

PRODUKTLINIE: ZUTRITTSKONTROLLE

ARTIKEL: ACT Enterprise

MODELL/Version: 2.10 **KATEGORIE:** UPDATE

KONTAKT: Technischer Support **DATUM:** 29.10.2019

Das vorliegende Dokument bezieht sich auf **ACT Enterprise**, Version 2.10 oder höher.

Es beschreibt die neuen Funktionen und Verbesserungen von **ACT Enterprise 2.10**. Einige Funktionen erfordern die entsprechende Controller-Firmware, die im Lieferumfang des **ACT Enterprise** Installationspakets enthalten ist. (Hinweis: Die Firmware der Türstation ACTpro-100 kann nicht aktualisiert werden).

Inhalt

Bluetooth-Leser/Anmeldedaten: 2

Biometrische Leser (ZKTeco):..... 4

OSDP-Leser mit Verschlüsselung: 6

Nutzungsgrenzen:..... 8

Weißlisten-Karten: 10

Tür bei erstem Zutritt entriegeln:..... 11

OP2 und OP3 bei den Ereignissen „Tür aufgebrochen“ und „Tür offen“ (Tür offen gelassen) aktivieren:..... 11

Protokollereignisse auf 20.000 erhöhen: 12

Anzahl der Benutzergruppen auf 2000 erhöhen:..... 12

Update für Finnisch und Schwedisch..... 12

Nach 5-maliger Verwendung des falschen PIN-Codes wird der Benutzer 5 Minuten lang ausgesperrt:..... 12

Sofortiges Zurücksetzen des Relais, wenn die Tür auf geschlossen umgeschaltet wird: 12

Unterstützung von Schlössern des Typs Assa Aperio Version 2:..... 13

Verbesserung der ACT Enterprise Lizenz:..... 13

Zurücksetzen der Zähler des Regelverarbeitungsmoduls:..... 13

Bluetooth-Leser/Anmeldedaten:

ACT Enterprise unterstützt die Verwendung von Bluetooth-Anmeldedaten mit den Bluetooth-Lesern von Vanderbilt.

Voraussetzung:

- **ACT Enterprise** oder **ACT Enterprise Lite** (kostenlose Version) **2.10** oder höher.
- Es werden ausschließlich Bluetooth-Leser von Vanderbilt unterstützt.
- Erfolgreich installierte Wiegand- oder OSDP- Bluetooth-Leser von Vanderbilt.
- Prüfen Sie, dass der Controller ACTpro-1500 über die Firmware-Version **1.08** oder höher verfügt.
- Die Lizenz für Bluetooth-Anmeldedaten wurde erfolgreich in **ACT Enterprise** installiert. Die Software wird mit einer kostenlosen Lizenz geliefert.

Übersicht unterstützter Bluetooth-Leser:

Materialnummer	Materialbeschreibung
P54508-P124-A100	ACTE-BT Bluetooth-Lizenz
N54504-Z160-A100	BLUE-A Bluetooth-Leser, Wiegand
N54504-Z161-A100	BLUE-B Bluetooth-Leser, Wiegand, Tastatur
N54504-Z162-A100	BLUE-C Bluetooth-Leser, OSDP
N54504-Z163-A100	BLUE-D Bluetooth-Leser, OSDP, Tastatur
*N54504-Z164-A100	BLUE-EX Türöffnertaster

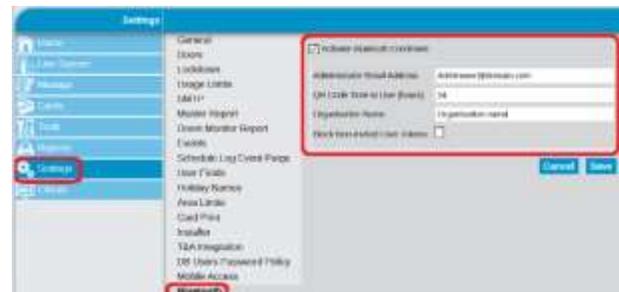
* BLUE-EX (N54504-Z164-A100) Hands-Free-Türöffnertaster (REX), der auf jedem Controller funktioniert.

Wichtig:

Lesen Sie die Dokumente **Bluetooth-Bedienungsanleitung** und **VI Mobile ID**, die ausführliche Informationen zur Konfiguration und Verwendung von Bluetooth-Anmeldedaten enthalten.

