ASSA ABLOY

OnGuard with DSR

(Door Service Router)

Software Installation Manual

SWMN3B

December 2015

The global leader in door opening solutions

Table of Contents

Overview

This Quick Reference provides information on performing a basic installation of OnGuard with DSR (Door Service Router) version 7.0

IMPORTANT: Be sure to verify all hardware for compatibility with Windows® operating system. See the Microsoft® website, (www.microsoft.com), for more information.

Pre-Installation Checklist

Verify you have the DSR DVD or DSR install file.

Have you performed these steps on each computer?

- Installed and configured the appropriate Windows operating system
- Installed appropriate service packs
- Verified that the network is currently operational

DSR Requirements

The following requirements apply:

DSR Software System Requirements

Operating System	Windows 7 (64 Bit), Windows 8.1 (64-bit), Windows 10 (64-bit), Windows Server 2008 R2 64 Bit or Windows Server 2012 64-bit
Java® Runtime Environment	Java 1.8.0_51 (installed with DSR)
Apache Tomcat™	8.0.21 (installed with DSR)

IMPORTANT: The server installation location, along with the username and password is required for DSR installation. If this is a previous installation, those details need to be available.

DSR Hardware Requirements (Minimal)

Central Processor	Intel® Core 2 Quad processors or equivalent for 128 locks/DSR or greater
RAM	8 GB RAM
Disk Drive	50 GB Free Hard Disk Space

IMPORTANT: Virtual machines should have equivalent resources

DSR Lock Capacity

For any capacity limits or recommendations, please contact 1-800-810-WIRE

Credits

Copyright© 1996-2015, The PostrgreSQL GLobal Development Group
Microsoft and Windows are trademarks of the Microsoft Corporation in the U.S. and/or other countries.
Intel Core is a trademark of Intel Corporation in the U.S. and/or other countries.
Oracle and Java are registered trademarks of Oracle and/or its affiliates.
Apache Tomcat is a trademark of Apache Software Foundation.

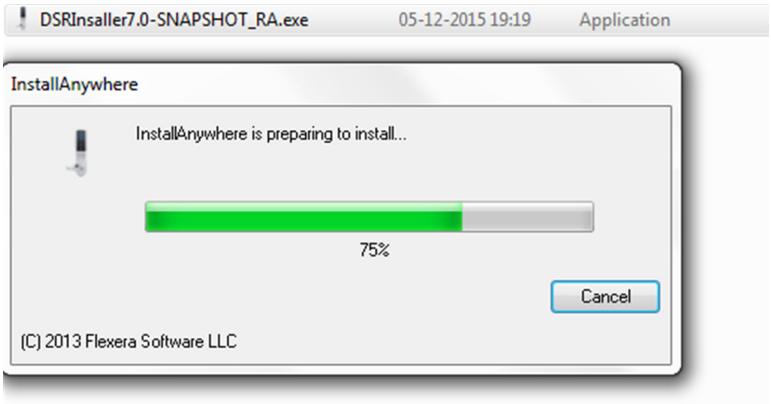
DSR Installation

1. Log in to the computer where you are installing DSR with a domain account with local Administrator privileges. (If a domain is not present, use an Administrator account.)
2. Close any open applications and disable virus-checking software.
3. Download DSR from **Lenel.Doorservicerouter.com**.
   Username: leneldealer
   Password: lenel

   Select and run the installer - DSRInstaller7.0.exe
4. Follow the instructions contained in the DSRInstaller.exe Installation screens, and the 'Windows Installer Prepare to Install' screens.

Run Installer

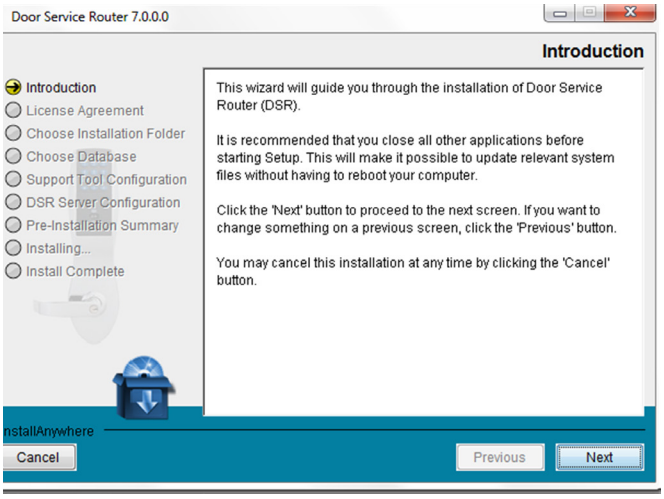
Once .net Framework is installed, run the DSR Setup Wizard and follow the onscreen directions.



Introduction

This is the Setup screen that guides the user through the installation process.

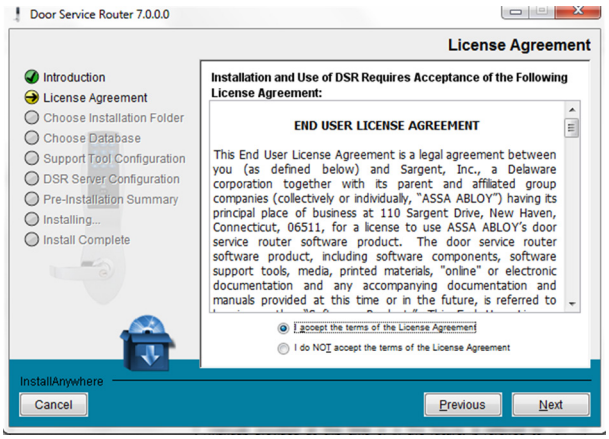
Click the Next > button to continue.



License Agreement

The DSR End User License Agreement (EULA) must be accepted for the DSR installation to continue. To accept terms and conditions, select "I accept the terms of the License Agreement".

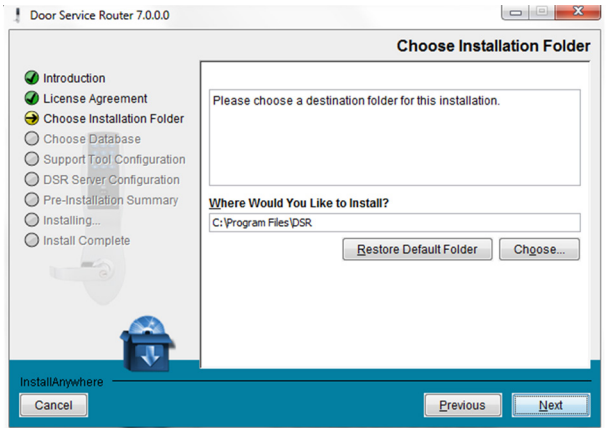
Click the Next > button to continue.



Choose Installation Folder

Select the destination folder for the installation. (Default is C:\Program Files\DSR)

Click the Next > button to continue.

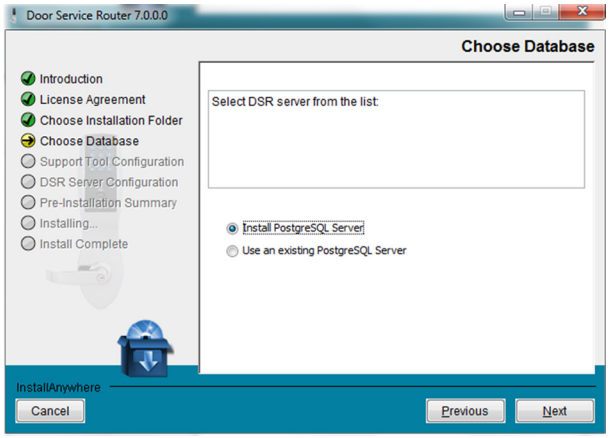


Choose Database

There are two options:

1) **Install PostgreSQL Server**- In this case Installer will install new PostgreSQL9.4

2) **Use an existing PostgreSQL Server**- if the DSR database is already in place.

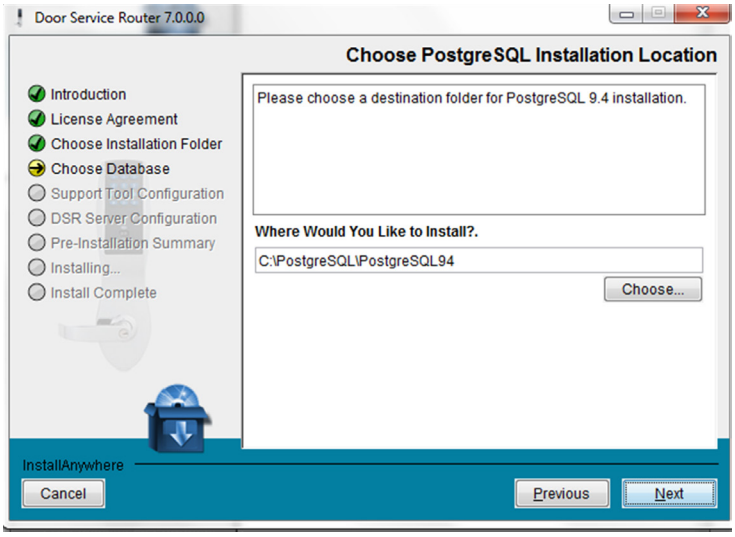


Choose PostgreSQL Installation Location

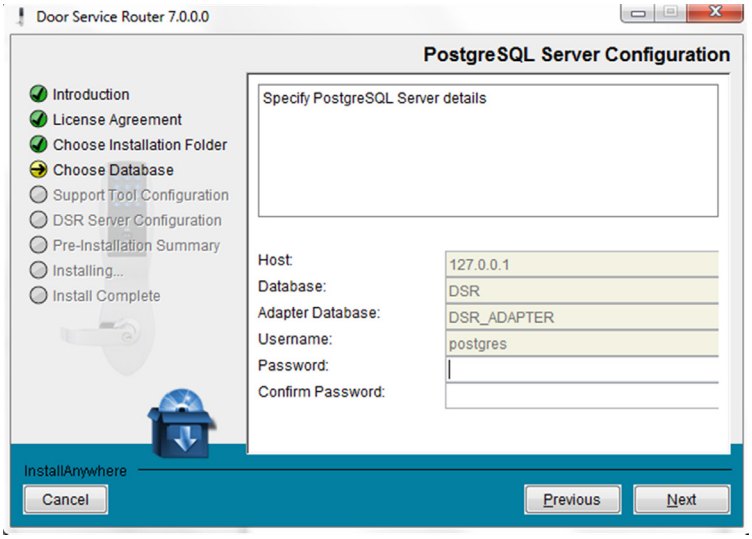
It is recommended to install or use PostgreSQL.

Select **Install PostgreSQL** to host the DSR database on its own environment on the local server. This is the most common option.

Select the proper option and click the Next > button to continue.

