BioStar v1.61
Guida Amministratore

BIOMETRIC TECHNOLOGIES

Contenuti

Contenuti

Contenuti

Contenuti

Contenuti

Contenuti

Contenuti

Contenuti

Contenuti

Contenuti

Contenuti

Contenuti

Warranty and Disclaimers

Suprema Warranty Policy

Suprema warrants to Buyer, subject to the limitations set forth below, that each product shall operate in substantial accordance with the published specifications for such product for a period of one (1) year from the date of shipment of products ("Warranty Period"). If Buyer notifies Suprema in writing within the Warranty Period of any defects covered by this warranty, Suprema shall, at its option, repair or replace the defective product that is returned to Suprema within the Warranty Period, with freight and insurance prepaid by Buyer. Such repair or replacement shall be Suprema's exclusive remedy for breach of warranty with respect to the Product. This limited warranty shall not extend to any product that has been: (i) subject to unusual physical or electrical stress, misuse, neglect, accident or abuse, or damaged by any other external causes; (ii) improperly repaired, altered or modified in any way unless such modification is approved in writing by the Supplier; (iii) improperly installed or used in violation of instructions furnished by Suprema.

Suprema shall be notified in writing of defects in the RMA (Return Material Authorization) report supplied by Suprema not later than thirty days after such defects have appeared and at the latest one year after the date of shipment of the Product. The report should include full details of each defective product, model number, invoice number, and serial number. No product without an RMA number issued by Suprema may be accepted and all defects must be reproducible for warranty service.

Except as expressly provided herein, the products are provided "as is" without warranty of any kind, either express or implied, including, but not limited to, warranties or merchantability and fitness for a particular purpose.

Disclaimers

The information in this document is provided in connection with Suprema products. No license, express or implied, by estoppels or otherwise, to any intellectual property rights is granted by this document, except as provided in Suprema's Terms and Conditions of Sale for such products.

Suprema assumes no liability whatsoever and Suprema disclaims any express or implied warranty, relating to sale and/or use of Suprema products, including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright, or other intellectual property right.

Suprema products are not intended for use in medical, life saving, or life sustaining applications or other applications in which the failure of the Suprema product could create a situation where personal injury or death may occur. Should Buyer purchase or use Suprema products for any such unintended or unauthorized application, Buyer shall indemnify and hold Suprema and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Suprema was negligent regarding the design or manufacture of the part.

Suprema reserves the right to make changes to specifications and product descriptions at any time without notice to improve reliability, function, or design. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Supreme reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

Please contact Suprema, local Suprema sales representatives or local distributors to obtain the latest specifications before placing your order.

Copyright Notice

01 Sistema BioStar

BioStar è la nuova generazione dei sistemi di controllo accessi, basato sulla connettività IP e la sicurezza biometrica. La maggior parte dei dispositivi integra scanner per impronte e lettori di carta per molteplici livelli di autenticazione per l'utente. I dispositivi biometrici, installati su ogni porta, funzionano non solo come lettori di carte o impronte, ma anche come controller intelligenti.

La versione BioStar con licenza standard è attivabile tramite chiave USB. Senza la chiave, BioStar funziona normalmente, ma ha una capacità operativa limitata. Attivando la licenza, BioStar offre grande versatilità e funzioni aggiuntive, come mostrato in tabella:

	Versione standard	Versione free
Massimo # porte	512	20
Massimo # clienti	32	2
Supporta zone	Si	No
Notifiche via E-mail	Si	No
Server matching	Si	No
Passaggi	Giornaliero e settimanale	Solo settimanale
IO	Si	No
Mappa	Si	No

BioStar V1.61 supporta i seguenti dispositivi:

- **BioStation (V1.5 o successiva)** - BioStation è un terminale multifunzionale con tastiera e monitor LCD da 2.5" che permette di effettuare le registrazioni degli utenti e l'utilizzo delle funzioni di amministrazione direttamente dal dispositivo.

1. Sistema BioStar

BioStation può essere conneso ad una rete tramite LAN wireless LAN o Ethernet e include host USB e interfacce dispositivo per un trasferimento rapido di dati. Il modello BioStation MIFARE (BSM) supporta anche l'opzione Smart Card.

- **BioStation T2** – BioStation T2 è un terminale di controllo accessi IP multifunzionale, dotato di fotocamera, touchscreen da 5", scanner per impronta, lettore di carte e videotelefono integrato.

- **D-Station** - D-Station è un terminale di controllo accessi IP multifunzione, dotato di fotocamera, touchscreen e doppio scanner per impronte, che permette più combinazioni di autorizzazione tramite riconoscimento impronta (singola o doppia), carte d'accesso MIFARE, ID utenti e riconoscimento del volto. D-Station può essere alimentata tramite connessione Ethernet per eliminare la necessità di ulteriori cablaggi o alimentazioni.

- **FaceStation** – FaceStation è un terminale di controllo accessi IP multifunzionale, dotato di schermo LCD e fotocamera per il riconoscimento del volto e delle funzioni di videotelefono. FaceStation supporta più interfacce per la connessione ai computer o alle reti e al controllo accessi tramite Wiegand o porte I/O. In aggiunta, il dispositivo permette l'autorizzazione tramite più carte d'accesso.

- **BioEntry Plus (V1.2 o successiva)** - BioEntry Plus è un dispositivo di controllo accessi IP che include il riconoscimento delle impronte e l'accesso tramite carta. Il dispositivo può essere controllato in modo indipendente tramite carte o BioStar. BioEntry Plus può essere connesso ad una serratura elettrica tramite un relè interno, oppure utilizzato con il dispositivo Secure I/O per garantire una maggior sicurezza e una capacità maggiore.

- **BioEntry W** – BioEntry W include tutte le caratteristiche del dispositivo BioEntry Plus in una struttura antivandalica e IP65. BioEntry W è ideale per le installazioni in esterno, poiché garantisce un'eccezionale resistenza agli ambienti più difficili. È dotato di interfacce di comunicazione estese e capacità PoE.

- **BioLite Net (V1.0 or later)** - BioLite Net è un dispositivo IP per il riconoscimento delle impronte, progettato per un'installazione esterna. La resistente struttura IP65 offre una resistenza superiore agli agenti atmosferici. Può essere utilizzato come semplice controller per una porta, oppure come parte di un complesso sistema in rete. BioLite Net supporta tutte le

1. Sistema BioStar

funzionalità garantite dal sistema di controllo presenze e controllo accessi BioStar.

- **Xpass** - Xpass è un lettore/controller IP progettato esclusivamente per le carte RF. È dotato di funzioni molto simili al dispositivo BioEntry Plus, resistente all'acqua per uso esterno e con la possibilità di collegarlo e alimentarlo tramite un singolo cavo CAT5/6.

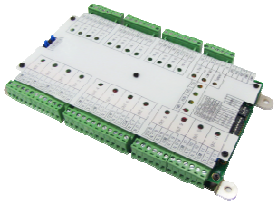
- **Xpass Slim** - Il dispositivo XPass Slim è una versione più sottile dell'Xpass che supporta carte FeliCa e ISO 15693. Grazie al profilo molto sottile, è possibile installarlo in spazi ristretti e garantisce le funzionalità di controllo accessi se connesso ad un dispositivo LIFT I/O tramite RS485.

- **X-Station** - X-Station è un terminale IP con un touchscreen LCD da 3.5" che supporta l'accesso tramite ID o carta. Il dispositivo è dotato di una fotocamera integrata per il riconoscimento del volto.
  X-Station permette di registrare fino a 200,000 utenti con 1GB di memoria flash interna e 256MB di RAM.

- **BioMini/BioMini Plus** - I dispositivi BioMini e BioMini Plus sono scanner per le impronte che possono essere utilizzati per la registrazione degli utenti. Installare il dispositivo è semplice: basta collegarlo tramite USB ad un computer connesso al server BioStar e installare il driver.

- **Secure I/O** - Il dispositivo Secure I/O fornisce un efficace metodo per incrementare il livello di sicurezza dei dispositivi montati in esterno o aumentare la capacità del sistema. Quando le porte sono regolate da Secure I/O, non sarà possibile accedere nemmeno rimuovendo i dispositivi esterni. Per aumentare ulteriormente il livello di sicurezza, il dispositivo Secure I/O garantisce una comunicazione criptata fra i componenti della porta. Secure I/O ha quattro ingressi e due uscite relè per consentire il controllo di più componenti con un singolo dispositivo..

- **LIFT I/O** – LIFT I/O supporta 0-9 dispositivi IDs ed è dotato di 12 ingressi e 12 uscite. Ogni uscita può essere connessa al tasto di un ascensore per controllare l'accesso ai piani. LIFT I/O può essere connesso tramite RS485 come slave ai dispositivi Xpass e Xpass Slim. Possono essere collegati ad un Xpass o Xpass Slim fino a 10 LIFT I/O, per controllare fino a 120 piani.

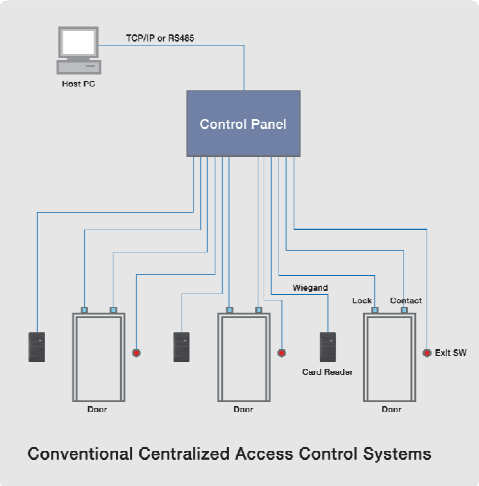


1. Sistema BioStar

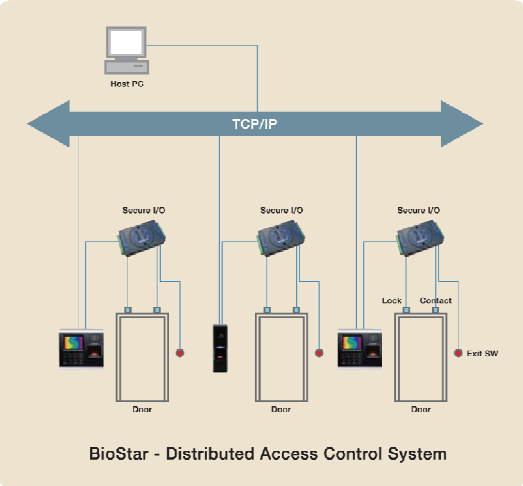
1.1 Configurazione

BioStar è un sistema a distribuzione intelligente. Invece dei complessi collegamenti e del controllo centralizzato richiesto dai sistemi di controllo accessi convenzionali, i dispositivi di controllo accessi Suprema possono essere connessi tramite TCP/IP o wireless ad una rete locale, o connesso direttamente tramite connessione seriale. Le informazioni utente, le regole d'accesso e gli altri dati possono essere distribuiti ai vari dispositivi per accelerare il tempo di autorizzazione e consentire l'operatività anche quando viene a mancare la connessione alla rete.

Come mostrato nelle figure successive, il sistema BioStar non richiede controller diversi. Questa caratteristica fornisce un vantaggio sui tipici sistemi di controllo accessi, in quanto i dispositivi BioStation, BioEntry Plus, o BioEntry W lavorano contemporaneamente sia come controller che come lettori. Il risultato è una richiesta inferiore di hardware e connessioni, a differenza dei tipici sistemi di controllo accessi centralizzati.



Conventional Centralized Access Control Systems

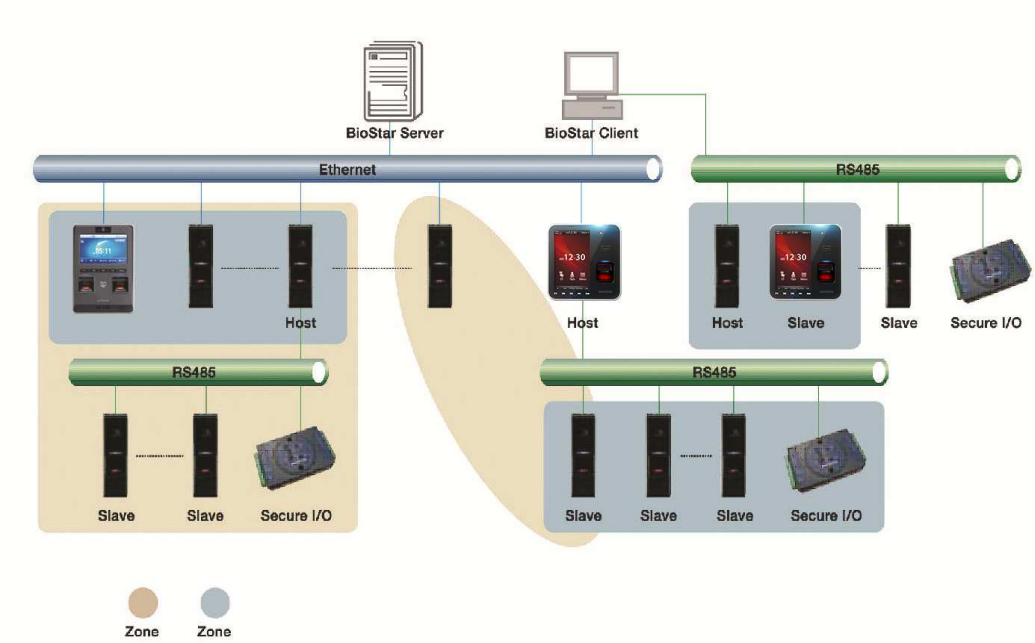


BioStar - Distributed Access Control System

BioStar è un'applicazione server-client che supporta fino a 32 clienti (2 clienti nella versione free). Una tipica configurazione consiste in numerosi dispositivi di controllo accessi connessi ad un server centrale via Ethernet, WLAN, e/o RS485. BioStar è compatibile con MS SQL Server e database MySQL.

Il sistema supporta un massimo di 512 porte e 512 dispositivi (20 porte e dispositivi nella versione free). I dispositivi in rete possono essere raggruppati per creare numerose combinazioni di zone anti-passback o allarmi, come illustrato nella figura successiva.

1. Sistema BioStar



1.2 Funzioni di Controllo Accessi

1.2.1 Autenticazione utente

I dispositivi di controllo accessi suprema sono dotati di un algoritmo avanzato di riconoscimento impronte per garantire la sicurezza in un sistema di controllo accessi. Dalla tastiera numerica sui terminali BioStation, all'individuazione del volto tramite D-Station, X-Station, BioStation T2, e FaceStation, il sistema consente un'ampia scelta di metodi d'autenticazione:

- **Impronta o carta d'accesso** – Accesso tramite impronta o carta.
- **Impronta + carta d'accesso** – Accesso utilizzando sia impronta che carta.
- **ID utente + impronta** – Accesso tramite ID utente e impronta in combinazione. l'ID identifica l'utente, l'impronta autorizza l'accesso.
- **ID utente + password** - Accesso tramite ID e password, in combinazione. the user ID identifies the user and the password is used for authorization.
- **ID utente + carta + impronta** – Accesso tramite ID utente, carta, e impronta in combinazione.
- **Impronta** – Autenticazione tramite impronta come unico metodo d'accesso
- **Carta** – Autenticazione tramite carta come unico metodo d'accesso.

[Solo D-Station]

- **Impronta + impronta** – Doppia impronta.
- **Impronta + individuazione del volto** – Impronta e individuazione del volto.

- **Impronta + impronta + individuazione del volto** – Doppia impronta e individuazione del volto.

[Solo FaceStation]

- **Volto** – Autenticazione tramite riconoscimento del volto.
- **Volto + password** – Autenticazione tramite riconoscimento del volto più password.
- **Volto + carta** – Autenticazione tramite riconoscimento del volto più carta d'accesso..
- **Volto + carta o password** – Autenticazione tramite riconoscimento del volto più carta o password.
- **Volto + carta + password** – Autenticazione tramite riconoscimento del volto più carta e password.
- **ID utente + volto** – Autenticazione tramite ID utente più riconoscimento del volto.
- **ID utente + volto o password** – Autenticazione tramite ID utente più riconoscimento del volto o password.
- **ID utente + volto + password** – Autenticazione tramite ID utente più riconoscimento del volto e password.

[D-Station, X-Station, BioStation T2, and FaceStation]

- **Individua volto** - Ad ogni autenticazione avvenuta con successo, verrà effettuata una foto.

BioStar registra due template di ogni impronta e fino a due impronte per utente (quattro template totali). Se lo si desidera, un'impronta può essere utilizzata come segnale di coercizione, per attivare un allarme o inviare segnalazioni nel caso un utente sia obbligato ad effettuare l'accesso sotto coercizione. Più template per ogni consentono una capacità di riconoscimento migliorata per ridurre gli errori di lettura dell'impronta.

BioStar consente all'amministratore di leggere le carte EM4100 e HID di prossimità, oltre la lettura, registrazione e formattazione delle carte MIFARE® e iCLASS®.

I dispositivi D-Station consentono al sistema di registrare le immagini del volto degli utenti che effettuano l'accesso, oltre alle impronte, la carta d'accesso è l'ID di autenticazione. I dispositivi D-Station, X-Station, BioStation T2 e FaceStation devices sono dotato di fotocamera per consentire il riconoscimento del volto e registrare le immagini del volto per garantire una maggior sicurezza.

1.2.2 Gestione Utente

BioStar supporta sia la modalità manuale che la modalità automatica per la gestione degli utenti. La sincronizzazione manuale è disponibile per registrare gruppi di utenti su particolari dispositivi o quando il numero totale degli utenti nel database BioStar supera i limiti di un dispositivoBioStation, BioEntry Plus, BioEntry W, BioLite Net, Xpass, Xpass Slim, D-Station, X-Station, BioStation T2 o FaceStation.

BioStar raccoglie i registri dai dispositivi e permette di esportare i dati come file di testo (.CSV). Il software supporta un numero illimitato di campi dell'utente (il numero massimo è limitato solo dalla configurazione hardware).

1.2.3 Gestione dei gruppi d'accesso

BioStar permette agli amministratori di creare gruppi d'accesso personalizzati combinando permessi per zone orarie e porte.

BioStar supporta fino a 128 zone orarie che consistono in 7 giorni di schedulazione, più due schedulazioni festive. Ogni giorno incluso nella zona oraria può contenere fino a 5 periodi distinti.

In totale, BioStar supporta fino a 128 gruppi d'accesso che possono essere trasferiti a tutti i dispositivi connessi.

1.2.4 Gestione dispositivo

Gli amministratori possono controllare molteplici aspetti dei dispositivi tramite il software BioStar. In aggiunta all'autenticazione, BioStar supporta la configurazione degli ingressi, uscite relè, azioni e suoni. Il sistema include opzioni per personalizzare le impostazioni riguardo il display e i suoni per BioStation, D-Station, X-Station, BioStation T2 e FaceStation, oltre alle impostazioni per i LED & Buzzer degli altri dispositivi.

Il sistema è dotato di una configurazione per controllare i dispositivi esterni, come le sirene d'allarme. BioStar può inoltre connettersi e comunicare con un dispositivo con interfaccia Wiegand.

1.2.5 Gestione porte e ascensori

BioStar permette il controllo delle porte e dei dispositivi ad esse connessi, come i relè della porta, i sensori e gli switch d'uscita. Fino a due dispositivi possono gestire ogni porta: quando sono connessi due dispositivi, l'amministratore può applicare il controllo anti-passback. BioStar permette inoltre il controllo degli ascensori tramite Xpass e Xpass Slim, con il dispositivo Secure I/O connesso come slaves.

BioStar consente una configurazione specifica per gli eventi d'allarme per le porte che vengono aperte in modo forzato o lasciate aperte oltre uno specifico intervallo, oltre agli allarmi d'attivazione dai singoli dispositivi, inviando delle segnalazioni alle sirene d'allarme esterne, segnalando l'allarme nell'interfaccia utente del software BioStar e inviando una mail di notifica (non disponibile nella versione free). Inoltre, gli amministratori o gli operatori possono bloccare o sbloccare le porte da remoto, o cancellare gli allarmi.

1.2.6 Gestione zone

Il sistema BioStar garantisce all'amministratore il completo controllo di numerose zone (non disponibile nella versione free). Le zone possono essere create tramite i dispositivi connessi Ethernet o RS485 e possono includere un dispositivo master e fino a 65 dispositivi. In aggiunta, i singoli dispositivi possono essere inclusi in un massimo di 4 zone.

BioStar supporta le zone per incrementare le funzionalità di controllo accessi, come l'anti-passback, il limite d'accesso alle zone e il controllo per gli allarmi, gli allarmi antincendio e altre azioni. BioStar permette agli amministratori di sincronizzare l'orario, il registro eventi e i dati degli utenti per tutti i dispositivi in una specifica zona.

1.2.7 Controllo presenze

La versione BioStar 1.2 e superiori includono la funzione di controllo presenze per garantire all'amministratore la possibilità di definire categorie orarie, schedulazioni giornaliere e impostazioni riguardo i festivi. La capacità di controllo presenze BioStar può essere utilizzata per rendere più efficaci le procedure di check-in, check-out, limitazioni d'accesso per il personale non in servizio e report.

BioStar permette all'amministratore di personalizzare le funzioni di controllo presenze per i dispositivi+ BioStation, D-Station, X-Station, BioStation T2 e FaceStation, specificando quali eventi verranno registrati. L'intefaccia BioStar permette all'amministratore di monitorare le procedure di check-in e check-out in tempo reale.

1.2.8 IP Camera and NVR Server Management

BioStar versione 1.5 o superiore supportano le telecamere con protocollo internet (IP) e i registratori video in rete (NVR), per consentire agli amministratori di monitorare le aree ed essere allertati in tempo reale per specifici eventi, osservandone lo svolgimento tramite le immagini delle telecamere IP. Interagendo con i server NVR, il sistema BioStar permette di visualizzare gli eventi di una determinate fascia di tempo. Dall'interfaccia BioStar, l'amministratore può aggiungere e personalizzare le telecamere IP e le relative funzioni.

02 Installare il software BioStar

Installare BioStar è molto semplice, è necessario seguire solo alcune brevi indicazioni:

- Selezionare un PC che rimarrà costantemente in funzione, operando come server BioStar. Il server riceverà e registrerà i dati dei dispositivi connessi in tempo reale.
- Selezionare la tipologia di database che si desidera utilizzare. Il Server BioStar supporta sia MySQL che MS SQL Server (inclusa la versione gratuita MS SQL Server Express). Indipendentemente dal database scelto, è necessario avere i diritti d'accesso per connettersi al database e creare nuovi elementi.
- Assicurarsi che i PC in uso come Server e Client soddisfino i prerequisiti minimi.

Il CD d'installazione BioStar include l'express installer BioStar, un installer per il server BioStar e un installer per il client BioStar. L'express installer installerà sia il server che il client con le caratteristiche minime. È possibile installare Server e Client singolarmente se si necessita di opzioni addizionali o si vogliono installare su PC differenti.

2.1 Requisiti di Sistema

BioStar supporta i seguenti sistemi operativi:

- Windows 7
- Windows Server 2008 R2
- Windows Vista
- Windows XP, Service Pack 1 o superiore
- Windows 2003
- Windows 2000, Service Pack 4 o superiore

2. Installare il software BioStar

I requisiti minimi di sitema per l'installazione includono i seguenti parametri:

- CPU - Intel Pentium o processore equivalente, 1GHz o superiore
- RAM - 512MB
- HDD - 5GB

I requisiti consigliati per ottime performance includono i seguenti parametri:

- CPU - Intel Pentium Dual Core o processore equivalente, 2GHz o superiore
- RAM - 1GB per Windows XP; 2GB per altri sistemi operativi
- HDD - 10GB

2.2 Express-Installer per BioStar

Se si desidera avere il Server e il Client BioStar sullo stesso PC, utilizzando il database MS SQL Server con le impostazioni di base, utilizzare l'Express Installer per l'installazione. Sarà necessario intervenire nel processo di installazione solo quando MS SQL Server o una variante è già installata. In questo caso, sarà richiesto se si desidera o meno installare MS SQL Server Express. Se non si desidera installare la versione express, saranno richiesti i dati per una corretta autenticazione.

Attenzione: Se sul PC vi è già un'installazione precedente tramite l'BioStar Express Express-Installer per BioStar, assicurarsi di rimuovere la versione precedente prima di attivare l'installare express.

L'installer express installerà i seguenti componenti:

- Server BioStar
- Librerie ausiliarie - OpenSSL e Microsoft Visual C++ Redistributable
- MS SQL Server Express
- Client BioStar
- BADB Conv (strumento migrazione database)

Prima di attivare l'installer express BioStar, chiudere tutte le altre applicazioni. Se una versione di BioAdmin precedente è installata sullo stesso PC, assicurarsi di interrompere le operazioni del server BioAdmin prima dell'installazione.
Per attivare l'installer express:

1. Inserire il CD d'installazione BioStar in un lettore compatibile.
2. Scegliere la directory di installazione ed attivare il Setup Express BioStar 1.61.
3. Seguire i comandi sullo schermo per inizializzare l'installazione.

Nota: La versione BioStar 1.3 e superiori includono i driver per la connessione ai dispositivi BioStation e D-Station tramite USB con Windows 7. Questi driver non saranno operativi con versioni precedenti di BioStar. Se si sta utilizzando una versione precedente di BioStar, assicurarsi di installare i driver corretti.

2. Installare il software BioStar

2.3 Installare l'applicazione Server BioStar

Se non si desidera utilizzare l'installer express, è necessario installare il server BioStar e il client separatamente. Assicurarsi che il sistema soddisfi i requisiti minimi di sistema, che le istruzioni precedentemente indicate siano state eseguite correttamente, oltre a chiudere tutte le altre applicazioni. Se sul PC è presente una versione precedente di BioAdmin, assicurarsi di arrestare il server BioAdmin prima di iniziare l'installazione.

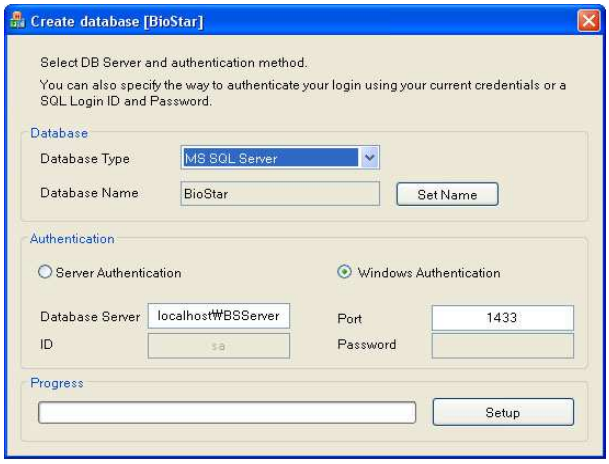
Attenzione: Se è presente sul PC un'installazione precedente con BioStar Express installer, rimuovere la versione precedente prima di attivare l'installer.

L'installer per il server BioStar aggiungerà i seguenti componenti al sistema:

- Server BioStar
- MS SQL Server Express (opzionale)
- Librerie ausiliarie - OpenSSL e Microsoft Visual C++ 2005 Redistributable
- BADB Conv (strumento migrazione database)

Per installare il server BioStar:

1. Inserire il CD d'installazione BioStar in un lettore compatibile.
2. Scegliere la directory d'installazione ed attivare il setup BioStar 1.61 Server.
3. Seguire i comandi sullo schermo per inizializzare l'installazione.
4. Durante l'installazione, verrà richiesto di confermare le condizioni per utilizzare OpenSSL e selezionare una cartella di destinazione per i file di programma OpenSSL.
5. Verrà richiesto se si vuole installare l'edizione MS SQL Server Express. Se si utilizzare una versione pre-installata di MS SQL Server, MySQL o Oracle, è possibile scegliere **No**. Se si desidera utilizzare la versione express, saltare il punto 7. L'installazione del database avverrà automaticamente una volta installata la versione express.
6. Quando comparirà la finestra di Creazione Database [BioStar], selezionare una tipologia di database (MS SQL Server, MySQL o Oracle). L'indirizzo e la porta del server verranno compilati automaticamente, ma si raccomanda di verificarli.



Nota: Il nome standard per il database è sempre "BioStar," per prevenire disinstallazioni non intenzionali di più database sullo stesso sistema o server. Il nome del database può essere cambiato modificatndo il file DBSetup.exe.

7. Se si sceglie MS SQL Server, è necessario configurare anche il metodo d'autenticazione (MySQL consente solo un'autenticazione server):
   - **Autenticazione Server** – questa opzione utilizza l'ID e la password per autenticare gli utenti che vengono creati e registrati nel server SQL. Queste credenziali non sono basate sull'account Windows dell'utente. Gli utenti connessi tramite l'autenticazione server devono fornire le proprie credenziali ogni volta che effettuano l'accesso.
   - **Autenticazione Windows** – questa opzione utilizzare gli account Windows degli utenti per l'autenticazione. Quando un utente si connette tramite un account Windows, il server SQL convalida l'accesso utilizzando nome utente e password. Il server SQL non richiede una password. Questo metodo è impostato di default su MS SQL Server.

   Nota: È necessario scegliere il metodo d'autenticazione supportato dal database. Sarà inoltre necessario forniren le credenziali per creare nuovi elementi nel database.
8. Cliccare **Setup** per creare il database SQL.
9. Quando il database SQL è completato, cliccare **Fine**.
10. Il programma di installazione completerà alcuni processi prima di terminare l'installazione del server. Cliccare **Fine**.

Nota: La versione BioStar 1.3 e superiori includono i driver per la connessione ai dispositivi BioStation e D-Station tramite USB con Windows 7. Questi driver non saranno operativi con versioni precedenti di BioStar. Se si sta utilizzando una versione precedente di BioStar, assicurarsi di installare i driver corretti.

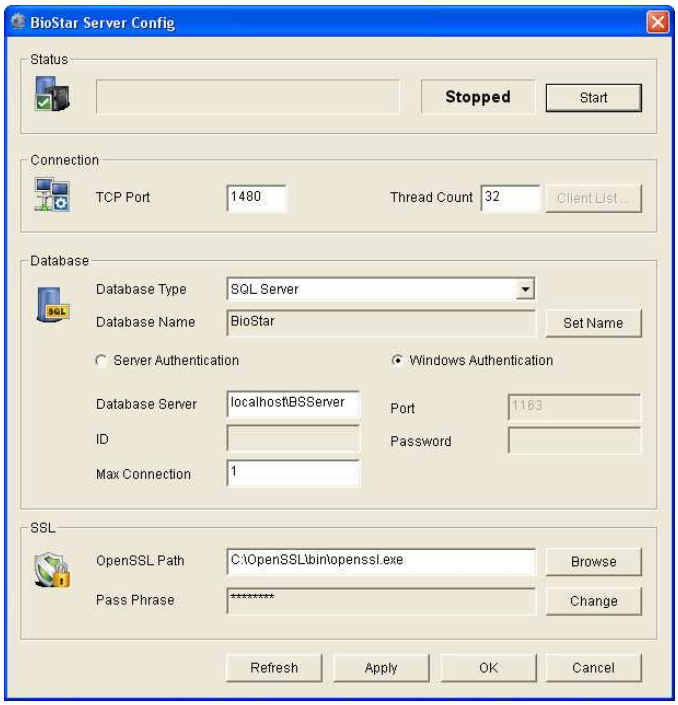
2.3.1 Configurare il Database MySQL

BioStar non può utilizzare il database MySQL se il pacchetto massimo è meno di 16MB. Per configurare la dimensione massima del pacchetto nel server MySQL, aprire il file di configurazione per il server MySQL (“my.ini” per un sistema Windows o “my.cnf” per un sistema Linux). In [mysqld], aggiungere o modificare la dimensione in 16MB o più (ad esempio: max_allowed_packet=16M). Dopo aver modificato e salvato il file, riavviare il server BioStar per confermare le modifiche.

2.3.2 Configurare il server BioStar

In alcuni casi, è necessaria una configurazione manuale del server BioStar. Se ci sono problemi di connessione al server dal client, ad esempio, potrebbe essere necessario modificare le impostazioni del server. Inoltre, è necessario interrompere e riavviare l’applicazione Server per confermare qualsiasi modifica venga fatta sulla configurazione del database o del server.

Per aprire la configurazione del server, aprire il file BSServerConfig.exe. Di default, verrà aggiunta una shortcut sul desktop durante l’installazione del server BioStar. È possibile trovarlo anche nella cartella “Server”, dove è installata l’applicazione BioStar.



La configurazione del server permette di controllare i seguenti elementi:

- **Stato** – visualizzare e modificare lo stato attuale del server BioStar (*Stopped* o *Started*). È inoltre possibile attivare o arrestare il server clicando i tasti **Start** o **Stop** posizionati sul lato destro.
- **Connessione** – visualizzare e modificare i dettagli per la connessione tra server e dispositivi.
  - **Porta TCP** – inserire la porta utilizzata dal dispositivo e dal client per la connessione al server. È necessario utilizzare una porta che non sia condivisa con nessuna altra applicazione. Nella maggior parte dei casi, è possibile utilizzare la porta standard (1480).
  - **Conteggio** – inserire il numero massimo di elementi che il server BioStar può creare. È possibile inserire un qualsiasi numero tra 32 e 512; in ogni caso, è importante considerare che un elemento più grande consuma più memoria del sistema.
  - **Lista client** – è possibile visualizzare la lista di tutti i dispositivi connessi al server BioStar. La lista mostra gli indirizzi IP e se è stata emessa una certificazione SSL per ogni singolo dispositivo. È possibile creare o rimuovere una certificazione SSL direttamente tramite l'opzione.
- **Database** – tramite questa opzione è possibile visualizzare e modificare il database.
  - **Conness. Max** – è necessario specificare il numero massimo di connessioni tramite il server e il database. Nella maggior parte dei casi, il valore standard (1) è corretto.
- **SSL** – è possibile visualizzare o modificare le opzioni per OpenSSL. Cliccare "Sfoglia" per selezionare il percorso dell'applicazione per OpenSSL o cliccare "Modifica" per modificare la password.

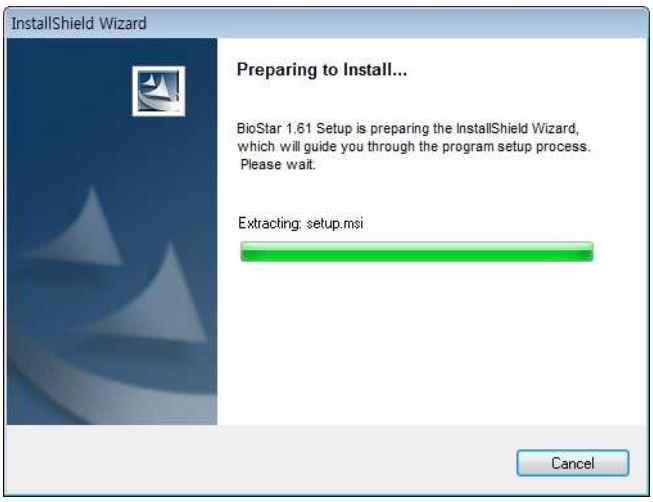
2.4 Installare l'applicazione Client BioStar

Prima di installare l'applicazione client BioStar, chiudere tutte le altre applicazioni. L'installazione aggiungerà i seguenti componenti al sistema:

- Client BioStar
- Librerie ausiliarie - OpenSSL e Microsoft Visual C++ 2005 Redistributable

Per installare l'applicazione client BioStar:

1. Inserire il CD d'installazione BioStar in un lettore compatibile.
2. Attivare il setup del client BioStar 1.61per inizializzare l'installazione.



3. Seguire le istruzuioni per installare il client.

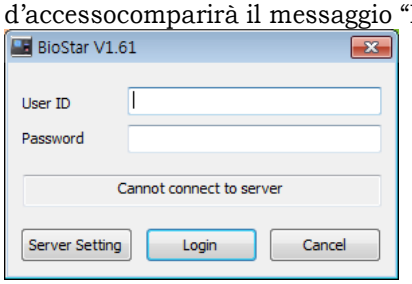
Nota: La versione BioStar 1.3 e superiori includono i driver per la connessione ai dispositivi BioStation e D-Station tramite USB con Windows 7. Questi driver non saranno operativi con versioni precedenti di BioStar. Se si sta utilizzando una versione precedente di BioStar, assicurarsi di installare i driver corretti.

2.4.1 Accedere a BioStar per la prima volta

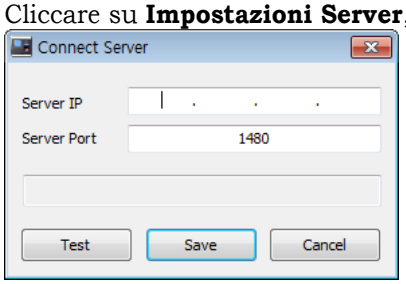
Dopo aver riavviato il sistema al termine dell'installazione, il server BioStar sarà automaticamente attivo in background. Se il sistema non è stato riavviato, potrebbe essere necessario connettere manualmente il server prima di procedere. Quando si effettua l'accesso a BioStar per la prima volta, sarà richiesta la creazione di un account amministratore.

Per effettuare l'accesso la prima volta:

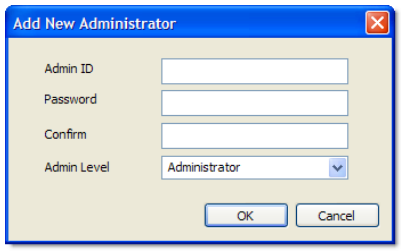
1. Attivare il programma BioStar. Se BioStar si connette con successo al server, si aprirà automaticamente la finestra per la creazione di un nuovo amministratore. In questo caso, saltare il punto 6. Se BioStar non si connette al server, nella finestra d'accessocomparirà il messaggio "Impossibile connettersi al server".



2. Cliccare su **Impostazioni Server**, che aprirà la finestra di connessione.



3. Inserire l'indirizzo IP e la porta del server BioStar.
4. Cliccare su **Verifica** per verificare la connessione.
5. Cliccare **Salva** per registrare i parametri della connessione. Si aprirà la finestra per la creazione di un nuovo amministratore.



6. Inserire ID e password per l'amministratore, confermare la password, quindi scegliere il livello dell'amministratore.
7. Cliccare **OK**. Il programma tornerà alla schermata d'accesso.
8. Inserire ID utente e password, quindi cliccare su **Login**.

2.5 Personalizzare l'interfaccia BioStar

Non è necessario effettuare alcuna modifica all'interfaccia per utilizzare BioStar, in quanto le impostazioni standard sono sufficienti per le operazioni. BioStar permette un ampio livello di personalizzazione per controllare l'aspetto e le funzionalità dell'interfaccia.

2.5.1 Modificare il tema

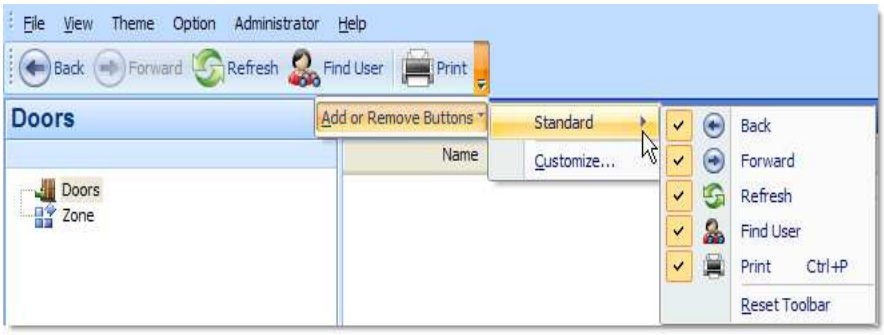
L'interfaccia BioStar include due temi preimpostati, basati sullo stile MS Office:

- Office 2003
- Office 2007

Per modificare il tema cliccare **Tema** dalla barra del menu e selezionare un tema.

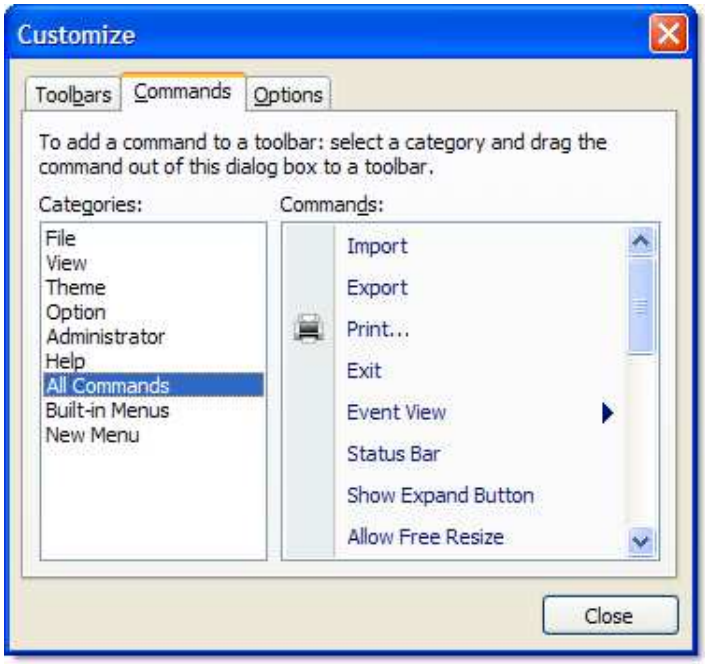
2.5.2 Personalizzare la barra degli strumenti

L'intefaccia BioStar include una barra degli strumenti standard, posizionata in alto a sinistra nella finestra. La barra degli strumenti contiene funzioni simili alle tipiche barre degli strumenti presenti nelle pagine web: Indietro, Avanti, Aggiorna, Trova Utente (cerca) e Stampa.



Per personalizzare la barra degli strumenti:

1. Cliccare la freccia verso il basso a destra della barra.
2. Cliccare **Aggiungi o Rimuovi Tasti > Personalizza**. Si aprirà la finestra di personalizzazione.
3. Cliccare sul paragrafo Comandi.
4. Cliccare *Tutti i Comandi* per mostrare una lista dei tasti disponibili.



5. Trascinare i comandi desiderati sulla barra. Questo aggiungerà un tasto per il nuovo comando.

2.5.3 Modificare la visualizzazione eventi

BioStar consente di modificare il periodo standard degli eventi mostrati nella pagina Eventi per gli utenti, le porte o le zone. È possibile impostare l'interfaccia per visualizzare i dettagli degli eventi per 1-3 giorni o 1 settimana.
Per modificare la visualizzare degli eventi:

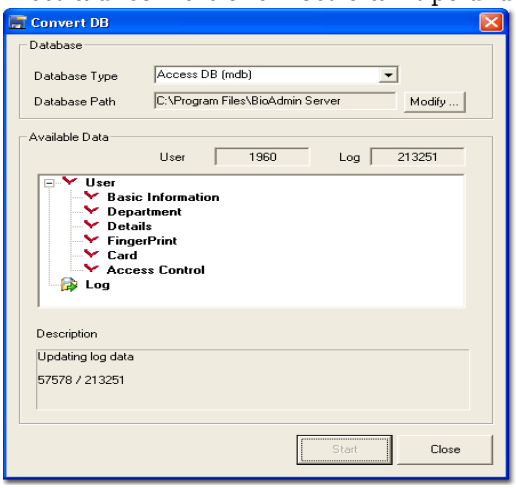
1. Dalla barra del menu, cliccare **Visualizza > Visualizzaione Eventi**.
2. Cliccare sulla tipologia di evento da modificare (*Utente* o *Porte/Zone*).
3. Cliccare su un periodo di tempo (*1 giorno*, *3 giorno* o *7 giorni*).

2.6 Trasferire un database da BioAdmin a BioStar

Il programma di installazione BioStar include uno strumento per il trasferimento denominato *BADB Conv*. Questo strumento permette di trasferire un database BioAdmin esistente in un nuovo sistema BioStar.

Quando si trasferisce un database, qualsiasi informazione identica presente nel database BioStar verrà sovrascritta. Ad esempio, se sono presenti utenti nel database BioStar che esistevano precedentemente nel database BioAdmin, i dati di questi utenti verranno sovrascritti. Per questo motivo, si consiglia di trasferire il vostro database BioStar precedente prima di creare nuovi account.
Per trasferire le informazioni da BioAdmin a BioStar:

1. Avviare il programma *BADBConv.exe*. Questo strumento viene installato nella stessa cartella del software BioStar.
2. Cliccare **Si** per confermare che le informazioni identiche verranno sovrascritte.
3. Cliccare **Inizio** per avviare il trasferimento. Quando il processo è completato, la finestra di conversione mostrerà il tipo di dati trasferiti.



4. Cliccare **Chiudi** per uscire dallo strumento di trasferimento.

03 Impostare il sistema BioStar

Questa sezione descrive come aggiungere account amministrore, dispositivi, zone, porte, reparti, utenti, gruppi d'accesso e impostare il controllo presenze tramite BioStar.
Nota: Questa guida non comprende le procedure d'installazione fisica dei componenti.

3.1 Creare account amministrativi

Prima di aggiungere degli utenti, è importante aggiungere e configurare account per gli amministratori di sistema e per gli operatori.

3.1.1 Livelli amministrativi

BioStar consente l'utilizzo di differenti livelli di amministrazione, operatività e interazione col sistema. Ogni livello amministrativo dispone di alcuni privilegi d'accesso al menu di sistema (Utenti, Porte, Mappe, Controllo Accessi, Monitoraggio, Dispositivi, Controllo Presenze). Il sistema BioStar include tre livelli di amministrazione predefiniti, oltre a quelli personalizzabili:

- Amministratore
- Operatore
- Manager
- Livello personalizzabile

Gli **amministratori** possono aggiungere e configurare dispositive, utenti, porte, zone e gruppi d'accesso. Possono inoltre gestire le funzioni di controllo presenze, incluso l'impostazione di categorie di tempo, schedulazioni giornaliere, regole per festivi e permessi. Inoltre, possono creare livelli d'amministrazione personalizzati che garantiscono i privilegi d'accesso al sistema BioStar.

Gli **operatori** possono monitorare e gestire il sistema BioStar tramite terminale remoto. Gli operatori hanno gli stessi privilegi degli amministratori, tranne i privilegi per creare e cancellare account di amministratori od operatori. Come gli amministratori, gli operatori possono aggiungere e configurare dispositive, utenti, porte, zone e gruppi d'accesso. Possono inoltre gestire le funzioni di controllo presenze, incluso l'impostazione delle categorie di tempo, schedulazioni giornaliere, regole per festivi e permessi, oltre a poter creare, modificare e visualizzare i report di controllo presenze.

I **manager** hanno i privilegi per leggere tutte le informazioni nei menu, ma non possono creare, modificare o cancellare alcun elemento nel menu.

Ad un livello personalizzato di amministrazione possono essere assegnati tutti o solo una parte dei privilegi per l'accesso ai menu. In ogni menu, è possibile assegnare una delle seguenti tre tipologie di privilegi: Tutti i diritti, Modifica, Leggi.

Una tipica configurazione consiste in un amministratore (o più di uno, in base alle dimensioni dell'organizzazione da gestire) che ha un accesso complete al sistema. Al di sotto del livello dell'amministratore, vi possono essere diversi operatori in grado di svolgere varie funzioni, come controllare da remoto porte e serrature, aggiungere utenti, registrare impronte, emettere carte, aggiungere gruppi d'accesso, definire zone orarie e configurare eventi d'allarme.

3.1.2 Aggiungere e personalizzare account amministrativi

Di default, BioStar include un account d'amministratore, che viene creato quando si installa il software. È possibile utilizzare questo account come unico amministratore del sistema e garantire privilegi come operatori a tutti gli altri utenti che gestiscono il sistema, oppure creare altri amministratori in grado di gestire l'intero sistema.

3.1.2.1 Aggiungere un account amministrativo

Per aggiungere un account amministrativo:

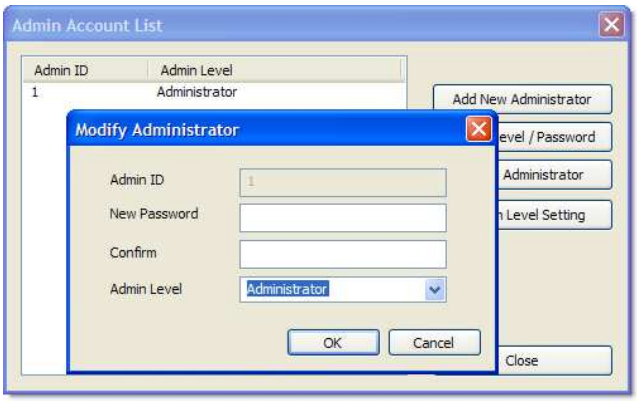
1. Dalla barra del menu, cliccare **Amministratore > Account Admin** per aprire la lista degli account amministratori.
2. Cliccare **Aggiungi Nuovo Amministratore**.
3. Nella finestra per l'aggiunta di un nuovo amministratore, inserire ID e password per l'amministratore.
4. Confermare la password inserendola nuovamente e selezionando il livello di amministratore desiderato:
   - **Amministratore** – tutti i privilegi.
   - **Operatore** – tutti i privilegi, tranne la creazione o la cancellazione degli account di amministratori e operatori.
   - **Manager** – privilegi di lettura per tutte le informazioni.
5. Cliccare **OK**.

3.1.2.2 Modificare il livello amministrativo o la password dell'account

Se non è stato impostato correttamente il livello amministrativo per un account, oppure si desidera modificare la password, è possibile farlo tramite il menu dell'amministratore.

Per modificare il livello amministrativo o la password:

1. Dalla barra dei menu, cliccare **Amministratore > Account Admin** per aprire la lista degli account amministratori.
2. Cliccare su un account amministratore nella lista sul lato sinistro della finestra.
3. Cliccare **Modifica Livello/Password**. Si aprirà la finestra di modifica amministratore.



4. Modificare le informazioni dell'account come necessario:
    - Per cambiare il livello amministrativo, selezionare un nuovo livello dal menu a tenda.
    - Per modificare la password, inserire una nuova password nei campi "Nuova Password" e "Conferma".
5. Cliccare **OK** per salvare le modifiche.

3.1.2.3 Creare un livello amministrativo personalizzato

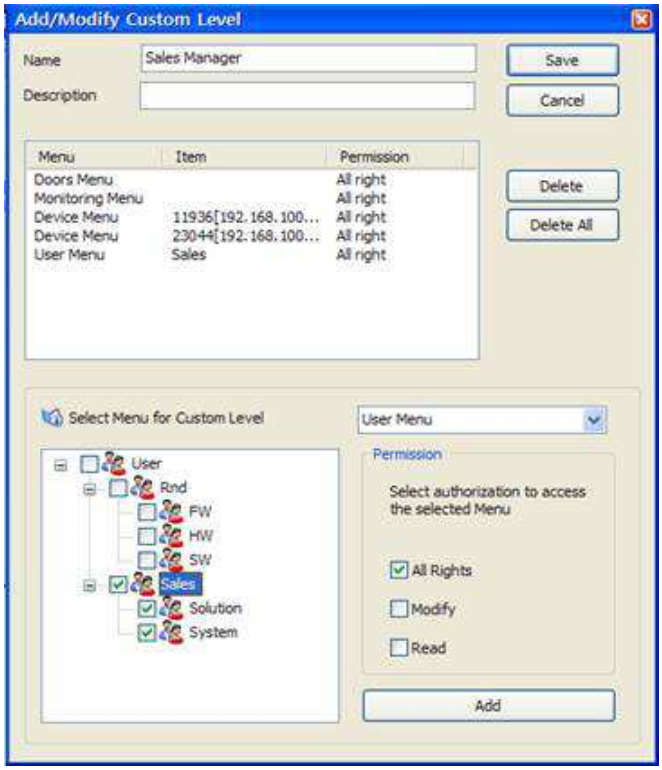
Se si desidera creare un amministratore con specifici privilegi, è possibile definire un livello amministrativo personalizzato. È possibile impostare il livello amministrativo con la possibilità di accedere completamente o solo in parte ai menu BioStar: Utenti, Porte, Mappe, Controllo Accessi, Monitoraggio, Dispositivi e Controllo Presenze.

È possibile creare un livello personalizzato per singoli dispositive o utenti. Un amministratore personalizzato avrà i privilegi che gli vengono assegnati alla creazione (Tutti i diritti, Modifica o Leggi) solo per gli utenti o i dispositivi specificati. Durante la creazione del livello personalizzato, nel menu Utente è possibile assegnare privilegi per gli utenti in un determinato settore. In questo caso, assicurarsi di non assegnare i privilegi ai singoli utenti, bensì ai settori a cui appartengono.

Nel menu Dispositivo, è possibile assegnare privilegi per i singoli dispositivi. Se un dispositivo è connesso ad un dispositivo Slave, i privilegi verranno applicati anche al dispositivo collegato Gli utenti e i dispositivi che non sono selezionati non appariranno nei menu Porte, Mappe, Controllo Accessi, Monitoraggio e Controllo Presenze. Se una porta o una zona è associata con un dispositivo a cui non sono assegnati privilegi, la porta o la zona non compariranno nel menu.

Per creare un livello amministrativo personalizzato:

1. Dalla barra del menu, cliccare **Amministratore > Account Admin** per aprire la lista degli account amministratore.
2. Cliccare **Impostazioni livello personalizzato**.
3. Nella finestra, cliccare **Aggiungi Livello Personalizzato**. Si aprirà la finestra di creazione e modifica del livello personalizzato.



4. Inserire un nome per il livello personalizzato nel campo Nome.
5. Se lo si desidera, aggiungere una descrizione aggiunta nel campo Descrizione.
6. Selezionare un menu dalla lista.
7. Quando si seleziona il menu Utente o il menu Dispositivo, selezionare l'utente o il dispositivo a cui garantire i privilegi d'accesso cliccando il quadratino corrispondente nella lista.
8. Selezionare un livello di permesso (Tutti i diritti, Modifica o Leggi) cliccando il quadratino corrispondente all'opzione desiderata
9. Cliccare **Aggiungi** per includere i permessi nel livello personalizzato.
10. Riptere i punti 6-9 per aggiungere altri permessi, se necessario.
11. Quando la personalizzazione del livello è terminata, cliccare **Salva**.

È ora possibile creare nuovi account amministrativi con uno qualsiasi dei livelli personalizzati creati.

3. Impostare il sistema BioStar

3.2 Impostare i dispositivi

Questa sezione descrive come impostare BioStar per cercare ed aggiungere nuovi dispositivi, oltre a dispositivi RF di altre tipologie. In aggiunta, le procedure che seguono descrivono la configurazione di base per il sistema BioStar.

3.2.1 Ricerca per l'aggiunta di dispositivi

BioStar include un comodo metodo per la ricerca e l'aggiunta dei dispositivi. Prima di iniziare la ricerca per nuovi dispositivi, verificare le connessioni. Se si hanno più dispositivi da aggiungere, potrebbe essere d'aiuto preparare una lista della posizione, ID, e indirizzo IP dei vari dispositivi, prima di aggiungerli.

Per cercare e aggiungere i dispositivi BioStar:

1. Cliccare **Dispositivo**.
2. Cliccare *Add Device*.
3. Cliccare il tasto vicino al tipo di connessione:
   - **LAN** – Scegliere questa opzione per cercare i dispositivi connessi tramite Ethernet o LAN Wireless.
   - **Seriale** – Scegliere questa opzione per cercare i dispositivi connessi tramite PC utilizzando RS485 e RS232 o dispositivi slave connessi tramite RS485 ad un altro dispositivo connesso ad un PC.
   - **USB** – Scegliere questa opzione per cercare dispositivi connessi tramite porta USB.

     Nota: La versione BioStar 1.3 e superiori includono i driver per la connessione ai dispositivi BioStation e D-Station tramite USB con Windows 7. Questi driver non saranno operativi con versioni precedenti di BioStar. Se si sta utilizzando una versione precedente di BioStar, assicurarsi di installare i driver corretti.
   - **Dispositivo USB Virtuale** – Scegliere questa opzione per cercare dispositivi virtuali aggiunti ad un'USB.
4. Cliccare **Successivo**.
5. Per le ricerche USB o USB Virtuale, seguire le istruzioni indicate al punto 7. Se si effettua una ricerca per i dispositivi connessi tramite LAN o porta seriale, impostare i seguenti parametri:
   - LAN – Selezionare se la ricerca è per dispositivi che utilizzano i protocolli TCP o UDP. Selezionando TCP, è possibile specificare l'indirizzo IP, la tipologia del dispositivo cercato e la relativa porta. Selezionando UDP, è possibile cercare dispositivi nella stessa sottorete.
   - Seriale – Specificare una porta COM (o selezionare *tutte le porte*) e il baud rate.
6. Cliccare **Successivo**.

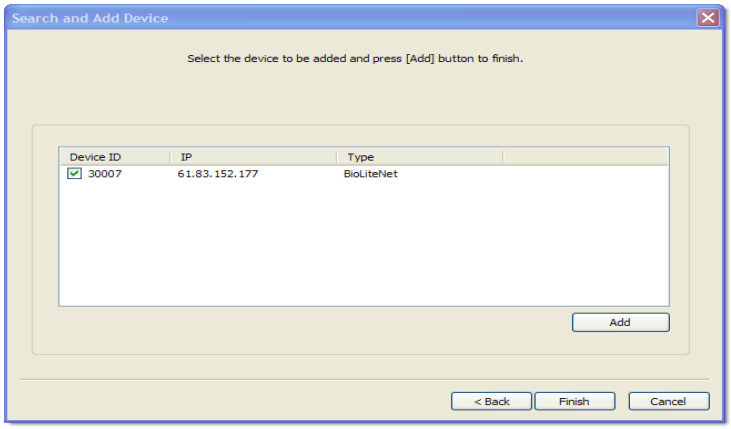
7. Quando BioStar completerà la ricerca, sarà possibile impostare la rete come descritto. Cliccare sul nome del dispositivo nella lista (sulla sinistra), quindi configurare come segue:

   Nota: Se le impostazioni di rete per un dispositivo vengono modificate, il dispositivo verrà rimosso dalla lista. Per aggiungere un dispositivo, sarà necessario rieffettuare la ricerca.

   Non aggiungere dispositivi con la modalità server. I dispositivi si connetteranno al server autonomamente e mostrati nella lista dei dispositivi.

   - **DHCP o IP statico -** Se si sceglie di utilizzare l'opzione DHCP, il dispositivo acquisirà automaticamente le impostazioni di rete dal server DHCP. Se non si utilizza, sarà necessario configurare la rete manualmente.
   - **Connessione diretta** - Questa è l'opzione di connessione standard. Il client BioStar si connetterà direttamente al dispositivo. Scegliendo questo tipo di connessione, il client dovrà essere attivo per ricevere i dati de registro dal dispositivo.
   - **Connessione al server** - Scegliendo questa opzione, il dispositivo si connetterà automaticamente al server BioStar. Configurando l'indirizzo IP del server e la porta correttamente, i campi del registro verranno raccolti nel server, indifferentemente se il client BioStar è attivo. Questa opzione può essere molto utile se la configurazione di rete richiede una connessione tramite indirizzi IP privati (ad esempio, tramite WAN) ad un server con un indirizzo IP pubblico. Questa opzione garantisce la crittografia SSL per i dispositivi BioStar.

8. Cliccare **Successivo**.
9. Selezionare il o i dispositivi da aggiungere cliccando nei checkbox a fianco degli ID dei vari dispositivi.



10. Cliccare **Aggiungi** per aggiungere i dispositivi al sistema BioStar.
11. Chiudere il messaggio di conferma che appare, quindi cliccare **Fine** per terminare.

3.2.2 Ricerca e aggiunta dei dispositivi Slave

Una caratteristica distintiva di BioStar è la possibilità di supportare dispositivi host e slave in RS485. Con questa caratteristica, solo il dispositivo host sarà connesso al pc tramite LAN. La rete potrà essere ampliata facilmente per includere i dispositivo connesso tramite RS485. Questa caratteristica permette il controllo dell'accesso agli ascensori tramite Xpass e Xpass Slim connessi ai dispositivi LIFT I/O.

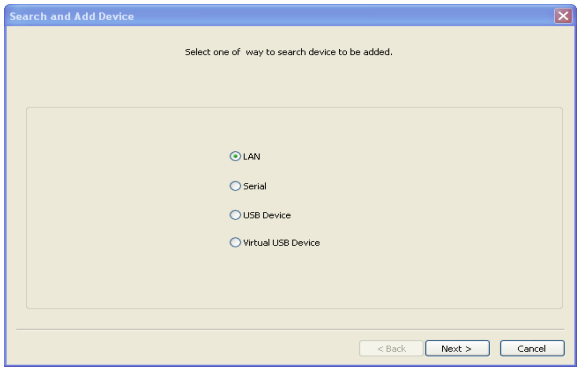
Se la configurazione include dispositivi slave, è necessaria un'ulteriore ricerca per trovare e aggiungere questi dispositivi.

First, configure the host device:

1. Ricerca e aggiunta dei dispositivi come descritto in precedenza.
2. Cliccare **Dispositivo** nel menu.
3. Nel menu di navigazione, cliccare il dispositivo host.
4. Nel menu del dispositivo, cliccare sulle impostazioni della Rete.
5. Modificare le impostazioni RS485 selezionando *Host* dalla lista.
6. Cliccare **Applica** per salvare le modifiche.

Successivamente, effettuare la ricerca per i dispositivi slave:

1. Nel menu di navigazione, cliccare con il tasto destro sul dispositivo host, quindi fare click su **Aggiungi Dispositivo (Seriale)**. Si aprirà una nuova finestra di ricerca.



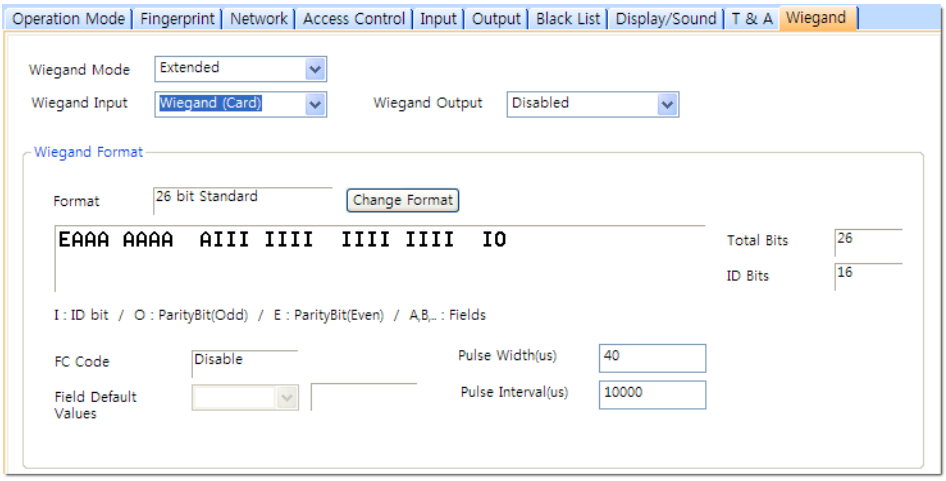
2. Cliccare **Successivo** per iniziare la ricerca.
3. Quando BioStar completa la ricerca, cliccare **Successivo**.
4. Selezionare il o i dispositivi cliccare i checkbox a fianco degli ID dei dispositivi.
5. Cliccare **Aggiungi** per aggiungere un dispositivo
6. Chiudere il messaggio di conferma che appare e cliccare **Fine** per uscire.
7. Nel menu di navigazione, cliccare sul dipositivo slave.
8. Nel menu dispositivo, cliccare sulle impostazioni di Rete.
9. Modificare le impostazioni RS485 selezionando *Slave* dalla lista.
10. Cliccare **Applica** per salvare le modifiche.

3.2.3 Aggiungere un dispositivo RF

Con la versione BioStar 1.2 e successive, i dispositivi RF connessi funzionano in modo indipendente e possono essere associati alle porte ed inclusi nelle zone.

Per aggiungere un dispositivo RF:

1. Connettere il dispositivo RF ad un dispositivo Suprema.
2. Assicurarsi che il dispositivo suprema sia stato aggiunto nel sistema BioStar.
3. Cliccare **Dispositivo** nel menu.
4. Nel menu di navigazione, clicccare sul nome del dispositivo Suprema.
5. Nel menu Wiegand, specificare le impostazioni come descritto di seguito:



   a. Selezionare **Esteso** nella lista delle modalità Wiegand.
   b. Selezionare **Wiegand (Carta)** nella lista.
   c. Cliccare **Applica**.
6. Nel menu di navigazione, fare click con il tasto destro sul nome del dispositivo BioStation, quindi cliccare *Aggiungi dispositivo RF*.

Nota: Per ulteriori informazioni riguardo l'uso di dispositivi RF, consultare la guida del prodotto. Il formato Wiegand deve essere configurato in modo corretto per garantire la compatibilità con i dispositivi.

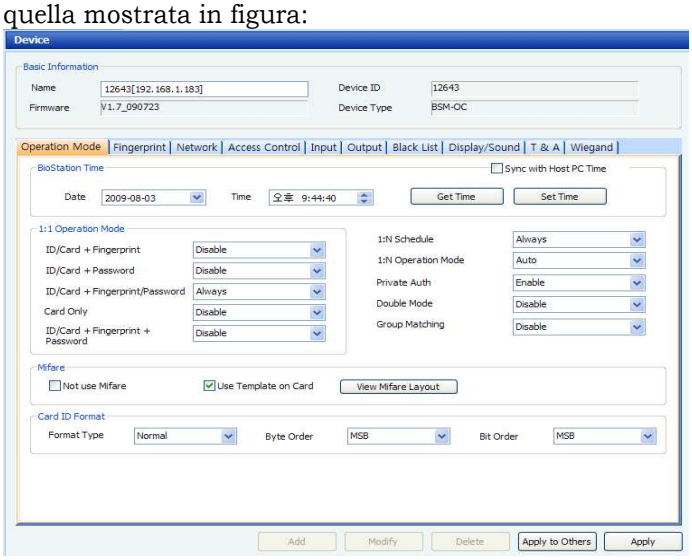
3.2.4 Configurare un dispositivo BioStation

Questa sezione fornisce una panoramica sulla configurazione dei dispositivi BioStation per operare con il software BioStar.

Per configurare un dispositivo BioStation:

1. Cliccare **Dispositivo** nel menu.

2. Doppio click sul nome del dispositivo BioStation nel menu. Si aprirà una finestra come quella mostrata in figura:



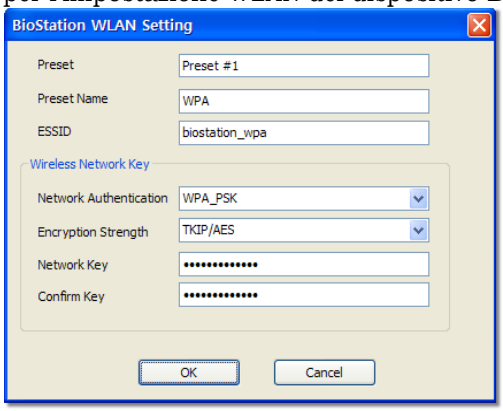
3. Configurare le impostazioni del dispositivo con le seguenti indicazioni:
   - **Modalità operativa** – Utilizzare questa opzione per impostare l'orario presente nel dispositivo od ottenerlo da un PC host e modificare le impostazioni per le modalità operative.
   - **Impronte** – Utilizzare questa opzione per specificare livello di sicurezza, qualità, corrispondenza e timeout per il riconoscimento delle impronte.
   - **Network** – Utilizzare questa opzione per specificare le impostazioni per la connessione seriale o LAN.
   - **Controllo Accessi** – Utilizzare questa opzione per specificare i limiti d'accesso e i gruppi d'accesso per un singolo dispositivo.
   - **Ingresso** – Utilizzare questa opzione per aggiungere, modificare o cancellare le impostazioni degli ingressi per il dispositivo.
   - **Uscita** - Utilizzare questa opzione per aggiungere, modificare o cancellare le impostazioni delle uscite per il dispositivo.
   - **Black List** – Utilizzare questa opzione per bloccare le carte d'accesso MIFARE sui dispositivi BioStation Mifare.
   - **Display/Suono** – Utilizzare questa opzione per modificare le impostazioni sonore o del display e modificare immagini di sfondo o suoni.
   - **T&A** – Utilizzare questa opzione per configurare le impostazioni di controllo presenze.
   - **Wiegand** - Utilizzare questa opzione per configurare il formato Wiegand.

4. Quando la configurazione del dispositivo è terminata, cliccare **Applica** per salvare le modifiche.
5. Per applicare le stesse impostazioni su altri dispositivi, cliccare **Applica ad altri** e selezionare gli altri dispositivi dall'elenco.