Schritt 1: **ACT Manage > Setting > Bluetooth** (ACT Manage > Einstellung > Bluetooth)

- **Activate Bluetooth Enrolment (Bluetooth-Einlernen aktivieren).**
- Geben Sie E-Mail-Adresse der Person (Administrator) ein, die die Bluetooth-Anmeldedaten verwaltet und den Karteninhabern hinzufügt.
- Geben Sie die Dauer in Stunden ein, die die QR-Code-Anfrage aktiv bleibt, bevor sie abläuft.
- Geben Sie den Namen der Organisation ein.
- Klicken Sie auf **Save (Speichern)**.



- Der Administrator gibt den von der mobilen App gemeldeten Code ein.
Beispielcode: BTAN#97653612D8DA728CA9401594C6F18088A1CD4F4D00#13



- Klicken Sie auf **Save** (Speichern).

Biometrische Leser (ZKTeco):

ACT Enterprise unterstützt Lesegeräte von ZKTeco (MA300 und SF420)

Voraussetzung:

- Installieren Sie **ACT Enterprise** oder **ACT Enterprise Lite** (kostenlose Version) 2.10 oder höher.
- Registrieren Sie eine biometrische Lizenz. Eine kostenlose Lizenz ist im Lieferumfang von ACT Enterprise enthalten
- Installieren Sie biometrische Leser von ZKTeco.
- Schließen Sie den Leser von ZKTeco direkt an die Wiegand-Schnittstelle des Controllers an.
- Verbinden Sie das IP-Netzwerk mit dem gleichen routbaren IP-Netzwerk wie den ACT Enterprise Server. (Der ACT Enterprise Server kommuniziert direkt mit den biometrischen Lesegegeräten von ZKTeco, um biometrische Vorlagen zu übermitteln).
- Installieren Sie den Treiber des USB-Einlernlesers und anschließend den USB-Einlernleser von ZKTeco.

Übersicht unterstützter biometrischer Leser:

Materialnummer	Materialbeschreibung
P54508-P123-A100	ACTE-BIO Biometrie-Lizenz (pro Leser)
N54504-Z152-A100	MA300 Fingerabdruckleser für die Zutrittskontrolle (MF)
N54504-Z151-A100	SF420 Fingerabdruckleser für die Zutrittskontrolle (MF)
*N54504-Z150-A100	SLK20R USB Silk ID Fingerabdruckleser (Personalisierungsleser)

* der Gerätetreiber für SLK20R ist im Lieferumfang der ACT Enterprise Installation enthalten und muss vor Anschluss des USB-Personalisierungslesers installiert werden..

Wichtig: Lesen Sie das Kapitel über biometrische Leser im **Benutzerhandbuch**, das eine umfassende Beschreibung der Konfiguration und Verwendung biometrischer Leser enthält.

Schritt 1: **ACT Install > Settings > Biometrics** (Install > Einstellungen > Biometrie)

Hinweis: Dieser Schritt MUSS abgeschlossen werden, bevor biometrische Leser hinzugefügt werden.

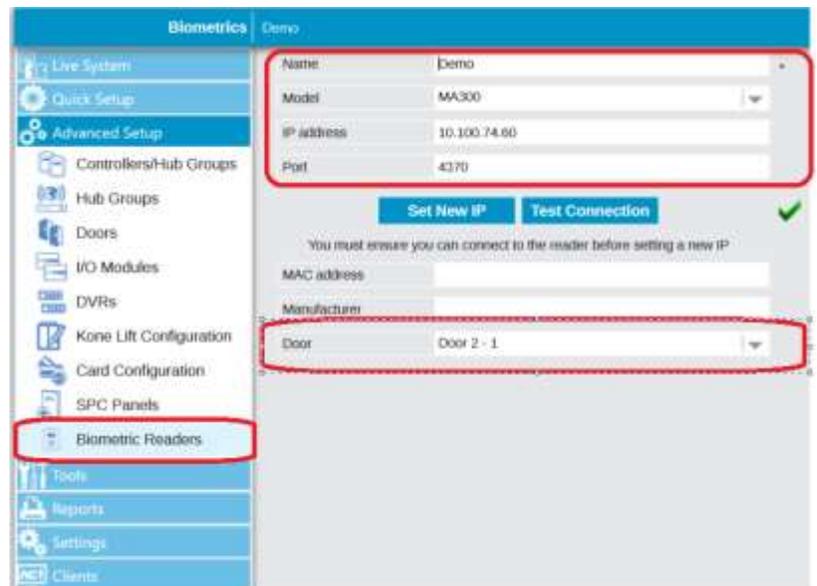
- Wählen Sie den ausgewählten Hersteller biometrischer Geräte.

