PRODUCT RELEASE

PRODUCT LINE:	ACCESS		
PRODUCT:	ACT Enterprise		
MODEL/Version:	2.10	**CATEGORY:**	UPDATE
CONTACT:	Local Technical Support	**DATE:**	2019-10-29

This document refers to **ACT Enterprise** 2.10 or later.

The following is a list of new features and improvements included with **ACT Enterprise** 2.10. Some features require the associated controller firmware which is shipped with the **ACT Enterprise** installation package (Note: the ACTpro-100 door station cannot be firmware updated).

Contents

Bluetooth Reader/Credentials:

ACT Enterprise supports the use of Bluetooth credentials with Bluetooth readers sold by Vanderbilt.

Prerequisite:

- **ACT Enterprise** or **ACT Enterprise Lite** (free version) **2.10** or later.
- Only Bluetooth readers sold by Vanderbilt are supported.
- Successfully Installed Wiegand or OSDP Bluetooth readers from Vanderbilt.
- Bluetooth Credential license successfully installed in **ACT Enterprise**. The software is shipped with one free license.

List of supported Bluetooth readers:

Material Number	Material Description
P54508-P124-A100	ACTE-BT Bluetooth License
N54504-Z160-A100	BLUE-A Bluetooth Reader, Wiegand
N54504-Z161-A100	BLUE-B Bluetooth Reader, Wiegand, Keypad
N54504-Z162-A100	BLUE-C Bluetooth Reader, OSDP
N54504-Z163-A100	BLUE-D Bluetooth Reader, OSDP, Keypad
*N54504-Z164-A100	BLUE-EX Door Exit Button

* BLUE-EX (N54504-Z164-A100) handsfree exit button (REX) and will work on any controller.

Important:

Review the **Bluetooth User Guide** and **VI Mobile ID** documents for a full description of how to configure and use Bluetooth credentials.

Step1: From **ACT Manage > Setting > Bluetooth**

- Enable **Activate Bluetooth Enrolment.**
- Enter the email address for the person (Administrator) managing and adding Bluetooth credentials to cardholders.
- Enter the duration in hours that the QR Code request shall live before it expires.
- Add the name of the organization.
- Click **Save.**

Step2: From **ACT Manage > Setting > SMTP**

- Enter the email server details so **ACT Enterprise** can send an email, Office 365 is used as this example.
- Click **Save.**
- Click **Send Test Email** to confirm ACT Enterprise is configured to send emails.

Step3: From **ACT Manage > Manage > Users > General**

- Add a valid email address. This is the email address to which an invitation is sent requesting a registration key from the "VI Mobile ID" App.
- Add a card number in the One-to-One field. This is the number the Bluetooth readers will report to the controller.
- Click **Save.**

Step4: From **ACT Manage > Manage > Users > Bluetooth**

- Click **Invite** to send an email to the card holder inviting them to create a Bluetooth credential.

Sample Email sent to card holder:
You have been invited to create a Bluetooth credential on your phone for ***Organization name****.*
Download the app called VI Mobile ID from the Vanderbilt app store account.
Go to Settings – Authorization.
Make an authorization request and send it to this address: adminuser@domain.com

Step5: From **ACT Manage > Manage > Users > Bluetooth**

- The administrator enters the code reported by the mobile app.
  Example code for reference : BTAN#97653612D8DA728CA9401594C6F18088A1CD4F4D00#13
- Click **Save.**

Biometric readers (ZKTeco):

ACT Enterprise supports ZKTeco readers (MA300 & SF420)

Prerequisite:

- Install **ACT Enterprise** or **ACT Enterprise Lite** (free version) 2.10 or later.
- Register a Biometric license. A single license is included free with ACT Enterprise
- Install ZKTeco biometric readers.
- Connect the ZKTeco reader directly to the Wiegand interface on the controller.
- Connect the IP network to the same routable IP network as the ACT Enterprise server (The ACT Enterprise server communicates directly with the ZKTeco biometric readers to transfer biometric templates).
- Install the USB enrollment reader device driver then install the ZKTeco USB enrollment reader.