3.2.4.1 Connessione di un dispositivo BioStation tramite LAN wireless

Alcuni dispositivi BioStation supportano la connessione LAN wireless.
Per configurare le impostazioni di connessione:

1. Cliccare **Dispositivo** nel menu.
2. Cliccare sul nome del dispositivo BioStation nel menu.
3. Cliccare sulle impostazioni della Rete.
4. Selezionare "Lan Wireless" nell'elenco.
5. Selezionare una delle configurazioni WLAN preimpostate (*Preset #1 - Preset #4*).
6. Cliccare **Modifica Impostazioni** nella sezione WLAN. Si aprirà la finestra per l'impostazione WLAN del dispositivo BioStation.

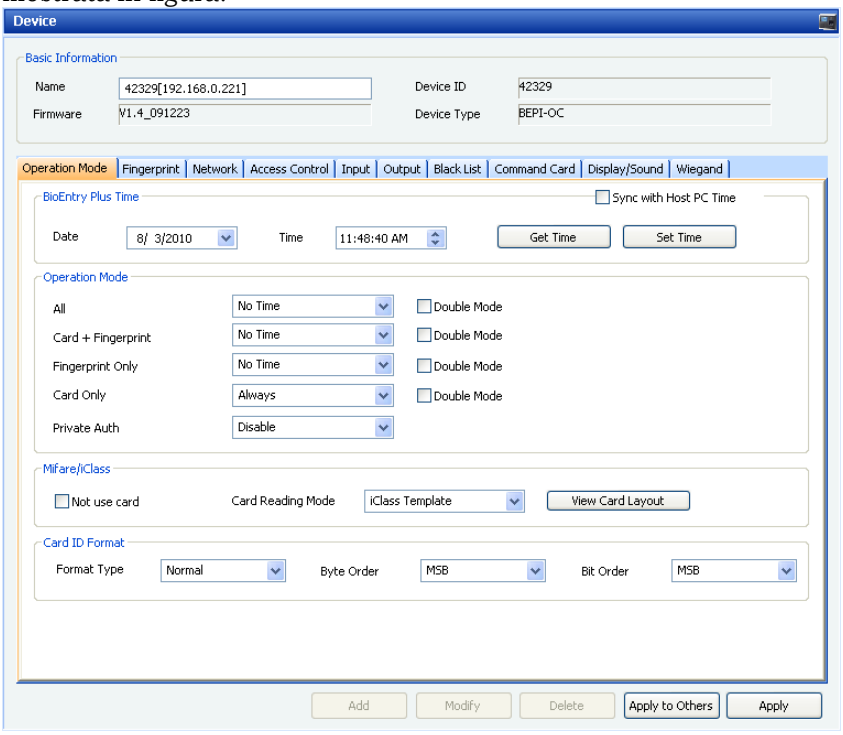


7. Configurare i seguenti parametri:
   - **Nome preimposato** – Inserire un nome per la configurazione che comparirà sul dispositivo BioStation connesso tramite WLAN.
   - **ESSID** – Inserire l'ID univoco per l'access point.
   - **Autenticazione di rete** – Selezionare una modalità di autenticazione di rete dall'elenco (Sistema aperto, Chiave condivisa, o WPA-PSK). L'autenticazaione dovrà essere la stessa per il dispositivo e l'access point.
   - **Crittografia** – Selezionare un livello di crittografia dall'elenco (le opzioni variano in base alle modalità di autenticazione di rete).
   - **Password rete** – inserire la password di rete.
   - **Conferma** – Reinserire la password.
8. Cliccare **OK** per salvare le modifiche.

3.2.5 Configurare un dispositivo BioEntry Plus o BioEntry W

Per configurare un dispositivo BioEntry Plus o BioEntry W:

1. Cliccare **Dispositivo** nel menu.
2. Doppio click sul nome del dispositivo nel menu. Si aprirà una finestra come quella mostrata in figura:



3. Configurare le impostazioni del dispositivo con le seguenti indicazioni:
   - **Modalità operativa** – Utilizzare questa opzione per impostare l'orario presente nel dispositivo od ottenerlo da un PC host e modificare le impostazioni per le modalità operative.
   - **Impronte** – Utilizzare questa opzione per specificare livello di sicurezza, qualità, corrispondenza e timeout per il riconoscimento delle impronte.
   - **Network** – Utilizzare questa opzione per specificare le impostazioni per la connessione seriale o LAN.
   - **Controllo Accessi** – Utilizzare questa opzione per specificare i limiti d'accesso, i gruppi d'accesso e le impostazioni di controllo presenze.
   - **Ingresso** – Utilizzare questa opzione per aggiungere, modificare o cancellare le impostazioni degli ingressi per il dispositivo.
   - **Uscita** - Utilizzare questa opzione per aggiungere, modificare o cancellare le impostazioni delle uscite per il dispositivo.
   - **Black List** – Utilizzare questa opzione per bloccare le carte d'accesso MIFARE sui dispositivi BioEntry Plus o BioEntry W Mifare o le carte iCLASS sui dispositivi BioEntry Plus iCLASS.

- **Command Card** – Utilizzare questa opzione per creare carte di comando che controllino i dispositivi BioEntry Plus o BioEntry.
- **Display/Sound** – Utilizzare questa opzione per configurare le impostazioni LED & Buzzer.
- **Wiegand** - Utilizzare questa opzione per configurare il formato Wiegand.

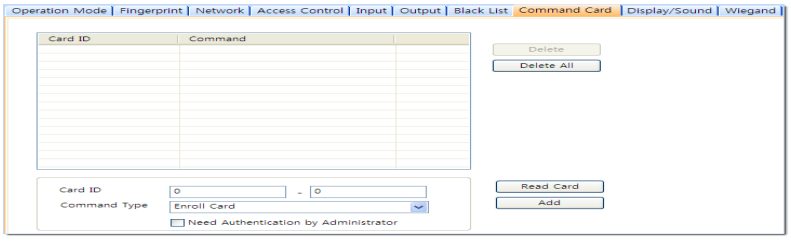
4. Quando la configurazione del dispositivo è terminata, cliccare **Applica** per salvare le modifiche.
5. Per applicare le stesse impostazioni su altri dispositivi, cliccare **Applica ad altri** e selezionare gli altri dispositivi dall'elenco.

3.2.5.1 Creare carte di comando

Le carte di comando consentono di registrare e cancellare gli utenti direttamente dai dispositivi BioEntry Plus o BioEntry W.

Per creare carte di comando:

1. Cliccare **Dispositivo** nel menu.
2. Nel menu, cliccare il nome del dispositivo BioEntry Plus o BioEntry W .
3. Cliccare sulla sezione Carta di Comando nel menu.

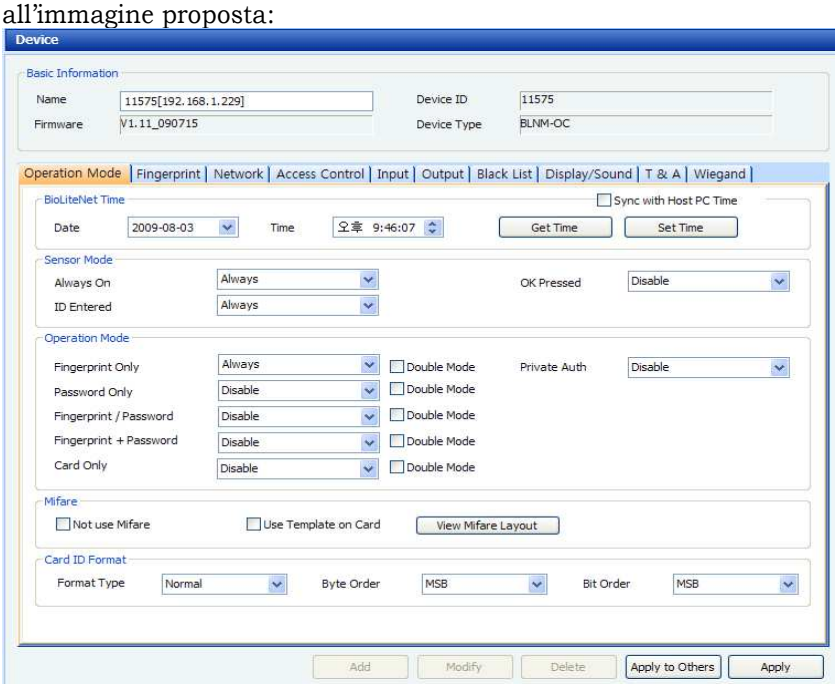


4. Cliccare **Leggi Carta**.
5. Avvicinare una carta al dispositivo.
6. Selezionare una tipologia dall'elenco.
7. Se lo si desidera, la carta può richiedere l'autenticazione di un amministratore selezionando il checkbox vicino alla relativa opzione.
8. Cliccare **Aggiungi**.

3.2.6 Configurare un dispositivo BioLite Net

Per configurare un dispositivo BioLite Net:

1. Cliccare **Dispositivo** nel menu.
2. Doppio click sul nome del dispositivo nel menu. Si aprirà una finestra simile all'immagine proposta:



3. Configurare le informazioni del dispositivo secondo le seguenti istruzioni:
   - **Modalità operativa** – Utilizzare questa opzione per impostare od ottenere l'orario dal PC, modificare le impostazioni per le modaità e le opzioni di riconoscimento impronte.
   - **Impronte** – Utilizzare questa finestra per specificare il livello di sicurezza, la qualità, il riconoscimento e le impostazioni di timeout relative al riconoscimento delle impronte.
   - **Rete** – Utilizzare questa finestra per specificare le impostazioni LAN o delle connessioni seriali.
   - **Controllo Accessi** – Utilizzare questa finestra per specificare i limiti d'entrata e i gruppi d'accesso.
   - **Ingresso** – Utilizzare questa finestra per aggiungere o modificare gli ingressi del dispositivo.
   - **Uscita** – Utilizzare questa finestra per aggiungere o modificare le uscite di questo dispositivo.
   - **Black List** – Utilizzare questa scheda per bloccare l'accesso alle carte MIFARE sui dispositivi BioLite Net Mifare.

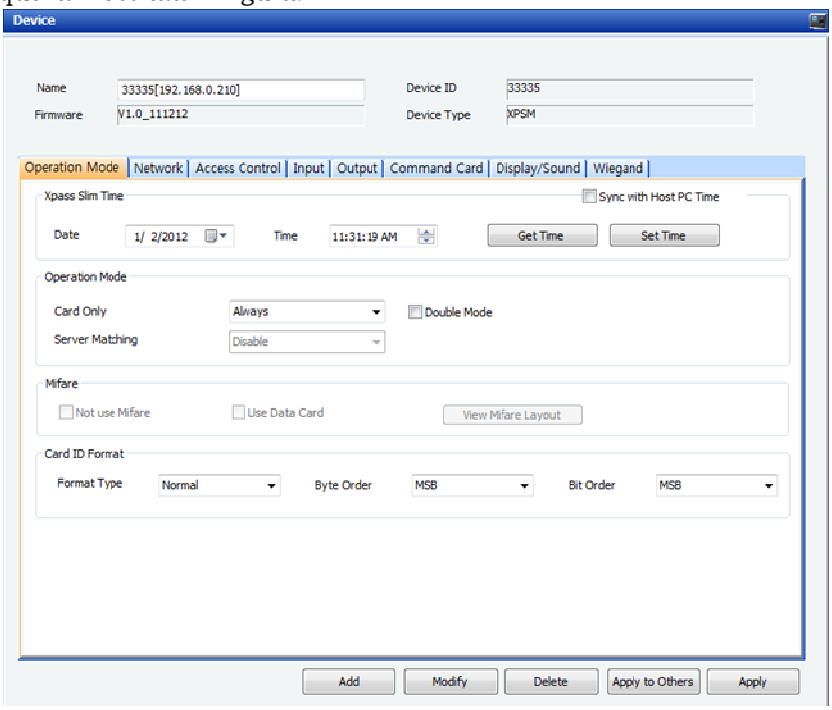
- **Display/Suono** – Utilizzare questa finestra per configurare LED & Buzzer in base agli eventi o agli stati.
- **T&A** – Utilizzare questa finestra per configurare le impostazioni di controllo presenze.
- **Wiegand** – Utilizzare questa finestra per configurare il formato Wiegand.

4. Quando la configurazione del dispositivo è terminata, cliccare **Applica** per salvare le modifiche.
5. Per applicare le stesse impostazioni ad altri dispositivi, cliccare **Applica ad altri**, selezionare gli altri dispositivi e cliccare **Applica**.

3.2.7 Configurare un Xpass o Xpass Slim Device

Per configurare un Xpass o Xpass Slim:

1. Cliccare **Dispositivo** nel menu.
2. Fare doppio click sul nome del dispositivo nel menu. Si aprirà una finestra come quella mostrata in figura:



3. Configurare le informazioni del dispositivo come indicato:
   - **Modalità Operativa** – Utilizzare questa finestra per impostare l'orario del dispositivo od ottenerlo dal PC, modificare le impostazioni per le modalità operative e modificare le impostazioni dei formati ID. I dispositivi Xpass Slime non supportano i template delle carte Mifare.
   - **Rete** – Utilizzare questa finestra per le impostazioni seriali o LAN.

- **Controllo Accessi** – Utilizzare questa finestra per impostare i limiti e i gruppi d'accesso.
- **Ingressi** – Utilizzare questa finestra per aggiungere o modificare gli ingressi.
- **Uscite** – Utilizzare questa finestra per aggiungere e modificare le uscite.
- **Carta di comando** – Utilizzare questa finestra per creare carte comando che possono controllare i dispositivi Xpass o Xpass Slim.
- **Display/Suono** – Utilizzare questa finestra per configurare LED & Buzzer in base agli eventi o agli stati.
- **Wiegand** – Utilizzare queta finestra per configurare il formato Wiegand.

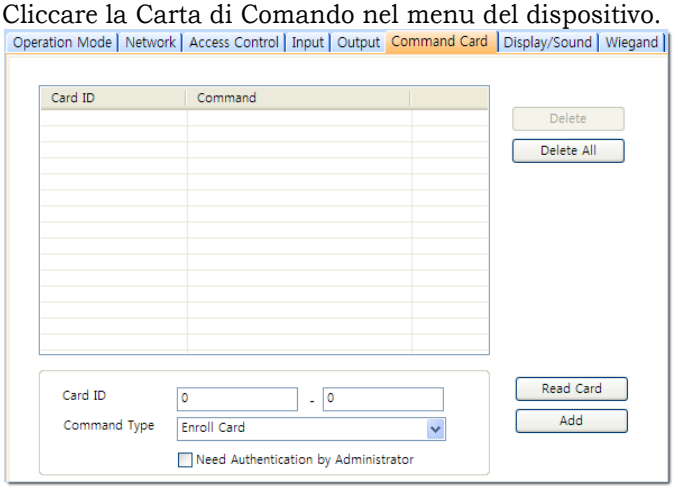
4. Quando la configurazione del dispositivo è terminato, cliccare **Applica** per salvare le modifiche.
5. Per applicare le stesse impostazioni agli altri dispositivi, cliccare **Applica ad Altri**, selezionare gli altri dispositivi dall'elenco e cliccare **Applica**.

3.2.7.1 Creare carte di comando

Le Carte di Comando permetto di registrare e cancellare utenti direttamente dai dispositivi Xpass o Xpass Slim.

Per creare carte comando:

1. Cliccarwe **Dispositivo** nel menu.
2. Nel menu di navigazione, cliccare sul nome del dispositivo Xpass.
3. Cliccare la Carta di Comando nel menu del dispositivo.

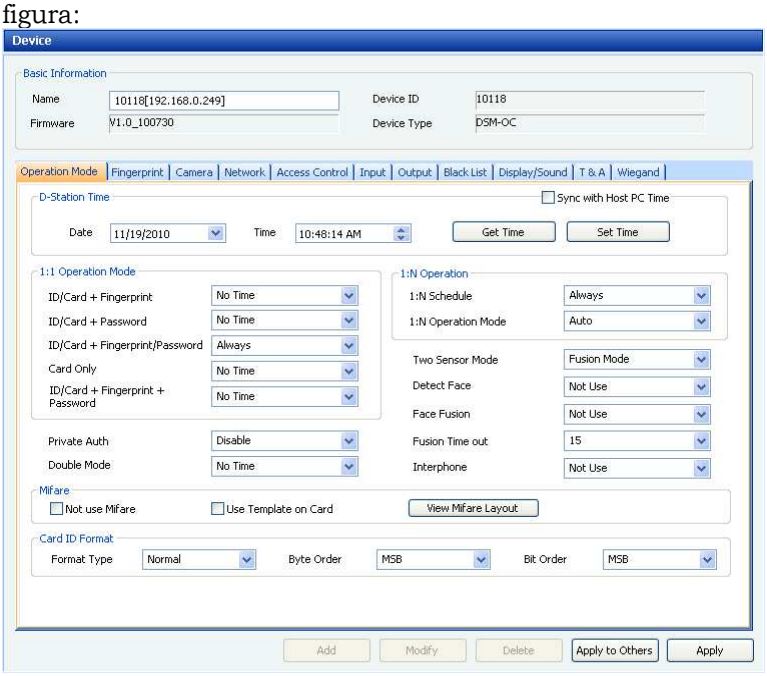


4. Cliccare **Leggi Carta**.
5. Presentare una carta di comando al dispositivo.
6. Selezionare un tipo di comando dal menu a tenda.
7. Se lo si desidera, è possibile impostare la carta per richiedere l'autenticazione dell'amministratore cliccando nella casella a fianco.
8. Cliccare **Aggiungi**.

3.2.8 Configurare un dispositivo D-Station

Per configurare un dispositivo D-Station:

1. Cliccare **Dispositivo** nel menu.
2. Doppio clic sul nome del dispositivo nel menu. Si aprirà una finestra come quella in figura:



3. Configurare le informazioni del dispositivo come indicato:
   - **Modalità Operativa** – Utilizzare questa finestra per impostare gli orari del dispositivo o modificare le modalità operative.
   - **Impronte** – Utilizzare questa finestra per specificare il livello di sicurezza, la qualità, il riconoscimento e il timeout per il riconoscimento delle impronte.
   - **Telecamera** – Utilizzare questa finestra per assegnare eventi, tramite zona oraria, che possono essere effettuati tramite telecamera e individuazione del volto.
   - **Rete** – Utilizzare questa finestra per specificare le impostazioni seriali o LAN.
   - **Controllo Accessi** – Utilizzare questa finestra per specificare i limiti d'accesso e i gruppi d'accesso per i singoli dispositivi.
   - **Ingressi** – Utilizzare questa finestra per aggiungere, modificare o cancellare le impostazioni degli ingressi.
   - **Uscite** - Utilizzare questa finestra per aggiungere, modificare o cancellare le impostazioni delle uscite.
   - **Black List** – Utilizzare questa finestra per bloccare l'accesso tramite carta MIFARE ai dispositivi D-Station.
   - **Display/Suono** – Utilizzare questa finestra per modificare le impostazioni audio o video, le immagini di sfondo e i suoni.

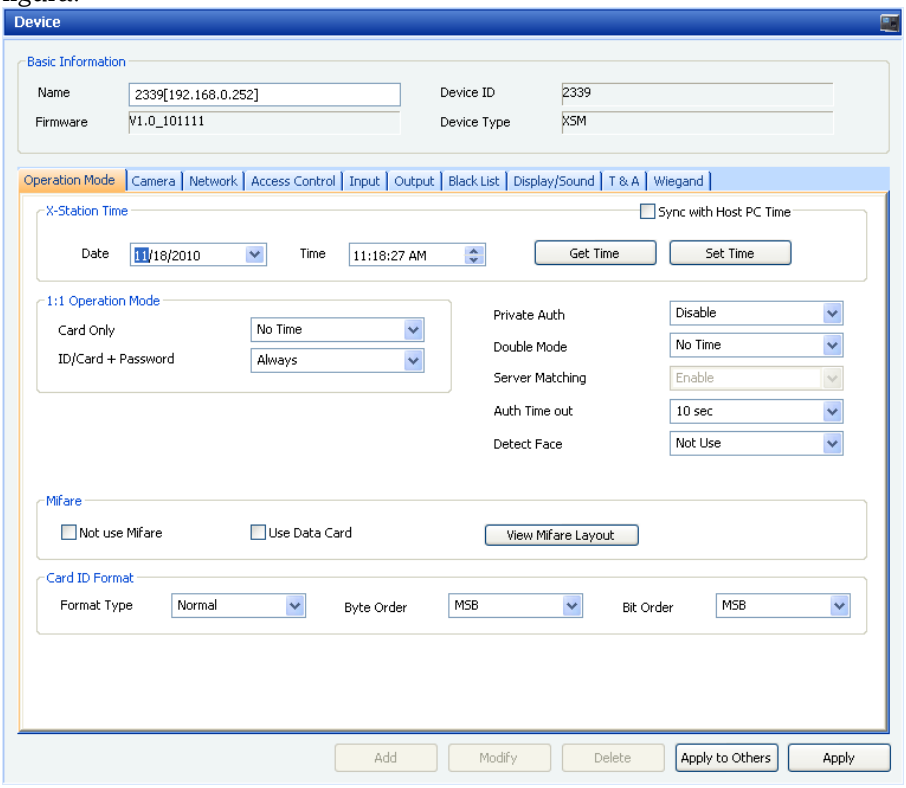
- **Controllo Presenze** – Utilizzare questa tabella per configurare le impostazioni di controllo presenze.
- **Wiegand** – Utilizzare questa tabella per configurare il formato Wiegand.

4. Quando la configurazione del dispositivo è terminata, cliccare **Applica** per salvare le modifiche.
5. Per applicare le stesse impostazioni ad altri dispositivi, cliccare **Applica ad Altri** e selezionare gli altri dispositivi dall'elenco.

3.2.9 Configurare un dispositivo X-Station

Per configurare un dispositivo X-Station:

1. Cliccare **Dispositivo** nel menu.
2. Doppio clic sul nome del dispositivo nel menu. Si aprirà una finestra come quella in figura:



3. Configurare le informazioni del dispositivo:
   - **Modalità Operativa** – Utilizzare questa finestra per impostare gli orari del dispositivo o modificare le modalità operative.
   - **Telecamera** – Utilizzare questa finestra per assegnare eventi, tramite zona oraria, che possono essere effettuati tramite telecamera e individuazione del volto.
   - **Rete** – Utilizzare questa finestra per specificare le impostazioni seriali o LAN.
   - **Controllo Accessi** – Utilizzare questa finestra per specificare i limiti d'accesso e i gruppi d'accesso per i singoli dispositivi.

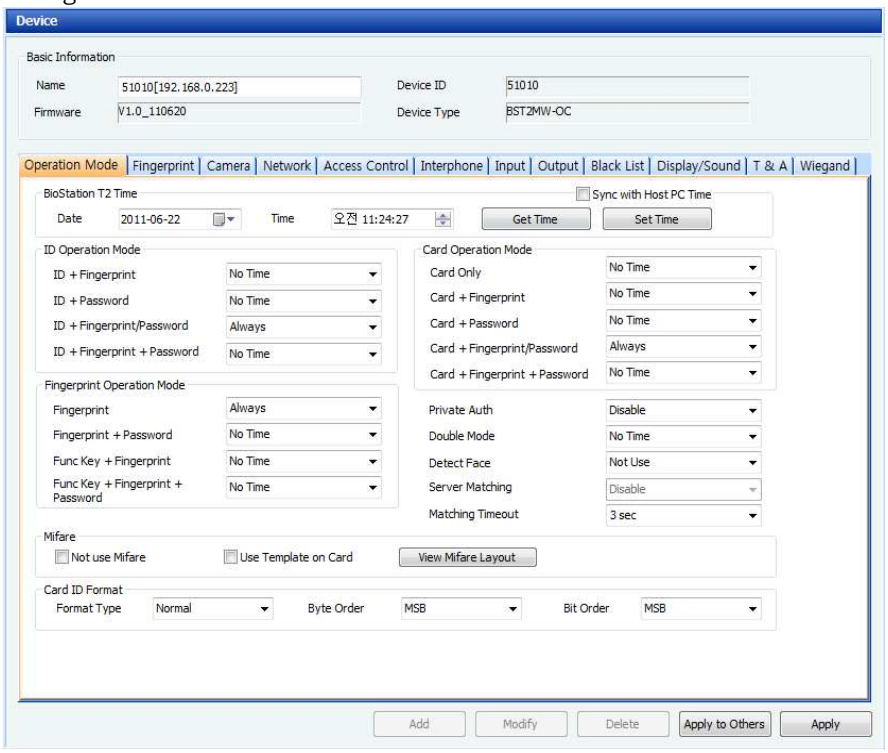
- **Ingressi** – Utilizzare questa finestra per aggiungere, modificare o cancellare le impostazioni degli ingressi.
- **Uscite** - Utilizzare questa finestra per aggiungere, modificare o cancellare le impostazioni delle uscite.
- **Black List** – Utilizzare questa finestra per bloccare l'accesso tramite carta MIFARE ai dispositivi X-Station.
- **Display/Suono** – Utilizzare questa finestra per modificare le impostazioni audio o video, le immagini di sfondo e i suoni.
- **Controllo Presenze** – Utilizzare questa tabella per configurare le impostazioni di controllo presenze.
- **Wiegand** – Utilizzare questa tabella per configurare il formato Wiegand.

4. Quando la configurazione del dispositivo è terminata, cliccare **Applica** per salvare le modifiche.
5. Per applicare le stesse impostazioni ad altri dispositivi, cliccare **Applica ad Altri** e selezionare gli altri dispositivi dall'elenco.

3.2.10 Configurare un dispositivo BioStation T2

Per configurare un dispositivo BioStation T2:

1. Cliccare **Dispositivo** nel menu.
2. Doppio clic sul nome del dispositivo nel menu. Si aprirà una finestra come quella in figura:

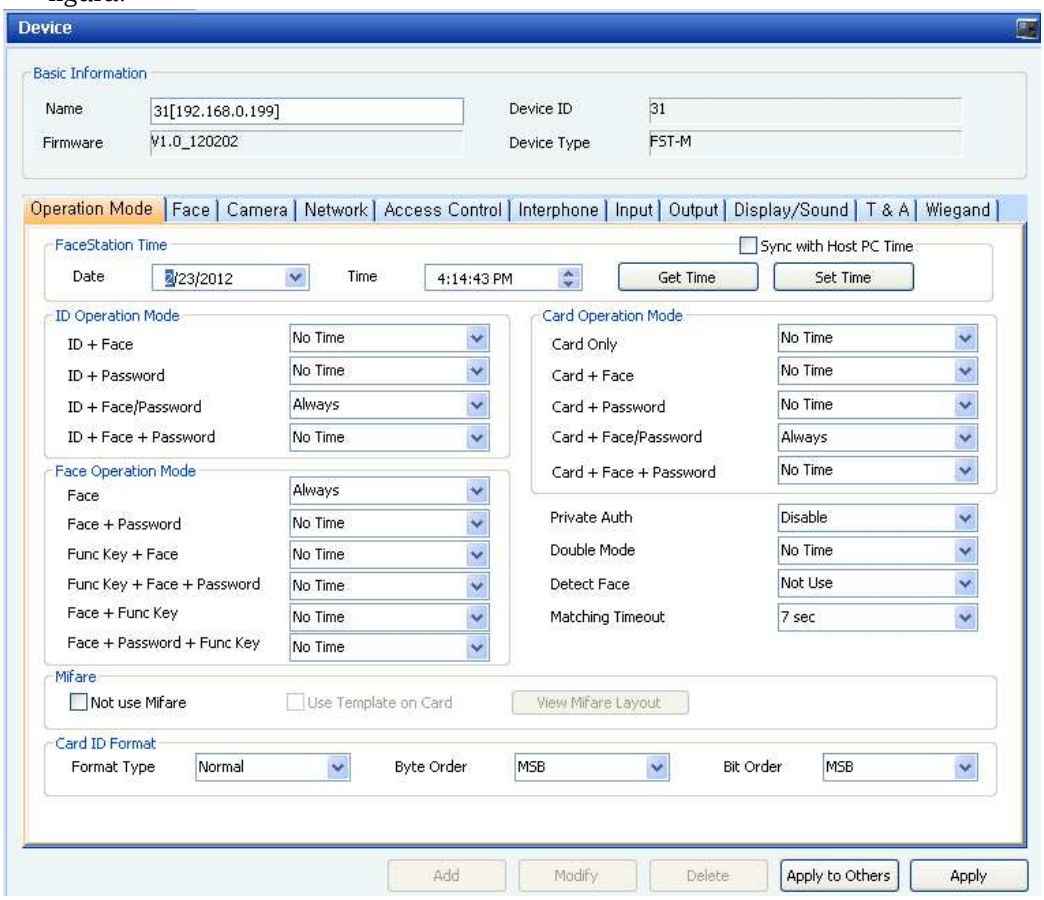


3. Configurare le informazioni del dispositivo come indicato:
   - **Modalità Operativa** – Utilizzare questa finestra per impostare gli orari del dispositivo o modificare le modalità operative.
   - **Impronte** – Utilizzare questa finestra per specificare il livello di sicurezza, la qualità, il riconoscimento e il timeout per il riconoscimento delle impronte.
   - **Telecamera** – Utilizzare questa finestra per assegnare eventi, tramite zona oraria, che possono essere effettuati tramite telecamera e individuazione del volto.
   - **Rete** – Utilizzare questa finestra per specificare le impostazioni seriali o LAN.
   - **Controllo Accessi** – Utilizzare questa finestra per specificare i limiti d'accesso e i gruppi d'accesso per i singoli dispositivi.
   - **Interfono** – Utilizzare questa finestra per funzionare come interfono che permette la comunicazione tra le persone da entrambi i lati della porta.
   - **Ingressi** – Utilizzare questa finestra per aggiungere, modificare o cancellare le impostazioni degli ingressi.
   - **Uscite** - Utilizzare questa finestra per aggiungere, modificare o cancellare le impostazioni delle uscite.
   - **Black List** – Utilizzare questa finestra per bloccare l'accesso tramite carta MIFARE ai dispositivi BioStation T2.
   - **Display/Suono** – Utilizzare questa finestra per modificare le impostazioni audio o video, le immagini di sfondo e i suoni.
   - **Controllo Presenze** – Utilizzare questa tabella per configurare le impostazioni di controllo presenze.
   - **Wiegand** – Utilizzare questa tabella per configurare il formato Wiegand.
4. Quando la configurazione del dispositivo è terminata, cliccare **Applica** per salvare le modifiche.
5. Per applicare le stesse impostazioni ad altri dispositivi, cliccare **Applica ad Altri** e selezionare gli altri dispositivi dall'elenco.

3.2.11 Configurare un dispositivo FaceStation

Per configurare un dispositivo Face Station:

1. Cliccare **Dispositivo** nel menu.
2. Doppio clic sul nome del dispositivo nel menu. Si aprirà una finestra come quella in figura:



3. Configurare le informazioni del dispositivo come indicato:
   - **Modalità Operativa** – Utilizzare questa finestra per impostare gli orari del dispositivo o modificare le modalità operative.
   - **Volto** – Utilizzare questa finestra per specificare il livello di sicurezza e la sensibilità per il riconoscimento del volto.
   - **Telecamera** – Utilizzare questa finestra per assegnare eventi, tramite zona oraria, che possono essere effettuati tramite telecamera e individuazione del volto.
   - **Rete** – Utilizzare questa finestra per specificare le impostazioni seriali o LAN.
   - **Controllo Accessi** – Utilizzare questa finestra per specificare i limiti d'accesso e i gruppi d'accesso per i singoli dispositivi.
   - **Interfono** – Utilizzare questa finestra per funzionare come interfono che permette la comunicazione tra le persone da entrambi i lati della porta.

- **Ingressi** – Utilizzare questa finestra per aggiungere, modificare o cancellare le impostazioni degli ingressi.
- **Uscite** - Utilizzare questa finestra per aggiungere, modificare o cancellare le impostazioni delle uscite.
- **Display/Suono** – Utilizzare questa finestra per modificare le impostazioni audio o video, le immagini di sfondo e i suoni.
- **Controllo Presenze** – Utilizzare questa tabella per configurare le impostazioni di controllo presenze.
- **Wiegand** – Utilizzare questa tabella per configurare il formato Wiegand.

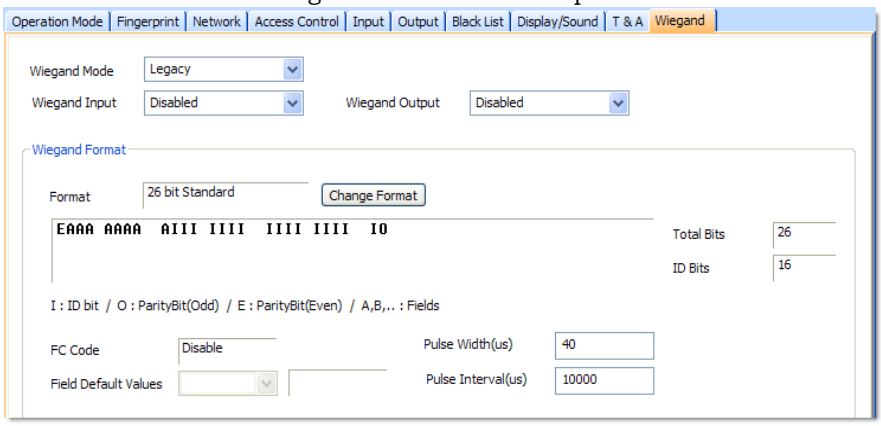
4. Quando la configurazione del dispositivo è terminata, cliccare **Applica** per salvare le modifiche.
5. Per applicare le stesse impostazioni ad altri dispositivi, cliccare **Applica ad Altri** e selezionare gli altri dispositivi dall'elenco.

3.2.12 Modificare il formato Wiegand

Dall'interfaccia BioStar, è possibile configurare il formato Wiegand di un dispositivo, per controllarne ingressi e uscite.

Per configurare il formato Wiegand:

1. Cliccare **Dispositivo** nel menu.
2. Nel menu di navigazione, cliccare il nome del dispositivo.
3. Cliccare nella scheda Wiegand nel menu del dispositivo.



4. Cliccare **Modifica Formato**. Si aprirà una finestra per la configurazione Wiegand.
5. Selezionare uno dei seguenti formati:
   - **Standard 26-bit** – questo formato è quello utilizzato comunemente e consiste in un codice FC a 8-bit e ID a 16-bit. Non è possibile modificare la definizione del formato.
   - **Pass-Through** – utilizzare questo formato per personalizzare solo i bit dell'ID. Durante la verifica, se l'ID viene riconosciuto, l'ingresso Wiegand effettuerà il passaggio nella sua forma normale. Non è possibile impostare valori alternativi del

formato. Per definizione, questo formato risulta utile quando la modalità operativa è uno-a-uno (1:1). In una modalità ono-a-molti (1:N), i bit senza ID sono impostati come 0..

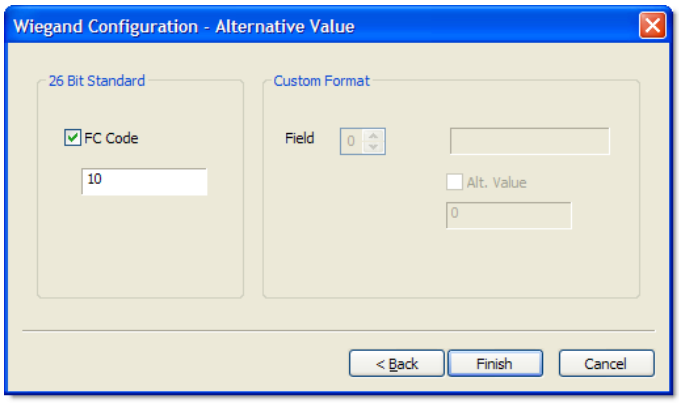
- **Personalizzato** – con un formato personalizzato, è possibile definire i bit degli ID e gli altri valori. Durante la verifica, il dispositivo verificherà la parità dei bit. Se questa risulterà corretta, il dispositivo verificherà l'ID. Quando tutte le verifiche saranno state completate, il dispositivo invierà una strina in uscita, anch'essa personalizzabile.

6. Utilizzare la configurazione Wiegand per personalizzare il formato Wiegand in base alle proprie esigenze (vedi sezione relativa per ulteriori informazioni).
7. Quando sono state effettuate tutte le modifiche, cliccare **Applica** per salvare.

3.2.12.1 Configurare un formato Wiegand a 26-bit

Quando viene selezionato un formato a 26-bit, l'unico elemento personalizzabile è il codice FC:

1. Dopo aver selezionato il formato, cliccare su **Successivo** fino a raggiungere la finestra Valore Alternativo.

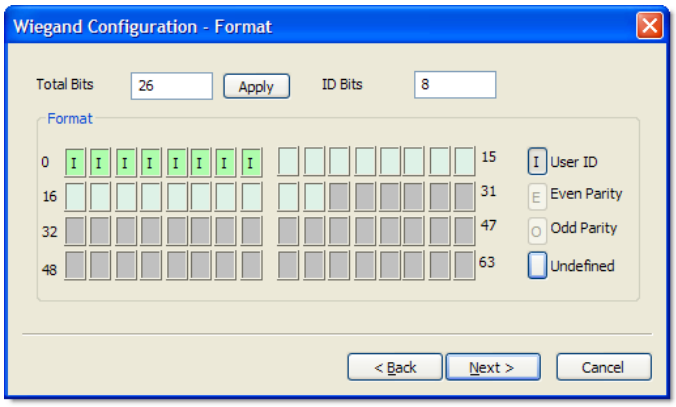


2. Selezionare il checkbox del codice FC e inserire il nuovo codice.
3. Cliccare **Fine** per chiudere la finestra.

3.2.12.2 Configurare un formato Wiegand Pass-through

Quando si seleziona un formato Pass-through, è possibile modificare il numero totale dei bit e assegnare degli ID:

1. Dopo aver selezionato il formato, cliccare **Successivo** per avanzare fino alla finestra “Formato”.

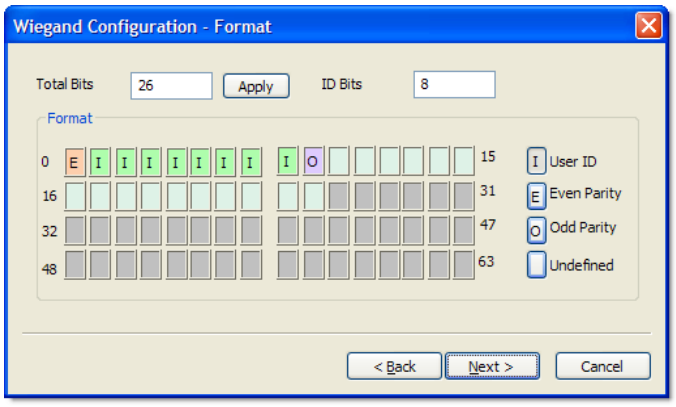


2. Se lo si desidera, inserire un numero per il totale dei bit e cliccare **Applica**.
3. Cliccare il tasto ID Utente (I) sulla destra.
4. Assegnare i bit dell’ID cliccando nella relativa casella.
5. Cliccare Successivo fino a raggiungere la finestra Valore Alternativo.
6. Cliccaare **Fine** per chiudere la finestra.

3.2.12.3 Configurare un formato Wiegand personalizzato

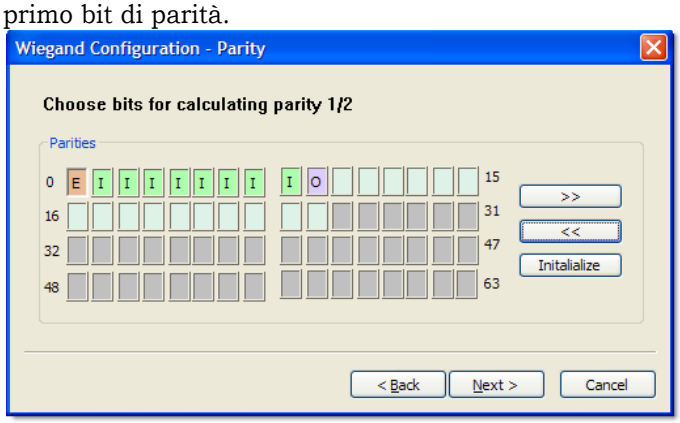
Quando si seleziona un formato personalizzato, è possibile personalizzare il numero totale dei bit, assegnare bit per l’ID, definore bit di parità e altri valori per la stringa in uscita.

1. Dopo aver selezionato il formato, cliccare **Successivo** per avanzare fino alla finestra “Formato”.

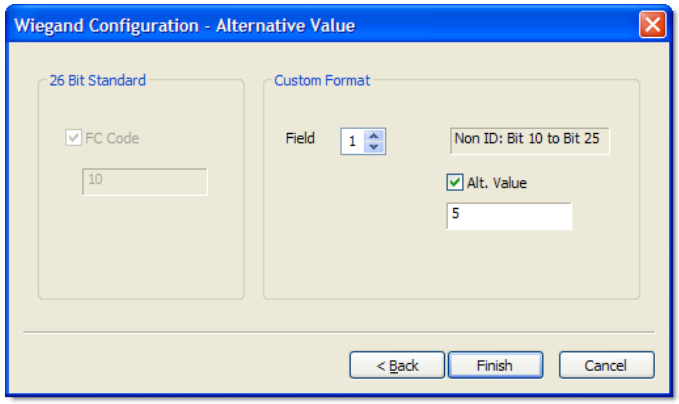


2. Se lo si desidera, è possibile inserire un nuovo numero totale di bit e cliccare **Applica**.

3. Cliccare il tasto ID Utente (I) sulla destra e assegnare i bit dell'ID nella relativa casella.
4. Cliccare il tasto (E) sulla destra per assegnare un bit cliccando nella relativa casella.
5. Cliccare il tasto (O) sulla destra per assegnare un bit cliccando nella relativa casella.
6. Cliccare **Successivo**.
7. Nella finestra Parità, selezionare i bit che verranno utilizzati per calcolare il primo bit di parità.



8. Se necessario, cliccare "**>>**" e selezionare i bit che verranno utilizzati per calcolare altri bit di parità. È necessario effettuare questo passaggio per ogni di bit di parità assegnato nel passaggio 4 e 5. È possibile cliccare **Inizializza** per effettuare un reset della selezione.
9. Cliccare **Successivo**.
10. Nella finestra Valori Alternativi, selezionare un campo da personalizzare (solo bit non appartenenti a ID).



11. Cliccare il checkbox Valore Alternativo e inserire un nuovo valore per la strina in uscita.
12. Ripetere i passaggi 10-11, se necessario, per personalizzare altre stringhe in uscita.

13. Cliccare **Fine** per chiudere la finestra.

3.3 Impostazione porte

Questa sezione descrive come impostare le porte tramite il sistema BioStar.
Per ulteriori informazioni riguardo l'installazione pratica del dispositivo, fare riferimento alla guida relativa al prodotto.

3.3.1 Aggiungere una porta

Aggiungere una porta:

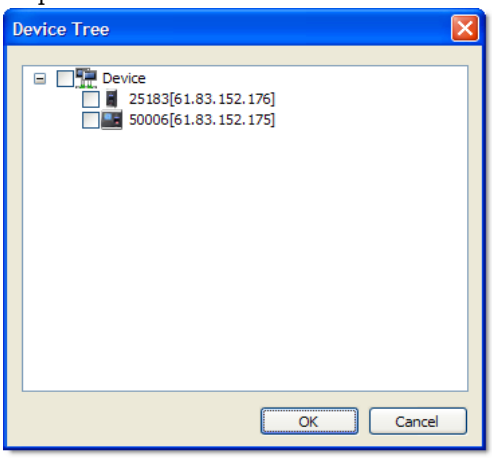
1. Cliccare **Porte** nel menu.
2. Nel menu delle attività, cliccare **Aggiungi Nuova Porta**.
4. Fare clic con il tasto destro su **Nuova Porta**, cliccare **Rinomina**, quindi digitare un nome per la porta.

3.3.2 Associare un dispositivo ad una porta

BioStar permette di associare un massimo di due dispositivi per ogni porta. Quando si utilizzano due dispositivi su una singola porta, essi devono essere connessi fra loro tramite RS485.

Associare un dispositivo ad una porta:

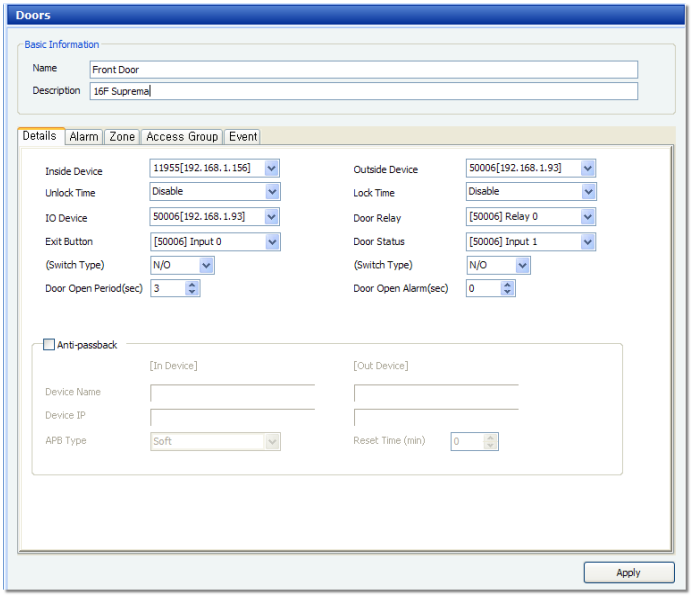
1. Cliccare **Porte** nel menu.
2. Fare clic con il tasto destro su una porta e cliccare **Aggiungere Dispositivo**.
3. Selezionare un dispositivo dall'elenco selezionando il checkbox a fianco del nome del dispositivo.



4. Cliccare **OK**.

3.3.3 Configurare una porta

1. Cliccare **Porte** nel menu.
2. Cliccare sul nome della porta nel menu di navigazione. Si aprirà una finestra “Porte”, come quelle indicata in figura:



3. Configurare le informazioni della porta seguendo le istruzioni:
   - **Dettagli** – Utilizzare questa sezione per controllare le interazioni fra porte, dispositivi, serrature e tasti d’uscita. Se si aggiungono due dispositivi alla porta, è possibile anche configurare le impostazioni di anti-passback.
   - **Allarme** – Utilizzare questa sezione per specificare quali azioni intraprendere quando una porta viene aperta in modo forzato o rimane tenuta aperta.
   - **Zone** – Utilizzare questa sezione per visualizzare le zone associate alla porta.
   - **Controllo Accessi** – Utilizzare questa sezione per visualizzare i gruppi d’accesso associati alla porta.
   - **Eventi** – Utilizzare questa sezione per ottenere e monitorare il registro degli eventi relativi alla porta.
4. Quando la configurazione del dispositivo è terminata, cliccare **Applica** per salvare le modifiche.

3.3.4 Creare un gruppo di porte

È possibile creare gruppi di porte per una gestione più semplice.

1. Cliccare **Porte** nel menu.
2. Nel menu di navigazione, fare clic con il tasto destro su *Doors*, quindi cliccare *Aggiungi Gruppo Porta.*
3. Digitare un nome per il gruppo e premere Invio.

4. Per aggiungere una porta al gruppo, trascinare la porta desiderata sul gruppo.

3.4 Impostare ascensori (Lifts)

Questa sezsione descrive come impostare gli ascensori tramite il sistema BioStar. Per informazioni sull'installazione pratica dei dispositivi e la relativa integrazione con i componenti per gli ascensori, fare riferimento ai manuali dei singoli prodotti. BioStar supporta fino a 128 ascensori (lifts).

3.4.1 Aggiungere un ascensore

Aggiungere un ascensore:

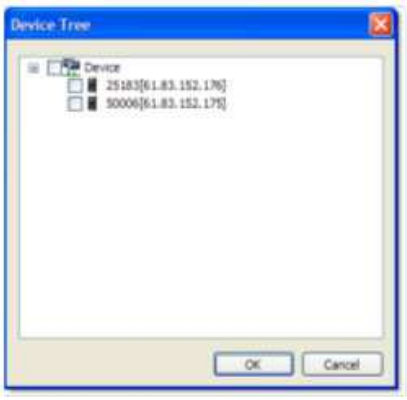
1. Cliccare **Ascensore** nel menu.
2. Nel menu delle attività, cliccare **Aggiungi Nuovo Ascensore**.
3. Fare clic con il tasto destro su **Nuovo Ascensore**, cliccare **Rinomina**, quindi digitare il nome per l'ascensore.

3.4.2 Associare un dispositivo ad un ascensore

BioStar permette di associare un dispositivo Xpass o Xpass Slim ad un dispositivo LIFT I/O per controllare l'accesso agli ascensori. LIFT I/O dev'essere connesso ad un dispositivo Xpass o Xpass Slim tramite RS485.

Associare un dispositivo Xpass o Xpass Slim ad un ascensore:

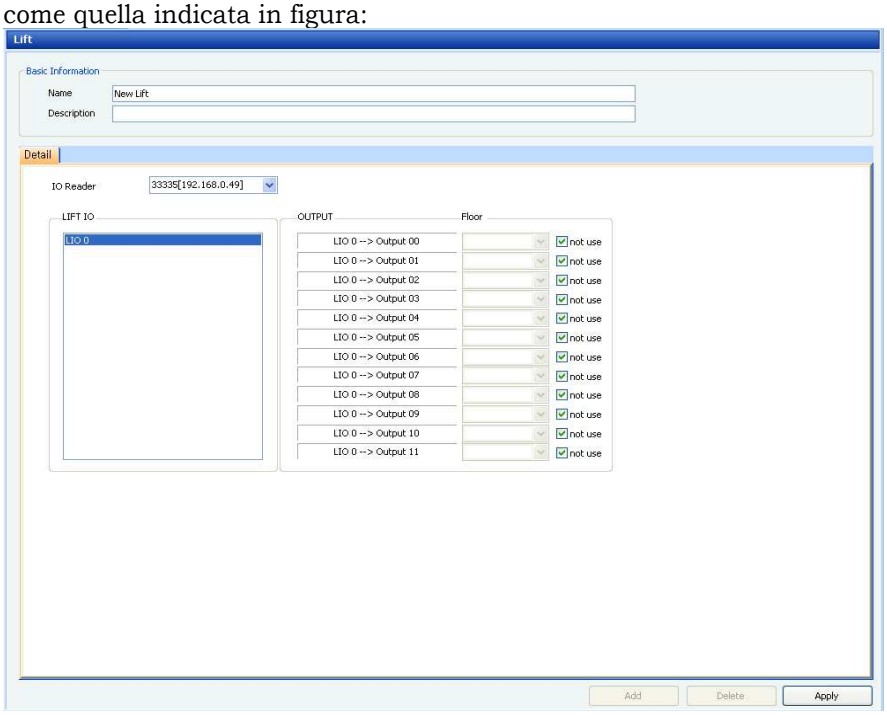
1. Cliccare **Ascensori** nel menu.
2. Fare clic con il tasto destro sul nome dell'ascensore e cliccare **Aggiungi Lettore**.
3. Selezionare un dispositivo Xpass o Xpass Slim dall'elenco cliccando il checkbox di fianco al nome del dispositivo.



4. Cliccare **OK**.

3.4.3 Configurare un ascensore

1. Cliccare **Ascensori** nel menu.
2. Cliccare sul nome di un ascensore nel menu di navigazione. Si aprirà una finestra come quella indicata in figura:

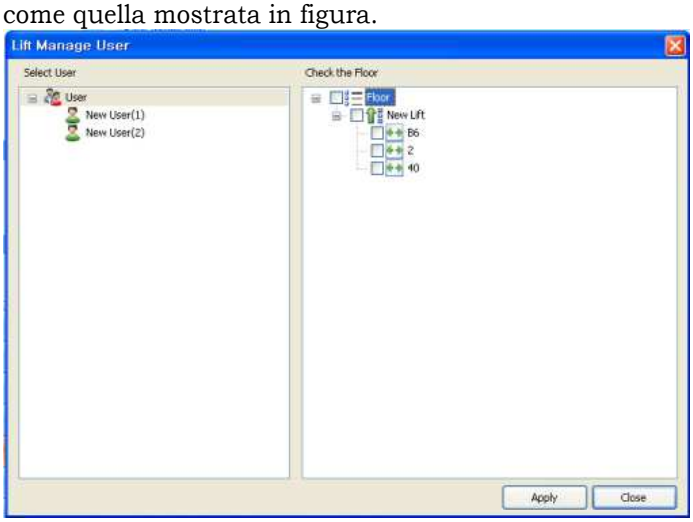


3. Configurare le informazioni di un ascensore come indicato:
   - **LIFT IO** – Selezionare un dispositivo LIFT I/O per visualizzare e modificare le impostazioni.
   - **USCITE** – Indica le uscite disponibili del dispositivo LIFT I/O.
   - **Piano** – Utilizzare questa sezione per visualizzare le zone associate ad una porta.
   - **Non in uso** – Selezionare il checkbox quando non si utilizza un'uscita del dispositivo LIFT I/O. Rimuovere le spunte dai checkbox per controllare l'accesso ai piani associati alle uscite.
4. Quando la configurazione è terminata, cliccare **Applica** per salvare i cambiamenti.

3.4.4 Aggiungere utenti ad un ascensore

1. Cliccare **Ascensore** nel menu.
2. Cliccare sul nome dell'ascensore nel menu di navigazione.

3. Cliccare *Gestione Utenti Ascensore* nel menu di navigazione. Si aprirà una finestra come quella mostrata in figura.



4. Nella schermata a sinistra, cliccare sul nome di un utente.
5. Nella schermata a destra, selezionare il checkbox a fianco del piano a cui si vuole assegnare l'utente.
6. Cliccare **Applica** per salvare le modifiche.

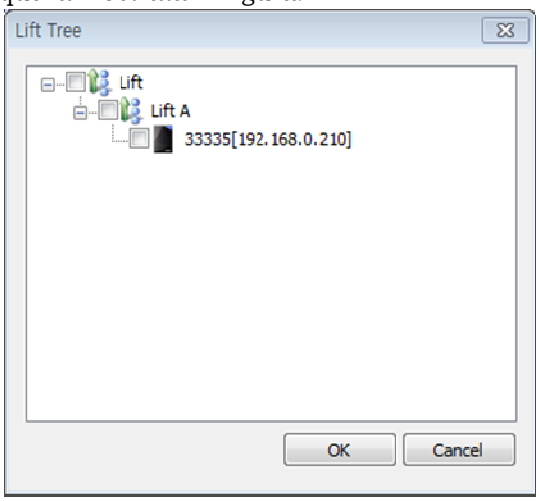
Trasferire le impostazioni ad un ascensore

Attenzione: Utilizzando i dispositivi Xpass o Xpass Slim come lettori per ascensori, il trasferimento delle impostazioni ad un dispositivo tramite il menu Utente comporterà il reset di tutti i dati utente e le impostazioni precedentemente registrate sul dispositivo. Per conservare le impostazioni, utilizzare la funzione *Trasferisci su Dispositivo* nel menu Ascensore.

Inviare le impostazioni e i dati utente ad un dispositivo Xpass o Xpass Slim:

1. Cliccare **Ascensori** nel menu.

2. Cliccare **Trasferisci su Dispositivo** nel menu attività. Si aprirà una finestra come quella mostrata in figura:



3. Nell'elenco degli ascensori, selezionare uno o più dispositivi selezionando il checkbox a fianco del nome.
4. Cliccare **Applica** per inviare le impostazioni dell'ascensore al dispositivo.

3.5 Impostazione Zone

BioStar consente di effettuare la funzione di controllo accessi a zone multiple.
Le zone possono essere utilizzate per controllare dispositivi, porte e altri componenti. Inoltre, le zone possono essere configurate per garantire differenti tipi di restrizione sull'accesso, come anti-passback, anti-passback temporizzato e limiti d'entrata. La sezione sottostante descrive come determinare quale zona utilizzare, come aggiungere e configurare le zone.

3.5.1 Determinare quale zona utilizzare

In totale, il sistema BioStar supporta sette tipologie di zona:

- **Zona Accesso** – Utilizzare questa zona per sincronizzare l'utente o il registro delle informazioni. Se si sceglie la sincronizzazione utente, i dati registrati nel dispositivo verranno automaticamente trasmessi agli altri dispositivi connessi. Se si seleziona l'opzione di sincronizzazione del registro, tutti i campi del registro verranno scritti sul dispositivo principale (oltre che sul server), così da poter visualizzare i campi dei vari dispositivi membri.
- **Zona Anti-passback** – Utilizzare questa zona per evitare che un utente passi la proria carta ad un altra persona, o che usi la propria impronta per garantire l'accesso ad un altro soggetto. La zona supporta due tipi di restrizioni anti-passback. Quando un utente viola il protocollo di anti-passback, il primo grado di restrizione registrerà l'evento nel registro dell'utente. Il secondo grado di restrizione invece impedirà l'accesso

e registrerà l'evento.

- **Limite accesso zona** – Utilizzare questa zona per limitare il numero di accessi all'area che un utente può effettuare. Il limite d'accesso può essere collegato ad una zona oraria, così un utente è limitato ad un numero massimo di accessi in un determinato periodo. È inoltre possibile impostare i limiti per il rientro, così da creare una restrizione anti-passback temporizzata.
- **Zona d'allarme** – Utilizzare questa zona per raggruppare gli ingressi di più dispositivi in una singola zona d'allarme. I dispositivi nella zona d'allarme possono essere armati o disarmati simultaneamente tramite carta o chiave.
- **Zona d'allarme antincendio** – Utilizzare questa zona per controllare quali porte saranno attive durante un incendio. Gli ingressi esterni possono essere impostati tramite BioStar per innescarsi automaticamente lo sblocco della porta o altre azioni.
- **Zona di raccolta** – Utilizzare questa zona per monitorare e tracciare i dipendenti durante un'emergenza, o per impostare una zona di ritrovo in cui è richiesta la presenza dei dipendenti in un particolare momento. La zona di raccolta permette agli amministratori di determinare se un dipendente non è presente nell'area e, se necessario, localizzarlo.
- **Zona di interblocco** – Utilizzare questa zona per creare un'area di interblocco tramite due porte con un dispositivo. Quando un ingreesso esterno indica che una delle due porte è aperta, l'altra rimarrà chiusa per garantire la zona di interblocco. Una porta dotata di lettore che non appartiene a nessun'altra zona può essere utilizzato a questo scopo (massimo 4 zone per lettore).

3.5.2 Aggiungere e configurare le zone

Quando si aggiunge una zona, è possibile utilizzare le quattro schede nella sezione Zone per la configurazione.

- **Dettagli** – Aggiungere dispositivi e specificare gli ingressi o altri parametri per una zona.
- **Allarme** – Specificare allarmi e uscite.
- **Gruppo d'Accesso** – Applicare i gruppi d'accesso alle zone (non disponibile per le zone d'allarme antincendio)
- **Eventi** – Visualizzare gli eventi associati ad una zona.

3.5.2.1 Aggiungere una zona

Aggiungere una nuova zona:

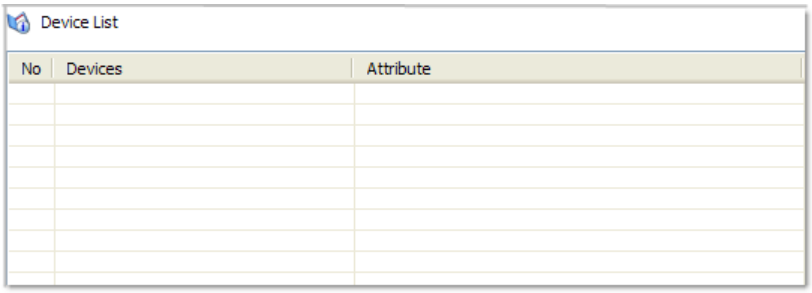
1. Cliccare **Porte** nel menu.
2. Nel menu di navigazione, fare clic con il tasto destro su *Zona*.
3. Cliccare *Aggiungi Zona*.
4. Digitare il nome per la zona nel campo Nome.

5. Selezionare la tipologia di zona dal menu a tenda.
6. Premere **OK**.

Il menu della zona apparirà sul lato destro della finestra.

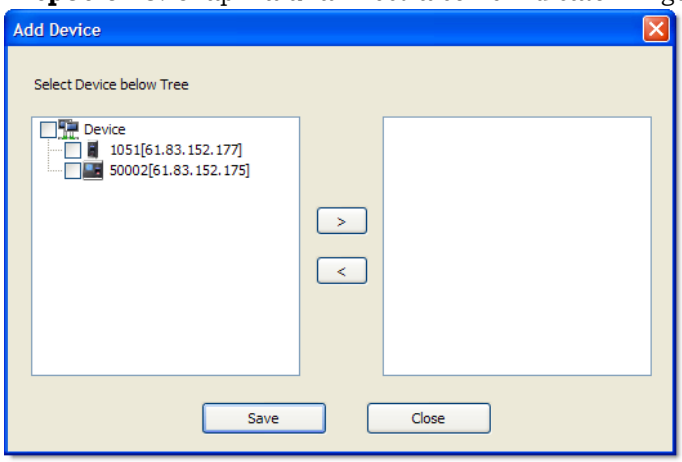
3.5.2.2 Aggiungere un dispositivo ad una zona

Per implementare il protocollo di una zona, è necessario associare i dispositivi alla zona. La scheda Dettagli (nel menu Zona) contiene la lista dei dispositivi, che indica ogni dispositivo associato alla relativa zona.



Aggiungere un dispositivo ad una zona:

1. Cliccare **Porte** nel menu.
2. Nel menu di navigazione, cliccare il nome della zona.
3. Nella scheda Zona, in fondo alla lista dei dispositivi, cliccare **Aggiungi Dispositivo**. Si aprirà una finestra come indicato in figura.



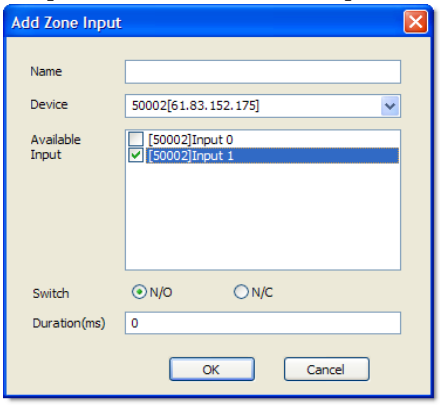
4. Selezionare un dispositivo (o più dispositivi) dalla lista e cliccare "**>**".
   - **Zone Anti-Passback** – quando appare la finestra di selezione, scegliere un elemento dalla lista.
5. **Zone d'Allarme** – quando appare la finestra di selezione, selezionare un dispositivo dall'elenco (Generale, Arma, Disarma, o Arma/Disarma). Se si seleziona l'opzione Arma, Disarma o Arma/Disarma, cliccare il tasto Carta o Chiave per specificare come armare o disarmare la zona, quindi premere **OK**.

3.5.2.3 Configurare gli ingressi delle zone

Quando si aggiungono dispositivi ad una zona d'allarme o d'allarme antincendio, è necessario configurare anche gli ingressi della zona.

Configurare gli ingressi:

1. Cliccare **Porte** nel menu.
2. Nel menu di navigazione, cliccare il nome della zona.
3. Nella finestra Zone, in fondo alla lista dispositivi, cliccare **Aggiungi Ingresso**. Si aprirà una finestra come quella indicata in figura:



4. Digitare un nome per l'ingresso nel campo Nome.
5. Selezionare un dispositivo dal menu a tenda.
6. Selezionare uno degli ingressi disponibili selezionando il checkbox a fianco del relativo ingresso.
7. Selezionare la posizione normale dell'ingresso (*N/O-normalmente aperto o N/C-normalmente chiuso*).
8. Impostare la durata (in millisecondi) del segnale d'ingresso.
9. Cliccare **OK** per aggiungere l'ingresso alla lista.

3.5.2.4 Configurare le azioni d'allarme e le uscite

Configurare le azioni d'allarme per specificare quale segnalazione ricevere e quale porta/relè utilizzare per le uscite d'allarme. La scheda Allarme (menu Zona) offre le seguenti opzioni per tutte le zone eccetto la zona d'accesso.

- **Programmazione Suono** – impostare il suono emesso dal software (PC host o Server BioStar). Per aggiungere suoni personalizzati, fare riferimento alla relativa sezione.
- **Suono Dispositivo** – impostare il suono emesso da un determinato dispositivo.
- **Invia Email** – creazione di una email di allerta quando vi è l'attivazione dell'allarme.
- **Dispositivo d'Uscita** – specificare il dispositivo che invierà una segnalazione d'allarme ad un dispositivo esterno, come una sirena.

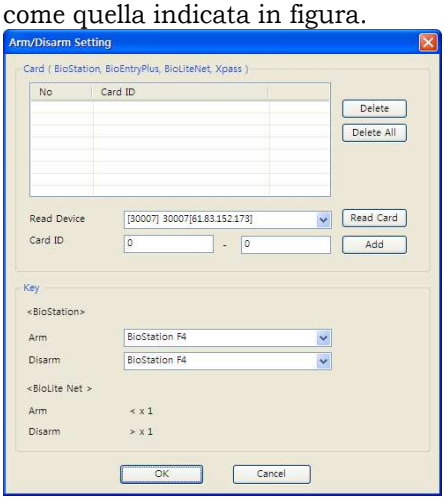
- **Porta Uscita** – specificare la porta utilizzata per il segnale d'uscita.
- **Segnale Uscita** – specificare la tipologia del segnale d'uscita.

3.5.2.5 Configurare le impostazioni arma e disarma

Dopo aver aggiunto una zona d'allarme, è possibile configurare le azioni che armeranno e disarmeranno la zona.

Configurare le impostazioni arma e disarma:

1. Cliccare **Porte** nel menu.
2. Nel menu di navigazione, cliccare sul nome della zona d'allarme. Se necessario, ampliare l'elenco Zona.
3. Cliccare sulla scheda Dettagli nel menu Zona.
4. Cliccare **Setup** a destra della tipologia Arma/Disarma. Si aprirà una finestra come quella indicata in figura.



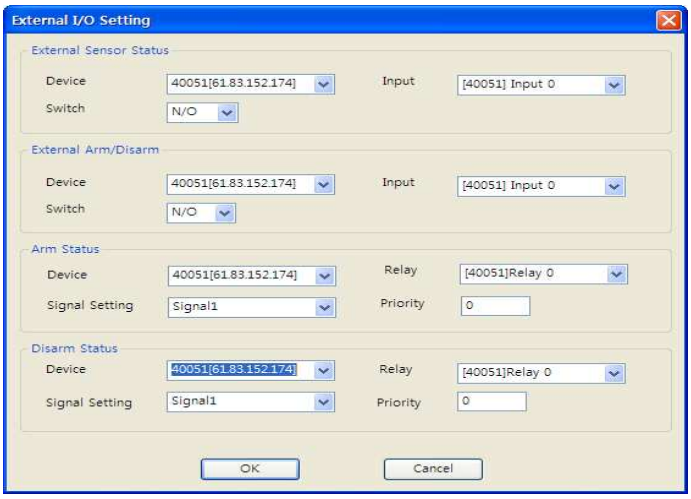
5. Configurare le carte per armare o disarmare le zone:
   a. Selezionare un dispositivo dal menu Leggi Dispositivo.
   b. Cliccare **Leggi Carta**. Il LED sul dispositivo selezionato si illumineranno.
   c. Avvicinare una carta al dispositivo.
   d. Quando la carta è stata letta, cliccare **Aggiungi**. La carta potrà ora essere utilizzata per armare o disarmare dispositivi nella zona d'allarme.
6. Configurare le chiavi per armare o disarmare le zone (BioStation):
   a. Selezionare una chiave per la funzione arma dall'elenco.
   b. Selezionare una chiave per la funzione disarma dall'elenco.
7. Quando la configurazione è terminata, cliccare **OK**.

3.5.2.6 Configurare le impostazioni ingresso/uscita esterni

Invece di effettuare la funzione arma e disarma manualmente, è possibile configurare il sistema BioStar per determinare automaticamente quando armare o disarmare una zona, in base allo stato di uno specifico ingresso. È inoltre possibile prevenire che il sistema BioStar armi una zona d'allarme quando un ingresso monitorato è in una posizione "non pronta". Infine, è possibile configurare il sistema per inviare uno specifico segnale ad un'uscita esterna quando si arma o disarma una zona. Le impostazioni di ingresso/uscita esterne sono disponibili per i dispositivi BioStation V1.8, BioEntry Plus V1.4, BioEntry W V1.0, BioLite Net V1.2, Xpass e Xpass Slim V1.0, D-Station V1.0, X-Station V1.0, BioStation T2 e FaceStation V1.0 o superiore.

Configurare le impostazioni di ingresso/uscita esterne:

1. Cliccare **Porte** nel menu.
2. Nel menu di navigazione, cliccare sul nome della zona d'allarme.
3. Cliccare la scheda Dettagli nel menu Zona.
4. Cliccare **Setup** a destra di Ingresso/Uscita Esterno.
   Si aprirà una finestra come quella indicata in figura.



