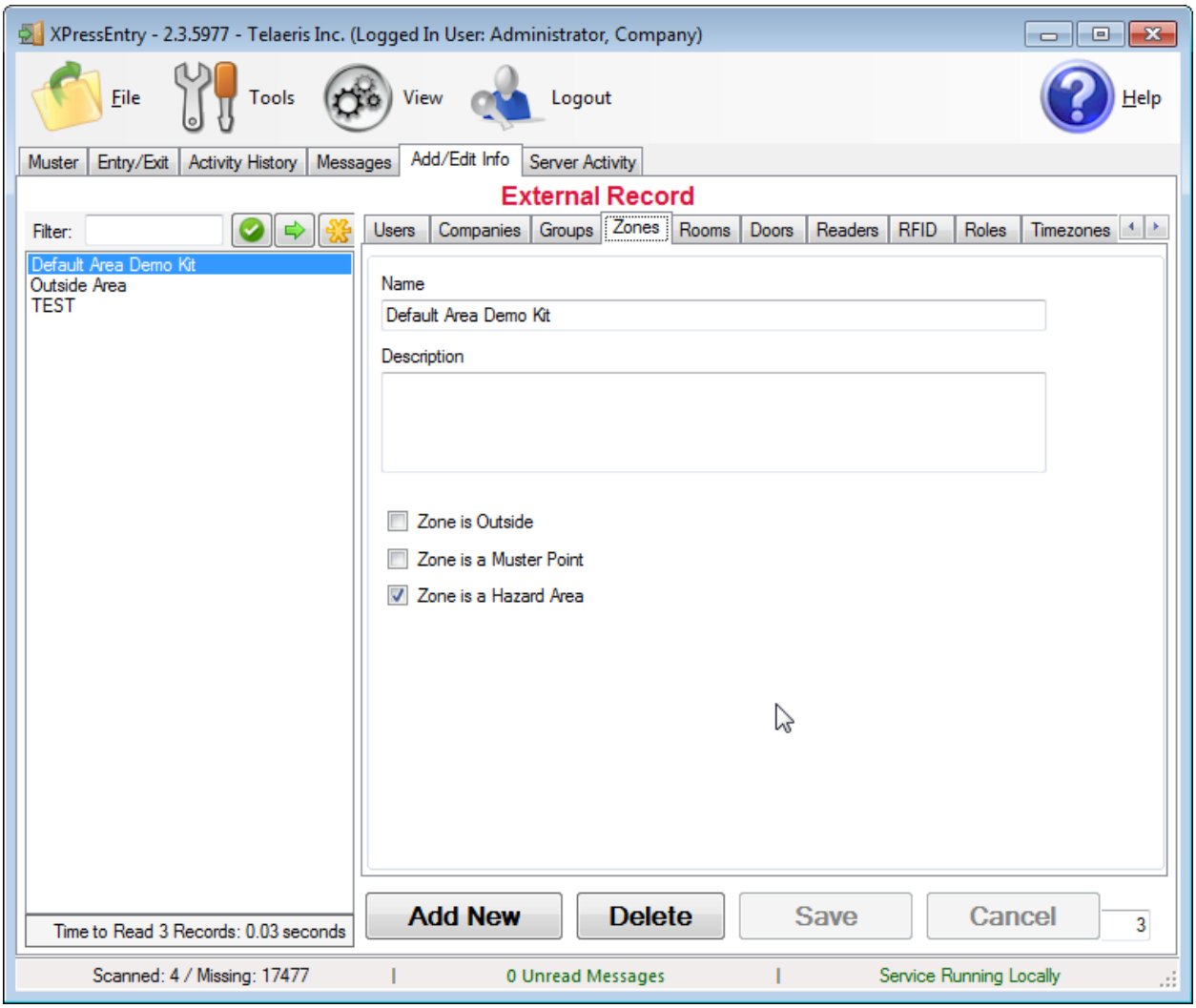


After you press the “Perform Merge” and confirm with “Yes”, the reader will be removed from the bottom “Readers” list and added to the “Handhelds” list.

