PRODUCT STATUS UPDATE

VANDERBILT

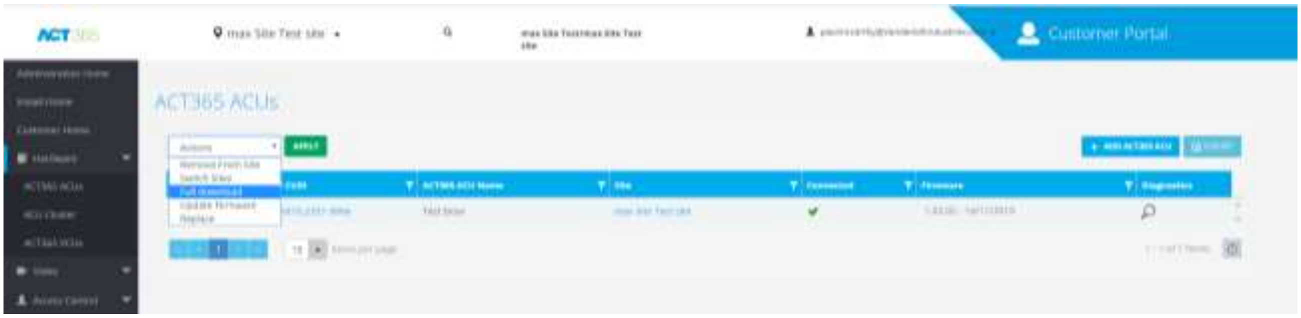
PRODUCT LINE:	ACCESS		
PRODUCT NAME:	ACT365 Portal		
MODEL(S):	1.3	**CATEGORY:**	RELEASE
CONTACT:	Local Technical Support	**DATE:**	2019-11-27

New Features and Improvements:

1. Twin Users [SW & FW]
2. Lockout/lockdown feature [SW & FW]
3. Purge Log events for GDPR
4. Add whitelisted cards (fire cards) to ACU
5. Docs Portal - Phase 1
6. Turkish language translations added
7. OP2 and OP3 logging [SW & FW].

Before introducing the new features, we advise that after the release of ACT365 1.3, all registered installers should perform a full download and upgrade the firmware on the ACT365 ACU to benefit from the new features in the 1.3 release. To do this, follow these steps:

1. Enter into a customer site on the ACT365 Portal
2. Under the hardware menu select ACT365 ACU's
3. Select the ACU's to be upgraded, and from the "Actions" dropdown select "Full Download" and click "Apply". Please wait as this firmware upgrade may take several minutes.



Warning: In the event of an upgrading firmware failure, it is advisable to Power Cycle the ACU should you have access to the site.

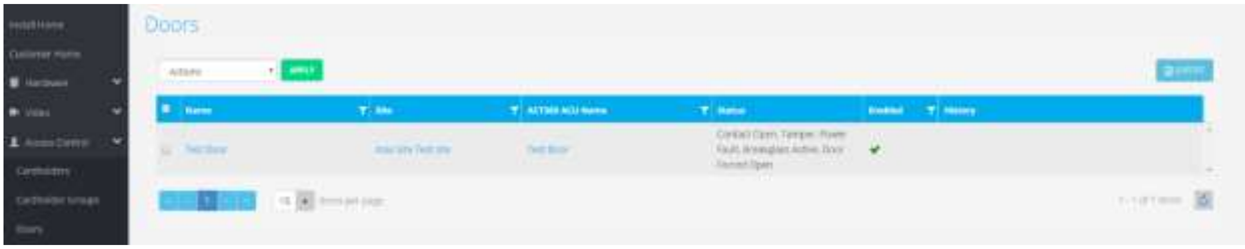
1. Twin Users

Twin Users is now a feature in ACT365. This allows for the setting to secure doors that require two people to have access at any given time. Certain scenarios include:

A) Access to a Medicine room (Pharmacy)
B) Financial Room (Bank, Cash Storage Room)
C) Highly sensitive Data room requiring two people on-site at once.

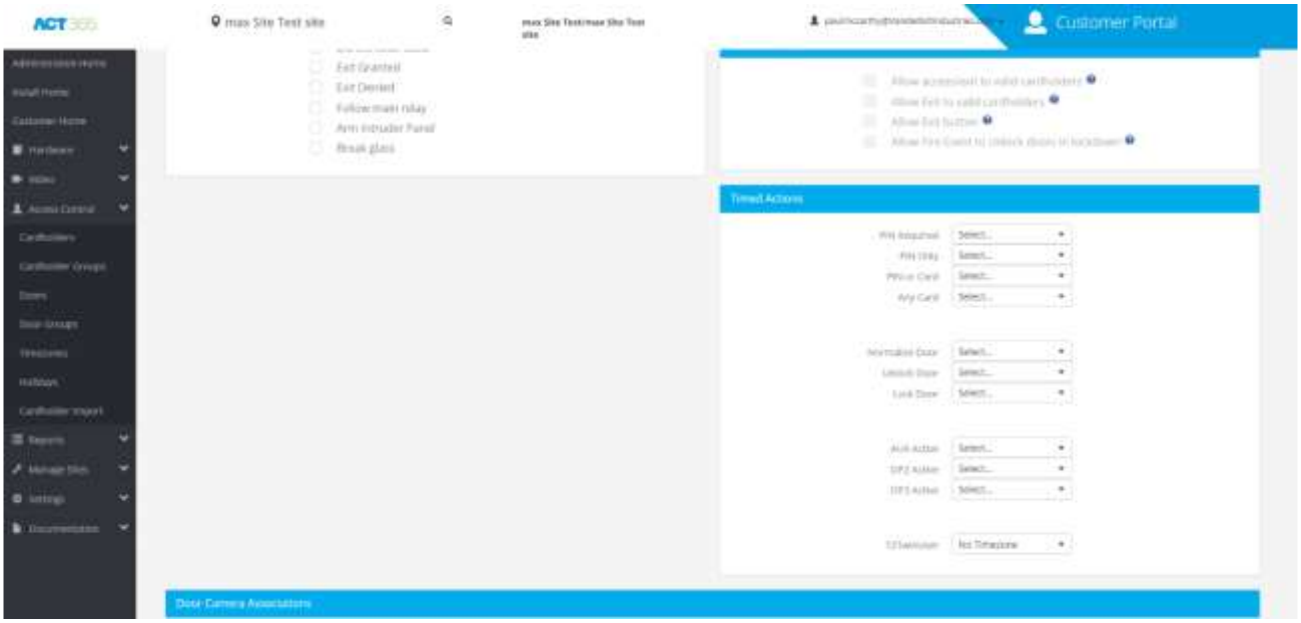
To configure the Twin User functionality, please follow these steps on the ACT365 Portal.