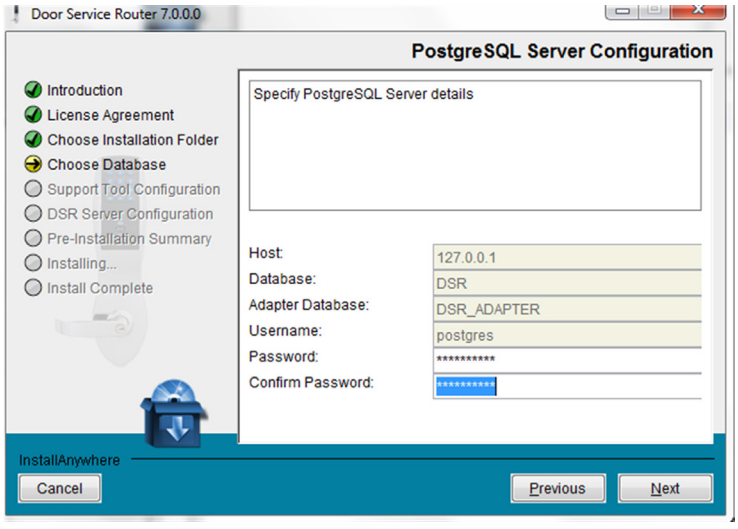


PostgreSQL Server Configuration

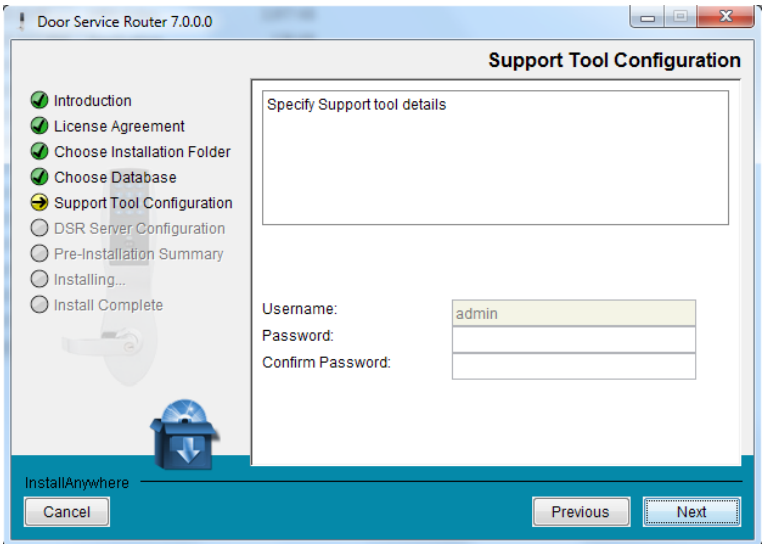


User enters password in 'password' and 'confirm' fields; if passwords do not match, an error message occurs.

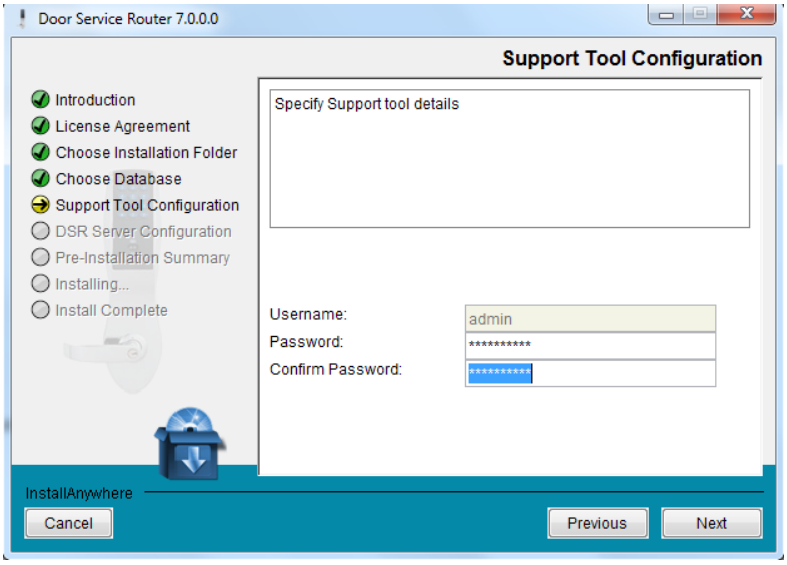
Click the Next > button to continue.



Support Tool Configuration



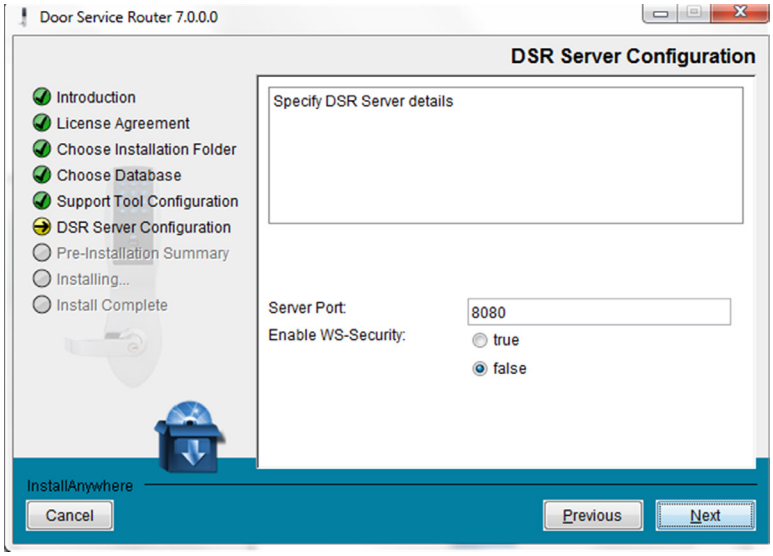
User enters password in 'password' and 'confirm' fields; if passwords do not match, an error message occurs.



Click the Next > button to continue.

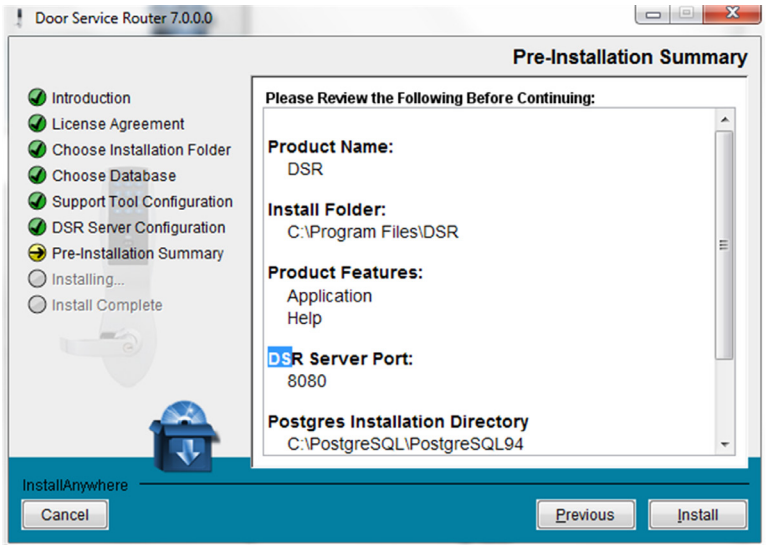
DSR Server Configuration

From this screen user can change the DSR port and enable or disable WS-security.



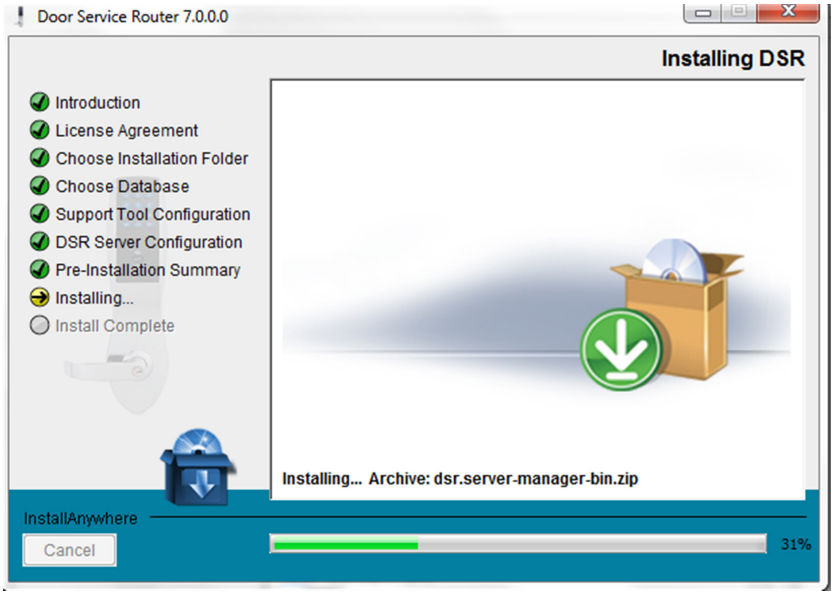
Pre-Installation Summary

When install details are confirmed correct, click on Install button.



Installing DSR

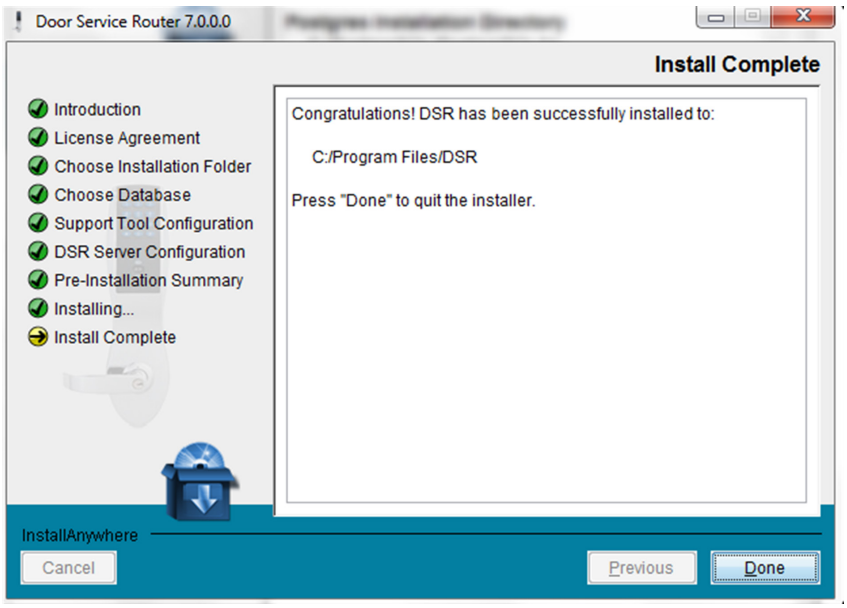
Files are extracted, then installed.



Installation Complete

DSR has installed successfully.

Click Done to complete installation.



Install OnGuard

Install OnGuard according to the manufacturer's instructions.