Zones

If you are going to be using OnGuard zones for mustering, it's suggested you double check the Zone settings.
Any outside zone should have the "Zone is Outside" checked.
In addition, it's normal to check the "Zone is a Muster Point" checkbox for outside zones.

Any area where you want to track occupancies for mustering should have the "Zone is a Hazard Area" box checked.

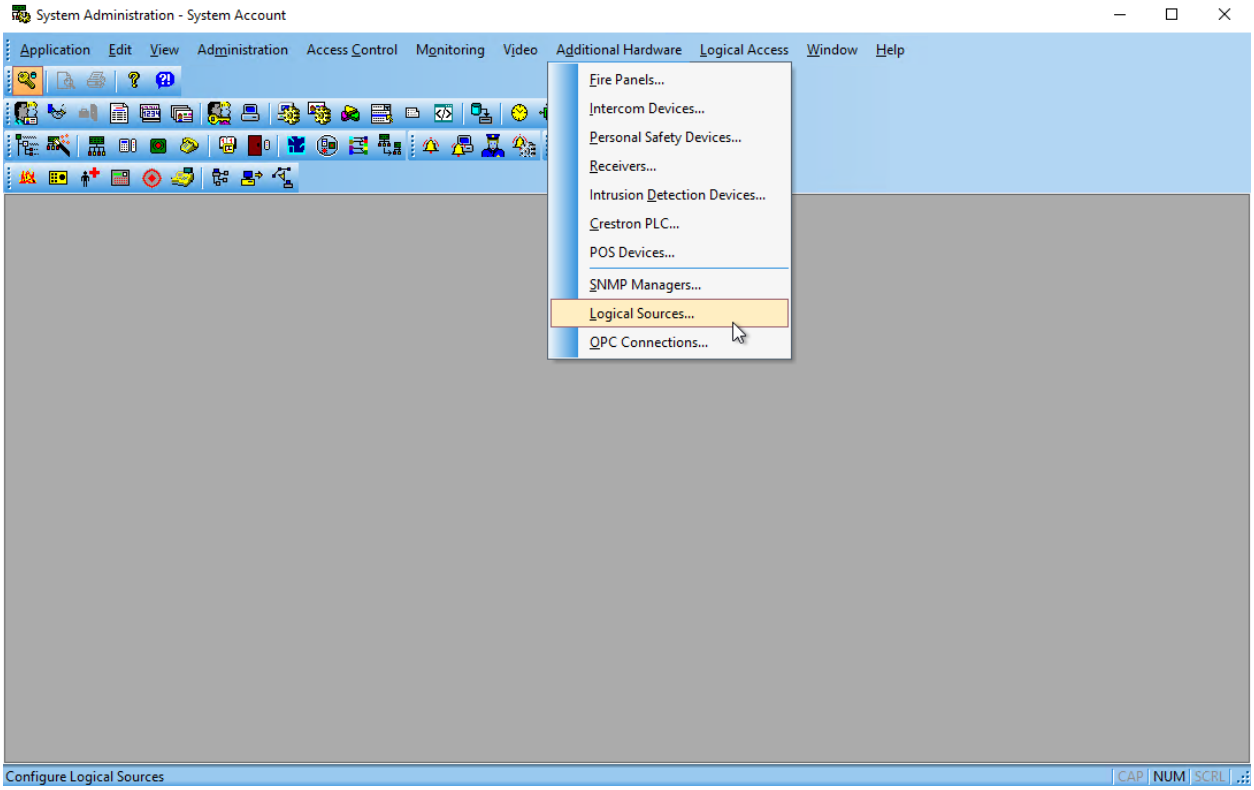


Activities

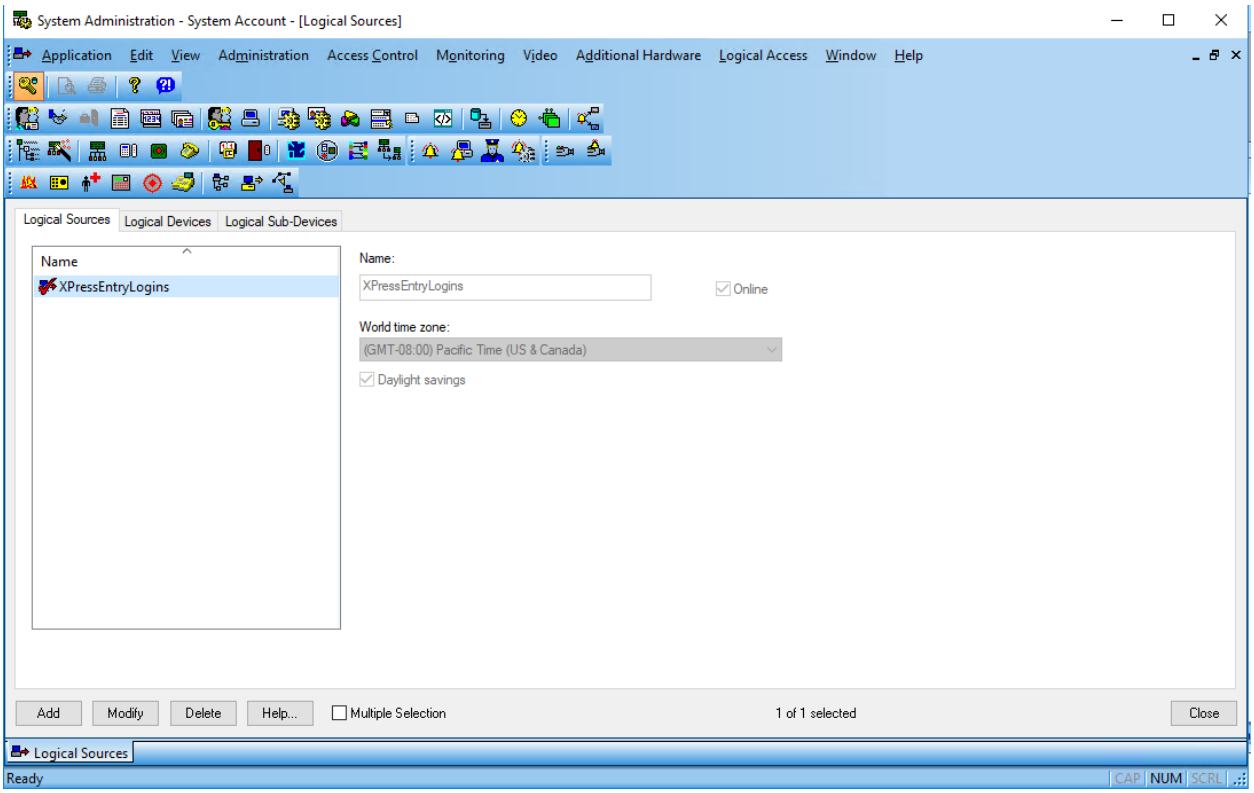
XPressEntry will synchronize activities if that option has been set by Data Manager.
Entry/Exit activities will be sent to the OnGuard reader set for External Entry/Exit Reader on the Door.
Verification and Muster activities will be sent to the specific reader they are scanned at.

