Allegion No Tour

Using Visual Doors
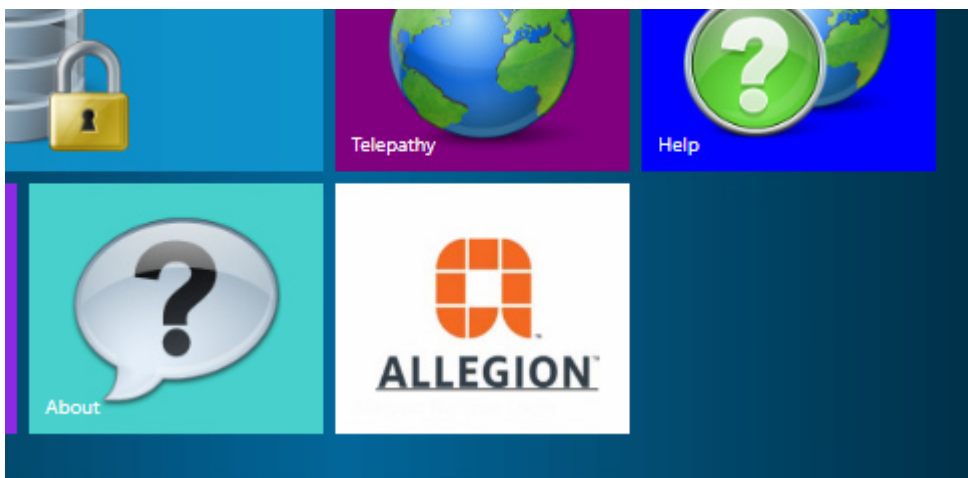
Table of Contents

P/N: 02323-001 Rev A

1.0   Introduction

This document explains how to use the Allegion No Tour feature in Visual Doors. Credentials are enrolled and updated using the MT20W USB enrollment reader. Following enrollment, the access rights information is written to the card and then subsequently written to the locks upon first presentation to the card reader.

IMPORTANT NOTES:

- Visual Doors in ONLY used for cardholder enrollment and administration. Setting up and creating access groups is performed using the Aetheros Web Portal (http://allegion.aetheros.net). This document assumes that you will already have an Allegion Aetheros site created with your locks added and ready to use.
- Allegion Aetheros requires the host PC to have an active, unrestricted internet connection (as you are required to log into your Allegion account which is hosted in The Cloud).

## Allegion Administrative Tasks Supported in Visual Doors:

- Enrolling new No Tour credentials
- Assigning Access Rights
- Deleting Credentials
- Replacing Credentials
- Change Credentials to Temporary

This setup guide assumes that you have an existing Allegion Aetheros system setup and configured using the Allegion ENGAGE app and the Aetheros Web Portal. The guide also assumes that you have used the Web Portal (allegion.aetheros.net) to setup access groups. Once the Allegion Aetheros system has been setup you can administer and enroll No Tour cardholders from Virtually any PC that has Visual Doors installed.

2.0 Licensing Requirements

Allegion No Tour is a licensed feature and therefore must be enabled on your Doors.NET license. To check your license has Allegion No Tour enabled, perform the following steps:

1. From Windows Start menu, go to Doors.NET >> License Manager.
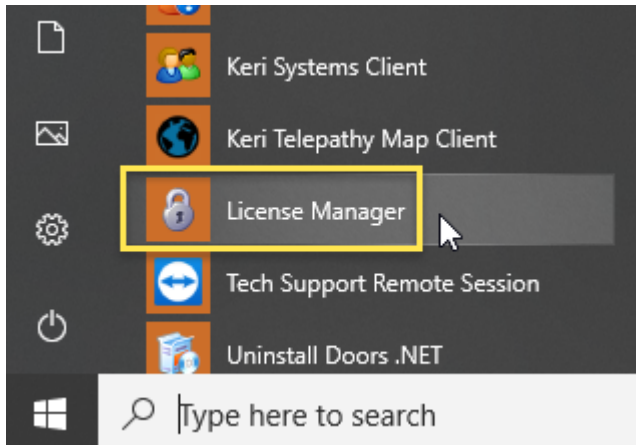
2. When the License Manager window opens, select Application Server from the list on the left.
3. Click on the License tab and the list of licensed features and components will be displayed.
4. Scroll down the list and locate: Supported Hardware >> **Aetheros Allegion No-Tour** - Ensure this is set to True *(as highlighted)*.

5. If No Tour is enabled you can close the License Manager window.

If No Tour is set to False you will need to contact Keri Systems inside sales.

