

**GAMMA PRODOTTI:** CONTROLLO ACCESSI

**PRODOTTO:** ACT Enterprise

**MODELLO/Versione:** 2.10

**CATEGORIA:** AGGIORNAMENTO

**CONTATTO:** Assistenza tecnica locale

**DATA:** 29/10/2019

Questo documento si riferisce a **ACT Enterprise** versione 2.10 o successive.

La lista che segue è un elenco di tutte le nuove funzioni e miglioramenti inclusi in **ACT Enterprise 2.10**. Alcune di queste funzioni richiedono il firmware del controllore associato, che viene spedito con la confezione di installazione di **ACT Enterprise**. (Nota: il firmware della stazione porta ACTpro-100 non è aggiornabile).

## Indice

<b>Letture/credenziali Bluetooth:</b> .....	2
<b>Lettori biometrici (ZKTeco):</b> .....	4
<b>Lettori OSDP con crittografia:</b> .....	6
<b>Limiti di utilizzo:</b> .....	8
<b>Carte nella "lista bianca":</b> .....	10
<b>Sblocco porta al primo accesso:</b> .....	11
<b>Attivare OP2 e OP3 agli eventi porta forzata e porta socchiusa (lasciata aperta):</b> .....	11
<b>Registro eventi aumentato a 20.000:</b> .....	12
<b>Numero dei gruppi utenti portato a 2.000:</b> .....	12
<b>Aggiornamenti per la lingua svedese e il finnico</b> .....	12
<b>Utente bloccato per 5 minuti se viene immesso per 5 volte un PIN errato:</b> .....	12
<b>Il relè si azzerà immediatamente quando la porta commuta su chiuso:</b> .....	12
<b>Supporto per le serrature Assa Aperio Versione 2:</b> .....	13
<b>Aggiunte alla licenza ACT Enterprise:</b> .....	13
<b>Reset contatori del motore di regole:</b> .....	13

## Lettore/credenziali Bluetooth:

**ACT Enterprise** supporta l'uso di credenziali Bluetooth tramite i lettori Bluetooth venduti da Vanderbilt.

### Prerequisiti:

- **ACT Enterprise** o **ACT Enterprise Lite** (versione gratuita) in versione **2.10** o successiva.
- Solo i lettori Bluetooth venduti da Vanderbilt sono supportati.
- Lettori Bluetooth OSDP o Wiegand forniti da Vanderbilt correttamente installati.
- Assicurarsi che il controllore ACTpro-1500 abbia firmware di versione **1.08** o successiva.
- Licenza per le credenziali Bluetooth correttamente installata in **ACT Enterprise**. Il software include una licenza gratuita.

### Elenco dei lettori Bluetooth supportati:

Numero materiale	Descrizione materiale
P54508-P124-A100	ACTE-BT, licenza Bluetooth
N54504-Z160-A100	BLUE-A, lettore Bluetooth, Wiegand
N54504-Z161-A100	BLUE-B, lettore Bluetooth, Wiegand, Tastiera
N54504-Z162-A100	BLUE-C, lettore Bluetooth, OSDP
N54504-Z163-A100	BLUE-D, lettore Bluetooth, OSDP, Tastiera
*N54504-Z164-A100	BLUE-X, pulsante apertura porta

\* BLUE-EX (N54504-Z164-A100), pulsante apri porta a mani libere (REX) utilizzabile con qualunque controllore.

### Importante:

Fare riferimento alla **Guida Utente Bluetooth** e alla documentazione **VI Mobile ID** per una descrizione completa della procedura di configurazione e uso delle credenziali Bluetooth.

Passo 1: in **ACT Manage > Setting > Bluetooth** (ACT Manage > Impostazioni > Bluetooth)

- Attivare **Activate Bluetooth Enrolment** (Attiva registrazione Bluetooth).
- Immettere l'indirizzo email della persona (Amministratore) responsabile per gestione e aggiunta delle credenziali Bluetooth per i titolari delle carte.
- Immettere la durata in ore dalla creazione alla scadenza della richiesta del Codice QR.
- Aggiungere il nome dell'organizzazione.
- Cliccare su **Save** (Salva).





