Brivo Configuration Guide for Allegion Offline Locks

The Brivo and Allegion Offline Lock integration is a data on card topology, using Allegion No-Tour application. The locks do not communicate with either Brivo controllers or services. The cards contain all of the user's permissions. This guide will walk you through commissioning and configuring the Allegion Offline Locks for use with Brivo Access.

Introduction

Before You Begin

The Brivo Offline Lock integration with Allegion No-Tour supports a variety of Allegion Schlage locks. Make sure that you review the commissioning instructions for the lock model that you are installing. The following are the required parts and tools to successfully use the Allegion Control Lock with Brivo:

Integration Specifications

The Integration uses a connection between Brivo Access and Allegion Engage for lock management and credential assignment. The integration synchronizes the lock information on a Brivo Engage site inside the Engage platform and then interfaces with the MT20W to write Brivo Access permissions to a credential. Credentials used for the integration are minimum 8K Mifare Classic or MiFare DESFire EV3. MiFare DESFire EV3 is recommended for better credential security.

The following features are supported with the Brivo Offline Lock Integration:

- Up to 11 Devices or Device Groups assigned per credential
- Up to 400 locks per site (Recommended) (Unlimited per account)
- One MT20W required per site
- Adjustable unlock period for Credential Unlock
- Set Unlock period of 3 seconds for BMP Unlock

Parts Required

Supported Locks:

- XE360 (T/M/EW) Intelligent lock. (Brivo Part Number: ALGN-XE360-T/M/EW)
- FE410 Control Lock (Brivo Part Number: ALGN-CTRL-I Interconnected lock)
- BE467 Control Lock (Brivo Part Number: ALGN-CTRL-D Deadbolt lock)
- NDE
- LE

Credentials:

- Brivo BUC3 8K credentials
  - B-BUC3-SF25
  - B-BUC3-SC50
- Allegion smart credentials MiFare 1k byte or larger

Allegion MT20W (Minimum firmware version required - 39.02)

Brivo Access account with Brivo Account Config Tool access

Application Tools Required

Brivo Install Mobile Application (To set account information on locks)

Allegion Engage Mobile Application (For commissioning locks)

Allegion Engage Desktop Application (Used for MT20W in USB mode)

Glossary of Terms

The terms listed below will help you understand this guide better

ACT - Account Config Tool
BLE - Bluetooth Low Energy - Communication media used for application management of locks and for mobile credentialing
Brivo Access - Brivo's Access Control Management Platform
Offline - Does not communicate to Brivo Access Central or any other platform. Events and updates are done at the credential or via a **BLE** device.

Identifying Your Lock

If you are unsure of which lock model you are installing and configuring just by looking at it, use this section to help you identify the lock model. Although the commissioning and configuration of the locks are very similar, some locks have different features than others.

FE410

BE467

XE360

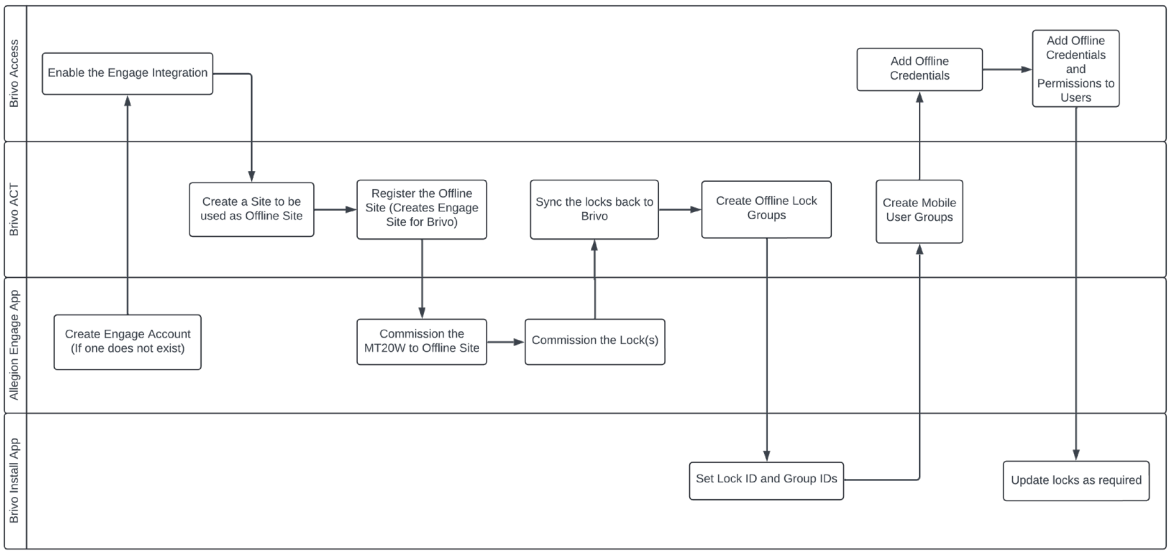
NDE (Coming Soon)

LE (Coming Soon)

IMPORTANT NOTE: If you are already familiar with this configuration process, but want to make sure you don't miss any steps, you may use the Control Lock Configuration walk-through below. For more detailed instructions on configuring Allegion Control Locks, begin with the Configurating the Brivo Offline Locks with Allegion section.

Configuring the Brivo Offline Locks with Allegion

There is a certain order to successfully configuring the Brivo and Allegion No-Tour integration. Deviating from this order may result in errors.



Consideration during Configuration

1. Ensure the correct control lock naming convention is agreed upon before starting.
    a. If the lock names need to be changed after the fact, then factory defaulting will need to be performed on all the locks and repeating the necessary steps below will be required.
2. If using the Allegion 9691T fob with Brivo Smart Readers, a High Frequency Disable Card is required. Brivo Readers are not compatible with the Allegion Smart 13.56Mhz format in the Allegion 9691T fob. This will eliminate a double read at each Brivo reader which results in one successful and one failed read. Be advised that this will make it so the doors using Brivo readers are only utilizing prox technology.
3. If using Brivo Unified Credentials, the ALGN-CFG-BUC (CE-052-861) Configuration card will need to be applied to all MT20Ws and locks.