3.0   System Requirements

- A supported Windows PC with Doors.NET v4.0.3.4 installed.
- A supported smart device (Android or iOS) with the Allegion ENGAGE app installed (this app is initially used for capturing your Control, NDE or LE locks and the MT20W USB enrollment reader) and also the Keri Mobile app installed (this app is used to send certain updates out to the locks - for example: new access groups and access group changes).
- A registered Allegion partner account.
- Partner account site should be registered and setup at www.allegion.aetheros.net
- Schlage Control, LE or NDE locks.

  Note: No Tour is supported on any NDE lock manufactured after February 2016 (with firmware 02.10.08).

- An MT20W USB Enrollment reader.

4.0   Log in to the Visual Doors Software

Visual Doors software is automatically installed when you install the Doors.NET (v4.0.3.4) software. If selected during install, you will have Visual Doors Desktop and Start menu shortcuts:

(or you can access Visual Doors from the following location on the host PC C:\Keri\DoorsNET\Visual Doors.exe

1. Double-click the Visual Doors icon to open the login window.
2. Enter the username and password (the default for both is **admin**).
3. Click on the small white cog if you need to specify a remote IP address for the Application Server.
4. Click the LOGIN button.
5. Visual Doors will open and you will see the homescreen.
6. You should see the Allegion tile.
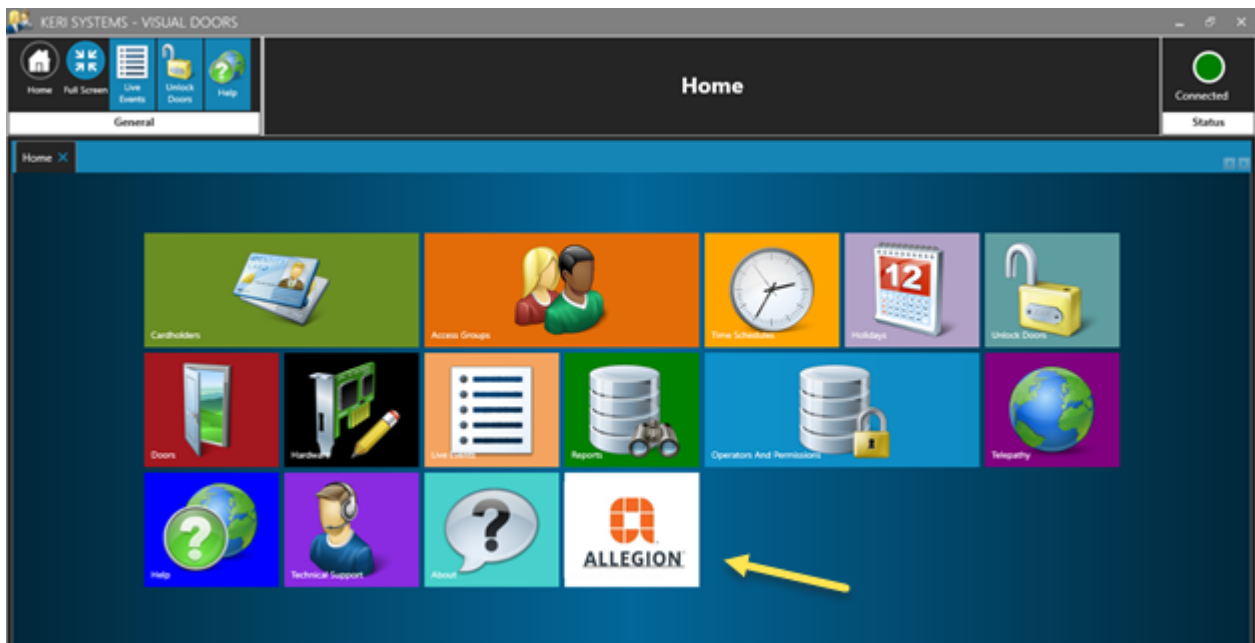
You are now ready to start enrolling new No Tour credentials.

5.0 No Tour Credential Enrollment

Note: Visual Doors client is only used for enrolling and administering No Tour credentials. It is NOT used for setting up or modifying access groups. Access groups are created and edited using the Web Portal (www.allegion.aetheros.net) and access group updates are sent to the locks using the Keri Mobile app.

1. Click on the Allegion tile to open the Allegion log in window.
2. Log into Visual Doors with your Allegion ENGAGE user name and password.
3. Ensure your MT20W USB enrollment reader is connected to the PC and displaying a solid blue LED (indicating that the reader is connected via Wi-Fi).