Esempio di codice per riferimento: BTAN#97653612D8DA728CA9401594C6F18088A1CD4F4D00#13

- Cliccare su **Save** (Salva).



## Lettori biometrici (ZKTeco):

ACT Enterprise supporta i lettori ZKTeco (MA300 & SF420)

### Prerequisiti:

- **ACT Enterprise** o **ACT Enterprise Lite** (versione gratuita) in versione 2.10 o successiva.
- Registrare una licenza biometrica. Un licenza singola è inclusa gratuitamente con ACT Enterprise.
- Installare i lettori biometrici ZKTeco.
- Collegare il lettore ZKTeco direttamente all'interfaccia Wiegand sul controllore.
- Collegare la porta Ethernet del lettore sulla stessa rete IP instradabile del server ACT Enterprise (il server ACT Enterprise comunica direttamente con i lettori biometrici ZKTeco per il trasferimento dei modelli biometrici).
- Installare il driver del dispositivo lettore di registrazione USB, quindi installare il lettore di registrazione USB ZKTeco.

### Elenco dei lettori biometrici supportati:

Numero materiale	Descrizione materiale
P54508-P123-A100	ACTE-BIO, licenza biometrica (per lettore)
N54504-Z152-A100	MA300, lettore di impronte digitali per controllo accessi (MF)
N54504-Z151-A100	SF420, lettore di impronte digitali per controllo accessi (MF)
*N54504-Z150-A100	SLK20R, lettore di impronte digitali USB Silk ID (lettori di registrazione)

\*I driver dei dispositivi SLK20R sono spediti insieme con l'installazione di ACT Enterprise e vanno installati prima di aggiungere i lettori di registrazione USB.

Importante: consultare la sezione Biometrica nella **guida utente** per la descrizione completa della procedura di configurazione e uso dei lettori biometrici.

Passo 1: in ACT **Install > Settings > Biometrics** (ACT Install > Impostazioni > Biometrica)

**Nota: questo passaggio DEVE essere completato prima di aggiungere i lettori biometrici.**

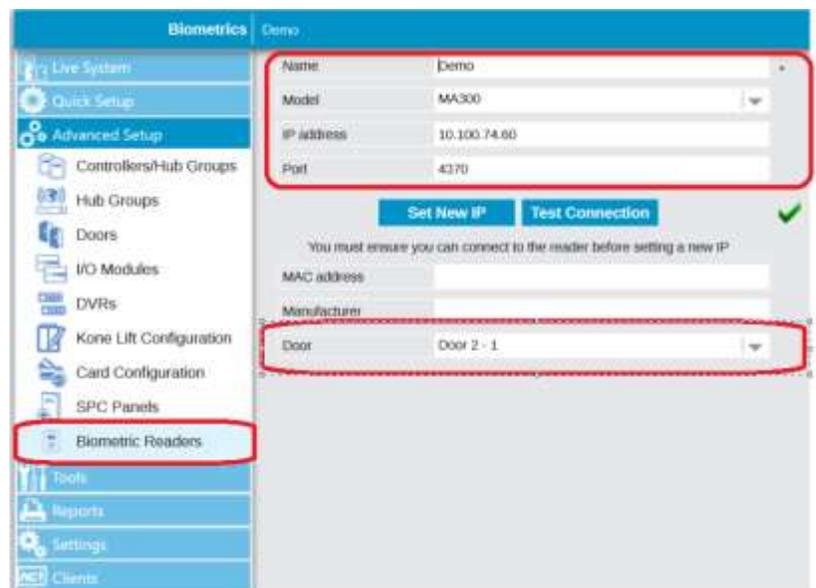
- Scegliere il fabbricante del lettore biometrico.