Configuring Allegion Hardware

Physical Installation of Allegion Control Lock

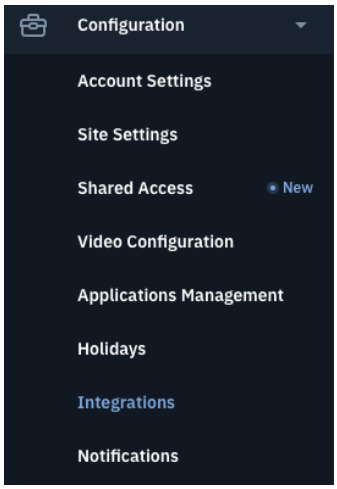
Follow Allegion's instructions to install the Control locks on the doors.

Enabling the Engage Integration in Brivo Access

NOTE: In order to complete this process, you must first download the Allegion Engage app from Google Play or Apple Store.

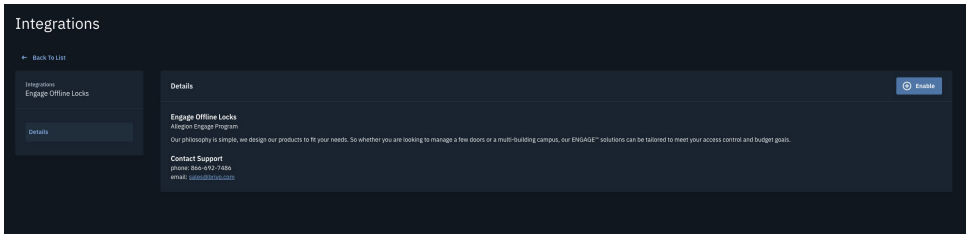
NOTE: Follow the instructions provided by Allegion on creating an Allegion Engage account found within the app. You do not need to create a site within Allegion Engage. One will be created as a part of the Engage Integration.

1. In Brivo Access, select **Configuration** and then **Integrations** on the left navigation bar. The Integration Library page displays.



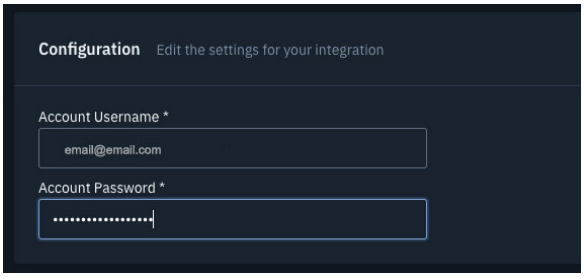
2. Within the Integration Library, you will see Engage Offline Lock as an available integration. Select the tile to configure the login information for your Engage account.

3. Once you have the Integrations Details open, click **Enable**.



4. Next, you will see the login credentials fields. The next step is to enter the Engage credentials associated with the Allegion Engage account that you want to associate the locks with.

5. Next, click **Save**. If the login credentials are correct, you will see that your Engage account is now connected. You will also notice that the Engage Integration has been moved to Enabled Integrations. You can now start creating an Offline Site to which you can add the locks.

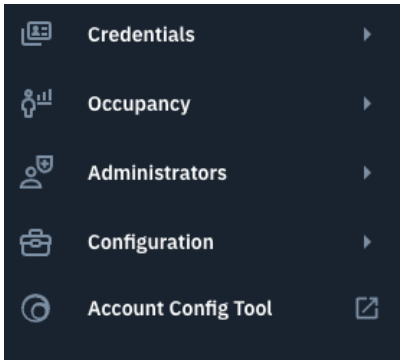


Configuring a Site in Brivo

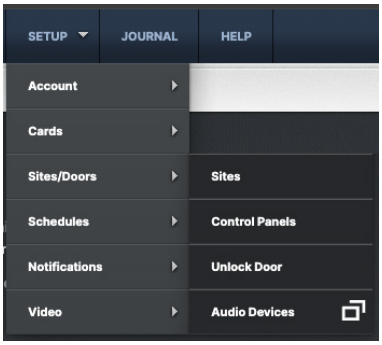
NOTE: You may utilize an existing site or create a new site for Offline Locks.

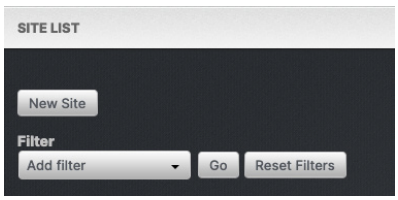
NOTE: If utilizing an existing site, jump to **Create an Offline Lock Site** below.

1. If creating a new site:
   a. From the left navigation bar, select **Account Config Tool.**
   b. Within the **Account Config Tool**, create a site to which the Control locks will be associated.
   c. Once in the Account Config Tool, go to **Setup**->**Sites/Doors**->**Sites** and click on the **New Site** button.

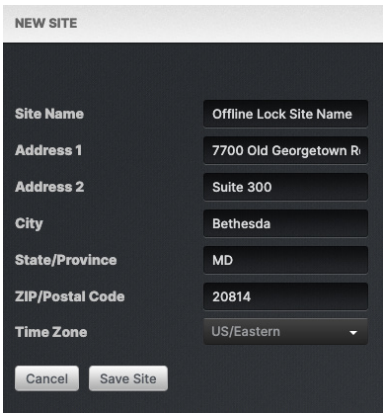


   d. Create a new site in the account as per normal and when finished, click **Save Site**.



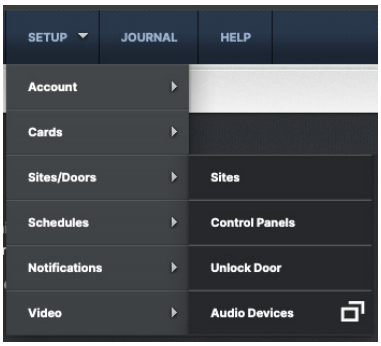


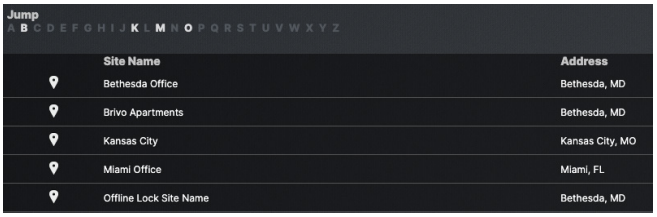
Creating an Offline Lock Site in Brivo

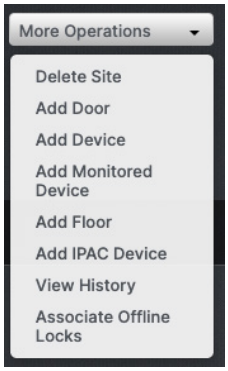


NOTE: This step is for use with an existing site in Brivo.