Install the ASSA ABLOY AddOn on the OnGuard Server

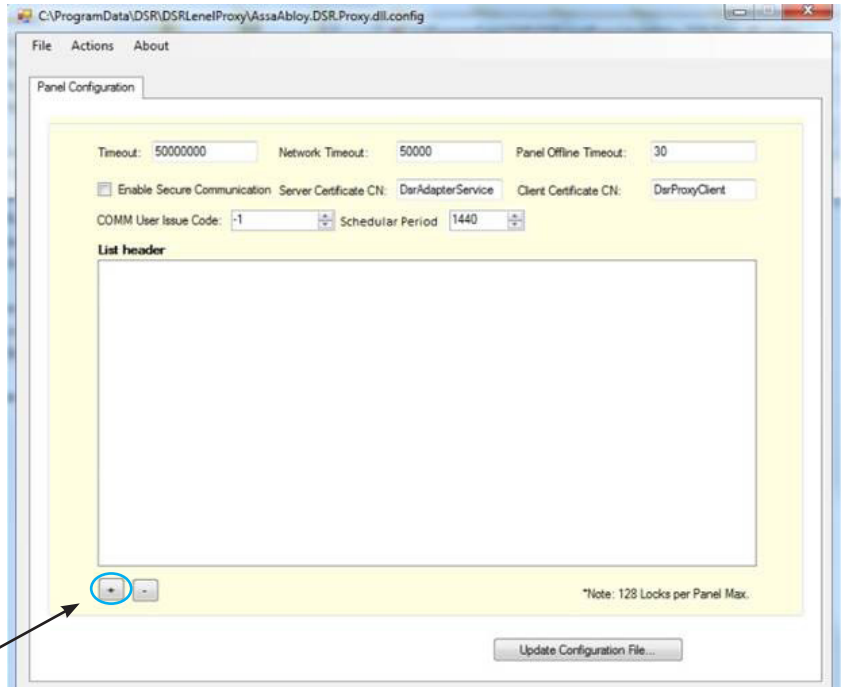
This application was written to help the OnGuard user create the configuration file used by the ASSA ABLOY integration. The application places the newly created or updated configuration file in the directory path that is expected by the OnGuard system based on the PC's Operating System. This file must be created before any ASSA ABLOY Panel can be created.

1. Run the ASSA ABLOY Add-On installer downloaded from the LENEL website and follow the on screen instructions.
   - Add-On must be installed on same machine as LENEL Communication Server.
2. Confirm DSR is installed. Please see page 3.
   - If there are any issues during install please contact ASSA ABLOY tech support at 800-810-WIRE (9473) or OEMSupport@assaabloyusa.com.
3. Open the "DSR-OnGuard Configuration Maker.exe" application located in C:\Program Files (x86)\ OnGuard.

Panel Configuration

The "Panel Configuration" tab presents the user with a quick way to create a new configuration from scratch. It presents the user with the ability to enter specific items about the OnGuard System as well as some items to start the creation of the Panels.

Here is an example of this tab and its items:

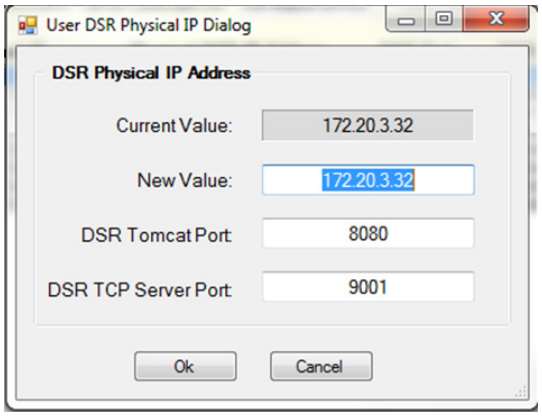


Click "+" to create a new panel.

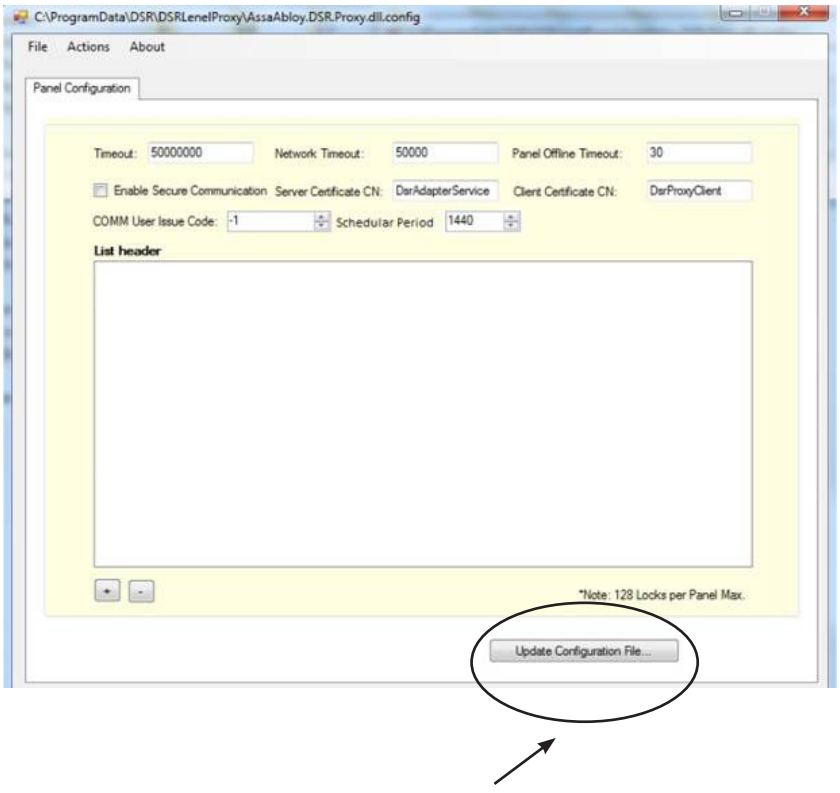
This tab allows access to more specific items about the Panel. Once a Panel is selected, its appropriate information is displayed and waits for any user modification.

Item	Description
Scheduler Period	Specifies the number of minutes in between the lock waking up. The default is 1440 (1 day).
Issue Code	Specifies what issue code will flag badges as being wakeup users.

Double click the entry requiring the DSR Physical IP address.



Enter the DSR physical IP address.
The DSR Tomcat Port will default to 8080.
The DSR TCP Server Port will default to 9001.
Do not change unless directed by support.

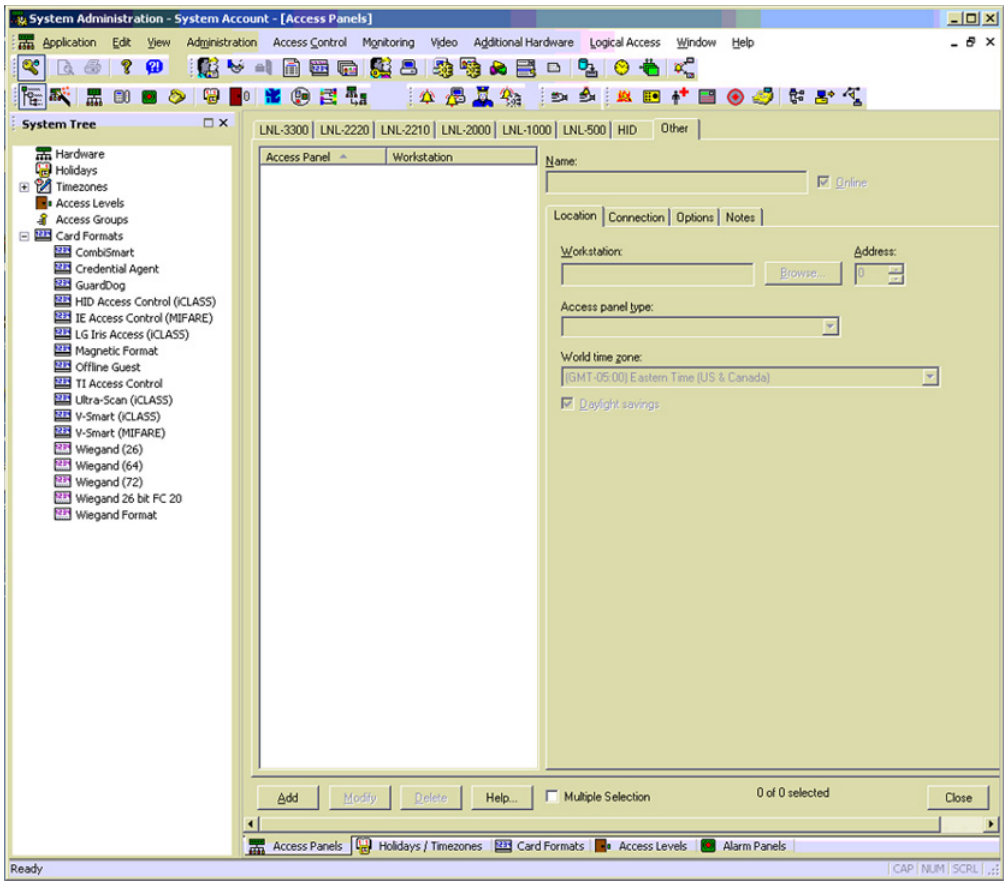


To update the Configuration File click “Update Configuration File”.

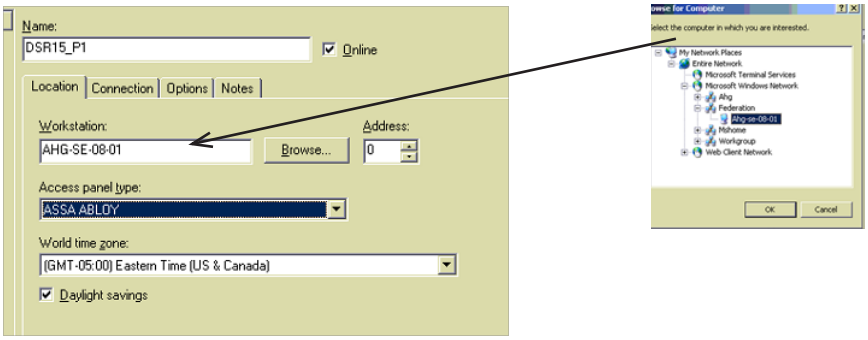
Add ASSA ABLOY Panel

In OnGuard System Admin:

- Go to “Panel”.
- Go to “Other” Tab.
- Click on “Add”.