- Immettere il numero della carta per la carta dell'amministratore. Se non configurate, le funzioni amministratore sono accessibili su tutti i dispositivi ZKTeco con LCD.
- Immettere il codice PIN utilizzato per collegare i lettori biometrici a ACT Enterprise.



Passo 2: In ACT **Install** > **Advanced Setup** > **Biometric Readers** (ACT Install > Configurazione avanzata > Lettori biometrici)

- Selezionare il **Modello** dal menu a tendina. *Nota: tutti i lettori biometrici devono essere dello stesso fabbricante.*
- Immettere il **Nome** (descrizione) del lettore, l'**indirizzo IP** e il numero di porta che ACT Enterprise utilizzerà per comunicare e inviare i template biometrici al dispositivo.
- Selezionare la **Door** (Porta) da associare al lettore biometrico.



Passo 3: in ACT **Manage** > **Manage** > **Users** > **General** (ACT Manage > Gestisci > Utenti > Generale)

- Immettere i dettagli dell'utente (nome e gruppo utenti).

- Selezionare l'icona biometrica accanto al campo Biometrica e seguire le istruzioni a schermo.
- Cliccare su **Save** (Salva).



## Lettori OSDP con crittografia:

ACT Enterprise 2.10 o versione successiva supporta i lettori OSDP di Vanderbilt e i lettori OSDP di HID.

### Prerequisiti:

- **ACT Enterprise** o **ACT Enterprise Lite** (versione gratuita) in versione 2.10 o successiva.
- ACTpro-1500 con firmware 1.08 o successivo.

### Nota:

- In caso di aggiornamento da una precedente versione di ACT Enterprise con lettori OSDP già configurati, i lettori OSDP devono essere aggiunti di nuovo.
- I lettori OSDP sono supportati solo sulla porta 1 dei controllori della famiglia ACT1500.
- I lettori OSDP non funzionano su controllori meno recenti privi di ponticello OSDP. Per maggiori informazioni, fare riferimento alla guida di installazione del controllore.
- Per evitare conflitti di indirizzo, collegare e configurare i lettori OSDP uno alla volta. Non collegare mai a un controllore più lettori OSDP con indirizzi corrispondenti.
- Il lettore OSDP configurato per comunicazione cifrata che viene rimosso dall'infrastruttura ACT Enterprise deve essere resettato manualmente. Consultare la documentazione del fabbricante per la procedura per il ripristino alle impostazioni di default dei loro lettori OSDP.
- La chiave di crittografia non può essere cambiata o cancellata mentre i lettori OSDP sono nel database.
- Solo i lettori OSDP di Vanderbilt e HID sono supportati da **ACT Enterprise**.

Passo 1: in **ACT Install > Advanced Setup > Controller > Operations** (ACT Install > Configurazione avanzata > Controllore > Operazioni)

- Abilitare **Support OSDP** (Supporta OSDP) sul controllore. Il firmware installato sul controllore deve essere di versione 1.08 o successiva.
- Cliccare su **Save** (Salva).



Passo 2: in **ACT Install > Advanced Setup > Doors > OSDP Readers** (ACT Install > Configurazione avanzata > Porte > Lettori OSDP)

- Selezionare **Autodiscover** (Rilevamento automatico). L'operazione può richiedere fino a 2 minuti.
- Abilitare **Support OSDP** (Supporta OSDP) sul controllore OSDP. Il firmware installato sul controllore deve essere di versione 1.08 o successiva.
- Immettere un nome per ciascuno dei lettori OSDP rilevati.
- Immettere una direzione di movimento (Ingresso o Uscita) per ciascuno dei lettori OSDP rilevati.
- Cliccare su **Save** (Salva).



**Nota:**

In caso di aggiornamento da una versione precedente di ACT Enterprise con lettori OSDP configurati, è necessario riconfigurare la descrizione e la direzione di movimento di tutti i lettori OSDP.