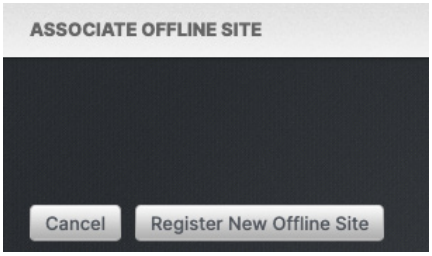
1. Once in Brivo, go to **Setup**->**Sites/Doors**->**Sites** and select the site you want to use.
2. Once on the **View Site** page, click on the **More Operations** button and select **Associate Offline** Locks.





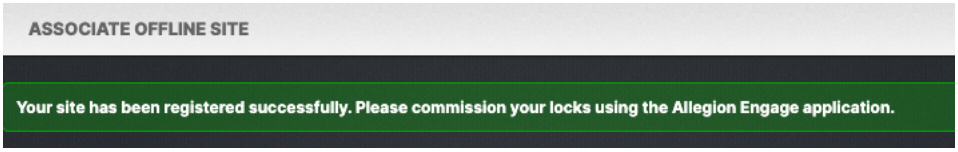


3. Follow the prompts to register this site in the Allegion Engage account.



NOTE: Step 3 will utilize the Engage Credentials entered above in **Applying Allegion Engage account credentials**.

4. Once completed, a message will appear showing a successful registration. Brivo will now create this site in the associated Allegion Engage account. It is recommended to log into the associated Allegion Engage account to confirm that the newly created site is listed.



Commissioning devices using the Allegion Engage mobile app

Using the **Allegion Engage** mobile application, you must now commission all devices to the site. Find the site name that Brivo created and commission the MT20Ws and Locks.

Commissioning the MT20W

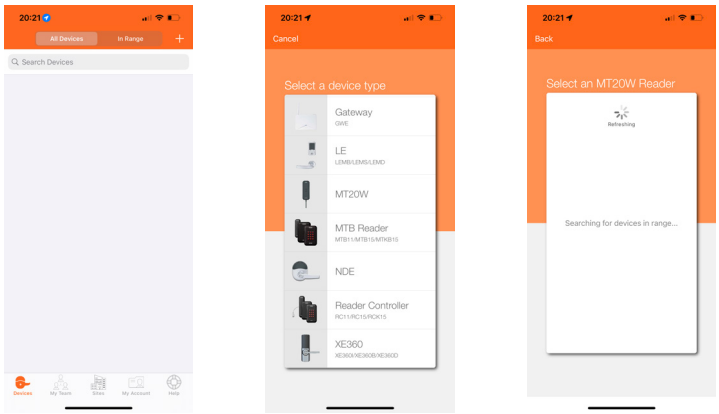
In the Engage mobile application, follow the prompts to commission the MT20W.

1. Plug the MT20W into the computer that you will be using the Allegion Engage Desktop App with Brivo Access for writing to credentials

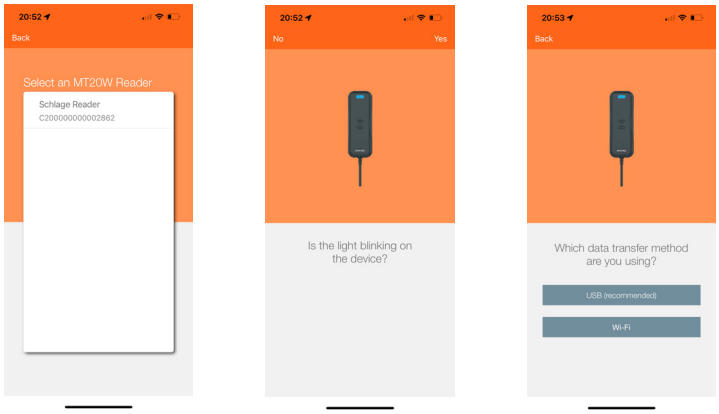
2. Even if new out of the box, it is recommended to default the MT20W using the included CE-000-040 Mt20x Factory Default Reset card. To do so, present the config card to the MT20W within on minute of power-up. Hold it in place until complete. Three beeps followed by a reset of the MT20W will indicate success. It is best practice to run through the default process twice.

3. If using the MT20W with the Brivo Unified Credential, this is a good time to present the ALGN-CFG-BUC (CE-052-861) to the reader using the same process as the Factory Default.

4. Within the Engage App, navigate to the site and select the **+** at the top right corner. In the next screen, select the MT20W from the list.



5. When the app locates the MT20W, it will display in the list. Verify the serial number of the MT20W and select it from the list. The next screen will ask you if the Blue light is blinking on the MT20W. If so, you are ready to continue. Select **Yes**. On the next screen you will be asked **Which data transfer method are you using?**, select **USB**.



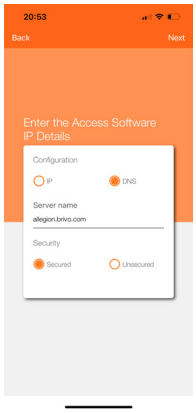
6. When you reach the step to enter the access software IP details, enter the following configuration:

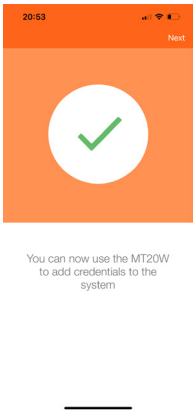
   a. **Configuration**: DNS
   b. **Server Name**: allegion.brivo.com
   c. **Security**: Secured

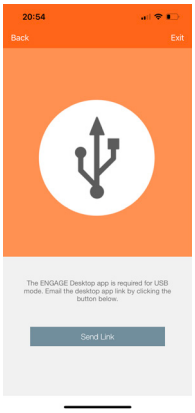
   Once this information has been successfully entered, a confirmation screen will appear.