4. The Cardholders screen will appear.
5. Click the green Add icon.
6. Enter a first name and a last name for the new record.
7. Enter an e-mail address for the new record.
8. Enter a location for the new cardholder (for example: work location).
9. Select if the cardholder will never expire or if it will expire at the end of the day.
10. Click the ADD button to create the new cardholder record.
11. Place the No Tour credential onto the USB enrollment reader - the LED will go green and the reader will beep every few seconds.
12. Click the ADD CREDENTIAL button and the card number will appear in the **Choose credential** box (you may see multiple card numbers).

13. Select the correct card number.
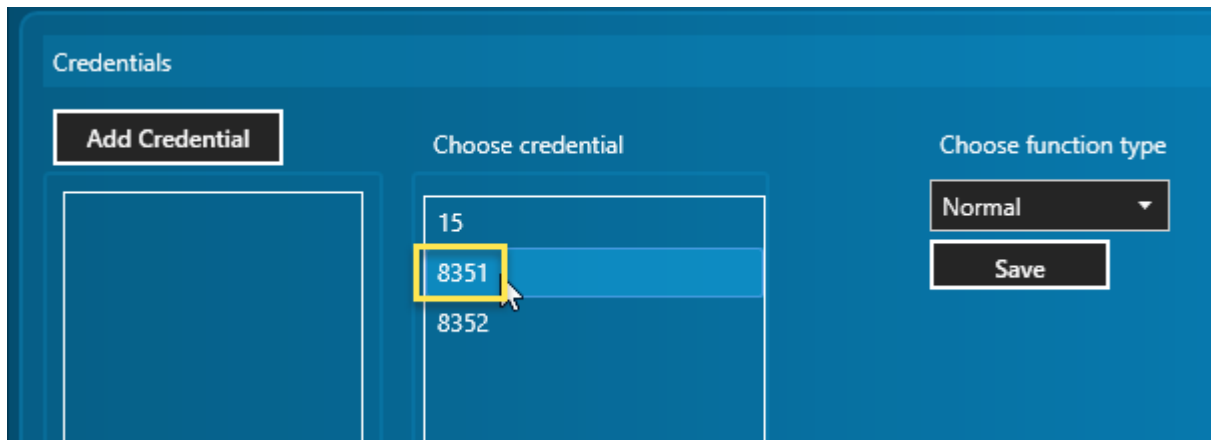
14. Click the SAVE button.
15. Go to the Access Rights tab and click the ASSIGN ACCESS button.
16. Select a doors/locks that the cardholder will have access to.
17. Select a time schedule to associate with the locks (to determine when the card-holder will be able to gain access).
18. Click the SAVE button.
19. Repeat steps 16-18 for any additional doors that the cardholder will have access to.
20. Wait for the MT20W USB Enrollment reader to beep three times.
21. The No Tour credential will be programmed with the access rights.
22. You will now be able to gain access with the card.

Notes:

- Cardholders that are set to 'Expire Daily' will have to be re-enabled at the beginning of each new day. The are re-enabled by presenting the card again to the USB enroll-ment reader.
- The One-Time Use setting is NOT supported on the Control locks. If a credential is set to One-Time Use it will get access denied on the Control locks.

6.0 Credential Function Types

There are several credential function types to choose from:

- **Normal** - Unlocks the lock momentarily (with specified relock delay period).
- **Toggle** - Changes the state of the lock from locked to unlocked, or vice versa.
- **Freeze** - Freezes the lock in the current state. Lock remains frozen until Freeze credential is presented again. Disables all other credentials except for Pass Through.
- **One Time Use** - Allows only one Normal access per assigned lock. "One Time Use" function only works on NDE/LE devices.
- **Pass Through** - Unlocks a lock momentarily, regardless of state. Overrides a lock in Freeze and Lock Down states.
- **Lock Down** - Changes the state of the lock to locked and disables all credentials except for Pass Through and Freeze. Present a Freeze to return lock to normal state.
- **Block** Denies access to the lock and records the access attempt as an audit.

7.0 Removing and De-activating Credentials

The following steps explain how to edit and administer No Tour credentials in Visual Doors: This section assumes you have connected the USB enrollment reader to the host PC and the reader should be displaying a solid blue LED.

7.1 Delete a Credential

Deleting a credential will immediately remove the credential from any lock that the credential was added to.

1. Select a cardholder from the list on the left.
2. On the cardholder's General tab select the credential that you wish to delete.
3. Click the DELETE CREDENTIAL button. The credential will immediately disappear.
4. Press the credential to the MT20W until the reader beeps 3 times.
5. The card will now be updated and will no longer be able to gain access.