Location Tab

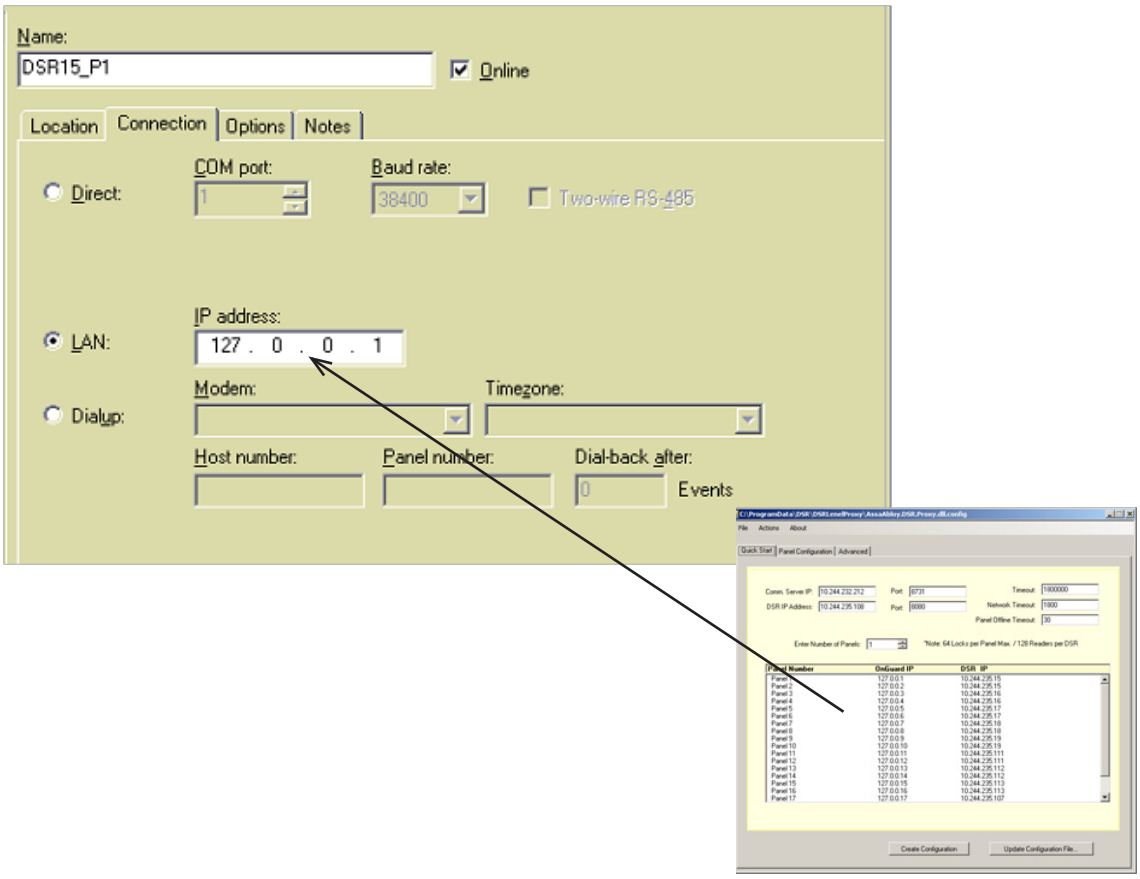


- Name the Panel.
- Select or enter the OnGuard Server or Workstation name.
- Select ASSA ABLOY for panel type.

NOTE: OnGuard World time zones only affect event log time stamps . All locks follow the world time zone of the DSR server they are assigned to. OnGuard can not adjust the time of the DSR Server.

Connection Tab

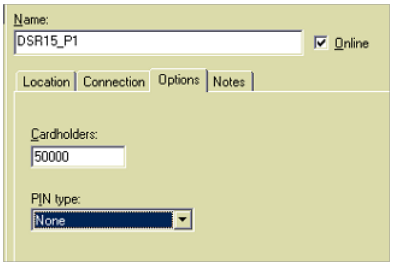
In the LAN area enter the DSR IP Address as configured in the ASSA ABLOY configuration add-on.



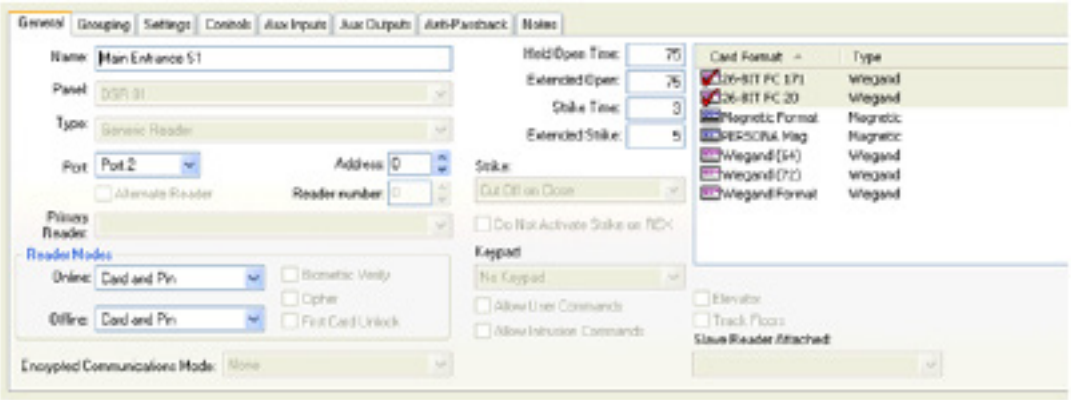
Option Tab

Enter the number of cardholders (up to 50,000 supported)

- PIN type = None
- Click **"OK"** to save



Add ASSA ABLOY Reader



- In OnGuard System Admin go to readers.
- Click **"Add"**.
- Name the reader.
- Select any valid port or address.
- Select the appropriate ASSA ABLOY panel.
- Select appropriate card formats –
  Please note there is not support for smart card formats, only standard Wiegand and Mag.

  NOTE: 2399 users per number of card formats – 1 format 2399 users, 2 formats 1199 users, 3 formats 799 users, etc.
- Readers only support online reader mode. Offline is disregarded.
- Strike time and extended strike time are configurable – held and extended open are not a function of the lockset.
- Right click on any reader and change the reader mode.

  NOTE: FC only mode is not supported.

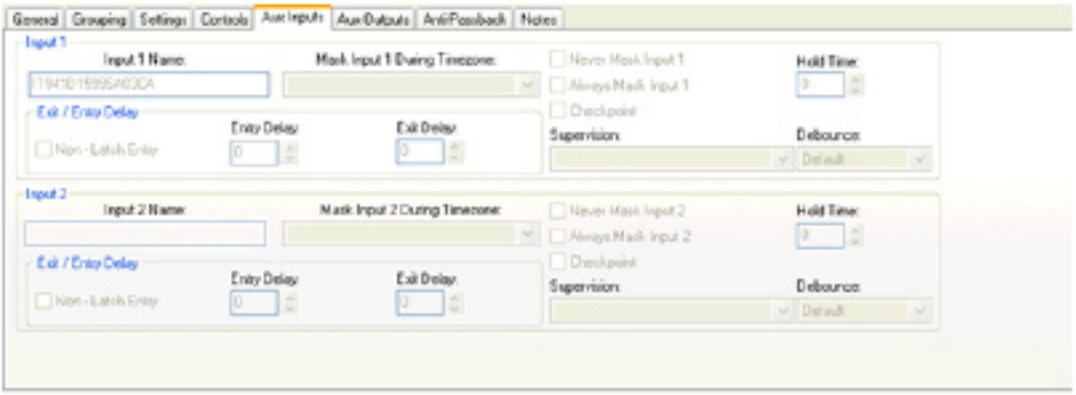
  Locked Mode: Locks out all users on a reader.

  Card and PIN mode: Only results in card and pin operation if a user has both a card and PIN. If a user does not have a card and PIN, the reader will operate as if the reader was in card only mode. Presentation is order dependent – card must be presented before the PIN is entered.

  Card only Mode: Unit will only require a card.

  Unlocked Mode: Leaves lock unlocked. Only supported on the PoE and hard-powered units.

  Card or PIN Mode: Will grant access with card or PIN. Not supported on units with mag card readers.
- Click **"OK"**.

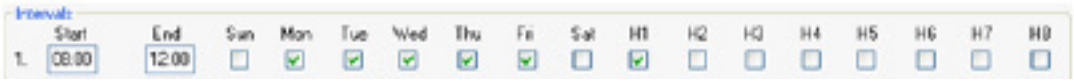


- Go to the **"Aux Inputs"** tab.
- Click **"Modify"**.
- Enter serial number of lock in Input 1 name. (Serial numbers can be found on the lock or in New_RDR message in hardware monitor.)
- Serial numbers will appear in alarm monitor as locks come online. If it has not appeared in the monitor the serial number is printed on the lock as well as its box.
- Serial number must be entered exactly and in all capital letters.

Add Time Zones

Time zones and Holidays operate in a different way for ASSA ABLOY locksets. This is illustrated through these three examples:

Example 1:



If the Time zone only has one interval (Example 1) operation is as follows:

Assume that H1 is December 24th and H2 is December 25th

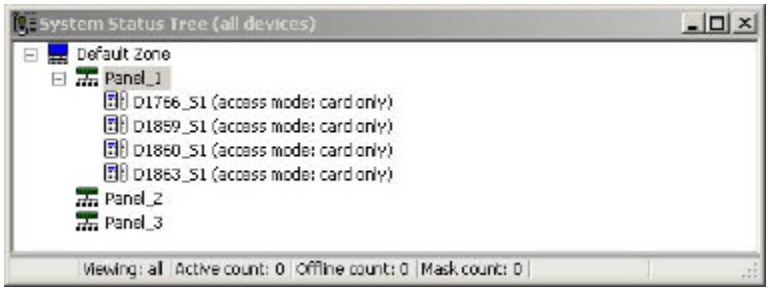
- If the 24th occurred on a M,Tu,W,Th,F – the user would have access from 8 – 12
- If the 24th occurred on a Su or Sa – the user would be denied
- If the 25th occurred any day – the user would be denied

Example 2:

Example 3:

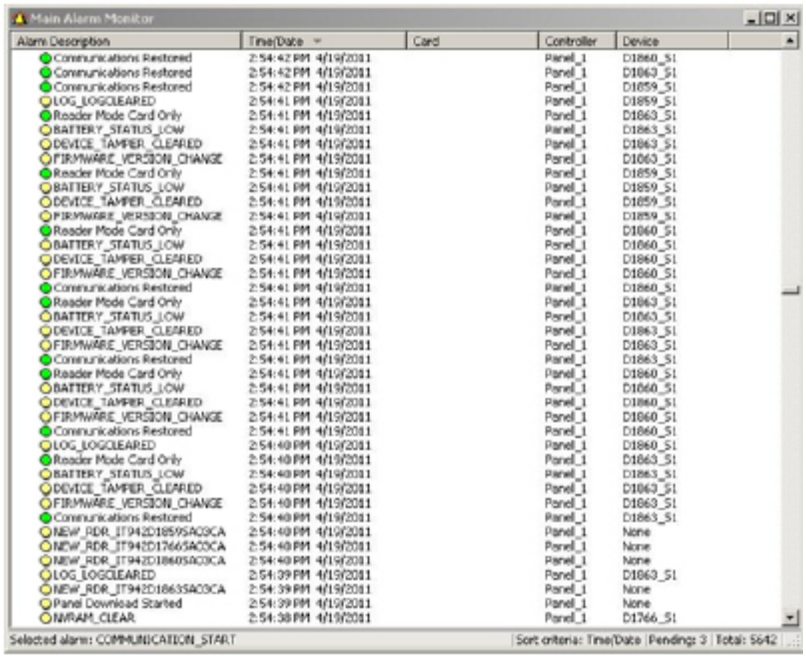
In both cases of examples 2 and 3, both intervals would prevent access on H1 and H2. If different operation between intervals is required, each interval needs to be a unique time zone.