5. Configurare ingressi/uscite secondo le proprie preferenze:

- Prevenire che il sistema BioStar armi una zona d'allarme:
  a. In "Stato Sensore Esterno", selezionare un dispositivo dall'elenco.
  b. Selezionare un ingresso dall'elenco degli ingressi.
  c. Selezionare la posizione dell'ingresso (*N/O – normalmente aperto* o *N/C – normalmente chiuso*) che previene l'attivazione della funzione Arma per la zona d'allarme.
- Permette al sistema BioStar di armare o disarmare automaticamente una zona d'allarme:
  a. In "Arma/Disarma Esterno", selezionare un dispositivo dall'elenco.
  b. Selezionare un ingresso dall'elenco degli ingressi.
  c. Selezionare la posizione dell'ingresso (*N/O – normalmente aperto o N/C – normalmente chiuso*) che permetterà al sistema di armare la zona d'allarme. L'altra posizione permetterà al sistema di disarmare la zona.
- Inviare una segnalazione "Arma" ad un dispositivo esterno:
  a. In "Arma Stato", selezionare un dispositivo dall'elenco.
  b. Selezionare un relè dall'elenco.
  c. Selezionare il tipo di segnale dall'elenco.
  d. Specificare un livello di priorità.
- Inviare una segnalazione "Disarma" ad un dispositivo esterno:
  a. In "Disarma Stato", selezionare un dispositivo dall'elenco.
  b. Selezionare un relè dall'elenco.
  c. Selezionare un tipo di segnale dall'elenco.
  d. Specificare un livello di priorità.

6. Quando la configurazione è terminata, cliccare **OK**.

3.5.2.7 Selezionare i gruppi d'accesso

La scheda "Gruppo d'Accesso" (nel menu Zona) permette di specificare i gruppi d'accesso che possono bypassare le normali restrizioni per la zona. Ad esempio, è possibile scegliere che un particolare gruppo d'accesso sia esente dalle restrizioni di una zona anti-passback. Per le zone d'allarme, questa scheda permette di specificare i gruppi d'accesso che possono armare e disarmare gli allarmi. Per selezionare un gruppo d'accesso, selezionare il checkbox a fianco del nome del gruppo e cliccare **Applica**.

3.5.2.8 Visualizzare gli eventi della zona

La scheda Evento (neln menu Zona) fornisce una lista di eventi per una particolare zona. È possibile impostare le date dal calendario e visualizzare gli eventi cliccando **Ottieni Registro**.

3.6 Impostazione Utenti

È necessario utilizzare uno scanner di impronte per poter registrare l'impronta di ogni utente. Per questo motivo, risulta funzionale avere un terminale connesso al sistema come centro di registrazione. BioStation, BioEntry Plus, BioEntry W, BioLite Net o D-Station possono essere utilizzati a questo scopo quando connessi in rete con il server BioStar. Oppure è possibile utilizzare il dispositivo BioMini USB, che può essere connesso direttamente al client BioStar.

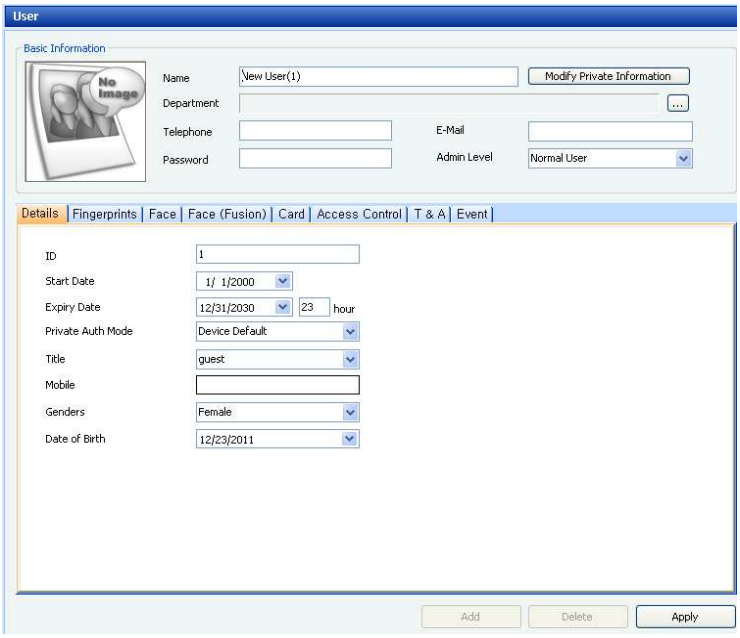
Quando si aggiunge un utente, è necessario prima di tutto creare un account. Quando si dispone dell'account, è possibile registrare le impronte e le carte d'accesso, oppure modificare i dettagli che si desiderano.

3.6.1 Creare un account utente

I dati dell'utente sono controllati tramite il relativo account. È possibile creare nuovi account per gli utenti od ottenere i dati da un dispositivo.

Creare account per nuovi utenti:

1. Cliccare **Utenti** nel menu.
2. Nel menu di navigazione, fare clic con il tasto destro su *Utente* o il nome di un reparto e cliccare *Aggiungi Utente*. Si aprirà un menu come quello in figura.



3. Aggiungere dettagli dell'account utente nel menu:
   - **Nome** – digitare il nome dell'utente.
   - **Settore** – digitare il settore o cliccare il tasto " (...) " per selezionare uno dei settori aggiunti tramite il sistema BioStar.
   - **Telefono** – inserire il numero di telefono dell'utente (solo cifre – nessun carattere alfabetico permesso in questo campo).
   - **E-mail** – digitare l'indirizzo email dell'utente.
   - **Password** – inserire la password per l'utente, se lo si desidera.
     Note: Le password salvate nei dispositivi FaceStation non sono compatibili con altri dispositivi. Quando si trasferiscono dati da un dispositivo FaceStation ad un altra tipologia di dispositivo, è necessario creare una nuova password.
   - **Livello Admin** – selezionare il livello di amministrazione per l'utente. (Utente normale o Utente amministratore).
   - **ID** – inserire un numero identificativo per l'utente.
   - **Data Inizio** – impostare una data iniziale in cui l'utente ottiene l'autorizzazione tramite il sistema BioStar.
   - **Data Scadenza** – impostare una data in cui scadrà la validità dell'account utente (è anche possibile specificare l'ora in cui scadrà).
   - **Titolo** – selezionare un titolo per l'utente (Ospite, Presidente, Direttore, Direttore Generale, Assistente, o un titolo personalizzato).
   - **Cellulare** – inserire il numero di cellulare per l'utente.
   - **Sesso** – selezionare il sesso dell'utente.
   - **Data di Nascita** – selezionare la data di nascita dell'utente dal calendario.

Note: È possibile aggiungere una foto dell'utente o un messaggio privato cliccando su **Modifica Informazioni Private**.

4. Registrare le impronte (vedi sezione 3.6.2), volti (see section 3.6.3), e carte d'accesso come necessario.
5. Quando l'inserimento dei dettagli è terminato, cliccare **Applica**.

3.6.2 Registrare le impronte

BioStar fornisce un'opzione per criptare i template delle impronte. Se si utilizza questa opzione, è necessario attivarla prima di effettuare la scansione. Qualsiasi impronta registrata precedentemente sarà inutilizzabile quando si attivan la crittografia.

Quando si effettua la registrazione delle impronte, è importante ottenere un'ottima qualità delle immagini.

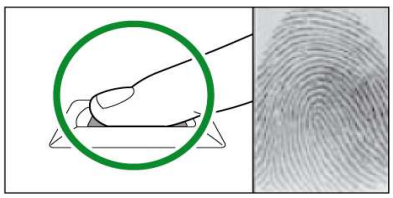
Quando si registrano le impronte digitali, seguire queste istruzioni:

- Registrare la stessa impronta, due volte (due template). È possibile registrare un totale di due impronte per ogni utente (per un totale di quattro template).
- Utilizzare impronte rovinate o con imperfezioni può risultare in una registrazione di qualità inferiore.
- Potrebbe risultare necessario cancellare e registrare nuovamente un'impronta se l'utente è soggetto a un certo numero di errori nel riconoscimento da parte del dispositivo.

3.6.2.1 Posizionare il dito sul sensore

Per garantire una buona qualità delle impronte, gli utenti devono posizionare il dito sul sensore con la maggior superficie possibile.
Si raccomanda l'utilizzo dell'indice o del dito medio per una registrazione dell'impronta performante. Coprire la maggior superficie possibile del sensore, con il dito quasi perpendicolare al sensore.

L'immagine successiva indica un posizionamento corretto e uno scorretto del dito sul sensore.



3.6.2.2 Registrazione impronte

BioStar consente di registrare fino a 10 impronte per utente. Alcuni dispositivi, però, possono contenere un numero limitato di impronte:

- BioEntry Plus, BioEntry W e BioLite Net: fino a due

- BioStation: fino a cinque
- D-Station e BioStation T2: fino a dieci

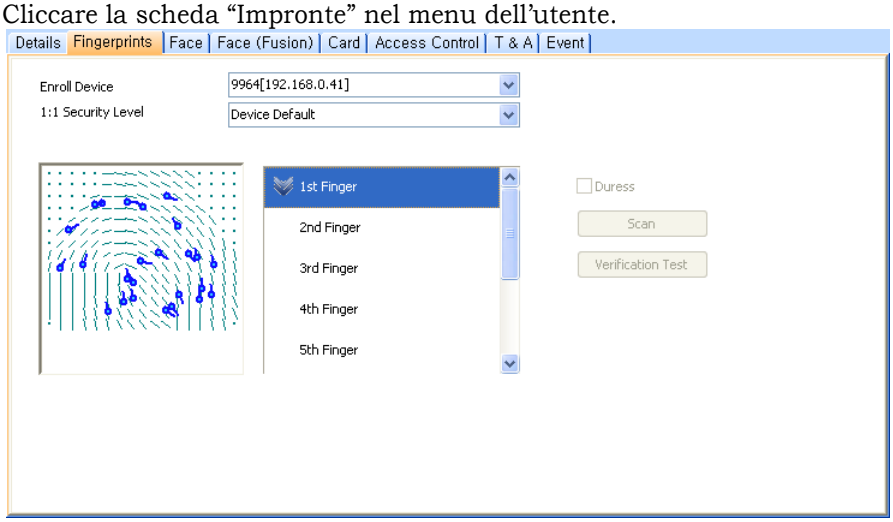
Quando le impronte sono state distribuite dal sistema BioStar, il dispositivo riceverà il massimo numero di impronte, a partire dalla prima impronta registrata.

Se lo si desidera, una delle impronte può essere utilizzata come segnale di coercizione, che farà scattare un allarme quando un utente viene forzato ad accedere ad un'area. Registrando un'impronta per la segnalazione di coercizione, ricordare che:

- Un'impronta coercizione non può essere utilizzata per il normale accesso.
- Utilizzare un dito come indice o medio per la funzione coercizione (la scelta di un dito inusuale potrebbe far sospettare l'intenzione di attivare un allarme)
- L'utente dovrà essere istruito su cosa accadrà quando verrà utilizzata la funzione coercizione (es., potrebbe attivare il blocco automatico della porta o un allarme silenzioso).

Registrare le impronte:

1. Cliccare **Utente** nel menu.
2. Nel menu di navigazione, cliccare sul nome dell'utente.
3. Cliccare la scheda "Impronte" nel menu dell'utente.



4. Selezionare dall'elenco il dispositivo con cui si effettuerà la registrazione delle impronte.
5. Selezionare il livello di sicurezza dall'elenco.
6. Cliccare **Aggiungi** in basso a destra del menu Utente per creare un nuovo elemento vuoto dove registrare l'impronta.
7. Premere **Scan**, quindi far posizionare il dito all'utente sullo scanner per due volte, come indicato dall'interfaccia BioStar.
8. Se lo si desidera, selezionare la checkbox a fianco dell'opzione Coercizione per assegnare l'impronta a quella funzione.

9. Ripetere i passaggi da 6 a 8 per le restanti impronte.
10. Cliccare **Applica** per salvare le modifiche.

3.6.2.3 Registrare gli utenti tramite le carte di comando

Dopo aver creato delle carte di comando, è possibile registrare utenti direttamente da un dispositivo BioEntry Plus, BioEntry W o Xpass.

Registrare un utente su un dispositivo BioEntry Plus o BioEntry tramite carta di comando:

1. Posizionare una carta di registrazione (carta di comando) su un dispositivo BioEntry Plus o BioEntry W.
2. Se è richiesta un'autorizzazione, un amministratore dovrà utilizzare la propria impronta per proseguire nell'operazione.
3. Per registrare le impronte, posizionare il dito sul sensore due volte (come indicato dal dispositivo).
4. Per registrare re impronte e creare carte d'accesso, avvicinare una carta al dispositivo. Quindi, posizionare il dito sul sensore due volte (come indicato dal dispositivo).

Registrare un utente su un dispositivo Xpass tramite carta di comando:

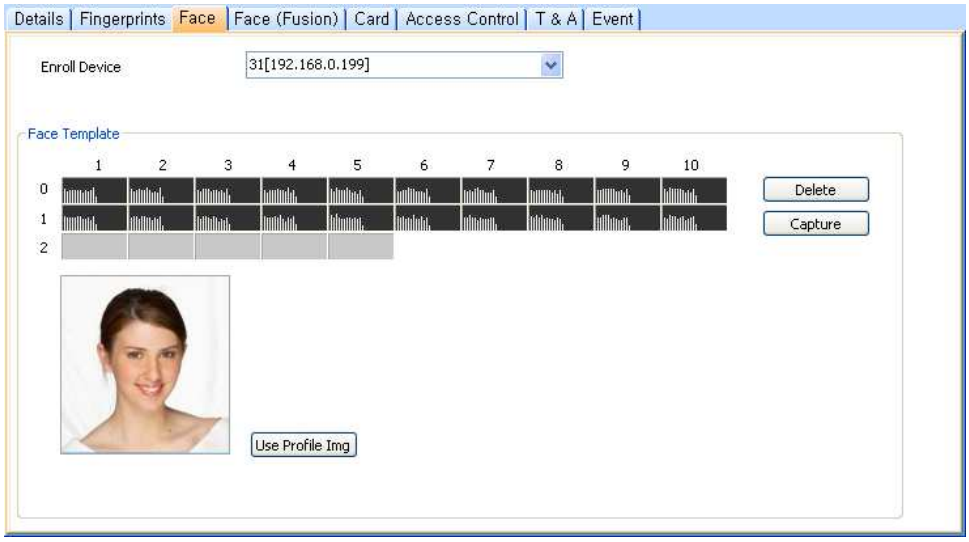
1. Avvicinare una carta di registrazione (carta di comando) su un dispositivo Xpass.
2. Se è richiesta un'autorizzazione, un amministratore dovrà utilizzare la propria carta d'accesso per proseguire nell'operazione.
3. Avvicinare la carta d'accesso dell'utente al dispositivo.
4. Avvicinare la carta di registrazione al dispositivo un'altra volta, per confermare l'azione.

3.6.3 Foto del volto

Con un dispositivo dotato di fotocamera, come ad esempio D-Station e FaceStation, è possibile effettuare le foto dei volti degli utenti, utilizzandole come metodo di autenticazione tramite la tecnologia di riconoscimento facciale BioStar. L'immagine del volto dell'utente viene comparata all'immagine registrata nel database. Il riconoscimento del volto può essere utilizzato contemporaneamente all'identificazione tramite impronte, per un alto livello di sicurezza.

Registrare immagini del volto con i dispositivi FaceSation:

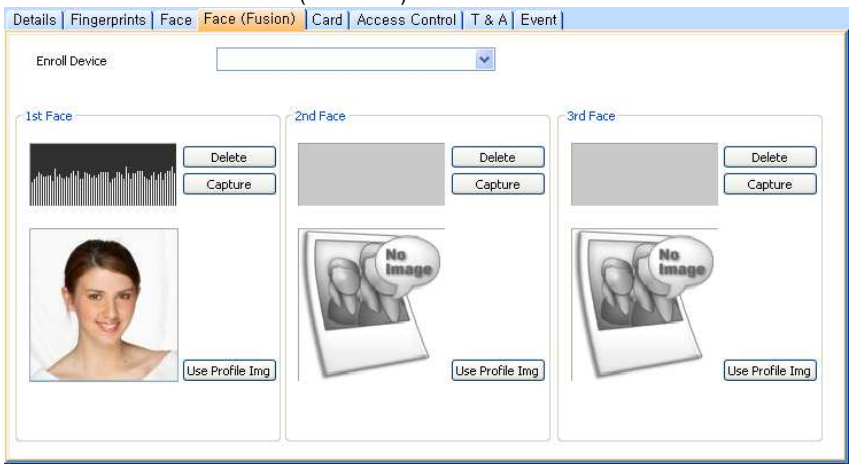
1. Cliccare **Utente** nel menu.
2. Nel menu di navigazione, cliccare sul nome dell'utente.
3. Cliccare la scheda Volto nel menu utente.



4. Selezionare dall'elenco il dispositivo che verrà utilizzato per la registrazione dell'immagine del volto.
5. Nella sezione Template Volto, cliccare **Ottieni foto**, quindi allineare il volto dell'utente alla fotocamera, come indicato dal dispositivo.
6. Se lo si desidera, cliccare **Utilizzare Immagine Profilo** per utilizzare l'immagine ottenuta nel profilo.
7. Cliccare **Applica** per salvare le modifiche.

Registrare immagini del volto con i dispositivi D-Station:

1. Cliccare **Utente** nel menu.
2. Nel menu di navigazione, cliccare sul nome utente.
3. Cliccare la scheda Volto (Fusione) nel menu Utente.



4. Selezionare dall'elenco il dispositivo che verrà utilizzato per la registrazione dell'immagine del volto.
5. Nella prima sezione, cliccare **Ottieni foto**, quindi allineare il volto dell'utente alla fotocamera, come indicato dal dispositivo.

6. Se lo si desidera, cliccare **Utilizzare Immagine Profilo** per utilizzare l'immagine ottenuta nel profilo.
7. Ripetere i passaggi 5-7 nella seconda e terza sezione per registrare ulteriori immagini.
8. Cliccare **Applica** per salvare le modifiche.

3.6.4 Creare carte d'accesso

I dispositivi Suprema supportano diverse tipologie di carte d'accesso:

- EM4100: BioStation, BioEntry Plus e BioLite Net
- MIFARE®: BioStation Mifare, BioEntry Plus Mifare, BioEntry W Mifare, BioLite Net, D-Station e FaceStation
- iCLASS®: BioEntry Plus iCLASS
- FeliCa®: BioEntry Plus iCLASS
- HID proximity: BioStation HID e BioEntry Plus HID

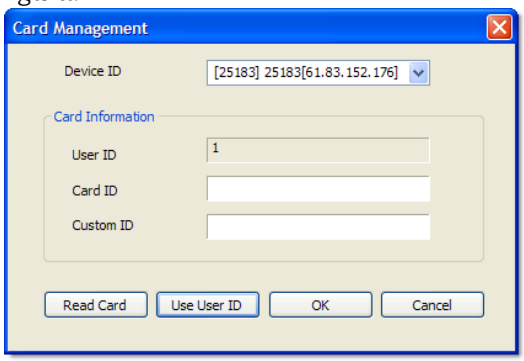
Le carte EM4100 e HID richiedono solo l'ID per effettuare la registrazione, mentre le carte MIFARE e iCLASS supportano due modalità operative: Numero Seriale della Carta (CSN) e Template-su-Carta. Le carte FeliCa supportano solo la modalità CSN. Quando si utilizza la modalità CSN, è possibile leggere il numero seriale come con una carta EM4100 o HID. Quando si utilizza la modalità Template-su-Carta, è necessario registrare le informazioni dell'utente, inclusi i template delle impronte, direttamente sulla carta.

Seguire le procedure per creare l'appropriata tipologia di carta, quindi aggiungerla all'account dell'utente.

3.6.4.1 Creare carte EM4100

Registrare una carta per l'utente:

1. Cliccare **Utente** nel menu.
2. Nel menu di navigazione, cliccare il nome dell'utente.
3. Nel menu Utente, cliccara la scheda Carta.
4. Selezionare come tipologia di carta "EM4100" dall'elenco.
5. Cliccare **Gestione Carta**. Si aprirà una finestra come quella indicata in figura.

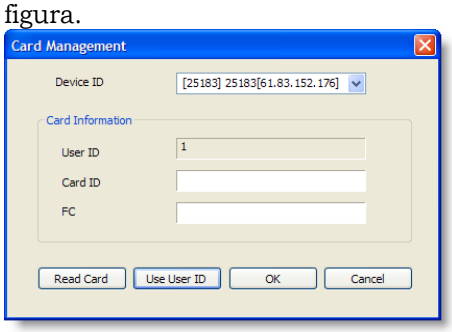


6. Selezionare l'ID del dispoisitivo dall'elenco.
7. Inserire l'ID della carta (32 bit) e l'ID personalizzato (8 bit) manualmente o leggendolo dalla carta (è anche possibile cliccare **Utilizza ID Utente** per inserire l'ID dell'utente in questi campi):
   - Per inserire i dati manualmente, digitare l'ID della carta e l'ID personalizzato nei campi corrispondenti, cliccare OK, quindi proseguire con le istruzioni riportate al punto 8.
   - Per leggere i dati dalla carta, cliccare **Leggi Carta** (il LED sul dispositivo selezionato si illuminerà), quindi avvicinare la carta al dispositivo. Dopo la lettura della carta, cliccare **OK**.
8. Cliccare **Applica** per salvare la carta nell'account utente.

3.6.4.2 Creare carte di prossimità HID

Registrare una carta per l'utente:

1. Cliccare **Utente** nel menu.
2. Nel menu di navigazione, cliccare sul nome dell'utente.
3. Nel menu Utente, cliccare sulla scheda Carta.
4. Selezionare "HID Prox" dall'elenco delle tipologie di carta.
5. Cliccare **Gestione Carta**. Si aprirà una finestra come quella indicata in figura.

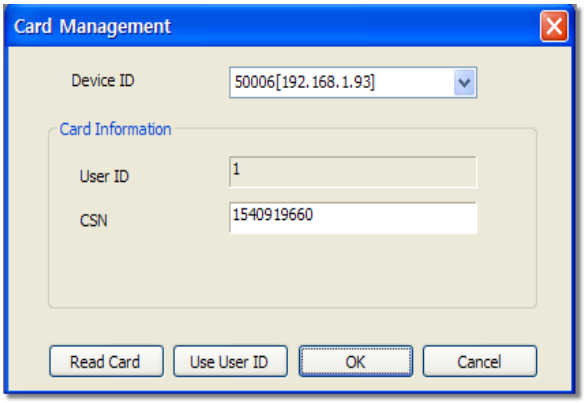


6. Selezionare l'ID di un dispositivo dall'elenco.
7. Digitare l'ID della carta e il codice di fabbrica (FC) manualmente o tramite lettura della carta (è anche possibile cliccare **Utilizza ID Utente** per inserire l'ID dell'utente in questi campi):
   - Per inserire i dati manualmente, digitare l'ID e il codice di fabbrica nei campi corrispondenti, cliccare OK, quindi proseguire con le istruzioni riportate al punto 8.
   - Per leggere i dati dalla carta, cliccare **Leggi Carta** (il LED sul dispositivo selezionato si illuminerà), quindi avvicinare la carta al dispositivo. Dopo la lettura della carta, cliccare **OK**.
8. Cliccare **Applica** per salvare la carta nell'account utente.

3.6.4.3 Creare carte MIFARE o iCLASS CSN

Le carte MIFARE e iCLASS CSN operano come le carte EM4100 e HID, in cui registrano un numero seriale non modificabile (CSN) per l'utente.
Registrare una carta per l'utente:

1. Cliccare **Utente** nel menu.
2. Nel menu di navigazione, cliccare In the navigation pane, click a user's name.
3. Nel menu Utente, cliccare sulla scheda Carta.
4. Selezionare "Mifare CSN" o "iCLASS CSN" dall'elenco.
5. Cliccare **Gestione Carta**. Si aprirà una finestra come quella indicata in figura.

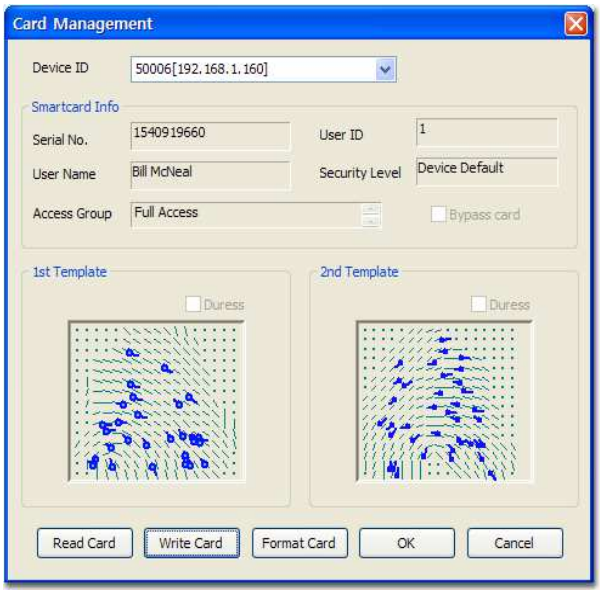


6. Selezionare l'ID del dispositivo dall'elenco.
7. Digitare l'ID della carta manualmente o tramite lettura della carta (è anche possibile cliccare **Utilizza ID Utente** per inserire l'ID dell'utente in questi campi):
   - Per inserire i dati manualmente, digitare l'ID e il codice di fabbrica nei campi corrispondenti, cliccare OK, quindi proseguire con le istruzioni riportate al punto 8.
   - Per leggere i dati dalla carta, cliccare **Leggi Carta** (il LED sul dispositivo selezionato si illuminerà), quindi avvicinare la carta al dispositivo. Dopo la lettura della carta, cliccare **OK**.
8. Cliccare **Applica** per creare la carta nell'account utente.

3.6.4.4 Issue MIFARE or iCLASS template cards

I template delle carte MIFARE e iCLASS permettono di registrare le informazioni dell'utente e i template delle impronte direttamente sulla carta.
Registrare una carta per l'utente:

1. Cliccare **Utente** nel menu.
2. Nel menu di navigazione, cliccare In the navigation pane, click a user's name.
3. Nel menu Utente, cliccare sulla scheda Carta.
4. Selezionare "Template Mifare" o "Template iCLASS" dall'elenco.
5. Cliccare **Gestione Carta**. Si aprirà una finestra come quella indicata in figura.



6. Selezionare l'ID del dispositivo o un dispositivoUSB MIFARE (se connesso) dall'elenco.
7. Se lo si desidera, cliccare Carta Bypass per consentire all'utente di evitare l'identificazione tramite impronta.
8. Cliccare **Leggi Carta**. Il LED sul dispositivo selezionato si illuminerà.
9. Avvicinare la carta al dispositivo.
10. Dopo aver terminato la lettura della carta, cliccare **OK**.
11. Cliccare **Applica** per creare la carta nell'account utente.

Note: Le carte iCLASS 2000, 2002 e 2004 non sono supportate come template.

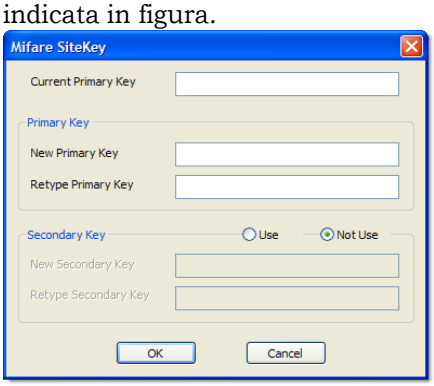
3.6.4.5 Modificare la site key MIFARE o iCLASS

La protezione crittografica per le carte MIFARE e iCLASS è gestita da una site key a 48-bit. Solo le carte con un'appropriata site key possono essere lette dai dispositivi connessi. BioStar permette di definire fino a due site key (primaria e secondaria), così da poter modificare quelle delle carte già esistenti.

Note: Le site keys devono essere protette con attenzione, in quanto sarebbe possibile bypassare il sistema di sicurezza se in possesso della stessa.

Modificare site key MIFARE o iCLASS:

1. Dalla barra del menu, cliccare **Opzioni > Carte Mifare** o **Carte iCLASS > Sitekey Mifare** o **Sitekey iCLASS**. Si aprirà una finestra come quella indicata in figura.



2. Digitare la chiave primaria nel campo "Nuova Chiave Primaria".
3. Digitare di nuovo la chiave primaria nel relativo campo.
4. Cliccare il tasto *Utilizza* per attivare la funzione di chiave secondaria. Questo permette la lettura con un vecchio codice, oltre alla possibilità di sovrascriverle con il nuovo codice:
   a. Digitare il sitekey precedente nel campo *Nuova Chiave Secondaria*.
   b. Digitare di nuovo nel relativo campo.
5. Quando le modifiche sono terminate, cliccare **OK**.

Note: Quando tutte le carte sono state riscritte, comparirà un messaggio per ricordare di disattivare la funzione, per prevenire accessi tramite le carte con il vecchio codice.

3.6.4.6 Modificare il layout MIFARE

BioStar permette di personalizzare il layout utilizzato per registrare le informazioni dell'utente e i template delle impronte. Questo layout verrà applicato a tutte le nuove carte MIFARE create con il dispositivo specificato (BioStawtion Mifare, BioEntry Plus Mifare, BioEntry W Mifare, BioLite Net, D-Station o FaceStation).

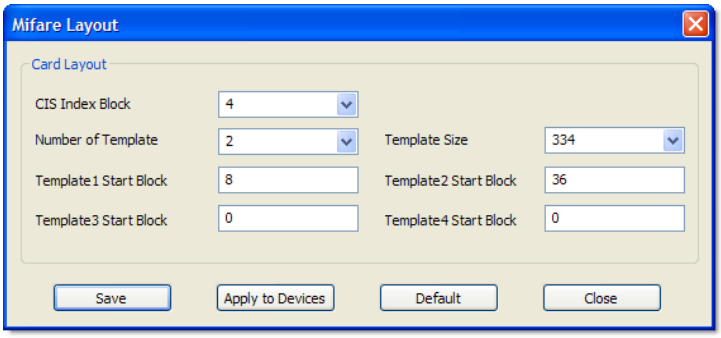
Le carte MIFARE 1K sono disposte in 16 settori, con 4 blocchi da 16 bite ognuno. Le carte MIFARE 4K sono diposte in 32 settori con 4 blocchi e 8 settori con 16 blocchi.

Caratteristiche dei layout MIFARE:

- Il primo settore (dal blocco 0 al blocco 3) è riservato e non potrà essere utilizzati per ulteriori dati.
- L'ultimo blocco di ogni settore (blocchi 3, 7, 11, ecc.) è riservato per le informazioni di protezione.
- Il settore delle informazioni sulla carta (CIS) occupa tre blocchi adiacenti e inizierà ad primo blocco disponibile di un settore (blocchi 4, 8, 12, ecc).
- Non dovranno esserci sovrapposizioni fra i dati di ogni template.

Modificare il layout MIFARE:

1. Dalla barra del menu, cliccare **Opzioni > Carta Mifare > Layout Mifare**. Si aprirà una finestra come indicata in figura.



2. Utilizzare il menu ad elenco e i campi per configurare i seguenti parametri nel layout MIFARE:
   - **Indice Blocco CIS** – selezionare l'indice del blocco da utilizzare per le informazioni (4, 8, 12 o 16).
   - **Numero di Template** – selezionare il numero di template da includere nel layout (da 0 a 4).
   - **Dimensione Template** – selezionare il numero di byte da utilizzare nel template. La dimensione stasndard è 334 byte.
   - **Blocco Iniziale Template 1-4** – inserire il blocco iniziale per ogni template.
3. Per utilizzare il layout personalizzato, cliccare **Applica ai Dispositivi** e selezionare i relativi numeri dei dispositivi nella finestra Dispositivi.
4. Per salvare le modifiche, cliccare **Salva**.
   Note: Per azzerare qualsiasi cambiamento effettuato, cliccare su **Default**. Per uscire senza salvare, cliccare **Chiudi**.

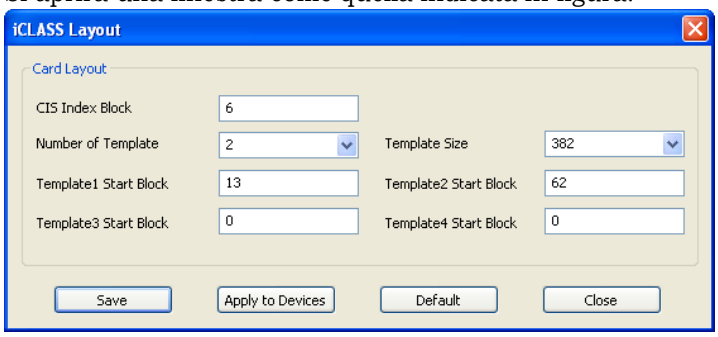
3.6.4.7 Modificare il layout iCLASS

BioStar permette di personalizzare il layout utilizzato per registrare le informazioni dell'utente e i template delle impronte. Questo layout verrà applicato a tutte le nuove carte iCLASS create con i dispositivi BioEntry Plus iCLASS.

I dispositivi BioEntry Plus iCLASS supportano carte iCLASS 16k bit (2k Byte) e 32k bit (4k Byte). Le carte 16k bit (2k Byte) sono disponibili con 2 o 16 aree d'applicazione, mentre sono organizzate in 237 blocchi da 8 byte ognuno. Le carte a 32k bit (4k Byte) sono disponibili con 2 o 16 aree d'applicazione, più 16k aggiuntivi di memoria configurabili dall'utente, organizzati in 8 pagine composte da 26 blocchi di 8 byte ognuno.

Modificare il layout iCLASS:

1. Dalla barra del menu, cliccare **Opzioni > Carta iCLASS > Layout iCLASS**. Si aprirà una finestra come quella indicata in figura.



2. Inserire i seguenti parametri del laout iCLASS:
   - **Indice Blocco CIS** – selezinare l'indice del blocco da utilizzare per le informazioni (il valore standard è 13).
   - **Numero di Template** – selezionare il numero di template da includere nel layout (di base 2).
   - **Dimensione del Template** – selezionare il numero di byte da utilizzare nel template. La dimensione standard è 382 byte.
   - **Blocco di Inizio Template 1-4** – inserire il blocco iniziale per ogni template delle impronte (Il valore di base del template 1 è 19; il valore di base del template 2 è 67).
3. Per utilizzare il layout personalizzato, cliccare **Applica ai Dispositivi** e selezionare i relativi numeri dei dispositivi dalla finestra Dispositivi.

Per salvare le modifiche, cliccare **Salva**.

Note: Per azzerare qualsiasi cambiamento effettuato, cliccare su **Default**.

Per uscire senza salvare, cliccare **Chiudi**.

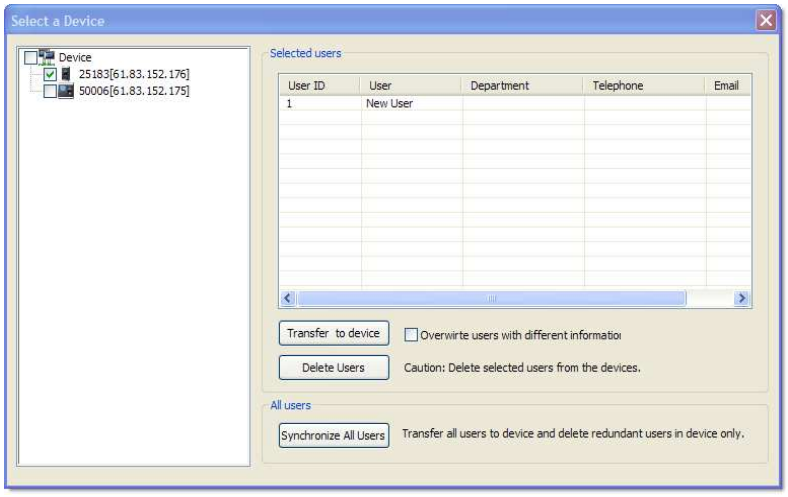
3.6.5 Trasferire Dati Utente

BioStar permette di trasferire automaticamente le informazioni degli utenti sui dispositivi, selezionando l'impostazione "Auto" nel menu (**Opzioni > Utente > Modalità Trasferimento > Auto**). È anche possibile trasferire i dati manualmente. In questo caso, è possibile selezionare singoli utenti o sincronizzarli tutti contemporaneamente. BioStar permette inoltre di ottenere dati da un dispositivo e trasferirli sul server BioStar.

3.6.5.1 Trasferire un utente su un dispositivo

Trasferire uno o più utenti ad uno o più dispositivi:

1. Cliccare **Utente** nel menu.
2. Nel menu, cliccare *Trasferire Utenti al Dispositivo*. Si aprirà una finestra come quella indicata in figura.



3. Selezionare uno o più dispositivi dall'elenco sulla sinistra selezionando i checkbox a fianco del nome.
4. Cliccare il nome di un utente (tener premuto CTRL e cliccare sui nomi per selezionare più utenti).
5. Se lo si desidera, cliccare le checkbox per sovrascrivere gli utenti con differenti informazioni.
6. Cliccare **Trasferisci al Dispositivo** per inviare le informazioni dell'utente ai dispositivi selezionati.

Note: È possbile cancellare gli utenti da questo menu. L'azione non può essere annullata, quindi utilizzare la funzione di cancellazione con cautela. Per cancellare gli utenti dal dispositivo, cliccare sul nome dell'utente, quindi cliccare **Cancella Utenti**.

Quando si utilizano i dispositivi Xpass o Xpass Slim come lettori per ascensori, trasferire le impostazioni sui dispositivi tramite il menu Utente comporterà la cancellazione dei dati precedenti. Per conservare questi dati, utilizzare invece la funzione *Trasferisci sul Dispositivo* dal menu ascensore.

3.6.5.2 Sincronizzare tutti gli utenti

Sincronizare tutte le informazioni degli utenti tra il server BioStar e i dispositivi connessi:

1. Cliccare **Utenti** nel menu.
2. Nel menu delle attività, cliccare *Trasferisci Utenti sul Dispositivo*. Si aprirà una finestra di selezione dei dispositivi.
3. Selezionare uno o più dispositivi dall'elenco sulla sinistra selezionando il checkbox a fianco del nome del dispositivo.
4. Cliccare **Sincronizza Tutti gli Utenti**.

3.6.5.3 Ottenere i dati utente da un dispositivo

Ottenere i dati utente da un dispositivo:

1. Cliccare **Utente** nel menu.
2. Nel menu attività, cliccare **Gestisci Utenti nel Dispositivo**.
   Si aprirà una finestra come quella indicata in figura.

3. Cliccare sul nome di un dispositivo nell'elenco a sinistra per visualizzare i template contenuti nel dispositivo.
4. Cliccare su un utente nella lista Informazioni Template (i nuovi utenti verranno evidenziati in giallo).
5. Cliccare **Ottieni dal Dispositivo**.

Note: È possbile cancellare gli utenti da questo menu. L'azione non può essere annullata, quindi utilizzare la funzione di cancellazione con cautela. Per cancellare gli utenti dal dispositivo, cliccare sul nome dell'utente, quindi cliccare **Cancella Utenti**.

Nelle informazioni sui template, il riferimento"Num Template" indica il numero di template impronte registrati nel dispositivo, mentre "Num Volto" indica il numero di template immagini del volto registrati nel dispositivo. Le immagini ottenute tramite i dispositivi D-Station non verranno conteggiate nel totale "Num Template".

Attenzione: Se vi sono utenti identici nel database BioStar quando si prelevano i dati dai dispositivi Xpass, i dati verranno sovrascritti senza includere l'impronta digitale, in quanto Xpass non supporta questo tipo di dato.

3. Impostare il sistema BioStar

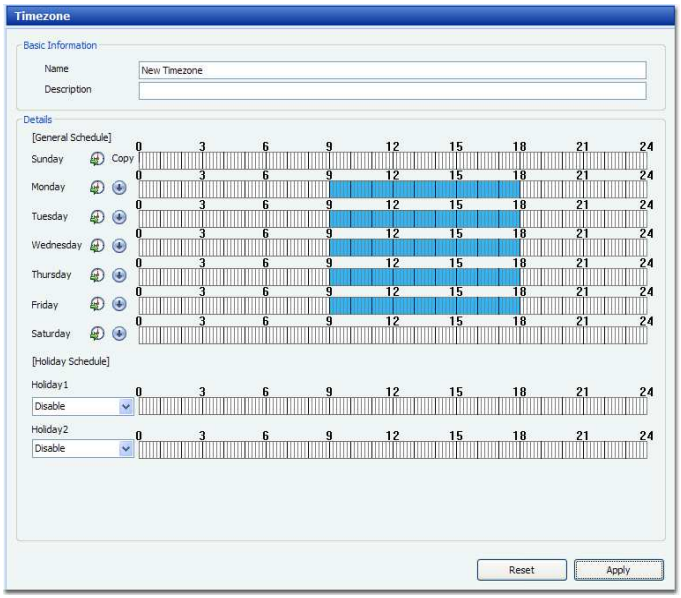
3.7 Setup Timezones

Nel sistema BioStar, le zone orarie sono utilizzate per schedulare i permessi e le restrizioni. È possibile applicare zone orarie per limitare le ore d'accesso ad una porta per un determinato utente, combinando porte e zone nei gruppi d'accesso.

3.7.1 Creare una zona oraria

Creare una schedulazione oraria:

1. Cliccare **Controllo Accessi** nel menu.
2. Nel menu attività, cliccare *Nuova Zona Oraria.*
3. Digitare il nome per la zona oraria.
4. Nel menu della zona oraria, creare una schedulazione settimanale evidenziando le ore effettive per ogni giorno. È possibile copiare la schedulazione per utilizzarla in altri giorni cliccando la freccia a destra del giorno.



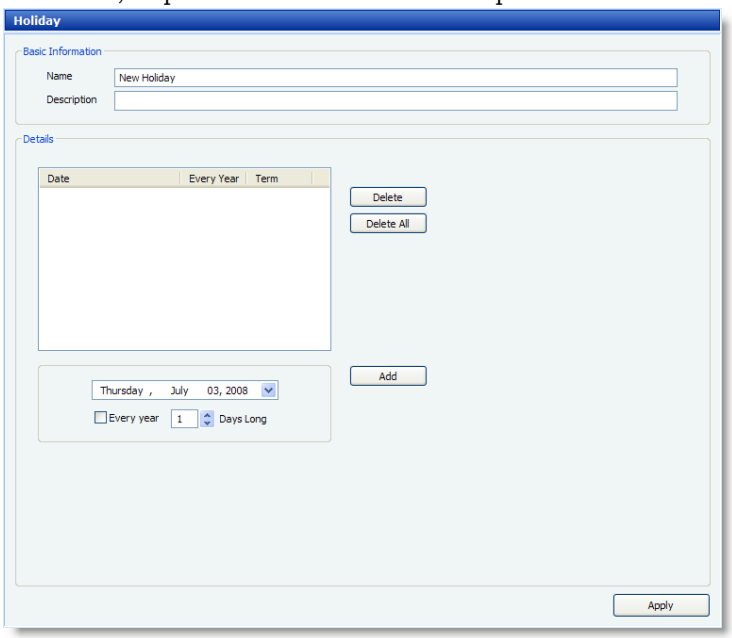
5. Se lo si desidera, è possibile aggungere fino a due schedulazioni festive alla zona oraria.
6. Quando la creazione delle zone orarie è terminata, cliccare **Applica**.
7. Successivamente, trasferire i dati delle zone orarie ai dispositivi:
   a. Nel menu attività, cliccare *Trasferisci al Dispositivo.* Si aprirà la finestra dei dispositivi.
   b. Selezionare uno o più dispositivi selezionando le checkbox nell'elenco Dispositivi.
   d. Cliccare **OK**.

Ora è possibile combinare le zone orarie con i permessi legati alle porte, per creare un gruppo d'accesso.

3.7.2 Creare una schedulazione festiva

Creare una schedulazione festiva:

1. Cliccare **Controllo Accessi** nel menu.
2. Nel menu attività, cliccare *Nuovo Festivo*.
3. Digitare il nome per il festivo.
4. Nel menu, impostare la data di inizio del periodo festivo.



5. Se ricorre ogni anno, selezionare la checkbox sotto l'elenco.
6. Impostare la durata del festivo (espresso in giorni).
7. Cliccare **Aggiungi** per aggiungere ferie alla lista.
8. Cliccare **Applica**.

3.8 Impostare i gruppi d'accesso

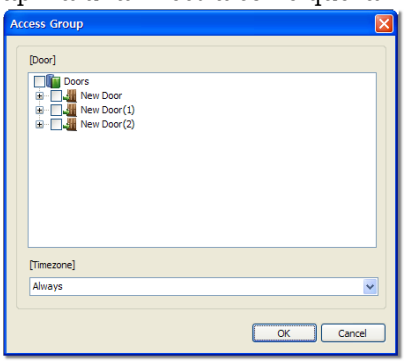
I gruppi d'accesso permettono di definire le autorizzazioni agli utenti ad accedere a determinate porte o zone orarie. Prima di aggiungere un gruppo d'accesso, è necessario impostare le porte e le zone orarie. Dopo aver creato i gruppi d'accesso, i dati dovranno essere trasferiti manualmente ai dispositivi collegati.

3.8.1 Add an Access Group

Aggiungere un gruppo d'accesso:

1. Cliccare **Controllo Accessi** nel menu.
2. Nel menu delle attività. cliccare *Nuovo Gruppo d'Accesso*.
3. Digitare un nome per il nuovo gruppo d'accesso nel box che appare nel menu, quindi cliccare Invio.

4. Nella sezione Controllo Accessi (nel menu Gruppo d'Accesso), cliccare **Aggiungi**. Si aprirà una finestra come quella mostrata in figura.



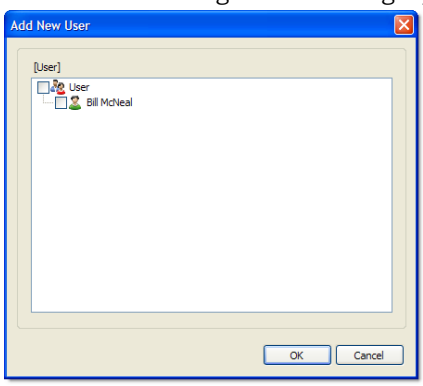
5. Selezionare le porte da aggiungere al gruppo selezionando le checkbox a fianco.
6. Selezionare la zona oraria da applicare al gruppo dall'elenco nella parte inferiore della finestra.
7. Ripetere i passaggi 5 e 6, se necessario, per aggiungere ulteriori porte e zone ai gruppi d'accesso.
8. Cliccare **OK** per aggiungere gli elementi selezionati ai gruppi.

3.8.2 Aggiungere utenti ai gruppi d'accesso

Dopo aver creato i gruppi d'accesso, è necessario aggiungere gli utenti. È possibile aggiungerli nella scheda Utente, oppure assegnare direttamente i gruppi agli utenti tramite il menu Utente. È possibile assegnare un utente ad un massimo di quattro gruppi d'accesso.

Aggiungere gli utenti ai gruppi d'accesso:

1. Cliccare **Controllo Accessi** nel menu.
2. Dalla scheda Utente (nel menu Gruppo d'Accesso), cliccare **Aggiungi**.
3. Nella schermata Aggiungi Nuovo Utente, selezionare gli elementi da aggiungere selezionando i singoli utenti o i gruppi.



4. Cliccare **OK**.

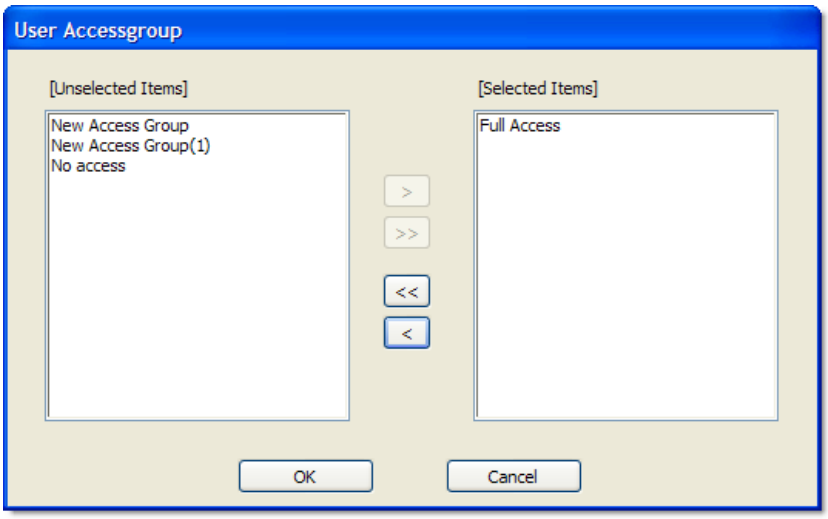
Se sono stati creati gruppi utente, gli utenti appariranno sotto il rispettivo gruppo.

3.8.3 Assegnare gruppi d'accesso agli utenti

È possibile definire a quali gruppi d'accesso appartiene un utente (fino ad un massimo di quattro) tramite il menu Utente.

Assegnare un gruppo d'accesso ad un utente:

1. Cliccare **Utente** nel menu.
2. Nel menu di navigazione, cliccare sul nome di un utente.
3. Cliccare sulla scheda Controllo Accessi nel menu Utente.
4. Cliccare **Aggiungi**. Si aprirà una finestra come quella mostrata in figura.



5. Cliccare sul nome di un gruppo d'accesso dall'elenco, quindi cliccare "**>**".
6. Ripetere, se necessario, il passaggio 5 per assegnare ulteriori gruppi d'accesso.
7. Quando l'assegnazione dei gruppi d'accesso è terminata, cliccare **OK**.

3.8.4 Trasferire i gruppi d'accesso ai dispositivi

1. Cliccare **Controllo Accessi** nel menu.
2. Cliccare *Trasferisci sul Dispositivo*. Si aprirà una finestra con l'elenco dei dispositivi.
3. Selezionare uno o più dispositivi selezionando le checkbox dall'elenco.
4. Cliccare **OK**.

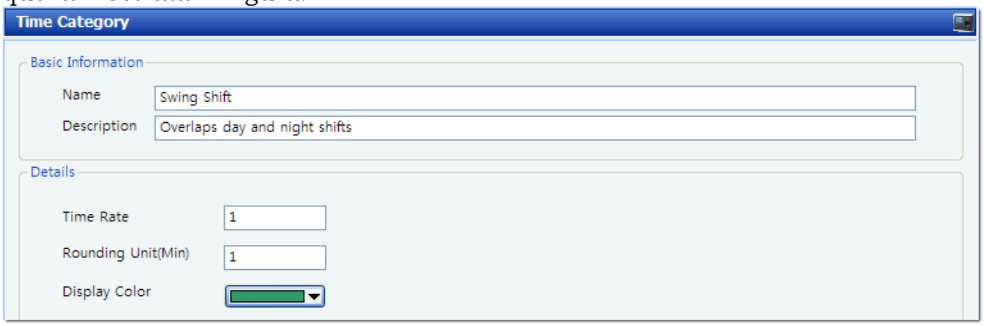
3.9 Impostazione controllo presenze

L'opzione di Controllo Presenze del software BioStar permette di definire categorie di tempo, passaggi e regole per i festivi.

3.9.1 Aggiungere una categoria di tempo

Aggiungere una categoria di tempo:

1. Cliccare **Controllo Presenze** nel menu.
2. Nel menu attività, cliccare *Aggiungi Categoria di Tempo*. Si aprirà una finestra come quella mostrata in figura.



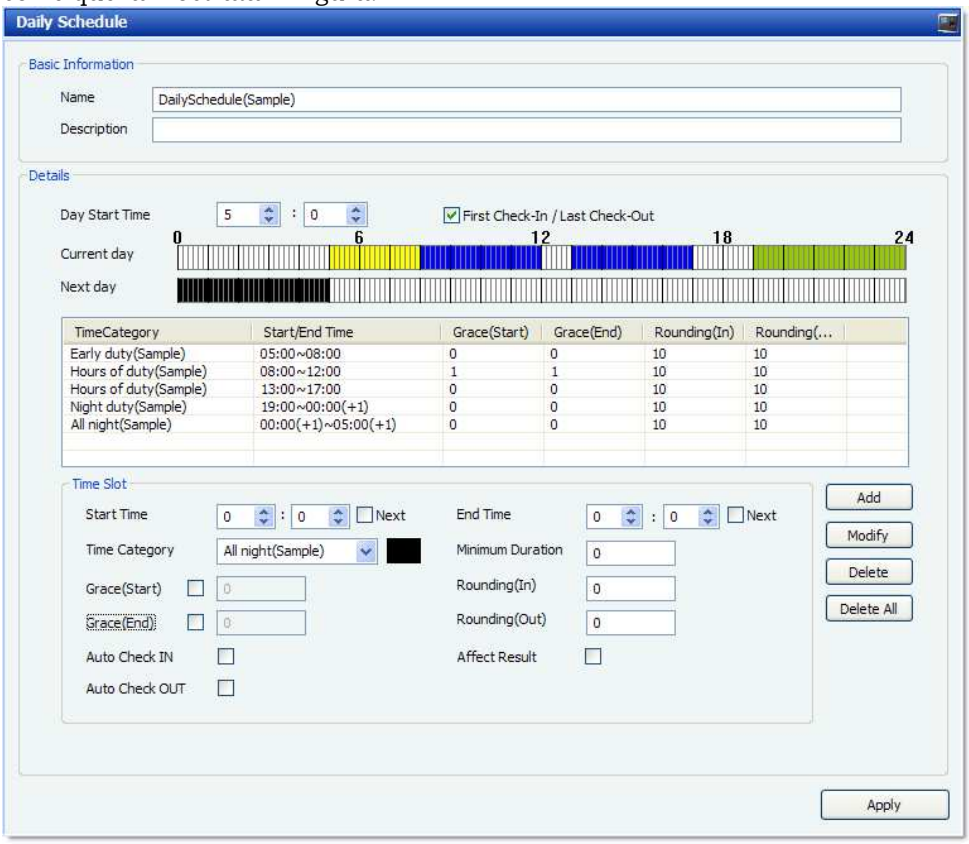
3. Digitare un nome e una descrizione per la categoria.
4. Aggiungere dettagli relativi all'elemento:
   - **Valore Tempo** – inserire il valore a cui fa riferimento questa categoria di tempo.
   - **Arrotondamento Unità (Min)** – specificare in minuti come arrotondare il calcolo per il tempo di lavoro (ad esempio, inserendo "5" verrà arrotondato per difetto all'ultima cifra multipla).
   - **Colore** – impostare come apparirà graficamente la categoria nella schedulazione.
5. Cliccare **Applica** per salvare la categoria di tempo.

3.9.2 Aggiungere una schedulazione giornaliera

Le versioni 1.35 o superiori del software BioStar supportano un massimo di 256 schedulazioni giornaliere.

Aggiungere una schedulazione:

1. Cliccare **Controllo Presenze** nel menu.
2. Nel menu attività, cliccare *Aggiungi Schedulazione Giornaliera*. Si aprirà una finestra come quella mostrata in figura.



3. Digitare un nome e una descrizione per la schedulazione giornaliera.
4. Impostare l'orario di inizio per la schedulazione e, se lo si desidera, selezionare la checkbox sulla destra per registrare tramite BioStar le attività del "primo accesso" e "ultima uscita", come attività di check-in e check-out giornaliere.
5. Definire la schedulazione giornaliera aggiungendo una o più sezioni:
   a. Specificare i dettagli per la sezione:
      - **Orario d'inizio** – impostare l'orario iniziale. Se inizia nel giorno seguente, selezionare la checkbox "Successivo" sulla destra.
      - **Orario di fine** – impostare l'orario del termine. Se finisce nel giorno seguente, selezionare la checkbox "Successivo" sulla destra.
      - **Categoria di Tempo** – selezionare una categoria di tempo dall'elenco.

- **Durata Minima** – impostare la durata minima per le sezioni (in minuti). I dipendenti dovranno effettuare il check-in per la durata minima, altrimenti il sistema registrerà un tempo lavorativo pari a 0.
- **Ritardo (Inizio)** – attivare ed impostare (in minuti) il periodo di ritardo per un check-in fuori dall'orario normale. Selezionare la checkbox per abilitare il periodo di ritardo e specificare la lunghezza di questo periodo nel rispettivo campo. I dipendenti che effettuano l'accesso nel periodo di ritardo consentito verranno considerati come se avessero avuto accesso entro l'orario iniziale prestabilito.
- **Uscita anticipata (Fine)** – attivare ed impostare (in minuti) il periodo di ritardo per un check-out fuori dall'orario normale. Selezionare la check vox per abilitare il periodo di uscita anticipata e specificare la lunghezza di questo periodo nel rispettivo campo. I dipendenti che effettuano l'uscita anticipata entro il periodo consentito verranno considerati come se avessero effettuato l'uscita al termine del normale orario prestabilito.
- **Arrotondamento (Ingresso)** – specificare, in minuti, come arrotondare il tempo di check-in.
- **Arrotondamento (Uscita)** – specificare, in minuti, come arrotondare il tempo di ckeck-out.
- **Check IN Automatico** – abilitare o disabilitare questa funzione per effettuare automaticamente il check-in per un utente che non ha potuto effettuarlo nel tempo prestabilito.
- **Auto Check OUT** – abilitare o disabilitare questa funzione per effettuare automaticamente il check-out per un utente che non ha potuto effettuarlo nella tempo prestabilito.
- **Risultati** – abilitare o disabilitare i dati ottenuti da questa sezione di tempo per determinare i risultati della funzione Controllo Presenze per la schedulazione giornaliera.

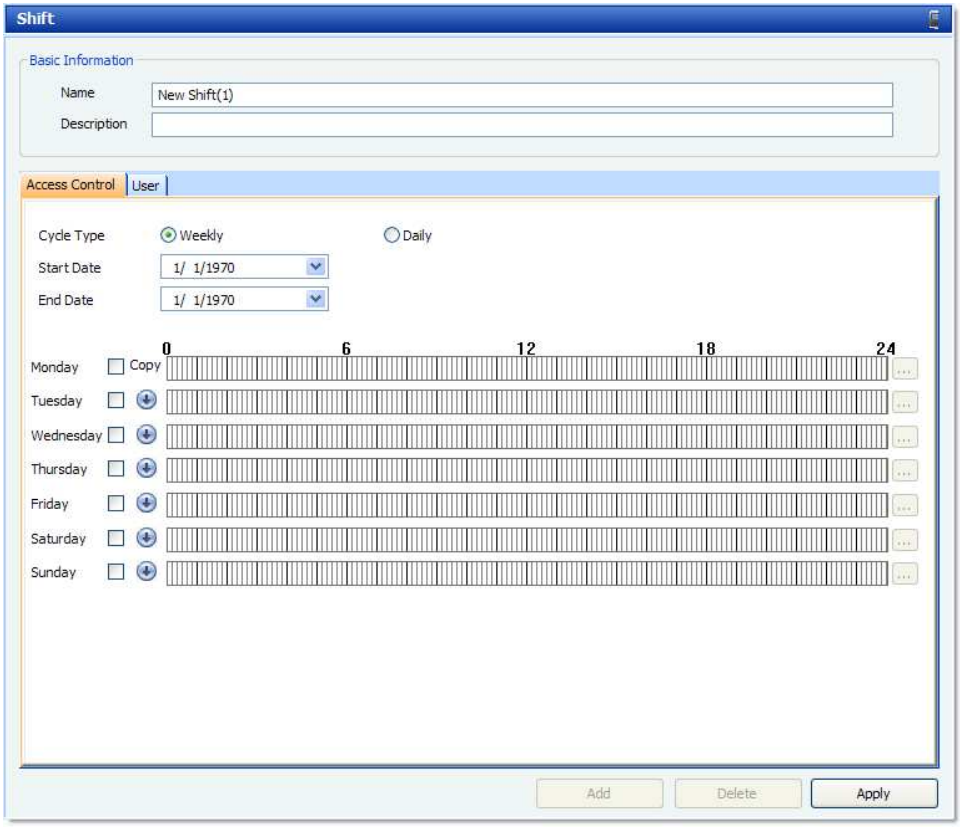
b. Cliccare **Aggiungi** per aggiungere una sezione alla schedulazione giornaliera.

6. Cliccare **Applica** per salvare la schedulazione giornaliera.

3.9.3 Aggiungere un passaggio

Per aggiungere un passaggio:

1. Cliccare **Controllo Presenze** nel menu.
2. Nel menu attività, cliccare *Aggiungi Passaggio*. Si aprirà una finestra come quella indicata in figura.

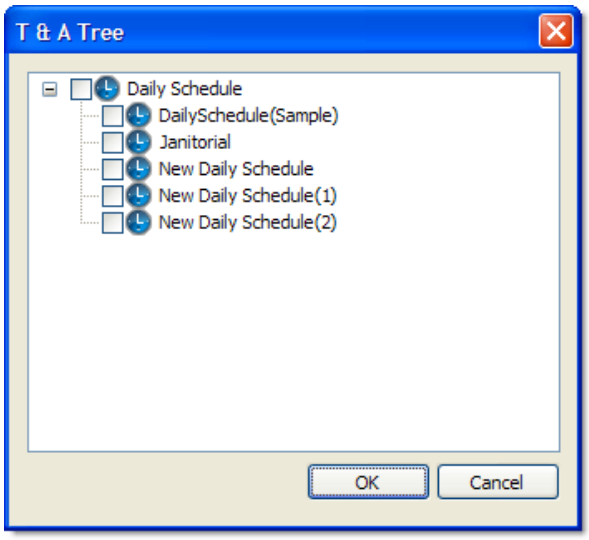


3. Cliccare uno dei tasti radio per impostare il passaggio come parte di un ciclo giornaliero o settimanale. Se si seleziona “settimanale”, il ciclo verrà considerato una settimana. Se si seleziona “giornaliero”, sarà possibile specificare un qualsiasi numero di giorni consecutivi (ad esempio 5, 10, 20, ecc.) come ciclo.

   Note: I cicli giornalieri sono disponibili solo con la versione Standard Edition del software BioStar.

4. Selezionare le date di inizio e fine tramite l’elenco.
5. Attivare i giorni del cliclo selezionando la checkbox sulla sinistra.

6. Cliccare il tasto “ (...) ” per selezionare una schedulazione giornaliera. Si aprirà la finestra del Controllo Presenze.



7. Selezionare una schedulazione giornaliera, quindi cliccare **OK** per applicare la schedulazione.
8. Ripetere i passaggi da 5a 7 quante volte è necessario.

   Note: È possibile copiare una schedulazione da un giorno cliccando sulla freccia posta a destra del giorno.
9. Cliccare **Applica** per salvare.

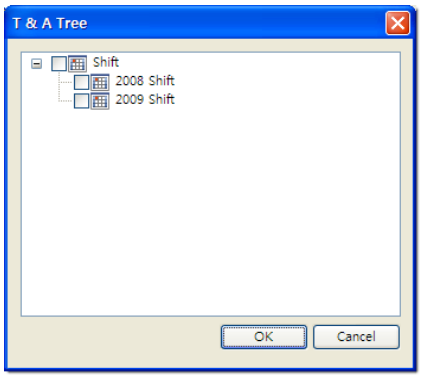
3.9.4 Assegnare gli utenti ai passaggi

È possibile assegnare gli utenti a determinati passaggi per abilitare la registrazione del controllo presenze da parte del software BioStar. Si possono assegnare singoli utenti tramite il menu Utente, oppure più utenti tramite il menu Controllo Presenze.

Assegnare un singolo utente tramite il pannello Utente:

1. Cliccare **Utente** nel menu.
2. Nel menu di navigazione, cliccare sul nome dell’utente.
3. Nel menu dell’utente, cliccare T&A.

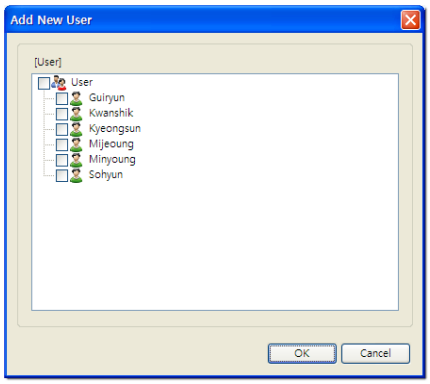
4. Cliccare il tasto radio a fianco di Gestione Passaggio, quindi cliccare **Aggiungi** in fondo al menu Utente. Si aprirà una finestra come quella mostrata in figura.



5. Selezionare un passaggio e premere **OK**.
6. Cliccare **Applica** per salvare le impostazioni di controllo presenze per l'utente.

Assegnare più utenti ad un passaggio tramite il menu Controllo Presenze:

1. Cliccare **Controllo Presenze** nel menu..
2. Nel menu di navigazione, cliccare sul nome di un passaggio.
3. Nel menu del passaggio, cliccare sulla scheda Utente, quindi cliccare **Aggiungi** in fondo alla pagina. Si aprirà una finestra come quella mostrata in figura.

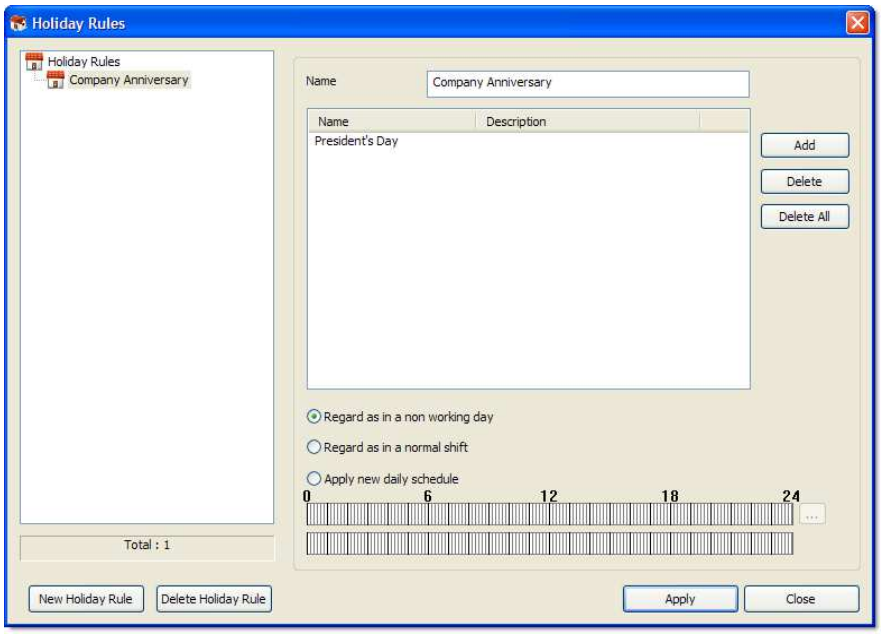


4. Selezionare uno o più utenti e cliccare **OK**.
5. Cliccare **Applica** per salvare le impostazioni di controllo presenze.

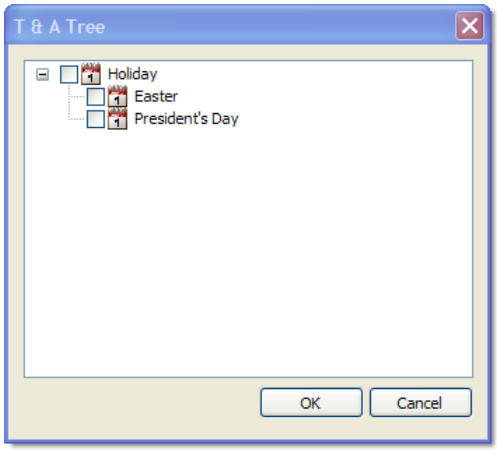
3.9.5 Aggiungere regole per i giorni festivi

Aggiungere una regola per i festivi:

1. Cliccare **Controllo Presenze** nel menu.
2. Nel menu delle attività, cliccare *Gestione Festivi*. Si aprirà una finestra come quella indicata in figura.



3. Cliccare Nuova Regola Festiva.
4. Digitare un nome per la regola.
5. Cliccare **Aggiungi**. Si aprirà una finestra come quella indicata in figura.



6. Selezionare una festività dall'elenco e premere **OK**.

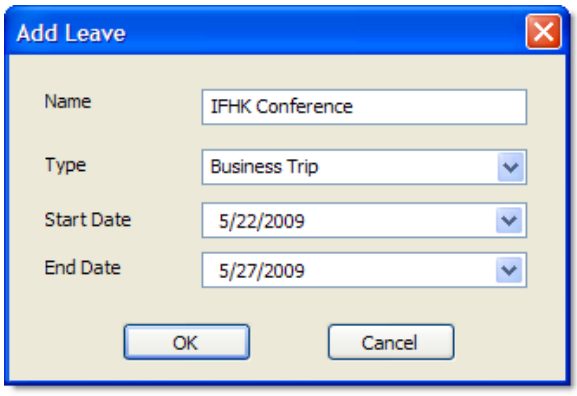
7. Cliccare su uno dei tasti nella parte bassa della finestra Regole dei Festivi per specificare come verrà influenzata la schedulazione di controllo presenze:
   - **Conteggio come giorno non lavorativo** – non viene registrato il tempo di lavoro per questo giorno, inoltre non appare nei report di controllo presenze.
   - **Conteggio come giorno normale** – viene registrato il tempo di lavoro per questo giorno e calcolato come di norma.
   - **Applicare una nuova schedulazione giornaliera** – il tempo trascorso viene registrato e calcolato in base ad una schedulazione predefinita.
8. Se si sceglie di applicare una nuova schedulazione giornaliera, cliccare sul tasto (...) per selezionare una nuova schedulazione.
9. Cliccare **Applica** per salvare le regole dei festivi.