- Geben Sie die Kartenummer der Administratorkarte ein. Ohne diese Einstellung stehen die Administratorfunktionen auf allen ZKTeco-Geräten mit LCD zur Verfügung.
- Geben Sie den PIN-Code für die Verknüpfung der biometrischen Leser mit ACT Enterprise ein.



Schritt 2: ACT Install > Advanced Setup > Biometric Readers (Install > Erweiterte Einrichtung > Biometrische Leser)

- Wählen Sie das **Modell** des Herstellers aus der Dropdownliste. **Hinweis: Alle biometrischen Leser müssen vom gleichen Hersteller stammen.**
- Geben Sie **Name** (Bezeichnung), **IP address** (IP-Adresse) und Port-Nummer des Lesers ein, den ACT Enterprise für die Kommunikation und das Senden biometrischer Vorlagen an das Gerät verwenden kann.
- Wählen Sie **Door** (die Tür, die mit dem biometrischen Leser verknüpft werden soll).



Schritt 3: ACT Manage > Manage > Users > General (Manage > Verwalten > Benutzer > Allgemein)

- Geben Sie Benutzerdetails an (Name und Benutzergruppe).

- Wählen Sie das biometrische Symbol neben dem Biometrie-Feld und folgen Sie den Anweisungen auf dem Bildschirm.
- Klicken Sie auf **Save** (Speichern).



OSDP-Leser mit Verschlüsselung:

ACT Enterprise 2.10 oder höher unterstützt OSDP-Leser von Vanderbilt und OSDP-Leser von HID.

Voraussetzung:

- **ACT Enterprise** oder **ACT Enterprise Lite** (kostenlose Version) 2.10 oder höher.
- ACTpro-1500 Firmware-Version 1.08 oder höher.

Hinweis:

- Bei einem Upgrade einer früheren Version von ACT Enterprise mit bereits konfigurierten OSDP-Lesern müssen die OSDP-Leser evtl. erneut hinzugefügt werden.
- OSDP-Leser werden nur an Tür 1 eines Controllers der ACT1500-Reihe unterstützt.
- Bei älteren Controllern ohne OSDP-Jumper funktionieren OSDP-Leser nicht. Weitere Informationen finden Sie im Installationsleitfaden zum Controller.
- Um Adressenkonflikte zu vermeiden, verbinden und konfigurieren Sie jeweils nur einen OSDP-Leser. Schließen Sie nie mehrere OSDP-Leser mit übereinstimmenden Adressen an einen Controller an.
- Wenn ein OSDP-Leser für verschlüsselte Kommunikationen konfiguriert ist und von der ACT Enterprise Infrastruktur entfernt wird, muss er manuell zurückgesetzt werden. Beachten Sie für das Zurücksetzen des OSDP-Lesers die technischen Unterlagen.
- Der OSDP-Verschlüsselungsschlüssel kann nicht geändert oder gelöscht werden, wenn die Datenbank OSDP-Leser enthält.
- **ACT Enterprise** unterstützt nur OSDP-Leser von Vanderbilt und HID.

Schritt 1: **ACT Install > Advanced Setup > Controller > Operations** (Install > Erweiterte Einrichtung > Controller > Vorgänge)

- **Support OSDP** (OSDP-Unterstützung) am Controller aktivieren. Auf dem Controller muss die Firmware 1.08 oder höher installiert sein.
- Klicken Sie auf **Save** (Speichern).



Schritt 2: **ACT Install > Advanced Setup > Doors > OSDP Readers** (ACT Install > Erweiterte Einrichtung > Türen > OSDP-Leser)

- Wählen Sie **Autodiscover** (AutoEntdeckung). Dies kann bis zu 2 Minuten dauern.
- Aktivieren Sie **Support OSDP** (OSDP-Unterstützung) am Controller-OSDP. Auf dem Controller muss die Firmware 1.08 oder höher installiert sein.
- Geben Sie einen Namen für jeden erkannten OSDP-Leser ein.
- Geben Sie für alle erkannten OSDP-Leser eine Richtung ein (Ein- oder Ausgang).
- Klicken Sie auf **Save** (Speichern).

Hinweis:

Bei Upgrades einer älteren Version von ACT Enterprise mit bereits konfigurierten OSDP-Lesern muss die Bezeichnung und Richtung für alle OSDP-Leser neu konfiguriert werden.