7. Tap the **Send Link** button to receive an email with the MT20W desktop application. This is required when setting up credentials.

NOTE: The link will be sent to the email address associated with the account that is currently logged in.







Commissioning Offline Locks

In the Engage mobile application, follow the prompts to commission Control Locks.

NOTE: If you have never installed Control Locks before with Brivo, it is recommended to choose **Use Default Settings** when asked **Do you want to use default Control Lock settings for this Site?**

NOTE: Before you commission any lock, it is a good idea to factory default the lock. Refer to the FDR instruction in the Allegion Installation Guide for the lock you are commissioning.

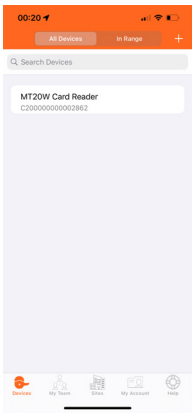
NOTE: Locks cannot be commissioned to a site if those locks:

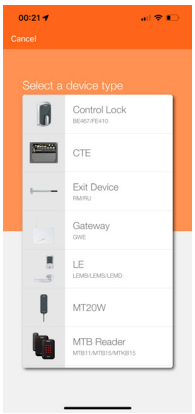
A. Exist on another account on a different system.
B. Exist on a different Brivo Account or Site.
C. Have been removed from a previous Engage account attached to Brivo but have not been synchronized.
D. Have not been Factory Defaulted after removing from existing account or site.

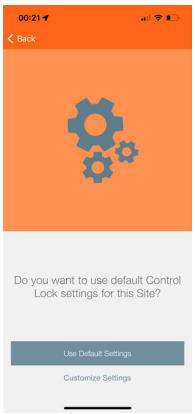
1. In the Engage Mobile App, enter the Offline Lock Site where you want to commission the locks. This should be the same site where you previously commissioned the MT20W.

2. Select the **+** icon on the top right part of the screen. You will then select the device type. The Brivo Offline Lock integration supports both Control and XE360 lock sets.

3. Next, select **Use Default Settings**. You can change these settings later if needed.



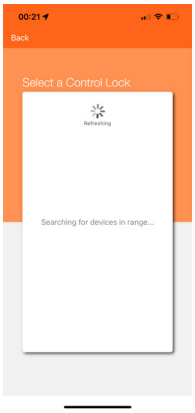


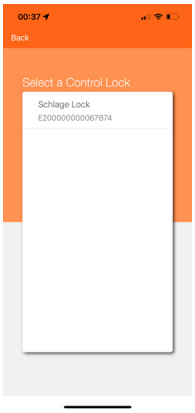


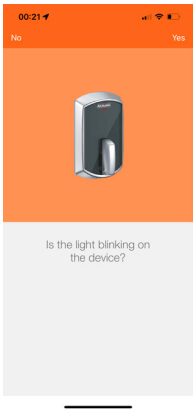
4 The Allegion Engage app will scan for devices in range. Select your device from the list provided.

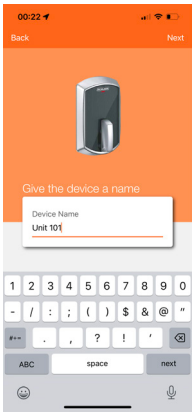
5. The Allegion Engage app will have you check and confirm that the LED on the lock is blinking. If the lock that you are trying to commission has a blinking LED, select **Yes**.

6. On the next screen you will give the device a name. Make sure that you give the name that you will be using for the site. If you ever need to rename the lock, you will need to completely remove the lock and recommission the lock.



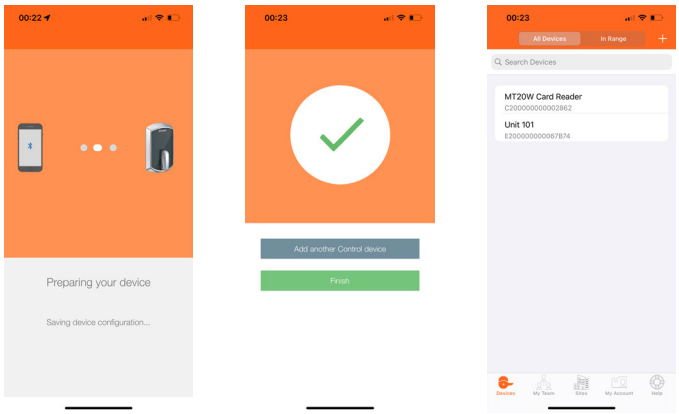






7. The Allegion Engage app will finish preparing your device and display a notice of successful configuration. You may either **Add another Control device** or **Finish** by selecting either option.

8. Your new Control Lock now displays in the Engage app.

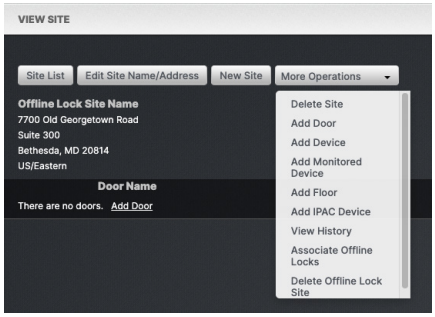


Synchronizing Control Locks in Brivo

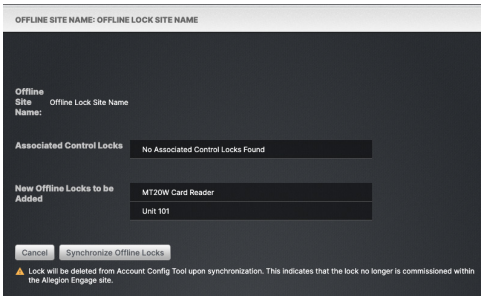
Once you have commissioned all of the devices, return to Brivo to synchronize them.

1. Once in Brivo, go to **Setup**->**Site/Doors**->**Sites** and select your site.

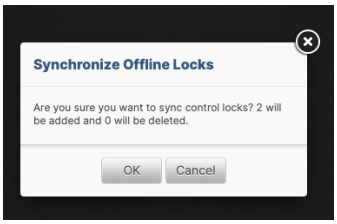
2. Once on the **View Site** page, select **More Operations** and then select **Associate Offline Locks**. The Offline Lock Synchronization pop-up window will appear.