- From the ACT365 Doors menu, select the door you wish to configure Twin Users.

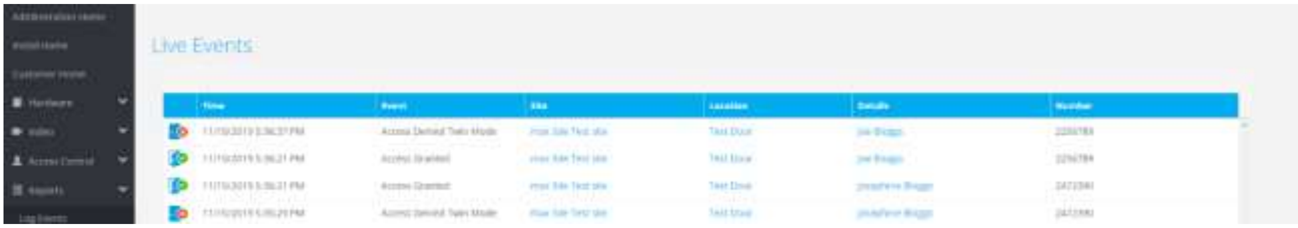


- Enter the door and scroll to the Timed Action section
- Select a Time zone (configured under Access Control >Time zones) or 24 hours and

save the settings



- After saving the settings for the Door, the readers will require two registered cardholders to badge their cards within 10 seconds of the first badge being swiped
- In the event of a single user swiping their card and no second user being present, the event will show as follows:

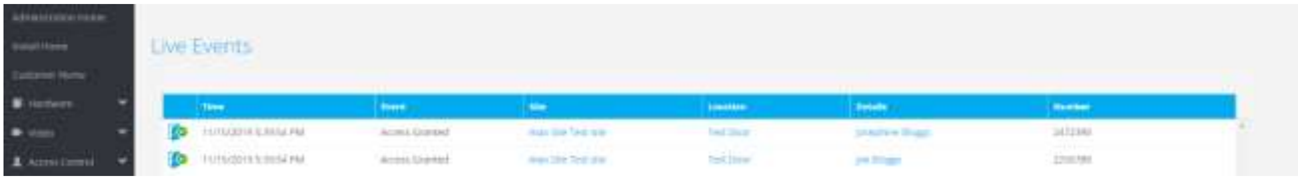


Live Events

	Time	Event	Site	Location	Details	Number
	11/15/2019 5:36:37 PM	Access Denied Twin Mode	[illegible]	Test Door	Joe Bloggs	[illegible]
	11/15/2019 5:36:21 PM	Access Granted	[illegible]	Test Door	Joe Bloggs	[illegible]
	11/15/2019 5:36:21 PM	Access Granted	[illegible]	Test Door	Josephine Bloggs	[illegible]
	11/15/2019 5:36:29 PM	Access Denied Twin Mode	[illegible]	Test Door	Josephine Bloggs	[illegible]

The card reader will normalize after the 10 second period.

- A successful Twin User swipe will grant access to both users, as shown below.



Live Events

	Time	Event	Site	Location	Details	Number
	11/15/2019 5:39:54 PM	Access Granted	[illegible]	Test Door	Josephine Bloggs	[illegible]
	11/15/2019 5:39:54 PM	Access Granted	[illegible]	Test Door	Joe Bloggs	[illegible]

Note: *This feature is set on the Door settings only. It is not possible to restrict which users have access to a particular door. To limit access to a particular door, enter into the cardholder settings and grant or restrict access to each user on a case-by-case basis.*

2. Lock Down/ Lockout

ACUs can be configured to lock down connected doors in the case of an emergency. Lockdown settings are configured on a per-site basis in ACT365. Once lockdown support is configured, a site lockdown can be set/cleared from the ACT365 website. In an emergency, it may not be possible to log in to ACT365. Therefore you should additionally install and configure lockdown readers at appropriate locations.

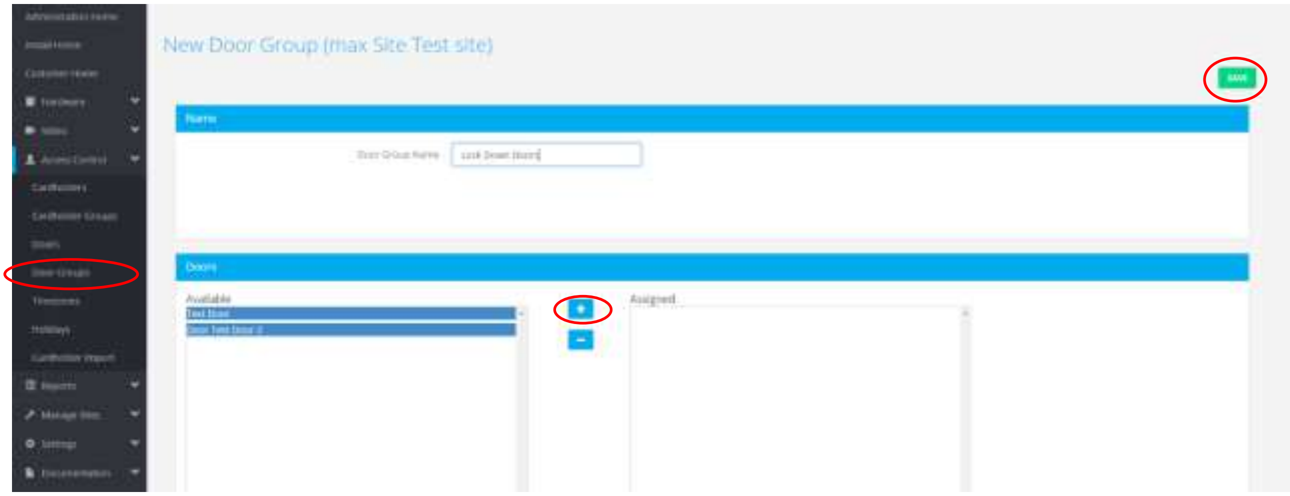
The ACT365 team advises that an ACU should be used exclusively for lockdown, or exclusively for access, but never both. To support lockdown functionality for a site in ACT365:

1. Configure a lockdown door group
2. Configure lockdown behavior for each door in the door group

3. Grant specific cardholder's rights to set/clear a lockdown.

Configuring a lockdown door group

1. Go to the relevant customer portal in ACT365
2. From the site picker, select the site for which you want to configure a lockdown door group
3. Create a door group that contains all lockdown doors. To do this:
    a. Click Access Control > Door Groups.
    b. Click New Group.
    c. Please select one or more doors from the Available list and click to move them to the Assigned list.
    d. Click Save.


New Door Group (max Site Test site)

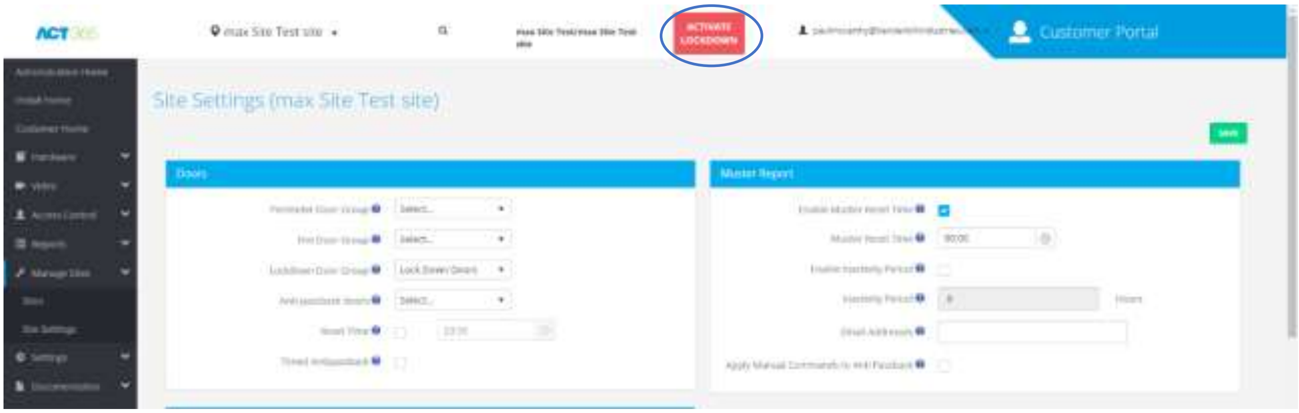
Door Group Name: Lock Down Doors

Configure the Lockdown Door Group under Site settings

To do this:

e. Click Manage Sites > Site Settings.
f. Select the door group containing lockdown doors from the Lockdown Door Group drop-down list.

g. Click Save. The ACTIVATE LOCKDOWN button will now appear in the Top Ribbon.



Site Settings (max Site Test site)

Doors

Lockdown Door Group: Lock Down Doors

Muster Report

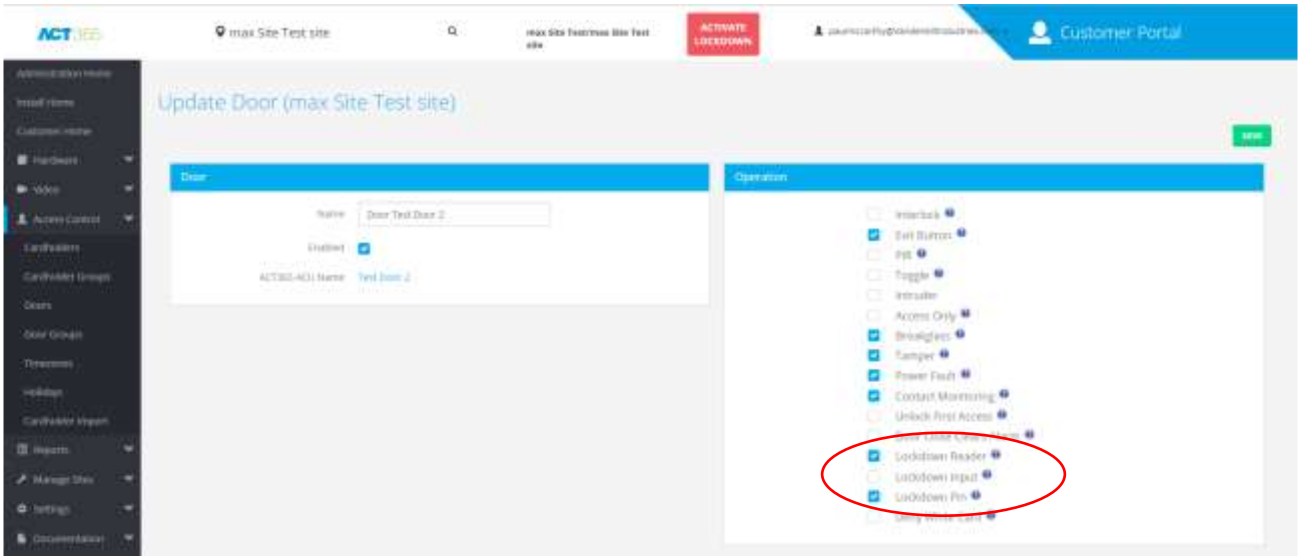
Enable Muster Reset Time ☑

Muster Reset Time: 00:00

Configuring lockdown behavior for a door:

1. Go to the relevant customer portal in ACT365
2. From the site picker, select the site for which you want to configure a door
3. Click Access Control > Doors
4. Click the name of the door whose lockdown behavior you want to configure
5. On the Update Door page, under Operation, select checkboxes for the lockdown operation settings that should apply to this door:
    a. Lockdown Reader – Select this checkbox to indicate that all readers connected to this door are used exclusively for lockdown, and never for normal access control
    b. Lockdown Input – Select this checkbox if the AUX input on the ACU has a lockdown input connected. In this case, if 0V is applied to the AUX input connection, this triggers a lockdown. If this checkbox is selected, the AUX input on the ACU can only be used for lockdown support
    c. Lockdown Pin – Select this checkbox if a PIN and Prox reader that should support normal access control and lockdown is connected to this door. In this case, cardholders can swipe their cards for normal access control, or enter a PIN to trigger/clear a lockdown.
6. On the Update Door page, under Lockdown Options, select checkboxes for the access settings that should apply to this door during a lockdown
7. Allow access/exit to valid cardholders – Select this checkbox to allow all valid cardholders to enter/exit this door during a lockdown
8. Allow Exit to valid cardholders – Select this checkbox to allow all valid cardholders to exit this door during a lockdown. Access will be denied
9. Allow Exit button – Select this checkbox to allow individuals to exit this door during a lockdown by pressing a wired Exit button

10. Allow Fire Event to Unlock doors in lockdown – Select this checkbox to unlock this door if there is a fire event during a lockdown. If this checkbox is not selected, the door will remain locked during a fire event
11. Click Save.



Update Door (max Site Test site)

Door

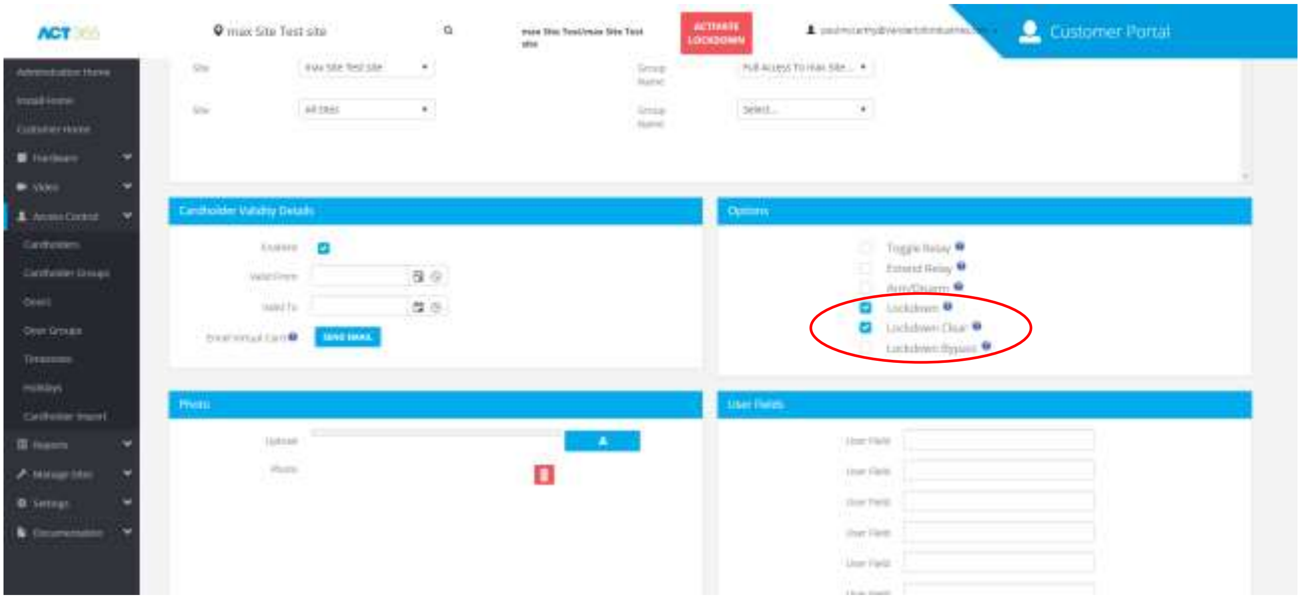
Name: Door Test Door 2
Enabled: ☑
ACT365-ACU Name: Test Door 2

Operation

☐ Interlock
☑ Exit Button
☐ PIR
☐ Toggle
☐ Intruder
☐ Access Only
☑ Breakglass
☑ Tamper
☑ Power Fault
☑ Contact Monitoring
☐ Unlock First Access
☐ Door Close Clears Alarm
☑ Lockdown Reader
☐ Lockdown Input
☑ Lockdown Pin
☐ Deny White Card

Configuring cardholder rights to set/clear a lockdown:

1. Go to the relevant customer portal in ACT365
2. From the site picker, select the site for which you want to configure cardholder rights
3. Click Access Control > Cardholders
4. Click the Name of the cardholder whose lockdown rights you want to configure
5. On the Update Cardholder page, select checkboxes for the lockdown rights this user should have:
   a) Lockdown – The user can initiate a lockdown from a lockdown reader using their access control credentials
   b) Lockdown Clear – The user can clear a lockdown using their access control credentials (card/PIN)
   c) Lockdown Bypass – The user can bypass lockdown doors using their access control credentials (card/PIN)
6. Click Save.



Site: max Site Test site
Site: All Sites
Group Name: Full Access To max Site...
Group Name: Select...

Cardholder Validity Details

Enabled ☑
Valid From
Valid To
Email Virtual Card

Options

☐ Toggle Relay
☐ Extend Relay
☐ Arm/Disarm
☑ Lockdown
☑ Lockdown Clear
☐ Lockdown Bypass

Photo

Upload
Photo

User Fields

User Field
User Field
User Field
User Field
User Field

How to trigger and clear lockdowns

If lockdown support is configured for a site in ACT365, an operator with sufficient permission can trigger and cancel lockdowns from the ACT365 web portal, or a cardholder can trigger and cancel lockdown from a lockdown reader. Triggering a lockdown locks all lockdown doors and overrides any timed actions active on those doors. All door actions, including normalize, are disabled during a lockdown. Clearing a lockdown normalizes all lockdown doors and cancels any manual door commands on those doors. Any active time zones are re-activated.