3.9.6 Aggiungere un permesso

Aggiungere un permesso di tempo per definire quando gli utenti escono dall'ufficio ma devono essere conteggiati comunque come "al lavoro", come nell'esempio di ferie pagate o viaggi di lavoro.

Includere un periodo di assenza o un permesso nelle impostazioni di controllo presenze:

1. Cliccare **Utente** nel menu.
2. Nel menu utente, cliccare sulla scheda Controllo Presenze.
3. Cliccare il tasto a fianco di Gestion Permesso, quindi cliccare **Aggiungi**. Si aprirà una finestra come quella indicata in figura.



4. Digitare un nome per il periodo di assenza, se lo si desidera.
5. Selezionare una tipologia di assenza dall'elenco.
6. Selezionare la data di inizio e fine del periodo d'assenza.
7. Cliccare **OK** per aggiungere il periodo di permesso alle impostazioni di controllo presenze dell'utente.
8. Cliccare **Applica** per salvare le impostazioni di controllo presenze dell'utente.

3. Impostare il sistema BioStar

3.10 Impostare gli allarmi

BioStar fornisce diversi livelli di notifiche d'allarme. Il sistema può attivare un allarme emettendo un suono tramite i dispositivi e i computer connessi. È inoltre possibile configurare il sistema per inviare mail di notifica a specifici contatti.
Infine, è possibile ricevere segnalazioni dai dispositivi esterni (ad esempio in caso di allarme antincendio) o attivarne uno (ad esempio una sirena d'allarme).

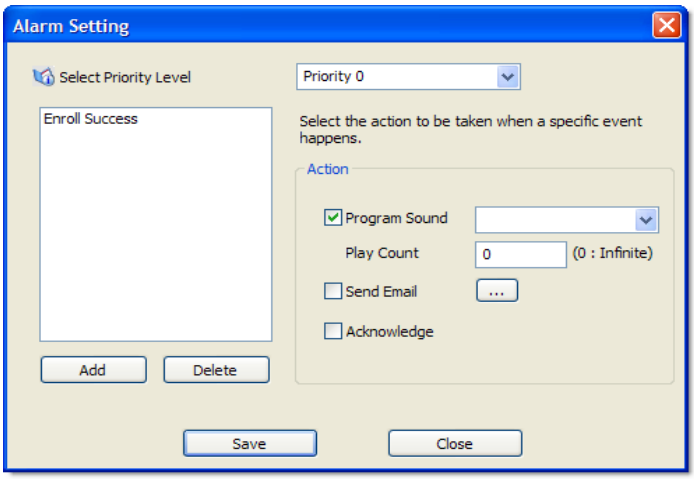
3.10.1 Configurare le impostazioni d'allarme e sonore

BioStar permette di personalizzare la risposta del sistema agli eventi. È possibile configurare gli allarmi creando livelli di priorità personalizzati e selezionare le azioni da eseguire all'attivazione di tali eventi. È inoltre possibile personalizzare ulteriormente il sistema inserendo il suono d'allarme che si desidera.

3.10.1.1 Personalizzare le azioni d'allarme

Personalizzare le azioni d'allarme:

1. Dal menu, cliccare **Opzioni > Eventi > Impostazioni Allarme**.
   Si aprirà una finestra come quella indicata in figura.



2. Selezionare il livello di priorità dall'elenco e cliccare **Aggiungi**. Si aprirù una lista di eventi.
3. Selezionare gli eventi da includere nel livello di priorità e cliccare **OK**.

4. Selezionare una o più azioni selezionando le checkbox a destra.
   - Se si seleziona *Programma Suono*, scegliere un suono dall'elenco e specificare la durata ("conteggio") del suono, in secondi. Se si imposta il conteggio su 0, il suono rimarrà attivo finché un amministratore interromperà la riproduzione sonora tramite il monitoraggio in tempo reale nel menu Monitoraggio.
   - Se si seleziona *Invia Email*, cliccare il tasto (...) a destra per selezionare i contatti che riceveranno le email.
   - Selezionare il Riconoscimento attiverà un pop-up di segnalazione sul PC del cliente.
5. Ripetere i passaggi da 2 a 4, se necessario, per personalizzare altri livelli di priorità.
6. Quando la configurazione è terminata, cliccare **Salva**.

3.10.1.2 Aggiungere un suono d'allarme personalizzato

Aggiungere un suono d'allarme personalizzato:

1. Dal menu, cliccare **Opzione > Evento > Impostazioni Suono**. Si Aprirà una finestra di gestione del suono.
2. Cliccare **Aggiungi**.
3. Trovare il percorso del file "waveform" (.wav) sul computer o in rete, quindi cliccare **Apri**.
4. Se lo si desidera, cliccare sul file e quindi su **Riproduci (Play)** per ascoltare il suono
5. Quando la configurazione è terminata, cliccare **Salva**.

3.10.2 Configurare le notifiche tramite email

BioStar può inviare notifiche tramite email quando si attiva un evento d'allarme (non disponibile nella versione gratuita). Come già precedentemente indicato nel manuale, è possibile personalizzare gli eventi che si attiveranno automaticamente in caso d'allarme.

Configurare le notifiche tramite email:

1. Dal menu, cliccare su **Opzioni > Eventi > Impostazioni E-mail**. Si aprirà una finestra come quella indicata in figura.

2. Inserire l'indirizzo email, l'SMTP del server, il numero della porta, l'ID e la password nella sezione *Informazioni Mittente*.
3. Inserire l'indirizzo email nella sezione *Informazioni Destinatario*.
4. Cliccare **Aggiungi** per aggiungere la configurazione alla lista.
5. Ripetere se necessario i passaggi da 2 a 4 per aggiungere altre configurazioni email.
6. Quando la configurazione è terminata, cliccare **Salva**.

3.10.3 Configurare le impostazioni per i dispositivi esterni

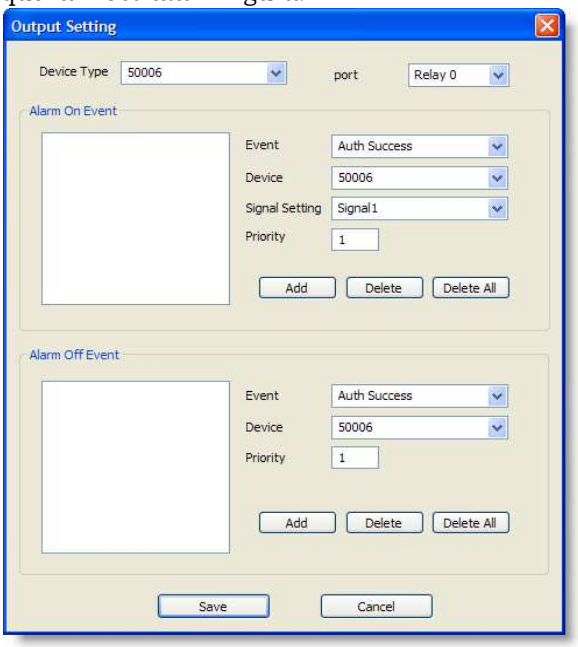
Quando si utilizzano dispositvi esterni con BioStar, è necessario configurare le informazioni per determinare quali azioni saranno effettuate in risposta al segnale in ingresso.

3.10.3.1 Configurare le uscite dedicate ai dispositivi esterni

È possibile impostare che determinati dispositivi inviino segnali ai dispositivi esterni, come una sirena d'allarme, quando si attiva un determinato evento. Configurare le uscite:

1. Cliccare su **Dispositivo** nel menu.
2. Nel menu di navigazione, cliccare sul nome di un dispositivo.
3. Nel menu del dispositivo, cliccare sulla scheda Uscite.

4. Cliccare **Aggiungi** nella parte inferiore del menu. Si aprirà una finestra come quella mostrata in figura.



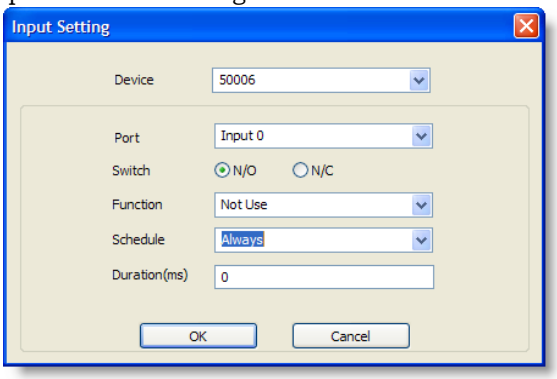
5. Configurare le azioni che attiveranno (quelle che, quindi, invieranno un segnale) ad uno specifico relè d'uscita:
   a. Nella sezione *Allarme su Evento*, selezionare un evento dall'elenco.
   b. Selezionare il numero di un dispositivo, oppure *Tutti i Dispositivi* dal secondo elenco.
   c. Selezionare le impostazioni del segnale dal terzo elenco.
   d. Inserire una priorità per l'evento. Solo un evento con priorità uguale o maggiore (1 è il massimo) può sovrascrivere un evento precedente. Ad esempio, un evento d'allarme (attivazione) con un livello di priorità 2 può essere cancellato solo da un evento di allarme (disattivazione) con un livello di proprità 1 o 2.
   e. Cliccare **Aggiungi**.
6. Configurare le azioni che arresteranno l'invio di segnali all'uscita:
   a. Nella sezione *Allarme termine evento*, selezionare un evento dal primo elenco.
   b. Selezionare il numero del dispositivo o *Tutti i Dispositivi* dal secondo elenco.
   c. Inserire una priorità per questo evento.
   d. Cliccare **Aggiungi**.
7. Quando la configurazione è terminata, cliccare **Salva**.

3.10.3.2 Configurare gli ingressi dai dispositivi esterni

Per integrare il controllo porte BioStar con altri sistemi d'allarme, come un sistema antincendio, è possibile specificare le azioni che il sistema adotterà alla ricezione di un ingresso. È inoltre possibile configurare gli ingressi per lavorare con il rilascio manuale della porta (pulsanti d'uscita) e altre tipologie di dispositivi esterni.

Configurare gli ingressi:

1. Cliccare **Dispositivo** nel menu.
2. Nel menu di navigazione, cliccare sul nome del dispositivo.
3. Nel menu del dispositivo, cliccare sulla scheda Ingressi.
4. Cliccare **Aggiungi** nella parte inferiore del menu. Si aprirà una finestra come quella indicata in figura.



5. Selezionare un ingresso porta dal secondo elenco.
6. Selezionare la posizione normale degli ingressi switch (*N/O-normalmente aperto* o *N/C-normalmente chiuso*).
7. Selezionare una funzione per gli ingressi (*Non in Uso, Ingresso Generico, Apertura d'Emergenza, Annulla tutti gli Allarmi, Riavviare il Dispositivo, Disabilita Dispositivo*).
8. Selezionare una schedulazione per la funzione (*Sempre*, *Disabilita* o una configurazione personalizzata).
9. Impostare la durata minima (in millisecondi) che un segnale di ingresso dovrà attendere prima di attivare una determinata funzione.
10. Cliccare **OK**.

3. Impostare il sistema BioStar

3.11 Impostazione telecamere

Questa sezione descrive come aggiungere telecamere IP e videoregistratori digitali (NVR) al sistema BioStar. Dopo aver impostato l'NVR e le telecamere IP, è possibile monitorare le aree in tempo reale e visualizzare il registro degli eventi, con le immagini e i video registrati. BioStar supporta le seguenti telecamere IP e NVR:

	Nome Modello	Produttore
Telecamera Protocollo Internet (IP)	AXIS PTZ 215	AXIS
	AXIS M3203-V	AXIS
	SNP-3120VH	Samsung Techwin
Registratore (NVR)	AXIS Camera Station	AXIS
	NET-I Ware	Samsung Techwin

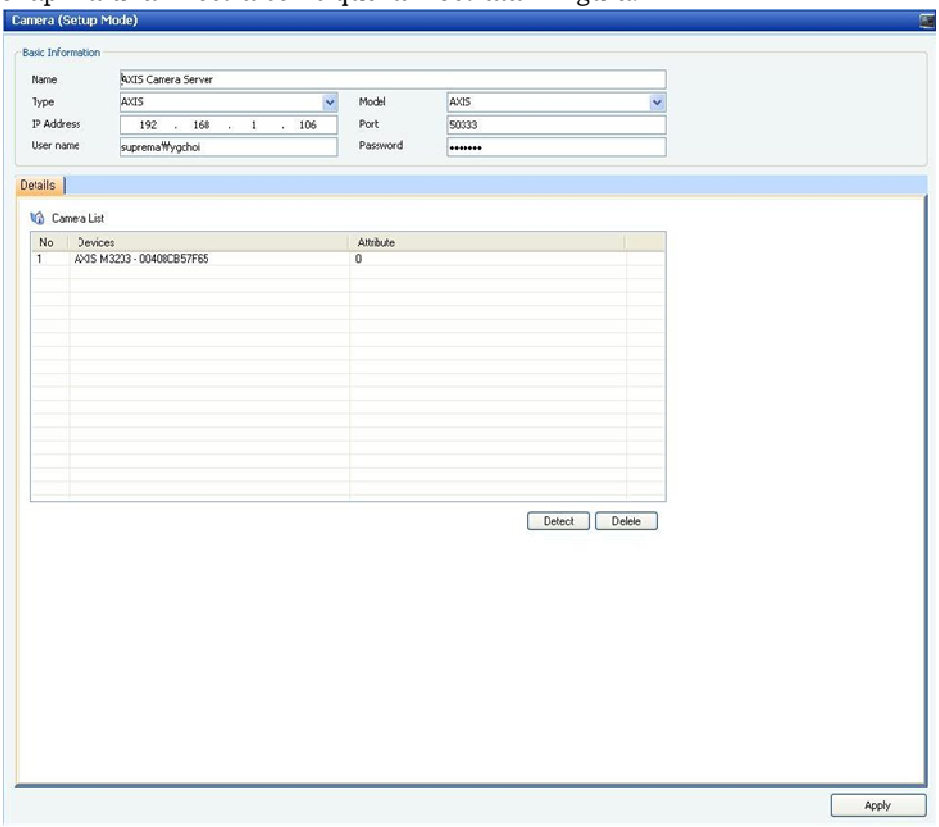
3.11.1 Aggiungere an NVR Server

Il server NVR registrano i video trasferiti da tutte le telecamere connesse, permettendo di visualizzarli consultando il registro.

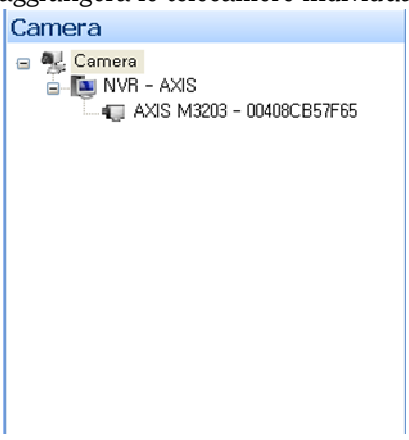
Aggiungere un NVR al sistema BioStar:

1. Cliccare **Telecamera** nel menu.
2. Cliccare **Imposta Telecamera** nel menu.

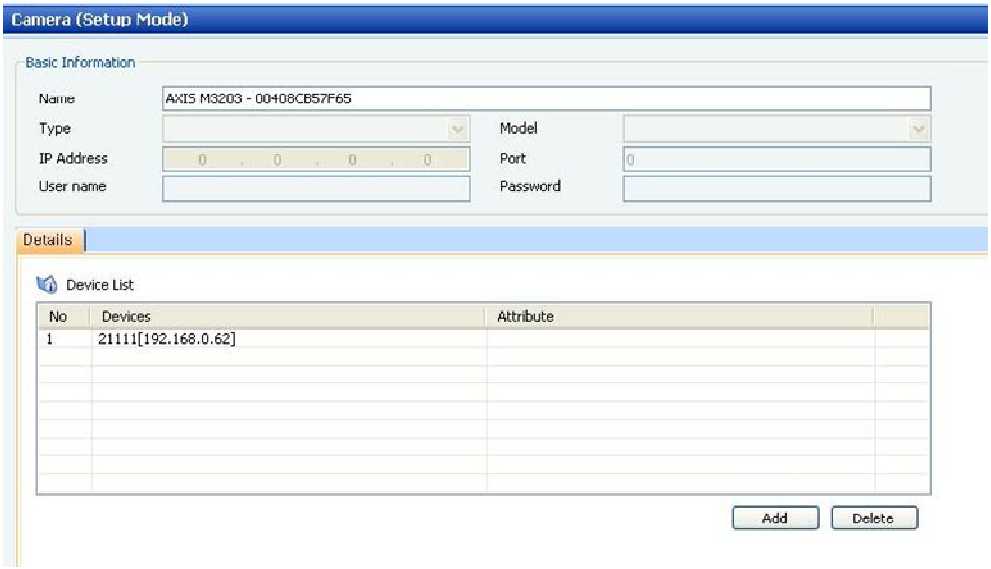
3. Nel menu delle attività, cliccare **Aggiungi Nuovo Server Telecamere**.
   Si aprirà una finestra come quella mostrata in figura.



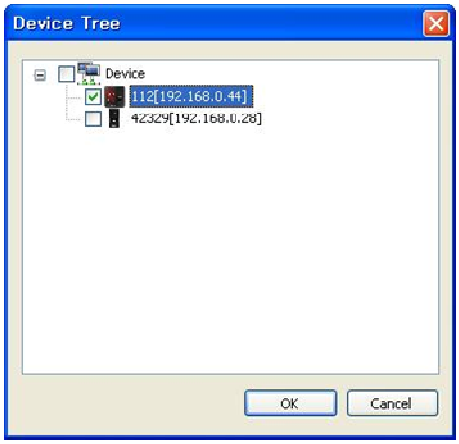
4. Nella sezione Informazioni di Base, inserire nome, tipo, modello, indirizzo IP e porta per il server NVR, quindi accedere a BioStar utilizzando nome e password richieste per accedere al server NVR.
5. Cliccare **Individua** per visualizzare le telecamere che sono attualmente connesse al server NVR.
6. Cliccare **Applica** nella parte inferiore del menu Telecamera. Questo processo aggiungerà le telecamere individuate nel menu di navigazione del server NVR.



7. Nel menu di navigazione, cliccare sul nome di una telecamera. Si aprirà una finestra come quella mostrata in figura.



8. Cliccare **Aggiungi** nella parte inferiore destra dei dispositivi per aprire l'elenco.



9. Selezionare la checkbox a fianco del nome del dispositivo, quindi cliccare **OK**.
10. Cliccare **Applica** nella parte inferiore destra per applicare le modifiche.

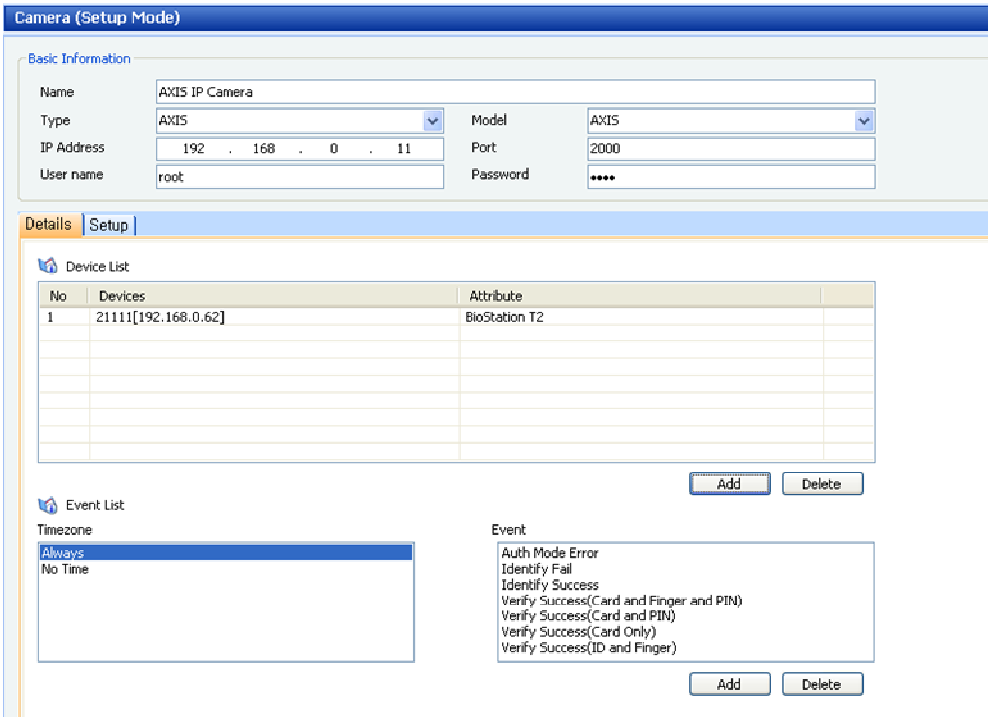
3.11.2 Aggiungere una telecamera IP

BioStar permette di aggiungere una telecamera IP associata ad un dispositivo di controllo accessi, specificando in base a quali venti la telecamera scatterà delle immagini e le invierà al sistema BioStar.

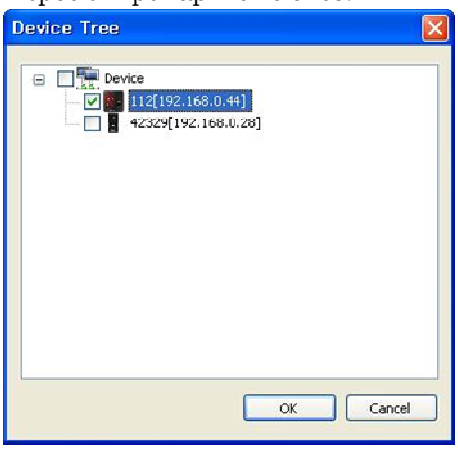
3. Impostare il sistema BioStar

Aggiungere una telecamera IP al sistema BioStar:

1. Cliccare **Telecamera** nel menu.
2. Cliccare **Imposta Telecamera** nel menu attività (opzionale).
3. Nel menu delle attività, cliccare **Aggiungi Nuova Telecamera**. Si aprirà una finestra come quella mostrata in figura.



4. Nella sezione Informazioni di Base, digitare il nome, il modello, l'indirizzo IP e la porta per la telecamera IP, quindi inserire il nome utente e la password BioStar per accedere alla telecamera.
5. Nella scheda Dettagli, cliccare **Aggiungi** nella parte inferiore destra della sezione Dispositivi per aprire l'elenco.



6 Selezionare un dispositivo a cui associare la telecamera IP e cliccare **OK**.

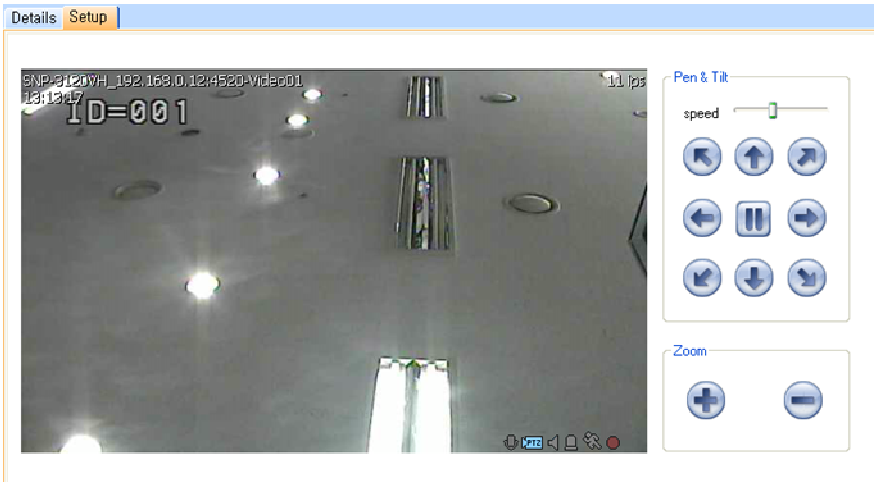
7. Cliccare **Aggiungi** nella parte inferiore della Lista Eventi e selezionare un evento che attiverà la telecamera e invierà l'immagine al sistema BioStar.
8. Cliccare **Applica** nella parte inferiore destra per applicare le modifiche al sistema BioStar.

3.11.3 Configurare una telecamera IP

BioStar può controllare il movimento del movimento (PTZ) delle telecamere. Quando si utilizzare una telecamera IP che supporta la funzione PTZ, è possibile indirizzarla sulla zona da sorvegliare.

Controllare i movimenti di una telecamera PTZ:

1. Cliccare su **Dispositivo** nel menu.
2. Cliccare sulla telecamera PTZ nel menu di navigazione.
3. Nel menu Telecamera, cliccare la scheda Setup.
4. Utilizzare i controlli per inquadrare la posizione che si desidera.

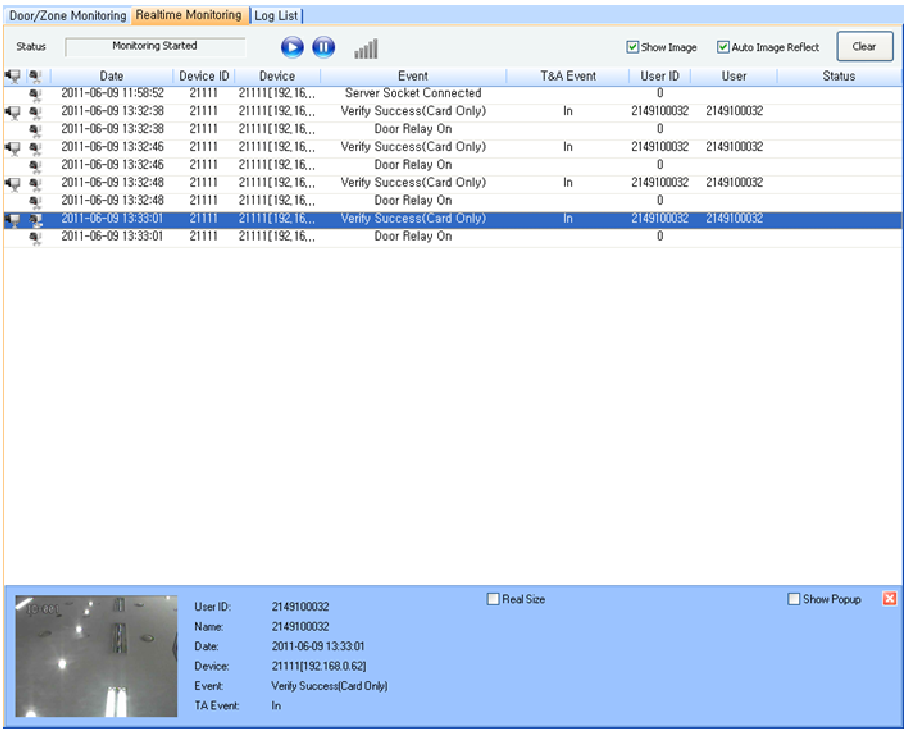


04 Gestione del sistema Bio Star

Dopo aver impostato correttamente il sistema BioStar, la gestione risulta semplice.
BioStar permette di monitorare gli eventi in tempo reale e visualizzare il registro eventi catagorizzato per data, controllare da remoto parti del sistema, gestire gli utenti e aggiornare i firmware direttamente tramite l'interfaccia. Inoltre, è possibile attivare la crittografia tramite impronta se necessario, per garantire un ulteriore livello di sicurezza e privacy.

4.1 Monitoraggio degli eventi in tempo reale

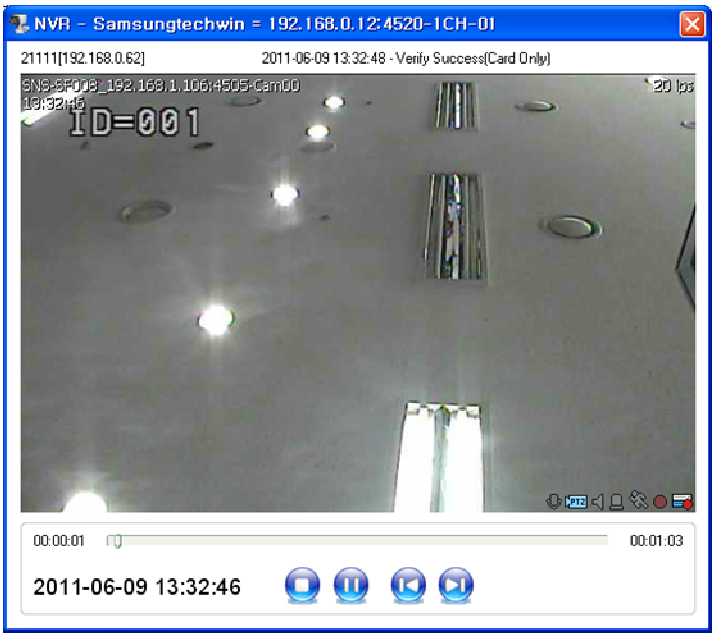
Il sistema BioStar registra eventi da tutti i dispositivi connessi. Per monitorarli in tempo reale, cliccare **Monitoraggio** nel menu, quindi cliccare sulla scheda "Monitoraggio in tempo reale".



- Questa tab shows all events that have occurred since you last logged into the system. The tab shows the current monitoring status (*Monitoring Started* or *Monitoring Paused*) and includes buttons for starting (play) or stopping (pause) real-time monitoring. The sound bar icon on the right shows whether an alarm sound is currently playing (green bars) or not (grey bars). To stop an alarm sound, click the sound bars icon.
- BioStar displays the following camera icons at the front of the event logs:

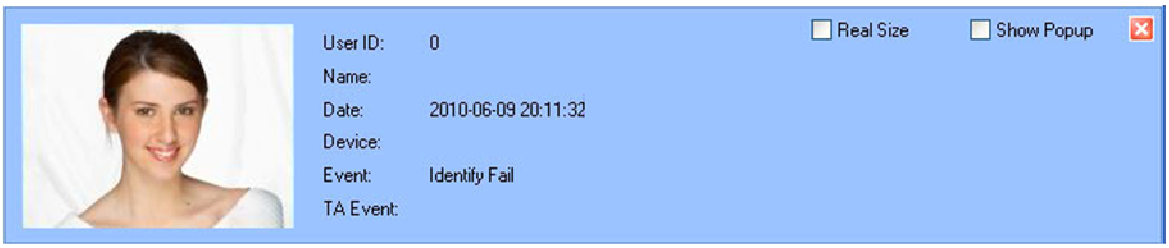
Icon	Description
	The event log includes a still image. Click the event log to view the image.
	The event log includes a video. Double-click the event log to view the video.

When both camera icons are displayed, single-click the icon to view the still image and double-click the icon to view the recorded video. When you double-click the video icon, a video playback window will appear that is similar to the one below.



Coupled with the face detection features of D-Station, X-Station, BioStation T2, or FaceStation, administrators can verify users' identity by clicking **Show Image** (to view the user's stored face image) and **Auto Image Reflect** (to view the most recent face image captured by the local device). Clicking **Show Image** also opens a window at the bottom where the user image will be displayed. Click **Real Size** to view the full-sized (640 x 480) stored image, instead of a thumbnail version and click **Show Popup** to open the image in a new window that can be repositioned on the screen.

4. Gestione del sistema BioStar



To see a users' photos upon successful authentication events, click **Option > Event > Profile Image Setting** in the menu bar, select event types, and then click the checkbox next to Show Image Profile. The user's image will appear on the realtime monitoring tab when he or she successfully completes one of the authentication events specified in the Profile Image Setting window.

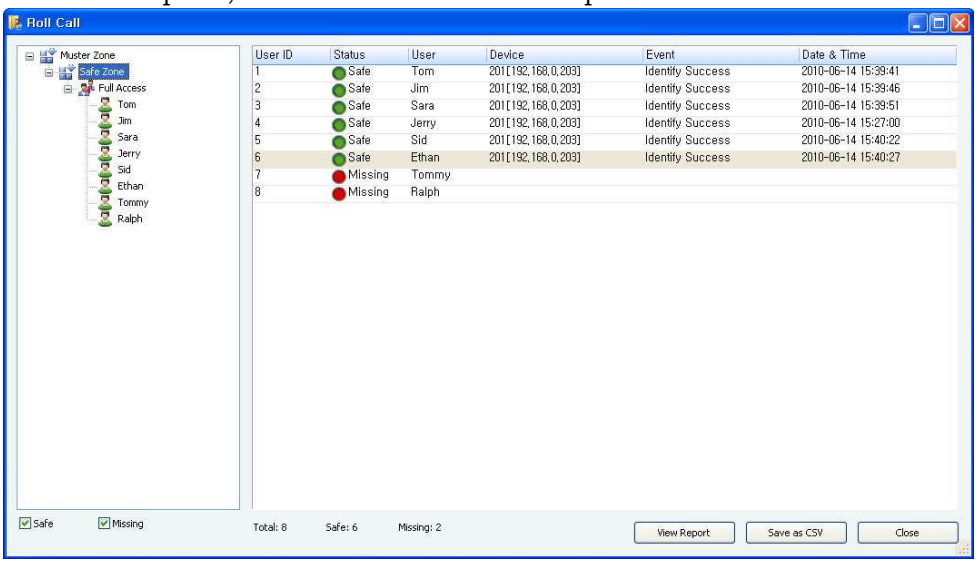
As of BioStar V1.3, administrators can monitor users' locations and authentication status via a Roll Call (muster) feature. This feature allows administrators to determine whether users are present, missing, or have gained entry to areas for which they are not authorized.

4.1.1 Monitor Muster Zones in Real Time

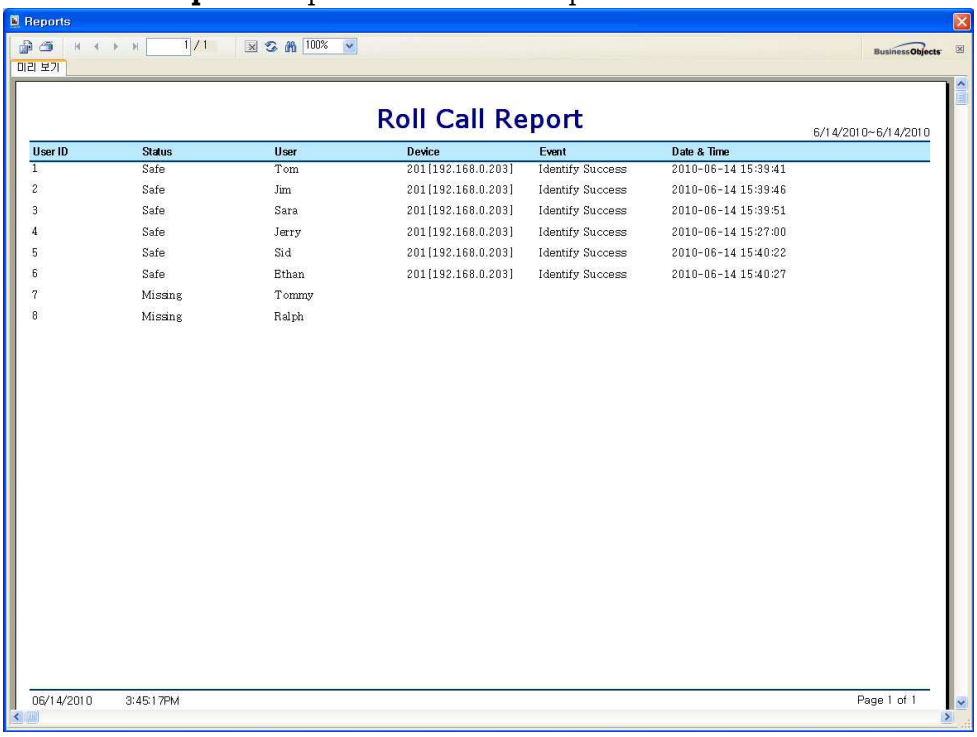
BioStar allows you to monitor and track employees during an emergency and determine whether or not all employees have reported to the muster area.

To monitor and track employees,

1. Click **Monitoring** in the shortcut pane.
2. Click a muster zone in the Monitoring pane.
3. In the Task pane, click **Roll Call**. This will open the Roll Call window.



4. Click **View Report** to open the Roll Call Report.



To save the report data as a comma delimited file, click **Save as CSV**. To print the report, click the printer icon. To export the report, click the export icon.

4.1.2 Monitor Areas with Cameras in Real Time

BioStar allows you to monitor specified areas with the connected camera in real time.

To monitor specified areas in real time,

1. Click **Camera** in the shortcut pane.
2. Click **Monitor Camera** in the Task pane (if desired).
3. Click a camera in the navigation pane.

4.2 View Event Logs

BioStar allows you to view event logs for users, doors, and zones. You can access pre-defined logs from the Event tabs in user, door, and zone panes or view access logs from the Administrator menu. You can also use the Log List tab in the Monitoring pane to specify log parameters.

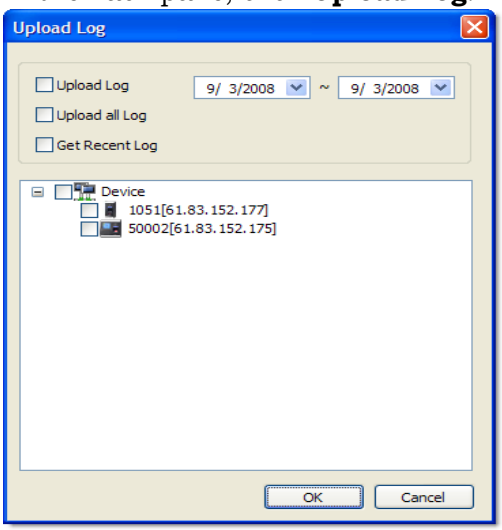
BioStar automatically collects log information from connected devices as long as the server is running. However, if you have devices that are not connected to the BioStar server, you must manually upload logs before viewing them.

4.2.1 Upload Logs to BioStar

For devices that are not connected to the BioStar server, you must manually upload logs before viewing them.

To upload logs to BioStar,

1. Click **Monitoring** in the shortcut pane.
2. Click the Log List tab in the Monitoring pane.
3. In the Task pane, click **Upload Log**. This will open the Upload Log window.



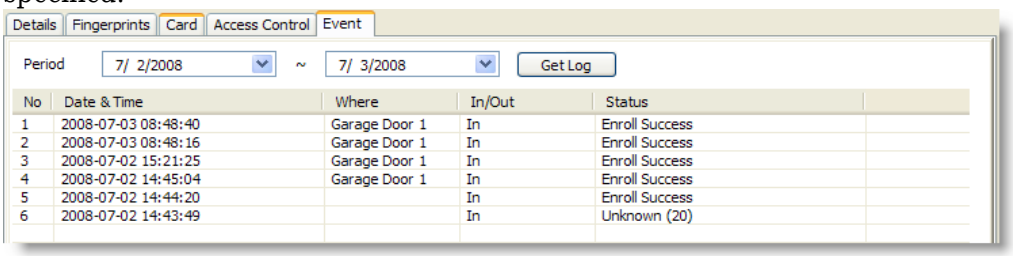
4. Select an upload option by clicking the corresponding box:
   a. **Upload Log** - Use this option to upload logs for a specific time period. Specify the period with the drop-down calendars.
   b. **Upload All Log** - Use this option to upload all logs.
   c. **Get Recent Log** - Use this option to upload logs written since the previous upload.
5. Select the devices from which to upload logs by clicking the checkboxes next to the device numbers.
6. Click **OK**. BioStar will download log records from the selected devices and display the activities in the log list.

4.2.2 View Logs in User, Door, and Zone Panes

To view pre-defined logs,

1. Click **User** or **Doors** in the shortcut pane.
2. In the navigation pane, click a user, door, or zone name.
3. In the User, Doors, or Zone panes, click the Event tab.
4. Set an event period (beginning and ending dates) with the drop-down calendars.

5. Click **Get Log**. This will generate a list of the relevant events for the period you specified.

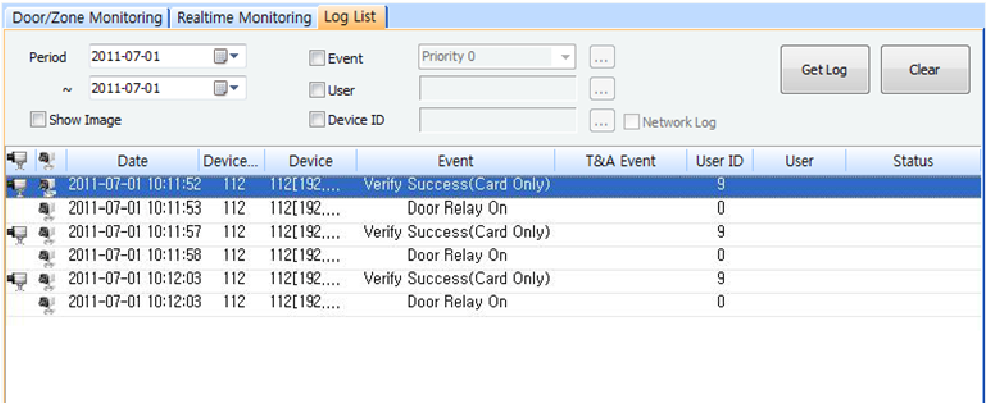


4.2.3 View Logs from the Monitoring Pane

To specify log filters or view logs for groups of users, doors, or zones,

1. Click **Monitoring** in the shortcut pane.
2. In the Monitoring pane, click the Log List tab.
3. Set an event period (beginning and ending dates) with the drop-down calendars.
4. Set the parameters to generate a log:
   - To show events by alarm priority, click the Event checkbox and select an event priority from the drop-down list. To add a new alarm priority, click the ellipsis button (...) to open the Alarm Priority window.
   - To show events by user, click the User checkbox and then click the ellipsis button (...) to select a user or users from the User/Department Tree window. You can select all users by selecting the top level of the user tree.
   - To show events for a particular device, click the Device ID checkbox and then click the ellipsis button (...) to select a device from the Device Tree window. To show only network events for a device, you can also click the Only Network History checkbox.
   - To show all events, leave all the checkboxes unchecked.
   - To show the user's image at the bottom of the tab, click **Show Image**. For more information about viewing user images, see section 4.1.

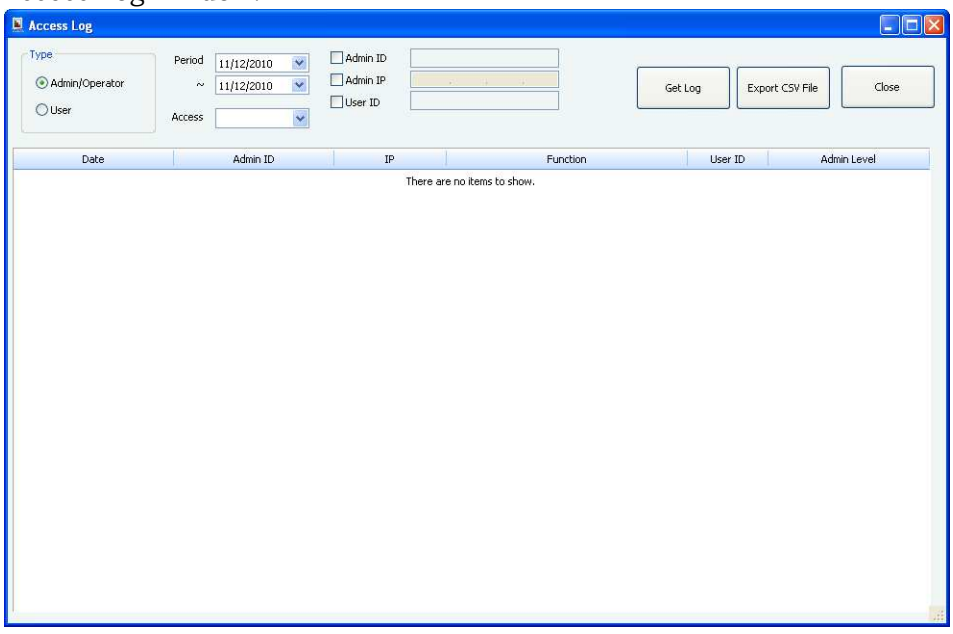
5. Click **Get Log** to display the events.



4.2.4 View Access Logs

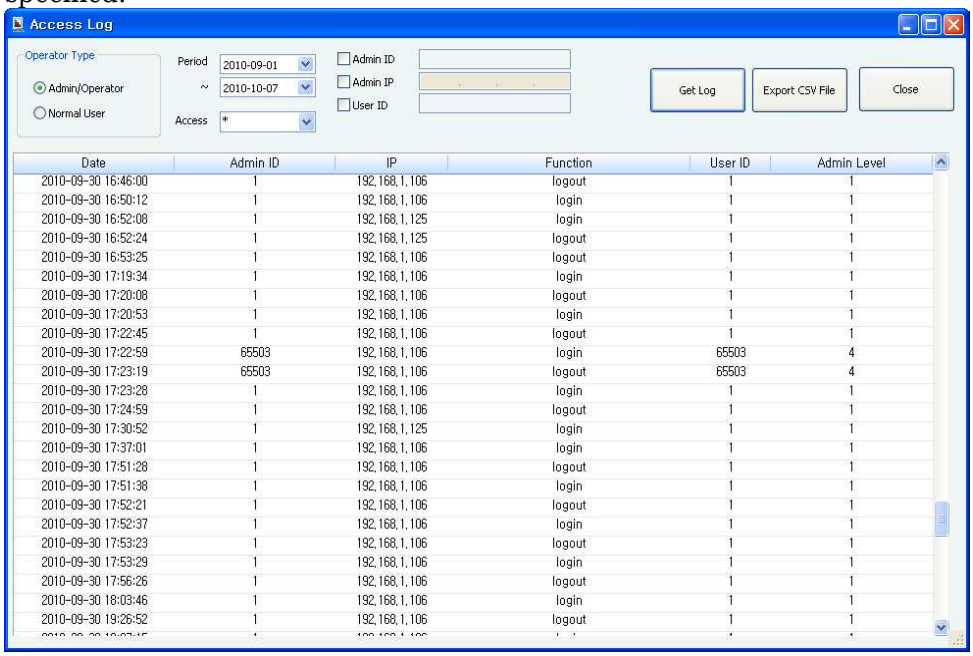
From the Administrator menu, you can view histories of system access and record modification by type of user. To view access logs,

1. From the menu bar, click **Administrator > Access Log**. This will open the Access Log window.



2. Click a radio button to select either administrators or users.
3. Set an event period (beginning and ending dates) with the drop-down calendars.
4. Select a type of access or modification event with the Access drop-down list.
5. If desired, specify a particular admin or user by clicking the checkbox next to the Admin ID, Admin IP, or User ID fields, and then entering the appropriate identification.

6. Click **Get Log**. This will generate a list of the relevant events for the period you specified.



4.3 Monitor Door Events via a Visual Map

BioStar allows you to conveniently manage doors on a visual representation of your actual floor plan. On the Visual Map, you can customize your floor plan, add doors, and monitor door status and activity (for example, whether the door is open or closed, authentication events, and door alarms). If you have more than one floor plan, you can create additional Visual Maps for each floor. The Visual Map feature is available only in the Standard Edition.

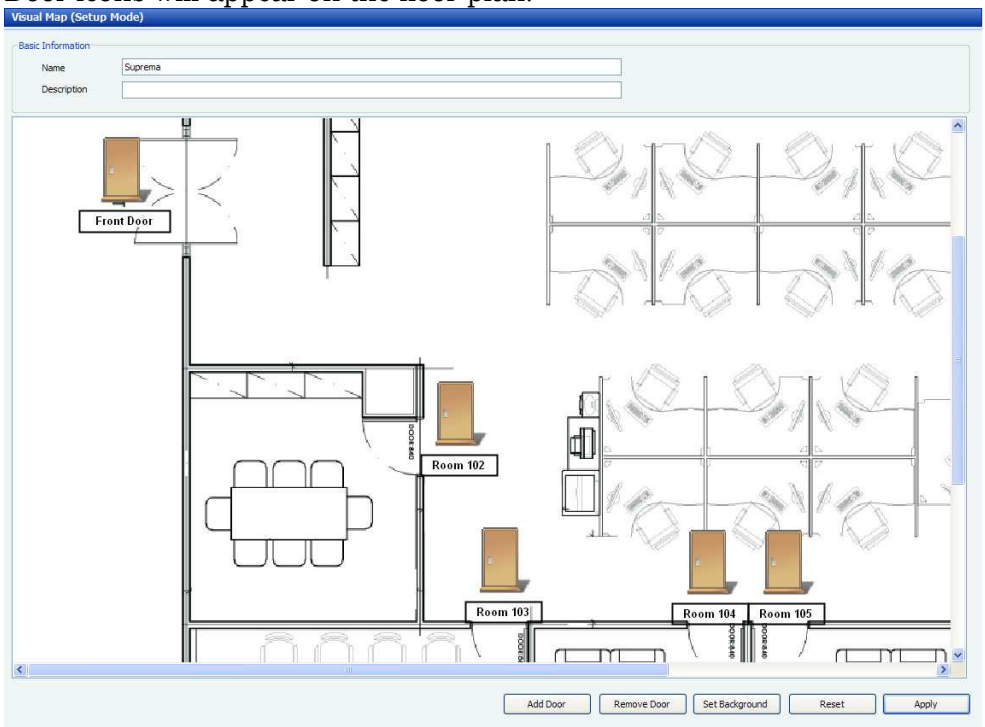
4.3.1 Create a Visual Map

In the setup mode, you can add the floor plan of your building and place doors. To add the floor plan and place doors on the plan,

1. In the shortcut pane, click **Visual Map**.
2. In the task pane, click **Setup Mode**.
   "Monitor Mode" will appear in the title bar of the Visual Map window.
3. In the task pane, click **Add Visual Map**. This will open a new Visual Map window on the right.
4. In the Visual Map window, type a name for the new Visual Map.
5. At the bottom of the Visual Map window, click **Set Background** to add a floor plan.

The BioStar supports images larger than resolution 730x470 in jpg, bmp, gif, or png format only.

6. Choose an image and click **Open**.
7. Click **Add Door** to add doors. This will open a window with a list of doors.
8. From the door list, click the checkboxes next to doors to add and click **Apply**. Door icons will appear on the floor plan.



9. Click and drag the door icon to the desired location on the floor plan. You can individually relocate a door icon or name by double-clicking the door icon or name.
10. To remove a door from the floor plan, click the door and then click **Remove Door**.
11. Repeat steps 7-10 as necessary to add additional doors.
12. When you are finished adding doors, click **Apply**.

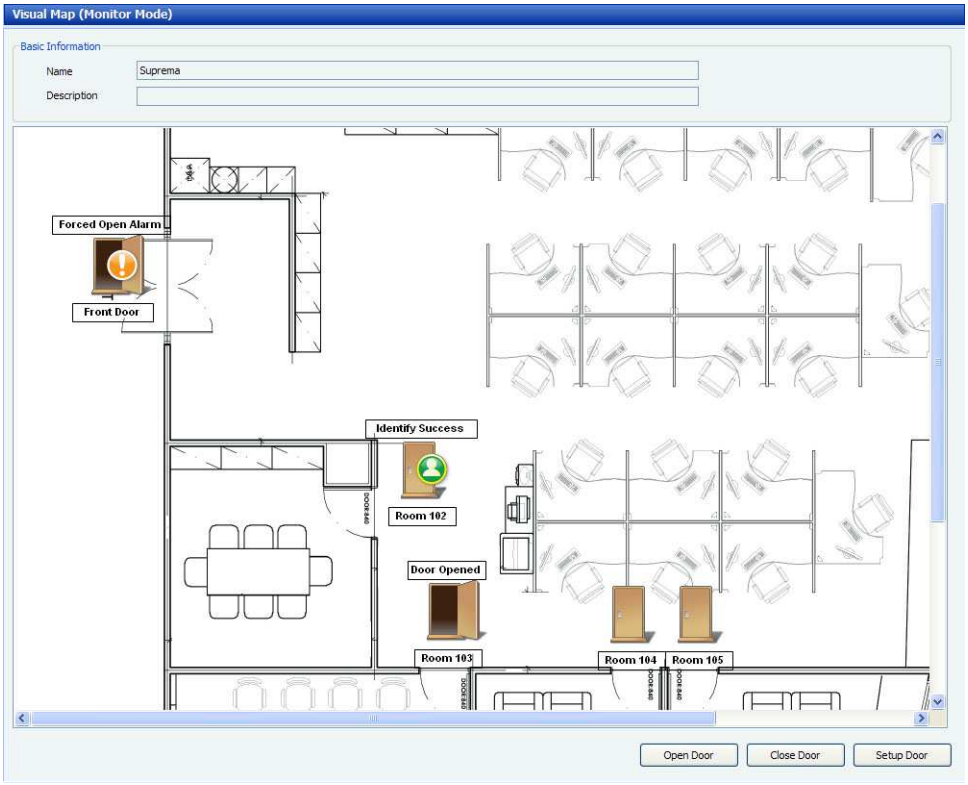
Note: To remove all doors from the plan and start over, click **Reset**.

4.3.2 Monitor Doors on a Visual Map

In the monitor mode, you can view the status and activities for each door on the visually enhanced map.

To monitor doors,

1. In the task pane, click **Monitor Visual Map**. “Monitor Mode” will appear in the title bar of the Visual Map window.



2. Monitor door status and activities on the visual map, as represented by the following icons. Door activities, such as successful authentication or alarms will appear on the door icons:

Icon	Activity
	Door is closed / Door alarm is clear
	Door is open
	Successful authentication while door is closed
	Successful authentication while door is open
	Failed authentication while door is closed
	Failed authentication while door is open
	Held or forced open door / Held or forced open door alarm

Note: Door icons will change only when door sensors have been assigned in the door settigns and detect the door status. In other words, door icons change only when the

door actually opens or closes and not when you click **Open Door** or **Close door.** For more information about door settings, see section 5.2.1.

3. To open or close a door, click a door and then click **Open Door** or **Close Door**.
4. To change settings for a door, click a door and then click **Setup Door**.

4.4 Control Doors, Alarms, and Devices Remotely

BioStar allows administrators or operators to control doors, alarms, and devices remotely. You can open or close doors via a computer connected to the BioStar system. You can also release (cancel) alarms remotely and lock or unlock devices.

4.4.1 Open or Close Doors

In some situations, an administrator or operator may need to open or close a door remotely. To open or close doors,

1. Click **Monitoring** in the shortcut pane.
2. The Door/Zone Monitoring tab lists door names and their statuses. To change the status (open or closed) of a door, click the door name and then click either **Open Door** or **Close Door**.

You can also open and close doors while monitoring a Visual Map. For more information, see section 4.3.2.

4.4.2 Release Alarms

When an event triggers an alarm, administrators or operators can release the alarm remotely. To release alarms,

1. Click **Monitoring** in the shortcut pane.
2. The Door/Zone Monitoring tab lists doors names and alarm events. To release (cancel) an alarm, click the door name and then click **Release Alarm**.

4.4.3 Lock or Unlock Devices

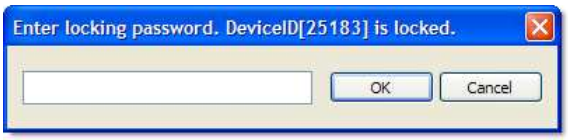
BioStar allows you to lock and unlock devices to prevent unauthorized access when BioStar is not running. This action blocks communication from devices. You can either lock devices manually from the BioStar interface or automatically when you exit the BioStar software. All connected devices can be simultaneously locked or unlocked, but you cannot lock or unlock devices that are connected directly to the BioStar server.

4.4.3.1 Lock or unlock connected devices

To lock all connected devices, from the menu bar, click **Option > Device > Lock All Devices**.

To unlock all connected devices,

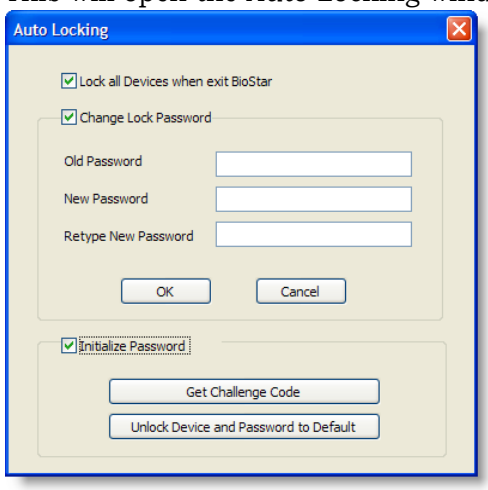
1. From the menu bar, click **Option > Device > Unlock All Devices**.
2. If necessary, enter a password in the Enter Locking Password window and click **OK** (if you have not created a locking password, simply click **OK**). See section 4.4.3.2 to create a locking password.



4.4.3.2 Set automatic device locking

To set automatic device locking,

1. From the menu bar, click **Option > Device > Automatic Locking**. This will open the Auto Locking window.

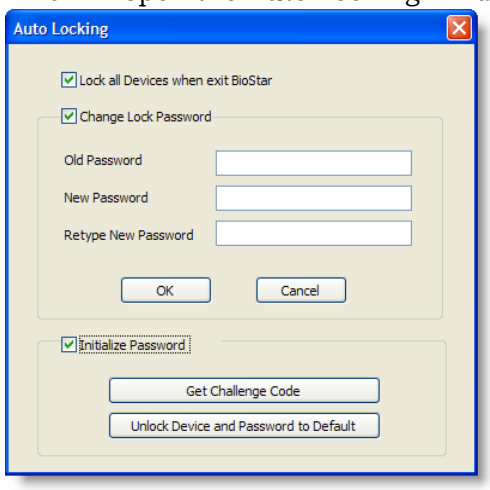


2. Click the first checkbox to lock all devices when exiting BioStar.
3. If desired, click the second checkbox to change the lock password:
   a. Enter the old password
   b. Enter the new password
   c. Retype the new password to confirm.

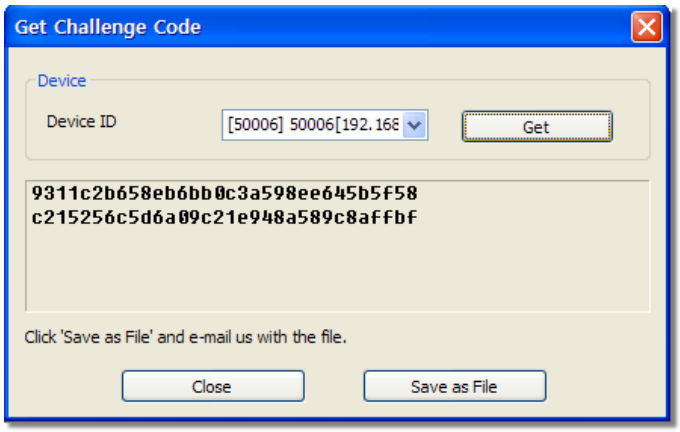
4.4.3.3 Reset a device lock

If you have forgotten the locking password for a device, Suprema's technical support team can send you an unlock code. To request the code,

1. From the menu bar, click **Option > Device > Automatic Locking**. This will open the Auto Locking window.

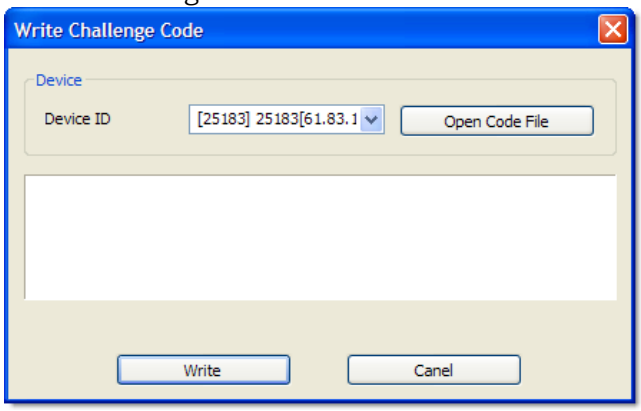


2. Click the Initialize Password checkbox to activate the buttons at the bottom of the window.
3. Click **Get Challenge Code**. This will open the Get Challenge Code window.



4. Select the appropriate device from the drop-down list and click **Get**.
5. Click **Save as File** to save the challenge code to your computer.
6. Email the challenge code to Suprema (*support@supremainc.com*). Suprema's technical support personnel will return an unlocking code to you via email.
7. When you receive the code from Suprema, open the Auto Locking window and activate the buttons (see steps 1-2).

8. Click **Unlock Device and Password to Default**. This will open the Write Challenge Code window.



9. Click **Open Code File** and locate the file sent to you by Suprema.
10. When you have opened the file, click **Write**. This will unlock the device and reset the locking password to the default (no password).

4.5 Manage Users

With the BioStar system, you can delete users, transfer users to other departments, and customize user information fields. You can also export or import user data for creating custom reports, batch editing, or other needs.

4.5.1 Delete Users

If the occasion arises, you can easily remove users from the BioStar system. To delete a user,

1. Click **User** in the shortcut pane.
2. Right-click a user's name.
3. Click *Delete User*.
4. Click **OK** to confirm the deletion.

4.5.1.1 Delete an individual user via command cards

After issuing command cards, you can delete an individual user directly from a BioEntry Plus, BioEntry W, Xpass, or Xpass Slim device. For more information about issuing command cards, see section 3.2.5.1 and 3.2.7.1.

To delete users directly from a BioEntry Plus or BioEntry W device via command cards,

1. Place a delete card (command card) on a BioEntry Plus or BioEntry W device.

2. If authorization is required, an administrator must scan his or her fingerprints to continue.
3. Place the user's access card on the device and then have the user place his or her finger on the scanner (as prompted by the device).

To delete users directly from an Xpass or Xpass Slim device via command cards,

1. Place a delete card (command card) on an Xpass or Xpass Slim device.
2. If authorization is required, an administrator must place his or her access card on the device to continue.
3. Place the user's access card on the device.
4. Place the delete card on the device again to confirm the action.

4.5.1.2 Delete all users via command cards

After issuing command cards, you can delete all users directly from a BioEntry Plus, BioEntry W, Xpass, or Xpass Slim device. For more information about issuing command cards, see section 3.2.5.1 and 3.2.7.1.

To delete all users directly from a BioEntry Plus or BioEntry W device via command cards,

1. Place a delete all card (command card) on a BioEntry Plus or BioEntry W device.
2. If authorization is required, an administrator must scan his or her fingerprints to continue.
3. Place the delete all card on the device again to confirm the action.

To delete all users directly from an Xpass or Xpass Slim device via command cards,

1. Place a delete all card (command card) on an Xpass or Xpass Slim device.
2. If authorization is required, an administrator must place his or her access card on the device to continue.
3. Place the delete all card on the device again to confirm the action.

4.5.2 Transfer Users to Other Departments

BioStar makes moving users to other departments very simple. Before transferring a user, you must create a department:

1. Click **User** in the shortcut pane.
2. In the navigation pane, right-click *User*.
3. Click *Add Department*.

4. Enter a name for the department.

To transfer users to a department, simply click and drag a user name onto a department name.

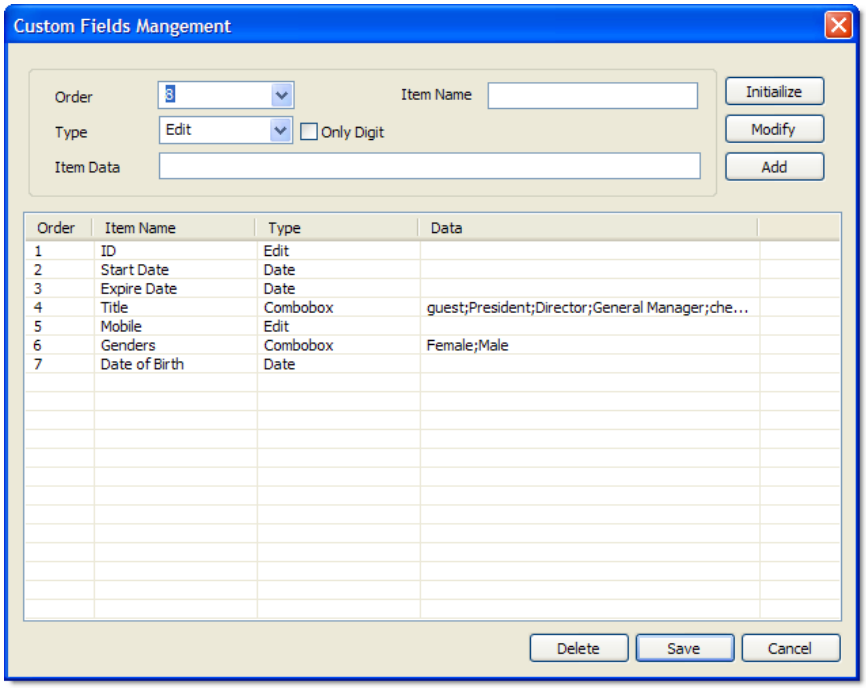
4.5.3 Customize User Information Fields

BioStar allows you to customize user information fields. This can be useful for altering the default information fields or for creating new fields.

4.5.3.1 Add new information fields

To add new information fields,

1. From the menu bar, click **Option > User > Custom Field Setting**. This will open the Custom Fields Management window.



2. Select an order number from the first drop-down list (choose a number that is not already in use).
3. Select a field type from the second drop-down list. To restrict the field to numerical values, click the Only Digit checkbox.
4. Enter item data (for example, items to appear in a combo box) and a name for the item.
5. Click **Add**.
6. Repeat steps 2-5 as desired to create additional information fields.
7. When you are finished, click **Save**.

4.5.3.2 Modify existing information fields

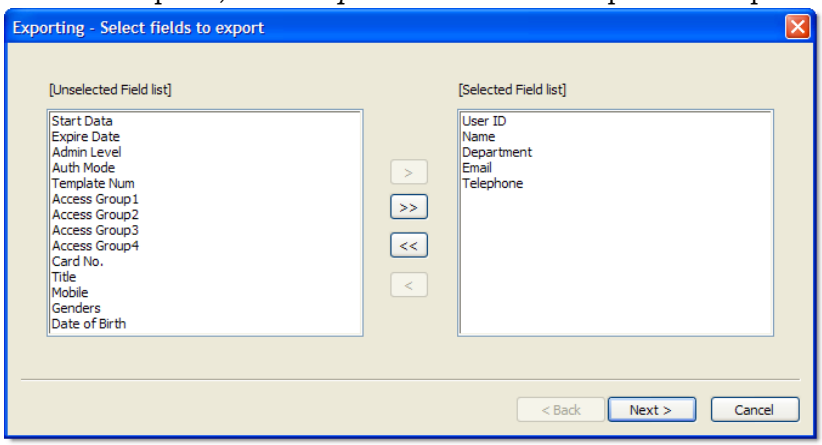
To modify existing information fields,

1. From the menu bar, click **Option > User > Custom Field Setting**. This will open the Custom Fields Management window (see section 4.5.3.1).
2. Click the item you want to modify in the list at the bottom. The data will appear in the fields at the top of the window.
   Note: Items 1-4 are required fields and cannot be modified or deleted.
3. Modify the data as desired.
4. Click **Modify**.
5. Repeat steps 2-4 as desired to modify additional information fields.
6. When you are finished, click **Save**.

4.5.4 Export User Data

Exported user data is formatted as a comma-delimited file (CSV), which can be edited with a text editor or Microsoft Excel. To export user data,

1. Click **User** in the shortcut pane.
2. In the task pane, click *Export User*. This will open the Exporting window.

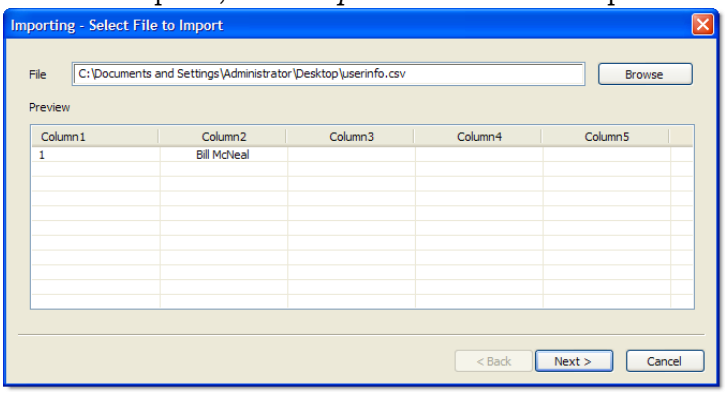


3. Select types of user data to export by clicking items in the list on the left and then clicking **>**.
4. After selecting all the types of user data to export, click **Next**.
5. Type a path and filename for the user data or click **Browse** to select a location to save the file.
6. Click **Next**.
7. Click **Export** to begin exporting the user data.
8. When the export is complete, click **Finish**.