List of supported Biometric readers:

Material Number	Material Description
P54508-P123-A100	ACTE-BIO Biometrics License (per reader)
N54504-Z152-A100	MA300 Access Control Fingerprint reader (MF)
N54504-Z151-A100	SF420 Access Control Fingerprint Reader (MF)
*N54504-Z150-A100	SLK20R USB Silk ID Fingerprint reader (enrollment readers)

*SLK20R Device drive shipped with ACT Enterprise installation and should be installed before attaching the USB enrollment reader.

Important: Review the Biometric section in the **user guide** for a full description of how to configure and use Biometric readers.

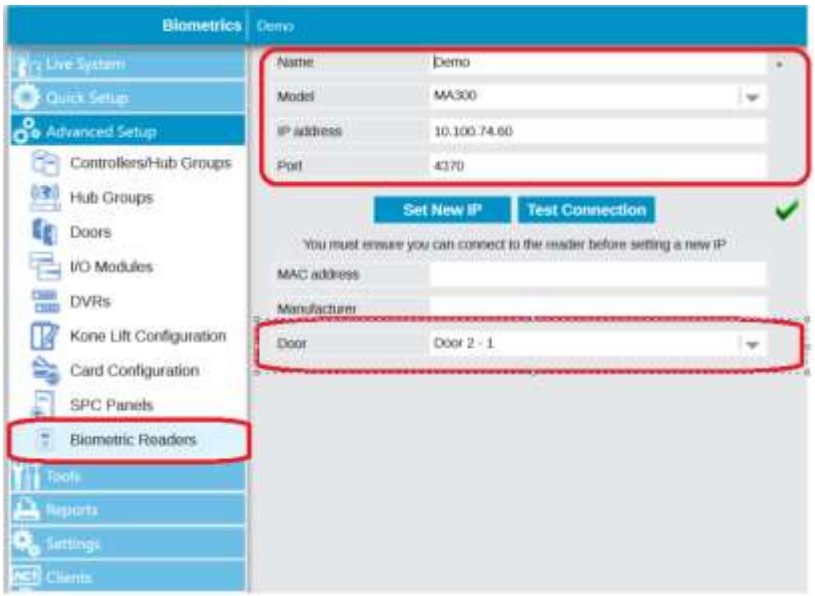
Step1: From **ACT Install > Settings > Biometrics**

Note: This step MUST be completed before adding biometric readers.

- Select the chosen biometric manufacturer.
- Enter the card number for the administrator card. If not set then administrator features are accessible on all ZKTeco devices with LCD display.
- Enter the PIN code that is used to link the Biometric readers to ACT Enterprise.

Step2: From **ACT Install > Advanced Setup > Biometric Readers**

- Select the Manufacture **Model** from the drop-down ***Note: all biometric readers must be from the same manufacturer.***
- Enter the **Name** (description) of the reader, the **IP address** and Port number that ACT Enterprise can use to communicate and send biometric templates to the device.
- Select the **Door** that will be associated with the biometric reader.



Step3: From **ACT Manage > Manage > Users > General**

- Enter Details for the User (name and usergroup).
- Select the biometric icon beside the Biometric field and follow the onscreen instructions.
- Click **Save.**

OSDP readers with encryption:

ACT Enterprise 2.10 or later supports Vanderbilt OSDP readers and OSDP readers from HID.

Prerequisite:

- **ACT Enterprise** or **ACT Enterprise Lite** (free version) 2.10 or later.
- ACTpro-1500 firmware version 1.08 or later.

Note:

- If upgrading from an earlier version of ACT Enterprise with OSDP readers already configured, the OSDP readers may have to be added again.
- OSDP readers are only supported on door 1 on an ACT1500-family controller.
- OSDP readers do not work on older controllers without the OSDP jumper. Refer to the controller installation guide for more information.
- To avoid address conflicts, connect and configure one OSDP reader at a time. Never connect multiple OSDP readers with matching addresses to a controller.
- If an OSDP reader is configured for encrypted communications and is removed from the ACT Enterprise infrastructure, it must be manually reset. Refer to the manufacturer's documentation for information on defaulting their OSDP readers.
- The OSDP encryption key cannot be changed or deleted while OSDP readers are in the database.
- Only OSDP readers from Vanderbilt and HID are supported by **ACT Enterprise**.

