ASSA ABLOY WiFi/POE Intelligent Lockset
Application Note

This Application Note is a guide for deploying Doors.NET software with ASSA ABLOY WiFi Sargent locksets. These locksets are fully intelligent and are of a “offline” nature. This means the locksets are NOT communicating with any software about 99.5% of the time. They are only on the network for brief periods, and as such, override commands such as door unlock, lock, temp unlock, and Global Lock/Unlock will NOT function with these locksets. In addition, configuration changes of the lockset itself, cardholders, schedules, etc. are NOT sent immediately to the lockset. Changes are made only when the lockset wakes up and starts communication. The lockset can be configured to wake up on a schedule, a specified event (such as door forced, door held, access denied, etc.), a designated user (known as a Comm User), or by pushing the white button underneath the RJ11 jack on the back of the lockset.

A summary of the setup process is listed below with details for each step following.

1. Install Doors.NET with the correct software options and license, and activate the license.
2. Configure the lockset definition file (.slct extension) to access the network using the Network Configuration Tool (NCT) from ASSA ABLOY.
3. Use the Lockset Configuration Tool (LCT) from ASSA ABLOY to configure the lockset by downloading the .slct file to the lockset. This is done from a serial port on any PC to the RJ11 jack on the back of the lockset. A serial cable is provided by ASSA ABLOY for this task.
4. Use LCT to verify communication to the AMT services. If communication is not established, then troubleshoot the network at this point. Do NOT call Keri tech support for this, call ASSA ABLOY tech support at 1-800-481-8464 x4209.
5. Perform a communication session from the lockset. This will add the lockset to the AHG420 database in the Locksets table.
6. In the Doors.NET software, select the ASSA Gateway in Hardware Setup and click Autoconfig. This adds any new locksets to Doors.NET. You will need to change the Accepted Property from No to Yes in order for the lockset to communicate on the next session.
7. Configure the contact schedules or alarm configuration that control when the lockset is to initiate a communication session.
8. Add the lockset to access groups as with any hardware.
9. Enroll cards and configure cardholders.
10. When you have configured cardholders, schedules, access groups, etc., perform a communication session so the lockset can obtain the updated configuration.

1.0 Install Doors.NET

You must install Doors.NET v3.5.1.15 or greater.

- Start the installation program.
- Choose Custom setup.
- At a minimum you must select Application Server and Gateway - ASSA ABLOY and a administrative client. You can install other software options but those are not required for ASSA ABLOY operation. You do NOT need to install the NXT, PXL, or MSC gateways as physical hardware (i.e. NXT controllers, NXT(MSC)) is NOT required to communicate with the locksets.

NOTE: The Doors.NET Gateway - ASSA does not communicate directly with the IP locksets. It is a database driver that links the operational database for the locksets (AHG420 database and OF_Transactions database) with the Doors.NET database.

2.0 Configure the Lock Set Definition File

You must have v2.2 or greater of the LCT/NCT software from ASSA ABLOY. Keri does NOT provide this software. Integrators installing these locksets MUST be certified by ASSA ABLOY and should already have the software and know how to configure the locksets for their network.

The steps for the LCT and NCT are for reference only as these are NOT software from Keri.

ftp://keri+assaabloysdk.com:keri@ftp.assaabloysdk.com

In this directory should be the LCT/NCT installer. This updates frequently so always check to see if you have the latest.