System Tree



- Red Xs in the tree indicate the connection between OnGuard and the DSR has failed.
- Yellow Xs on WiFi locks indicate the lock has not communicated with the system for <scheduler period> x 2.1 or is new to the system.
- Yellow Xs on PoE locks indicate the lock is offline.

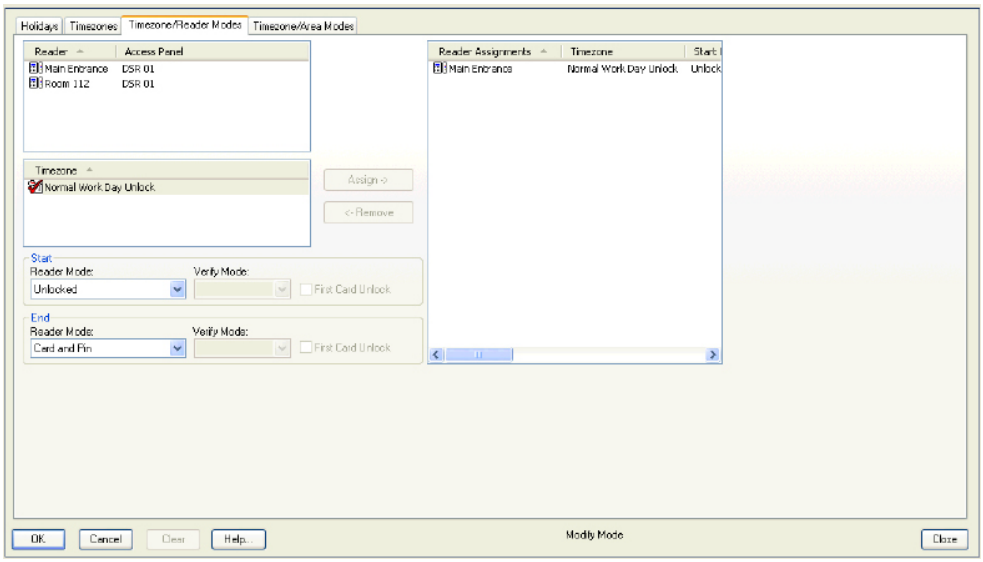
NOTE: Reader mode changes will not go into effect until the WiFi lock has undergone a communication session. PoE locks reader state could be delayed by up to 15 minutes. Reader mode will not revert to the default mode of the reader if lock goes online/offline.



- All ASSA ABLOY specialty events are in CAPS and display the reader and panel with the event.
- Declined cards are only shown as card numbers if the format is assigned to the reader.

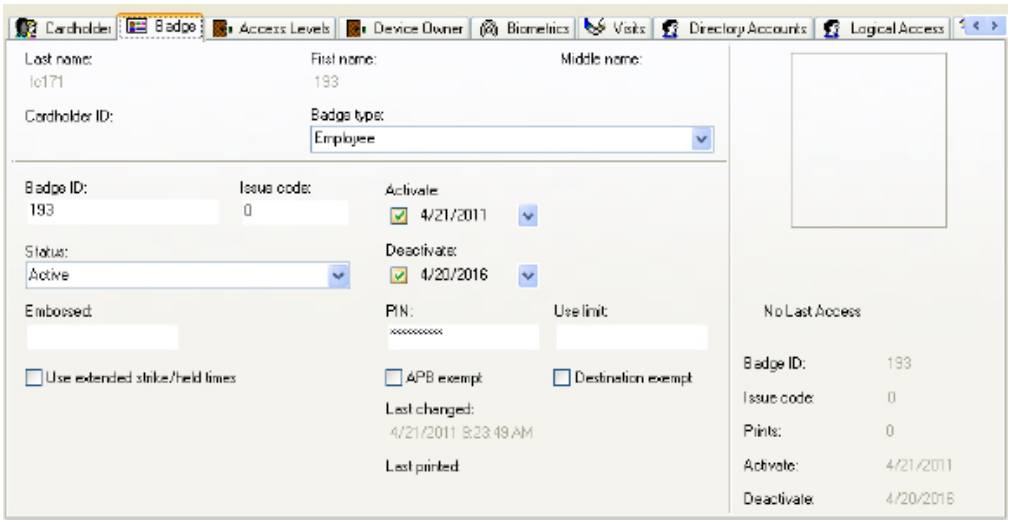
NOTE: OUT_OF_SYNC could indicate a reader issue. If OUT_OF_SYNC message occurs, please select "update hardware status" from the status tree. If there is no SYNC_RESTORED message please contact ASSA ABLOY technical support for hardware support.

Unlock Schedules



- Unlock Mode is the only supported start mode.
- End reader mode is not valid. Reader will return to previous state.

Badging Limits



Activate Date: Not evaluated.

Deactivate Date: Evaluated.

Use Limit: Not functional.

Pin Type: Limited to 4-digits only.

Extended User: Operates lock in extended mode.

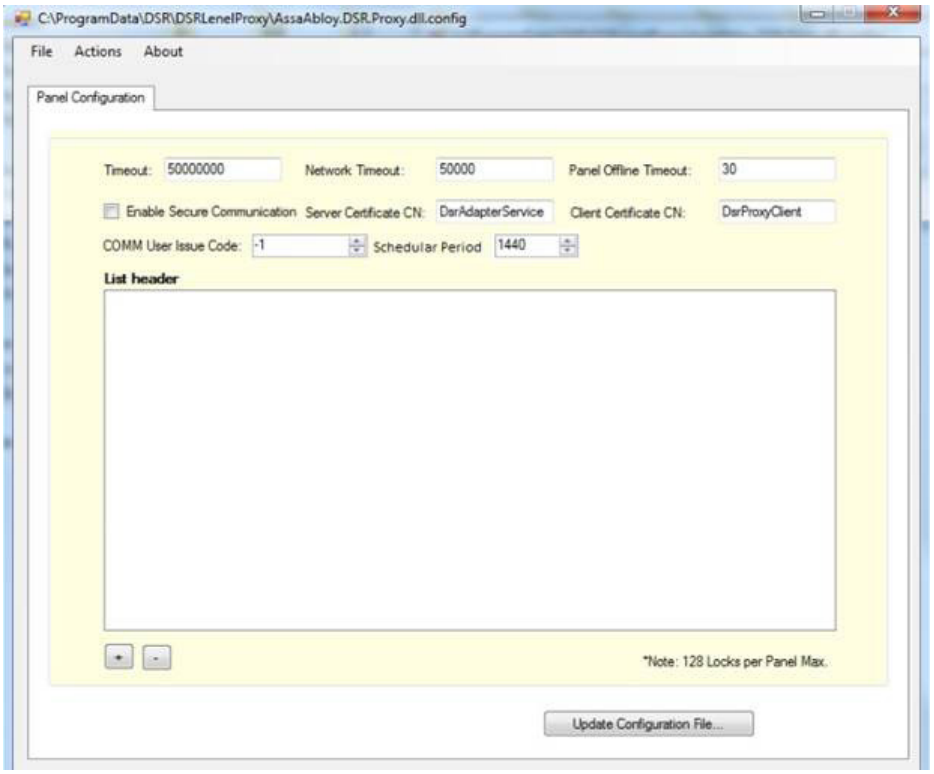
Wakeup-COMM User

Communication users will wakeup a lock and establish a connection with the server. These users are typically used on ASSA ABLOY offline Wi-Fi locks. If a communication session is already in progress the request is discarded.

Enabling a COMM User

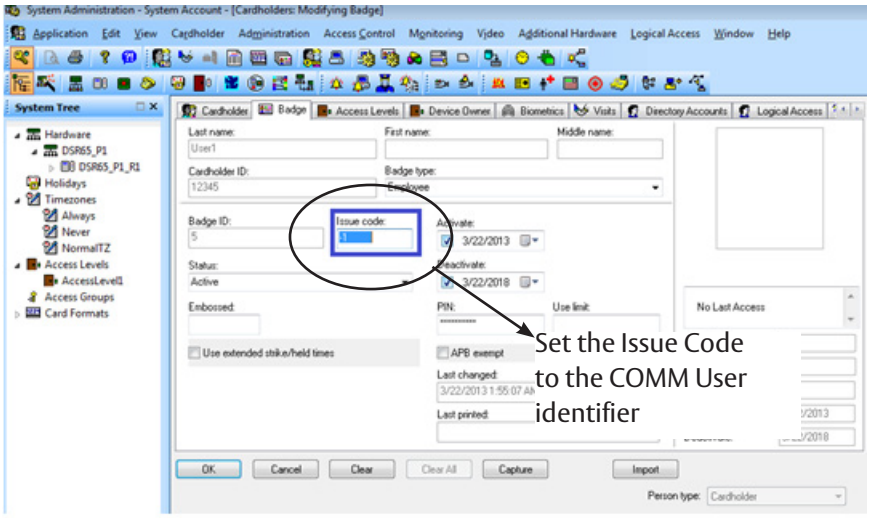
Select the COMM User Identifier

In the ASSA ABLOY Configuration Maker Tool, select the COMM User identifier. This identifier will be used when creating a cardholder in OnGuard. The default value = '-1'



Create a COMM User in OnGuard

Create a cardholder in OnGuard and set the Issue Code to the COMM User identifier created above. The default value = '-1'



NOTES:

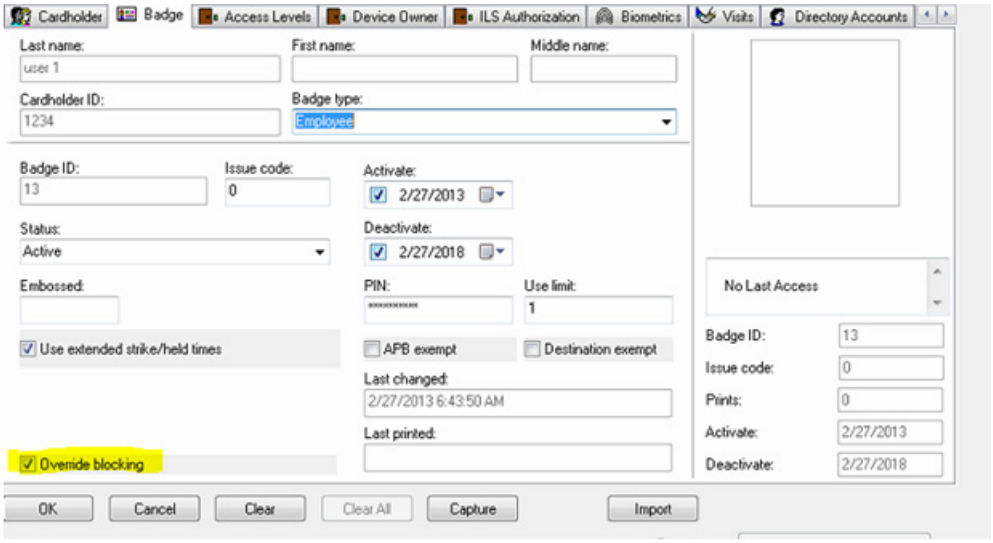
1. A COMM User initiates communication between the lock and the host but it does not grant access.
2. A COMM User overrides Dead bolt override, PASSAGE users, Double Swipe & Extended users capabilities.