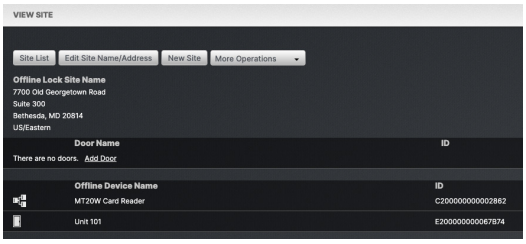


3. In the pop-up window, verify the devices being associated and click the **Synchronize Offline Locks** button.



4. Click **OK** in the confirmation pop-up window and the **View Site** page will display with the **Offline Devices** listed.





NOTE: If your installation plan requires you to create and add device groups, such as the need for a “Master Credential,” view the Creating and Assigning Device Groups to Lock section first before continuing to set the No Tour address.

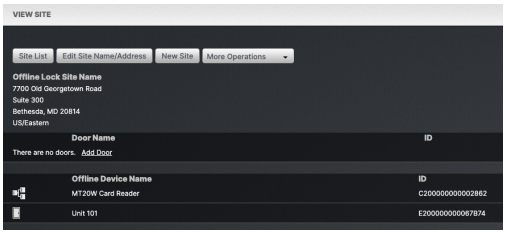
Creating and Assigning Device Groups to Locks

A device group is used if there is a need for a master credential (one that can be used across many locks). This section will provide the steps needed to create and assign a device group to a lock. It is recommended (but not required) to perform this step before setting to No Tour Address on the lock(s).

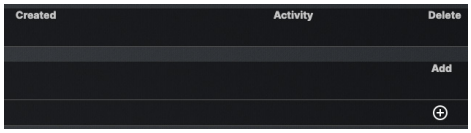
IMPORTANT NOTE: You must assign the device group(s) to your card(s) for them to work correctly with locks in a device group.

1. Go to the **Setup -> Sites**.

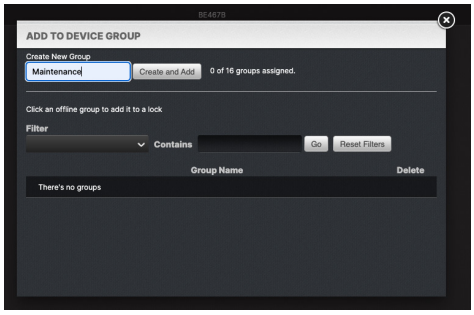
2. Find the control lock under the **Offline Device Name** section.



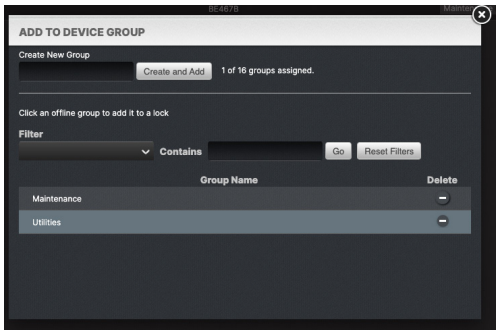
3. Click on Add **+** at the far right of the page. This will bring up a new popup window.



4. If you need to create a new device group, enter a name and click the **Create and Add** button.



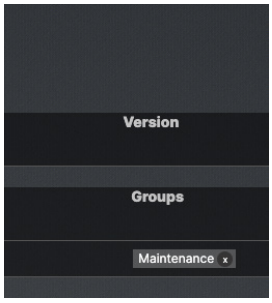
5. You may instead select an existing group from the list.

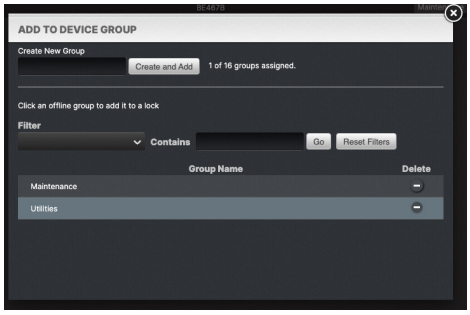


6. Once you have added (or created and added) your device group, you will see that the group shows up in the Lock Details

NOTE: An Allegion Control Lock can only be associated with a maximum of 16 device groups.

7. A group may be removed from the Control Lock by clicking on the **X** within the label of the lock. A Group may be deleted permanently by selecting **Delete** in the ADD TO DEVICE GROUP pop-up.





Set No Tour Address through the Brivo Install Mobile Application

Once the devices have been installed, commissioned, and synchronized with Brivo, the last step is to set a No Tour address for each lock.

NOTE: It may be easier to do this per lock or all at once after all locks have been installed. Practice with each installation and commissioning step to see which works best for you.

NOTE: This will require the use of the Brivo Install Mobile Application. If you have not done so already, please download the application through Google Play or Apple Store.

NOTE: Brivo Install version 1.6.1 is used in these instructions. The login procedure is different for older version of the application.

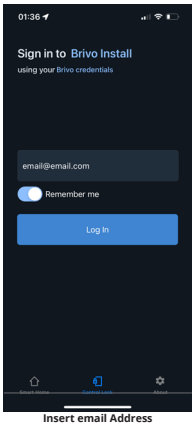
1. Open the Brivo Install application. The application has two separate logins. One for Brivo Smart Home and one for Control Lock. Select **Control Lock** from the bottom of the screen.

2. Log in using your Account Config Tool Administrator username or your email address associated with Brivo Access. Once you select **Login**, you will be prompted for your password.

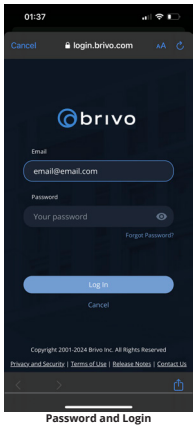
3. Once you have logged in, select the **Account** that you are working with and select **Go To Account**. Next, Select the site your lock exists in.

4. You will then select the lock that you need to set the IDs on. On the next screen, you will see that the lock does not have a Lock ID set. You should also see any of the groups that are associated with the lock.