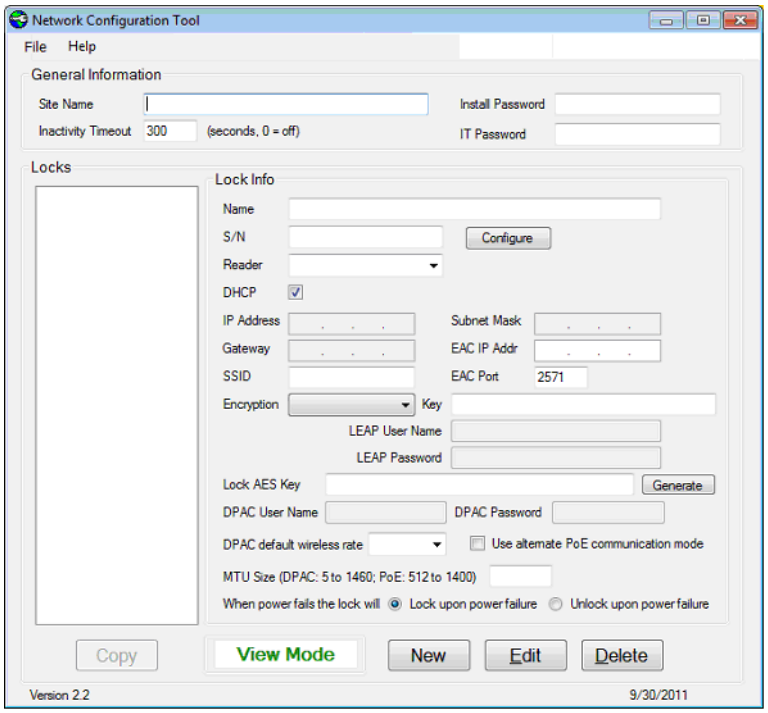
/DEVICES/IP_LOCKSET_TOOLS_AND_DATA/LCT_NCT/

There is also a wiki page available at www.ahgatlanta.com/wiki

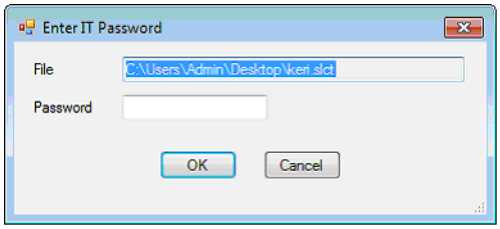
There are two requirements to meet before starting this process:

1. The Gateway PC must be on a static IP.
2. You must know your SSID (Service Set Identifier) and associated encryption keys. You may need to contact the IT department for this information as it may be hidden. This is the name of the 802.11 wireless access point to which the locksets will connect in order to obtain their IP address.

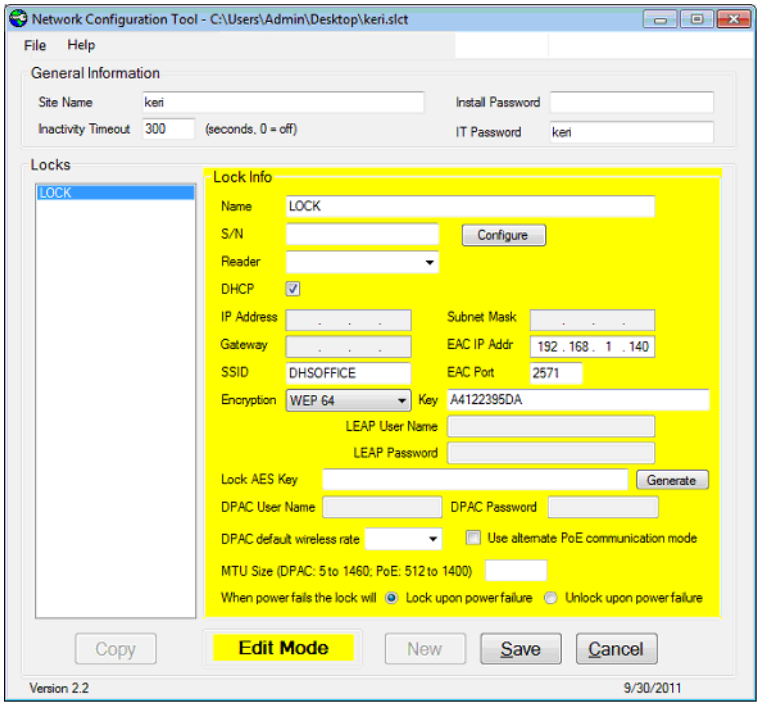
Start the NCT program. The default screen for NCT is shown below.



Choose File then open an existing .slct file or create a new one.



Enter the IT password to access the configuration parameters contained in the .slct file. Click OK.