Triggering a lockdown

To trigger a lockdown from the ACT365 web portal:

1. Go to the relevant customer portal in ACT365.
2. From the site picker, select the site for which you want to trigger a lockdown.
3. At the top of the page, click ACTIVATE LOCKDOWN to trigger a lockdown for the selected site.

Note: *The ACTIVATE LOCKDOWN button only appears if lockdown doors are configured*.

Click Apply to confirm triggering the lockdown

To trigger a lockdown from a lockdown reader, depending on the reader type and configuration in ACT365, a cardholder with the Lockdown right should either:

- Present their card.
- Enter their PIN
- Present their card and enter their PIN.

The lockdown reader LED turns orange to indicate that the system is in lockdown.

Clearing lockdowns

To clear a lockdown from the ACT365 web portal:

1. Go to the relevant customer portal in ACT365.
2. From the site picker, select the site for which you want to clear a lockdown.
3. At the top of the page, click CLEAR LOCKDOWN to clear the lockdown for the selected site.
4. Click Apply to confirm clearing the lockdown.

To clear lockdown rights from a Lockdown reader:

Trusted cardholders only should be granted the ability to clear Lockdown. Cardholder settings must be set accordingly. This gives the ability to clear a site from a dedicated lockdown reader. Following the instructions in granting the User rights above. Please follow these steps on clearing lockdown from a Dedicated lockdown reader.

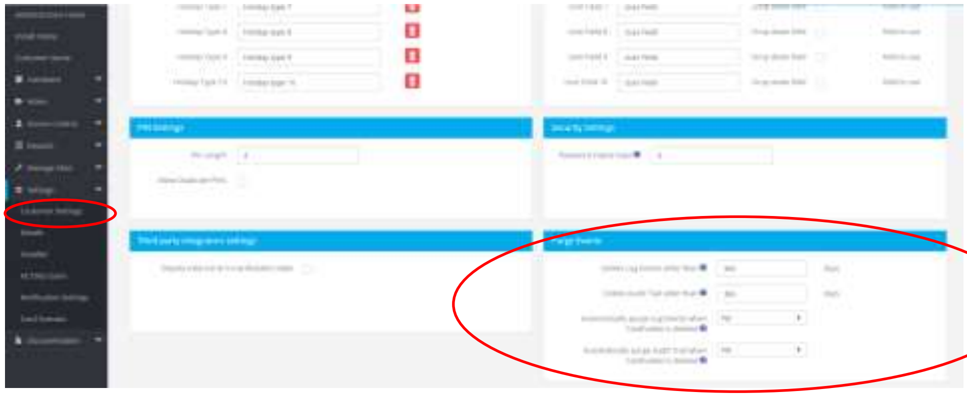
5. At a Lockdown reader, the user should present his/her card twice in quick succession
   Note: *If the door settings are set to Pin and Card, the user must present their card and enter pin immediately to clear the lockdown.*
6. The Site will now be cleared of lockdown, and doors will normalize and revert to any timed actions set before the lockdown was activated.
   Note: *The portal may need to be refreshed to show Lockdown has been cleared.*

3. Purge Log Events:

The new feature of Purging log events now gives the ability for a user on 365 to be forgotten in line with GDPR. With this new feature, customers will have the ability to automatically purge the log events for all users on a site or purge information on the user directly from the cardholder page.

Configuring Purge Log Events for a Customer:

1. Go to the relevant customer portal in ACT365
2. From the Settings menu, select the Customer Settings
3. Scroll to Purge Events.

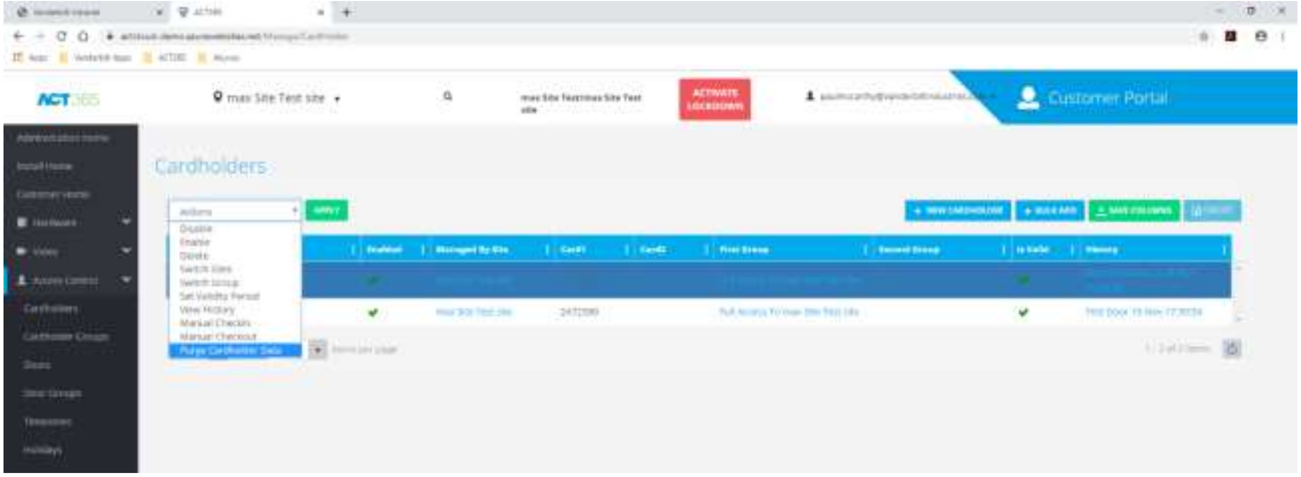


1. Select the Options you wish to amend including:
    a. Delete Log events older than x amount of days
    b. Delete Audit Trail older than x amount of days
    c. Automatically Purge log events when cardholder deleted
    d. Automatically Purge Audit trail when cardholder deleted.