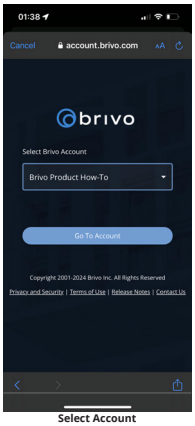
5. Tap the **Set Lock to No Tour**. Once successful, tap **OK** in the pop-up Success window.



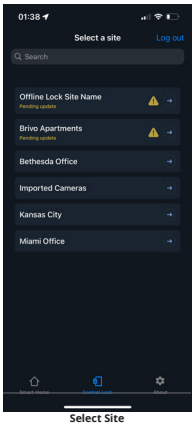
Insert email Address



Password and Login

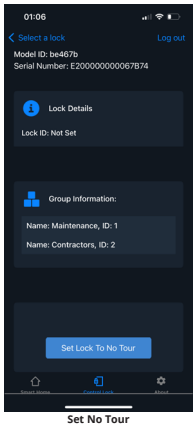


Select Account

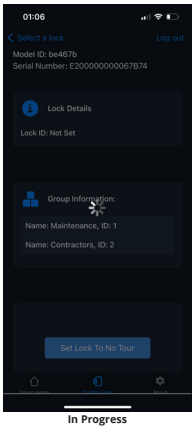


Select Site

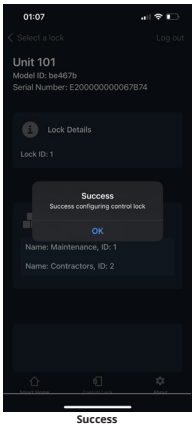
Select Lock



Set No Tour



In Progress



Success

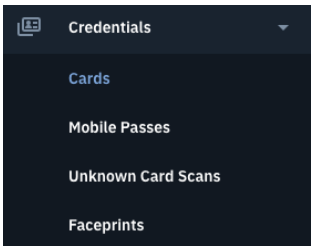
User and Permission Setup

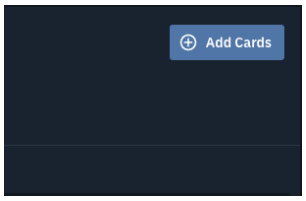
Adding Cards for Use with Offline Locks

This section describes adding card to the Brivo Card Bank and setting them for use with both online and offline locks.

NOTE: Cards need to be added to the Brivo account in a specific fashion. If you plan to use any supported Allegion smart cards that have been previously added, they must be readded.

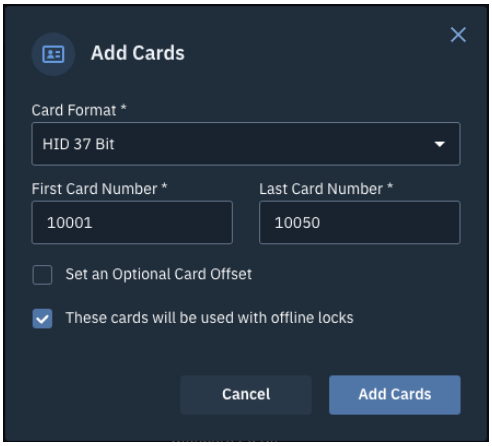
1. In Brivo Access, select **Credentials** from the left navigation bar. The Card Bank displays. In the Card Bank, click **Add Cards**. An **Add Cards** pop-up window will display.



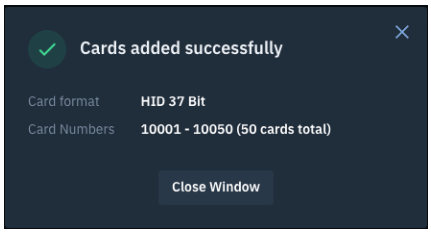


2. In the **Add Cards** pop up window, you will select the card format. The supported Formats are Standard 26 bit, HID 37 bit and HID 37 bit w/ Facility Code.

3. Next you will enter the card range by entering the first and last card numbers. You will then check the **These cards will be used with offline locks** checkbox. Finally, click **Add Cards**.

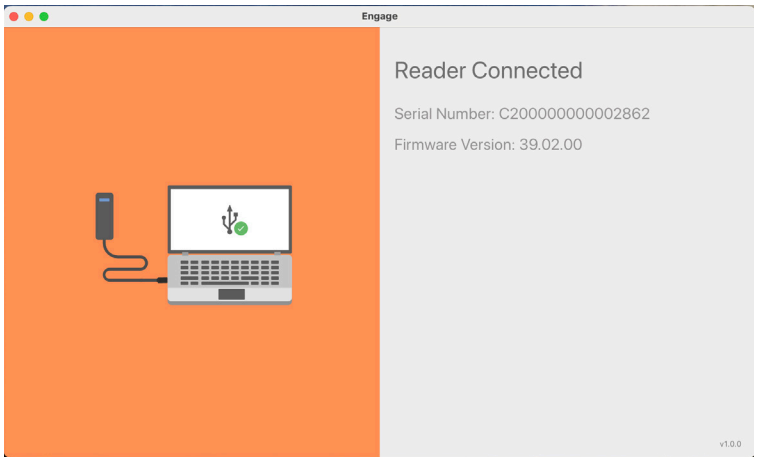


4. You should see a confirmation that your cards were added. Only when **These cards will be used with offline locks** is selected can the cards be used with Offline Locks.

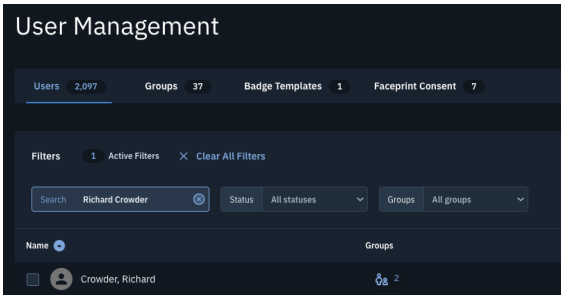


Associating a Card to a User under Offline Lock

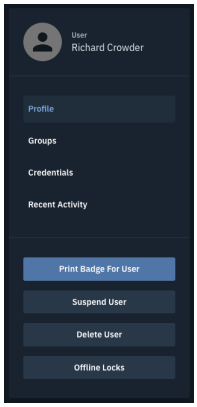
NOTE: Before associating a card, be sure to have the Engage MT20W desktop application open and displaying that the reader is connected.