## Limiti di utilizzo:

I limiti di utilizzo consentono di limitare il numero di eventi in entrata o in uscita in un dato periodo. Ci sono molti scenari in cui questa funzione può essere utile. Un tipico caso è quello del club in cui l'utente acquista, per esempio, 10 accessi e quando viene utilizzato il decimo ingresso le credenziali di accesso vengono disabilitate.

### Prerequisiti:

- **ACT Enterprise 2.10** o successivo

Passo 1: in ACT **Manage > Settings > Usage Limits** (ACT Manage > Impostazioni > Limiti di utilizzo)

- Abilitare i limiti di utilizzo e configurarli come necessario.
- **Event Window (sec)** stabilisce che solo il primo evento che si verifica entro la **finestra eventi (sec)** definita sarà accettato. In questo modo si evita un doppio rilevamento delle credenziali.
- Indicare il gruppo porte che contiene la o le porte da usare per il conteggio degli utilizzi, in genere ingresso o uscita.



Passo 2: in ACT **Manage > Manage > User Groups > Usage Limits** (ACT Manage > Gestisci > Gruppi utenti > Limiti di utilizzo)

Per default, i gruppi utenti ignorano i limiti di utilizzo fino a quando il flag "Usage Limits Ignore" (Ignora limiti di utilizzo) non viene disabilitato. **Una volta attivati, i limiti di utilizzo si applicano a tutti gli utenti, a meno che non siano esplicitamente disattivati.**

Se vengono applicati limiti di utilizzo suddivisi in livelli per gruppo o per categoria di persone in cui ogni gruppo è soggetto a limitazioni differenti:

- Definire un gruppo di utenti per categoria, per esempio, Oro, Argento, Bronzo.
- Dal menu **Usage Limit Settings** (Impostazioni limiti di utilizzo), assegnare il valore del contatore associato con ciascun gruppo di utenti. Il comportamento dei limiti di utilizzo è definito nel Passo 1 più sopra.
- In ACT **Manage > Manage (Gestisci) > Users (Utenti)**, assegnare l'utente al gruppo di utenti appropriato.



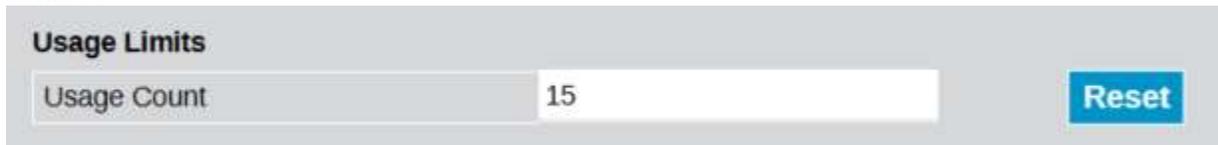
Passo 3: in ACT **Manage > Manage > Users > Usage Limits** (ACT Manage > Gestisci > Utenti > Limiti di utilizzo)

- I limiti di utilizzo devono essere abilitati nel gruppo utenti e, una volta abilitati, sono abilitati per tutti gli utenti del gruppo, a meno che non siano esplicitamente disabilitati.
- I singoli utenti possono essere configurati per ignorare i limiti di utilizzo abilitando il campo **Usage Limits ignored** (ignora limiti di utilizzo).



Passo 4: in ACT **Manage > Manage > Users > General** (ACT Manage Gestisci > Utenti > Generale)

I limiti di utilizzo possono essere reimpostati manualmente per i singoli utenti. Immettere il nuovo valore e fare clic su **Reset**.



**Note:**

Se i contatori di utilizzo sono configurati per l'accesso e se un utente ha 5 crediti, se l'utente entra 5 volte e cerca di uscire, l'uscita gli sarà negata, in quanto il suo account è disabilitato dopo il quinto ingresso. In questo scenario che prevede lettori di ingresso e uscita, si consiglia di assegnare all'utente 10 crediti da scalare a seguito di ogni evento di ingresso e uscita. Selezionare **Both entry and exit events** (Sia eventi di ingresso che di uscita) in ACT **Manage > Settings > Usage Limits > Usage event types** (Manage > Impostazioni > Limiti di utilizzo > Tipo enti utilizzo).