Nutzungsgrenzen:

Durch Nutzungsgrenzen können Unternehmen die Anzahl der Ein- oder Ausgänge für einen bestimmten Zeitraum begrenzen. Diese Funktion kann in zahlreichen Situationen eingesetzt werden. Ein Beispiel aus dem Alltag sind 10er-Karten für Clubs, deren Konto nach dem 10. Besuch deaktiviert wird.

Voraussetzung:

- **ACT Enterprise 2.10** oder höher

Schritt 1: **ACT Manage > Settings > Usage Limits** (ACT Manage > Einstellungen > Nutzungsgrenzen)

- Aktivieren und konfigurieren Sie Nutzungsgrenzen nach Bedarf.
- **Event Window (sec)** (Ereignisfenster (Sekunden)) legt fest, dass nur das erste Ereignis im festgelegten **Event Window (sec)** akzeptiert wird. So wird vermieden, dass sich jemand versehentlich doppelt anmeldet.
- Bestimmen Sie eine Türgruppe, die die Tür(en) enthält, die für die Nutzungszählung verwendet wird (meist Ein- oder Ausgang)



Schritt 2: **ACT Manage > Manage > User Groups > Usage Limit Settings** (ACT Manage > Verwalten > Benutzergruppen > Einstellungen der Nutzungsgrenzen)

In der Standardeinstellung ignorieren Benutzergruppen Nutzungsgrenzen, bis der Merker “Usage Limits Ignore” („Nutzungsgrenzen ignorieren“) deaktiviert ist. **Dann sind für alle Benutzer in der Benutzergruppe Nutzungsgrenzen aktiviert, sofern keine ausdrückliche Deaktivierung erfolgt.**

Verwendung gestaffelter Benutzergruppen pro Personengruppe oder -kategorie, wenn jede Gruppe unterschiedliche Grenzen hat.

- Legen Sie eine Benutzergruppe pro Kategorie fest, beispielsweise Gold, Silber, Bronze.
- Ordnen Sie über die **Usage Limit Settings** (Einstellungen der Nutzungsgrenzen) den auf dem Regeltähler angezeigten Wert zu, der jeder Benutzergruppe zugeordnet wird. Das Verhalten für die Nutzungsgrenze ist oben in Schritt 1 definiert.
- Ordnen Sie den Benutzer über **ACT Manage > Manage > Users** (ACT Manage > Verwalten > Benutzer) der entsprechenden Benutzergruppe zu.



Schritt 3: **ACT Manage > Manage > Users > Usage Limit Settings** (ACT Manage > Verwalten > Benutzer > Einstellungen der Nutzungsgrenzen)

- Nutzungsgrenzen müssen in der Benutzergruppe aktiviert werden. Nach der Aktivierung werden Nutzungsgrenzen für alle Benutzer in dieser Benutzergruppe aktiviert, sofern keine ausdrückliche Deaktivierung erfolgt.
- Über das Feld **Usage Limits ignored** (Nutzungsgrenzen ignoriert) kann das Ignorieren von Nutzungsgrenzen für jeden Benutzer konfiguriert werden.



Schritt 4: **ACT Manage > Manage > Users > General** (Manage > Verwalten > Benutzer > Allgemein)

Nutzungsgrenzen können für jeden Benutzer manuell zurückgesetzt werden. Geben Sie den neuen Wert ein und klicken Sie auf **Reset** (Zurücksetzen).



Hinweise:

Sind für den Zutritt Nutzungszähler konfiguriert, gilt folgendes: Wenn ein Benutzer Berechtigungen für 5 Zutritte hat, dieses Recht 5 Mal nutzt und dann versucht, den Bereich zu verlassen, wird Ihm der Ausgang verweigert, da sein Konto nach dem 5. Eingang deaktiviert wird. In diesem Szenario mit Ein- und Ausgangslesern wird empfohlen, dem Benutzer 10 Zutrittsberechtigungen zu erteilen und diese für die Ereignisse „Zutritt gewährt“ und „Ausgang gewährt“ zu verringern. Wählen Sie **Both entry and exit events**



events (Sowohl Ein- als auch Austrittsereignisse) über den Menüpunkt **ACT Manage > Settings > Usage Limits > usage event types** (ACT Manage > Einstellungen > Nutzungsgrenzen > Nutzungsereignistypen).