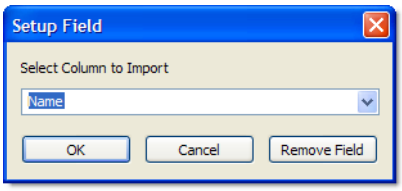
4.5.5 Import User Data

User data in comma-delimited format (CSV) can be imported to BioStar. To import user data,

1. Click **User** in the shortcut pane.
2. In the task pane, click *Import User*. This will open the Importing window.



3. Type a path and filename where the user data is located or click **Browse** to select a file.
4. Click **Next**. The raw data types will be displayed and the User list field will default to “Not use. Click here to change.”
5. Click the cell to the right of a data sample. This will open the Setup Field window, which allows you to map the raw data to a user information field in BioStar.



6. Map the data to a field by selecting a field label from the drop-down list and then click **OK**.

   Note: Up to four department levels can be displayed in BioStar. In the CSV file, include department levels in the same cell, separated by slashes (for example, “Department 1/Department 2/Department 3”), and then map the cell to the “Department” field in BioStar.

7. Repeat steps 5-6 as necessary to map additional data.
8. When you are finished mapping data to fields, click **Next**.
9. Click **Import**.

10. If you map data to fields in an existing user account, you will prompted to confirm that you wish to overwrite the existing data. Click **Yes** or **Yes to All** to confirm or click **No** or **No to All** to deny.
11. Click **Finish**.

4.6 Manage Time and Attendance

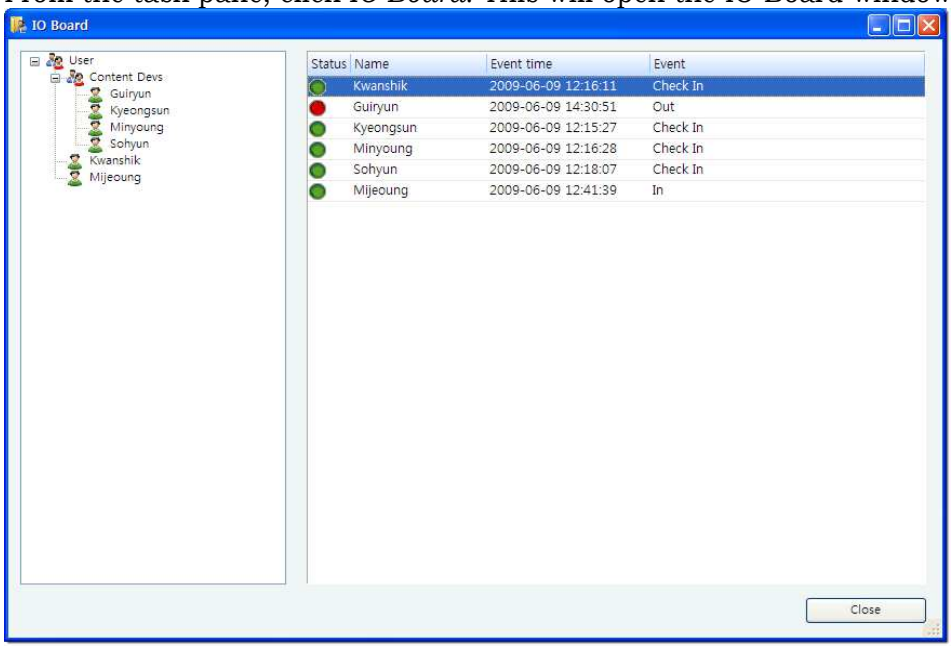
BioStar allows you to monitor the time and attendance status of users and generate reports of T&A events, which you can edit or export as needed.

4.6.1 Monitor T&A Status via the IO Board

The IO Board displays time and attendance events only for entrance and exit events performed via the T&A function keys of access control devices. This feature is available only in the Standard Edition of BioStar.

You can use the board to verify recent T&A activities or to quickly determine which users are checked in or out. Users can use the board to view their own T&A activities. To monitor the time and attendance status of users,

1. Click **Time and Attendance** in the shortcut pane.
2. From the task pane, click *IO Board*. This will open the IO Board window.

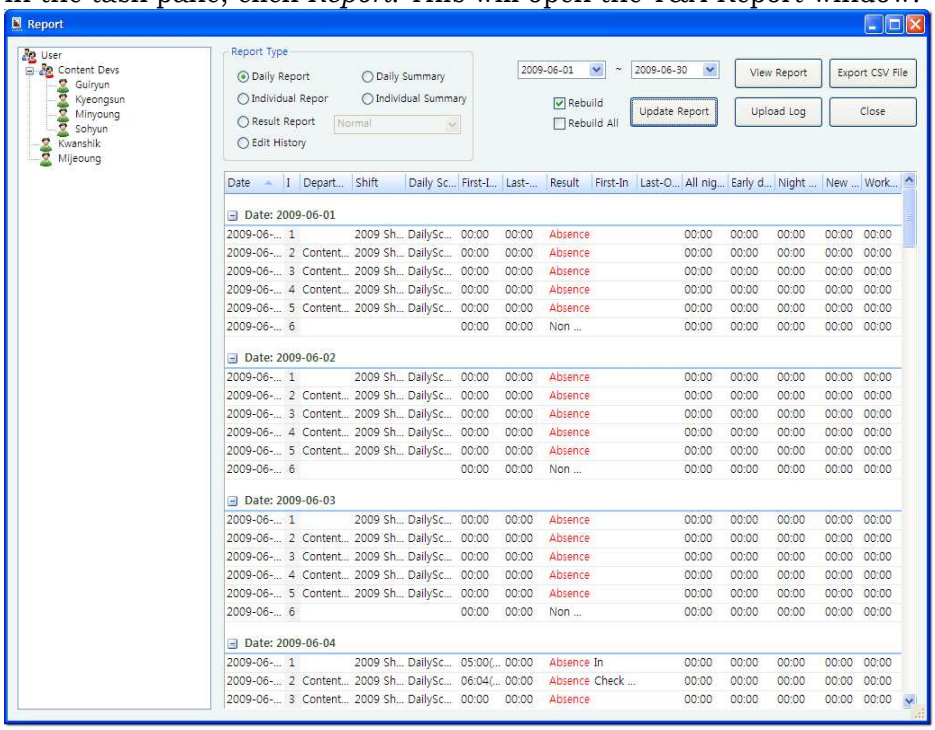


3. Click **User**, a user name, or a department name in the pane on the left. This will display the corresponding T&A status in the pane on the right.
4. To close the window, click **Close**.

4.6.2 Generate T&A Reports

You can generate T&A reports to view various time and attendance events for users. You can also modify and print time and attendance data for other uses, such as calculating payrolls. To generate a T&A report,

1. Click **Time and Attendance** in the shortcut pane.
2. In the task pane, click *Report*. This will open the T&A Report window.



3. Click a radio button to select a report type:
   - **Daily Report** - a report of all activities for the specified date range sorted by date.
   - **Individual Report** - a report of activities for the specified date range sorted by user ID.
   - **Result Report** - a report of activities that you specify via the drop-down list.
   - **Edit History** - a report of edited entries.
   - **Daily Summary** - a summary of activities for the specified date range sorted by date.
   - **Individual Summary** - a summary of activities for the specified date range sorted by user ID.
4. Select a date range by clicking the drop-down calendars.
5. Click **View Report** to retrieve and display the results.

Note: Click **Upload Log** to retrieve data from all networked devices. Click **Update Report** to refresh the report with any data you have modified (see section 4.5.3).

You can sort report data by clicking any column header (the sort will toggle between ascending and descending orders). You can also rearrange the columns by dragging and dropping column headers in a new location. Furthermore, you can add or remove columns by using the menu that appears when you right-click on any column header:

To add a column to the report,

1. Right-click on any column header.
2. Click **Column** and select a column to add to the report.

To remove a column from the report,

1. Right-click on the column you want to remove.
2. Click **Remove column**.

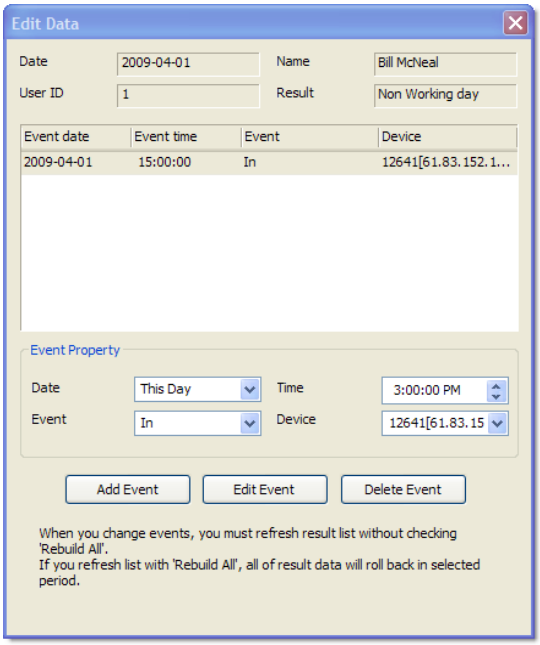
4.6.3 Modify T&A Reports

Time and attendance data can be modified for time reporting or payroll purposes. After generating a T&A report, you can locate cells that you want to modify and then click the cell and enter a new value or select an option from the drop-down list. This will save the modification to the report, but it will not overwrite the original data collected from access control devices. If you want to reproduce the report with the original data, click the checkbox next to “Rebuild” and then click **Update Report**.

To perform detailed modifications on report data,

1. Generate a T&A report as described in 4.5.2.

2. Right-click a cell and click *Detailed editing*. This will open the Edit Data window.



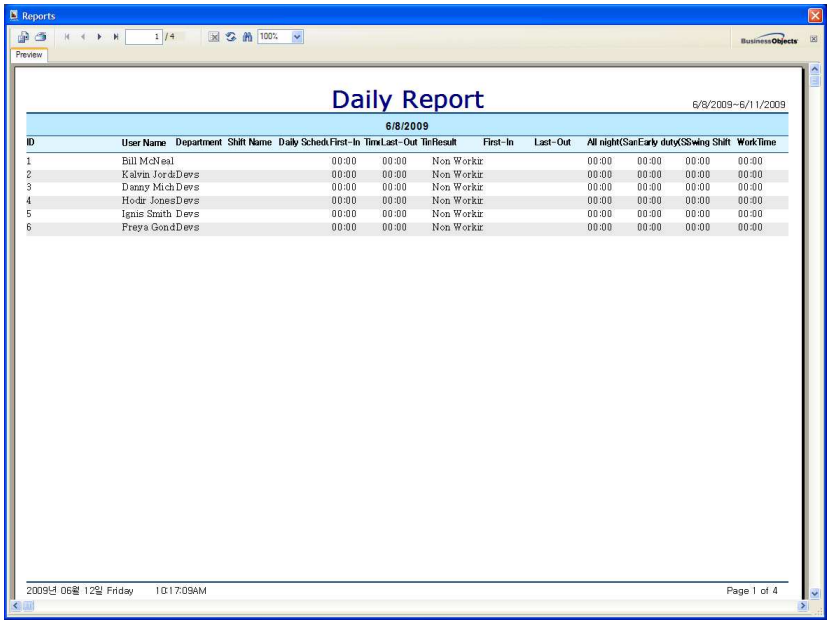
3. To edit an event, change the following event properties as necessary and then click **Edit Event**. To add an event, change the following event properties as necessary and then click **Add Event**. To delete the event, click **Delete Event**.
   - **Date** - select whether the event occurred on this day or the next day.
   - **Event** - select the type of event.
   - **Time** - set the time of the event.
   - **Device** - set the device where the event occurred.
4. When you are finished modifying the event data, click the "X" in the top right corner to close the window.
5. In the T&A Report window, ensure that the "Rebuild" checkbox is NOT checked.
6. Click **Update Report**. The report will show the changes you have made. The changes you have made via the detailed editing will not be restored to the original data even if you click the check box next to "Rebuild" and click **Update Report**. If you want to reproduce the report with the original data, click the checkboxes next to "Rebuild" and "Rebuild All" and then click **Update Report**.

Note: You can sort report data by clicking any column header (the sort will toggle between ascending and descending orders). You can also rearrange the columns by dragging and dropping column headers in a new location.

4.6.4 Print or Export T&A Report Data

To print or export T&A report data,

1. Generate a T&A report as described in 4.5.2 and make any necessary modifications as described in 4.5.3.
2. Click **View Report**. This will open a preview window similar to the one below.



4. To print the report, click the print icon on the toolbar.
5. To export report data, click the export icon on the toolbar and then select an export format and a destination. You can export data in the following formats:
   - Adobe Acrobat (PDF)
   - Crystal Report (RPT)
   - HTML 3.2 or 4.0
   - Microsoft Excel 97-2000 or Microsoft Excel 97-2000–data only (XLS)
   - Microsoft Word or Microsoft Word–editable (RTF)
   - Open Database Connectivity (ODBC)
   - Record Style–Columns with spaces (REC)
   - Report Definition (TXT)
   - Rich Text Format (RTF)
   - Comma Separated Values (CSV)
   - Tab Separated Text (TTX)
   - Text (TXT)
   - XML

Note: You can refresh the report data by clicking the refresh icon on the toolbar. You can also search for text in the report by clicking the search (binoculars) icon on the toolbar.

4.7 Manage Devices

You can easily remove devices, if necessary, and upgrade the device firmware directly from the BioStar interface. When removing devices, first ensure that any new data that may have been added at the terminal has been transferred to the BioStar server.

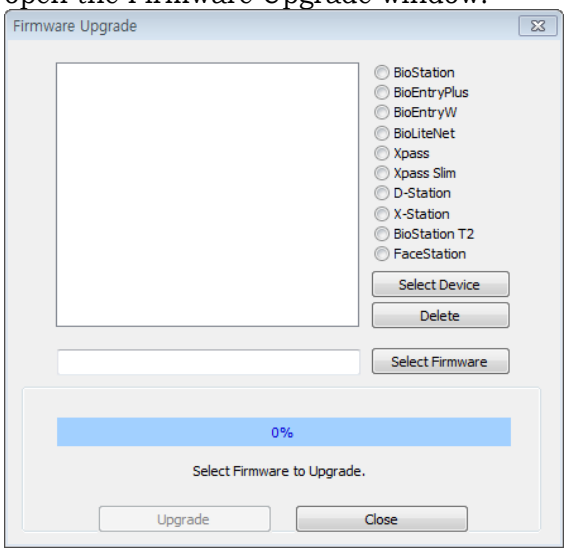
4.7.1 Remove Devices

If you need to remove a device from the BioStar system, click **Device** in the shortcut pane, then right-click the device name and click *Remove Device*.

4.7.2 Upgrade Device Firmware

On occasion, it is necessary to upgrade your devices to the latest firmware version. To upgrade device firmware,

1. From the menu bar, click **Option > Device > Firmware Upgrade**. This will open the Firmware Upgrade window.



2. Click the radio button next to the type of device you want to upgrade.
3. Click **Select Device** and select a device or devices from the Device Tree window.
4. Click **OK** to close the Device Tree window.
5. Click **Select Firmware**.
6. Locate the firmware file on your computer or network and click **Open**.
7. Click **Upgrade**.
8. When the firmware upgrade is complete, wait for the device to restart, and then click **Close**.

4.7.3 Downgrade Device Firmware

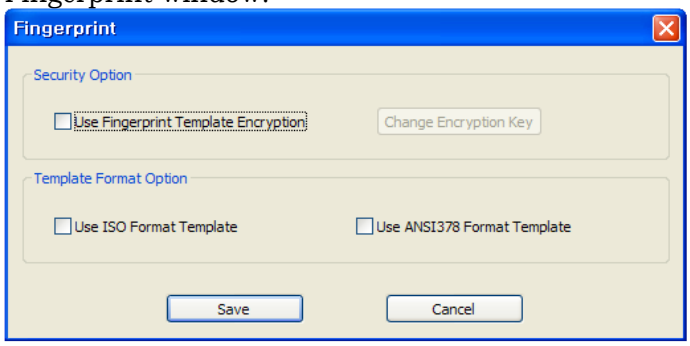
Devices may not work properly if downgraded or reverted back to an older version of firmware. Suprema does not recommend a downgrade. If your devices require a downgrade, please contact Suprema Technical Support (Email: support@supremainc.com), your Suprema distributor, or a local Suprema dealer.

4.8 Activate Fingerprint Encryption

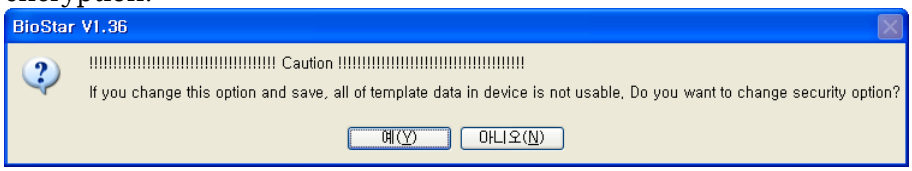
By default, additional fingerprint encryption is turned off. In most cases, activating this encryption is unnecessary. However, you may choose to turn on the encryption to provide extra security or privacy. Keep in mind that activating fingerprint encryption requires management of encryption keys and should be performed only by advanced users.

Activating fingerprint encryption will render all previously saved templates unusable. As a result, it is best to activate the encryption prior to registering users. To activate fingerprint encryption,

1. From the menu bar, click **Option > Fingerprint**. This will open the Fingerprint window.

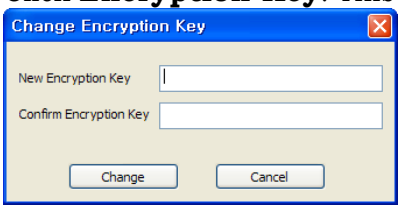


2. Click the checkbox under “Security Option” to activate the fingerprint template encryption.



3. Click **Yes** to acknowledge the warning statement.
4. If desired, you may also change the encryption key:

a. Click **Encryption Key**. This will open the Change Encryption Key window.



b. Enter a new encryption key in the first field.
c. Confirm the key by entering it in the second field.
d. Click **Change**.

5. Click **Save**. The option you have chosen will appear on the Fingerprint tab in the Device pane.

4.9 Change the Fingerprint Template

BioStar offers three types of fingerprint templates: ISO 19794-2, ANSI378, or Suprema's proprietary format. Suprema's format is active by default. Changing fingerprint template options will render all previously saved templates unusable. As a result, it is best to choose a template option prior to registering users. To change the fingerprint template option,

1. From the menu bar, click **Option > Fingerprint**. This will open the Fingerprint window.
2. Click the checkbox under "Use ISO Format Template" to select the ISO format or "Use ANSI378 Format Template" to select the ANSI format.
3. Click **Yes** to acknowledge the warning statement.
4. Click **Save**.

05 Customize Settings

This section describes the settings available in the BioStar software. BioStar provides precise control and customization of the access control system via settings for device functions, door and zone behaviors, and user accounts.

5.1 Customize Device Settings

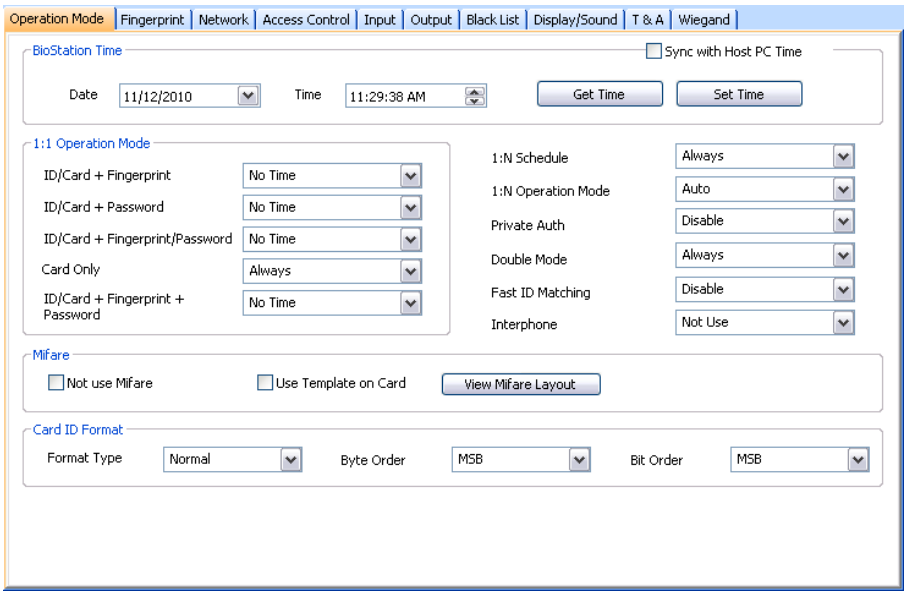
While most device settings are similar for BioStation, BioEntry Plus, BioEntry W, BioLite Net, Xpass, Xpass Slim, D-Station, and X-Station devices, the devices provide slightly different capabilities. The sections that follow describe the settings for each device separately. To access the tabs described below, click **Device** in the shortcut pane, then click a device name.

5.1.1 Customize Settings for BioStation Devices

The sections that follow describe the settings available for BioStation devices. Customize the way BioStation devices function by changing these settings to suit your particular environment and operational needs.

5.1.1.1 Operation Mode tab

The Operation Mode tab allows you to customize time and various operation modes settings for BioStation devices.



- **BioStation Time**
  - **Date** - manually set the device date with a drop-down calendar.
  - **Time** - manually set the device time.
  - **Sync with Host PC Time** - check this box to automatically synchronize the device time with the time of the host computer.
  - **Get Time** - get the current time displayed by the device.
  - **Set Time** - set the time on the device.
- **1:1 Operation Mode** - the drop-down lists in this area allow you to control the authentication mode by schedule. For example, you can choose a normal authentication mode for working hours and a more strict authentication mode for hours outside the normal schedule. You can specify authentication modes either by device or by user (see section 5.4.1). Unless a particular mode is specified for a user, the device authentication mode will apply.
  - **ID/Card + Fingerprint** - set the device to require ID or card plus fingerprint authorization (*Always*, *Disable*, or custom schedule).
  - **ID/Card + Password** - set the device to require ID or card plus password authorization (*Always*, *Disable*, or custom schedule).
  - **ID/Card + Fingerprint/Password** - set the device to require ID or card plus fingerprint or password authorization (*Always*, *Disable*, or custom schedule).

- **Card Only** - set the device to require only card authorization (*Always*, *Disable*, or custom schedule).
- **ID/Card + Fingerprint + Password** - set the device to require ID or card plus fingerprint plus password authorization (*Always*, *Disable*, or custom schedule).

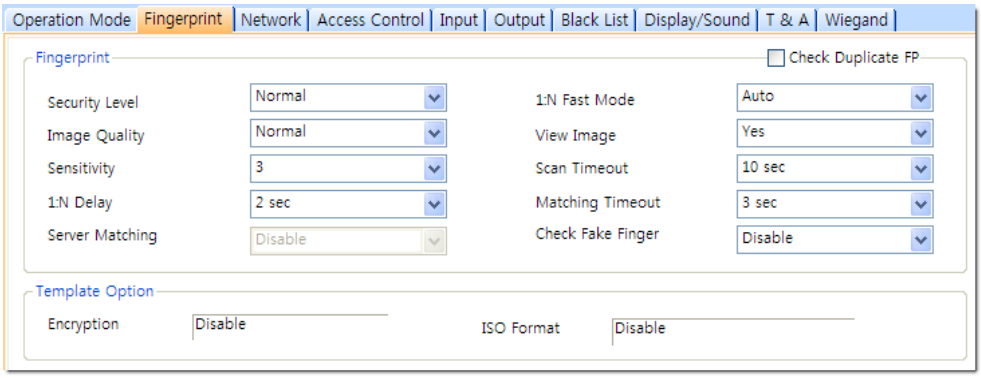
- **Mifare** (available only on BioStation Mifare devices)
  - **Not use Mifare** - check this box to disable MIFARE card authorization.
  - **Use Template on Card** - check this box to use the template on the MIFARE card for authorization.
  - **View Mifare Layout** - click this button to view the MIFARE layout used by the device. For more information about configuring MIFARE layouts, see section 3.6.4.6.
- **Card ID Format**
  - **Format Type** - set the type of pre-processing to occur on card ID data (*Normal* or *Wiegand*). If "Normal" is selected, the card ID data will processed in its original form. If "Wiegand" is selected, devices will interpret card ID data according to the Wiegand format settings.
  - **Byte Order** - specify whether to swap ID card data between cards and devices by most significant byte (*MSB*) or least significant byte (*LSB*).
  - **Bit Order** - specify whether to swap ID card data between cards and devices by most significant bit (*MSB*) or least significant bit (*LSB*).
- **Other options**
  - **1:N Schedule** - set a schedule for using fingerprint only authentication (*Always*, *Disable*, or custom schedule).
  - **1:N Operation Mode** - set a method for activating the fingerprint sensor (*Auto*, *Ok/Function Key*, or *None*).
  - **Private Auth** - set the device to allow a private authorization method (*Disable* or *Enable*). If enabled, the authentication mode of the user will be determined by a user's "Authorization" setting, which is located on the Details tab. If disabled, the authentication mode will be determined by operation mode settings of the device.
  - **Double Mode** - set the device to require authentication of two users' access cards or fingerprints (*Always*, *Disable*, or custom schedule). The timeout for presenting the second authentication is 15 seconds.
  - **Fast ID Matching** - set the device to allow quicker authentication, by requiring users to input only the first two digits of the user ID and scan a single fingerprint (*Enable* or *Disable*). This option

attempts authentication for a smaller subset of users (only those with the same first two digits in their user IDs) to increase matching speed.

- **Note:** This option does not support server matching (see 5.1.1.2). When using function keys for T&A events (see 5.1.1.8), only keys F1-F4 are supported (BioStation V1.7 and higher).
- **Interphone** - set the device to act as an interphone to allow communication between people on either side of the door (*Not Use* or *Use*).

5.1.1.2 Fingerprint tab

The Fingerprint tab allows you to customize fingerprint authorization settings for BioStation devices.



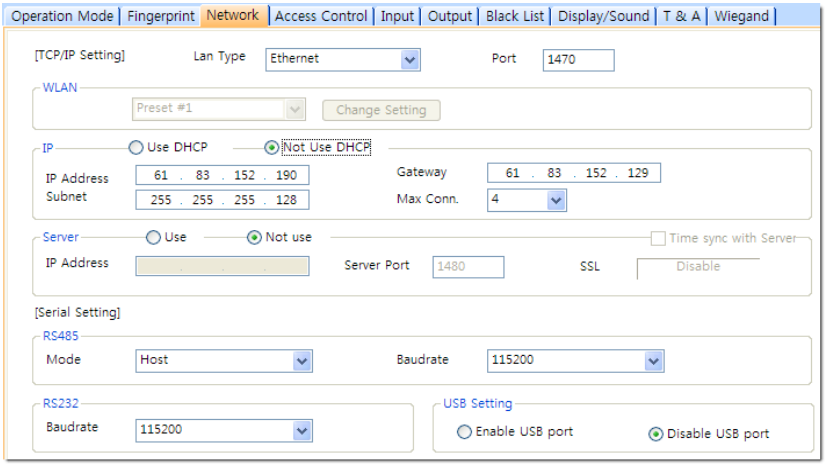
- **Fingerprint**
  - **Security Level** - set the security level to use for fingerprint authorization (*Normal*, *Secure*, or *Most Secure*). Keep in mind that as the security level is increased, so too is the likelihood of a false rejection.
  - **Image Quality** - set the strictness of the quality check for fingerprint scans (*Weak*, *Normal*, or *Strict*). If a fingerprint image is below the specified quality level, it will be rejected.
  - **Sensitivity** - set the sensitivity of the fingerprint scanner (*0 [Min]* to *7 [Max]*). A higher sensitivity setting will result in more easily captured fingerprint scans, but also increases the sensitivity to external noise.
  - **1:N Delay** - set the delay between scans when identifying fingerprints (*0 sec* to *10 sec*). This delay prevents the scanner from processing the same fingerprint more than once if a user has not yet removed his or her finger from the scanner.

- **1:N Fast Mode** - set the device to use Fast Mode to reduce the amount of time required for matching fingerprints (*Auto*, *Normal*, *Fast*, or *Fastest*). Setting Fast Mode to *Auto* will adjust the matching speed according to the number of enrolled templates.
- **View Image** - set to show or hide fingerprint images on the BioStation display (*Yes* or *No*).
- **Scan Timeout** - set the length of time before the fingerprint scanner will timeout (*1 sec* to *20 sec*). If a user does not place a finger on the device within the timeout period, the authorization will fail.
- **Matching Timeout** - set the length of time before the device will timeout when trying to identify a fingerprint match (*0 [Infinite]* to *10 sec*).
- **Server Matching** - enable this setting to perform fingerprint or card ID matching at the BioStar server, instead of the device. When this mode is enabled, the devices will send the fingerprint template or card ID to the server to verify a match. This mode is useful when you have more users than can be downloaded to a device or user information cannot be distributed due to security concerns.
- **Check Fake Finger** – set the device to detect the use of fake fingerprints, such as those made from silicon or rubber, and prevent unauthorized access.

• **Check Duplicate FP** - set the device to determine whether or not a scanned fingerprint has been previously enrolled. If the device determines that a fingerprint has been previously enrolled, the enrollment process will fail.

5.1.1.3 Network tab

The Network tab allows you to customize network and server settings for BioStation devices.



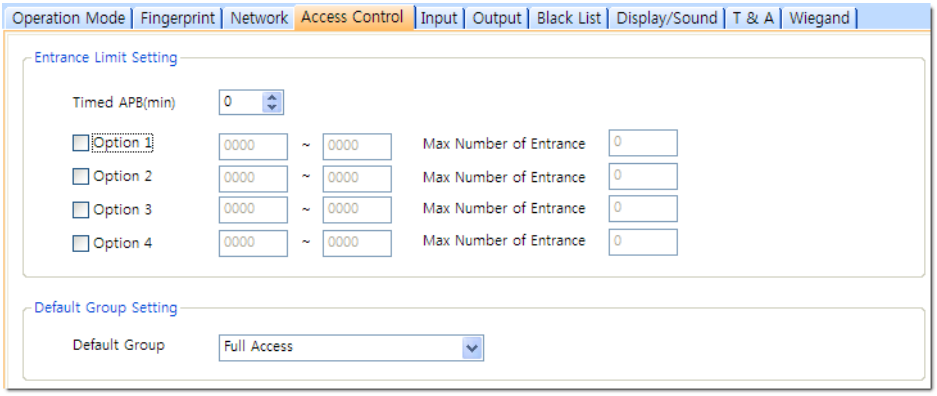
- **TCP/IP Setting**
  - **LAN Type -** select a type of LAN connection from the drop-down list (*Disable*, *Ethernet*, or *Wireless LAN*).
  - **Port** - specify a port to use for the device.
  - **WLAN** - select a preset WLAN configuration from the drop-down list. This option is active only when WLAN is selected as the TCP/IP setting.
  - **Change setting** - click to specify settings for a wireless local area network (WLAN). This option is active only when WLAN is selected as the TCP/IP setting. For more information about configuring settings for a WLAN, see section 3.2.4.1.
  - **Use DHCP** - click this radio button to enable the dynamic host configuration protocol (DHCP) for the device.
  - **Not Use DHCP** - click this radio button to disable the dynamic host configuration protocol (DHCP) for this device.
  - **IP Address** - specify an IP address for the device.
  - **Subnet** - specify a subnet address for the device.
  - **Gateway** - specify a network gateway.
  - **Max Conn.** - specify the maximum number of connections to allow.
- **Server**
  - **Use** - click this radio button to enable the server mode.
  - **Not use** - click this radio button do disable server settings.
  - **IP Address** - specify an IP address for the BioStar server.

- **Server Port** - specify the port used to connect to the server.
- **SSL** - displays the status of SSL for the server connection.
- **Time sync with Server** - check this box to synchronize the device time with the time maintained at the server.

- **RS485**
  - **Mode** - set the mode for a device connected via RS485 (*Disable*, *Host*, *Slave*, or *PC Connection*). For more information about RS485 modes, see sections 3.2.1 and 3.2.2.
  - **Baudrate** - set the baud rate for a device connected via RS485 (*9600* to *115200*).
- **RS232** - set the baud rate for a device connected via RS232 (9600 to 115200).
- **USB Setting** - click the radio buttons to enable or disable the USB port on the BioStation device.

5.1.1.4 Access Control tab

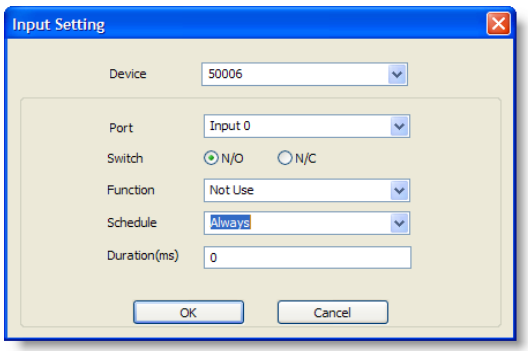
The Access Control tab allows you to customize entrance limit settings and default access groups for a BioStation device.



- **Entrance Limit Setting**
  - **Timed APB (min)** - set the duration (in minutes) that a user will be unable to regain entry to an area via the device. Once a user has gained entry, the device will reject the user's card or fingerprint authorization for the time period specified here.
  - **Option 1-4** - click the checkbox to enable an entrance limit setting, and then specify the effective hours for the entrance limit.
  - **Max Number of Entrance** - set the maximum number of entries allowed during the specified time limit.
- **Default Group Setting** - select a default access group to be applied to new users who have not been assigned to another access group.

5.1.1.5 Input tab

The input tab lists input settings you have specified for a BioStation device. Buttons at the bottom of the tab allow you to add, modify, or delete input settings. To add or modify settings, you must specify them from the Input Setting window. For more information about configuring input settings, see section 3.10.3.2.

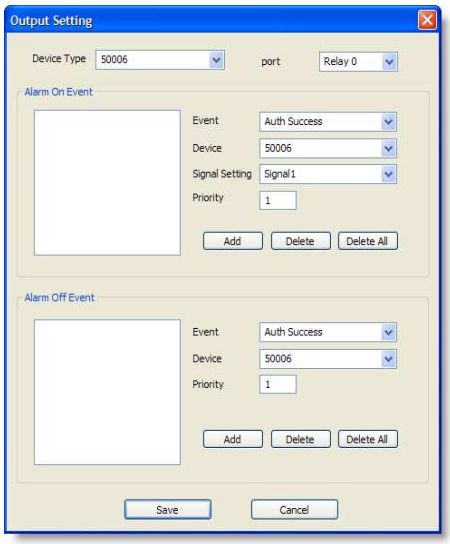


- **Device** - select the BioStation (or Secure I/O) device for which you will add or modify settings.
- **Port** - select an input port (Input 0, Input 1, or Tamper). For Secure I/O devices, these settings are available: Input 0, Input 1, Input 2, Input 3.
- **Switch** - click the radio buttons to specify the normal position of the input switch (N/O - normally open or N/C - normally closed).
- **Function** - select an action to associate with the input:
  - **Not Use** - the input port will not be monitored.
  - **Generic Input** - the input port will be monitored for a triggering action (events specified with “Detect Input 0-3” in the Output settings window—see section 5.1.1.6).
  - **Emergency Open** - open doors controlled by this device. The normal door open period will be ignored and doors will remain open until an operator sends a “Close Door” command via the Door/Zone Monitoring tab (see section 4.4.1).
  - **Release All Alarms** - cancel alarms associated with this device.
  - **Restart Device** - restart the device.
  - **Disable Device** - disable the device. A disabled device will not communicate with the BioStar server or process fingerprints or card inputs. To enable communication again, an administrator must enter the master password for a BioStation device or provide authentication locally for a BioEntry Plus or BioEntry W device.

- **Schedule** - set the schedule during which the inputs will be monitored (*Always*, Disable, or custom schedule).
- **Duration (ms)** - set the duration (in milliseconds) an input signal must last to trigger the specified action.

5.1.1.6 Output tab

The Output tab lists output settings you have specified for a BioStation device. Buttons at the bottom of the tab allow you to add, modify, or delete output settings. To add or modify settings, you must specify them from the Output Setting window. For more information about configuring output settings, see section 3.10.3.1.



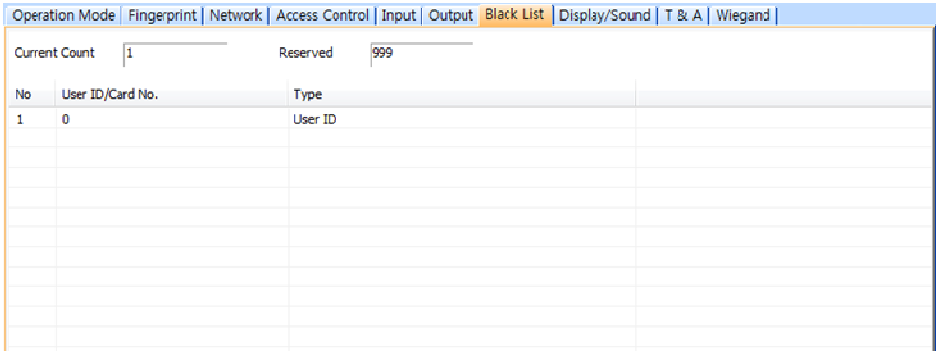
- **Device Type** - select the device type for which you will add or modify settings.
- **Port** - select an output port (Relay 0). For Secure I/O devices, these settings are available: Relay 0 or Relay 1.
- **Alarm On Event** - specify settings and click **Add** to add the event to the Alarm On Event list. These events will activate an alarm.
  - **Event** - select an event that will activate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, *Detect Input # 1-3*).
  - **Device** - select the device to monitor for an alarm event.
  - **Signal Setting** - select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).

- **Priority** - set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on (activate) event with a priority of 2 can be canceled only by an alarm off (deactivate) event with a priority of 1 or 2.

- **Alarm Off Event** - specify settings and click **Add** to add the event to the Alarm Off Event list. These events will deactivate an alarm.
  - **Event** - select an event that will deactivate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input # 1-3*).
  - **Device** - select the device to monitor for an alarm event.
  - **Priority** - set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, a priority 2 “alarm on” event (activate) can be overridden only by an “alarm off” (deactivate) event with a priority of 1 or 2.

5.1.1.7 Black List tab

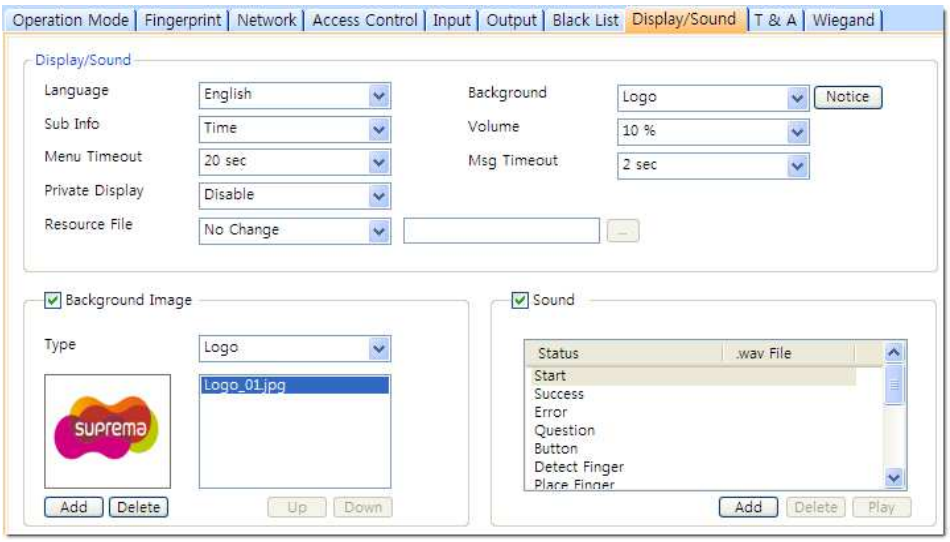
The Black List tab allows you to register user IDs or access card numbers and prevent them from being authenticated with the device.



- **Current Count** – indicates the total number of user IDs and access cards that have been registered.
- **Reserved** – indicates the remaining number of user IDs and access cards that can be registered.

5.1.1.8 Display/Sound tab

The Display/Sound tab allows you to customize the BioStation display and event sounds. To save changes to display or sound settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.



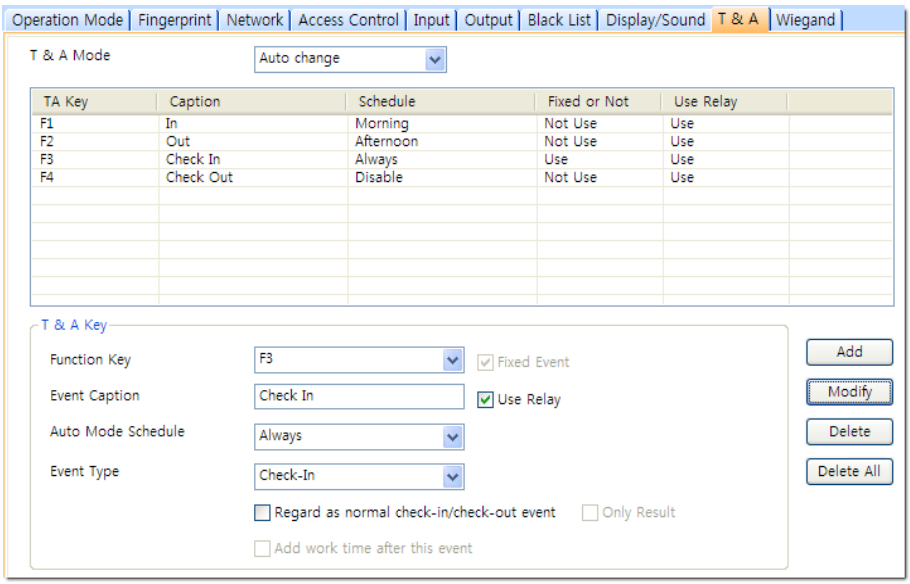
- **Display/Sound**
  - **Language** - set the language to use on the display (*Korean*, *English*, or *Custom*).
  - **Sub Info** - set the info to display at the bottom of the BioStation display (*Time*, or *None*).
  - **Menu Timeout** - set the length of time before the display will return to the idle screen (*Infinite*, *10 sec*, *20 sec*, or *30 sec*).
  - **Private Msg** - enable or disable the option to show a private message on the BioStation display (*Disable* or *Enable*). You can add a private message from the Event tab in the User pane: click **Modify Private Information**, set options for display count and display duration, enter text in the Private Message field, and then click **Save**.
  - **Resource** - set the language resource file to use for the BioStar interface (*No Change*, *English*, *Korean*, or *Custom*). To use a language resource file other than English or Korean, select *Custom* and then click the ellipsis (...) button to locate the resource file.

- **Background** - set the type of background for the BioStation display (*Logo*, *Notice*, or *Slide Show*). Supported file types (JPG, GIF, BMP, and PNG) cannot exceed 320x240 pixels each. Only one image at a time can be used as a logo or notice, while up to 16 images can be displayed (at a set interval) in a slide show.
- **Notice** - click this button to create a notice that will be shown on the BioStation display. After creating a notice, you can click **Apply** to apply the notice to the current device or **Apply to Others** to apply the notice to additional devices.
- **Volume** - set the volume of the BioStation device (*10%* to *100%*).
- **Msg Timeout** - set the length of time that a failure or confirmation message will be displayed.

- **Background Image** - click this checkbox to upload new background images. Click the plus sign (+) to locate and add a new image file.
- **Sound** - click this checkbox to enable and add custom event sounds. Click an event from the list and then click the plus sign (+) to locate and add a new sound file.

5.1.1.9 T&A tab

The T&A tab allows you to configure the mode and key settings for a BioStation device. To save changes to time and attendance settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.



- **T&A Mode** - set the time and attendance mode:
  - **Not Use** - disable the time and attendance functions for this device.

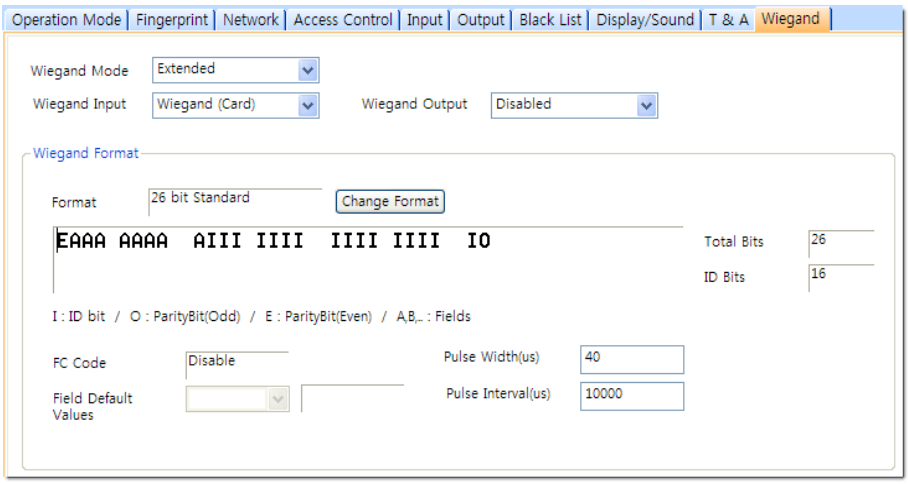
- **Manual** - users must press the specified key every time they enter or leave to record their T&A events.
- **Manual Fix** - when a T&A key is pressed, the device will remain in that mode until a different T&A key is pressed.
- **Auto change** - the device will automatically change T&A modes to correspond with the functions specified for a time period.
- **Event Fix** - the device will perform only the specified T&A function.

• **T&A Key** - specify which keys to use for T&A events and the event types associated with them:

- **Function Key** - select a function key from the drop-down list to assign a T&A event (*F1-F4*, *1-9*, *CALL*, *0*, or *ESC)*. If you are using the Event Fix mode, you can click the checkbox to the right to designate a fixed event.
- **Event Caption** - enter a caption for the event.
- **Auto Mode Schedule** - when using the Auto Change mode, you can specify when the event will occur by selecting a timezone in the drop-down list. For more information on creating a timezone, see section 3.7.1.
- **Event Type** - set the type of event to assign to the key (*Not Use*, *Check In*, *Check Out*, *In*, or *Out*). In/Out indicates the general check in/out events during a day whereas Check In/Out indicates the formal check in/out events upon arrival and departure at work—or the first check–in and the last check–out events on that day. When you choose Check In or Check Out, you can enable the “Regard as normal check-in/check-out event” option. If this option is enabled, users who activate the appropriate keys will be regarded as arriving or leaving on time at work even though they actually arrive late or leave early. If you enable the “Only Result” option, they appear being on time on T&A reports but their work time will be calculated correctly based on their actual check in/out time. If you choose *Out*, you can enable the “Add work time after this event” option. If this option is enabled, users activating the appropriate key will be considered working for the remainder of the time slot even if they leave the office early.

5.1.1.10 Wiegand tab

The Wiegand tab allows you to configure the Wiegand format for a BioStation device. Click **Change Format** to launch the Wiegand Configuration wizard. For more information on configuring the Wiegand format, see section 3.2.12.



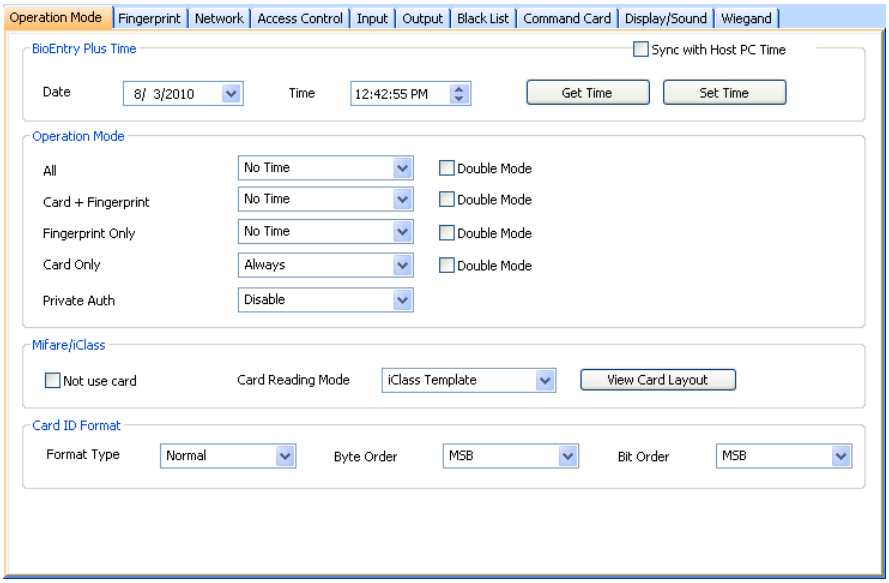
- **Wiegand Mode** - set the mode of Wiegand input to use when reading card ID data (*Legacy* or *Extended*). The Legacy mode will treat connected RF devices as part of their host devices (this is the typical function of previous versions of BioStar). The Extended mode will allow RF card readers to operate independently, which allows them to be associated with doors, included in zones, and leave logs with their own device IDs.
- **Wiegand Input** - assign the Wiegand input:
  - **Disabled** - the input will not be used.
  - **Wiegand [Card]** - the ID field of the Wiegand string is interpreted as a card ID.
  - **Wiegand [User]** - the ID field of the Wiegand string is interpreted as a user ID.
- **Wiegand Output** - assign the Wiegand output:
  - **Disabled** - the output will not be used.
  - **Wiegand [Card]** - inserts the card ID of the authenticated user in the ID field of the Wiegand string.
  - **Wiegand [User]** - inserts the user ID of the authenticated user in the ID field of the Wiegand string.

5.1.2 Customize Settings for BioEntry Plus or BioEntry W Devices

The sections below describe the settings available for BioEntry Plus and BioEntry W devices. Customize the way BioEntry Plus or BioEntry W devices function by changing these settings to suit your particular environment and operational needs.

5.1.2.1 Operation Mode tab

The Operation Mode tab allows you to customize time and various operation modes settings for BioEntry Plus or BioEntry W devices.



- **BioEntry Plus Time/BioEntry W Time**
  - **Date** - manually set the device date with a drop-down calendar.
  - **Time** - manually set the device time.
  - **Sync with Host PC Time** - check this box to automatically synchronize the device time with the time of the host computer.
  - **Get Time** - get the current time displayed by the device.
  - **Set Time** - set the time on the device.
- **Operation Mode** - for each of the following options, click the corresponding checkbox to enable Double Verification Mode, which requires verification of two users' credentials to gain entry to a door.
  - **All** - set the device to allow all types of authorization (*Always*, *Disable*, or custom schedule).
  - **Card + Fingerprint** - set the device to require card plus fingerprint authorization (*Always*, *Disable*, or custom schedule).
  - **Only Fingerprint** - set the device to require only fingerprint authorization (*Always*, *Disable*, or custom schedule).

- **Only CARD** - set the device to require only card authorization (*Always*, *Disable*, or custom schedule).
- **Private Auth** - set the device to allow a private authorization method (*Disable* or *Enable*). If enabled, the authentication mode of the user will be determined by a user's authorization setting (Private Auth Mode), which is located on the Details tab in the User pane. If disabled, the authentication mode will be determined by the operation mode settings of the device.
- **Double Verification Mode** - set the device to require verification from two users during a selected schedule (*Always*, *Disable*, or custom schedule).

• **Mifare/iCLASS** (available on select models)

- Bio Entry Plus Mifare devices:
- **Not use Card** - check this box to disable MIFARE card authorization.
- **Card Reading Mode** - set the tyupe of card authorization mode (*Mifare Template* or *Mifare CSN only*)
- **View Mifare Layout** - click this button to configure the MIFARE layout used by the device. For more information about configuring MIFARE layouts, see section 3.6.4.6.

Bio Entry Plus iCLASS devices:

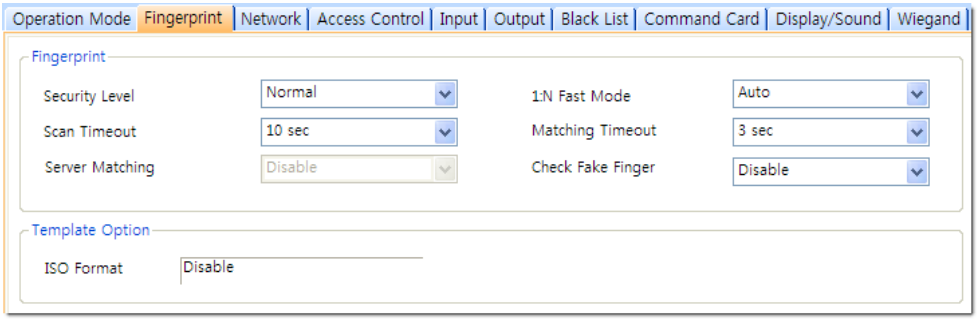
- **Not use Card** - check this box to disable iCLASS or FeliCa card authorization.
- **Card Reading Mode** – set the type of card authorization mode (*iCLASS Template*, *iCLASS CSN only*, or *FeliCa CSN only*).
- **View Card Layout** - click this button to configure the iCLASS layout used by the device. For more information about configuring iCLASS layouts, see section 3.6.4.7.

• **Card ID Format**

- **Format Type** - set the type of pre-processing to occur on card ID data (*Normal* or *Wiegand*). If "Normal" is selected, the card ID data will processed in its original form. If "Wiegand" is selected, devices will interpret card ID data according to the Wiegand format settings.
- **Byte Order** - specify whether to swap ID card data between cards and devices by most significant byte (*MSB*) or least significant byte (*LSB*).
- **Bit Order** - specify whether to swap ID card data between cards and devices by most significant bit (*MSB*) or least significant bit (*LSB*).

5.1.2.2 Fingerprint tab

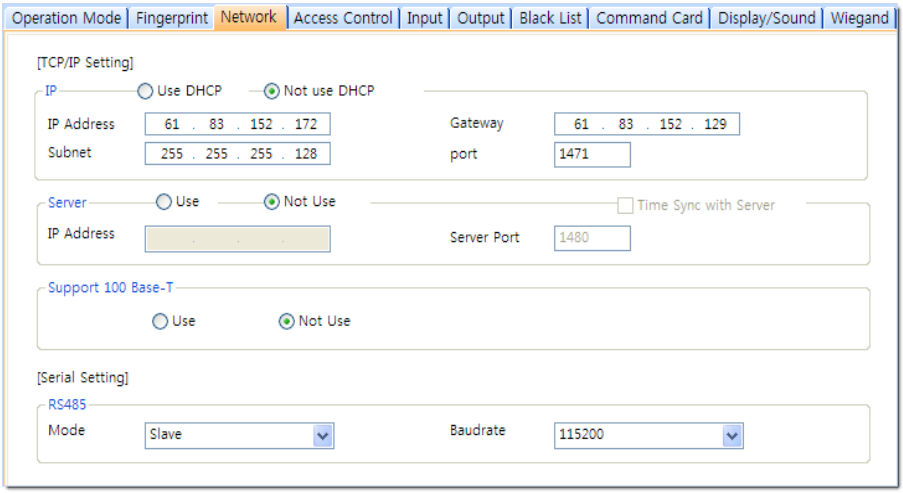
The Fingerprint tab allows you to customize fingerprint authorization settings for BioEntry Plus or BioEntry W devices.



- **Fingerprint**
  - **Security Level** - set the security level to use for fingerprint authorization (*Normal*, *Secure*, or *Most Secure*). Keep in mind that as the security level is increased, so too is the likelihood of a false rejection.
  - **Scan Timeout** - set the length of time before the fingerprint scanner will timeout (*1 sec* to *20 sec*). If a user does not place a finger on the device within the timeout period, the authorization will fail.
  - **Server Matching** - enable this setting to perform fingerprint or card ID matching at the BioStar server, instead of the device. When this mode is enabled, the devices will send the fingerprint template or card ID to the server to verify a match. This mode is useful when you have more users than can be downloaded to a device or user information cannot be distributed due to security concerns.
  - **1:N Fast Mode** - set the device to use Fast Mode to reduce the amount of time required for matching fingerprints (*Auto*, *Normal*, *Fast*, or *Fastest*). Setting Fast Mode to *Auto* will adjust the matching speed according to the number of enrolled templates.
  - **Matching Timeout** - set the length of time before the device will timeout when trying to identify a fingerprint match (*0 [Infinite]* to *10 sec*).
  - **Check Fake Finger** – set the device to detect the use of fake fingerprints, such as those made from silicon or rubber, and prevent unauthorized access.

5.1.2.3 Network tab

The Network tab allows you to customize network and server settings for BioEntry Plus or BioEntry W devices.



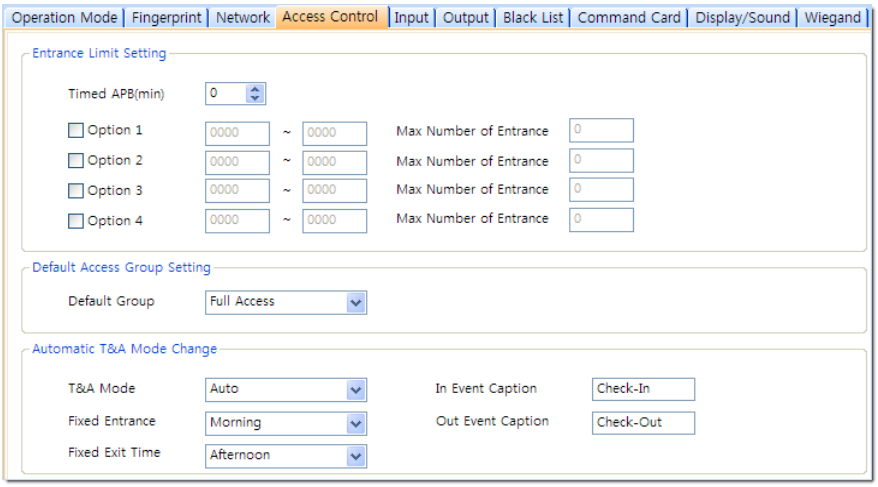
- **TCP/IP**
  - **Use DHCP** - click this radio button to enable the dynamic host configuration protocol (DHCP) for the device.
  - **Not Use DHCP** - click this radio button to disable the dynamic host configuration protocol (DHCP) for this device.
  - **IP Address** - specify an IP address for the device.
  - **Subnet** - specify a subnet address for the device.
  - **Gateway** - specify a network gateway.
  - **Port** - specify a port to use for the device.
- **Server**
  - **Use** - click this radio button to use specific server settings.
  - **Not use** - click this radio button to disable server settings.
  - **IP Address** - specify an IP address for the BioStar server.
  - **Time sync with Server** - check this box to synchronize the device time with the time maintained at the server.
- **Support 100 Base-T** - this option allows you to enable or disable a fast Ethernet connection for the device. When enabled, the device will detect the Ethernet network and automatically establish the best connection. If you do not enable this option, the device will attempt to establish a 10Base-T Ethernet connection.
  - **Use** - click this radio button to enable the 100base-T connection for the device.

- **Not Use** - click this radio button to disable the 100base-T connection for the device.

- **RS485**
  - **Mode** - set the mode for a device connected via RS485 (*Disable*, *Host*, *Slave*, or *PC Connection*).
  - **Baudrate** - set the baud rate for a device connected via RS485 (*9600* to *115200*).

5.1.2.4 Access Control tab

The Access Control tab allows you to customize entrance limit settings and default access groups, and T&A mode settings for a BioEntry Plus or BioEntry W device.

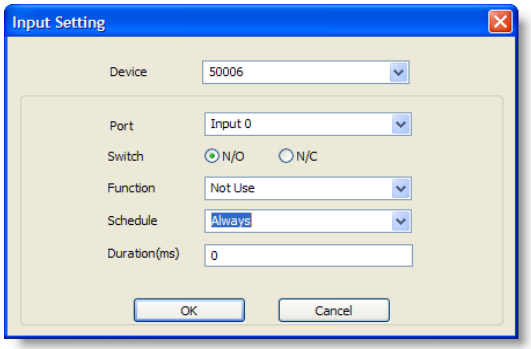


- **Entrance Limit Setting**
  - **Timed APB (min)** - set the duration (in minutes) that a user will be unable to regain entry to an area via the device. Once a user has gained entry, the device will reject the user's card or fingerprint authorization for the time period specified here.
  - **Option 1-4** - click the checkbox to enable an entrance limit setting, and then specify the effective hours for the entrance limit.
  - **Max Number of Entrance** - set the maximum number of entries allowed during the specified time limit.
- **Default Access Group Setting** - select a default access group to be applied to new users who have not been assigned to another access group.
- **Automatic T&A Mode Change**
  - **T&A Mode** - set the time and attendance mode for the device (*Disable*, *Fixed In*, *Fixed Out*, and *Auto*).

- **Fixed Entrance** - when the "Auto" T&A mode is selected, specify when to allow entrance events by selecting a timezone (*Always*, *Disable*, or custom timezone) in the drop-down list. For more information on creating a timezone, see section 3.7.1.
- **Fixed Exit Time** - when the "Auto" T&A mode is selected, specify when to allow exit events by selecting a timezone (*Always*, *Disable*, or custom timezone) in the drop-down list. For more information on creating a timezone, see section 3.7.1.
- **In Event Caption** - set a caption for check-in.
- **Out Event Caption** - set a caption for check-out.

5.1.2.5 Input tab

The input tab lists input settings you have specified for a BioEntry Plus or BioEntry W device. Buttons at the bottom of the tab allow you to add, modify, or delete input settings. To add or modify settings, you must specify them from the Input Setting window. For more information about configuring input settings, see section 3.10.3.2.



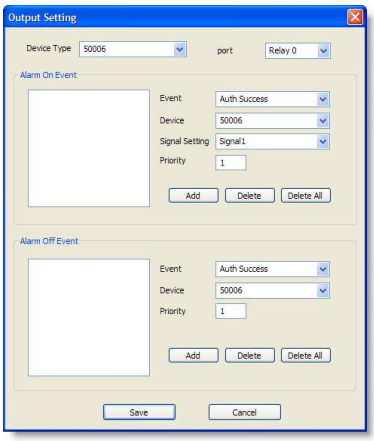
- **Device** - select the BioEntry Plus or BioEntry W (or Secure I/O) device for which you will add or modify settings.
- **Port** - select an input port (Input 0, Input 1, or Tamper). For Secure I/O devices, these settings are available: Input 0, Input 1, Input 2, Input 3.
- **Switch** - click the radio buttons to specify the normal position of the input switch (N/O - normally open or N/C - normally closed).
- **Function** - select an action to associate with the input:
  - **Not Use** - the input port will not be monitored.
  - **Generic Input** - the input port will be monitored for a triggering action (events specified with "Detect Input 1-3" in the Output settings window—see section 5.1.2.6).

- **Emergency Open** - open doors controlled by this device. The normal door open period will be ignored and doors will remain open until an operator sends a “Close Door” command via the Door/Zone Monitoring tab (see section 4.4.1).
- **Release All Alarms** - cancel alarms associated with this device.
- **Restart Device** - restart the device.
- **Disable Device** - disable the device. A disabled device will not communicate with the BioStar server or process fingerprints or card inputs. To enable communication again, an administrator must enter the master password for a BioStation device or provide authentication locally for a BioEntry Plus or BioEntry W device.

- **Schedule** - set the schedule for the input actions (*Always*, *Disable*, or custom schedule).
- **Duration (ms)** - set the duration (in milliseconds) an input signal must last to trigger the specified action.

5.1.2.6 Output tab

The Output tab lists output settings you have specified for a BioEntry Plus or BioEntry W device. Buttons at the bottom of the tab allow you to add, modify, or delete output settings. To add or modify settings, you must specify them from the Output Setting window. For more information about configuring output settings, see section 3.10.3.1.



- **Device Type** - select the device type for which you will add or modify settings.
- **Port** - select an output port (*Relay 0*). For Secure I/O devices, these settings are available: *Relay 0* or *Relay 1*.
- **Alarm On Event** - specify settings and click **Add** to add the event to the Alarm On Event list. These events will activate an alarm.

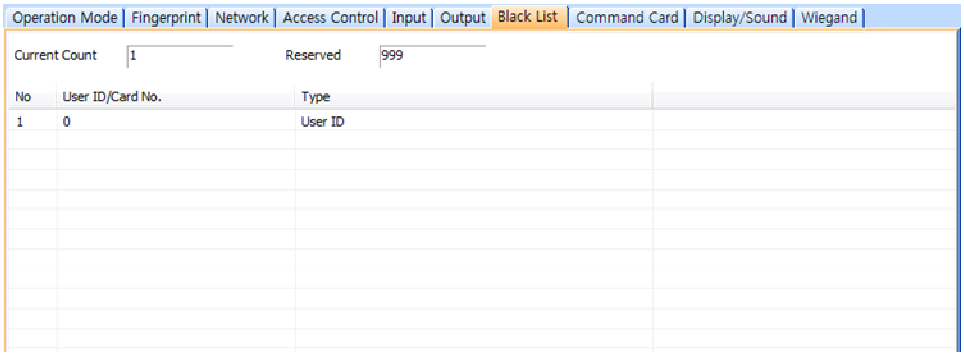
- **Event** - select an event that will activate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input #1-3*).
- **Device** - select the device to monitor for an alarm event.
- **Signal Setting** - select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).
- **Priority** - set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on (activate) event with a priority of 2 can be canceled only by an alarm off (deactivate) event with a priority of 1 or 2.

• **Alarm Off Event** - specify settings and click **Add** to add the event to the Alarm Off Event list. These events will deactivate an alarm.

- **Event** - select an event that will deactivate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input #1-3*).
- **Device** - select the device to monitor for an alarm event.
- **Priority** - set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on event (activate) can be overridden only by an alarm off (deactivate) event with a priority of 1 or 2.

5.1.2.7 Black List tab

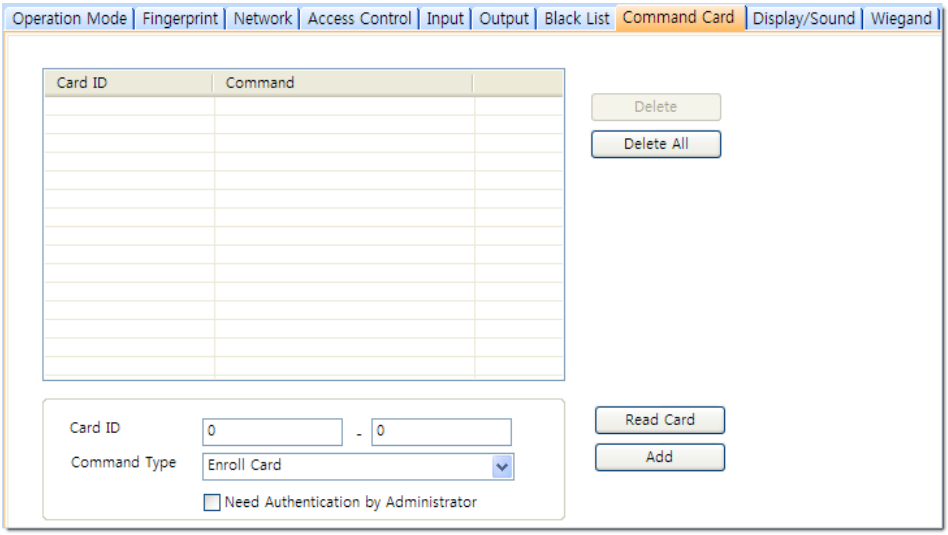
The Black List tab allows you to register user IDs or access card numbers and prevent them from being authenticated with the device.



- **Current Count** – indicates the total number of user IDs and access cards that have been registered.
- **Reserved** – indicates the remaining number of user IDs and access cards that can be registered.

5.1.2.8 Command Card tab

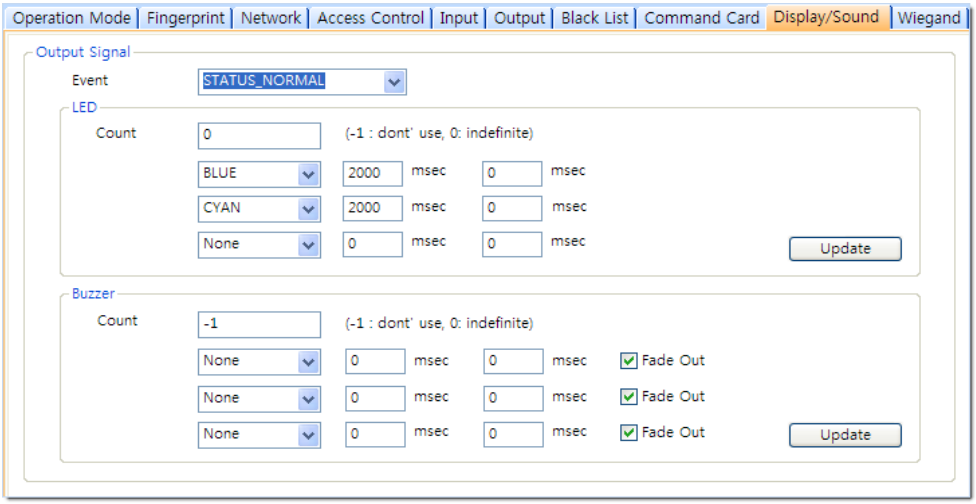
The Command Card tab allows you to issue command cards. For more information about command cards, see section 3.2.5.1.