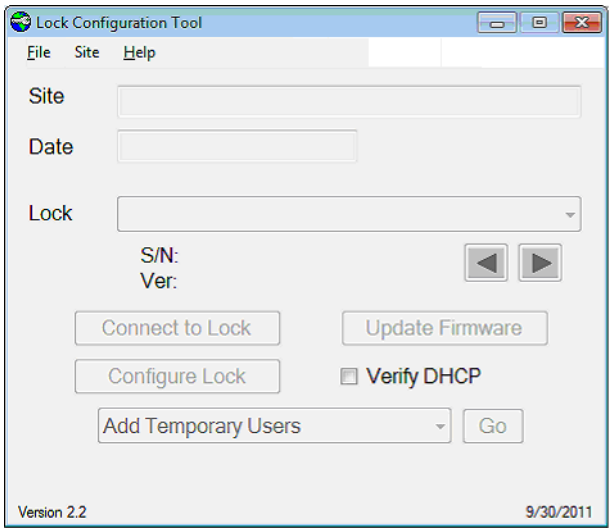


Click Edit to enter edit mode. Background will turn yellow indicating you are in edit mode.

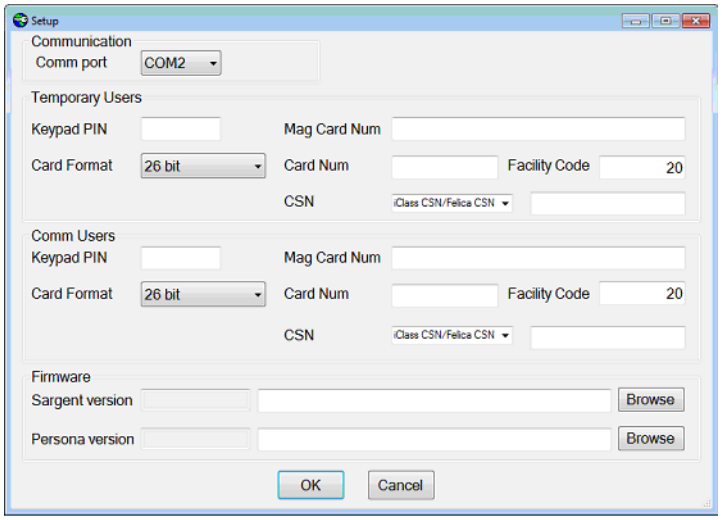
1. Enter a Name for this lock wireless network configuration.
2. Enter the SSID.
3. Choose the Encryption that the access point uses and enter the encryption key.
4. Enter the EAC IP Address. This is the STATIC IP Address where the AMT OpenFoundation and Doors.NET Gateway - Assa are installed. THIS MUST BE A STATIC IP ADDRESS AS THIS IS THE IP ADDRESS TO WHICH THE LOCKSET WILL TRY TO COMMUNICATE ONCE IT OBTAINS AN IP ADDRESS FROM THE WIRELESS ACCESS POINT.
5. Click Save and exit the program. Keep track of where you have saved the .slct file as you will need it for the LCT program.

3.0 Configure the Lockset with the Lockset Configuration Tool

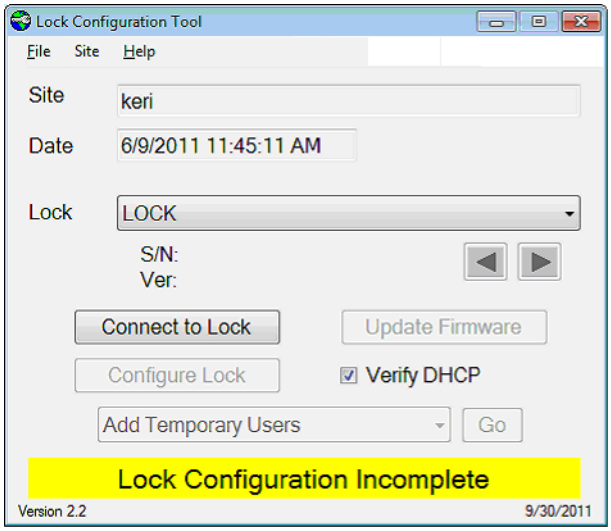
Start the LCT program.