Weißlisten-Karten:

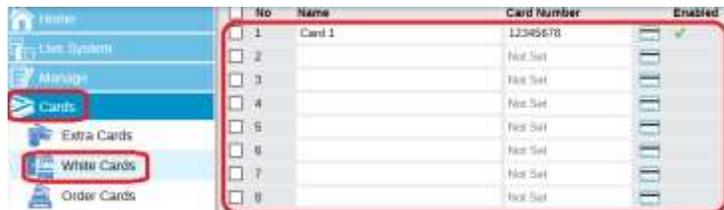
Weißlisten-Karten gewährleisten den Zutritt für Notfalldienste und umgehen alle Beschränkungen der Zutrittskontrolle. Die Weißlisten-Karten werden heruntergeladen und auf den Controllern gespeichert, um den Zutritt selbst dann zu gewähren, wenn der Controller offline ist.

Voraussetzung:

- **ACT Enterprise** 2.10 oder höher
- ACTpro-1500 Firmware 1.08 oder höher
- ACTpro-4000 Firmware 1.59 oder höher
- ACTpro-100 Türstation-Firmware 1.25 oder höher

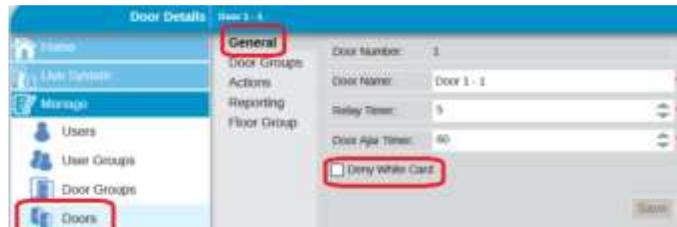
Schritt 1: **ACT Manage > Cards > White Cards** (ACT Manage > Karten > White Cards)

- Fügen Sie bis zu 16 White Cards hinzu und geben Sie den zu meldenden Namen und die Kartenummer ein.
- Hinweis: Die Karten dürfen jeweils nur einmal verwendet werden und keinen Einzelbenutzern zugewiesen sein.
- Klicken Sie auf **SAVE** (Speichern)



Schritt 2: **ACT Manage > Manage > Doors** (ACT Manage > Verwalten > Türen)

- Um für bestimmte Türen zu verhindern, dass White Cards verwendet werden können, aktivieren Sie das Feld **Deny white card** (White Card verweigern).
- Klicken Sie auf **SAVE** (Speichern)



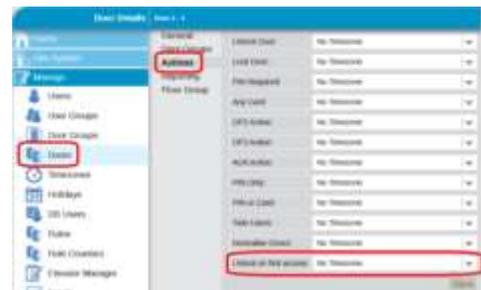
Tür bei erstem Zutritt entriegeln:

Türen können so konfiguriert werden, dass sie für eine bestimmte Zeitzone entriegelt werden. Es ist möglich, dass die Mitarbeiter beim Start der Zeitzone noch nicht im Büro angekommen sind. Ist diese Funktion konfiguriert, ist eine gültige Zutrittserlaubnis an der Tür erforderlich, damit sie für die konfigurierte Zeitzone entriegelt wird.

Voraussetzung:

- **ACT Enterprise 2.10** oder höher
- ACTpro-1500 Firmware 1.08 oder höher
- ACTpro-4000 Firmware 1.59 oder höher
- ACTpro-100 Türstation-Firmware 1.25 oder höher

Schritt 1: **ACT Manage > Manage > Doors > Actions** (ACT Manage > Verwalten > Türen > Vorgänge)



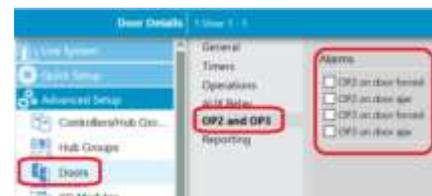
- Weisen Sie dem Vorgang **Unlock on first access** (Bei erstem Zutritt entriegeln) eine Zeitzone zu. Es ist darauf zu achten, dass kein widersprüchliches Verhalten konfiguriert wird und sich die Zeitzonen nicht überschneiden. **Unlock Door** (Tür entriegeln) und **Unlock on first access** (Bei erstem Zutritt entriegeln) sind widersprüchlich.
- Klicken Sie auf **SAVE** (Speichern)

OP2 und OP3 bei den Ereignissen „Tür aufgebrochen“ und „Tür offen“ (Tür offen gelassen) aktivieren:

Voraussetzung:

- **ACT Enterprise 2.10** oder höher
- ACTpro-1500 Firmware 1.08 oder höher
- ACTpro-100 Türstationen Firmware 1.21 oder höher

Schritt 1: **ACT Install > Advanced Setup > Doors > OP2 and OP3** (ACT Install > Erweiterte Einrichtung > Türen > OP2 und OP3)



- Konfigurieren Sie OP2 und OP3 nach Bedarf für die Aktivierung bei den Ereignissen „Tür aufgebrochen“ und „Tür offen gelassen“ .