Deadbolt Override

A Supervisor user type in the lock can override a deadbolt when engaged. In the Px locks a Supervisor user type will always have access to the lock while in the Sx locks a Supervisor user type will be bound by his schedule. **Please note - IN120 locks do not support this feature.**

Enabling Deadbolt Override

Deadbolt override can be enabled through the OnGuard UI by enabling the check box 'Override Blocking' while creating a Badge:



NOTES:

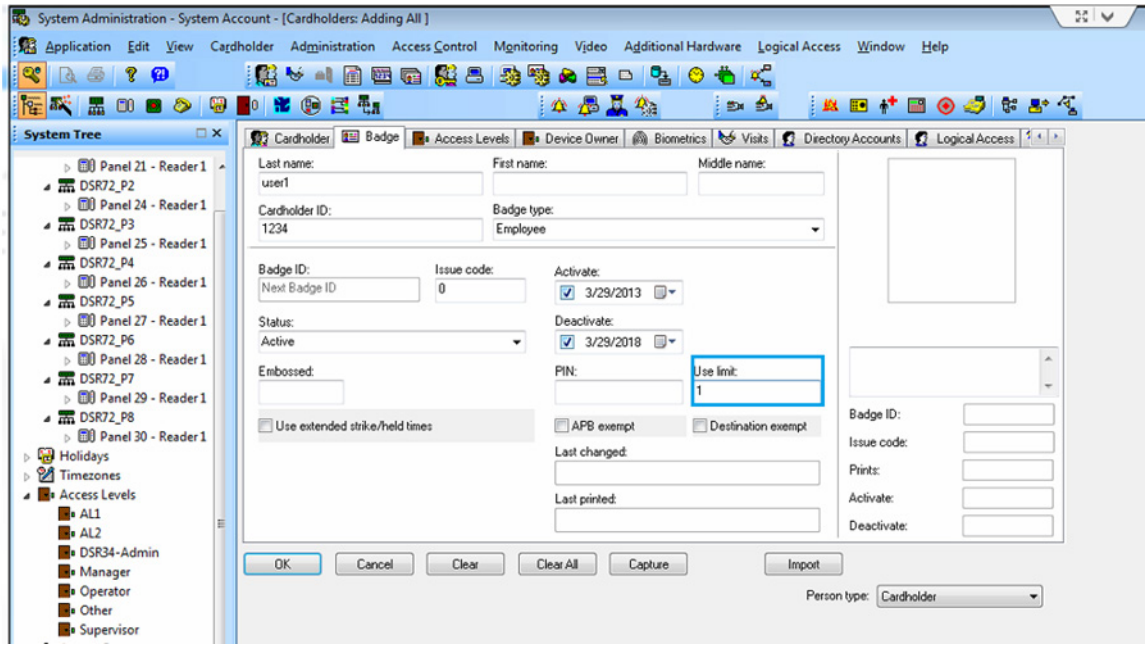
1. Enabling a COMM User will override the Deadbolt Override capability of the Supervisor.
2. Deadbolt Override will override the Extended user & Double swipe capabilities.

Limited Time Use

The Limited Time Use functionality allows OEMs to configure a cardholder in a way that the cardholder can access the door only once. This feature is supported in Sx and Px locks with firmware version N08 and higher. In Px locks with firmware version N07 or lower a cardholder with a Limited Time Use authorization will be denied access.

Creating a Limited Time Use Cardholder

To create cardholder with Limited Time Use the User Limit field must be set to '1' when entering the badge information:



1. Once the Limited Time Use cardholder has accessed the lock the cardholder will become inactive and be denied further access.
2. To re-activate the Limited Time Use, the cardholder information must be modified and re-downloaded to the DSR.
3. To change the cardholder type to a normal cardholder, clear the Use Limit field.

NOTE:

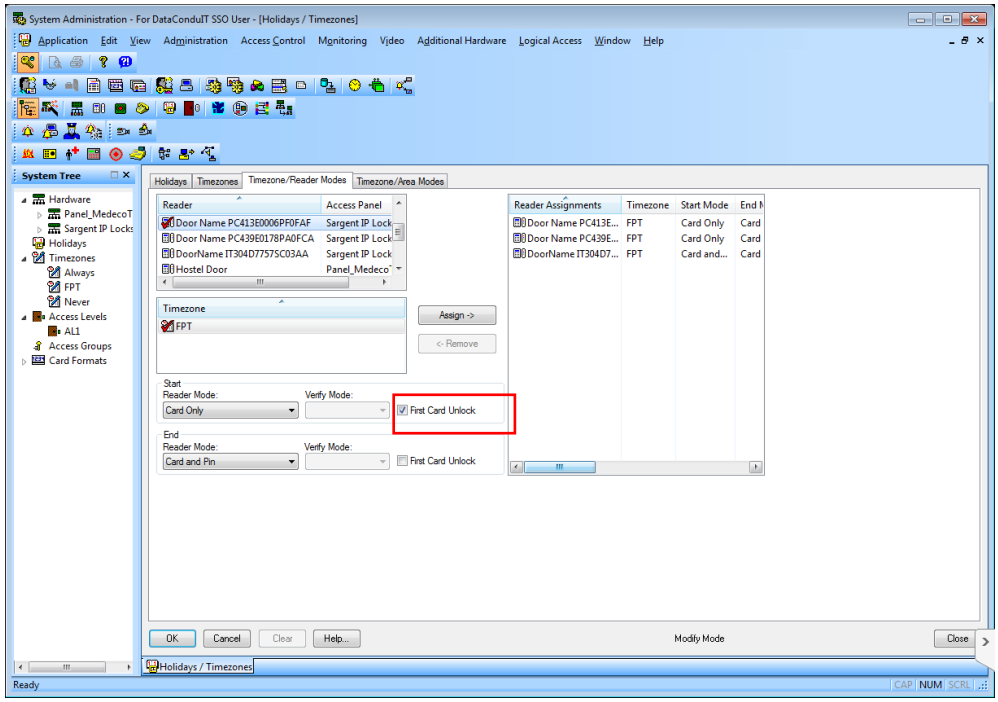
1. The Use Limit value should be set to '1'. Any other positive value will be defaulted to 1. Any negative values, 0 or null will make the user normal.
2. Enabling a COMM or PASSAGE user or a user with Dead Bolt Override or Extended user credentials will supersede the Limited Time Use capability.

First Person Through/ First Card Unlock

The First Person Through/First Card Unlock feature allows end users to configure a Timezone access mode that will unlock a door as the first cardholder gains access through the door. The door will remain unlocked until the Timezone expires.

Creating a First Person Through/First Card Unlock Timezone

1) Create a Timezone
2) In the Timezone/Reader Modes tab check the top “First Card Unlock” checkbox as shown below
3) Select the locks and assign them to the Timezone



Usability

- Once the First Person Through/First Card Unlock Access Mode Timezone is activated at the lock the door it will unlock as the first cardholder gains access through the door.
- The door will remain unlocked until the Timezone expires.

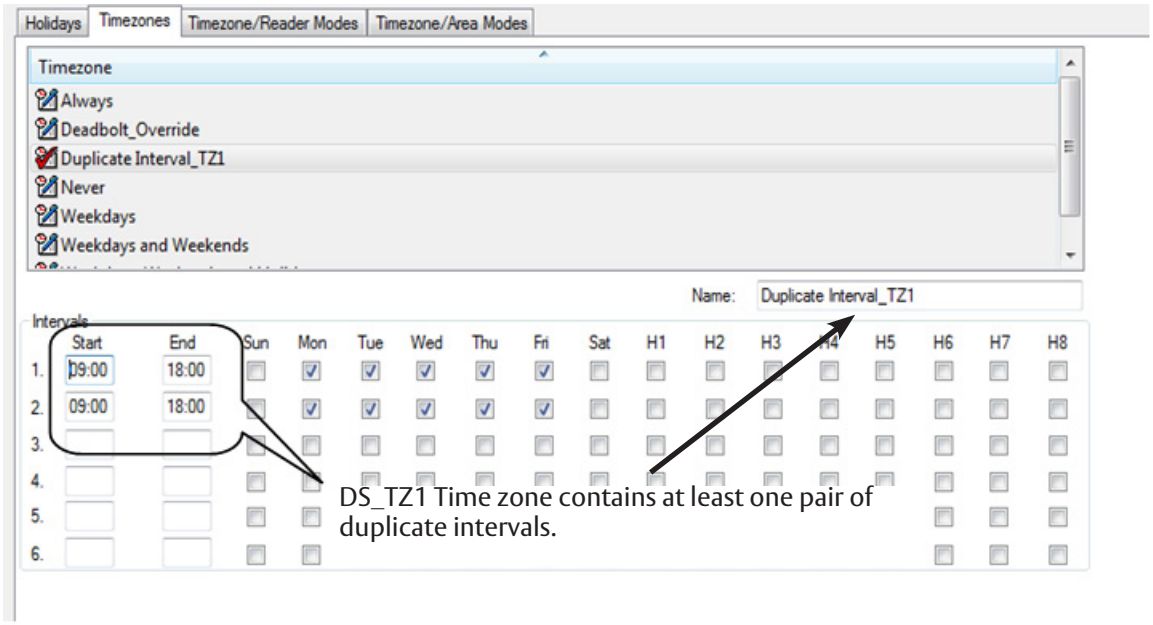
Double Swipe/ Passage User

Double Swipe is a feature available in the ASSA ABLOY Px locks. A user with Double Swipe credentials can swipe the card twice and the lock will remain unlocked for the length of the schedule. While in the unlocked mode any user with Double Swipe credentials can double swipe his/her card and the lock will be relocked. The Double Swipe feature is not available in the ASSA ABLOY Sx locks.

PASSAGE User type is a feature available in the ASSA ABLOY Sx and IN120 locks. A user with PASSAGE credentials can swipe the card and the lock will remain unlocked for the length of the schedule. While in the unlocked mode any user with PASSAGE credentials can swipe his/her card and the lock will be relocked. The PASSAGE feature is not available in the ASSA ABLOY Px locks.