7.2 Delete a Cardholder

Deleting an Allegion cardholder from Visual Doors will completely remove the card from the software and also from the locks that the cardholder had access to:

1. From the cardholder list, select a cardholder.
2. Click the large red DELETE icon then click the small black DELETE button.
3. Present the credential to the reader to remove the programmed access rights.
4. Wait for the reader to beep 3 times.
5. Remove the credential from the MT20W reader and it will now not be able to gain access at any of the locks.

7.3   Replace a Credential

Replacing a credential will program the same access rights as the previously enrolled card. Upon presentation of the replacement card the old card will be de-activated and the replacement card will be activated.

1. Select a cardholder from the list on the left.
2. Click the ADD CREDENTIAL button.
3. Present the replacement credential to the MT20W reader.
4. The replacement card number will appear in the Choose credential box.
5. Select the new credential number.
6. Click the REPLACE CREDENTIAL button.
7. The old credential will be deleted.
8. The new credential will need to be presented to the MT20W for the access rights to be written to it.
9. Wait for the MT20W to beep 3 times. The credential will then be programmed.

8.0   Assigning and Unassigning Access Rights

Notes regarding No Tour access rights:

- There are two methods of assigning access to cardholders, either 'Individual Access' or 'Group Access'. With Group Access, doors are assigned to access groups and these access groups are then assigned to cardholders. With Individual Access, the access rights are assigned directly to each lock (you simply select which locks the cardholder will have access to. A cardholder can use one of these methods. You cannot have a system that uses both Individual Access and Group Access.

- When you remove or disable a cardholders access rights you will have to physically visit the individual locks and update them via Bluetooth using the Mobile app. To immediately de-activate a cardholder you have the option of deleting the assigned credential - once the credential is updated using the MT20W it will be immediately removed from the locks upon the next card presentation.

- When a cardholder is assigned an access group and you go to tab "Access Rights", you can see the list of devices that are assigned to that group, but you can not assign new devices to the user because the cardholder is assigned a group.

- If the cardholder is using 'individual access' then the ADD TO GROUP button will be greyed-out (because you cannot assign an access group to a cardholder that has individual access'

8.1   Assigning Individual Access

The following steps explain how to assign individual access to a cardholder.

1. From the Visual Doors home screen, click on the Cardholders tile.
2. Select a cardholder from the cardholder list on the left (or enroll a new card-holder).
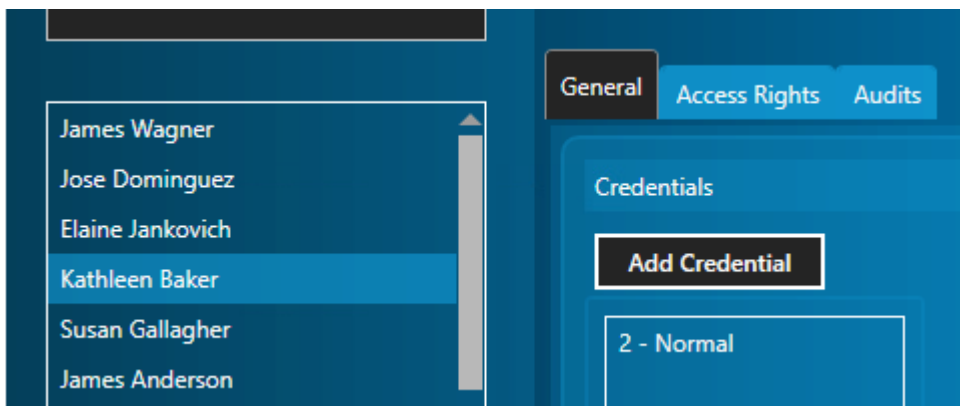
3. Select the cardholder's assigned credential.
4. Go to the Access Rights tab.
5. Click the ASSIGN ACCESS button.
6. The locks on the system will appear.
7. Select a lock that the cardholder will have access to, then select a valid time sched-ule.
8. Click the SAVE button to create the assignment (the lock and time schedule will appear in the **Available Access Rights** list.
9. Present the card to the MT20W enrollment reader and wait for the reader to beep three times.

8.2   Un-assigning Access Rights

If you un-assign access rights (you de-select a lock from the cardholder record) you will need to update the lock and there are three different ways that you can update the lock:

- Using the Keri Mobile App... *(see section 8.0)*
- If the lock is configured with a Wi-Fi connection, it has be scheduled for automatic updates... *(see section 9.0)*
- Linking the lock to a Gateway - Updates can be initiated directly from the Web Portal... *see section 10.0)*

9.0   Lock Updating Using the Keri Mobile App

Certain changes cannot be written to the credentials and so the lock will need to be updated manually. Changes such as removing access rights and deleting credentials will require a manual update. This section explains how to update the locks using the Keri Mobile App.