Choose File > Setup to configure serial port, temporary users (useful for construction mode), Comm User, or update the firmware in the lockset.



If you have a lockset with keypad, enter a simple PIN under the Comm Users. A Comm User is only used to initiate a communication session and does not unlock the door. You can also use a card provided you know the format, card number, and facility code.
Click OK to save the setup information.



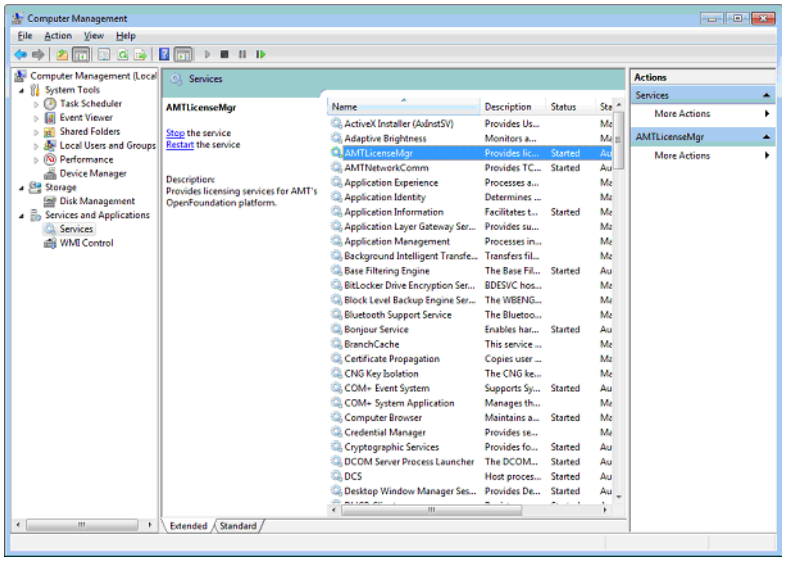
After configuring the setup for LCT, choose File > Open and select the .slct file created by the NCT program. Click the Connect to Lock button. This will send the configuration to the lockset over the serial link. Typically, this takes about 5 minutes to complete.

4.0 Verify Communication to the AMT Services

Once you have the confirmation that configuration is complete, choose Verify Connection To Host from the drop-down menu and click Go. This will cause the lockset to use the .slct configuration and attempt communication to the Host. If this part is not successful, then you need to troubleshoot the network, firewalls, check services are running, etc. These checks are all basic troubleshooting and at this point Doors.NET software is not involved at all. The default incoming TCP port is 2571 and the outgoing TCP port is 8023. The Doors.NET installer should have already allowed these ports through the Windows firewall. If you are using a third party firewall (i.e TrendNET, Eset, Norton, etc.) you will have to manually add these exceptions through their software.

5.0 Add the Lockset to the AGH420 Database

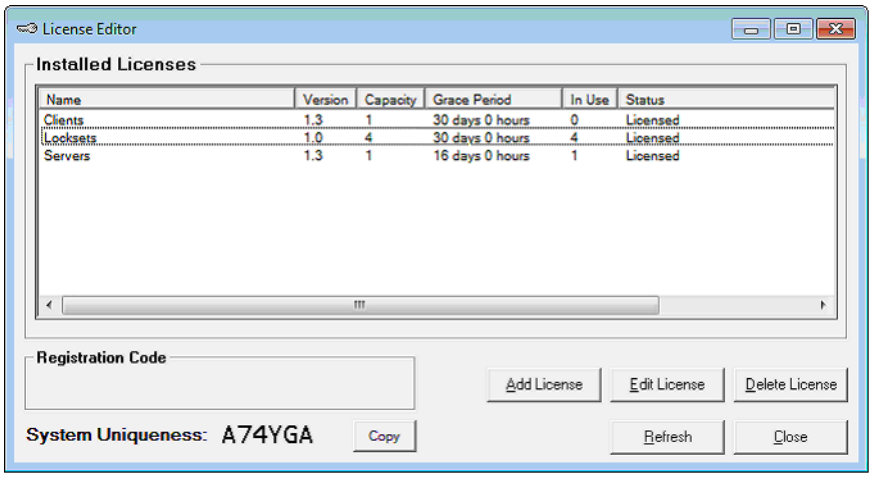
The services responsible for communicating with the locksets are AMTLicenseMgr, AMTNetworkComm, and DCS. Ensure that these services are running. These services are installed by the AHG420Setup.exe (an ASSA ABLOY product) that is run silently from the Doors.NET installer when the Assa Gateway option is selected. That file should be located in the Doors.NET directory. There should not be a reason to manually run this file again (as the software should already be installed) but can be used to verify where the services have been installed, database configuration, etc. Each of those options in the AHG420 installer are set automatically by the Doors.NET installer.