Enabling Double Swipe/ PASSAGE USER

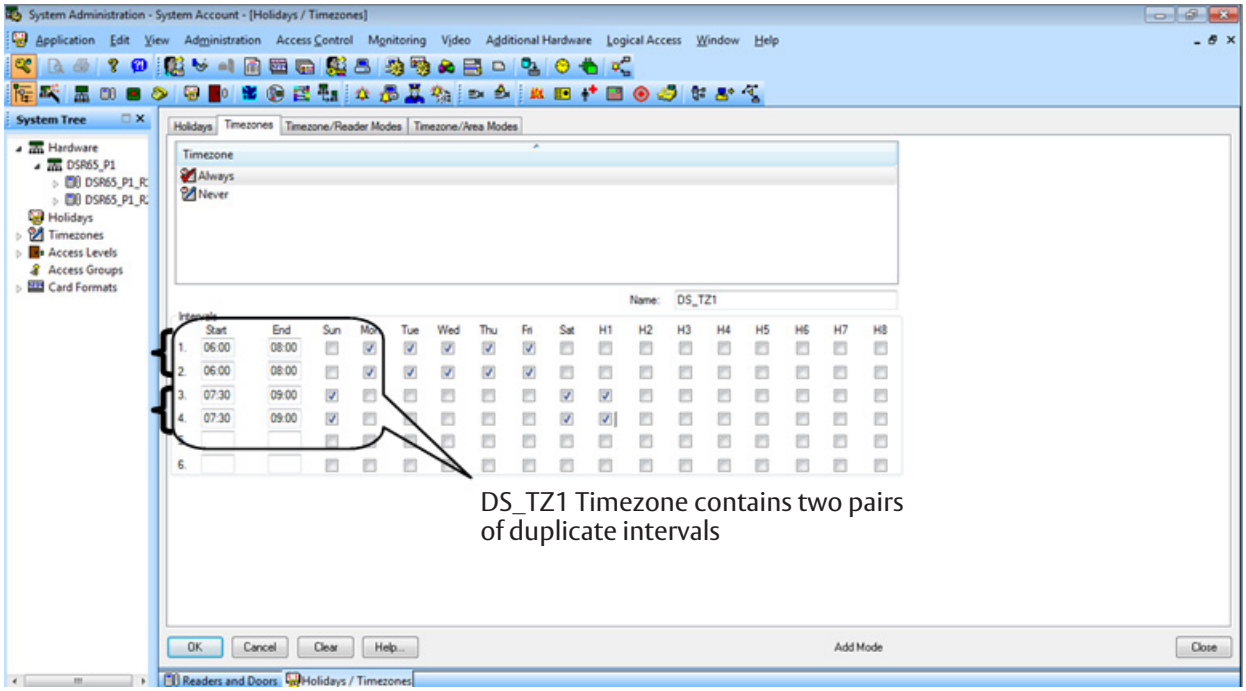
The Double Swipe/PASSAGE User function can be enabled by creating a special Timezone with at least one set of duplicate intervals. Each pair of identical intervals will reflect one User Activated PASSAGE Mode (UAPM) Timezone in the ASSA ABLOY Px locks. In Px locks Double Swipe is enabled. In Sx locks PASSAGE User is enabled.



Limitations

1. Once a Double Swipe/PASSAGE User Timezone is created it cannot be converted to a standard Timezone (i.e. remove one of the intervals). If a standard Timezone is desired then a new Timezone must be created.
2. Once a standard Timezone is created it cannot be converted to a Double Swipe/PASSAGE User Timezone (i.e. by adding another identical interval). If a Double Swipe/PASSAGE User Timezone is desired then a new Timezone must be created.

Once the Double Swipe/PASSAGE User Timezone is created continue with the creation of an Access Level and the assignment of this Timezone, Readers and Cardholders.



Example: 2 UAPM Timezones will be created in the lock(s):

1. 06:00 AM to 08:00 AM, Monday - Friday
2. 0700 AM to 09:00 AM, Saturday, Sunday, and during Type H1 holidays.

NOTES:

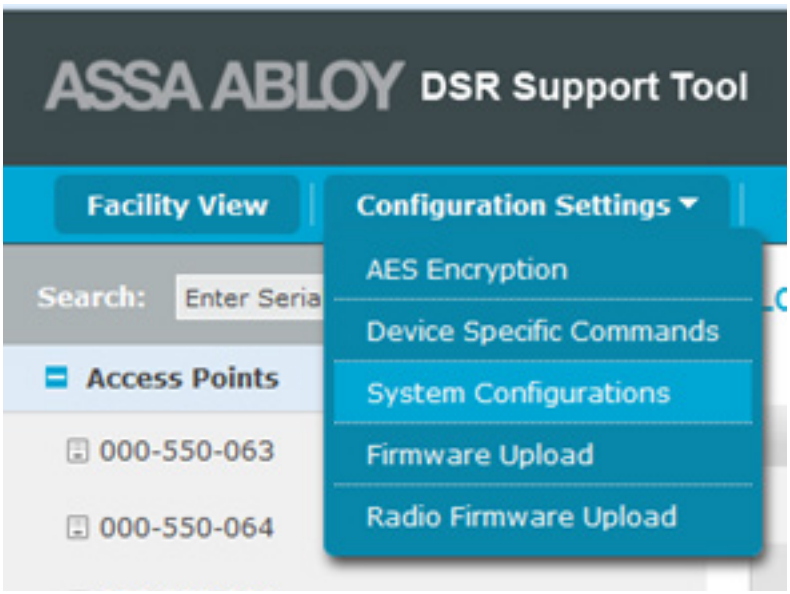
1. Up to 3 identical pairs of intervals can be specified in an OnGuard Timezone and therefore up to 3 UAPM Timezones can be created at a time from OnGuard.
2. If any of the intervals is not paired in the Timezone then Double Swipe/ PASSAGE User will not be enabled.
3. Enabling a COMM User with Dead Bolt Override credentials will supersede the Double Swipe/ PASSAGE user capability.

Battery Powered IP Locks Pulse Open

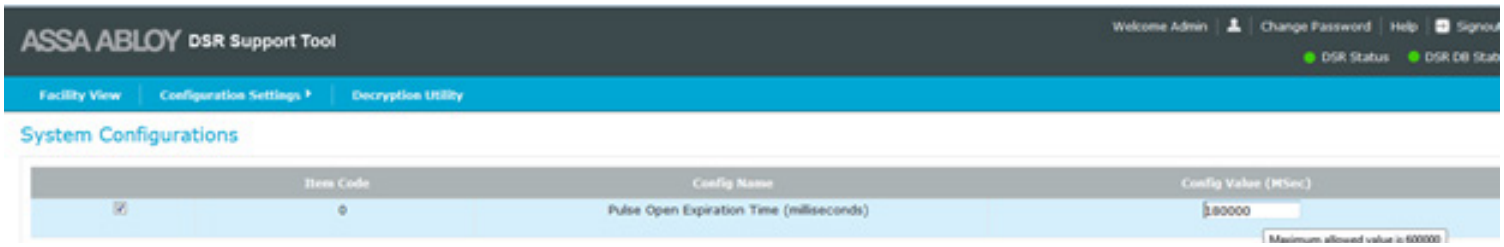
Offline battery powered IP locks can be remotely unlocked through the Pulse Open command.

Enabling Pulse Open on Battery-Powered Locks

1) Navigate to the DSR Support Tool System Configurations screen:



2) Check to enable Pulse Open on battery powered locks and specify the duration for which the command will be valid:



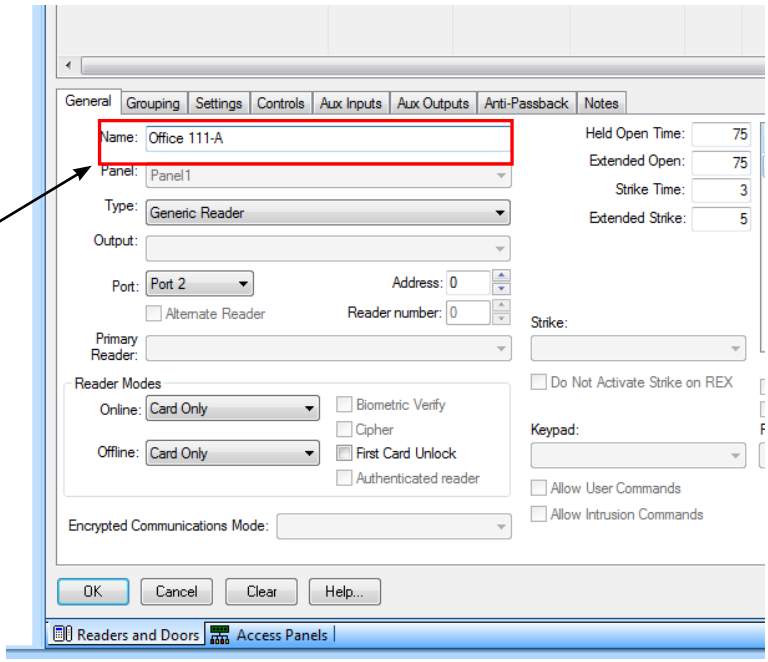
- Default value = 180,000 MSec = 3 Minutes
- Max value = 600,000 MSec = 10 Minutes

Enrolling an ASSA ABLOY Medeco XT eCylinder

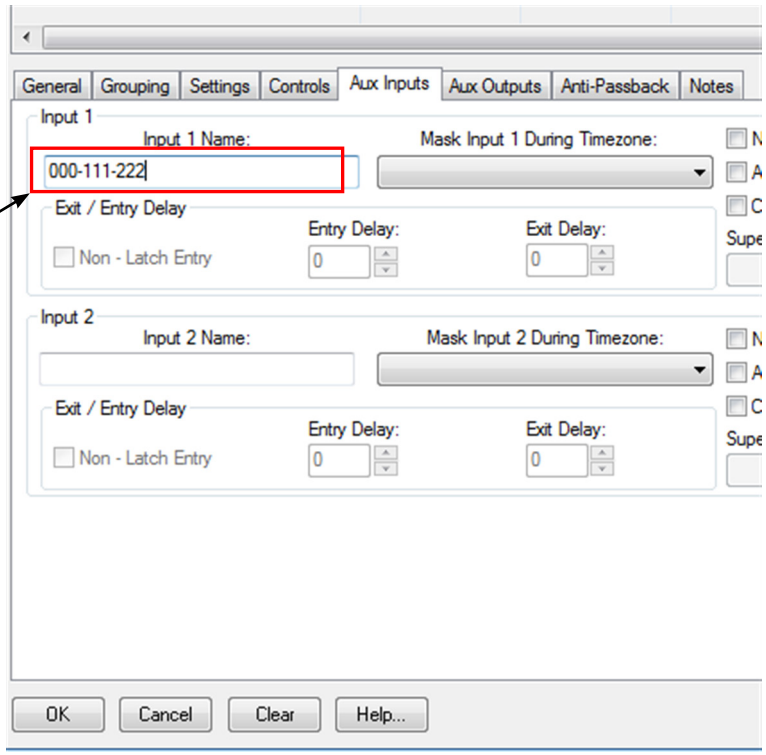
A Medeco XT eCylinder can be enrolled through OnGuard's System Administration 'Readers and Doors' in the same fashion as any other ASSA ABLOY IP lock.