Login Activities

When utilizing handheld device login, the login and logout records can be sent to OnGuard as an Alarm Event. To enable this feature, Start with Creating a new Logical Source. From System Administration, go to *Additional Hardware -> Logical Sources.*



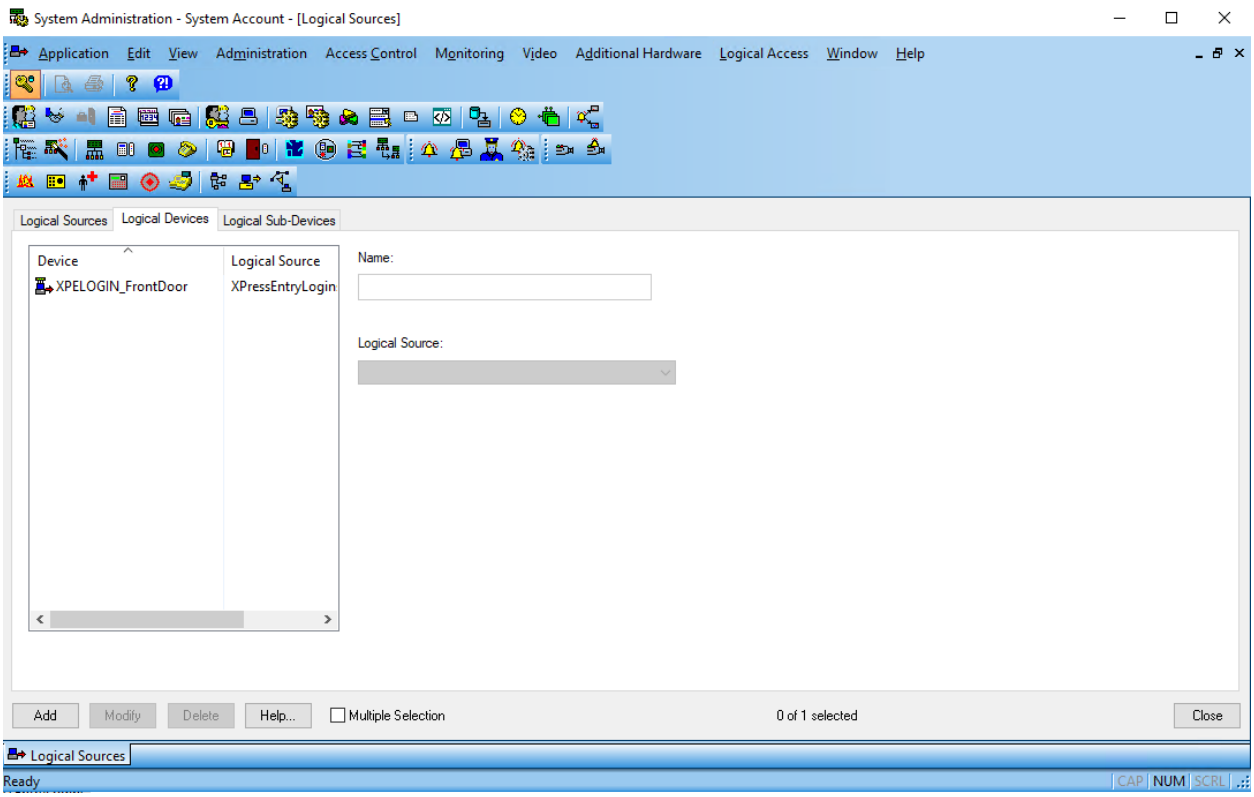
Add a new Logical Source.