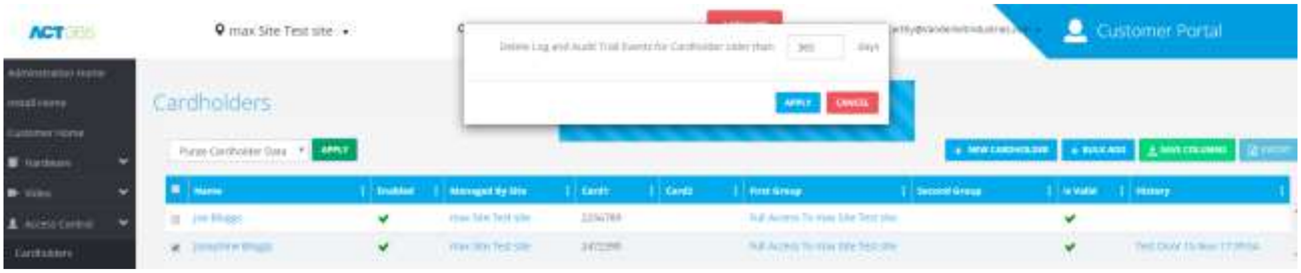
Note: *Purge events occur automatically at midnight*

Purging Cardholder information:

1. Go to the relevant customer portal in ACT365
2. From the Access control menu, select the Cardholder you wish to delete/purge events on
3. From the Actions drop-down menu select Purge Cardholder Data and click apply.



4. A prompt will appear with the default message of Deleting Log and Audit Trail events for cardholder events older than 365 days. By setting the days to 0, this will delete all cardholder events. Click Apply, and the user information on a log event will disappear from the log events page.

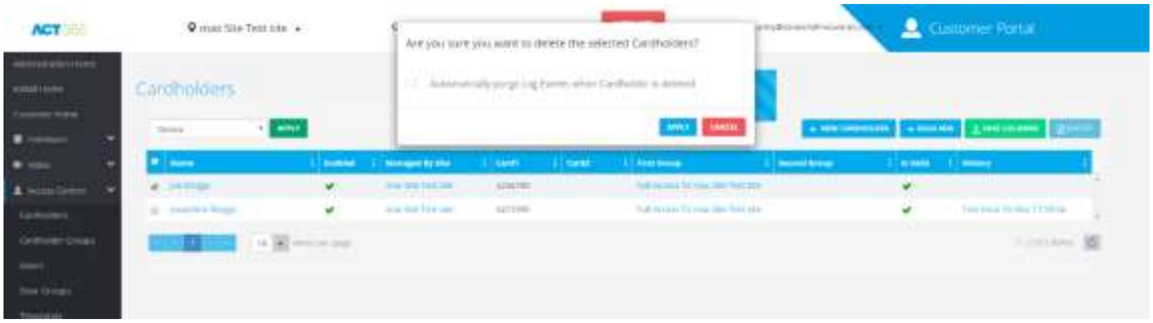


Delete Log and Audit Trail Events for Cardholder older than 365 days

APPLY CANCEL

	Name	Enabled	Managed By Site	Card1	Card2	First Group	Second Group	Is Valid	History
□	Joe Bloggs	✓	max Site Test site	[illegible]		Full Access To max Site Test site		✓	
☑	Josephine Bloggs	✓	max Site Test site	[illegible]		Full Access To max Site Test site		✓	[illegible]

5. If you select a Cardholder to be deleted completely, the settings in Customer Settings will apply to the cardholder. Below is the message that will appear should you set the Customer Settings to prompt on Deleting Log events and Audit Trail.



Are you sure you want to delete the selected Cardholders?

□ Automatically purge Log Events when Cardholder is deleted

APPLY CANCEL

4. Adding White Cards (fire Cards) to ACT365 ACU:

How to configure a white card list in ACT365

In some regions, white cards are provided to police and emergency services in case emergency access is required to a site. White cards bypass all access control restrictions, including locked doors, timed actions, user group and door group restrictions, or the requirement to enter a PIN. A white list of cards is configured per customer site in ACT365. The list of white cards is downloaded to door stations so that they can even be used when the door station is offline. In ACT365, you can configure up to 16 white cards per site.

Configuring a white card list in ACT365

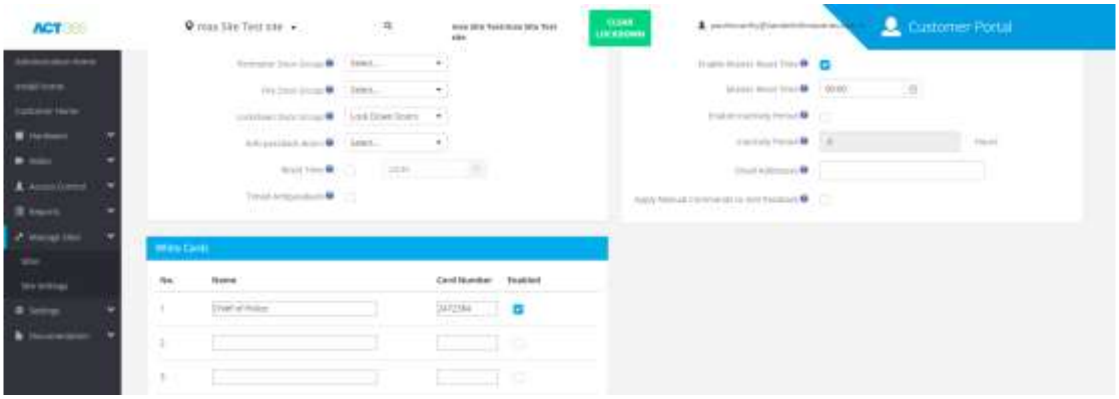
To configure a list of white cards in ACT365:

1. Go to the relevant customer portal in ACT365.
2. From the site picker, select the site for which you want to configure a white card list
3. Click **Manage Sites > Site Settings**
4. In the **White Cards** area, configure up to 16 white cards. For each card: Enter a **Name**
5. Enter the **Card Number**

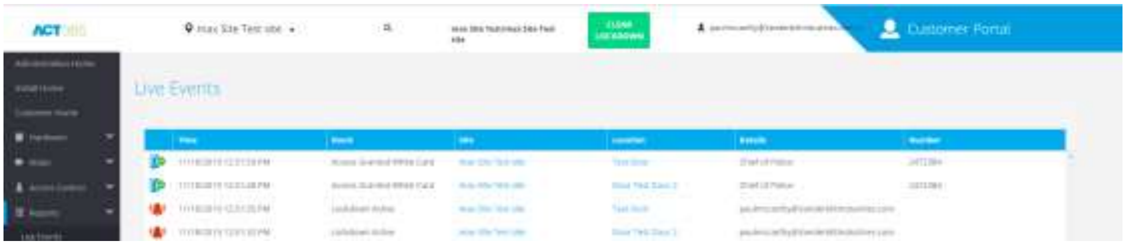
6. Select the **Enabled** checkbox
7. Click **Save.**

Example of Whitelisted Card being used on a locked-down site

In the Example below- the Chief of Police has been granted a Whitelisted Card. The site has been activated for Lockdown.