- **Card ID** - enter the card ID or click **Read Card** and place a command card on the reader to automatically populate the fields.
- **Command Type** - select a type of command card to issue (*Enroll Card*, *Delete Card*, or *Delete All Card*).

5.1.2.9 Display/Sound tab

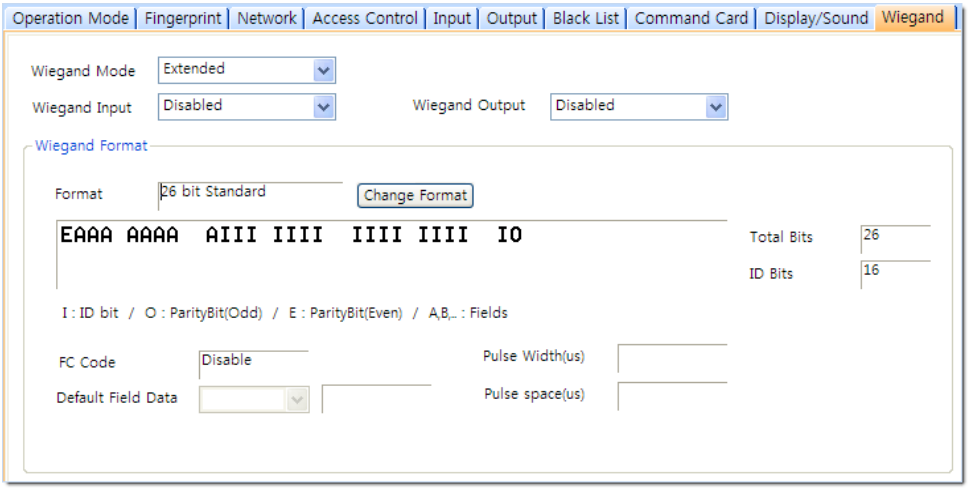
The Display/Sound tab allows you to customize the LED and buzzer behaviors by event. To save changes to these settings, you must click **Update** in the corresponding section for each event.



- **Event** - specify the affected event by selecting it from the drop-down list.
- **LED** - set the LED behavior for a specified event.
  - **Count** - enter a number of LED cycles for the specified event. Enter "0" to enable an infinite loop or "-1" to disable the LED.
  - **Colors** - specify up to three display colors from the drop-down list. The LED will cycle through these colors in order, from top to bottom. Next to each color, enter the duration (in milliseconds) that the LED should display the selected color and the duration (in milliseconds) that the LED should remain off before advancing to the next color in the cycle.
- **Buzzer** - set the buzzer behavior for a specified event.
  - **Count** - enter a number of buzzer cycles for the specified event. Enter "0" to enable an infinite loop or "-1" to disable the buzzer.
  - **Volume** - set up to three tone volumes from the drop-down list (*Low*, *Middle*, or *High*). The buzzer will cycle through these volumes in order, from top to bottom. Next to each volume, enter the duration (in milliseconds) that the buzzer should maintain the selected volume and the duration (in milliseconds) that the buzzer should remain off before advancing to the next volume in the cycle.
  - **Fade Out** - set the tone volume to fade out before advancing to the next volume in the cycle by clicking this checkbox.

5.1.2.10 Wiegand tab

The Wiegand tab allows you to configure the Wiegand format for a BioEntry Plus or BioEntry W device. Click **Change Format** to launch the Wiegand Configuration wizard. To activate the Wiegand feature for a BioEntry Plus or BioEntry W device, click the checkbox at the top right of the tab. For more information on configuring the Wiegand format, see section 3.2.12.



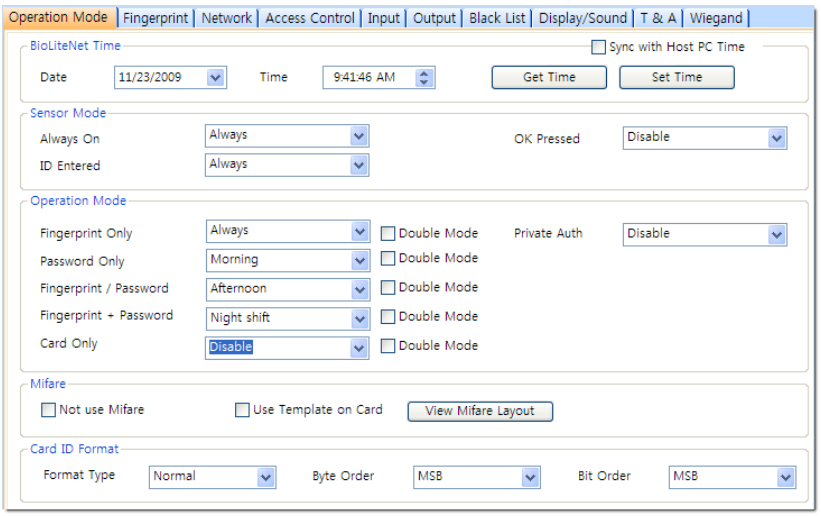
- **Wiegand Mode** - set the mode of Wiegand input to use when reading card ID data (*Legacy* or *Extended*). The Legacy mode will treat connected RF devices as part of their host devices (this is the typical function of previous versions of BioStar). The Extended mode will allow RF card readers to operate independently, which allows them to be associated with doors, included in zones, and leave logs with their own device IDs.
- **Wiegand Input** - assign the Wiegand input:
  - **Disabled** - the input will not be used.
  - **Wiegand [Card]** - the ID field of the Wiegand string is interpreted as a card ID.
  - **Wiegand [User]** - the ID field of the Wiegand string is interpreted as a user ID.
- **Wiegand Output** - assign the Wiegand output:
  - **Disabled** - the output will not be used.
  - **Wiegand [Card]** - inserts the card ID of the authenticated user in the ID field of the Wiegand string.
  - **Wiegand [User]** - inserts the user ID of the authenticated user in the ID field of the Wiegand string.

5.1.3 Customize Settings for BioLite Net Devices

The sections that follow describe the settings available for BioLite Net devices. Customize the way BioLite Net devices function by changing these settings to suit your particular environment and operational needs.

5.1.3.1 Operation Mode tab

The Operation Mode tab allows you to customize time and various operation modes settings for BioLite Net devices.



- **BioLiteNet Time**
  - **Date** - manually set the device date with a drop-down calendar.
  - **Time** - manually set the device time.
  - **Sync with Host PC Time** - check this box to automatically synchronize the device time with the time of the host computer.
  - **Get Time** - get the current time displayed by the device.
  - **Set Time** - set the time on the device.
- **Sensor Mode**
  - **Always On** - set the device sensor to be always available on standby (*Always* or *Disable*).
  - **ID Entered** - set the device sensor to be available on standby only after a valid ID is entered (*Always* or *Disable*).
  - **OK Pressed** - set the device sensor to be available on standby only after the OK key is pressed *(Always* or *Disable*).
- **Operation Mode** - for each of the following options, click the corresponding checkbox to enable Double Verification Mode, which requires verification of two users' credentials to gain entry to a door.

- **Fingerprint Only** - set the device to require fingerprint only authorization (*Always*, *Disable*, or Custom Schedule).
- **Password Only** - set the device to require password only authorization (*Always*, *Disable*, or Custom Schedule).
- **Fingerprint/Password** - set the device to require fingerprint or password authorization (*Always*, *Disable*, or Custom Schedule).
- **Fingerprint+Password** - set the device to require fingerprint plus password authorization (*Always*, *Disable*, or Custom Schedule).
- **Card Only** - set the device to require only card authorization (*Always*, *Disable*, or Custom Schedule).
- **Private Auth** - set the device to allow a private authorization method (*Disable* or *Enable*). If enabled, the authentication mode of the user will be determined by a user's "Authorization" setting, which is located on the Details tab. If disabled, the authentication mode will be determined by operation mode settings of the device.

• **Mifare**

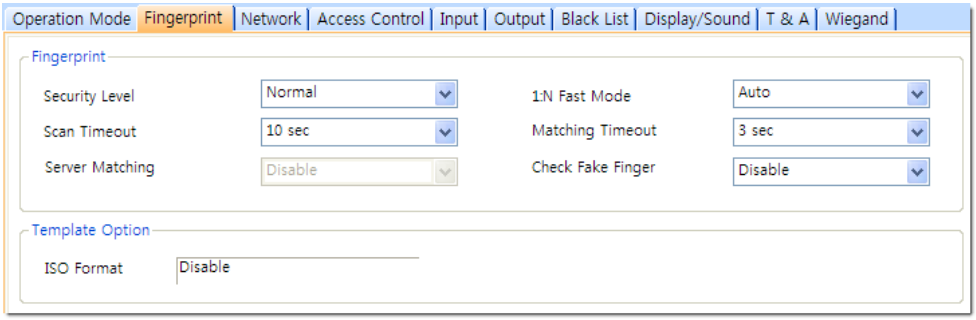
- **Not use Mifare** - check this box to disable MIFARE card authorization.
- **Use Template on Card** - check this box to use the template on the MIFARE card for authorization.
- **View Mifare Layout** - click this button to configure the MIFARE layout used by the device. For more information about configuring MIFARE layouts, see section 3.6.4.6.

• **Card ID Format**

- **Format Type** - set the type of pre-processing to occur on card ID data (*Normal* or *Wiegand*). If "Normal" is selected, the card ID data will processed in its original form. If "Wiegand" is selected, devices will interpret card ID data according to the Wiegand format settings.
- **Byte Order** - specify whether to swap ID card data between cards and devices by most significant byte (*MSB*) or least significant byte (*LSB*).
- **Bit Order** - specify whether to swap ID card data between cards and devices by most significant bit (*MSB*) or least significant bit (*LSB*).

5.1.3.2 Fingerprint tab

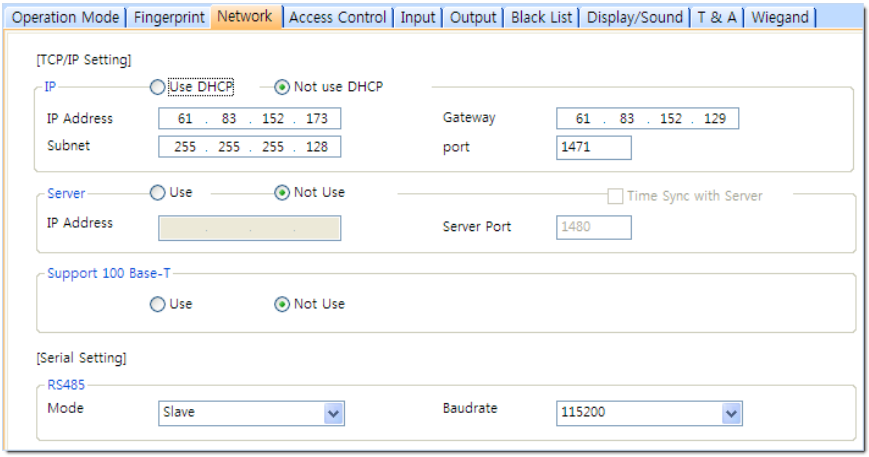
The Fingerprint tab allows you to customize fingerprint authorization settings for BioLite Net devices.



- **Fingerprint**
  - **Security Level** - set the security level to use for fingerprint authorization (*Normal*, *Secure*, or *Most Secure*). Keep in mind that as the security level is increased, so too is the likelihood of a false rejection.
  - **Scan Timeout** - set the length of time before the fingerprint scanner will timeout (*1 sec* to *20 sec*). If a user does not place a finger on the device within the timeout period, the authorization will fail.
  - **Server Matching** - enable this setting to perform fingerprint or card ID matching at the BioStar server, instead of the device. When this mode is enabled, the devices will send the fingerprint template or card ID to the server to verify a match. This mode is useful when you have more users than can be downloaded to a device or user information cannot be distributed due to security concerns.
  - **1:N Fast Mode** - set the device to use Fast Mode to reduce the amount of time required for matching fingerprints (*Auto*, *Normal*, *Fast*, or *Fastest*). Setting Fast Mode to *Auto* will adjust the matching speed according to the number of enrolled templates.
  - **Matching Timeout** - set the length of time before the device will timeout when trying to identify a fingerprint match (*0 [Infinite]* to *10 sec*).
  - **Check Fake Finger** – set the device to detect the use of fake fingerprints, such as those made from silicon or rubber, and prevent unauthorized access.

5.1.3.3 Network tab

The Network tab allows you to customize network and server settings for BioLite Net devices.

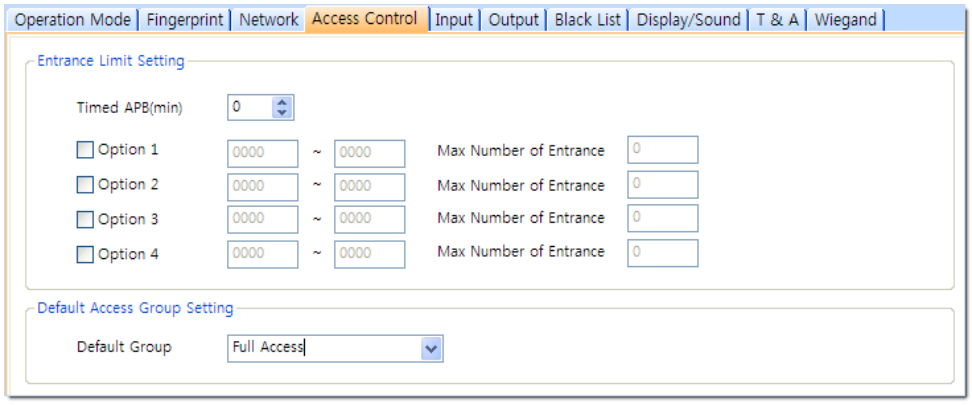


- **TCP/IP**
  - **Use DHCP** - click this radio button to enable the dynamic host configuration protocol (DHCP) for the device.
  - **Not Use DHCP** - click this radio button to disable the dynamic host configuration protocol (DHCP) for this device.
  - **IP Address** - specify an IP address for the device.
  - **Subnet** - specify a subnet address for the device.
  - **Gateway** - specify a network gateway.
  - **Port** - specify a port to use for the device.
- **Server**
  - **Use** - click this radio button to use specific server settings.
  - **Not use** - click this radio button to disable server settings.
  - **IP Address** - specify an IP address for the BioStar server.
  - **Time sync with Server** - check this box to synchronize the device time with the time maintained at the server.
- **Support 100 Base-T** - this option allows you to enable or disable a fast Ethernet connection for the device. When enabled, the device will detect the Ethernet network and automatically establish the best connection. If you do not enable this option, the device will attempt to establish a 10Base-T Ethernet connection.
  - **Use** - click this radio button to enable the 100base-T connection for the device.
  - **Not Use** - click this radio button to disable the 100base-T connection for the device.

- **RS485**
  - **Mode** - set the mode for a device connected via RS485 (*Disable*, *Host*, *Slave*, or *PC Connection*).
  - **Baudrate** - set the baud rate for a device connected via RS485 (*9600* to *115200*).

5.1.3.4 Access Control tab

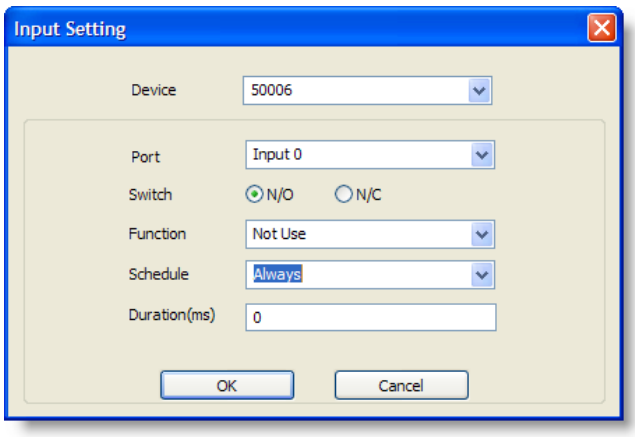
The Access Control tab allows you to customize entrance limit settings and default access groups for a BioLite Net device.



- **Entrance Limit Setting**
  - **Timed APB (min)** - set the duration (in minutes) that a user will be unable to regain entry to an area via the device. Once a user has gained entry, the device will reject the user's card or fingerprint authorization for the time period specified here.
  - **Option 1-4** - click the checkbox to enable an entrance limit setting, and then specify the effective hours for the entrance limit.
  - **Max Number of Entrance** - set the maximum number of entries allowed during the specified time limit.
- **Default Access Group Setting** - select a default access group to be applied to new users who have not been assigned to another access group.

5.1.3.5 Input tab

The input tab lists input settings you have specified for a BioLite Net device. Buttons at the bottom of the tab allow you to add, modify, or delete input settings. To add or modify settings, you must specify them from the Input Setting window. For more information about configuring input settings, see section 3.10.3.2.



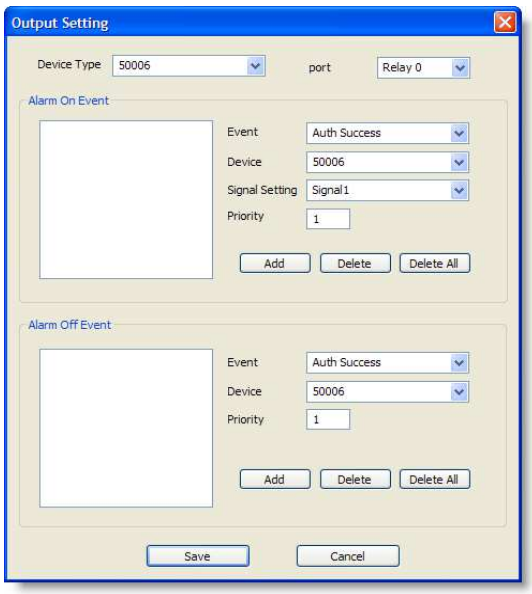
- **Device** - select the BioLite Net (or Secure I/O) device for which you will add or modify settings.
- **Port** - select an input port (*Input 0*, *Input 1*, or *Tamper*). For Secure I/O devices, these settings are available: *Input 0*, *Input 1*, *Input 2*, *Input 3*.
- **Switch** - click the radio buttons to specify the normal position of the input switch (*N/O* - *normally open* or *N/C* - normally *closed*).
- **Function** - select an action to associate with the input:
  - *Not Use* - the input port will not be monitored.
  - *Generic Input* - the input port will be monitored for a triggering action (events specified with “Detect Input 1-3” in the Output settings window—see section 5.1.3.6).
  - *Emergency Open* - open doors controlled by this device. The normal door open period will be ignored and doors will remain open until an operator sends a “Close Door” command via the Door/Zone Monitoring tab (see section 4.4.1).
  - *Release All Alarms* - cancel alarms associated with this device.
  - *Restart Device* - restart the device.
  - *Disable Device* - disable the device. A disabled device will not communicate with the BioStar server or process fingerprints or card inputs. To enable communication again, an administrator must

enter the master password for a BioStation device or provide authentication locally for a BioLite Net device.

- **Schedule** - set the schedule for the input actions (*Always*, *Disable*, or custom schedule).
- **Duration (ms)** - set the duration (in milliseconds) an input signal must last to trigger the specified action.

5.1.3.6 Output tab

The Output tab lists output settings you have specified for a BioLite Net device. Buttons at the bottom of the tab allow you to add, modify, or delete output settings. To add or modify settings, you must specify them from the Output Setting window. For more information about configuring output settings, see section 3.10.3.1.



- **Device Type** - select the device type for which you will add or modify settings.
- **Port** - select an output port (*Relay 0*). For Secure I/O devices, these settings are available: *Relay 0* or *Relay 1*.
- **Alarm On Event** - specify settings and click **Add** to add the event to the Alarm On Event list. These events will activate an alarm.
  - **Event** - select an event that will activate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input # 1-3*).
  - **Device** - select the device to monitor for an alarm event.

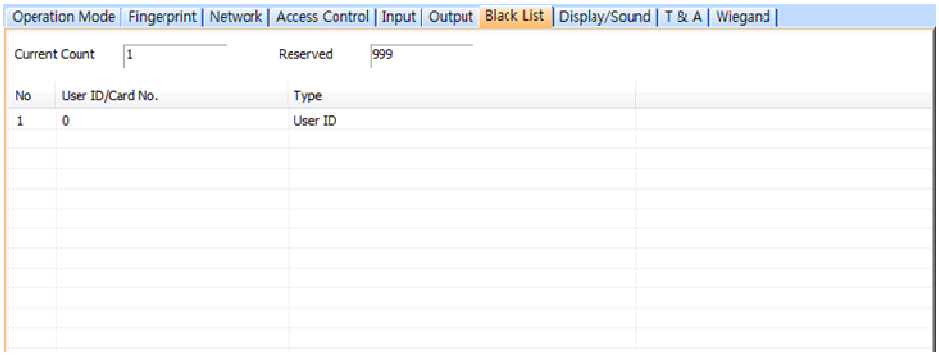
- **Signal Setting** - select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).
- **Priority** - set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on (activate) event with a priority of 2 can be canceled only by an alarm off (deactivate) event with a priority of 1 or 2.

• **Alarm Off Event** - specify settings and click **Add** to add the event to the Alarm Off Event list. These events will deactivate an alarm.

- **Event** - select an event that will deactivate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input # 1-3*).
- **Device** - select the device to monitor for an alarm event.
- **Priority** - set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on event (activate) can be overridden only by an alarm off (deactivate) event with a priority of 1 or 2.

5.1.3.7 Black List tab

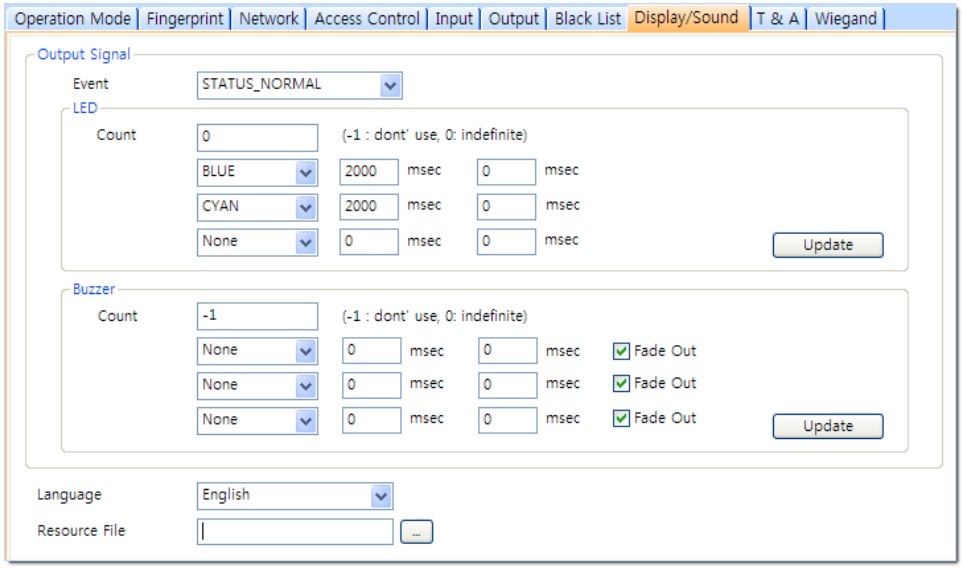
The Black List tab allows you to register user IDs or access card numbers and prevent them from being authenticated with the device.



- **Current Count** – indicates the total number of user IDs and access cards that have been registered.
- **Reserved** – indicates the remaining number of user IDs and access cards that can be registered.

5.1.3.8 Display/Sound tab

The Display/Sound tab allows you to customize LED and buzzer behaviors by event. To save changes to these settings, you must click **Update** in the corresponding section for each event. You can also customize the language used on the device display.



- **Event** - specify the affected event by selecting it from the drop-down list.
- **LED** - set the LED behavior for a specified event.
  - **Count** - enter a number of LED cycles for the specified event. Enter “0” to enable an infinite loop or “-1” to disable the LED.
  - **Colors** - specify up to three display colors from the drop-down list. The LED will cycle through these colors in order, from top to bottom. Next to each color, enter the duration (in milliseconds) that the LED should display the selected color and the duration (in milliseconds) that the LED should remain off before advancing to the next color in the cycle.
- **Buzzer** - set the buzzer behavior for a specified event.
  - **Count** - enter a number of buzzer cycles for the specified event. Enter “0” to enable an infinite loop or “-1” to disable the buzzer.
  - **Volume** - set up to three tone volumes from the drop-down list (*Low*, *Middle*, or *High*). The buzzer will cycle through these volumes in

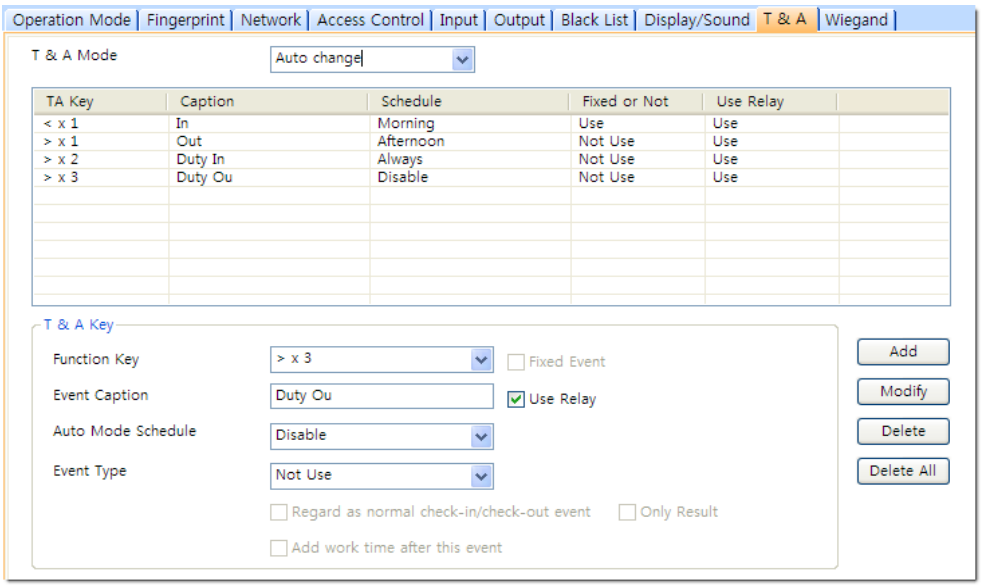
order, from top to bottom. Next to each volume, enter the duration (in milliseconds) that the buzzer should maintain the selected volume and the duration (in milliseconds) that the buzzer should remain off before advancing to the next volume in the cycle.

- **Fade Out** - set the tone volume to fade out before advancing to the next volume in the cycle by clicking this checkbox.

- **Language** - set the language to use on the display (*Korean*, *English*, or *Custom*).
- **Resource File** - set the language resource file to use for the BioStar interface by clicking the ellipsis (…) button and locating the resource file.

5.1.3.9 T&A tab

The T&A tab allows you to configure the mode and key settings for a BioLite Net device. To save changes to time and attendance settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.

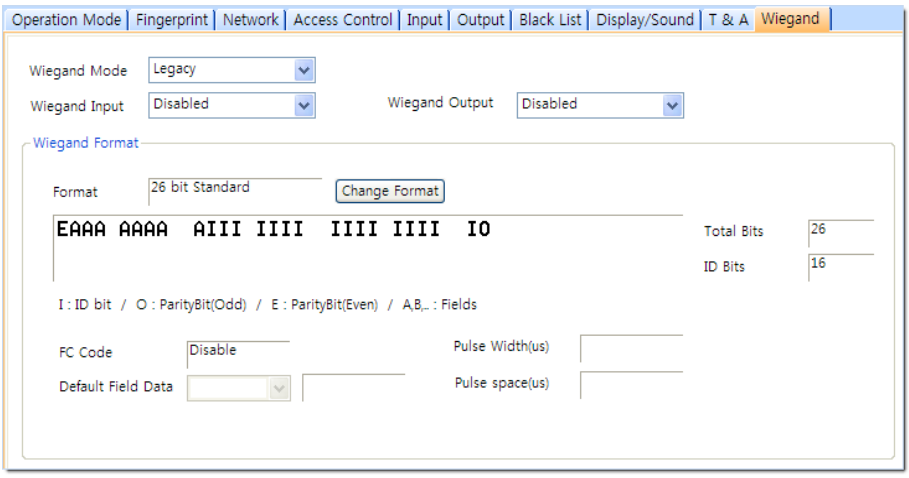


- **T&A Mode** - set the time and attendance mode:
  - **Not Use** - disable the time and attendance functions for this device.
  - **Manual** - users must press the specified key every time they enter or leave to record their T&A events.
  - **Manual Fix** - when a T&A key is pressed, the device will remain in that mode until a different T&A key is pressed.
  - **Auto change** - the device will automatically change T&A modes to correspond with the functions specified for a time period.
  - **Event Fix** - the device will perform only the specified T&A function.
- **T&A Key** - specify which keys to use for T&A events and the event types associated with them:
  - **Function Key** - select a function key from the drop-down list to assign a T&A event (**1-*15*). If you are using the Event Fix mode, you can click the checkbox to the right to designate a fixed event.
  - **Event Caption** - enter a caption for the event.
  - - **Auto Mode Schedule** - when using the Auto Change mode, you can specify when the event will occur by selecting a timezone in the drop-down list. For more information on creating a timezone, see section 3.7.1.

- **Event Type** - set the type of event to assign to the key (*Not Use*, *Check In*, *Check Out*, *In*, or *Out*). In/Out indicates the general check in/out events during a day whereas Check In/Out indicates the formal check in/out events upon arrival and departure at work—or the first check–in and the last check–out events on that day. When you choose Check In or Check Out, you can enable the "Regard as normal check-in/check-out event" option. If this option is enabled, users using the appropriate keys will be regarded arriving or leaving on time at work even though they actually come late or leave early. If you enable the "Only Result" option, they appear being on time on T&A reports but their work time will be calculated correctly based on their actual check in/out time. If you choose *Out*, you can enable the "Add work time after this event" option. If this option is enabled, users using the appropriate key will be considered working for the remainder of the time slot even though they leave the office early.

5.1.3.10 Wiegand tab

The Wiegand tab allows you to configure the Wiegand format for a BioLite Net device. Unlike BioStation devices, only one Wiegand format can be configured at a time (either input only or output only). Click **Change Format** to launch the Wiegand Configuration wizard. To activate the Wiegand feature for a BioLite Net device, click the checkbox at the top right of the tab. For more information on configuring the Wiegand format, see section 3.2.12.



- **Wiegand Mode** - set the mode of Wiegand input to use when reading card ID data (*Legacy* or Extended). The Legacy mode will process ID data from networked devices and RF card readers in the same way (this is the typical function of previous versions of BioStar). The

Extended mode will allow RF card readers to operate independently, which allows them to be associated with doors, included in zones, and leave logs with their own device IDs.

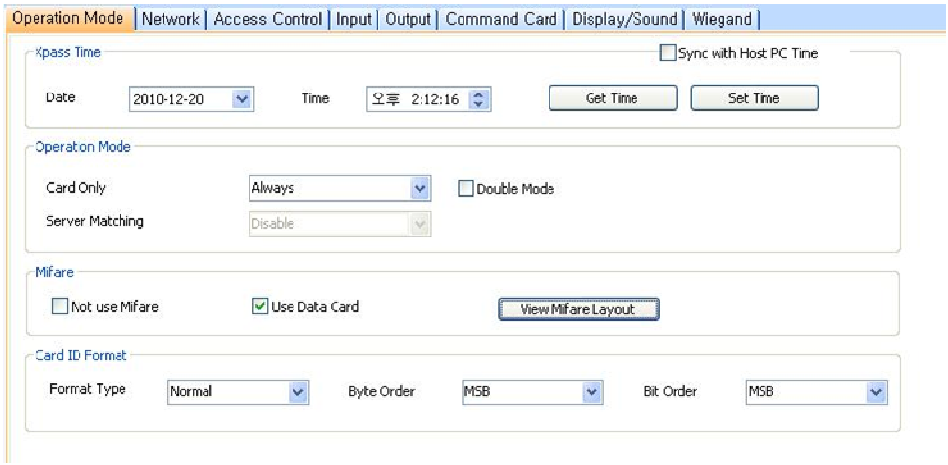
- **Wiegand Input** - assign the Wiegand input:
  - **Disabled** - the input will not be used.
  - **Wiegand [Card]** - the ID field of the Wiegand string is interpreted as a card ID.
  - **Wiegand [User]** - the ID field of the Wiegand string is interpreted as a user ID.
- **Wiegand Output** - assign the Wiegand output:
  - **Disabled** - the output will not be used.
  - **Wiegand [Card]** - inserts the card ID of the authenticated user in the ID field of the Wiegand string.
  - **Wiegand [User]** - inserts the user ID of the authenticated user in the ID field of the Wiegand string.

5.1.4 Customize Settings for Xpass Devices

The sections below describe the settings available for Xpass devices. Customize the way Xpass devices function by changing these settings to suit your particular environment and operational needs.

5.1.4.1 Operation Mode tab

The Operation Mode tab allows you to customize time and various operation modes settings for Xpass devices.



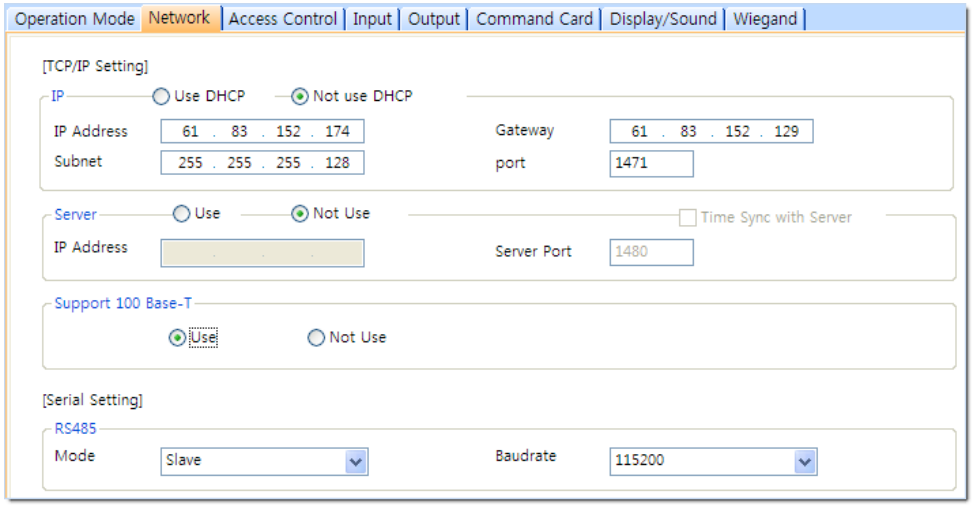
- **Xpass Time**
  - **Date** - manually set the device date with a drop-down calendar.
  - **Time** - manually set the device time.

- **Sync with Host PC Time** - check this box to automatically synchronize the device time with the time of the host computer.
- **Get Time** - get the current time displayed by the device.
- **Set Time** - set the time on the device.

- **Operation Mode** - for each of the following options, click the corresponding checkbox to enable Double Verification Mode, which requires verification of two users' credentials to gain entry to a door.
  - **Card Only** - set the device to require only card authorization (*Always*, *Disable*, or custom schedule).
  - **Server Matching** - enable this setting to perform card ID matching at the BioStar server, instead of the device. When this mode is enabled, the device will send card ID to the server to verify a match. This mode is useful when you have more users than can be downloaded to a device or user information cannot be distributed due to security concerns.
- **Mifare**
  - **Not use Mifare** - check this box to disable MIFARE card authorization.
  - **Use Data Card** - check this box to use the user data on the MIFARE card for authorization. The user data card does not provide fingerprint templates.
  - **View Mifare Layout** - click this button to view the MIFARE layout used by the device. For more information about configuring MIFARE layouts, see section 3.6.4.6.
- **Card ID Format**
  - **Format Type** - set the type of pre-processing to occur on card ID data (*Normal* or *Wiegand*). If "Normal" is selected, the card ID data will processed in its original form. If "Wiegand" is selected, devices will interpret card ID data according to the Wiegand format settings.
  - **Byte Order** - specify whether to swap ID card data between cards and devices by most significant byte (*MSB*) or least significant byte (*LSB*).
  - **Bit Order** - specify whether to swap ID card data between cards and devices by most significant bit (*MSB*) or least significant bit (*LSB*).

5.1.4.2 Network tab

The Network tab allows you to customize network and server settings for Xpass devices.



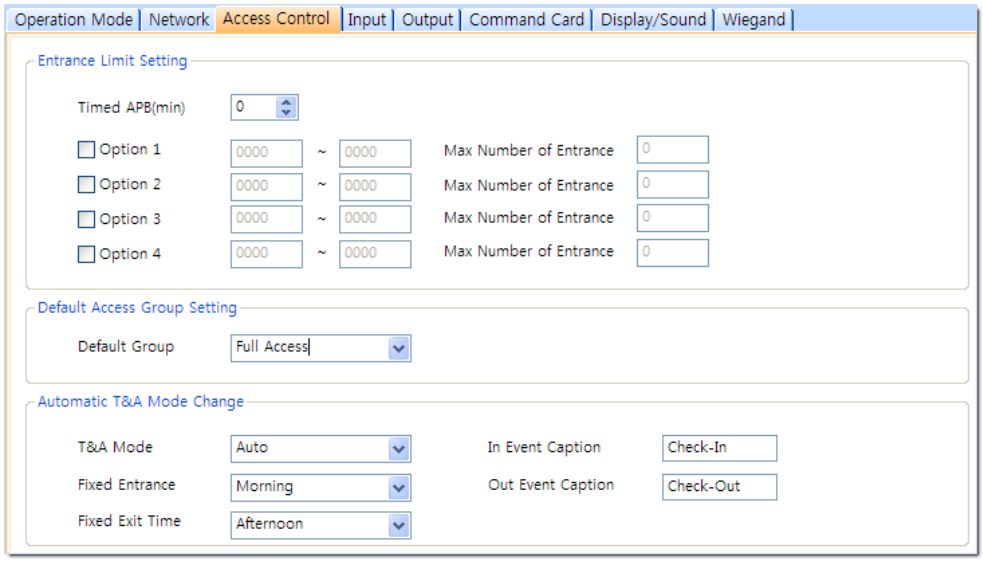
- **TCP/IP**
  - **Use DHCP** - click this radio button to enable the dynamic host configuration protocol (DHCP) for the device.
  - **Not Use DHCP** - click this radio button to disable the dynamic host configuration protocol (DHCP) for this device.
  - **IP Address** - specify an IP address for the device.
  - **Subnet** - specify a subnet address for the device.
  - **Gateway** - specify a network gateway.
  - **Port** - specify a port to use for the device.
- **Server**
  - **Use** - click this radio button to use specific server settings.
  - **Not use** - click this radio button to disable server settings.
  - **IP Address** - specify an IP address for the BioStar server.
  - **Time sync with Server** - check this box to synchronize the device time with the time maintained at the server.
- **Support 100 Base-T** - this option allows you to enable or disable a fast Ethernet connection for the device. When enabled, the device will detect the Ethernet network and automatically establish the best connection. If you do not enable this option, the device will attempt to establish a 10Base-T Ethernet connection.
  - **Use** - click this radio button to enable the 100base-T connection for the device.

- **Not Use** - click this radio button to disable the 100base-T connection for the device.

- **RS485**
  - **Mode** - set the mode for a device connected via RS485 (*Disable*, *Host*, *Slave*, or *PC Connection*).
  - **Baudrate** - set the baud rate for a device connected via RS485 (*9600* to *115200*).

5.1.4.3 Access Control tab

The Access Control tab allows you to customize entrance limit settings, default access groups, and T&A mode settings for Xpass devices.

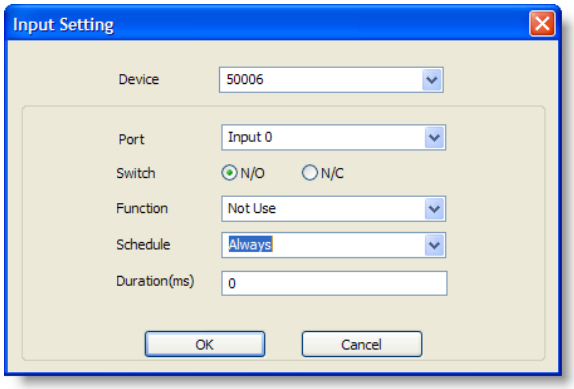


- **Entrance Limit Setting**
  - **Timed APB (min)** - set the duration (in minutes) that a user will be unable to regain entry to an area via the device. Once a user has gained entry, the device will reject the user's card or fingerprint authorization for the time period specified here.
  - **Option 1-4** - click the checkbox to enable an entrance limit setting, and then specify the effective hours for the entrance limit.
  - **Max Number of Entrance** - set the maximum number of entries allowed during the specified time limit.
- **Default Access Group Setting** - select a default access group to be applied to new users who have not been assigned to another access group.
- **Automatic T&A Mode Change**
  - **T&A Mode** - set the time and attendance mode for the device (*Disable*, *Fixed In*, *Fixed Out*, and *Auto*).

- **Fixed Entrance** - when the "Auto" T&A mode is selected, specify when to allow entrance events by selecting a timezone (*Always*, *Disable*, or custom timezone) in the drop-down list. For more information on creating a timezone, see section 3.7.1.
- **Fixed Exit Time** - when the "Auto" T&A mode is selected, specify when to allow exit events by selecting a timezone (*Always*, *Disable*, or custom timezone) in the drop-down list. For more information on creating a timezone, see section 3.7.1.
- **In Event Caption** - set a caption for check-in.
- **Out Event Caption** - set a caption for check-out.

5.1.4.4 Input tab

The input tab lists input settings you have specified for an Xpass device. Buttons at the bottom of the tab allow you to add, modify, or delete input settings. To add or modify settings, you must specify them from the Input Setting window. For more information about configuring input settings, see section 3.10.3.2.



- **Device** - select the Xpass (or Secure I/O) device for which you will add or modify settings.
- **Port** - select an input port (Input 0, Input 1, or Tamper). For Secure I/O devices, these settings are available: Input 0, Input 1, Input 2, Input 3.
- **Switch** - click the radio buttons to specify the normal position of the input switch (N/O - normally open or N/C - normally closed).
- **Function** - select an action to associate with the input:
  - **Not Use** - the input port will not be monitored.
  - **Generic Input** - the input port will be monitored for a triggering action (events specified with "Detect Input 1-3" in the Output settings window—see section 5.1.4.5).

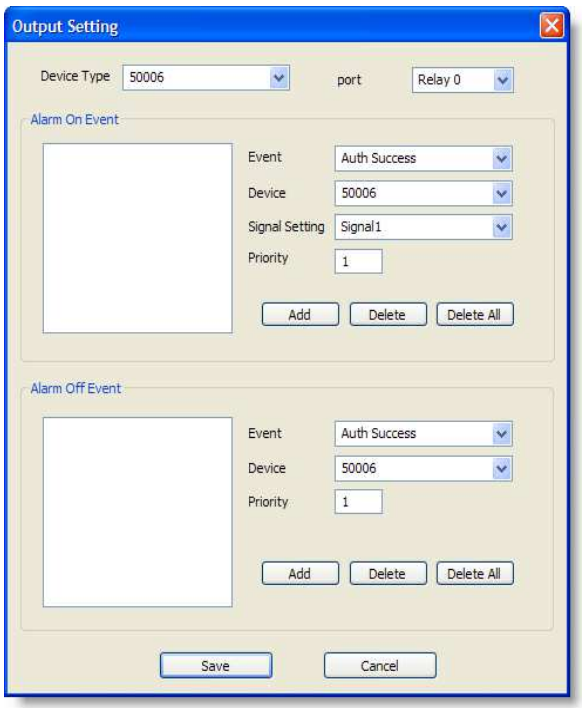
- **Emergency Open** - open doors controlled by this device. The normal door open period will be ignored and doors will remain open until an operator sends a “Close Door” command via the Door/Zone Monitoring tab (see section 4.4.1).
- **Release All Alarms** - cancel alarms associated with this device.
- **Restart Device** - restart the device.
- **Disable Device** - disable the device. A disabled device will not communicate with the BioStar server or process fingerprints or card inputs. To enable communication again, an administrator must enter the master password for a BioStation device or provide authentication locally for a BioEntry Plus or BioEntry W device.

• **Schedule** - set the schedule for the input actions (*Always*, *Disable*, or custom schedule).

• **Duration (ms)** - set the duration (in milliseconds) an input signal must last to trigger the specified action.

5.1.4.5 Output tab

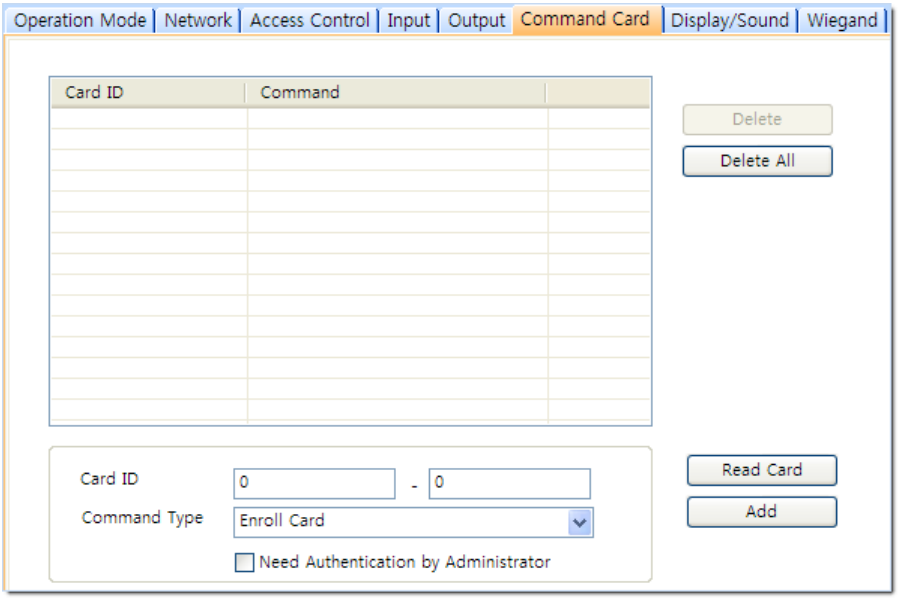
The Output tab lists output settings you have specified for an Xpass device. Buttons at the bottom of the tab allow you to add, modify, or delete output settings. To add or modify settings, you must specify them from the Output Setting window. For more information about configuring output settings, see section 3.10.3.1.



- **Device Type** - select the device type for which you will add or modify settings.
- **Port** - select an output port (*Relay 0*). For Secure I/O devices, these settings are available: *Relay 0* or *Relay 1*.
- **Alarm On Event** - specify settings and click **Add** to add the event to the Alarm On Event list. These events will activate an alarm.
  - **Event** - select an event that will activate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input # 1-3*).
  - **Device** - select the device to monitor for an alarm event.
  - **Signal Setting** - select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).
  - **Priority** - set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on (activate) event with a priority of 2 can be canceled only by an alarm off (deactivate) event with a priority of 1 or 2.
- **Alarm Off Event** - specify settings and click **Add** to add the event to the Alarm Off Event list. These events will deactivate an alarm.
  - **Event** - select an event that will deactivate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input # 1-3*).
  - **Device** - select the device to monitor for an alarm event.
  - **Priority** - set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on event (activate) can be overridden only by an alarm off (deactivate) event with a priority of 1 or 2.

5.1.4.6 Command Card tab

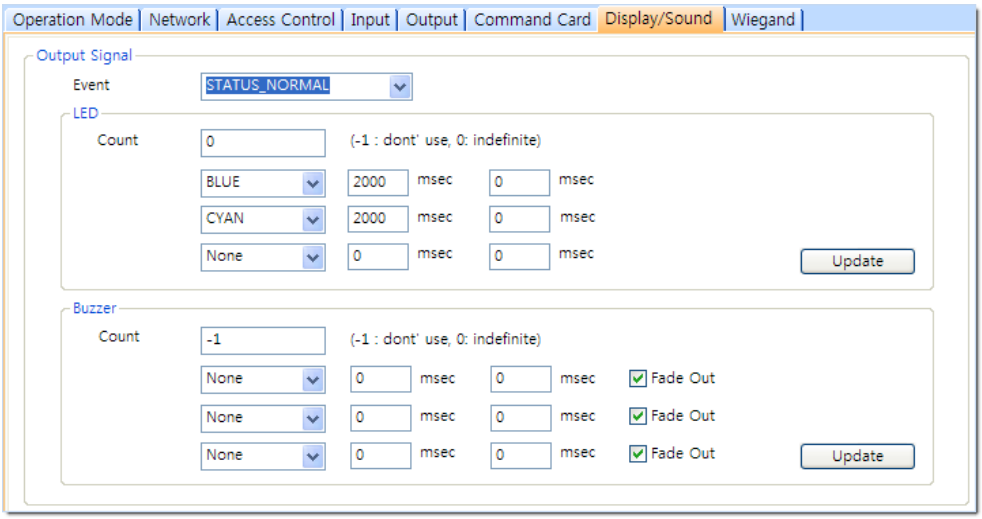
The Command Card tab allows you to issue command cards. For more information about command cards, see section 3.2.7.1.



- **Card ID** - enter the card ID or click **Read Card** and place a command card on the reader to automatically populate the fields.
- **Command Type** - select a type of command card to issue (*Enroll Card*, *Delete Card*, or *Delete All Card*).

5.1.4.7 Display/Sound tab

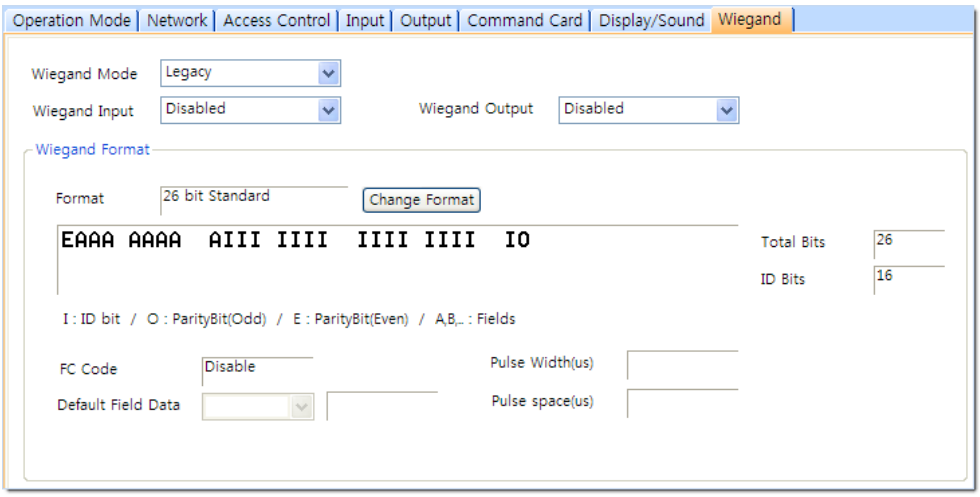
The Display/Sound tab allows you to customize LED and buzzer behaviors by event. To save changes to these settings, you must click **Update** in the corresponding section for each event.



- **Event** - specify the affected event by selecting it from the drop-down list.
- **LED** - set the LED behavior for a specified event.
  - **Count** - enter a number of LED cycles for the specified event. Enter "0" to enable an infinite loop or "-1" to disable the LED.
  - **Colors** - specify up to three display colors from the drop-down list. The LED will cycle through these colors in order, from top to bottom. Next to each color, enter the duration (in milliseconds) that the LED should display the selected color and the duration (in milliseconds) that the LED should remain off before advancing to the next color in the cycle.
- **Buzzer** - set the buzzer behavior for a specified event.
  - **Count** - enter a number of buzzer cycles for the specified event. Enter "0" to enable an infinite loop or "-1" to disable the buzzer.
  - **Volume** - set up to three tone volumes from the drop-down list (*Low*, *Middle*, or *High*). The buzzer will cycle through these volumes in order, from top to bottom. Next to each volume, enter the duration (in milliseconds) that the buzzer should maintain the selected volume and the duration (in milliseconds) that the buzzer should remain off before advancing to the next volume in the cycle.
  - **Fade Out** - set the tone volume to fade out before advancing to the next volume in the cycle by clicking this checkbox.

5.1.4.8 Wiegand tab

The Wiegand tab allows you to configure the Wiegand format for an Xpass device. Click **Change Format** to launch the Wiegand Configuration wizard. To activate the Wiegand feature for an Xpass device, click the checkbox at the top right of the tab. For more information on configuring the Wiegand format, see section 3.2.12



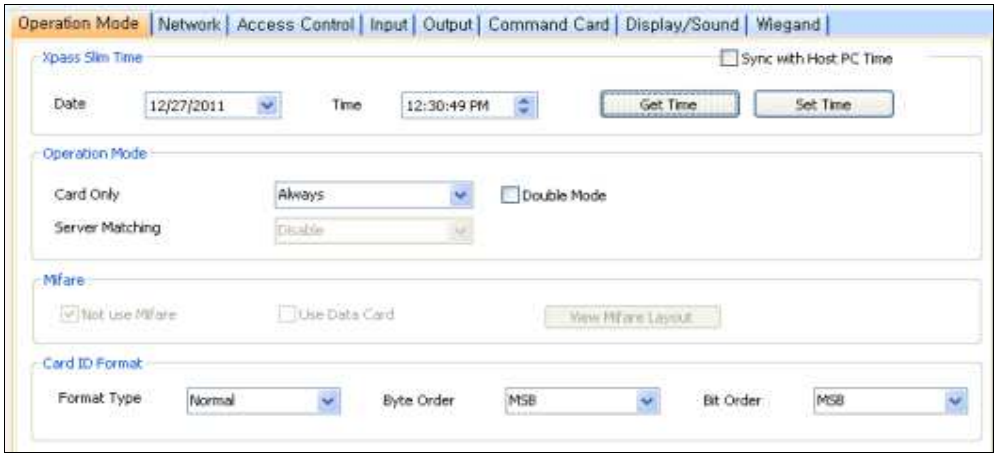
- **Wiegand Mode** - set the mode of Wiegand input to use when reading card ID data (*Legacy* or *Extended*). The Legacy mode will treat connected RF devices as part of their host devices (this is the typical function of previous versions of BioStar). The Extended mode will allow RF card readers to operate independently, which allows them to be associated with doors, included in zones, and leave logs with their own device IDs.
- **Wiegand Input** - assign the Wiegand input:
  - **Disabled** - the input will not be used.
  - **Wiegand [Card]** - the ID field of the Wiegand string is interpreted as a card ID.
  - **Wiegand [User]** - the ID field of the Wiegand string is interpreted as a user ID.
- **Wiegand Output** - assign the Wiegand output:
  - **Disabled** - the output will not be used.
  - **Wiegand [Card]** - inserts the card ID of the authenticated user in the ID field of the Wiegand string.
  - **Wiegand [User]** - inserts the user ID of the authenticated user in the ID field of the Wiegand string.

5.1.5 Customize Settings for Xpass Slim Devices

The sections below describe the settings available for Xpass Slim devices. Customize the way Xpass Slim devices function by changing these settings to suit your particular environment and operational needs.

5.1.5.1 Operation Mode tab

The Operation Mode tab allows you to customize time and various operation modes settings for Xpass Slim devices.

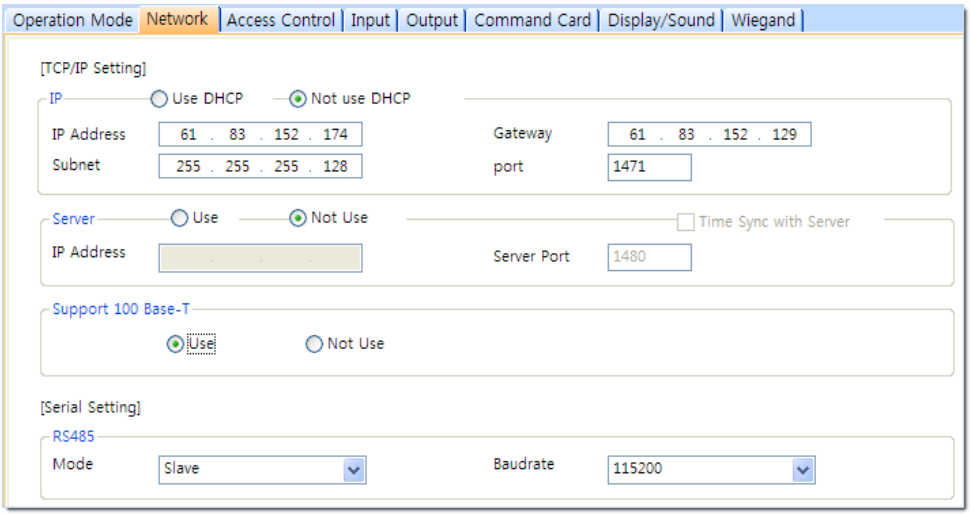


- **Xpass Slim Time**
  - **Date** - manually set the device date with a drop-down calendar.
  - **Time** - manually set the device time.
  - **Sync with Host PC Time** - check this box to automatically synchronize the device time with the time of the host computer.
  - **Get Time** - get the current time displayed by the device.
  - **Set Time** - set the time on the device.
- **Operation Mode** - for each of the following options, click the corresponding checkbox to enable Double Verification Mode, which requires verification of two users' credentials to gain entry to a door.
  - **Card Only** - set the device to require only card authorization (*Always*, *Disable*, or custom schedule).
  - **Server Matching** - enable this setting to perform card ID matching at the BioStar server, instead of the device. When this mode is enabled, the device will send card ID to the server to verify a match. This mode is useful when you have more users than can be downloaded to a device or user information cannot be distributed due to security concerns.
- **Mifare**: Mifare template cards are not supported in the Xpass slim device.

- **Card ID Format**
  - **Format Type** - set the type of pre-processing to occur on card ID data (*Normal* or *Wiegand*). If “Normal” is selected, the card ID data will processed in its original form. If “Wiegand” is selected, devices will interpret card ID data according to the Wiegand format settings.
  - **Byte Order** - specify whether to swap ID card data between cards and devices by most significant byte (*MSB*) or least significant byte (*LSB*).
  - **Bit Order** - specify whether to swap ID card data between cards and devices by most significant bit (*MSB*) or least significant bit (*LSB*).

5.1.5.2 Network tab

The Network tab allows you to customize network and server settings for Xpass Slim devices.



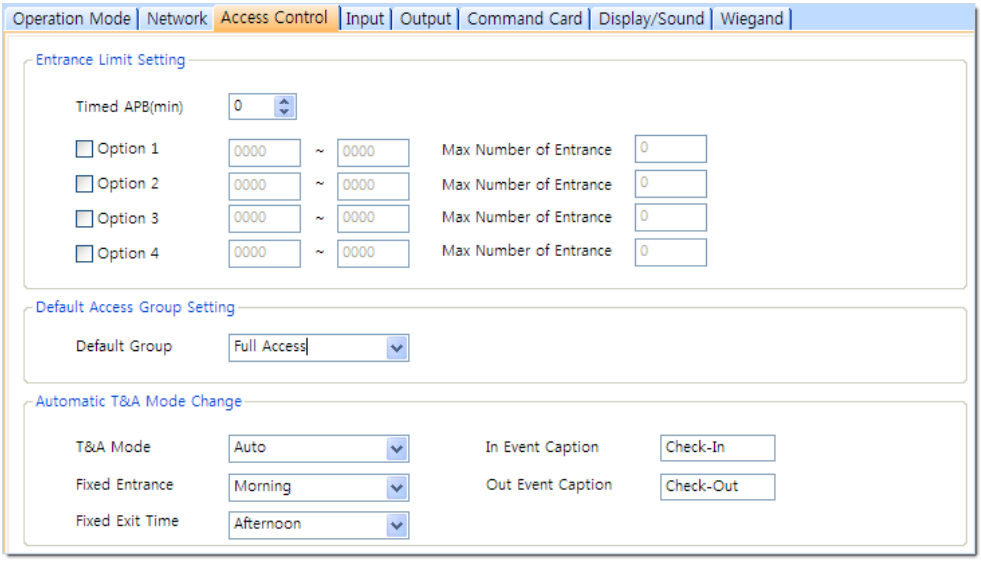
- **TCP/IP**
  - **Use DHCP** - click this radio button to enable the dynamic host configuration protocol (DHCP) for the device.
  - **Not Use DHCP** - click this radio button to disable the dynamic host configuration protocol (DHCP) for this device.
  - **IP** - specify an IP address for the device.
  - **Subnet** - specify a subnet address for the device.
  - **Gateway** - specify a network gateway.
  - **Port** - specify a port to use for the device.
- **Server**
  - **Use** - click this radio button to use specific server settings.
  - **Not use** - click this radio button to disable server settings.

- **IP Address** - specify an IP address for the BioStar server.
- **Time sync with Server** - check this box to synchronize the device time with the time maintained at the server.

- **Support 100 Base-T** - this option allows you to enable or disable a fast Ethernet connection for the device. When enabled, the device will detect the Ethernet network and automatically establish the best connection. If you do not enable this option, the device will attempt to establish a 10Base-T Ethernet connection.
  - **Use** - click this radio button to enable the 100base-T connection for the device.
  - **Not Use** - click this radio button to disable the 100base-T connection for the device.
- **RS485**
  - **Mode** - set the mode for a device connected via RS485 (*Disable*, *Host*, *Slave*, or *PC Connection*).
  - **Baudrate** - set the baud rate for a device connected via RS485 (*9600* to *115200*).

5.1.5.3 Access Control tab

The Access Control tab allows you to customize entrance limit settings, default access groups, and T&A mode settings for Xpass Slim devices.



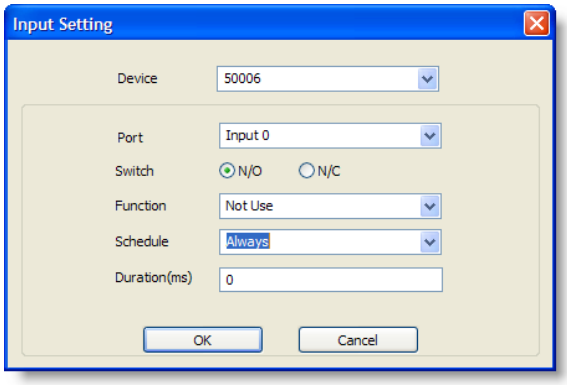
- **Entrance Limit Setting**
  - **Timed APB (min)** - set the duration (in minutes) that a user will be unable to regain entry to an area via the device. Once a user has gained entry, the device will reject the user's card or fingerprint authorization for the time period specified here.

- **Option 1-4** - click the checkbox to enable an entrance limit setting, and then specify the effective hours for the entrance limit.
- **Max Number of Entrance** - set the maximum number of entries allowed during the specified time limit.

- **Default Access Group Setting** - select a default access group to be applied to new users who have not been assigned to another access group.
- **Automatic T&A Mode Change**
  - **T&A Mode** - set the time and attendance mode for the device (*Disable*, *Fixed In*, *Fixed Out*, and *Auto*).
  - **Fixed Entrance** - when the "Auto" T&A mode is selected, specify when to allow entrance events by selecting a timezone (*Always*, *Disable*, or custom timezone) in the drop-down list. For more information on creating a timezone, see section 3.7.1.
  - **Fixed Exit Time** - when the "Auto" T&A mode is selected, specify when to allow exit events by selecting a timezone (*Always*, *Disable*, or custom timezone) in the drop-down list. For more information on creating a timezone, see section 3.7.1.
  - **In Event Caption** - set a caption for check-in.
  - **Out Event Caption** - set a caption for check-out.

5.1.5.4 Input tab

The input tab lists input settings you have specified for an Xpass Slim device. Buttons at the bottom of the tab allow you to add, modify, or delete input settings. To add or modify settings, you must specify them from the Input Setting window. For more information about configuring input settings, see section 3.10.3.2.



- **Device** - select the Xpass Slim (or Secure I/O) device for which you will add or modify settings.

- **Port** - select an input port (Input 0, Input 1, or Tamper). For Secure I/O or LIFT I/O devices, these settings are available: Input 0, Input 1, Input 2, Input 3.
- **Switch** - click the radio buttons to specify the normal position of the input switch (N/O - normally open or N/C - normally closed).
- **Function** - select an action to associate with the input:
  - **Not Use** - the input port will not be monitored.
  - **Generic Input** - the input port will be monitored for a triggering action (events specified with "Detect Input 1-3" in the Output settings window—see section 5.1.5.5).
  - **Emergency Open** - open doors controlled by this device. The normal door open period will be ignored and doors will remain open until an operator sends a "Close Door" command via the Door/Zone Monitoring tab (see section 4.4.1).
  - **Release All Alarms** - cancel alarms associated with this device.
  - **Restart Device** - restart the device.
  - **Disable Device** - disable the device. A disabled device will not communicate with the BioStar server or process fingerprints or card inputs. To enable communication again, an administrator must enter the master password for a BioStation device or provide authentication locally for a BioEntry Plus or BioEntry W device.
- **Schedule** - set the schedule for the input actions (*Always*, *Disable*, or custom schedule).
- **Duration (ms)** - set the duration (in milliseconds) an input signal must last to trigger the specified action.

5.1.5.5 Output tab

The Output tab lists output settings you have specified for an Xpass device. Buttons at the bottom of the tab allow you to add, modify, or delete output settings. To add or modify settings, you must specify them from the Output Setting window. For more information about configuring output settings, see section 3.10.3.1.

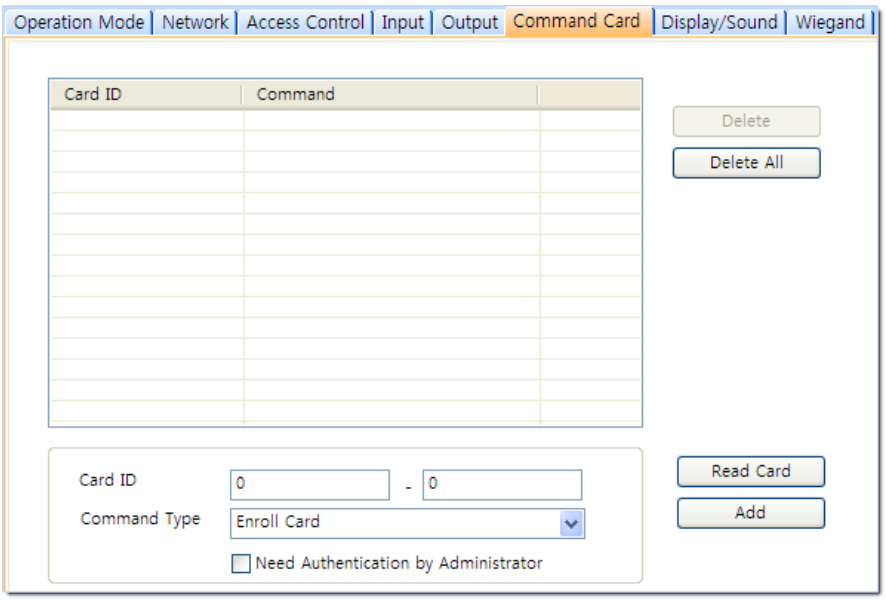
- **Device Type** - select the device type for which you will add or modify settings.
- **Port** - select an output port (*Relay 0*). For Secure I/O devices, these settings are available: *Relay 0* or *Relay 1*.
- **Alarm On Event** - specify settings and click **Add** to add the event to the Alarm On Event list. These events will activate an alarm.
  - **Event** - select an event that will activate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input # 1-3*).
  - **Device** - select the device to monitor for an alarm event.
  - **Signal Setting** - select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).

- **Priority** - set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on (activate) event with a priority of 2 can be canceled only by an alarm off (deactivate) event with a priority of 1 or 2.

- **Alarm Off Event** - specify settings and click **Add** to add the event to the Alarm Off Event list. These events will deactivate an alarm.
  - **Event** - select an event that will deactivate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input # 1-3*).
  - **Device** - select the device to monitor for an alarm event.
  - **Priority** - set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on event (activate) can be overridden only by an alarm off (deactivate) event with a priority of 1 or 2.