The Doors.NET Installer should have shown a warning message about licensing the ASSA product. This is a separate license issued by ASSA. Without activating the ASSA license, the AMT services will shutdown in 14 days from install. The default location of the License Editor is:

C:\Program Files\AHG420 Driver\bin on 32-bit machines
C:\Program Files (x86)\AHG420 Driver\bin on 64-bit machines

You will need to take a screen shot of the License Editor.



E-mail that screen shot.

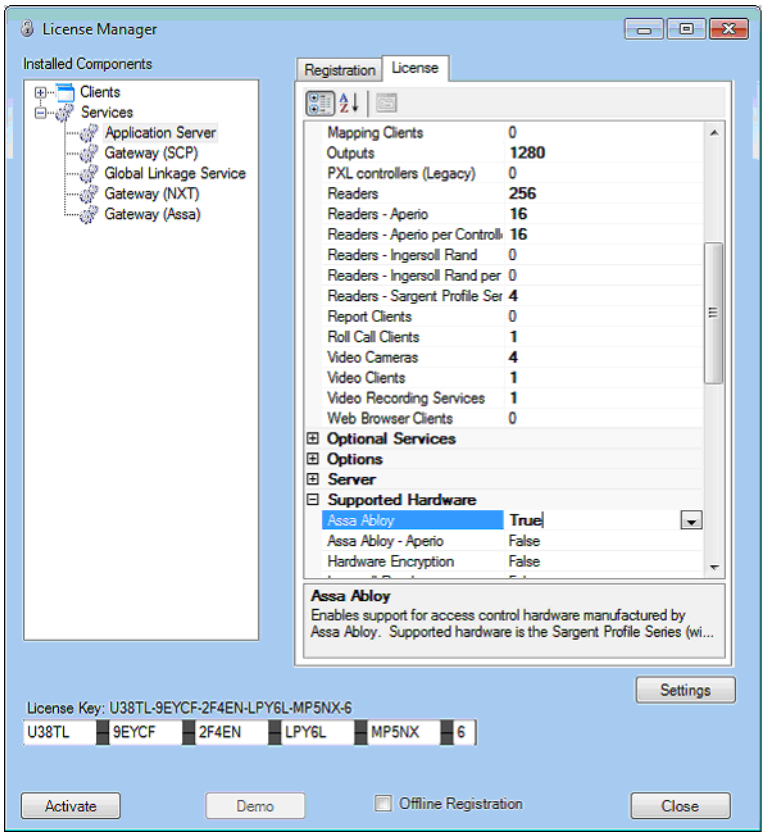
to: regcodes@amt-us.com
cc: oemsupport@assaabloyusa.com
Subject: License Request
Body: I am with Keri Systems and I need a license for XX locks.
The return e-mail with the license codes will usually arrive in about an hour but could be the next day.
The e-mail should appear similar to the below information.