Step1: From **ACT Install > Advanced Setup > Controller > Operations**

- Enable **Support OSDP** on the controller. The controller should have 1.08 firmware or later installed.
- Click **Save.**

Step2: From **ACT Install > Advanced Setup > Doors > OSDP Readers**

- Select **Autodiscover**. This may take up to 2 minutes.
- Enable **Support OSDP** on the controller OSDP. The controller should have 1.08 firmware or later installed.
- Enter a name for each discovered OSDP reader.
- Enter a direction of travel (Entry or Exit) for each discovered OSDP readers.
- Click **Save.**

Note:

If upgrading from a previous version of ACT Enterprise with OSDP readers configured all OSDP readers mush have description and direction of travel reconfigured.

Usage Limits:

Usage limits allow organizations to limit the number of entry or exits events over a defined period. There are many scenarios where this can be used. An everyday use case is in a club scenario where the user purchases for example 10 accesses and when the 10th access is used the account is disabled.

Prerequisite:

- **ACT Enterprise 2.10** or later

Step1: From **ACT Manage > Settings > Usage Limits**

- Enable usage limits and configure as required.
- **Event Window (sec)** defines that only the first event in the defined **Event Window (sec)** window will be accepted. This prevents accidental double-badging.
- Define a door group that contains the door(s) that will be used for usage counting, usually entry or exit.

Step2: From **ACT Manage > Manage > User Groups > Usage Limit Settings**

By default, usergroups ignores usage limits until the "Usage Limits Ignore" flag is disabled. **All users in the usergroup will then have usage limits enabled unless explicitly disabled.**

If using tiered user limits per groups or category of people where each group has different limits.

- Define a user group per category, for example, Gold, Silver, Bronzes.
- From the **Usage Limit Settings**, assign the counter value associated with each user group. The usage limit behavior is defined in Step 1 above.
- **ACT Manage > Manage > Users,** assign the user to the appropriate user group.

Step3: From **ACT Manage > Manage > Users > Usage Limit Settings**

- Usage limits must be enabled in the user group and once enabled usage limits are enabled for all users in that user group unless explicitly disabled.
- Each user can be configured to ignore usage limits by enabling the **Usage Limits ignored** field.

Step4: From **ACT Manage > Manage > Users > General**

Usage limits can be reset manually per user. Enter the new value and press click **Reset**.

Notes:

If usage counters are configured for access, and if a user has 5 credits, then if the user enters 5 times and tries to exit they will be denied exit as their account is disabled after the 5th entry. In this scenario where entry and exit readers are used, it is recommended to give the user 10 credits and decrement on Access and Exit granted events. Select **Both entry and exit events** from **ACT Manage > Settings > Usage Limits > usage event types**.

Whitelisted cards:

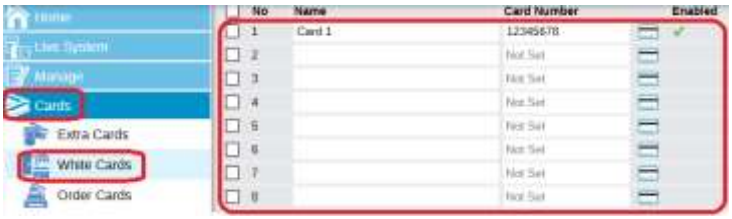
Whitelisted cards provide emergency services access and bypass all access control restrictions. The whitelisted cards are downloaded and stored on the controllers so they will grant access even if the controller is off line.