## Carte nella "lista bianca":

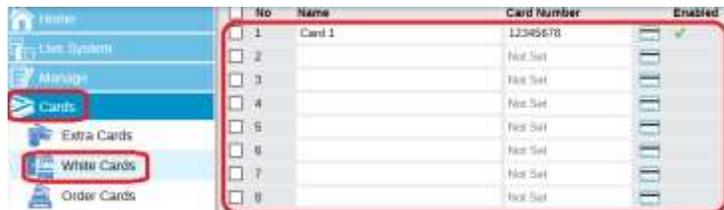
Le carte inserite nella "lista bianca" (whitelist) forniscono accesso per i servizi di emergenza e scavalcano tutte le restrizioni dei controlli di accesso. Le carte nella lista bianca sono scaricate e memorizzate nei controllori in modo da consentire l'accesso anche quando il controllore è offline.

### Prerequisiti:

- **ACT Enterprise 2.10** o successivo
- ACTpro-1500 con firmware 1.08 o successivo
- ACTpro-4000 con firmware 1.59 o successivo
- Stazione porta ACTpro-100 con firmware 1.25 o successivo

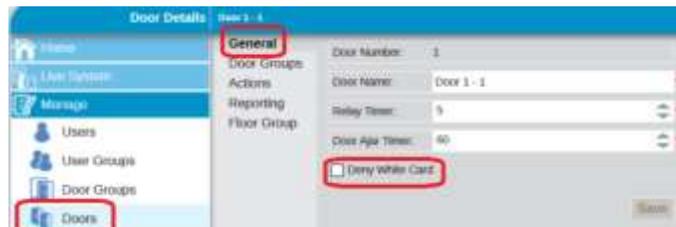
Passo 1: in ACT **Manage** > **Cards** > **White Cards** (ACT Manage > Carte > Carte bianche)

- È possibile aggiungere fino a 16 carte bianche, inserendo il nome di riferimento e il numero della carta.
- Nota: Le carte devono essere uniche e non assegnate a nessun utente individuale.
- Cliccare su **SAVE** (Salva)



Passo 2: in ACT **Manage** > **Manage** > **Doors** (ACT Manage > Gestisci > Porte)

- Per disattivare sulle porte il supporto per le schede bianche, abilitare il campo **Deny white card** (Nega schede bianche).
- Cliccare su **SAVE** (Salva)



## Sblocco porta al primo accesso:

Le porte possono essere configurate per rimanere sbloccate in una determinata fascia oraria. È possibile che i dipendenti non siano ancora arrivati in ufficio quando la fascia oraria inizia. Questa funzione, se configurata, fa in modo che lo sblocco della porta avvenga solo dopo il primo accesso valido che si registra durante la fascia oraria.

### Prerequisiti:

- **ACT Enterprise 2.10** o successivo
- ACTpro-1500 con firmware 1.08 o successivo
- ACTpro-4000 con firmware 1.59 o successivo
- Stazione porta ACTpro-100 con firmware 1.25 o successivo

Passo 1: Da ACT **Manage > Manage > Doors > Actions ACT** (Manage > Gestisci > Porte > Azioni)

- Assegnare una fascia oraria all'azione **Unlock on first access** (Sblocca al primo accesso). Bisogna prestare attenzione a non configurare profili di azione conflittuali e ad assicurare che le fasce orarie non si sovrappongano. **Unlock Door** (Sblocca porta) e **Unlock on first access** (Sblocca al primo accesso) creano conflitto.
- Cliccare su **SAVE** (Salva)



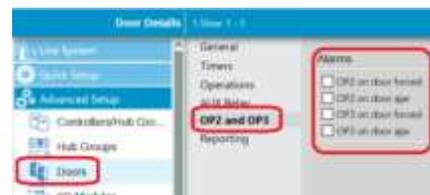
## Attivare OP2 e OP3 agli eventi porta forzata e porta socchiusa (lasciata aperta):

### Prerequisiti:

- **ACT Enterprise 2.10** o successivo
- ACTpro-1500 con firmware 1.08 o successivo
- Stazioni porta ACTpro-100 con firmware 1.21 o successivo

Passo 1: in ACT **Install > Advanced Setup > Doors > OP2 and OP3** (ACT Install > Configurazione avanzata > Porte > OP2 e OP3)

- Configurare OP2 e OP3 attivati a seguito degli eventi porta forzata e porta socchiusa (lasciata aperta).