AMT's RegCode Notification			
This is an automated response from AMT's RegCode System. We have received your RegCode request and have assigned it the **Support Case RegCodes-####**			
If you need to update the request before you are contacted, you can update this request by replying to this email. **Do not modify the ID in the subject line.**			
License Request			
[admin - date/time stamp]			
Uniqueness:	ID Number		**REGISTER SERVER FIRST**
Feature	**Capacity**	**Grace Period**	**Reg Code**
Servers	1	104 Days	<CODE IS 29 CHARACTERS LONG>
Clients	1	104 Days	<CODE IS 29 CHARACTERS LONG>
Cameras	0	104 Days	<CODE IS 29 CHARACTERS LONG>
Edge Readers	0	104 Days	<CODE IS 29 CHARACTERS LONG>
LockSets	2	104 Days	<CODE IS 29 CHARACTERS LONG>
VertX Vx00 units	0	104 Days	<CODE IS 29 CHARACTERS LONG>
Please go to this link for complete directions on obtaining and applying registration codes.			
http://support.amt-us.com/amtdn/index.html?how_to_obtain_and_apply_regist.htm			
Note: You can copy each registration code above and paste it in to the 'Edit' screen for each feature by double-clicking the desired feature in the License Editor. The paste button will be enabled when the correct number of characters is in the clipboard.			

6.0 Add the New Lockset to Doors.NET

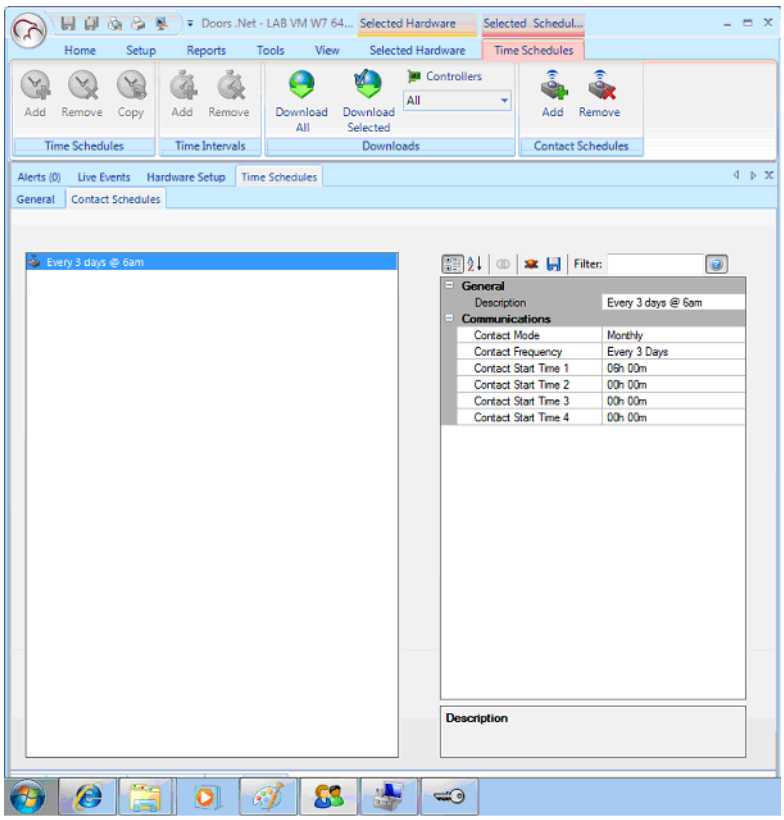
The Doors.NET license needs to be configured as follows:

- Supported Hardware/Assa Abloy = True
- Readers - Sargent Profile Series = the number of locksets for which you have paid
- Gateways - there may be an additional license fee for this if there are other hardware gateways installed as the Assa gateway does count against the number of gateways in the license.