5.1.5.6 Command Card tab

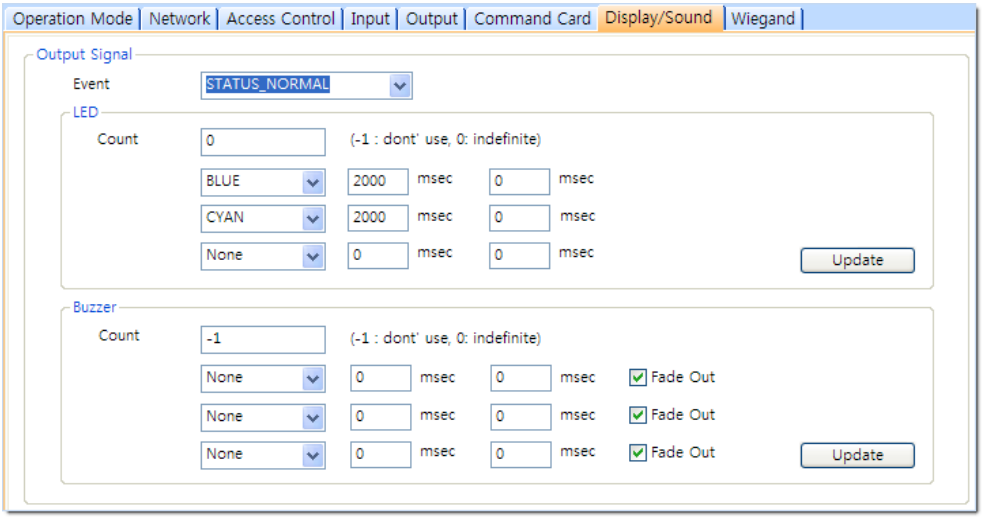
The Command Card tab allows you to issue command cards. For more information about command cards, see section 3.2.7.1.



- **Card ID** - enter the card ID or click **Read Card** and place a command card on the reader to automatically populate the fields.
- **Command Type** - select a type of command card to issue (*Enroll Card*, *Delete Card*, or *Delete All Card*).

5.1.5.7 Display/Sound tab

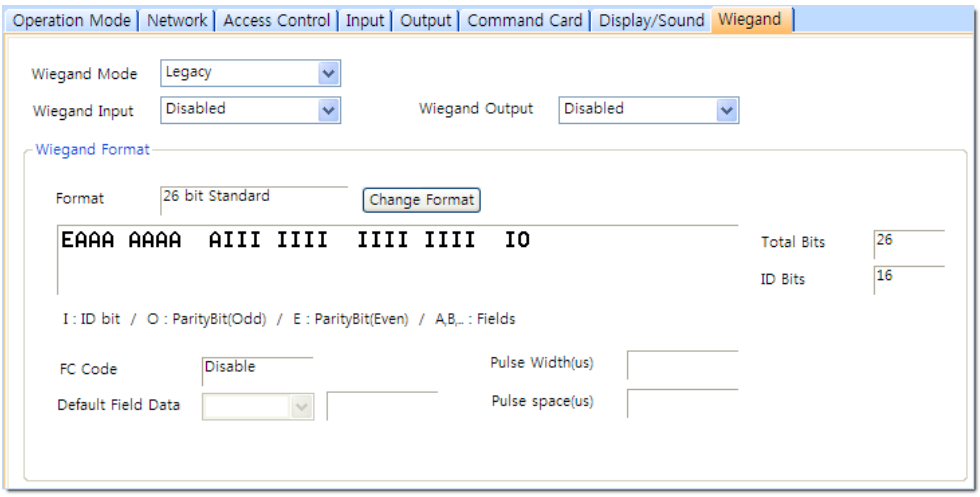
The Display/Sound tab allows you to customize LED and buzzer behaviors by event. To save changes to these settings, you must click **Update** in the corresponding section for each event.



- **Event** - specify the affected event by selecting it from the drop-down list.
- **LED** - set the LED behavior for a specified event.
  - **Count** - enter a number of LED cycles for the specified event. Enter “0” to enable an infinite loop or “-1” to disable the LED.
  - **Colors** - specify up to three display colors from the drop-down list. The LED will cycle through these colors in order, from top to bottom. Next to each color, enter the duration (in milliseconds) that the LED should display the selected color and the duration (in milliseconds) that the LED should remain off before advancing to the next color in the cycle.
- **Buzzer** - set the buzzer behavior for a specified event.
  - **Count** - enter a number of buzzer cycles for the specified event. Enter “0” to enable an infinite loop or “-1” to disable the buzzer.
  - **Volume** - set up to three tone volumes from the drop-down list (*Low*, *Middle*, or *High*). The buzzer will cycle through these volumes in order, from top to bottom. Next to each volume, enter the duration (in milliseconds) that the buzzer should maintain the selected volume and the duration (in milliseconds) that the buzzer should remain off before advancing to the next volume in the cycle.
  - **Fade Out** - set the tone volume to fade out before advancing to the next volume in the cycle by clicking this checkbox.

5.1.5.8 Wiegand tab

The Wiegand tab allows you to configure the Wiegand format for an Xpass device. Click **Change Format** to launch the Wiegand Configuration wizard. To activate the Wiegand feature for an Xpass device, click the checkbox at the top right of the tab. For more information on configuring the Wiegand format, see section 3.2.12.



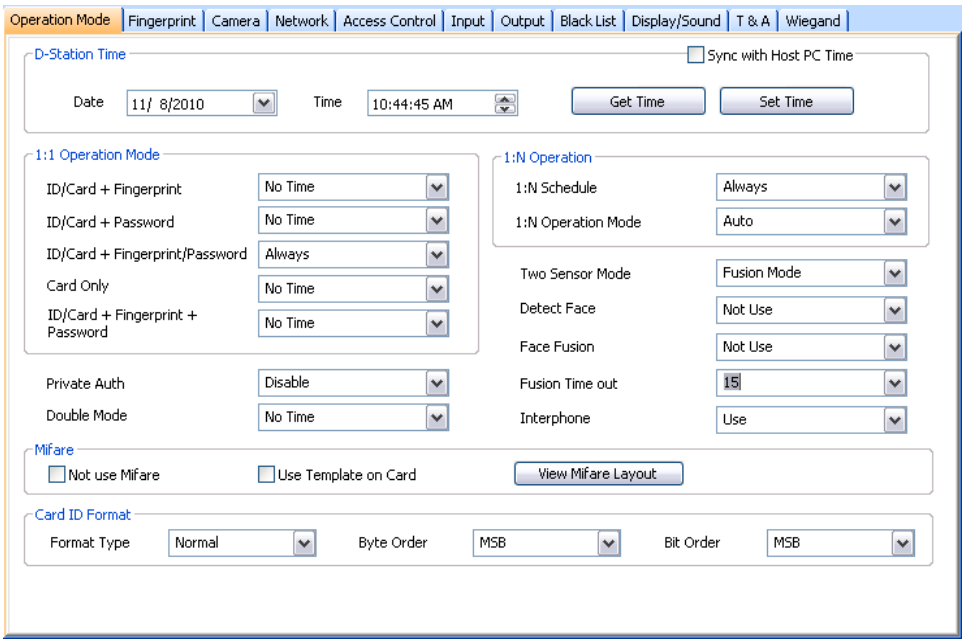
- **Wiegand Mode** - set the mode of Wiegand input to use when reading card ID data (*Legacy* or *Extended*). The Legacy mode will treat connected RF devices as part of their host devices (this is the typical function of previous versions of BioStar). The Extended mode will allow RF card readers to operate independently, which allows them to be associated with doors, included in zones, and leave logs with their own device IDs.
- **Wiegand Input** - assign the Wiegand input:
  - **Disabled** - the input will not be used.
  - **Wiegand [Card]** - the ID field of the Wiegand string is interpreted as a card ID.
  - **Wiegand [User]** - the ID field of the Wiegand string is interpreted as a user ID.
- **Wiegand Output** - assign the Wiegand output:
  - **Disabled** - the output will not be used.
  - **Wiegand [Card]** - inserts the card ID of the authenticated user in the ID field of the Wiegand string.
  - **Wiegand [User]** - inserts the user ID of the authenticated user in the ID field of the Wiegand string.

5.1.6 Customize Settings for D-Station Devices

The sections below describe the settings available for D-Station devices. Customize the way D-Station devices function by changing these settings to suit your particular environment and operational needs.

5.1.6.1 Operation Mode tab

The Operation Mode tab allows you to customize time and various operation modes settings for D-Station devices.



- **D-Station Time**
  - **Date** - manually set the device date with a drop-down calendar.
  - **Time** - manually set the device time.
  - **Sync with Host PC Time** - check this box to automatically synchronize the device time with the time of the host computer.
  - **Get Time** - get the current time displayed by the device.
  - **Set Time** - set the time on the device.
- **1:1 Operation Mode** - the drop-down lists in this area allow you to control the authentication mode by schedule. For example, you can choose a normal authentication mode for working hours and a more strict authentication mode for hours outside the normal schedule. You can specify authentication modes either by device or by user (see section 5.4.1). Unless a particular mode is specified for a user, the device authentication mode will apply.

- **ID/Card + Fingerprint** - set the device to require ID or card plus fingerprint authorization (*Always*, or *No Time*).
- **ID/Card + Password** - set the device to require ID or card plus password authorization (*Always*, or *No Time*).
- **ID/Card + Fingerprint/Password** - set the device to require ID or card plus fingerprint or password authorization (*Always*, or *No Time*).
- **Card Only** - set the device to require only card authorization (*Always*, or *No Time*).
- **ID/Card + Fingerprint + Password** - set the device to require ID or card plus fingerprint plus password authorization (*Always*, or *No Time*).

• **1:N Operation**
- **1:N Schedule** - set a schedule for using fingerprint only authentication (*Always*, or *No Time*).
- **1:N Operation Mode** - set a method for activating the fingerprint sensor (*Auto*, *Ok/Function Key*, or *None*).

• **Two Sensor Mode**
- **Fast Mode** – The device will provide the quickest authentication.
- **Fusion Mode** – Authentication is provided by a fusion algorithm that allowes users to scan either of two registered fingers and increases the authentication rate for each finger.
- **Twin Mode** – Each sensor works independently to authenticate up to two users simultaneously.

• **Detect Face**
- set the device to capture a face image. Upon successful authentication, the captured image is stored in the event log and can be used later for verification purposes.

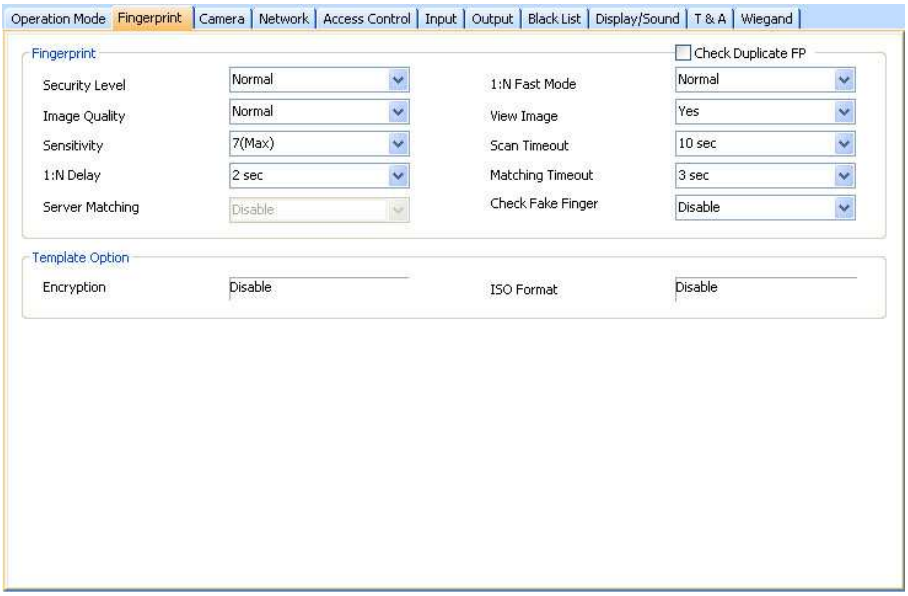
• **Face Fusion**
- set the device to use face fusion for authentication. This setting can improve authentication rates for some users. This setting can be used in conjunction with either the Fast Mode or the Fusion Mode in the Two Sensor Mode setting.

• **Fusion Time out**
- set the device to automatically time out after a specified number of minutes, if authentication is unsuccessful (1-20).

- **Interphone** - set the device to act as an interphone to allow communication between people on either side of the door (*Not Use* or *Use*).
- **Other options**
  - **Private Auth** - set the device to allow a private authorization method (*Disable* or *Enable*). If enabled, the authentication mode of the user will be determined by a user's "Authorization" setting, which is located on the Details tab. If disabled, the authentication mode will be determined by operation mode settings of the device.
  - **Double Mode** - set the device to require authentication of two users' access cards or fingerprints (*Always*, or *No Time*). The timeout for presenting the second authentication is 15 seconds.
- **Mifare**
  - **Not use Mifare** - check this box to disable MIFARE card authorization.
  - **Use Template on Card** - check this box to use the template on the MIFARE card for authorization.
  - **View Mifare Layout** - click this button to view the MIFARE layout used by the device. For more information about configuring MIFARE layouts, see section 3.6.4.6.
- **ISO Format**
  - **Format Type** - set the type of pre-processing to occur on card ID data (*Normal* or *Wiegand*). If "Normal" is selected, the card ID data will processed in its original form. If "Wiegand" is selected, devices will interpret card ID data according to the Wiegand format settings.
  - **Byte Order** - specify whether to swap ID card data between cards and devices by most significant byte (*MSB*) or least significant byte (*LSB*).
  - **Bit Order** - specify whether to swap ID card data between cards and devices by most significant bit (*MSB*) or least significant bit (*LSB*).

5.1.6.2 Fingerprint tab

The Fingerprint tab allows you to customize fingerprint authorization settings for D-Station devices.



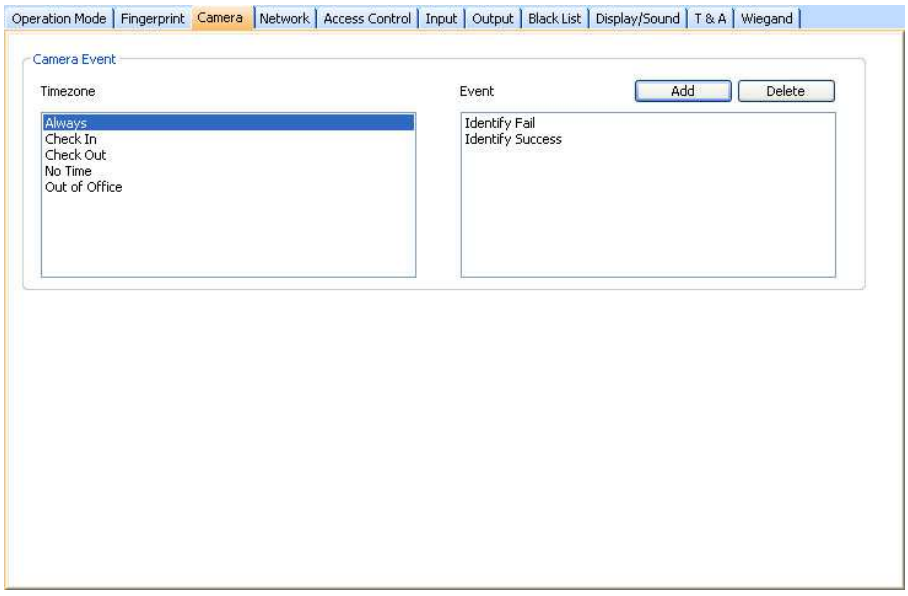
- **Fingerprint**
  - **Security Level** - set the security level to use for fingerprint authorization (*Normal*, *Secure*, or *Most Secure*). Keep in mind that as the security level is increased, so too is the likelihood of a false rejection.
  - **Image Quality** - set the strictness of the quality check for fingerprint scans (*Weak*, *Normal*, or *Strict*). If a fingerprint image is below the specified quality level, it will be rejected.
  - **Sensitivity** - set the sensitivity of the fingerprint scanner (*0 [Min]* to *7 [Max]*). A higher sensitivity setting will result in more easily captured fingerprint scans, but also increases the sensitivity to external noise.
  - **1:N Delay** - set the delay between scans when identifying fingerprints (*0 sec* to *10 sec*). This delay prevents the scanner from processing the same fingerprint more than once if a user has not yet removed his or her finger from the scanner.
  - **Server Matching** - enable this setting to perform fingerprint or card ID matching at the BioStar server, instead of the device. When this mode is enabled, the devices will send the fingerprint template or card ID to the server to verify a match. This mode is useful when

you have more users than can be downloaded to a device or user information cannot be distributed due to security concerns.

- **1:N Fast Mode** - set the device to use Fast Mode to reduce the amount of time required for matching fingerprints (*Auto*, *Normal*, *Fast*, or *Fastest*). Setting Fast Mode to *Auto* will adjust the matching speed according to the number of enrolled templates.
- **View Image** - set to show or hide fingerprint images on the BioStation display (*Yes* or *No*).
- **Scan Timeout** - set the length of time before the fingerprint scanner will timeout (*1 sec* to *20 sec*). If a user does not place a finger on the device within the timeout period, the authorization will fail.
- **Matching Timeout** - set the length of time before the device will timeout when trying to identify a fingerprint match (*0 [Infinite]* to *10 sec*).
- **Check Fake Finger** - set the device to detect the use of fake fingerprints, such as those made from silicon or rubber, and prevent unauthorized access.
- **Template Option** - displays the global fingerprint template settings. For more information about fingerprint templates, see section 4.9.

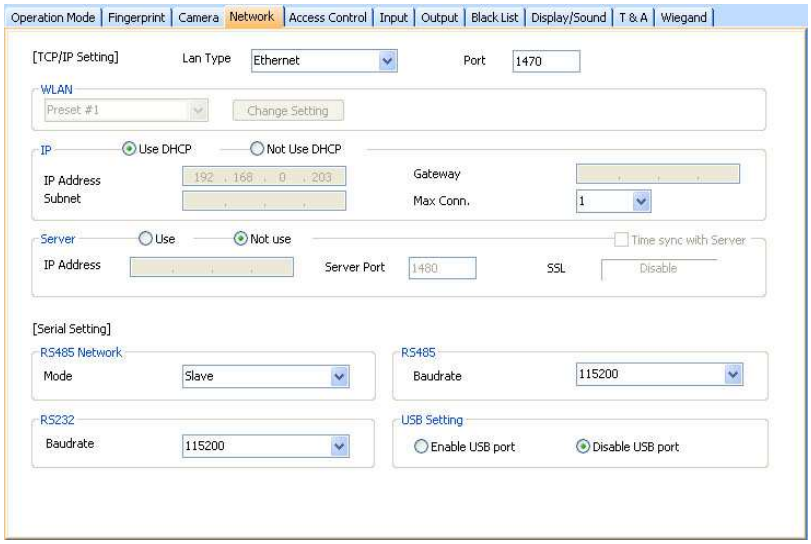
5.1.6.3 Camera tab

The Camera tab allows you to control how the camera is used for authorization purposes. In the Timezone field, select a timezone for the specified event. Click **Add** to select an event that will activate the camera. Click **Apply** to save your settings.



5.1.6.4 Network tab

The Network tab allows you to customize network and server settings for D-Station devices.



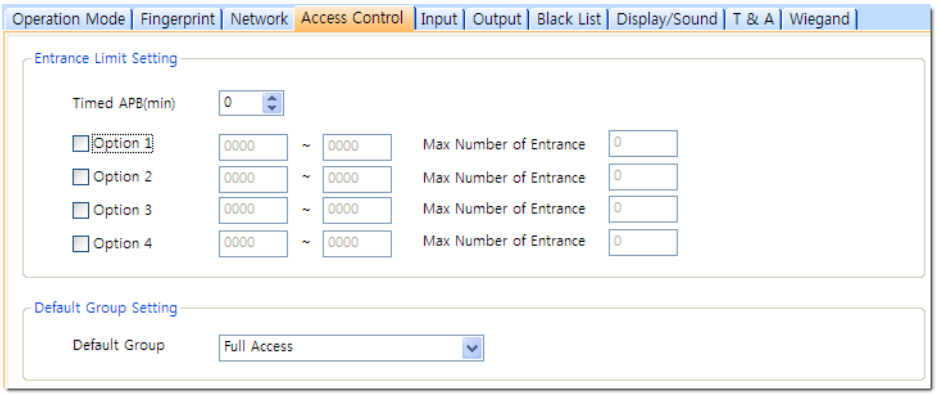
- **TCP/IP Setting**
  - **LAN Type -** select a type of LAN connection from the drop-down list (*Disable*, *Ethernet*, or *Wireless LAN*).
  - **Port** - specify a port to use for the device.
- **WLAN**
  - **Change setting** - click to specify settings for a wireless local area network (WLAN). This option is active only when WLAN is selected as the TCP/IP setting. For more information about configuring settings for a WLAN, see section 3.2.4.1.
- **IP**
  - **Use DHCP** - click this radio button to enable the dynamic host configuration protocol (DHCP) for the device.
  - **Not Use DHCP** - click this radio button to disable the dynamic host configuration protocol (DHCP) for this device.
  - **IP Address** - specify an IP address for the device.
  - **Subnet** - specify a subnet address for the device.
  - **Gateway** - specify a network gateway.
  - **Max Conn.** - specify the maximum number of connections to allow.
- **Server**
  - **Use** - click this radio button to enable the server mode.
  - **Not use** - click this radio button do disable server settings.
  - **IP Address** - specify an IP address for the BioStar server.

- **Server Port** - specify the port used to connect to the server.
- **SSL** - displays the status of SSL for the server connection.
- **Time sync with Server** - check this box to synchronize the device time with the time maintained at the server.

- **RS485 Network**
  - **Mode** - set the mode for a device connected via RS485 (*Disable*, *Host*, or *Slave*). For more information about RS485 modes, see sections 3.2.1 and 3.2.2.
- **RS485**
  - **Baudrate** - set the baud rate for a device connected via RS485 (*9600* to *115200*).
- **RS232**
  - **Baudrate** - set the baud rate for a device connected via RS232 (*9600* to *115200*).
- **USB Setting** - click the radio buttons to enable or disable the USB port on the D-Station device.

5.1.6.5 Access Control tab

The Access Control tab allows you to customize entrance limit settings and default access groups for a D-Station device.

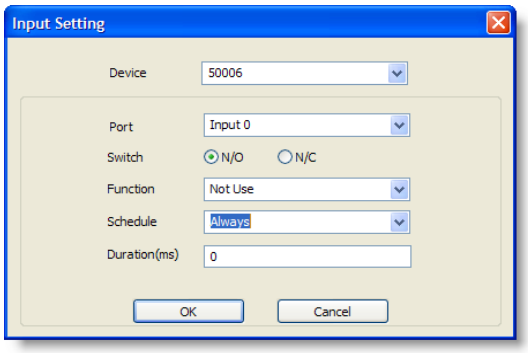


- **Entrance Limit Setting**
  - **Timed APB (min)** - set the duration (in minutes) that a user will be unable to regain entry to an area via the device. Once a user has gained entry, the device will reject the user's card or fingerprint authorization for the time period specified here.
  - **Option 1-4** - click the checkbox to enable an entrance limit setting, and then specify the effective hours for the entrance limit.
  - **Max Number of Entrance** - set the maximum number of entries allowed during the specified time limit.

- **Default Group Setting** - select a default access group to be applied to new users who have not been assigned to another access group.

5.1.6.6 Input tab

The input tab lists input settings you have specified for a D-Station device. Buttons at the bottom of the tab allow you to add, modify, or delete input settings. To add or modify settings, you must specify them from the Input Setting window. For more information about configuring input settings, see section 3.10.3.2.



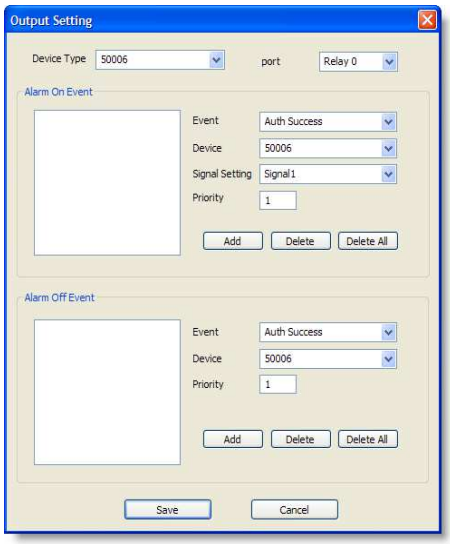
- **Device** - select the D-Station device for which you will add or modify settings.
- **Port** - select an input port (Input 0, Input 1, or Tamper). For Secure I/O devices, these settings are available: Input 0, Input 1, Input 2, Input 3.
- **Switch** - click the radio buttons to specify the normal position of the input switch (N/O - normally open or N/C - normally closed).
- **Function** - select an action to associate with the input:
  - **Not Use** - the input port will not be monitored.
  - **Generic Input** - the input port will be monitored for a triggering action (events specified with “Detect Input 0-3” in the Output settings window—see section 5.1.1.6).
  - **Emergency Open** - open doors controlled by this device. The normal door open period will be ignored and doors will remain open until an operator sends a “Close Door” command via the Door/Zone Monitoring tab (see section 4.4.1).
  - **Release All Alarms** - cancel alarms associated with this device.
  - **Restart Device** - restart the device.
  - **Disable Device** - disable the device. A disabled device will not communicate with the BioStar server or process fingerprints or card

inputs. To enable communication again, an administrator must provide authentication at the device.

- **Schedule** - set the schedule during which the inputs will be monitored (*Always* or *No Time*).
- **Duration (ms)** - set the duration (in milliseconds) an input signal must last to trigger the specified action.

5.1.6.7 Output tab

The Output tab lists output settings you have specified for a D-Station device. Buttons at the bottom of the tab allow you to add, modify, or delete output settings. To add or modify settings, you must specify them from the Output Setting window. For more information about configuring output settings, see section 3.10.3.1.



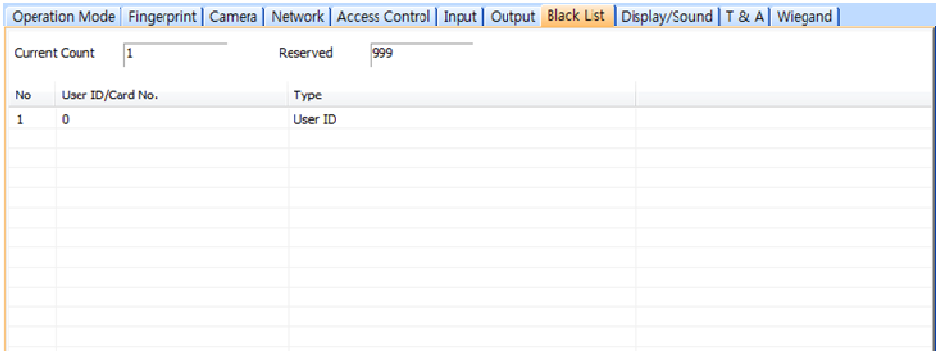
- **Device Type** - select the device type for which you will add or modify settings.
- **Port** - select an output port (Relay 0). For Secure I/O devices, these settings are available: Relay 0 or Relay 1.
- **Alarm On Event** - specify settings and click **Add** to add the event to the Alarm On Event list. These events will activate an alarm.
  - **Event** - select an event that will activate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, *Detect Input # 1-3*).
  - **Device** - select the device to monitor for an alarm event.

- **Signal Setting** - select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).
- **Priority** - set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on (activate) event with a priority of 2 can be canceled only by an alarm off (deactivate) event with a priority of 1 or 2.

- **Alarm Off Event** - specify settings and click **Add** to add the event to the Alarm Off Event list. These events will deactivate an alarm.
  - **Event** - select an event that will deactivate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input # 1-3*).
  - **Device** - select the device to monitor for an alarm event.
- **Priority** - set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, a priority 2 “alarm on” event (activate) can be overridden only by an “alarm off” (deactivate) event with a priority of 1 or 2.

5.1.6.8 Black List tab

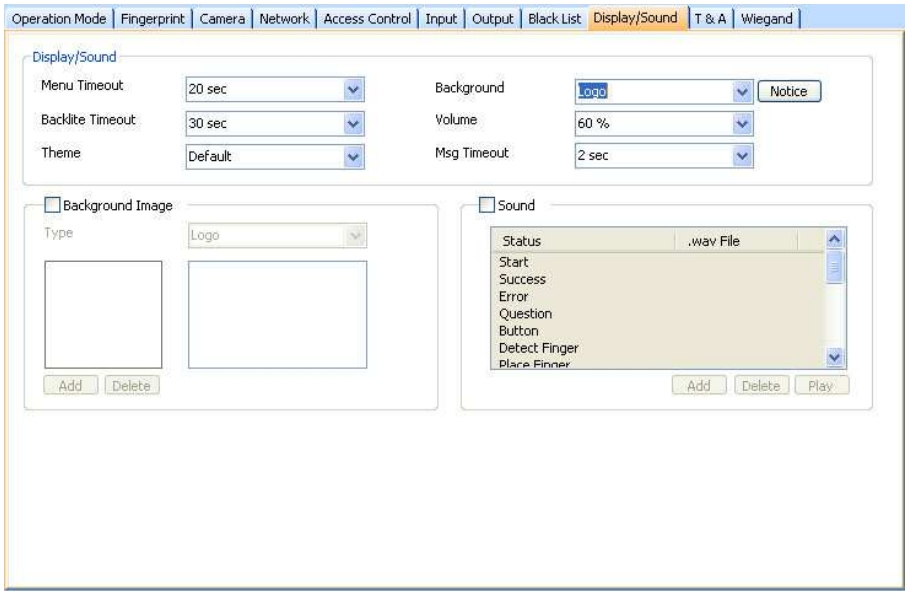
The Black List tab allows you to register user IDs or access card numbers and prevent them from being authenticated with the device.



- **Current Count** – indicates the total number of user IDs and access cards that have been registered.
- **Reserved** – indicates the remaining number of user IDs and access cards that can be registered.

5.1.6.9 Display/Sound tab

The Display/Sound tab allows you to customize the D-Station display and event sounds. To save changes to display or sound settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.



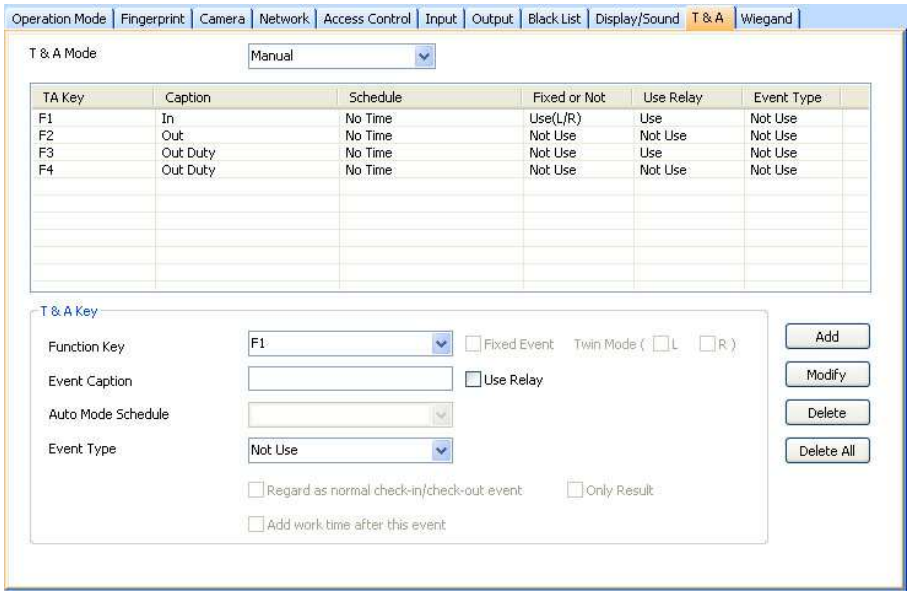
- **Display/Sound**
  - **Menu Timeout** - set the length of time before the display will return to the idle screen.
  - **Backlight Timeout** – set the length of time before the display goes dim.
  - **Theme** - set a display theme.
  - **Background** - set the type of background for the BioStation display (*Logo*, *Notice*, or *Slide Show*). Supported file types (JPG, GIF, BMP, and PNG) cannot exceed 320x240 pixels each. Only one image at a time can be used as a logo or notice, while up to 16 images can be displayed (at a set interval) in a slide show.
  - **Notice** - click this button to create a notice that will be shown on the BioStation display. After creating a notice, you can click **Apply** to apply the notice to the current device or **Apply to Others** to apply the notice to additional devices.
  - **Volume** - set the volume of the BioStation device (*10%* to *100%*).
  - **Msg Timeout** - set the length of time that a failure or confirmation message will be displayed.
- **Background Image** - click this checkbox to upload new background images. Click the plus sign (+) to locate and add a new image file.

- **Type** - set the type of background for the BioStation display (*Logo* or *Notice*). Supported file types (JPG, GIF, BMP, and PNG) cannot exceed 800x427 pixels for Notices and 800x327 pixels for Logos. Only one image at a time can be used as a logo or notice.

- **Sound** - click this checkbox to enable and add custom event sounds. Click an event from the list and then click the plus sign (+) to locate and add a new sound file. Click **Add** to add new sound files, **Delete** to remove sound files, or **Play** to preview a selected sound file.

5.1.6.10 T&A tab

The T&A tab allows you to configure the mode and key settings for a D-Station device. To save changes to time and attendance settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.

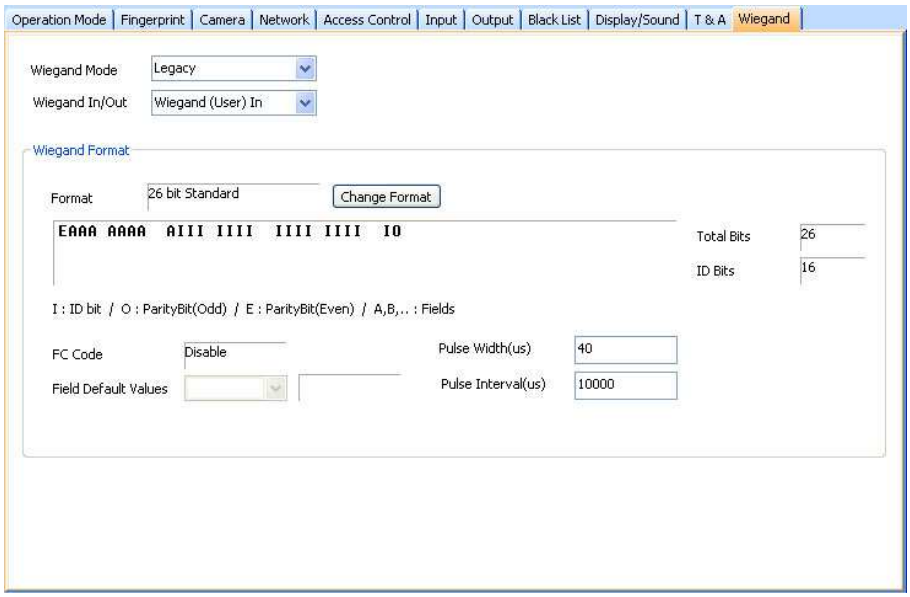


- **T&A Mode** - set the time and attendance mode:
  - **Not Use** - disable the time and attendance functions for this device.
  - **Manual** - users must press the specified key every time they enter or leave to record their T&A events.
  - **Manual Fix** - when a T&A key is pressed, the device will remain in that mode until a different T&A key is pressed.
  - **Auto change** - the device will automatically change T&A modes to correspond with the functions specified for a time period.
  - **Event Fix** - the device will perform only the specified T&A function. In this mode, each sensor can work independently. You can set an event for each sensor.

- **T&A Key** - specify which keys to use for T&A events and the event types associated with them:
  - **Function Key** - select a function key from the drop-down list to assign a T&A event (*F1-F4*, *EXT01-EXT12)*. If you are using the Event Fix mode, you can click the checkbox to the right to designate a fixed event.
  - **Event Caption** - enter a caption for the event.
  - **Auto Mode Schedule** - when using the Auto Change mode, you can specify when the event will occur by selecting a timezone in the drop-down list. For more information on creating a timezone, see section 3.6.1.
  - **Event Type** - set the type of event to assign to the key (*Not Use*, *Check In*, *Check Out*, *In*, or *Out*). In/Out indicates the general check in/out events during a day whereas Check In/Out indicates the formal check in/out events upon arrival and departure at work—or the first check–in and the last check–out events on that day. When you choose Check In or Check Out, you can enable the "Regard as normal check-in/check-out event" option. If this option is enabled, users who activate the appropriate keys will be regarded as arriving or leaving on time at work even though they actually arrive late or leave early. If you enable the "Only Result" option, they appear being on time on T&A reports but their work time will be calculated correctly based on their actual check in/out time. If you choose *Out*, you can enable the "Add work time after this event" option. If this option is enabled, users activating the appropriate key will be considered working for the remainder of the time slot even if they leave the office early.

5.1.6.11 Wiegand tab

The Wiegand tab allows you to configure the Wiegand format for a D-Station device. Click **Change Format** to launch the Wiegand Configuration wizard. For more information on configuring the Wiegand format, see section 3.2.12.



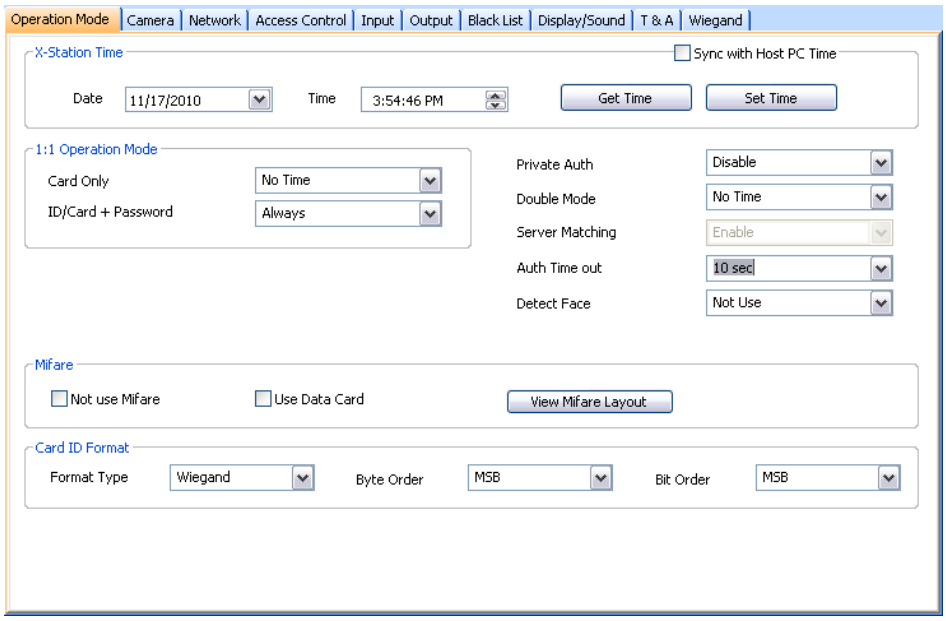
- **Wiegand Mode** - set the mode of Wiegand input to use when reading card ID data (*Legacy* or *Extended*). The Legacy mode will treat connected RF devices as part of their host devices (this is the typical function of previous versions of BioStar). The Extended mode will allow RF card readers to operate independently, which allows them to be associated with doors, included in zones, and leave logs with their own device IDs.
- **Wiegand In/Out** - assign the Wiegand input or output:
  - **Wiegand (User) In** - the ID field of the Wiegand string is interpreted as a user ID.
  - **Wiegand (Card) In** - the ID field of the Wiegand string is interpreted as a card ID.
  - **Wiegand (User) Out** - inserts the user ID of the authenticated user in the ID field of the Wiegand string.
  - **Wiegand (Card) Out** - inserts the card ID of the authenticated user in the ID field of the Wiegand string.

5.1.7 Customize Settings for X-Station Devices

The sections below describe the settings available for X-Station devices. Customize the way X-Station devices function by changing these settings to suit your particular environment and operational needs.

5.1.7.1 Operation Mode tab

The Operation Mode tab allows you to customize time and various operation modes settings for X-Station devices.

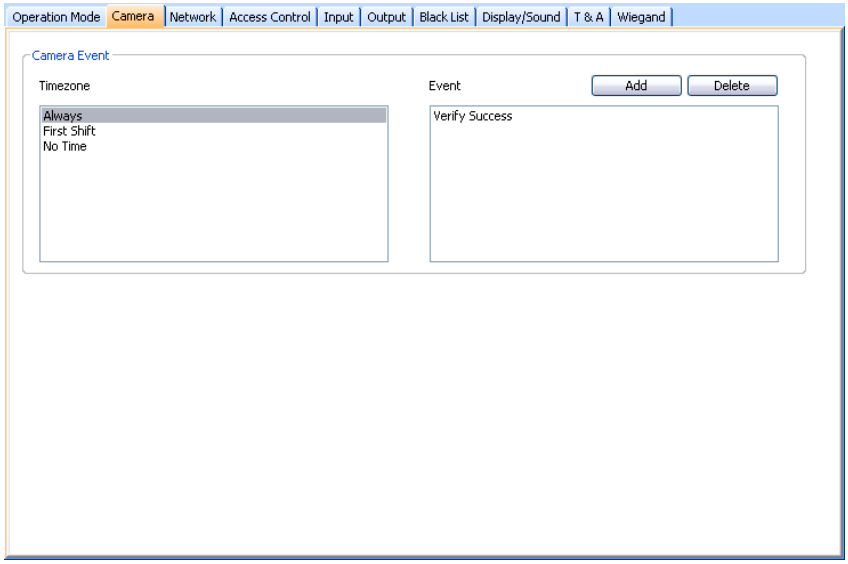


- **X-Station Time**
  - **Date** - manually set the device date with a drop-down calendar.
  - **Time** - manually set the device time.
  - **Sync with Host PC Time** - check this box to automatically synchronize the device time with the time of the host computer.
  - **Get Time** - get the current time displayed by the device.
  - **Set Time** - set the time on the device.
- **1:1 Operation Mode** - the drop-down lists in this area allow you to control the authentication mode by schedule. For example, you can choose a normal authentication mode for working hours and a more strict authentication mode for hours outside the normal schedule. You can specify authentication modes either by device or by user (see section 5.4.1). Unless a particular mode is specified for a user, the device authentication mode will apply.
  - **Card Only** - set the device to require only card authorization (*No Time*, *First Shift*, or *Always*).

  - **ID/Card + Password** - set the device to require ID or card plus password authorization (*No Time*, *First Shift*, or *Always*).
- **Private Auth** - set the device to allow a private authorization method (*Disable* or *Enable*). If enabled, the authentication mode of the user will be determined by a user's "Authorization" setting, which is located on the Details tab. If disabled, the authentication mode will be determined by operation mode settings of the device.
- **Double Mode** - set the device to require authentication of two users' access cards or fingerprints (*Always*, or *No Time*). The timeout for presenting the second authentication is 15 seconds.
- **Server Matching** - enable this setting to perform card ID matching at the BioStar server, instead of the device. When this mode is enabled, the device will send card ID to the server to verify a match. This mode is useful when you have more users than can be downloaded to a device or user information cannot be distributed due to security concerns.
- **Auth Timeout** - set the length of time before the device will timeout when trying to identify an ID match (*5*, *10*, *15*, *20*, or *30 sec*).
- **Detect Face** - set the device to capture a face image. Upon successful authentication, the captured image is stored in the event log and can be used later for verification purposes.
- **Mifare**
  - **Not use Mifare** - check this box to disable MIFARE card authorization.
  - **Use Data Card** - check this box to use the template on the MIFARE card for authorization.
  - **View Mifare Layout** - click this button to view the MIFARE layout used by the device. For more information about configuring MIFARE layouts, see section 3.6.4.6.
- **Card ID Format**
  - **Format Type** - set the type of pre-processing to occur on card ID data (*Normal* or *Wiegand*). If "Normal" is selected, the card ID data will processed in its original form. If "Wiegand" is selected, devices will interpret card ID data according to the Wiegand format settings.
  - **Byte Order** - specify whether to swap ID card data between cards and devices by most significant byte (*MSB*) or least significant byte (*LSB*).
  - **Bit Order** - specify whether to swap ID card data between cards and devices by most significant bit (*MSB*) or least significant bit (*LSB*).

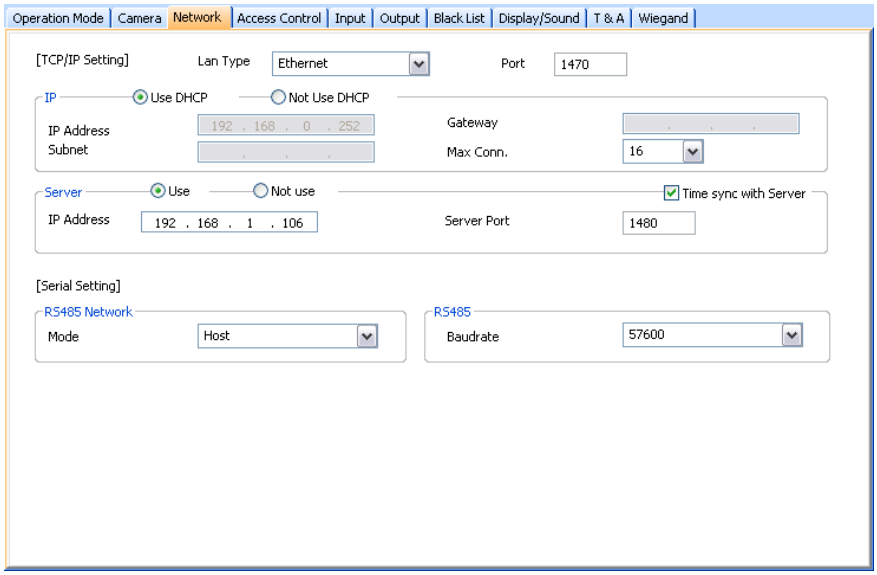
5.1.7.2 Camera tab

The Camera tab allows you to control how the camera is used for authorization purposes. In the Timezone field, select a timezone for the specified event. Click **Add** to select an event that will activate the camera. Click **Apply** to save your settings.



5.1.7.3 Network tab

The Network tab allows you to customize network and server settings for X-Station devices.



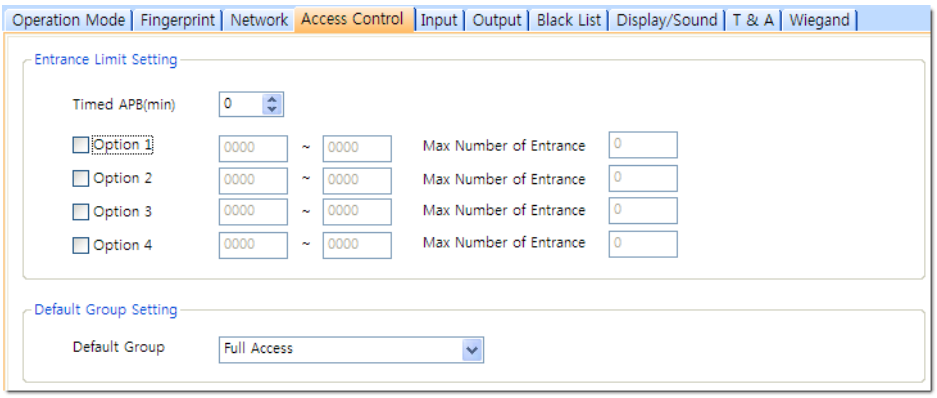
- **TCP/IP Setting**
  - **LAN Type -** select a type of LAN connection from the drop-down list (*Disable*, or *Ethernet*).

- **Port** - specify a port to use for the device.

- **IP**
  - **Use DHCP** - click this radio button to enable the dynamic host configuration protocol (DHCP) for the device.
  - **Not Use DHCP** - click this radio button to disable the dynamic host configuration protocol (DHCP) for this device.
  - **IP Address** - specify an IP address for the device.
  - **Subnet** - specify a subnet address for the device.
  - **Gateway** - specify a network gateway.
  - **Max Conn.** - specify the maximum number of connections to allow.
- **Server**
  - **Use** - click this radio button to enable the server mode.
  - **Not use** - click this radio button do disable server settings.
  - **IP Address** - specify an IP address for the BioStar server.
  - **Server Port** - specify the port used to connect to the server.
  - **Time sync with Server** - check this box to synchronize the device time with the time maintained at the server.
- **RS485 Network**
  - **Mode** - set the mode for a device connected via RS485 (*Disable*, *Host*, or *Slave*). For more information about RS485 modes, see sections 3.2.1 and 3.2.2.
- **RS485**
  - **Baudrate** - set the baud rate for a device connected via RS485 (*9600* to *115200*).

5.1.7.4 Access Control tab

The Access Control tab allows you to customize entrance limit settings and default access groups for an X-Station device.



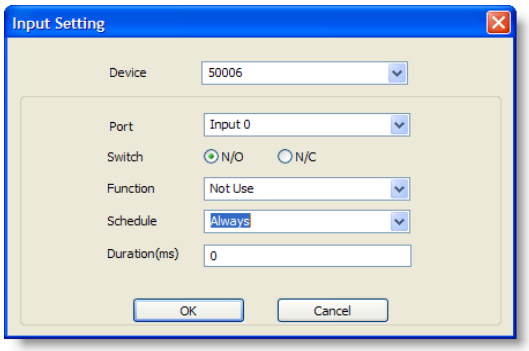
- **Entrance Limit Setting**

- **Timed APB (min)** - set the duration (in minutes) that a user will be unable to regain entry to an area via the device. Once a user has gained entry, the device will reject the user's card or fingerprint authorization for the time period specified here.
- **Option 1-4** - click the checkbox to enable an entrance limit setting, and then specify the effective hours for the entrance limit.
- **Max Number of Entrance** - set the maximum number of entries allowed during the specified time limit.

- **Default Group Setting** - select a default access group to be applied to new users who have not been assigned to another access group.

5.1.7.5 Input tab

The input tab lists input settings you have specified for an X-Station device. Buttons at the bottom of the tab allow you to add, modify, or delete input settings. To add or modify settings, you must specify them from the Input Setting window. For more information about configuring input settings, see section 3.10.3.2.



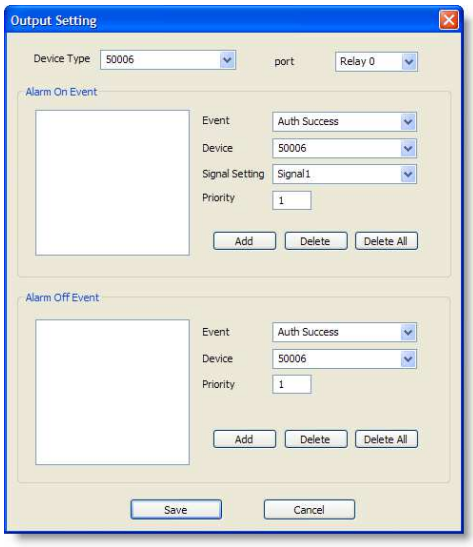
- **Device** - select the X-Station device for which you will add or modify settings.
- **Port** - select an input port (*Input 0*, *Input 1*, or *Tamper*). For Secure I/O devices, these settings are available: Input 0, Input 1, Input 2, Input 3.
- **Switch** - click the radio buttons to specify the normal position of the input switch (N/O - normally open or N/C - normally closed).
- **Function** - select an action to associate with the input:
  - **Not Use** - the input port will not be monitored.
  - **Generic Input** - the input port will be monitored for a triggering action (events specified with "Detect Input 0-3" in the Output settings window—see section 5.1.1.6).

- **Emergency Open** - open doors controlled by this device. The normal door open period will be ignored and doors will remain open until an operator sends a “Close Door” command via the Door/Zone Monitoring tab (see section 4.4.1).
- **Release All Alarms** - cancel alarms associated with this device.
- **Restart Device** - restart the device.
- **Disable Device** - disable the device. A disabled device will not communicate with the BioStar server or process fingerprints or card inputs. To enable communication again, an administrator must provide authentication at the device.

- **Schedule** - set the schedule during which the inputs will be monitored (*Always*, *First Shift*, or *No Time*).
- **Duration (ms)** - set the duration (in milliseconds) an input signal must last to trigger the specified action.

5.1.7.6 Output tab

The Output tab lists output settings you have specified for an X-Station device. Buttons at the bottom of the tab allow you to add, modify, or delete output settings. To add or modify settings, you must specify them from the Output Setting window. For more information about configuring output settings, see section 3.10.3.1.

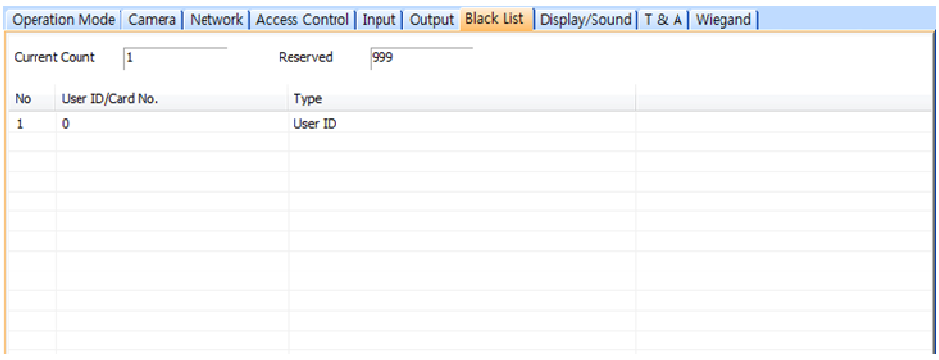


- **Device Type** - select the device type for which you will add or modify settings.
- **Port** - select an output port (Relay 0). For Secure I/O devices, these settings are available: Relay 0 or Relay 1.

- **Alarm On Event** - specify settings and click **Add** to add the event to the Alarm On Event list. These events will activate an alarm.
  - **Event** - select an event that will activate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Closed*, *Forced Open Door*, *Held Open Door*, *Detect Input #0-3*).
  - **Device** - select the device to monitor for an alarm event.
  - **Signal Setting** - select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).
  - **Priority** - set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on (activate) event with a priority of 2 can be canceled only by an alarm off (deactivate) event with a priority of 1 or 2.
- **Alarm Off Event** - specify settings and click **Add** to add the event to the Alarm Off Event list. These events will deactivate an alarm.
  - **Event** - select an event that will deactivate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input #1-3*).
  - **Device** - select the device to monitor for an alarm event.
- **Priority** - set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, a priority 2 “alarm on” event (activate) can be overridden only by an “alarm off” (deactivate) event with a priority of 1 or 2.

5.1.7.7 Black List tab

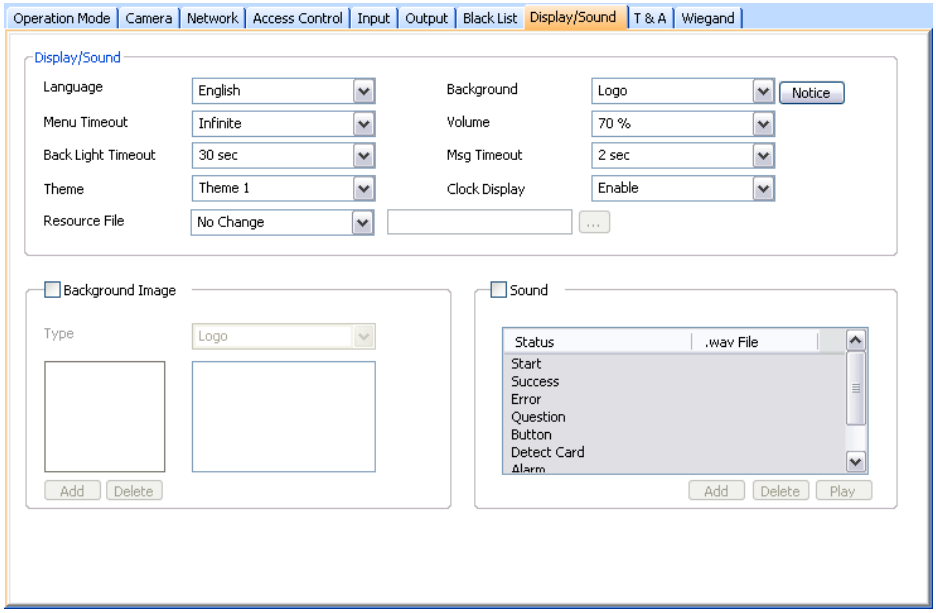
The Black list tab allows you to register user IDs or access card numbers and prevent them from being authenticated with the device.



- **Current Count** – indicates the total number of user IDs and access cards that have been registered.
- **Reserved** – indicates the remaining number of user IDs and access cards that can be registered.

5.1.7.8 Display/Sound tab

The Display/Sound tab allows you to customize the X-Station display and event sounds. To save changes to display or sound settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.



- **Display/Sound**
  - **Language** - set the language to use on the display (*Korean*, *English*, or *Custom*).
  - **Menu Timeout** - set the length of time before the display will return to the idle screen.
  - **Back Light Timeout** – set the length of time before the display goes dim (*Infinite*, *10*, *20*, *30*, *40*, *50*, or *60 sec*).
  - **Theme** - set a display theme (*Theme 1-3*).
  - **Resource File** - set the language resource file to use for the X-Station interface (*No Change*, *English*, *Korean*, or *Custom*). To use a language resource file other than English or Korean, select *Custom* and then click the ellipsis (...) button to locate the resource file.
  - **Background** - set the type of background for the X-Station display (*Logo*, *Notice*, or *Slide Show*). Supported file types (JPG, GIF, BMP, and PNG) cannot exceed 240x320 pixels each. Only one image at a

time can be used as a logo or notice, while up to 16 images can be displayed (at a set interval) in a slide show.

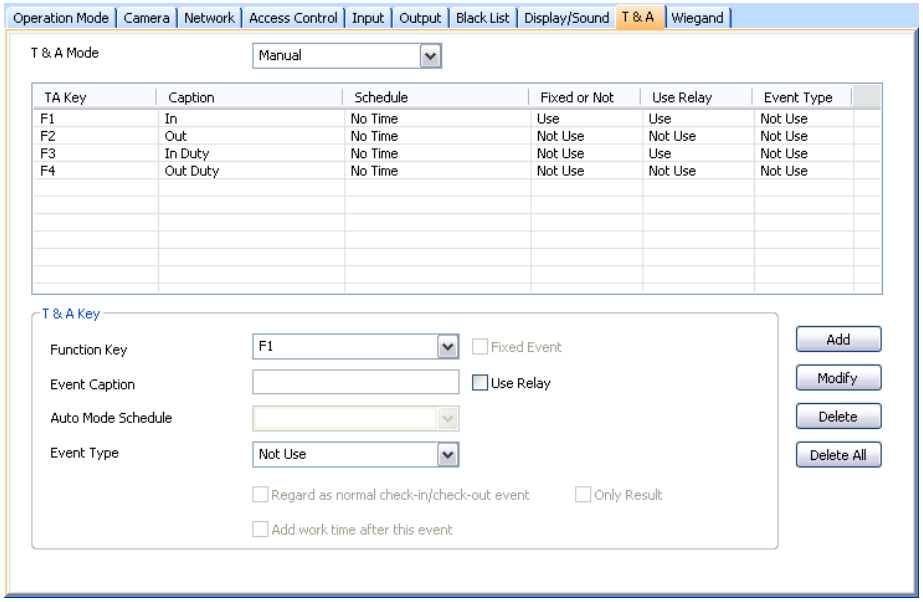
- **Notice** - click this button to create a notice that will be shown on the X-Station display. After creating a notice, you can click **Apply** to apply the notice to the current device or **Apply to Others** to apply the notice to additional devices.
- **Volume** - set the volume of the X-Station device (*0%* to *100%*).
- **Msg Timeout** - set the length of time that a failure or confirmation message will be displayed.
- **Clock Display** - set to display the current time on the device (*Enable* or *Disable*).

- **Background Image** - click this checkbox to upload new background images. Click **Add** to locate and add a new image file. To delete an existing image, click the image name and then click **Delete**.
  - **Type** - set the type of background for the X-Station display (*Logo*, *Notice*, or *Slide Show*). Supported file types (JPG, GIF, BMP, and PNG) cannot exceed 240x320 pixels for Notices and 240x320 pixels for Logos. Only one image at a time can be used as a logo or notice.
- **Sound** - click this checkbox to enable and add custom event sounds. Click an event from the list and then click **Add** to locate and add a new sound file. Click **Delete** to remove custom sound files or **Play** to preview a custom sound file.

5.1.7.9 T&A tab

The T&A tab allows you to configure the mode and key settings for an X-Station device. To save changes to time and attendance settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.

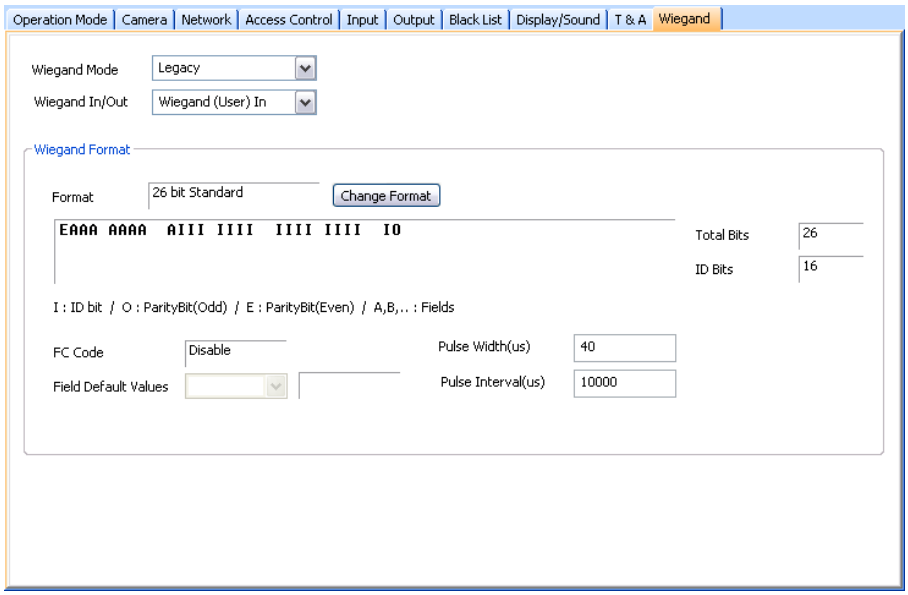
5. Customize Settings



- **T&A Mode** - set the time and attendance mode:
  - **Not Use** - disable the time and attendance functions for this device.
  - **Manual** - users must press the specified key every time they enter or leave to record their T&A events.
  - **Manual Fix** - when a T&A key is pressed, the device will remain in that mode until a different T&A key is pressed.
  - **Auto change** - the device will automatically change T&A modes to correspond with the functions specified for a time period.
  - **Event Fix** - the device will perform only the specified T&A function.
- **T&A Key** - specify which keys to use for T&A events and the event types associated with them:
  - **Function Key** - select a function key from the drop-down list to assign a T&A event (**1-*15*). If you are using the Event Fix mode, you can click the checkbox to the right to designate a fixed event.
  - **Event Caption** - enter a caption for the event.
  - **Auto Mode Schedule** - when using the Auto Change mode, you can specify when the event will occur by selecting a timezone in the drop-down list. For more information on creating a timezone, see section 3.7.1.
  - **Event Type** - set the type of event to assign to the key (*Not Use*, *Check In*, *Check Out*, *In*, or *Out*). In/Out indicates the general check in/out events during a day whereas Check In/Out indicates the formal check in/out events upon arrival and departure at work—or the first check–in and the last check–out events on that day. When you choose Check In or Check Out, you can enable the "Regard as normal check-in/check-out event" option. If this option is enabled, users using the appropriate keys will be regarded arriving or leaving on time at work even though they actually come late or leave early. If you enable the "Only Result" option, they appear being on time on T&A reports but their work time will be calculated correctly based on their actual check in/out time. If you choose *Out*, you can enable the "Add work time after this event" option. If this option is enabled, users using the appropriate key will be considered working for the remainder of the time slot even though they leave the office early.

5.1.7.10 Wiegand tab

The Wiegand tab allows you to configure the Wiegand format for an X-Station device. Click **Change Format** to launch the Wiegand Configuration wizard. For more information on configuring the Wiegand format, see section 3.2.12.



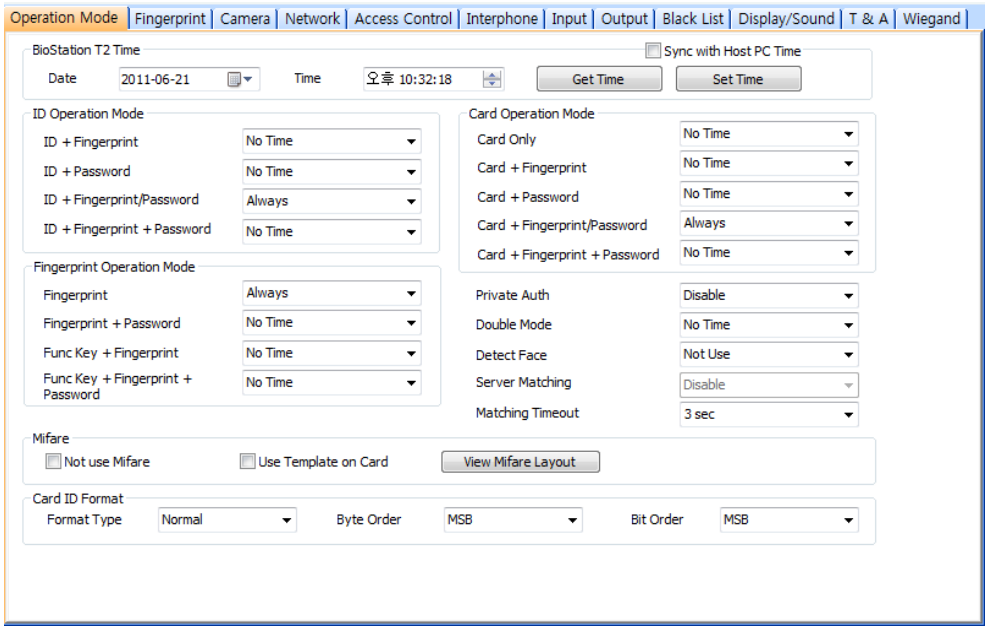
- **Wiegand Mode** - set the mode of Wiegand input to use when reading card ID data (*Legacy* or Extended). The Legacy mode will process ID data from networked devices and RF card readers in the same way (this is the typical function of previous versions of BioStar). The Extended mode will allow RF card readers to operate independently, which allows them to be associated with doors, included in zones, and leave logs with their own device IDs.
- **Wiegand In/Out** - assign the function of the Wiegand input or output:
  - **Wiegand (User) In** - the ID field of the Wiegand string is interpreted as a user ID.
  - **Wiegand (Card) In** - the ID field of the Wiegand string is interpreted as a card ID.
  - **Wiegand (User) Out** - inserts the user ID of the authenticated user in the ID field of the Wiegand string.
  - **Wiegand (Card) Out** - inserts the card ID of the authenticated user in the ID field of the Wiegand string.

5.1.8 Customize Settings for BioStation T2 Devices

The sections below describe the settings available for BioStation T2 devices. Customize the way BioStation T2 devices function by changing these settings to suit your particular environment and operational needs.

5.1.8.1 Operation Mode tab

The Operation Mode tab allows you to customize time and various operation modes settings for BioStation T2 devices.



- **BioStation T2 Time**
  - **Date** - manually set the device date with a drop-down calendar.
  - **Time** - manually set the device time.
  - **Sync with Host PC Time** - check this box to automatically synchronize the device time with the time of the host computer.
  - **Get Time** - get the current time displayed by the device.
  - **Set Time** - set the time on the device.
- **ID Operation Mode** - the drop-down lists in this area allow you to control the authentication mode by schedule. For example, you can choose a normal authentication mode for working hours and a more strict authentication mode for hours outside the normal schedule. You can specify authentication modes either by device or by user (see section 5.4.1). Unless a particular mode is specified for a user, the device authentication mode will apply.
  - **ID + Fingerprint** - set the device to require ID plus fingerprint authorization (*Always*, or *No Time*).

- **ID + Password** - set the device to require ID plus password authorization (*Always*, or *No Time*).
- **ID + Fingerprint/Password** - set the device to require ID plus fingerprint or password authorization (*Always*, or *No Time*).
- **ID + Fingerprint + Password** - set the device to require ID plus fingerprint plus password authorization (*Always*, or *No Time*).

• **Card Operation Mode**

- **Card Only** - set the device to require only card authorization (*Always*, or *No Time*).
- **Card + Fingerprint** - set the device to require card plus fingerprint authorization (*Always*, or *No Time*).
- **Card + Password** - set the device to require card plus password authorization (*Always*, or *No Time*).
- **Card + Fingerprint/Password** - set the device to require card plus fingerprint or password authorization (*Always*, or *No Time*).
- **Card + Fingerprint + Password** - set the device to require card plus fingerprint plus password authorization (*Always*, or *No Time*).