From the Live Events page, it is clear that the site has been put into a Lockdown Scenario. The chief of police has arrived on site and obtained his White Card- Perhaps located in a safe in the reception of a building or security hut. He has swiped at two doors and is granted access. The Site will remain in Lockdown until cleared by a trusted Cardholder or admin for the Site.



Denying white cards access to a specific door

In the scenario where you do not want to grant access to a White Card to a room for any reason such as a cash room, rooms holding highly sensitive data, etc. it is possible to deny the use of white Cards. Please follow these steps below.

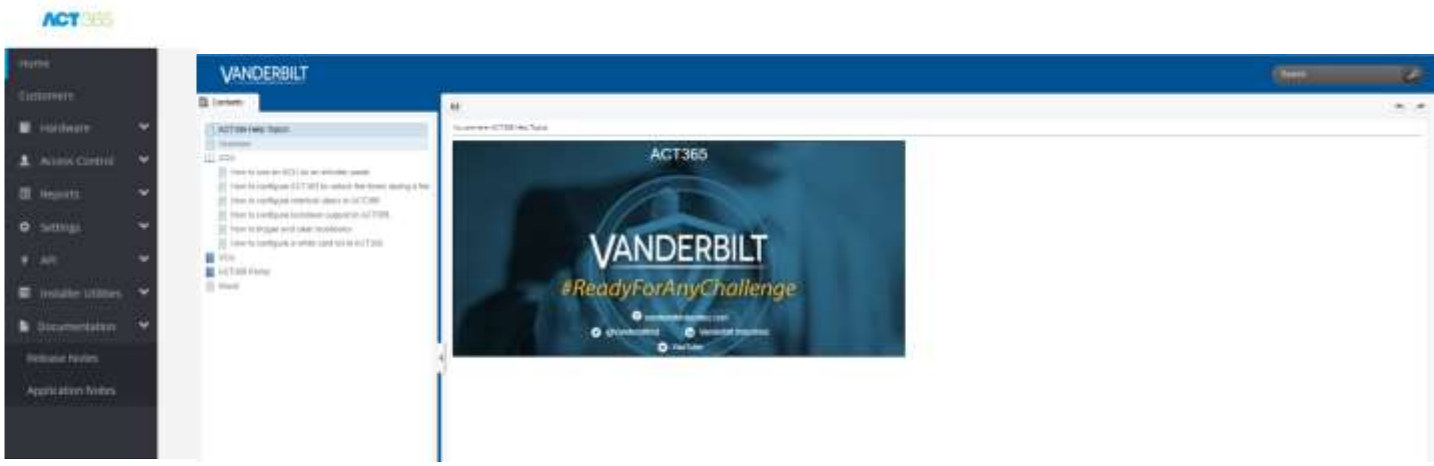
To configure a door so that it cannot be opened using a white card:

1. Go to the relevant customer portal in ACT365.
2. From the site picker, select the site for which you want to configure a door.
3. Click **Access Control > Doors**.
4. Click the **Name** of the door whose white card behavior you want to configure.
5. On the **Update Door** page, under **Operation**, select the **Deny White Card** checkbox.
6. Click **Save**.

5. Docs Portal

To assist our installer base, the introduction of the ACT365 Docs portal is available for any registered installer covering topics in ACT365. To access this Docs Portal, please follow these steps:

1. Log into ACT365 Portal
2. Under the Documentation menu, select Application Notes
3. This will redirect you to the Docs Portal covering multiple Documents (In English only for ACT365 1.3 release).