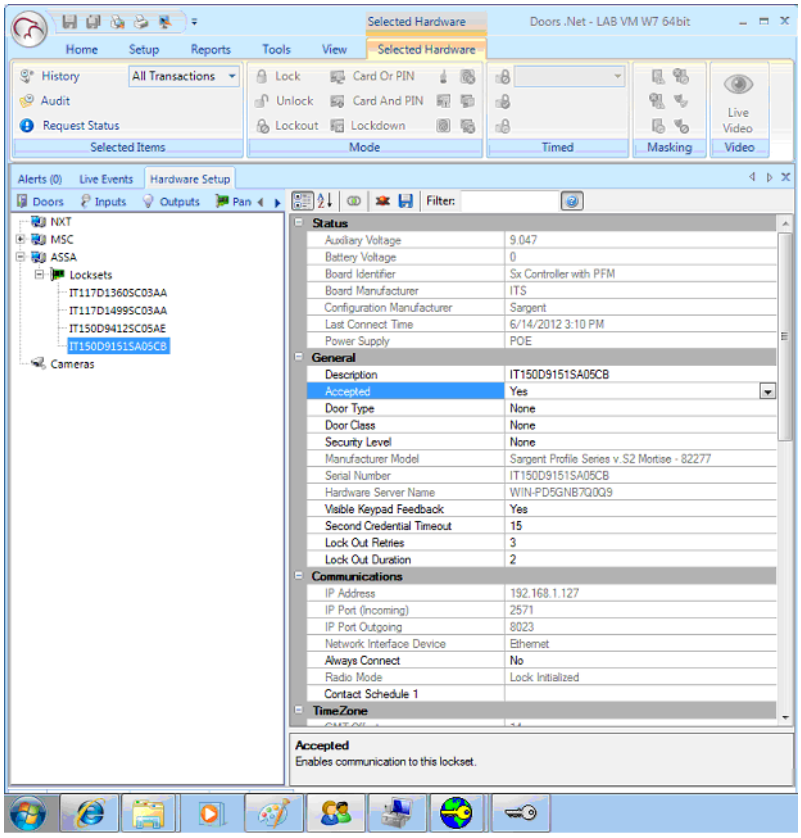


7.0 Configure the Contact Schedules or Alarm Configuration

On the same screen where you setup Time schedules, a second tab shows the contact schedules. This is where you can define the different times of day/week/month that can be assigned to a lockset. The property on the lockset is “Contact Schedule.”



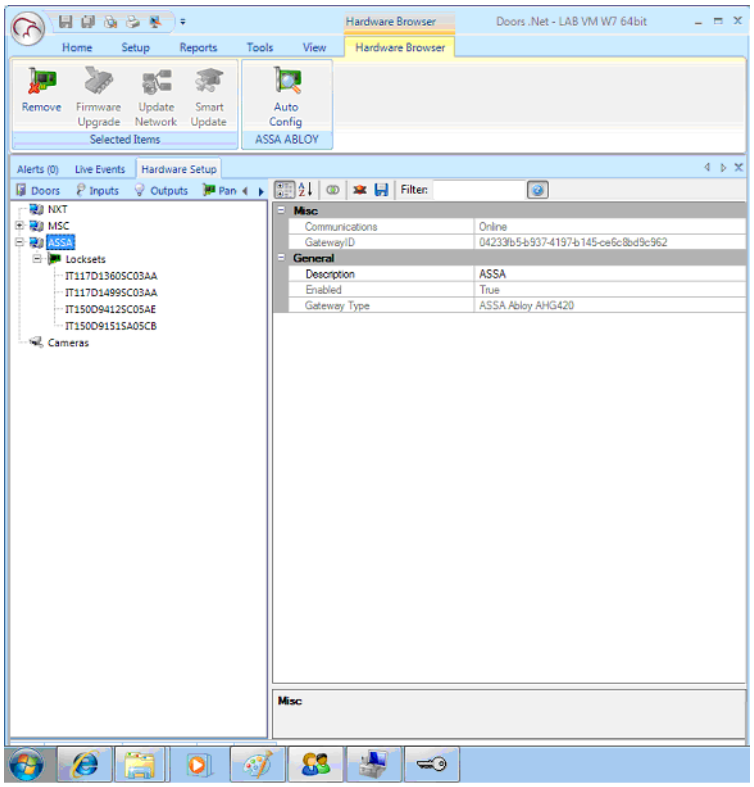
When a new lockset is added (either an Autoconfig on the gateway or the gateway has restarted), it will be defaulted with Accepted set to **No**. You MUST change this to **Yes** in order for anything to be sent to or from that lockset.