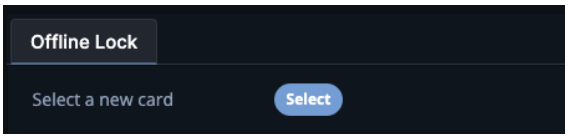
1. To set up a card for a user, navigate to **Users**->**Users** and then select their **User Profile**.

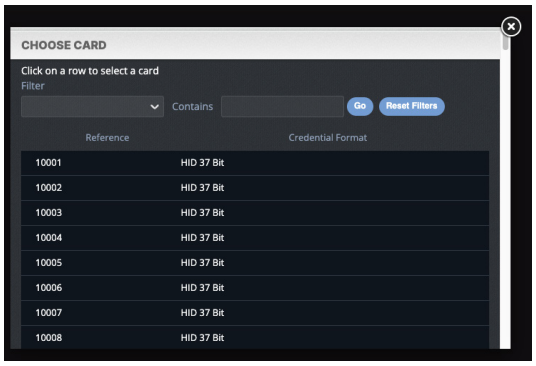


2. Once on their **User Profile** page, click on the **Offline Lock** tab.

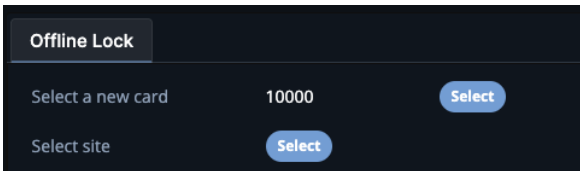


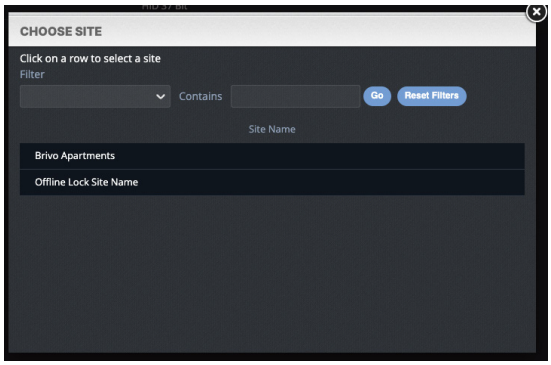
3. Within the Offline Lock Permissions screen, you will first select the card to program. Click on the **Select** button. You will then select your **Card.**



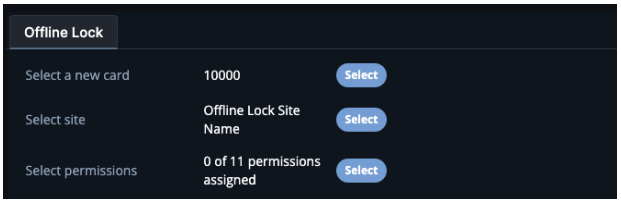


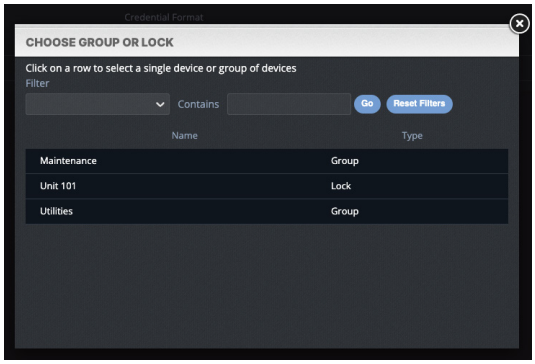
4. You can now select the Site you are assigning permissions to by clicking on **Select** next to **Select Site** and selecting the site from the list.





5. Next you will add the permissions to the card by clicking on **Select** next to **Select permissions.** In this step you can either add individual locks or Groups that you have assigned to the locks.

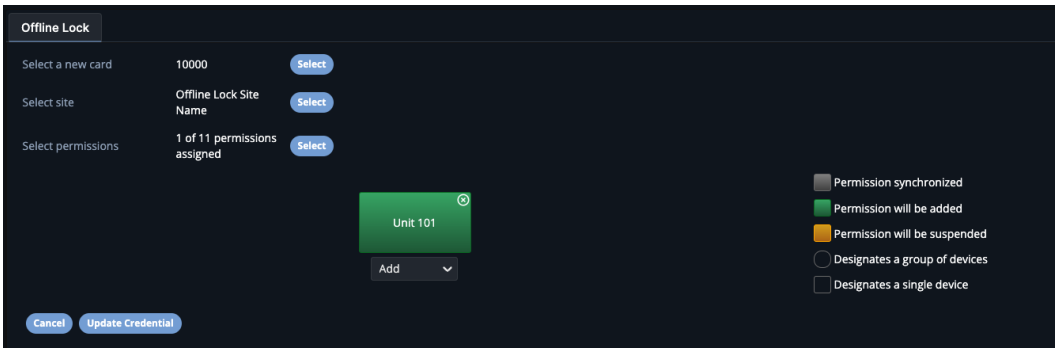




NOTE: Each card has a limit of eleven (11) single devices or device groups to which it can be assigned.

Setting Permissions

Once permissions have been added to the card, a legend will display showing the different permission types.



Green: Permission added

Yellow: Permission is suspended

Gray: Permission already added

Green signifies the permissions you are currently adding.

Yellow signifies the permissions you are suspending or reinstating.

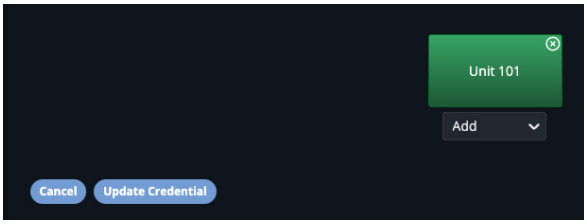
Gray signifies permissions already on the card.

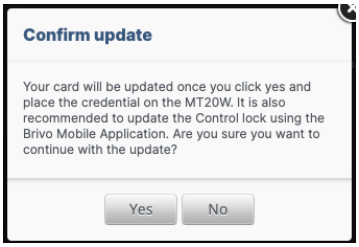
After setting permissions on a credential, there are additional steps that must be followed depending upon the type of permission.