## Registro eventi aumentato a 20.000:

Il numero di eventi che è possibile registrare sul controllore ACTpro-1500 passa da 5.000 a 20.000

### Prerequisiti:

- ACTpro-1500 con firmware 1.08 o successivo.

## Numero dei gruppi utenti portato a 2.000:

Il numero dei gruppi utenti è stato portato da 1.000 a 2.000

### Prerequisiti:

- **ACT Enterprise 2.10** o successivo
- ACTpro-1500 con firmware 1.08 o successivo
- ACTpro-4000 con firmware 1.59 o successivo

## Aggiornamenti per la lingua svedese e il finnico

Aggiornamenti per la lingua svedese e il finnico sono stati apportati a **ACT Enterprise 2.10**

## Utente bloccato per 5 minuti se viene immesso per 5 volte un PIN errato:

Quando si utilizzano carte e PIN, gli utenti vengono temporaneamente bloccati per 5 minuti dopo 5 tentativi falliti di inserimento del PIN.

### Prerequisiti:

- **ACT Enterprise 2.10** o successivo
- ACTpro-1500 con firmware 1.08 o successivo
- Stazione porta ACTpro-100 con firmware 1.25 o successivo

## Il relè si azzerà immediatamente quando la porta commuta su chiuso:

Quando la porta commutata su chiusa commuta su aperto, il relè cambia immediatamente stato.

### Prerequisiti:

- **ACT Enterprise 2.10** o successivo
- ACTpro-1500 con firmware 1.08 o successivo
- ACTpro-4000 con firmware 1.59 o successivo
- Stazione porta ACTpro-100 con firmware 1.08 o successivo

## Supporto per le serrature Assa Aperio Versione 2:

Supporto è stato aggiunto per le serrature Assa Aperio versione 2, che sono sostituite dalle serrature correnti Aperio V3.

### Prerequisiti:

- ACTpro-1500 con firmware 1.08 o successivo

### Nota:

Le serrature Aperio versione 2 non comunicano costantemente con l'hub Aperio e richiedono un trigger (presentazione di una scheda o pressione della maniglia) per avviare la comunicazione con l'hub. Quando un comando o un'azione della porta viene inviata dal software, la richiesta attenderà nell'hub di Aperio fino all'attivazione della serratura, in questo scenario la scheda presentata verrà ignorata.

## Aggiunte alla licenza ACT Enterprise:

**ACT Enterprise** supporta i lettori OSDP, Bluetooth e Biometrici con tecnologia ZK. **ACT Enterprise** include una credenziale Bluetooth gratuita e una credenziale Biometrica gratuita.

## Reset contatori del motore di regole:

**ACT Enterprise** 2.10 consente all'operatore di impostare se i contatori devono essere resettati ogni notte. Nelle versioni precedenti i contatori venivano resettati automaticamente ogni notte.

### Prerequisiti:

- **ACT Enterprise 2.10** o successivo

Da **ACT Manage > Settings > General** (ACT Manage > Impostazioni > Generale)

Abilitare "Reset rule counters to zero nightly" se si desidera azzerare i contatori delle regole ogni notte.



**Nota:**

È possibile usare il motore delle regole per azzerare singoli contatori alla data e all'ora decise dall'operatore. Nell'esempio, il contatore del parcheggio è incrementato quando l'accesso è consentito e decrementato quando è consentita l'uscita. Il contatore del parcheggio è azzerato alla mezzanotte di venerdì.