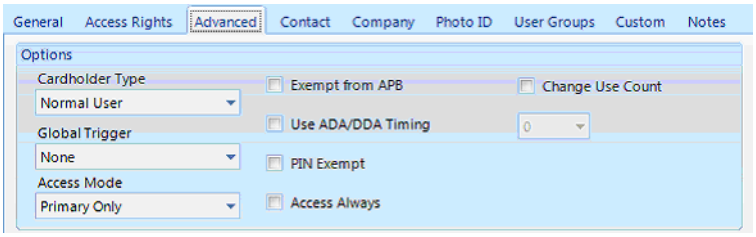
You should also configure the contact schedule for the lockset to call in. Normally, this would be about once a week to report transactions. However, during initial commissioning when you expect to be adding cardholders frequently, set the Alarm Configuration/Access Denied to Enabled when secure. That will cause the lockset to wake up on any Access Denied and report it and at the same time update the configuration.

8.0 Add the Lockset to Access Groups

If you have added locksets via the LCT tool and performed a communication from the lockset (push the button, comm user, etc) then the lockset should be in the AHG420 database in the Locksets table. That does NOT mean it is in the Doors.NET database. Part of the Gateway Assa start procedure is to verify what is in the AHG420 database and what is configured in the Doors.NET database. The gateway will add locksets that are in the AHG420 database that are not present in the Doors.NET database. It does this automatically and can be configured to behave in this way while it is running (thus avoiding a restart of the gateway service). By selecting the Gateway in the Hardware Setup screen and clicking the Autoconfig button, any new locksets will be added automatically. You can do this one at a time or add all the locksets and click Autoconfig once to grab them all.



9.0 Enroll Cards and Configure Cardholders



There are additional options under the Advanced tab that pertain to the locksets only.

These options are:

Cardholder Type – Now expanded to include all of the different types supported by the lockset. If you are using this with NXT hardware, be careful as NXT only supports Normal and Extended.

Access Mode – This defines the access mode for the cardholder NOT the lockset. If you want the cardholder to be able to use a PIN, then select either “Primary or Secondary” or “Primary then Secondary.” The lockset will NOT accept a cardholder if you define either of these without assigning a PIN. The UI should warn you about this condition. Note that this is backwards from traditional access control where we define the door portal to be in a certain mode (i.e., dual verification on a schedule) where the controller requires all cardholders to present both credentials.
The locksets operate in a mode where the cardholder is required to present credentials based on this setting so you can have some cardholders requiring both and other cardholders just a card. This cannot be scheduled to change at the lockset like we can on all other hardware.

Access Always – This check box basically overrides all the access rights and tells the lockset to always allow this cardholder.

Limitations:

- Only 2,400 cards can be sent to a lockset. The gateway will return a NAK if the configured cardholder access rights exceed 2,400.
- Testing has shown the locksets start to run low on battery power after about 600 communication sessions. Be careful when configuring when you want the lockset to call in.
- If you are mixing hardware (i.e. NXT hardware and Wifi locksets) and are using a card format other than Wiegand 26-bit, you will need to enter two cardnumbers for each cardholder. The first cardnumber for NXT will be the value of all of the bits on the card. The second will be the value of the cardnumber as defined by the card format assigned to that card. This may or may not be the imprint number. If you are using NXT(MSC), there is a good chance that both can use the same number as NXT(MSC) supports card formatting.

10.0 Update the Lockset’s Configuration

Finally you must wake up the lockset to start communication and upload the final changes to configuration information. Since the schedule, specified event, and Comm User information probably are not in the lockset yet, you will likely need to perform this update by pressing the white button underneath the RJ11 jack on the back of the lockset.

11.0 Contact Keri Systems

Keri USA	Keri UK, Ireland, Europe
2305 Bering Drive San Jose, CA 95131	Unit 17 Park Farm Industrial Estate Ermine Street Buntingford Herts SG9 9AZ UK
Telephone: (800) 260-5265 (408) 435-8400	Telephone: + 44 (0) 1763 273 243
Fax: (408) 577-1792	Fax: + 44 (0) 1763 274 106
Web: www.kerisys.com	Web: www.kerisystems.co.uk
E-mail: sales@kerisys.com techsupport@kerisys.com	E-mail: sales@kerisystems.co.uk tech-support@kerisystems.co.uk

end of document