Permission Type	Description
Adding permissions only	Set up the credential using the MT20W
Suspending permissions	Set up the credential using the MT20W OR Update the Control Lock using the Brivo Install Mobile Application if immediate action is required or there is no access to the credential
Removing permissions	Set up the credential using the MT20W AND Update the Control Lock using the Brivo Install Mobile Application
Reinstating permissions	Set up the credential using the MT20W AND Update the Control Lock using the Brivo Install Mobile Application

Updating the Credential on the MT20W

1. Once you have finished setting up the device permissions on the card, click on the **Update Credential** button. A confirmation pop-up will appear.





2. Brivo Access will send the permissions to the card on the MT20W.

3. Ensure that you have the Engage desktop application open and place the card on the MT20W. The MT20W will beep while accepting the card followed by a solid green. When the MT20W is done writing to the card you will hear three beeps with three green LED flashes. If you see red, refer to the Error Codes and Troubleshooting sections.

4. Congratulations, you have successfully set up the card for use at the selected Control Lock(s).

Error Codes for the MT20W

If there is an issue writing to the card, the Engage App will display certain codes. You will see these on the Engage Desktop app in red at the bottom of the window.

Error 401 - The MT20W has not been commissioned yet. This will require someone to go through the installation process for the MT20W.

Error 402 - The MT20W failed to read the credential that was placed on it. One reason is because the credential was removed too early. Please try again by placing the credential on the MT20W and leaving it through the set up process.

Error 407 - The lock you are applying permissions for does not have an ID set on it. This can be confirmed by viewing the Brivo Access journal at the time the credential was placed on the MT20W

Error 411 - Server error, the MT20W could not reach the services required to update the credential.

Error 417 - Invalid sector, the credential was not successfully written. Position the credential in the upper center of the reader and repeat the syncing process. Do not remove the credential during sync.

Error 426 - Invalid Permissions. This is indicating that either the MT20W or one of the locks is assigned to another site or account. If locks or MT20Ws are moved between Accounts or Sites, they must be removed in Engage and the previous site must be synchronized in the Offline Lock Association window.

How to update the firmware on the MT20W

1. Connect to the desired MT20W you wish to upgrade using the Allegion Engage mobile application.
2. Tap on **Settings** to adjust the DNS settings.
3. You must temporarily change the DNS server name to api.allegionengage.com/ then **Save**.
4. Back out to the device home page, tap on **Update Firmware** and long press on **Update**.
5. Choose the firmware version you wish to install on the MT20W and follow the prompts to complete the process.
6. Once the firmware upgrade is complete, ensure it is up to date under settings.
7. Lastly, be sure to change the DNS address back to allegion.brivo.com as listed on step 2 of Commissioning the MT20W.

Adding Mobile Credentials

Configuring Control Lock with Brivo Mobile Pass

Brivo Mobile Pass allows users to configure Allegion Control Locks to open doors using mobile credentials.

Assigning Brivo Mobile Pass with Brivo

1. To assign a Brivo Mobile Pass, navigate to **Users**->**Users** and then select the user.
2. Once the user is selected, go to the **Groups** tab and assign that user to your Control Lock group. Make certain that group has access to the site with your Control Lock(s). To verify this, you may check the Group Permissions for that specific group under by going to **Users->Groups** and selecting your Control Lock group.
3. If you do not already have a group set up, follow step 3, otherwise, skip to step 4. Click on **Groups->New Group** and complete the standard creation process. Make certain to provide privileges to the site with your Control Locks before saving.
4. Now from the selected user, go to the **Credentials** tab and click the **Add** button next to Brivo Mobile Pass. In the pop-up window, add an **Email Address** and click the **Send** button to send the Brivo Mobile Pass invitation.

NOTE: The Brivo Mobile Pass invitation must be redeemed within 72 hours. If not redeemed within that period, that Brivo Mobile Pass will need to be revoked and a new Brivo Mobile Pass invitation will need to be sent.

Redeeming a Brivo Mobile Pass with Allegion Control Locks

1. If you have not done so already, download the **Brivo Mobile Pass** app from App Store or Google Play Store.
2. Open the email invitation and click on **Add to Brivo Pass**. You may also manually enter the **Pass ID** and **Pass Code** from the app.
3. Now that the invitation has been accepted, you should see the Control Lock listed on the door listing page.

IMPORTANT NOTE: Make sure your **Brivo Mobile Pass** app has Bluetooth turned on, and you are near the Control Lock while opening it.

4. You may now open the Control Lock using the **Brivo Mobile Pass** app.

NOTE: To provide a faster **Brivo Mobile Pass** interaction with the Control Lock(s), please check the Mobile Credential Performance setting on the lock(s). This can be done by connecting to the lock(s) with the **Engage Mobile App** and going to **Settings->Mobile Credential->Performance**. Setting the performance to Max will increase the read range on the lock(s). Please be aware that changing this setting may impact the battery life of the lock.

Appendix

Troubleshooting

Control Lock does not appear in Brivo Access

Verify that the Control Lock has been commissioned to the correct site using the Engage mobile application.

Verify that the Allegion Engage account credentials have been added to the account.

Synchronize the Brivo Access and Engage accounts.

Control Lock does not appear in Brivo Install

Verify that the lock appears in Brivo Access. If it does not, follow the troubleshooting step listed above.

Verify that you have an active internet connection and are within range of the lock.

Lock does not appear in Engage app after it was commissioned

Verify you are viewing the site to which the lock has been commissioned.

Verify that you have an active internet connection and are within range of the lock.

Lock does not appear in range when trying to commission it with the site in Engage

The lock may have been previously installed/commissioned on another site or account.

Make sure to remove it from its current location, factory default it and commission it to the proper site.

Error when setting No Tour

Ensure the phone is within Bluetooth range of the lock.

Repeat the No Tour setup process.

User requires access to more than 11 doors

Create a device group and apply it to the user's credential. Each credential can be associated with up to 11 devices or device groups. A lock can be a part of 16 device groups.

Revision List

Date	Version	Description
November 3, 2020	1.0	Initial version
November 19, 2020	1.1	Updated content
April 28, 2021	1.2	Updated content
July 21, 2021	1.3	Added the Control Lock Configuration Walkthrough
May 15, 2024	1.4	Updated content