1. In Visual Doors, make a change, such as removing a cardholder's access rights (i.e. de-selecting a lock on the assign access rights screen).
2. Physically visit the lock that you unassigned and ensure you are within Bluetooth range of the lock.
3. Open the Aetheros Mobile App on your smart phone/device. Log in with your ENGAGE username and password.
4. Tap the site name. The app will then scan for locks on your site that are within range.
5. Any lock that requires an update will have an update indicator against it. As shown here:
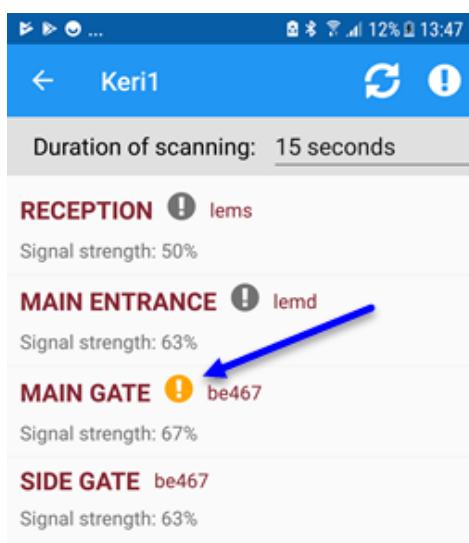
6. Tap on the lock name and the app will give you the options to either Unlock or Connect.
7. Select Connect.
8. The app will connect to the lock and once connected the current database information will be downloaded.
9. You can disconnect from the lock once the door settings screen appears - the disconnect icon is in the upper-right corner .
10. Once disconnected, the update indicator will have disappeared from the app and the card will no longer be able to gain access at that lock.

# 10.0 Lock Updating when the Lock is Connected via Wi-Fi

If the lock is setup with a Wi-Fi connections then you can configure the lock to be automatically updated twice each day. The following steps explain how to configure the lock in the Aetheros web portal to be updated at 9am and at 6pm. Setting the lock up with a Wi-Fi connection is covered in the Aetheros No Tour - Quick Start Guide.

1. In Visual Doors, make a change, such as removing a cardholder's access rights (i.e. de-selecting a lock on the assign access rights screen).
2. Go to the Aetheros Web Portal >> Devices >> Devices list - you will see that the lock has an update indicator against it.
3. From the **Action** drop-down list, select Edit to open the lock settings screen.
4. In the lower-right corner locate the Database download time settings.
5. For Option #1 set the time to 09:00am.
6. For Option #2 set the time to 06:00pm.
7. Click the SUBMIT button.
8. You will now need to update the lock using the Mobile app.
9. Once the update is completed, the lock will then receive a full database download at 9am and 6pm.
10. You can make as many changes as you wish… they will all be queued-up and sent at once during the scheduled download.
11. Following the schedule download the update indicator will disappear from the device screen of the web portal.

11.0 Lock Updating when the Lock is Connected to a Wi-Fi Gateway

Certain database changes will require a 'door file update', for example, changes to access rights or removing access rights from a cardholder. The following steps explain how to update the locks via the Gateway:

1. From the device list in the web portal, click on the Gateway entry.
2. Click on the Allegion Gateway.
3. The device screen will appear and the linked devices will be listed.
4. Use the drop-down list for a lock that requires an update.
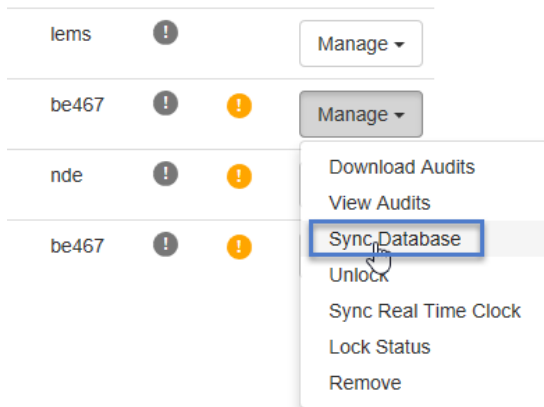
5. Select Sync Database from the list. Status indicators will inform you of when the update has completed.
6. Once update is complete the pending update indicator will disappear.

Contact Keri Systems

Keri USA	Keri UK, Ireland, Europe
302 Enzo Drive. Suite 190, San Jose, CA, 95138 USA	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

Knowledge Base Website - www.keri-kb.com

YouTube Channel - https://www.youtube.com/user/kerisystems

end of document

P/N: 02323-001 Rev A