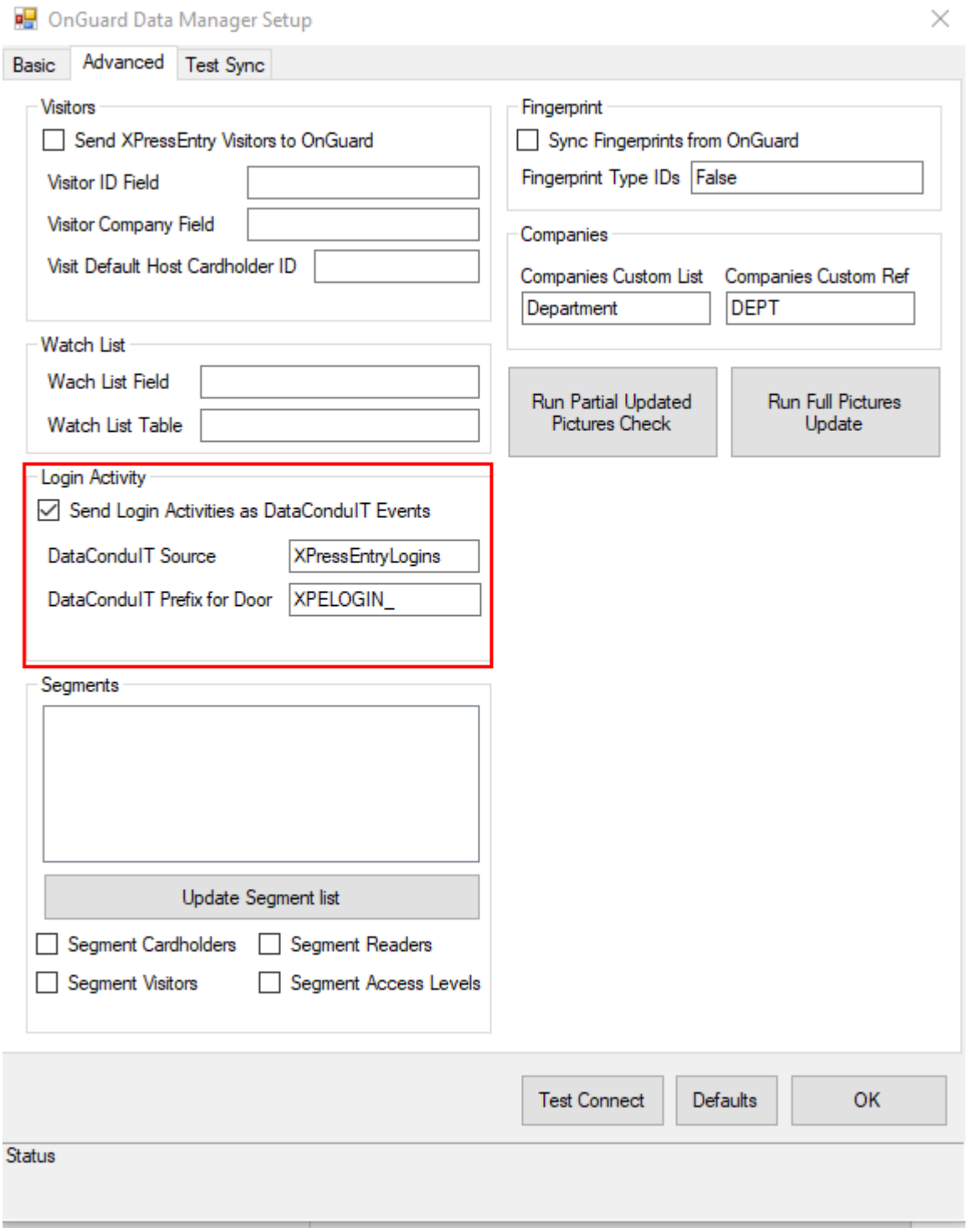
Create a new Logical Device. The Logical Device name is important, and requires 2 things:

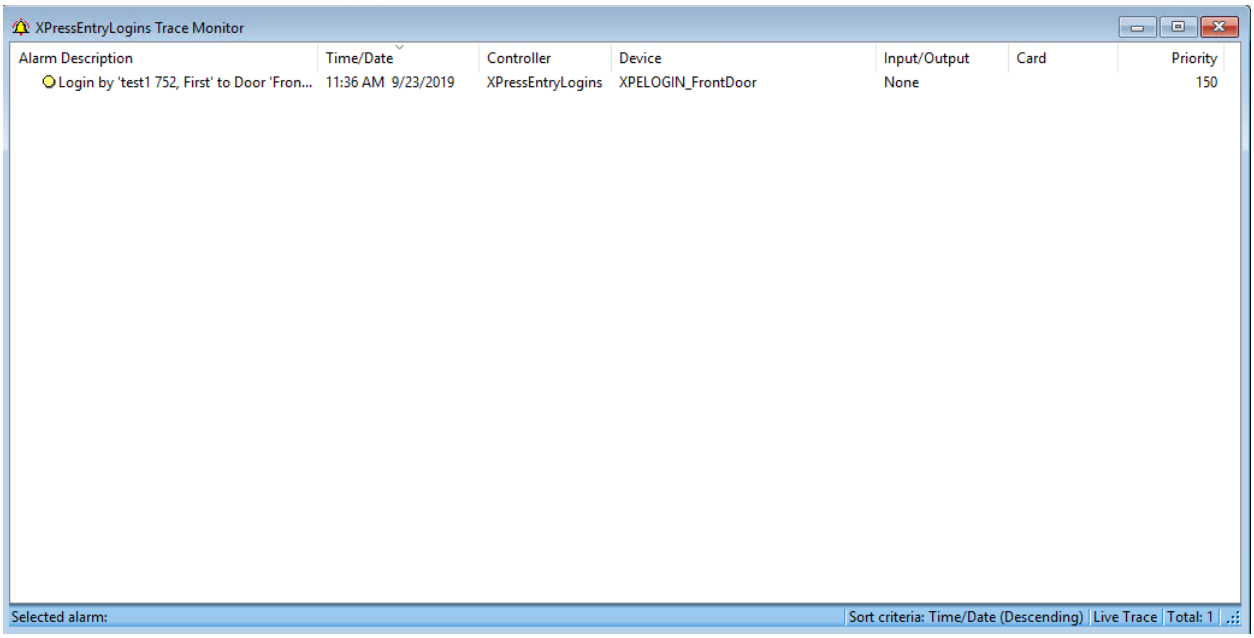
1. A Prefix Identifier. For example, XPELOGIN_
2. The logical device name needs to contain the name of the Door that is created in XPressEntry. For example, FrontDoor is the door name we will be using in XPressEntry for a single unit.

Combine the two to form XPELOGIN_FrontDoor. If there was a different door, the second logaical device can be called XPELOGIN_BackDoor.



Back to XPressEntry DataManager Setup, Under the *Advanced* Tab, look at the Login Activity Tab. Select *Send Login Activities as DataConduIT Events.*(At the time of this writing, only DatConduIT events are supported. OpenAccess support coming soon.) Set the *DataConduIT Source* field to the name of the Logical Source. Set the *DataConduIT Prefix for Door* as the prefix created for the Logical Device. Press OK, then Save. Login and Logout handheld activities will now be sent to OnGuard Alarm Monitoring when *Send XPressEntry Activities to Data Manager* is enabled.


OnGuard Data Manager Setup
Basic
Advanced
Test Sync
Visitors
Send XPressEntry Visitors to OnGuard
Visitor ID Field
Visitor Company Field
Visit Default Host Cardholder ID
Watch List
Wach List Field
Watch List Table
Login Activity
Send Login Activities as DataConduIT Events
DataConduIT Source
XPressEntryLogins
DataConduIT Prefix for Door
XPELOGIN_
Segments
Update Segment list
Segment Cardholders
Segment Readers
Segment Visitors
Segment Access Levels
Fingerprint
Sync Fingerprints from OnGuard
Fingerprint Type IDs
False
Companies
Companies Custom List
Companies Custom Ref
Department
DEPT
Run Partial Updated Pictures Check
Run Full Pictures Update
Test Connect
Defaults
OK
Status


XPressEntryLogins Trace Monitor
Alarm Description
Time/Date
Controller
Device
Input/Output
Card
Priority
Login by 'test1 752, First' to Door 'Fron...
11:36 AM 9/23/2019
XPressEntryLogins
XPELOGIN_FrontDoor
None
150
Selected alarm:
Sort criteria: Time/Date (Descending)
Live Trace
Total: 1