Protokollereignisse auf 20.000 erhöhen:

Erhöhen der Anzahl der im Controller ACTpro-1500 gespeicherten Log Events von 5000 auf 20.000

Voraussetzung:

- ACTpro-1500 Firmware 1.08 oder höher.

Anzahl der Benutzergruppen auf 2000 erhöhen:

Erhöhen der Anzahl der Benutzergruppen von 1000 auf 2000

Voraussetzung:

- **ACT Enterprise** 2.10 oder höher
- ACTpro-1500 Firmware 1.08 oder höher
- ACTpro-4000 Firmware 1.59 oder höher

Update für Finnisch und Schwedisch

ACT Enterprise 2.10 umfasst ein Update für Finnisch und Schwedisch

Nach 5-maliger Verwendung des falschen PIN-Codes wird der Benutzer 5 Minuten lang ausgesperrt:

Bei der Verwendung von Karte und PIN werden die Benutzer nach 5 fehlgeschlagenen Versuchen mit ihrer PIN vorübergehend 5 Minuten lang ausgesperrt.

Voraussetzung:

- **ACT Enterprise** 2.10 oder höher
- ACTpro-1500 Firmware 1.08 oder höher
- ACTpro-100 Türstation-Firmware 1.25 oder höher

Sofortiges Zurücksetzen des Relais, wenn die Tür auf geschlossen umgeschaltet wird:

Wenn eine Tür von offen auf geschlossen umgeschaltet wird, wechselt das Relais sofort den Status.

Voraussetzung:

- **ACT Enterprise** 2.10 oder höher
- ACTpro-1500 Firmware 1.08 oder höher
- ACTpro-4000 Firmware 1.59 oder höher
- ACTpro-100 Türstation-Firmware 1.08 oder höher

Unterstützung von Schlössern des Typs Assa Apero Version 2:

Neu: Jetzt mit Unterstützung für Assa Apero Version 2 Schlösser, die durch die aktuellen V3 Apero Schlösser ersetzt werden.

Voraussetzung:

- ACTpro-1500 Firmware 1.08 oder höher

Hinweis:

Apero Version 2-Schlösser kommunizieren nicht ständig mit dem Apero-Hub und erfordern einen Auslöser (Vorzeigen einer Karte oder Drücken des Griffs), um die Kommunikation mit dem Hub einzuleiten. Wenn ein Befehl oder eine Türaktion von der Software ausgegeben wird, wartet die Anforderung im Apero-Hub, bis die Sperre ausgelöst wird. In diesem Szenario wird die vorgelegte Karte ignoriert.

Verbesserung der ACT Enterprise Lizenz:

ACT Enterprise unterstützt OSDP-Leser, Bluetooth- und biometrische Leser von ZK Tech. Der Lieferumfang von **ACT Enterprise** enthält für Bluetooth und biometrische Leser kostenlose Anmeldedaten für eine Person.

Zurücksetzen der Zähler des Regelverarbeitungsmoduls:

Mit **ACT Enterprise 2.10** kann der Benutzer konfigurieren, ob die Zähler jede Nacht zurückgesetzt werden sollen. In Vorversionen wurden die Zähler automatisch jede Nacht zurückgesetzt.

Voraussetzung:

- **ACT Enterprise 2.10** oder höher

ACT Manage > Settings > General (ACT Manage > Einstellungen > Allgemein)

Aktivieren Sie „Reset rule counters to zero nightly“ („Zähler automatisch jede Nacht zurücksetzen“), um die Zähler jede Nacht zurückzusetzen.



Hinweis:

Das Regelverarbeitungsmodul kann verwendet werden, um einzelne Zähler zu einem benutzerdefinierten Zeitpunkt (Tag und Uhrzeit) zurückzusetzen. Im Beispiel wird der Zähler des Parkhauses erhöht, wenn die Zufahrt genehmigt wird und verringert, wenn eine Ausfahrt genehmigt wird. Der Zähler des Parkhauses wird am Freitag um Mitternacht zurückgesetzt.