The only requirement is that the cylinder identifier must follow this format '*###-###-###*' (9 digits separated by a dash in groups of 3):

Medeco Door/Opening Name



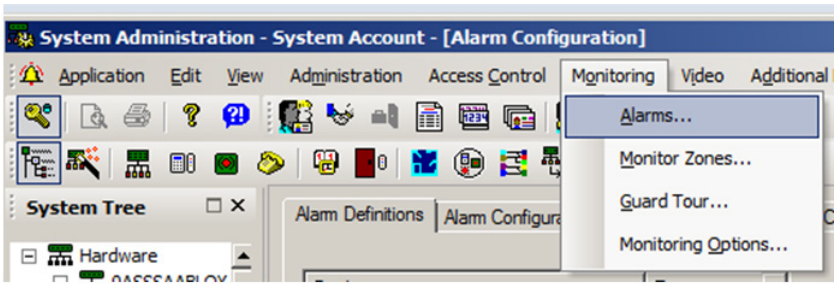
Medeco Cylinder Identifier (*###-###-###*)



Filtering Alarms and Events in OnGuard Alarm Monitor

OnGuard supports the ability to filter alarms and events from appearing in the Alarm Monitor. To filter specific alarms and events follow these steps:

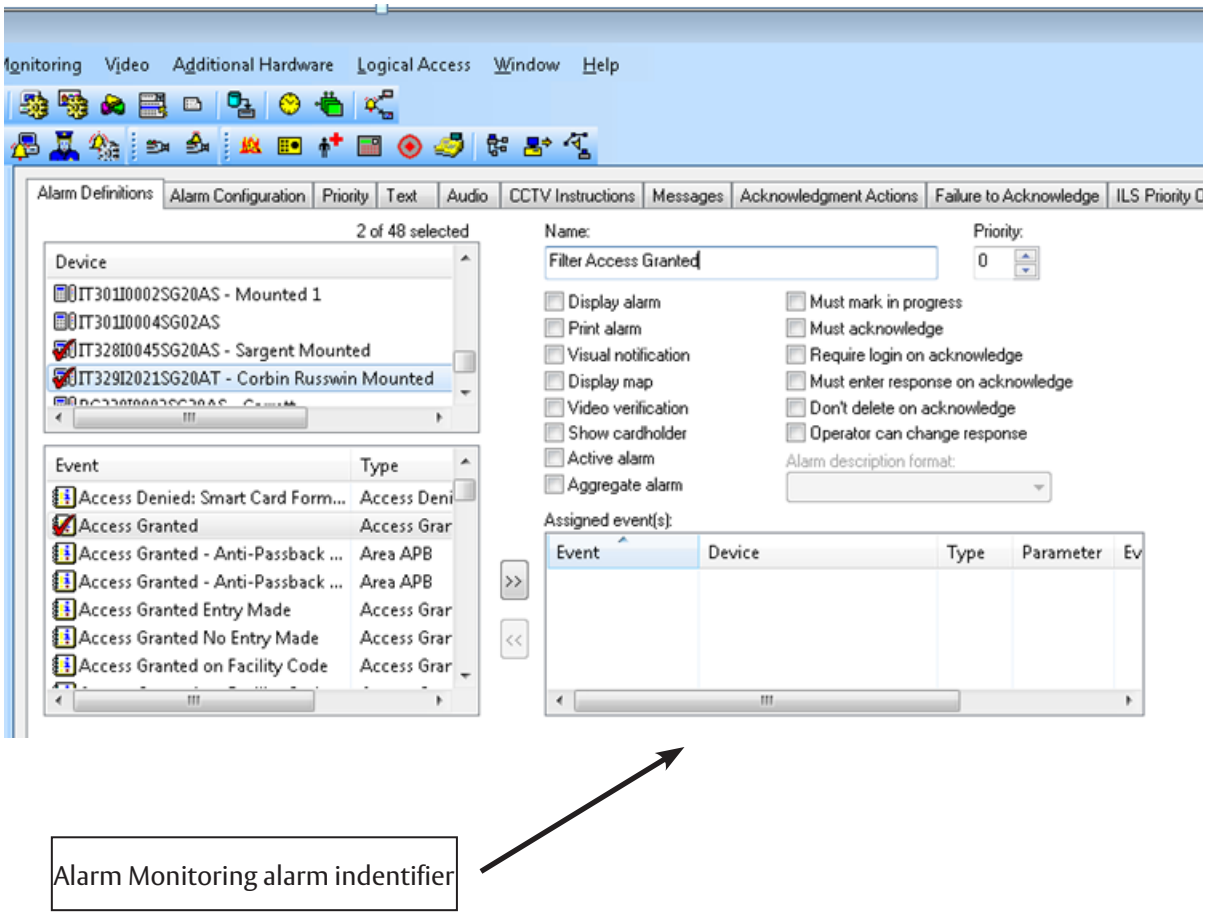
1. From OnGuard System Administration, click the "Monitoring" tab and select "Alarms ...".



2. In the Alarms Definitions tab, click on the "Add" button at the bottom of the screen; next select the Readers and Generic Event, uncheck the Display Alarm checkbox, and enter the name for the filter:

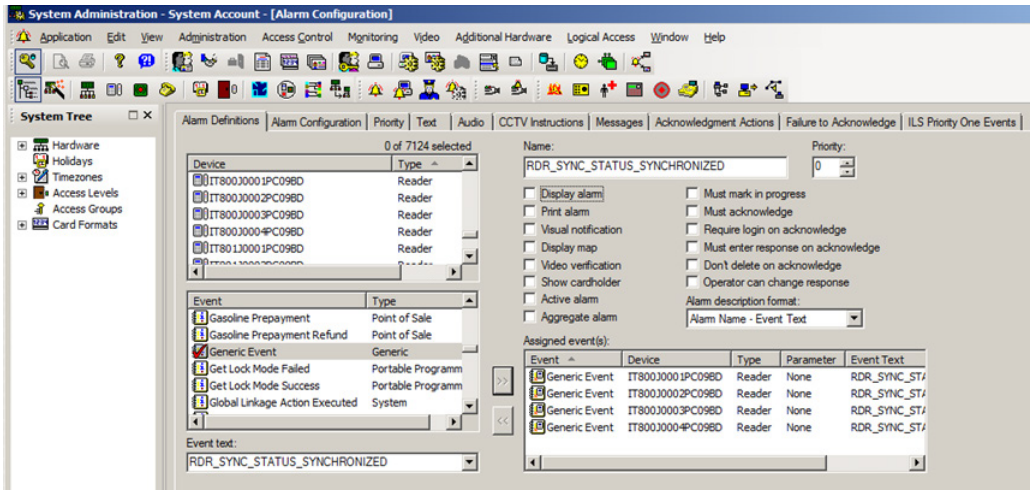
   A. Built-In Event:

   Select the built-in Event (ex. Access Denied)



Alarm Monitoring alarm indentifier

3. Assign the alarm/event to be filtered and choose 'Alarm Name – Event Text' in the Alarm description format dropdown and push the Ok button to add the filter:

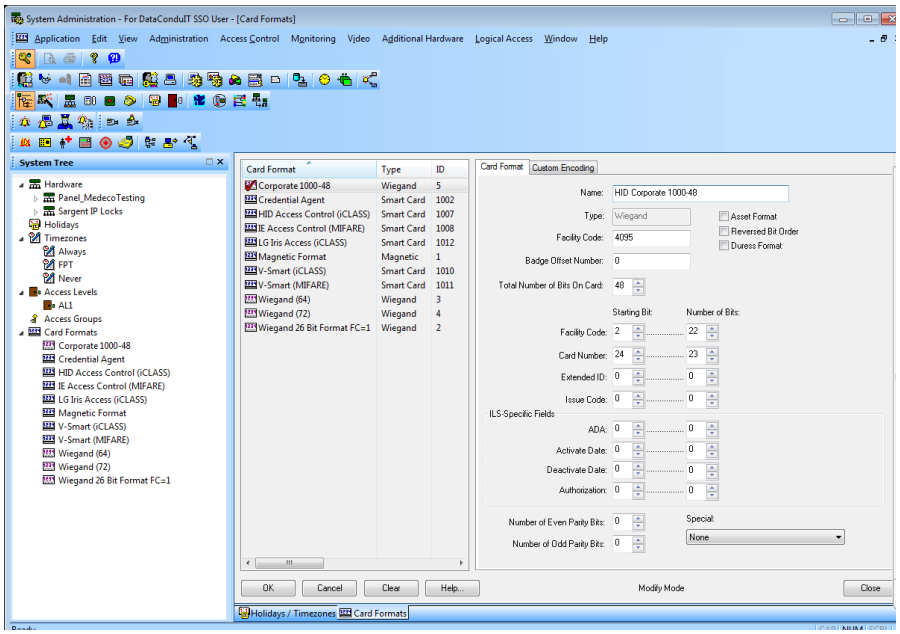


HID Corporate 1000-48 Card Format

HID Corporate 1000-48 card format is a new 48 bit Wiegand card format developed by HID.

Creating A Standard HID Corporate 1000-48 Card Format

Create a 48 bit Wiegand card format as specified below:



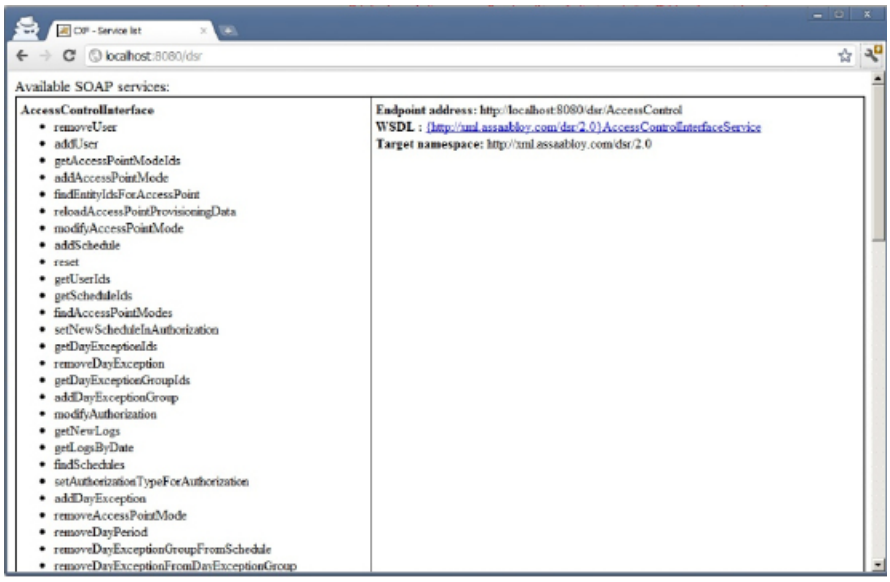
Limitations

- 48 bits Weigand cards associated to this card format will be formatted as HID Standard Corporate 1000-48.

  Any deviation from this specification will result in a 48 bit Weigand card format.

Troubleshooting/ Install Configuration

1. OPEN Browser on DSR hardware.
2. Navigate to <DSR Machine IP>: 8080/DSR.



If you can not reach this page from both the DSR machine and EAC host:

- Confirm DSR service is started.
- Confirm Windows firewall on DSR and SQL machines are turned off or have exceptions for Ports 8080 & 8731.

If DSR service is started but no webpage, confirm:

- SQL service is running
- Start > Programs > SQL Server > Configuration
    - Confirm named PIPES and TCP/IP protocols are active
- Restart Apache Tomcat DSR service

Notes

ASSA ABLOY

ASSA ABLOY Americas
110 Sargent Drive
New Haven, CT 06511
800-377-3948
www.intelligentopenings.com