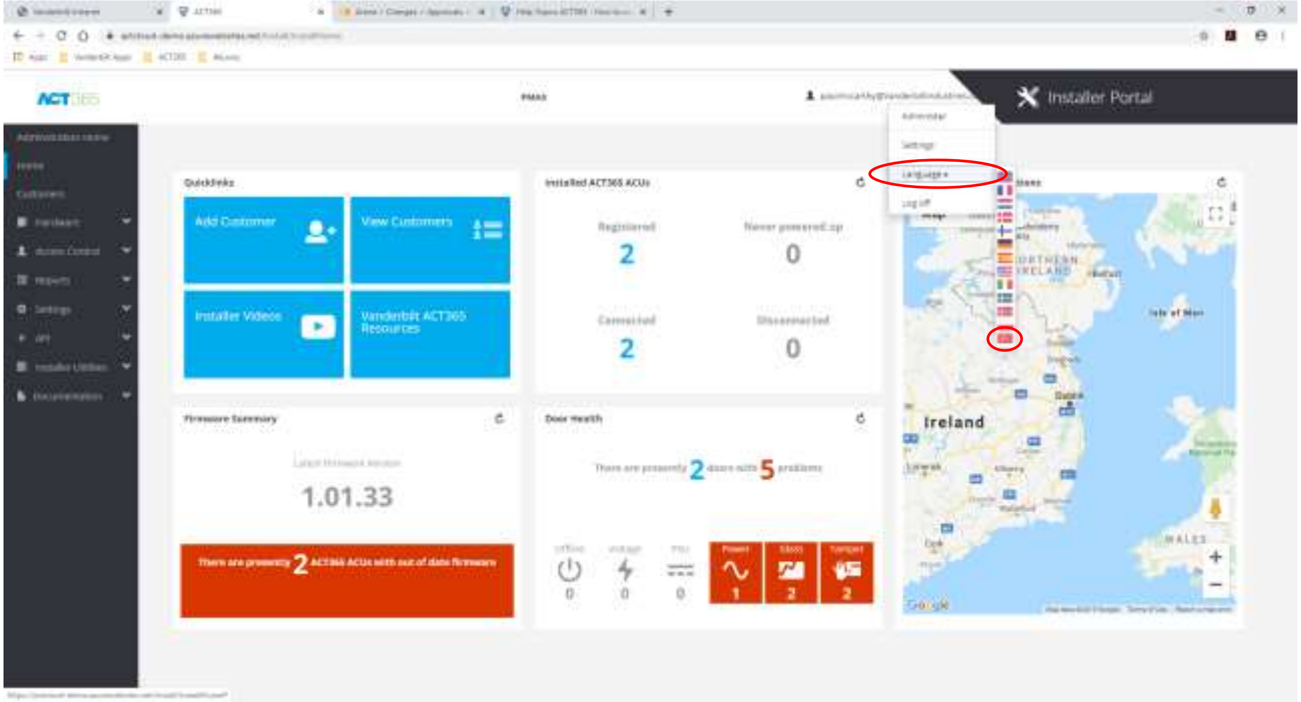
6. Turkish Language added

In the ACT365 1.3 release, we have introduced the Turkish language to the portal.

Configuring the Turkish Language:

1. Enter into the ACT365 Portal

2. Under the User drop-down menu, select Language and select the Turkish flag from the list of flags.



There are presently 2 ACT365 ACUs with out of date firmware

There are presently 2 doors with 5 problems

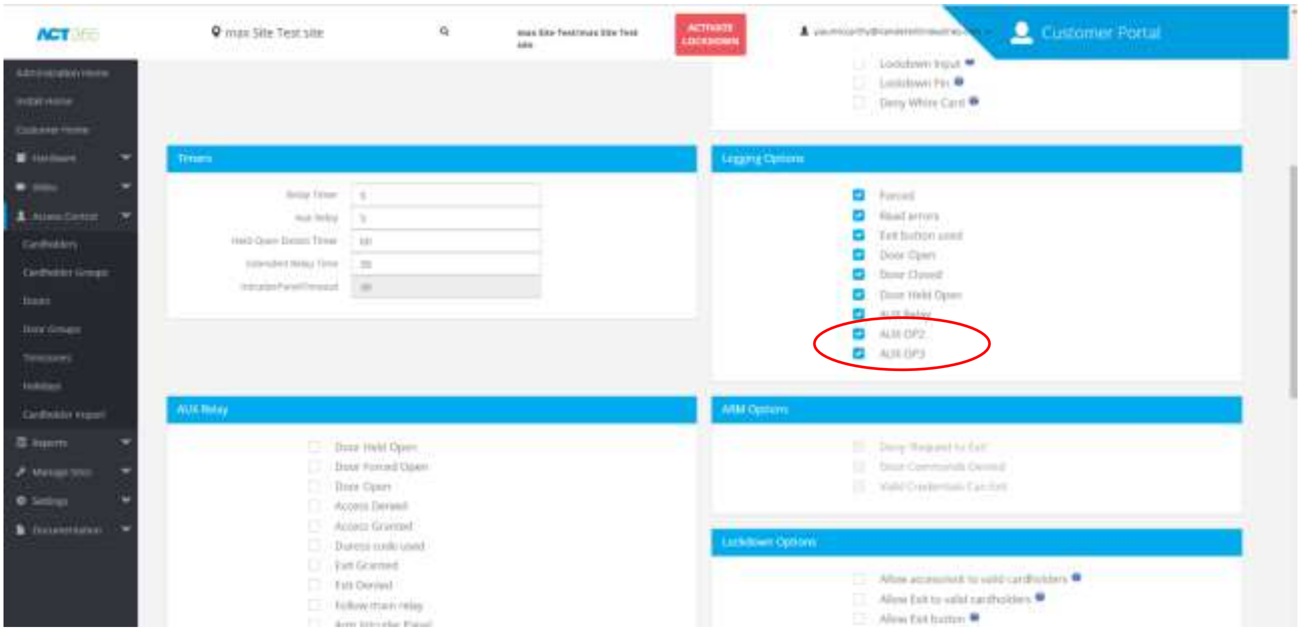
7. OP2 &OP3 Logging

In the ACT365 Release, it is now possible to log events for the output 2 and 3 from the ACT365 ACU. This will allow any device wired to the OP2 or OP3 to now capture a log event relating to these outputs. Once a device is activated, for example, external lighting, the event will now appear as a Log event in the ACT365 Portal.

Configuring OP2 And OP3 Log Events in ACT365:

1. Enter into the ACT365 Portal and select the Customer you wish to change
2. Go to Access Control>Doors>select the door you wish to configure
3. Enter the Update Doors Page
4. Under Logging Options check the Aux OP2 or OP3 Checkbox
5. You may also set the OP2 and OP3 Timed Actions
6. Click **Save.**

7. Any device activated that is wired to the OP2/OP3 outputs on the ACT365 portal will now create log events.



Timers

Relay Timer: 5
Aux Relay: 5
Held Open Detect Time: 10
Extended Relay Time: 35
IntruderPanelTimeout: 30

AUX Relay

□ Door Held Open
□ Door Forced Open
□ Door Open
□ Access Denied
□ Access Granted
□ Duress code used
□ Exit Granted
□ Exit Denied
□ Follow main relay
□ Arm Intruder Panel

□ Lockdown Input
□ Lockdown Pin
□ Deny White Card

Logging Options

☑ Forced
☑ Read errors
☑ Exit button used
☑ Door Open
☑ Door Closed
☑ Door Held Open
☑ AUX Relay
☑ AUX OP2
☑ AUX OP3

ARM Options

□ Deny Request to Exit
□ Door Commands Denied
□ Valid Credentials Can Exit

Lockdown Options

□ Allow access/exit to valid cardholders
□ Allow Exit to valid cardholders
□ Allow Exit button