Prerequisite:

- **ACT Enterprise** 2.10 or later
- ACTpro-1500 firmware 1.08 or later
- ACTpro-4000 firmware 1.59 or later
- ACTpro-100 door station firmware 1.25 or later

Step1: From **ACT Manage > Cards > White Cards**

- Add up to 16 white cards, entering the name that will be reported and the number of the card.
- Note: The cards must be unique and not assigned to individual users.
- Click **SAVE**



Step2: From **ACT Manage > Manage > Doors**

- To exclude doors from supporting white cards enable the **Deny white card** field.
- Click **SAVE**

Unlock door on first access:

Doors can be configured to unlock during a timezone. It is possible that employees have not arrived into the office by the start of the timezone. This feature, if configured, requires that a valid access granted must be performed at the door before it will unlock for the configured timezone.

Prerequisite:

- **ACT Enterprise** 2.10 or later
- ACTpro-1500 firmware 1.08 or later
- ACTpro-4000 firmware 1.59 or later
- ACTpro-100 door station firmware 1.25 or later

Step1: From **ACT Manage > Manage > Doors > Actions**

- Assign a timezone to the **Unlock on first access** action. Care should be taken not to configure conflicting behavior and to ensure that timezones do not overlap. **Unlock Door** and **Unlock on first access** are conflicting.
- Click **SAVE**

Activate OP2 and OP3 on door forced and door ajar (left open) events:

Prerequisite:

- **ACT Enterprise** 2.10 or later
- ACTpro-1500 firmware 1.08 or later
- ACTpro-100 door stations firmware 1.21 or later

Step1: From **ACT Install > Advanced Setup > Doors > OP2 and OP3**

- Configure as required OP2 and OP3 to activate on door forced or door ajar (door left open) events.

Increase log events to 20,000:

Increase the number of log events stored on the ACTpro-1500 controller from 5,000 to 20,000

Prerequisite:

- ACTpro-1500 firmware 1.08 or later.

Increase the number of usergroups to 2,000:

Increase the number of user groups from 1,000 to 2,000

Prerequisite:

- **ACT Enterprise** 2.10 or later
- ACTpro-1500 firmware 1.08 or later
- ACTpro-4000 firmware 1.59 or later

Update to Finnish and Swedish language:

Update to Finnish and Swedish language added to **ACT Enterprise** 2.10

User locked out for 5 minutes if wrong Pin code used 5 times:

When using card and PIN, users are temporarily locked out for 5 minutes after 5 failed attempts with their PIN.

Prerequisite:

- **ACT Enterprise** 2.10 or later
- ACTpro-1500 firmware 1.08 or later
- ACTpro-100 door station firmware 1.25 or later

Relay resets immediately when door toggled closed:

If a door is toggled open, when toggled closed the relay changes state immediately.

Prerequisite:

- **ACT Enterprise** 2.10 or later
- ACTpro-1500 firmware 1.08 or later
- ACTpro-4000 firmware 1.59 or later
- ACTpro-100 door station firmware 1.08 or later

Support for Assa Aperio Version 2 locks:

Support has been added for Assa Aperio version 2 locks, which are replaced by the current V3 Aperio locks.

Prerequisite:

- ACTpro-1500 firmware 1.08 or later

Note:
Aperio Version 2 locks do not constantly communicate with the Aperio hub and require a trigger (presenting a card or pressing the handle) to initiate communication with the hub. When a command or door action is issued from the software the request will wait in the Aperio hub till the lock is triggered, in this scenario the card presented will be ignored.

Enhancement to ACT Enterprise license:

ACT Enterprise supports OSDP readers, Bluetooth and Biometric with ZK tech. **ACT Enterprise** includes one free Bluetooth credential and one free Biometric credential.

Reset rule engine counters:

ACT Enterprise 2.10 allows the operator to configure if counters are reset nightly. In previous versions, counters were automatically reset nightly.

Prerequisite:

- **ACT Enterprise** 2.10 or later

From **ACT Manage > Settings > General**

Enable “Reset rule counters to zero nightly” if you want all counters to reset nightly.

Note:
It is possible to use the rules engine to reset individual counters on a day and time decided by the operators. In the example, the CarPark counter increments when an access is granted and decrements when exit is granted. The CarPark counter is reset at midnight on Friday.