• **Fingerprint Operation Mode**

- **Fingerprint** - set the device to require only fingerprint authorization (*Always*, or *No Time*).
- **Fingerprint + Password** - set the device to require fingerprint plus password authorization (*Always*, or *No Time*).
- **Func Key + Fingerprint** - set the device to require function key plus fingerprint authorization (*Always*, or *No Time*).
- **Func Key + Fingerprint + Password** - set the device to require function key plus fingerprint plus password authorization (*Always*, or *No Time*).

• **Other options**

- **Private Auth** - set the device to allow a private authorization method (*Disable* or *Enable*). If enabled, the authentication mode of the user will be determined by a user's "Authorization" setting, which is located on the Details tab. If disabled, the authentication mode will be determined by operation mode settings of the device.
- **Double Mode** - set the device to require authentication of two users' IDs, access cards or fingerprints (*Always*, or *No Time*). The timeout for presenting the second authentication is 15 seconds.

- **Detect Face** - set the device to capture a face image. Upon successful authentication, the captured image is stored in the event log.
- **Server Matching** - enable this setting to perform user ID, fingerprint or card ID matching at the BioStar server, instead of the device. When this mode is enabled, the devices will send the user ID, fingerprint template or card ID to the server to verify a match. This mode is useful when you have more users than can be downloaded to a device or user information cannot be distributed due to security concerns.
- **Matching Timeout** - set the length of time before the device will timeout when trying to identify a fingerprint match within the device itself or via the server (*3, 7, 10, 15, 20, 30 sec*).

• **Mifare**

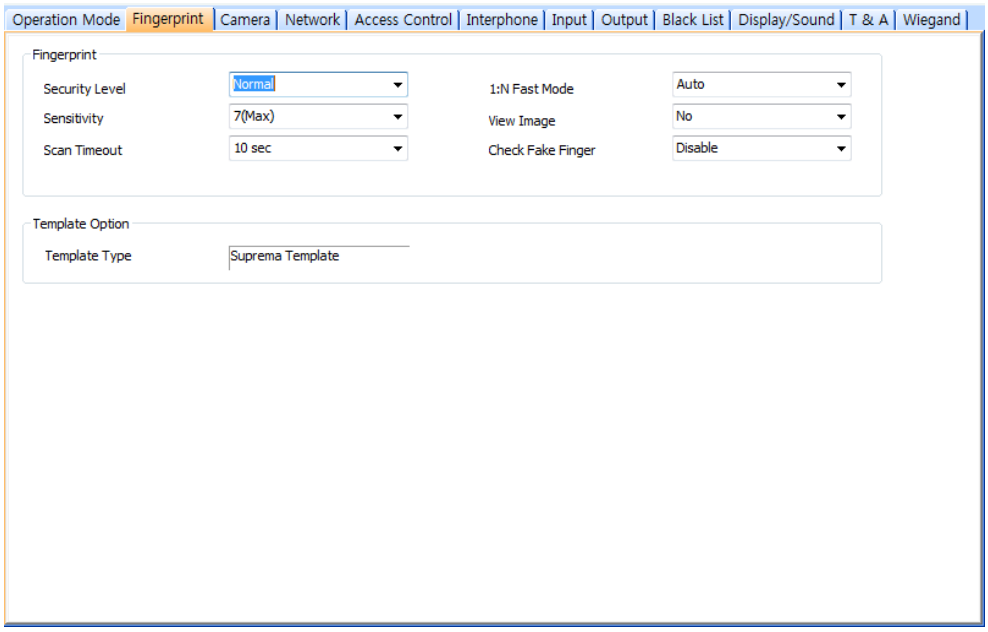
- **Not use Mifare** - check this box to disable MIFARE card authorization.
- **Use Template on Card** - check this box to use the template on the MIFARE card for authorization.
- **View Mifare Layout** - click this button to view the MIFARE layout used by the device. For more information about configuring MIFARE layouts, see section 3.6.4.6.

• **Card ID Format**

- **Format Type** - set the type of pre-processing to occur on card ID data (*Normal* or *Wiegand*). If "Normal" is selected, the card ID data will processed in its original form. If "Wiegand" is selected, devices will interpret card ID data according to the Wiegand format settings.
- **Byte Order** - specify whether to swap ID card data between cards and devices by most significant byte (*MSB*) or least significant byte (*LSB*).
- **Bit Order** - specify whether to swap ID card data between cards and devices by most significant bit (*MSB*) or least significant bit (*LSB*).

5.1.8.2 Fingerprint tab

The Fingerprint tab allows you to customize fingerprint authorization settings for BioStation T2 devices.

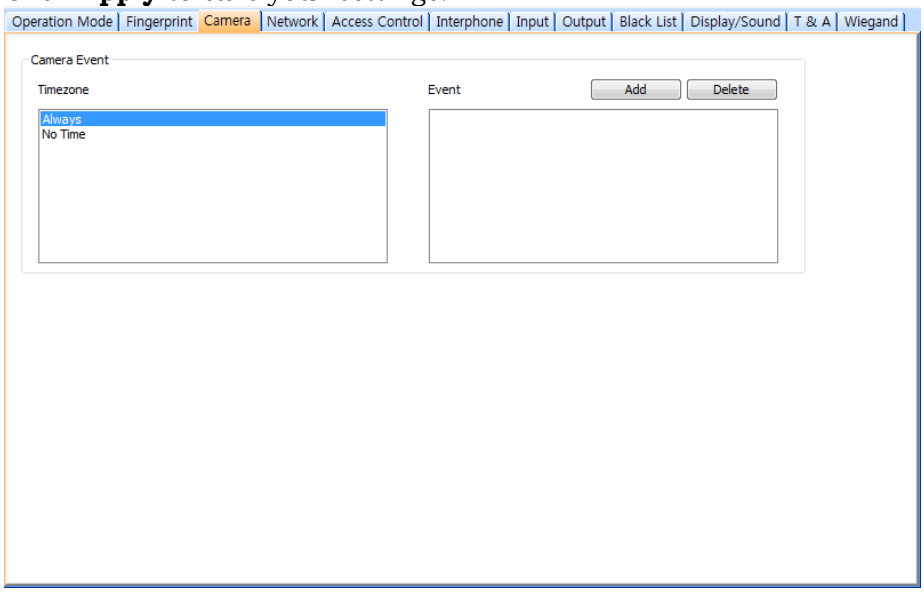


- **Fingerprint**
  - **Security Level** - set the security level to use for fingerprint authorization (*Normal*, *Secure*, or *Most Secure*). Keep in mind that as the security level is increased, so too is the likelihood of a false rejection.
  - **Sensitivity** - set the sensitivity of the fingerprint scanner (*0 [Min]* to *7 [Max]*). A higher sensitivity setting will result in more easily captured fingerprint scans, but also increases the sensitivity to external noise.
  - **Scan Timeout** - set the length of time before the fingerprint scanner will timeout (*1 sec* to *20 sec*). If a user does not place a finger on the device within the timeout period, the authorization will fail.
  - **1:N Fast Mode** - set the device to use Fast Mode to reduce the amount of time required for matching fingerprints (*Auto*, *Normal*, *Fast*, or *Fastest*). Setting Fast Mode to *Auto* will adjust the matching speed according to the number of enrolled templates.
  - **View Image** - set to show or hide fingerprint images on the BioStation T2 display (*Yes* or *No*).

- **Check Fake Finger** - set the device to detect the use of fake fingerprints, such as those made from silicon or rubber, and prevent unauthorized access.
- **Template Option** - displays the global fingerprint template settings. For more information about fingerprint templates, see section 4.9.

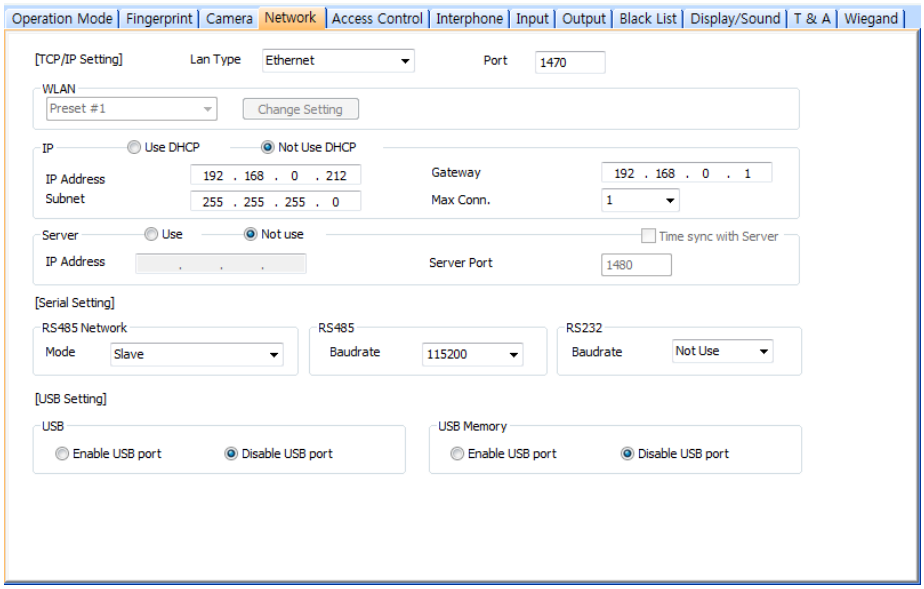
5.1.8.3 Camera tab

The Camera tab allows you to control how the camera is used for authorization purposes. In the Timezone field, select a timezone for the specified event. Click **Add** to select an event that will activate the camera. Click **Apply** to save your settings.



5.1.8.4 Network tab

The Network tab allows you to customize network and server settings for BioStation T2 devices.



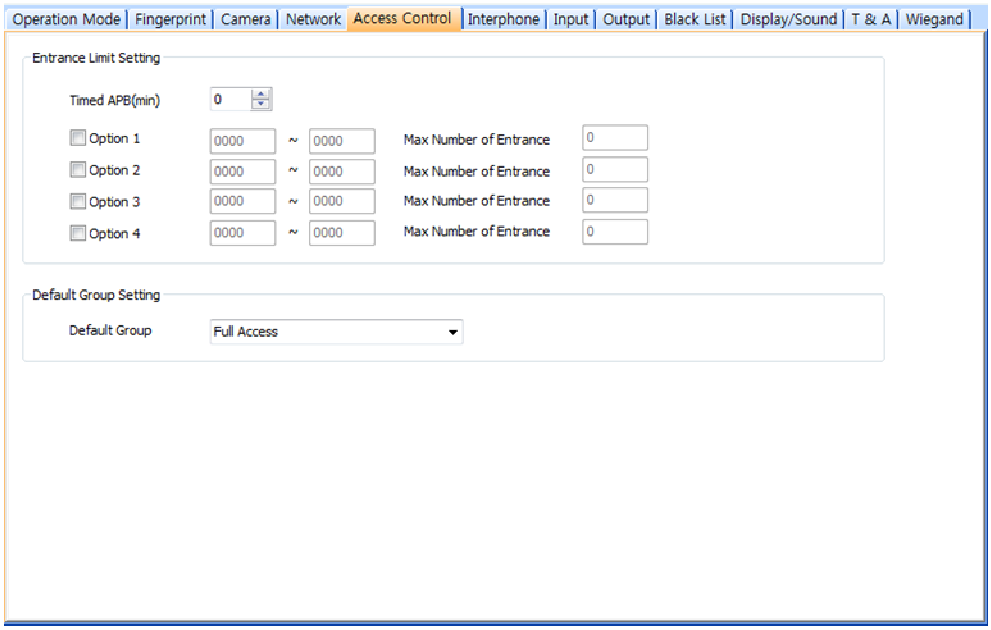
- **TCP/IP Setting**
  - **LAN Type -** select a type of LAN connection from the drop-down list (*Disable*, *Ethernet*, or *Wireless LAN*).
  - **Port** - specify a port to use for the device.
- **WLAN**
  - **Change setting** - click to specify settings for a wireless local area network (WLAN). This option is active only when WLAN is selected as the TCP/IP setting. For more information about configuring settings for a WLAN, see section 3.2.4.1.
- **IP**
  - **Use DHCP** - click this radio button to enable the dynamic host configuration protocol (DHCP) for the device.
  - **Not Use DHCP** - click this radio button to disable the dynamic host configuration protocol (DHCP) for this device.
  - **IP Address** - specify an IP address for the device.
  - **Subnet** - specify a subnet address for the device.
  - **Gateway** - specify a network gateway.
  - **Max Conn.** - specify the maximum number of connections to allow.
- **Server**
  - **Use** - click this radio button to enable the server mode.
  - **Not use** - click this radio button do disable server settings.
  - **IP Address** - specify an IP address for the BioStar server.
  - **Server Port** - specify the port used to connect to the server.
- **RS485 Network**

- **Mode** - set the mode for a device connected via RS485 (*Disable*, *Host*, or *Slave*). For more information about RS485 modes, see sections 3.2.1 and 3.2.2.

- **RS485**
  - **Baudrate** - set the baud rate for a device connected via RS485 (*9600* to *115200*).
- **RS232**
  - **Baudrate** - set the baud rate for a device connected via RS232 (*9600* to *115200*).
- **USB** - click the radio buttons to enable or disable the USB port on the BioStation T2 device.
- **USB Memory** - click the radio buttons to enable or disable the USB memory on the BioStation T2 device.

5.1.8.5 Access Control tab

The Access Control tab allows you to customize entrance limit settings and default access groups for a BioStation T2 device.



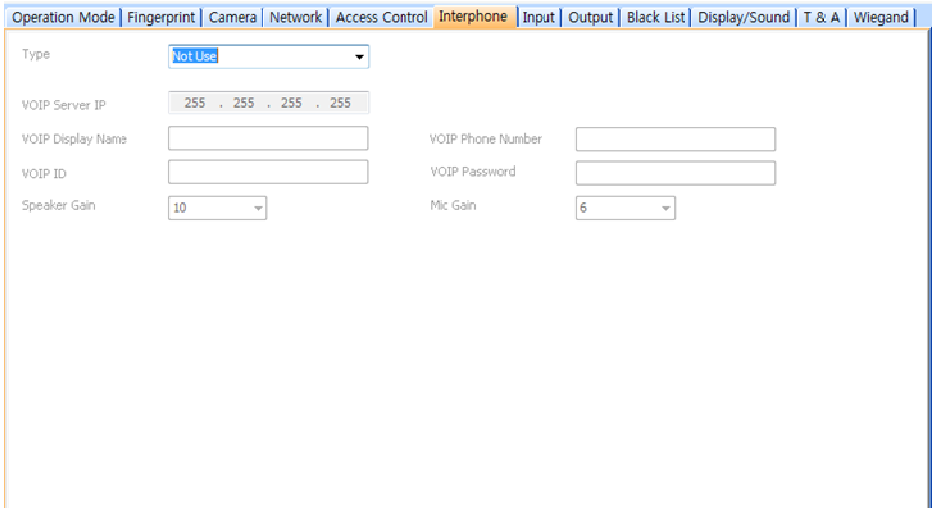
- **Entrance Limit Setting**
  - **Timed APB (min)** - set the duration (in minutes) that a user will be unable to regain entry to an area via the device. Once a user has gained entry, the device will reject the user's ID, access card, or fingerprint authorization for the time period specified here.
  - **Option 1-4** - click the checkbox to enable an entrance limit setting, and then specify the effective hours for the entrance limit.

- **Max Number of Entrance** - set the maximum number of entries allowed during the specified time limit.

- **Default Group Setting** - select a default access group to be applied to new users who have not been assigned to another access group.

5.1.8.6 Interphone tab

The Interphone tab allows you to set the device to act as an interphone to allow communication between people on either side of the door.



- **Type** – select one of the following options:
  - **Aanlogue Interphone** – choose this option to enable the analogue interphone.
  - **IP Interphone** – choose this option to enable the VoIP feature. A telephone is required.
  - **BioStar Videophone** – choose this option to enable the videophone feature that supports both video and voice calls. The supplied PC software is required. The BioStar vidoephone works only with the device firmware version of BioStation T2 V1.1 or later.

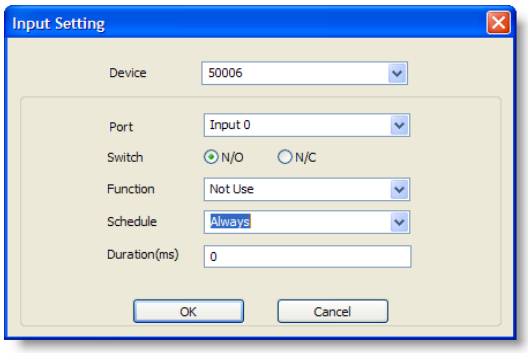
When you select **IP Interphone** in the Type drop-down list, specify the following settings:

- **VoIP Server IP** – specify an IP address for the VoIP server.
- **VoIP Phone Number** – specify a phone number for the interphone.
- **VoIP Display Name** – specify a name to use for communication through the interphone.
- **VoIP ID** – specify a user name to access the VoIP server.
- **VoIP Password** – specify a password to access the VoIP server.
- **VoIP Speaker Gain** – specify the volume of the speaker.

- **VoIP Mic Gain** – specify the volume of the microphone.

5.1.8.7 Input tab

The input tab lists input settings you have specified for a BioStation T2 device. Buttons at the bottom of the tab allow you to add, modify, or delete input settings. To add or modify settings, you must specify them from the Input Setting window. For more information about configuring input settings, see section 3.10.3.2.

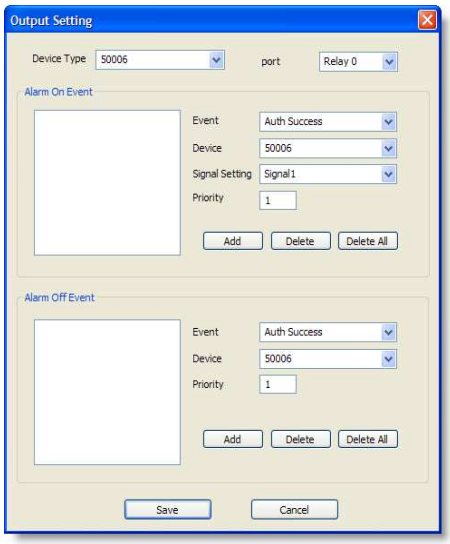


- **Device** - select the BioStation T2 device for which you will add or modify settings.
- **Port** - select an input port (Input 0, Input 1, or Tamper). For Secure I/O devices, these settings are available: Input 0, Input 1, Input 2, Input 3.
- **Switch** - click the radio buttons to specify the normal position of the input switch (N/O - normally open or N/C - normally closed).
- **Function** - select an action to associate with the input:
  - **Not Use** - the input port will not be monitored.
  - **Generic Input** - the input port will be monitored for a triggering action (events specified with “Detect Input 0-3” in the Output settings window—see section 5.1.1.6).
  - **Emergency Open** - open doors controlled by this device. The normal door open period will be ignored and doors will remain open until an operator sends a “Close Door” command via the Door/Zone Monitoring tab (see section 4.4.1).
  - **Release All Alarms** - cancel alarms associated with this device.
  - **Restart Device** - restart the device.
  - **Disable Device** - disable the device. A disabled device will not communicate with the BioStar server or process fingerprints or card inputs. To enable communication again, an administrator must provide authentication at the device.

- **Schedule** - set the schedule during which the inputs will be monitored (*Always* or *No Time*).
- **Duration (ms)** - set the duration (in milliseconds) an input signal must last to trigger the specified action.

5.1.8.8 Output tab

The Output tab lists output settings you have specified for a BioStation T2 device. Buttons at the bottom of the tab allow you to add, modify, or delete output settings. To add or modify settings, you must specify them from the Output Setting window. For more information about configuring output settings, see section 3.10.3.1.



- **Device Type** - select the device type for which you will add or modify settings.
- **Port** - select an output port (Relay 0). For Secure I/O devices, these settings are available: Relay 0 or Relay 1.
- **Alarm On Event** - specify settings and click **Add** to add the event to the Alarm On Event list. These events will activate an alarm.
  - **Event** - select an event that will activate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, *Detect Input # 1-3*).
  - **Device** - select the device to monitor for an alarm event.
  - **Signal Setting** - select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).

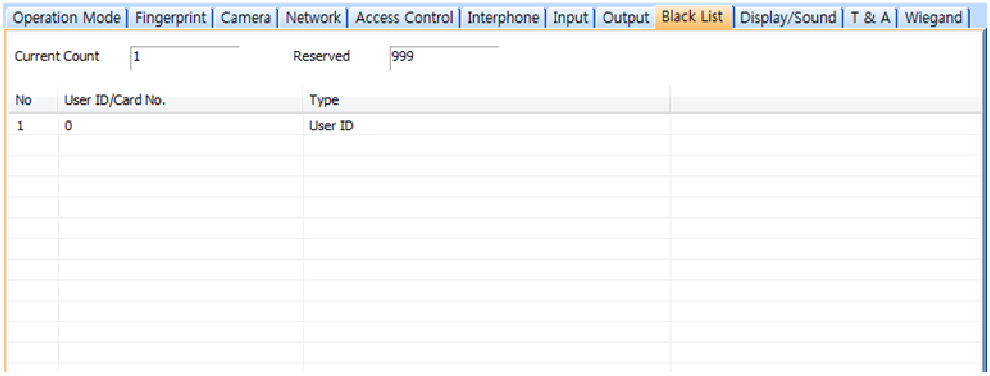
- **Priority** - set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on (activate) event with a priority of 2 can be canceled only by an alarm off (deactivate) event with a priority of 1 or 2.

- **Alarm Off Event** - specify settings and click **Add** to add the event to the Alarm Off Event list. These events will deactivate an alarm.
  - **Event** - select an event that will deactivate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input # 1-3*).
  - **Device** - select the device to monitor for an alarm event.

- **Priority** - set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, a priority 2 “alarm on” event (activate) can be overridden only by an “alarm off” (deactivate) event with a priority of 1 or 2.

5.1.8.9 Black List tab

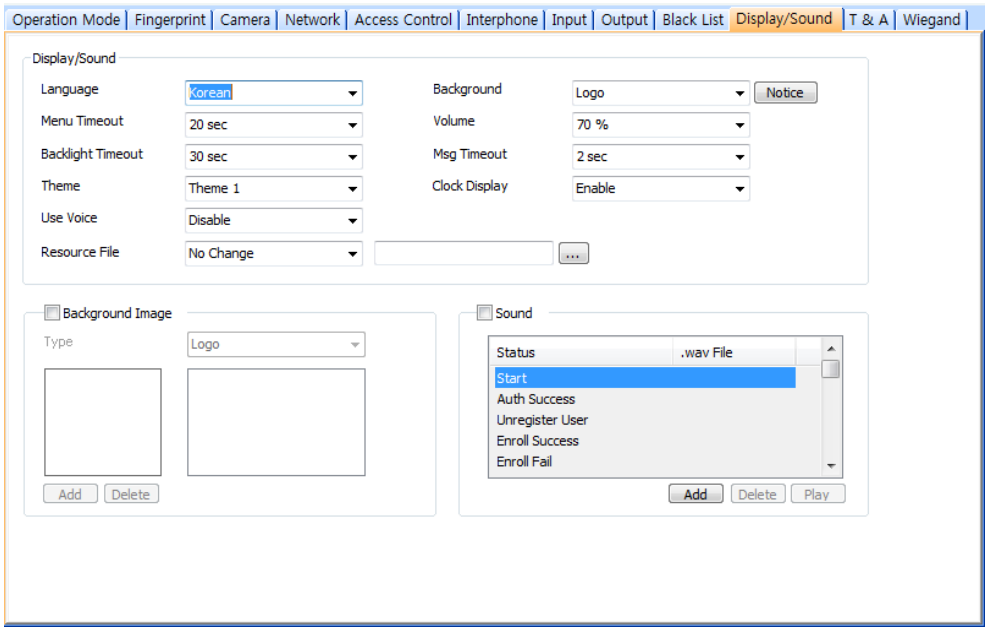
The Black List tab allows you to register user IDs or access card numbers and prevent them from being authenticated with the device.



- **Current Count** – indicates the total number of the user IDs and access cards that have been registered.
- **Reserved** – indicates the remaining number of user IDs and access cards to be registered.

5.1.8.10 Display/Sound tab

The Display/Sound tab allows you to customize the BioStation T2 display and event sounds. To save changes to display or sound settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.

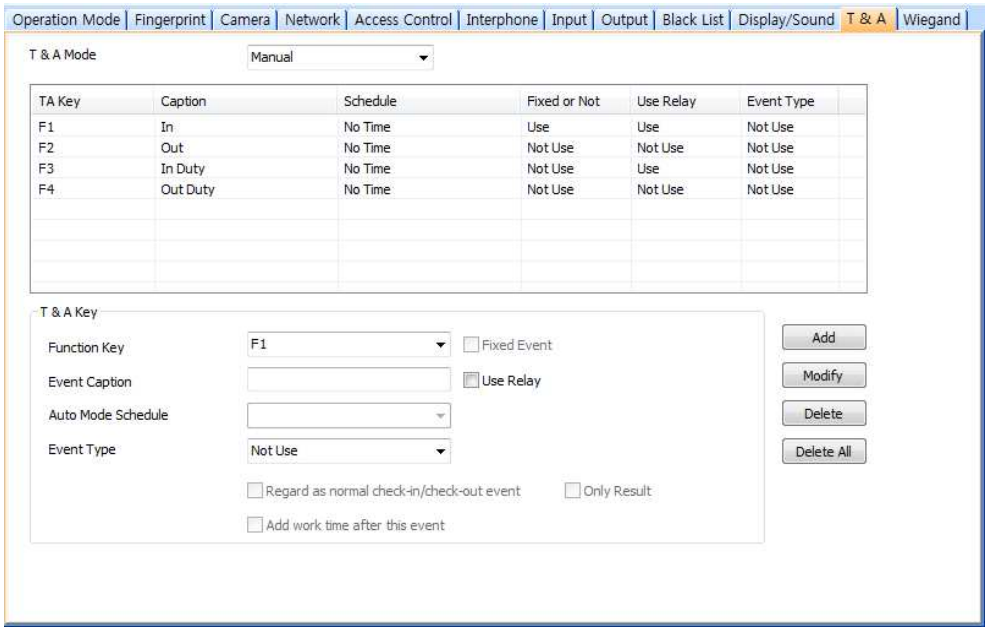


- **Display/Sound**
  - **Language** - set the language to use on the display (*Korean*, *English*, or *Custom*).
  - **Menu Timeout** - set the length of time before the display will return to the idle screen.
  - **Backlight Timeout** – set the length of time before the display goes dim.
  - **Theme** - set a display theme.
  - **Use Voice** – set the device to notify you with voice messages (*Disable* or *Enable*).
  - **Resource File** – set the language resource file to use for the BioStar interface (*No Change*, *English*, *Korean*, or *Custom*). To use a language resource file other than English or Korean, select *Custom* and then click the ellipsis (...) button to locate the resource file..
  - **Background** - set the type of background for the BioStation T2 display (*Logo*, *Notice*, or *Slide Show*). Supported file types (JPG, GIF, BMP, PNG and PDF) cannot exceed 480x800 pixels each. Only one image at a time can be used as a logo or notice, while up to 16 images can be displayed (at a set interval) in a slide show.
  - **Volume** - set the volume of the BioStation device (*0%* to *100%*).
  - **Msg Timeout** - set the length of time that a failure or confirmation message will be displayed.
  - **Clock Display** - set to display the current time on the device (*Enable* or *Disable*).

- **Background Image** - click this checkbox to upload new background images. Click the plus sign (+) to locate and add a new image file.
  - **Type** - set the type of background for the BioStation display (*Logo* or *Notice*). Supported file types (JPG, GIF, BMP, PNG and PDF) cannot exceed 480x800 pixels for Notices and 480x800 pixels for Logos. Only one image at a time can be used as a logo or notice.
- **Sound** - click this checkbox to enable and add custom event sounds. Click an event from the list and then click the plus sign (+) to locate and add a new sound file. Click **Add** to add new sound files, **Delete** to remove sound files, or **Play** to preview a selected sound file.

5.1.8.11 T&A tab

The T&A tab allows you to configure the mode and key settings for a BioStation T2 device. To save changes to time and attendance settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.

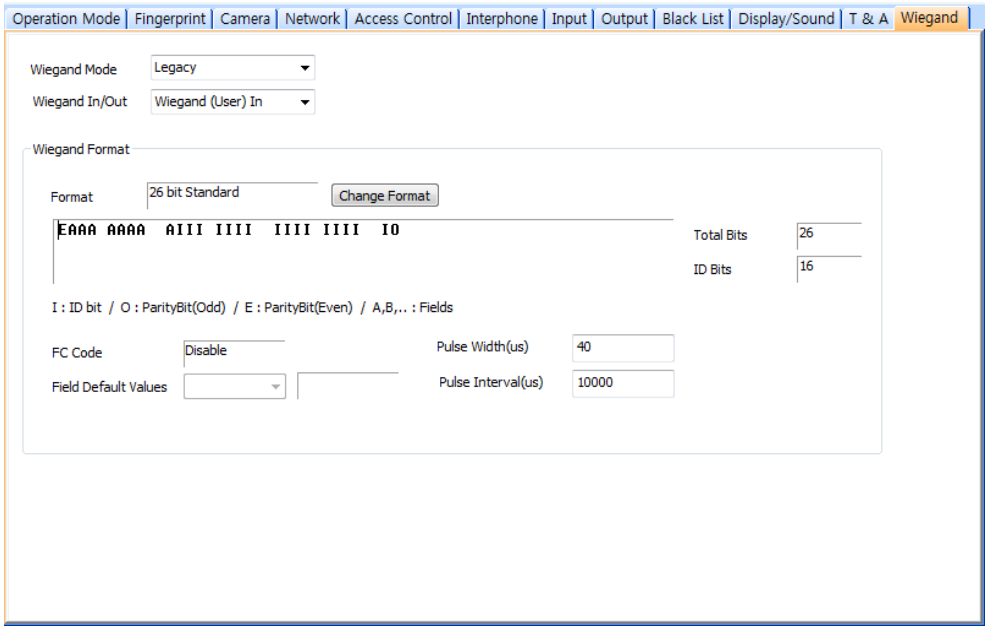


- **T&A Mode** - set the time and attendance mode:
  - **Not Use** - disable the time and attendance functions for this device.
  - **Manual** - users must press the specified key every time they enter or leave to record their T&A events.
  - **Manual Fix** - when a T&A key is pressed, the device will remain in that mode until a different T&A key is pressed.
  - **Auto change** - the device will automatically change T&A modes to correspond with the functions specified for a time period.
  - **Event Fix** - the device will perform only the specified T&A function.

- **T&A Key** - specify which keys to use for T&A events and the event types associated with them:
  - **Function Key** - select a function key from the drop-down list to assign a T&A event (*F1-F4*, *EXT01-EXT12)*. If you are using the Event Fix mode, you can click the checkbox to the right to designate a fixed event.
  - **Event Caption** - enter a caption for the event.
  - **Auto Mode Schedule** - when using the Auto Change mode, you can specify when the event will occur by selecting a timezone in the drop-down list. For more information on creating a timezone, see section 3.6.1.
  - **Event Type** - set the type of event to assign to the key (*Not Use*, *Check In*, *Check Out*, *In*, or *Out*). In/Out indicates the general check in/out events during a day whereas Check In/Out indicates the formal check in/out events upon arrival and departure at work—or the first check–in and the last check–out events on that day. When you choose Check In or Check Out, you can enable the "Regard as normal check-in/check-out event" option. If this option is enabled, users who activate the appropriate keys will be regarded as arriving or leaving on time at work even though they actually arrive late or leave early. If you enable the "Only Result" option, they appear being on time on T&A reports but their work time will be calculated correctly based on their actual check in/out time. If you choose *Out*, you can enable the "Add work time after this event" option. If this option is enabled, users activating the appropriate key will be considered working for the remainder of the time slot even if they leave the office early.

5.1.8.12 Wiegand tab

The Wiegand tab allows you to configure the Wiegand format for a BioStation T2 device. Click **Change Format** to launch the Wiegand Configuration wizard. For more information on configuring the Wiegand format, see section 3.2.12.



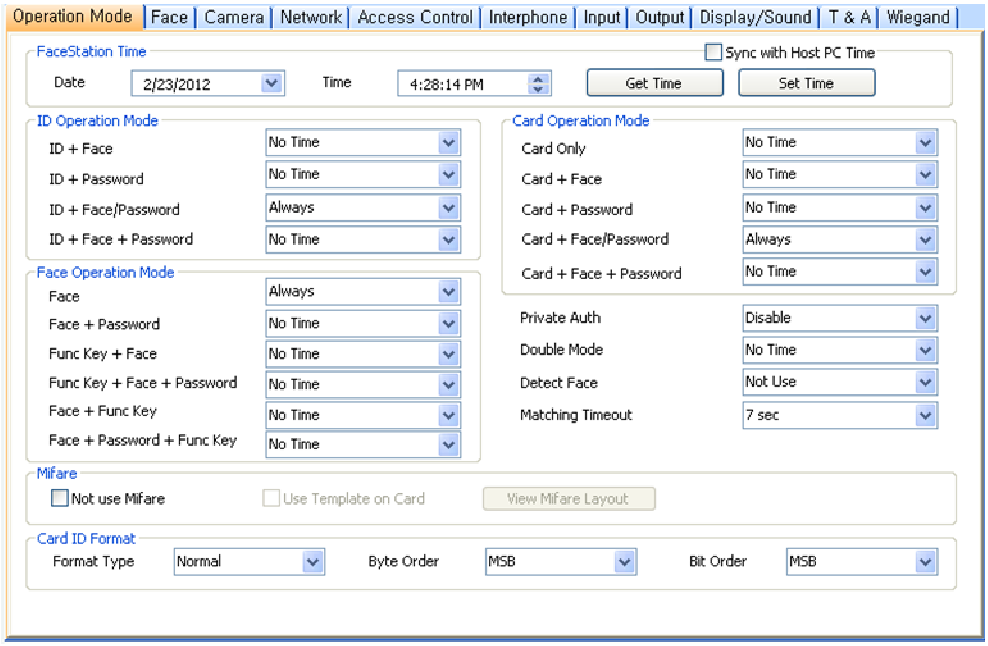
- **Wiegand Mode** - set the mode of Wiegand input to use when reading card ID data (*Legacy* or *Extended*). The Legacy mode will treat connected RF devices as part of their host devices (this is the typical function of previous versions of BioStar). The Extended mode will allow RF card readers to operate independently, which allows them to be associated with doors, included in zones, and leave logs with their own device IDs.
- **Wiegand In/Out** - assign the Wiegand input or output:
  - **Wiegand (User) In** - the ID field of the Wiegand string is interpreted as a user ID.
  - **Wiegand (Card) In** - the ID field of the Wiegand string is interpreted as a card ID.
  - **Wiegand (User) Out** - inserts the user ID of the authenticated user in the ID field of the Wiegand string.
  - **Wiegand (Card) Out** - inserts the card ID of the authenticated user in the ID field of the Wiegand string.

5.1.9 Customize Settings for FaceStation Devices

The sections below describe the settings available for FaceStation devices. Customize the way FaceStation devices function by changing these settings to suit your particular environment and operational needs.

5.1.9.1 Operation Mode tab

The Operation Mode tab allows you to customize time and various operation modes settings for FaceStation devices.



- **FaceStation Time**
  - **Date** - manually set the device date with a drop-down calendar.
  - **Time** - manually set the device time.
  - **Sync with Host PC Time** - check this box to automatically synchronize the device time with the time of the host computer.
  - **Get Time** - get the current time displayed by the device.
  - **Set Time** - set the time on the device.
- **ID Operation Mode** - the drop-down lists in this area allow you to control the authentication mode by schedule. For example, you can choose a normal authentication mode for working hours and a more strict authentication mode for hours outside the normal schedule. You can specify authentication modes either by device or by user (see section 5.4.1). Unless a particular mode is specified for a user, the device authentication mode will apply.

- **ID + Face** – set the device to require ID plus face recognition for authorization (*Always*, *New Time Zone*, or *No Time*).
- **ID + Password** - set the device to require ID plus password authorization (*Always*, *New Time Zone*, or *No Time*).
- **ID + Face/Password** - set the device to require ID plus face recognition or password authorization (*Always*, *New Time Zone*, or *No Time*).
- **ID + Face + Password** - set the device to require ID plus face recognition plus password authorization (*Always*, *New Time Zone*, or *No Time*).

• **Card Operation Mode**

- **Card Only** - set the device to require only card authorization (*Always*, *New Time Zone*, or *No Time*).
- **Card + Face** - set the device to require card plus face recognition for authorization (*Always*, *New Time Zone*, or *No Time*).
- **Card + Password** - set the device to require card plus password authorization (*Always*, *New Time Zone*, or *No Time*).
- **Card + Face/Password** - set the device to require card plus face recognition or password authorization (*Always*, *New Time Zone*, or *No Time*).
- **Card + Face + Password** - set the device to require card plus face recognition plus password authorization (*Always*, *New Time Zone*, or *No Time*).

• **Face Operation Mode**

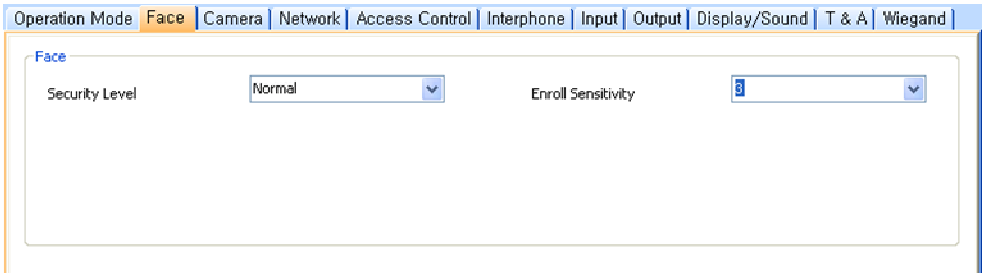
- **Face** - set the device to require only face recognition for authorization (*Always*, *New Time Zone*, or *No Time*).
- **Face + Password** - set the device to require face recognition plus password authorization (*Always*, *New Time Zone*, or *No Time*).
- **Func Key + Face** - set the device to require function key plus face recognition for authorization (*Always*, *New Time Zone*, or *No Time*).
- **Func Key + Face + Password** - set the device to require function key plus face recognition plus password authorization (*Always*, *New Time Zone*, or *No Time*).
- **Face + Func Key** - set the device to require face recognition plus function key authorization, and then immediately proceed to T&A functions (*Always*, *New Time Zone*, or *No Time*).
- **Face + Password + Func Key** - set the device to require face recognition plus password plus function key authorization, and then

immediately proceed to T&A functions (*Always*, *New Time Zone*, or *No Time*).

- **Other options**
  - **Private Auth** - set the device to allow a private authorization method (*Disable* or *Enable*). If enabled, the authentication mode of the user will be determined by a user's "Authorization" setting, which is located on the Details tab. If disabled, the authentication mode will be determined by operation mode settings of the device.
  - **Double Mode** - set the device to require authentication of two users' IDs, access cards or face recognitions (*Always*, *New Time Zone*, or *No Time*). The timeout for presenting the second authentication is 15 seconds.
  - **Detect Face** - set the device to capture a face image (*Use* or *Not Use*). Upon successful authentication, the captured image is stored in the event log.
  - **Matching Timeout** - set the length of time before the device will timeout when trying to identify a fingerprint match within the device itself or via the server (*3*, *7*, *10*, *15*, *20, 30 sec*).
- **Mifare**
  - **Not use Mifare** - check this box to disable MIFARE card authorization.
  - **Use Template on Card** – not available with FaceSation devices.
  - **View Mifare Layout** - not available with FaceSation devices.
- **Card ID Format**
  - **Format Type** - set the type of pre-processing to occur on card ID data (*Normal* or *Wiegand*). If "Normal" is selected, the card ID data will processed in its original form. If "Wiegand" is selected, devices will interpret card ID data according to the Wiegand format settings.
  - **Byte Order** - specify whether to swap ID card data between cards and devices by most significant byte (*MSB*) or least significant byte (*LSB*).
  - **Bit Order** - specify whether to swap ID card data between cards and devices by most significant bit (*MSB*) or least significant bit (*LSB*).

5.1.9.2 Face tab

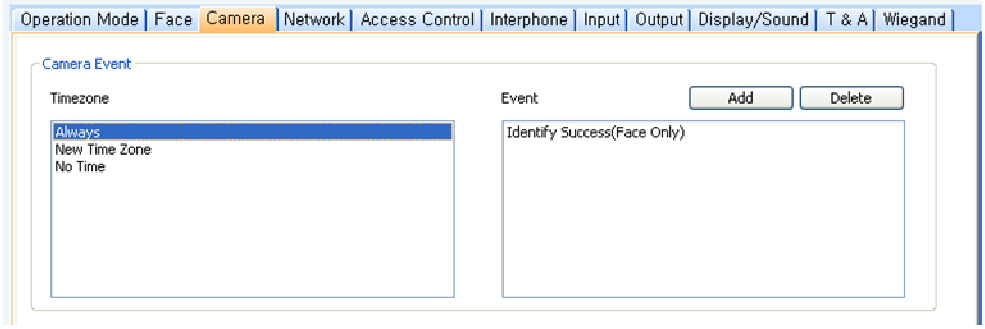
The Face tab allows you to customize face recognition settings for FaceStation devices.



- **Face**
  - **Security Level** - set the security level to use for face recognition (*Normal, Secure, or Most Secure*). Keep in mind that as the security level is increased, so too is the likelihood of a false rejection.
  - **Enroll Sensitivity** - set the sensitivity of the face recognition system (*0 [Min]* to *9 [Max]*). A higher sensitivity setting will result in easier face recognition, but also increases the sensitivity to external visual noise.

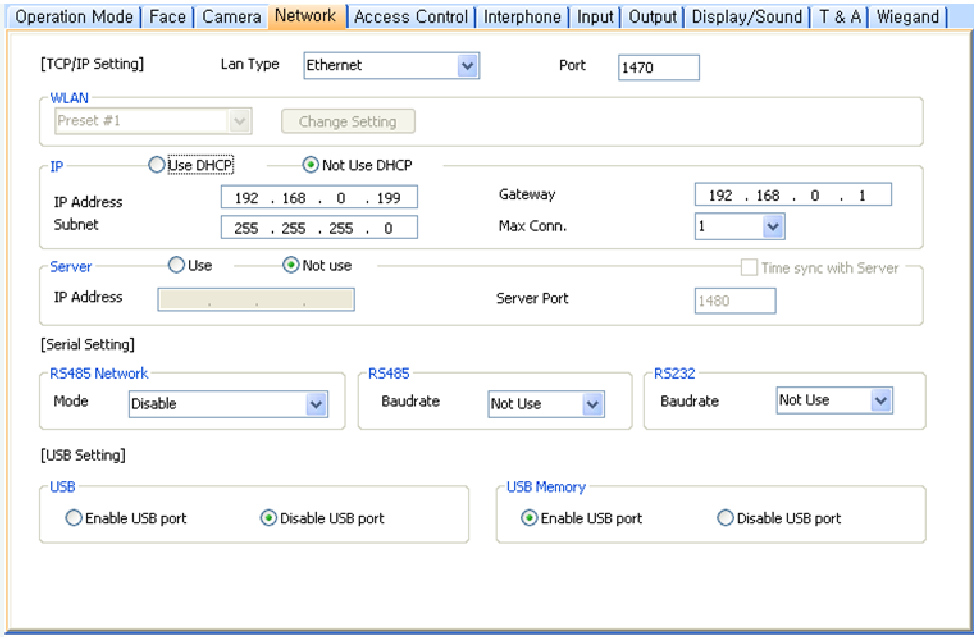
5.1.9.3 Camera tab

The Camera tab allows you to control how the camera is used for authorization purposes. In the Timezone field, select a timezone for the specified event. Click **Add** to select an event that will activate the camera. Click **Apply** to save your settings.



5.1.9.4 Network tab

The Network tab allows you to customize network and server settings for FaceStation devices.

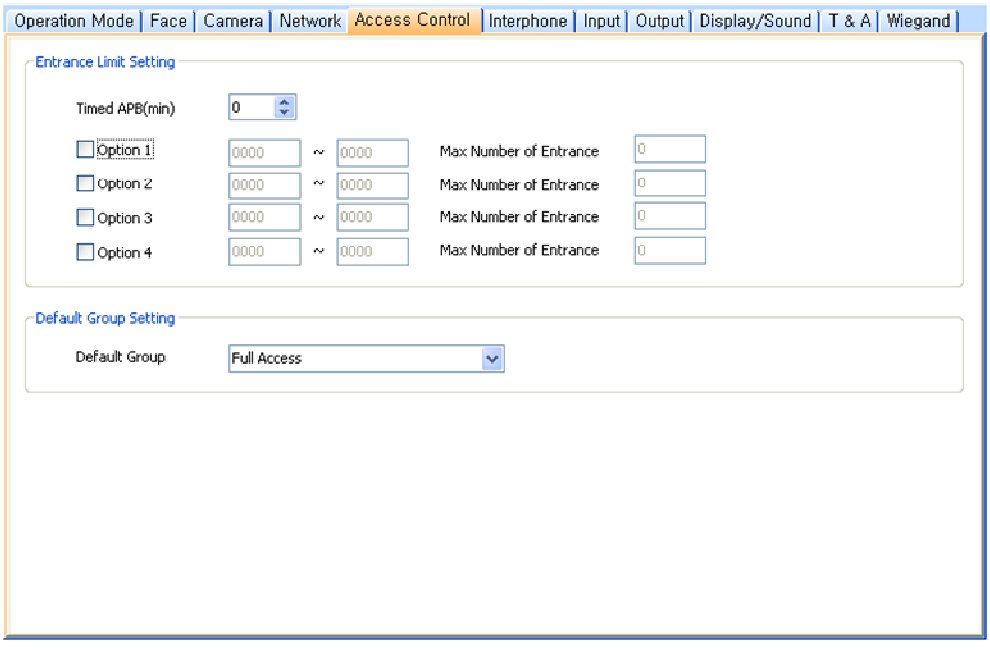


- **TCP/IP Setting**
  - **LAN Type -** select a type of LAN connection from the drop-down list (*Disable*, *Ethernet*, or *Wireless LAN*).
  - **Port** - specify a port to use for the device.
- **WLAN**
  - **Change setting** - click to specify settings for a wireless local area network (WLAN). This option is active only when WLAN is selected as the TCP/IP setting. For more information about configuring settings for a WLAN, see section 3.2.4.1.
- **IP**
  - **Use DHCP** - click this radio button to enable the dynamic host configuration protocol (DHCP) for the device.
  - **Not Use DHCP** - click this radio button to disable the dynamic host configuration protocol (DHCP) for this device.
  - **IP Address** - specify an IP address for the device.
  - **Subnet** - specify a subnet address for the device.
  - **Gateway** - specify a network gateway.
  - **Max Conn.** - specify the maximum number of connections to allow.

- **Server**
  - **Use** - click this radio button to enable the server mode.
  - **Not use** - click this radio button do disable server settings.
  - **IP Address** - specify an IP address for the BioStar server.
  - **Server Port** - specify the port used to connect to the server.
- **RS485 Network**
  - **Mode** - set the mode for a device connected via RS485 (*Disable*, *Host*, or *Slave*). For more information about RS485 modes, see sections 3.2.1 and 3.2.2.
- **RS485**
  - **Baudrate** - set the baud rate for a device connected via RS485 (*9600* to *115200*).
- **RS232**
  - **Baudrate** - set the baud rate for a device connected via RS232 (*9600* to *115200*).
- **USB** - click the radio buttons to enable or disable the USB port on the FaceStation device.
- **USB Memory** - click the radio buttons to enable or disable the USB memory on the FaceStation device.

5.1.9.5 Access Control tab

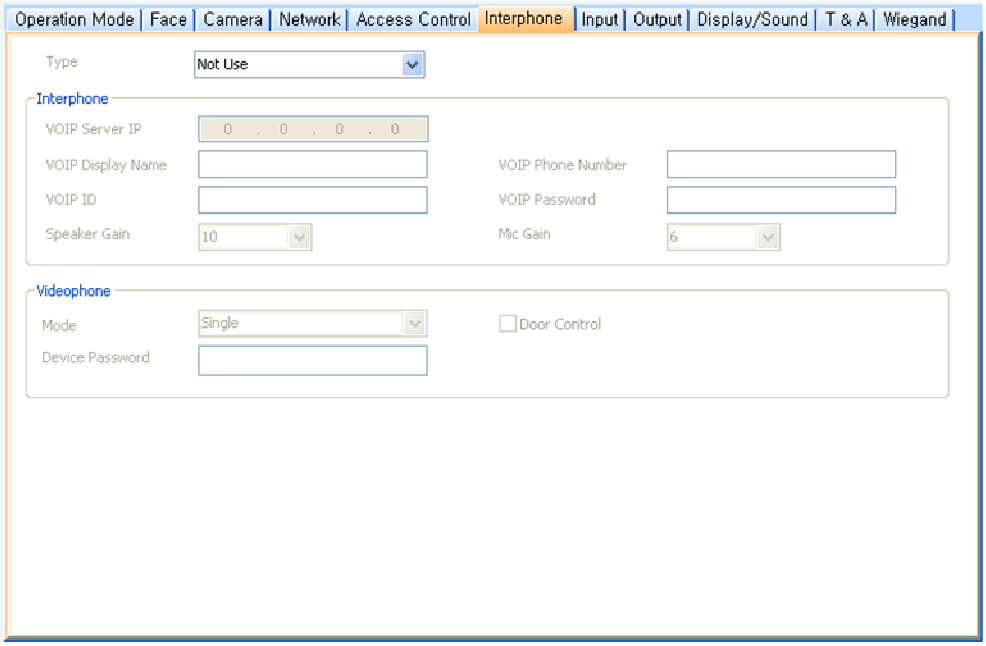
The Access Control tab allows you to customize entrance limit settings and default access groups for a FaceStation device.



- **Entrance Limit Setting**
  - **Timed APB (min)** - set the duration (in minutes) that a user will be unable to regain entry to an area via the device. Once a user has gained entry, the device will reject the user's ID, access card, or fingerprint authorization for the time period specified here.
  - **Option 1-4** - click the checkbox to enable an entrance limit setting, and then specify the effective hours for the entrance limit.
  - **Max Number of Entrance** - set the maximum number of entries allowed during the specified time limit.
- **Default Group Setting** - select a default access group to be applied to new users who have not been assigned to another access group.

5.1.9.6 Interphone tab

The Interphone tab allows you to set the device to act as an interphone to allow communication between people on either side of the door.



- **Type** – select one of the following options:
  - **Aanlogue Interphone** – choose this option to enable the analogue interphone.
  - **IP Interphone** – choose this option to enable the VoIP feature. A telephone is required.
  - **BioStar Videophone** – choose this option to enable the videophone feature that supports both video and voice calls. The supplied PC

software is required. The BioStar vidoephone works only with the device firmware version of FaceStation V1.0 or later.

When you select **IP Interphone** in the Type drop-down list, specify the following settings:

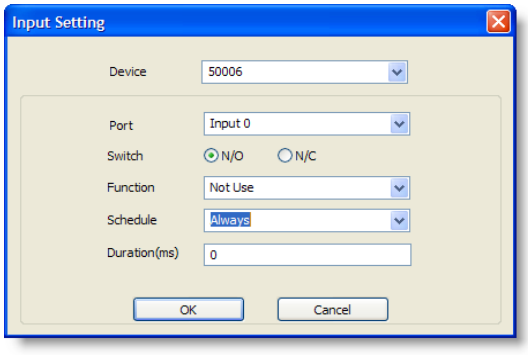
- **VOIP Server IP** – specify an IP address for VOIP server.
- **VoIP Display Name** – specify a name to use for communication through the interphone.
- **VoIP Phone Number** – specify a phone number for the interphone.
- **VoIP ID** – specify a user name to access the VoIP server.
- **VoIP Password** – specify a password to access the VoIP server.
- **Speaker Gain** – specify the volume of the speaker.
- **Mic Gain** – specify the volume of the microphone.

When you select **Videophone** in the Type drop-down list, specify the following settings:

- **Mode** – specify the videophone purpose (*Single* or *Extension*).
- **Door Control** – check this option if the videophone is used for door access.
- **Device Password** – enter the videophone device password.

5.1.9.7 Input tab

The input tab lists input settings you have specified for a FaceStation device. Buttons at the bottom of the tab allow you to add, modify, or delete input settings. To add or modify settings, you must specify them from the Input Setting window. For more information about configuring input settings, see section 3.10.3.2.

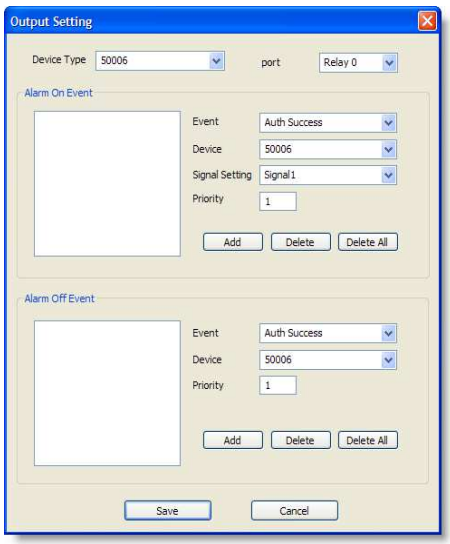


- **Device** - select the FaceStation device for which you will add or modify settings.
- **Port** - select an input port (Input 0, Input 1, or Tamper). For Secure I/O devices, these settings are available: Input 0, Input 1, Input 2, Input 3.
- **Switch** - click the radio buttons to specify the normal position of the input switch (N/O - normally open or N/C - normally closed).

- **Function** - select an action to associate with the input:
  - **Not Use** - the input port will not be monitored.
  - **Generic Input** - the input port will be monitored for a triggering action (events specified with “Detect Input 0-3” in the Output settings window—see section 5.1.1.6).
  - **Emergency Open** - open doors controlled by this device. The normal door open period will be ignored and doors will remain open until an operator sends a “Close Door” command via the Door/Zone Monitoring tab (see section 4.4.1).
  - **Release All Alarms** - cancel alarms associated with this device.
  - **Restart Device** - restart the device.
  - **Disable Device** - disable the device. A disabled device will not communicate with the BioStar server or process face or card inputs. To enable communication again, an administrator must provide authentication at the device.
- **Schedule** - set the schedule during which the inputs will be monitored (*Always* or *No Time*).
- **Duration (ms)** - set the duration (in milliseconds) an input signal must last to trigger the specified action.

5.1.9.8 Output tab

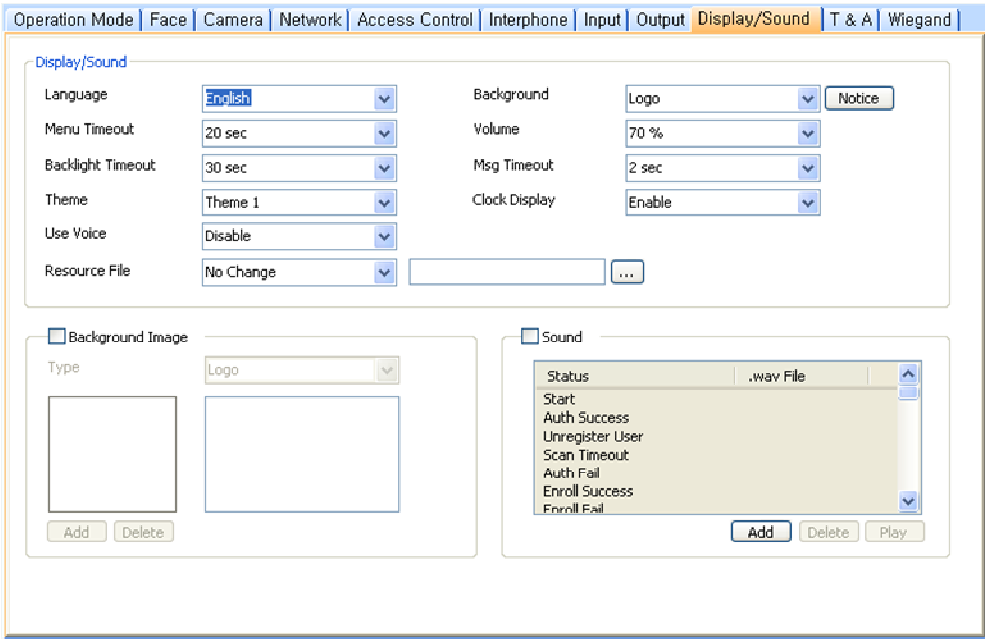
The Output tab lists output settings you have specified for a FaceStation device. Buttons at the bottom of the tab allow you to add, modify, or delete output settings. To add or modify settings, you must specify them from the Output Setting window. For more information about configuring output settings, see section 3.10.3.1.



- **Device Type** - select the device type for which you will add or modify settings.
- **Port** - select an output port (Relay 0). For Secure I/O devices, these settings are available: Relay 0 or Relay 1.
- **Alarm On Event** - specify settings and click **Add** to add the event to the Alarm On Event list. These events will activate an alarm.
  - **Event** - select an event that will activate an alarm (*Auth Success*, *Auth Fail*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, *Detect Input #1-3*).
  - **Device** - select the device to monitor for an alarm event.
  - **Signal Setting** - select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).
  - **Priority** - set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on (activate) event with a priority of 2 can be canceled only by an alarm off (deactivate) event with a priority of 1 or 2.
- **Alarm Off Event** - specify settings and click **Add** to add the event to the Alarm Off Event list. These events will deactivate an alarm.
  - **Event** - select an event that will deactivate an alarm (*Auth Success*, *Auth Fail*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input #1-3*).
  - **Device** - select the device to monitor for an alarm event.
- **Priority** - set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, a priority 2 “alarm on” event (activate) can be overridden only by an “alarm off” (deactivate) event with a priority of 1 or 2.

5.1.9.9 Display/Sound tab

The Display/Sound tab allows you to customize the FaceStation display and event sounds. To save changes to display or sound settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.



- **Display/Sound**
  - **Language** - set the language to use on the display (*Korean*, *English*, or *Custom*).
  - **Menu Timeout** - set the length of time before the display will return to the idle screen (*Infinite*, *10 sec*, *20 sec*, or *30 sec*).
  - **Backlight Timeout** – set the length of time before the display goes dim (*Infinite*, *10 sec*, *20 sec*, *30 sec, 40 sec, 50 sec,* or *60 sec*).
  - **Theme** - set a display theme (*Theme 1-4*)
  - **Use Voice** – set the device to notify you with voice messages (*Disable* or *Enable*).
  - **Resource File** – set the language resource file to use for the BioStar interface (*No Change*, *Korean*, *English*, or *Custom*). To use a language resource file other than English or Korean, select *Custom* and then click the ellipsis (...) button to locate the resource file..
  - **Background** - set the type of background for the FaceStation display (*Logo*, *Notice*, *Slide Show,* or *PDF*). Supported file types (JPG, GIF, BMP, PNG and PDF) cannot exceed 480x800 pixels each. Only

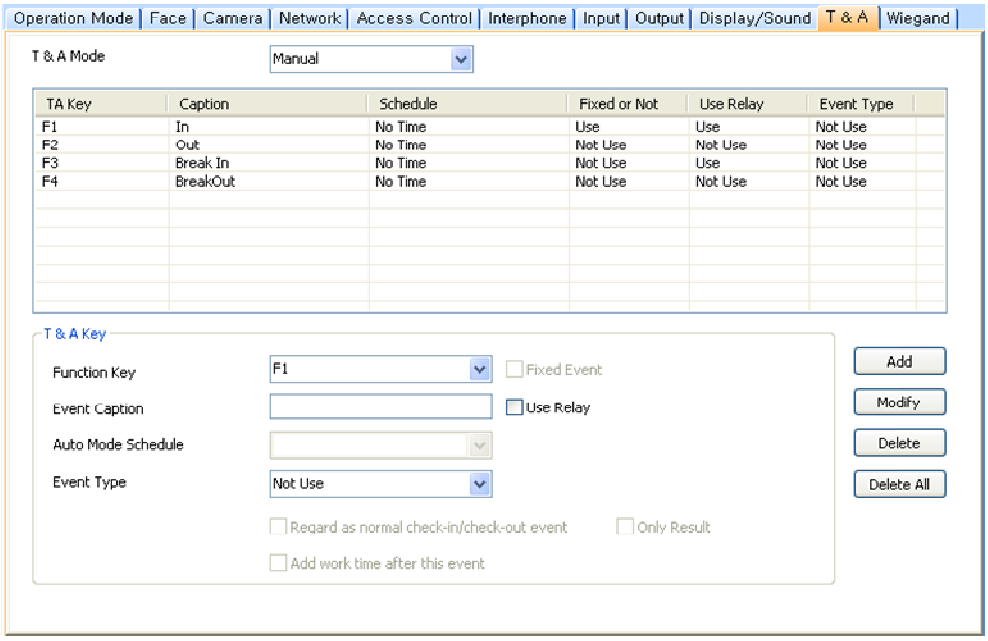
one image at a time can be used as a logo or notice, while up to 16 images can be displayed (at a set interval) in a slide show.

- **Volume** - set the volume of the FaceStation device (*0%* to *100%*).
- **Msg Timeout** - set the length of time that a failure or confirmation message will be displayed (*0.5-5 sec*).
- **Clock Display** - set to display the current time on the device (*Enable* or *Disable*).

- **Background Image** - click this checkbox to upload new background images. Click the plus sign (+) to locate and add a new image file.
  - **Type** - set the type of background for the FaceStation display (*Logo*, *Notice*, *Slide Show,* or *PDF*). Supported file types (JPG, GIF, BMP, PNG and PDF) cannot exceed 480x800 pixels for Notices and 480x800 pixels for Logos. Only one image at a time can be used as a logo or notice.
- **Sound** - click this checkbox to enable and add custom event sounds. Click an event from the list and then click the plus sign (+) to locate and add a new sound file. Click **Add** to add new sound files, **Delete** to remove sound files, or **Play** to preview a selected sound file.

5.1.9.10 T&A tab

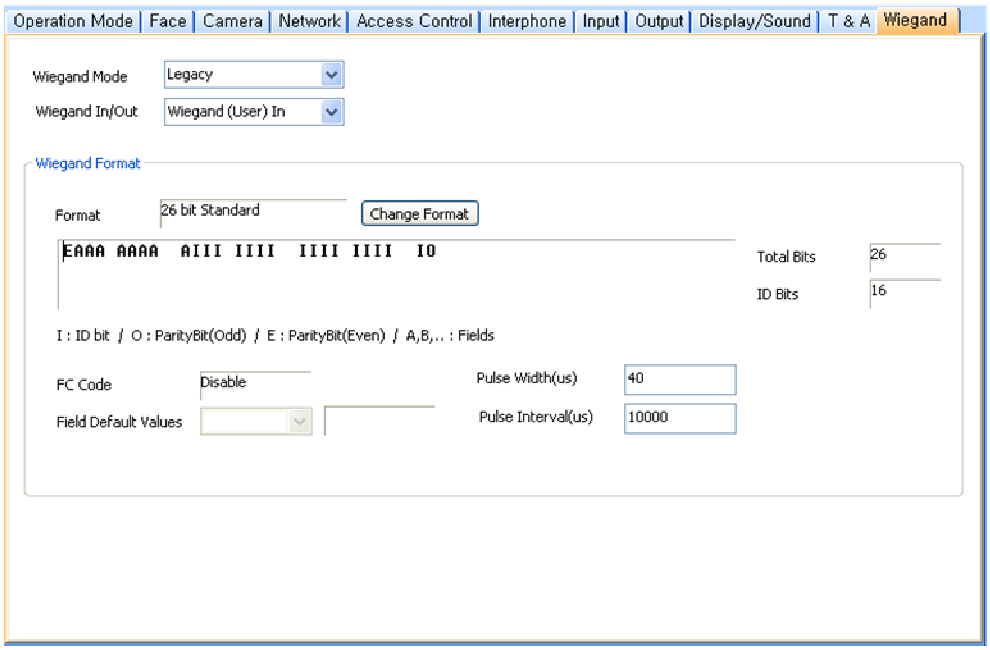
The T&A tab allows you to configure the mode and key settings for a FaceStation device. To save changes to time and attendance settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.



- **T&A Mode** - set the time and attendance mode:
  - **Not Use** - disable the time and attendance functions for this device.
  - **Manual** - users must press the specified key every time they enter or leave to record their T&A events.
  - **Manual Fix** - when a T&A key is pressed, the device will remain in that mode until a different T&A key is pressed.
  - **Auto change** - the device will automatically change T&A modes to correspond with the functions specified for a time period.
  - **Event Fix** - the device will perform only the specified T&A function.
- **T&A Key** - specify which keys to use for T&A events and the event types associated with them:
  - **Function Key** - select a function key from the drop-down list to assign a T&A event (*F1-F4*, *EXT01-EXT12)*. If you are using the Event Fix mode, you can click the checkbox to the right to designate a fixed event.
  - **Event Caption** - enter a caption for the event.
  - **Auto Mode Schedule** - when using the Auto Change mode, you can specify when the event will occur by selecting a timezone in the drop-down list. For more information on creating a timezone, see section 3.6.1.
  - **Event Type** - set the type of event to assign to the key (*Not Use*, *Check In*, *Check Out*, *In*, or *Out*). In/Out indicates the general check in/out events during a day whereas Check In/Out indicates the formal check in/out events upon arrival and departure at work—or the first check–in and the last check–out events on that day. When you choose Check In or Check Out, you can enable the "Regard as normal check-in/check-out event" option. If this option is enabled, users who activate the appropriate keys will be regarded as arriving or leaving on time at work even though they actually arrive late or leave early. If you enable the "Only Result" option, they appear being on time on T&A reports but their work time will be calculated correctly based on their actual check in/out time. If you choose *Out*, you can enable the "Add work time after this event" option. If this option is enabled, users activating the appropriate key will be considered working for the remainder of the time slot even if they leave the office early.

5.1.9.11 Wiegand tab

The Wiegand tab allows you to configure the Wiegand format for a FaceStation device. Click **Change Format** to launch the Wiegand Configuration wizard. For more information on configuring the Wiegand format, see section 3.2.12.



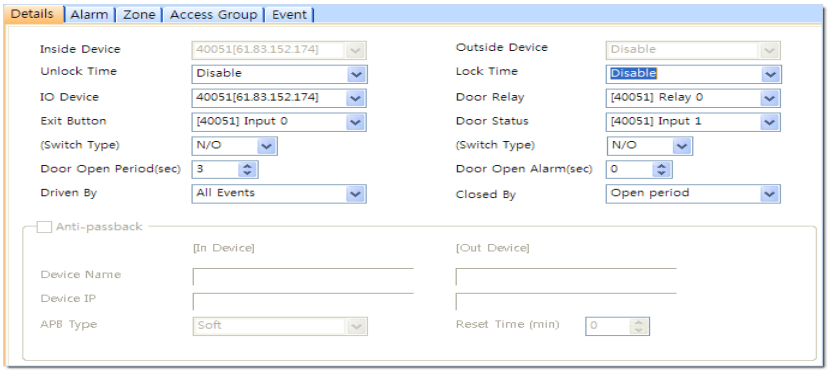
- **Wiegand Mode** - set the mode of Wiegand input to use when reading card ID data (*Legacy* or *Extended*). The Legacy mode will treat connected RF devices as part of their host devices (this is the typical function of previous versions of BioStar). The Extended mode will allow RF card readers to operate independently, which allows them to be associated with doors, included in zones, and leave logs with their own device IDs.
- **Wiegand In/Out** - assign the Wiegand input or output:
  - **Wiegand (User) In** - the ID field of the Wiegand string is interpreted as a user ID.
  - **Wiegand (Card) In** - the ID field of the Wiegand string is interpreted as a card ID.
  - **Wiegand (User) Out** - inserts the user ID of the authenticated user in the ID field of the Wiegand string.
  - **Wiegand (Card) Out** - inserts the card ID of the authenticated user in the ID field of the Wiegand string.

5.2 Customize Door Settings

The sections below describe the settings available for doors that have been added to the BioStar system. Customize the way these doors function by changing settings to suit your particular environment and operational needs. To access the tabs described below, click **Doors** in the shortcut pane, then click a door name.

5.2.1 Details tab

The Details tab allows you to specify which devices are used on the inside or outside of a door, how the devices control the door, and anti-passback features. When connecting two devices to a single door, the devices should be connected to each other by RS485. In this case, the I/O ports of only one device can be used. Specify which device's I/O ports to use in the "IO Device" drop-down list.



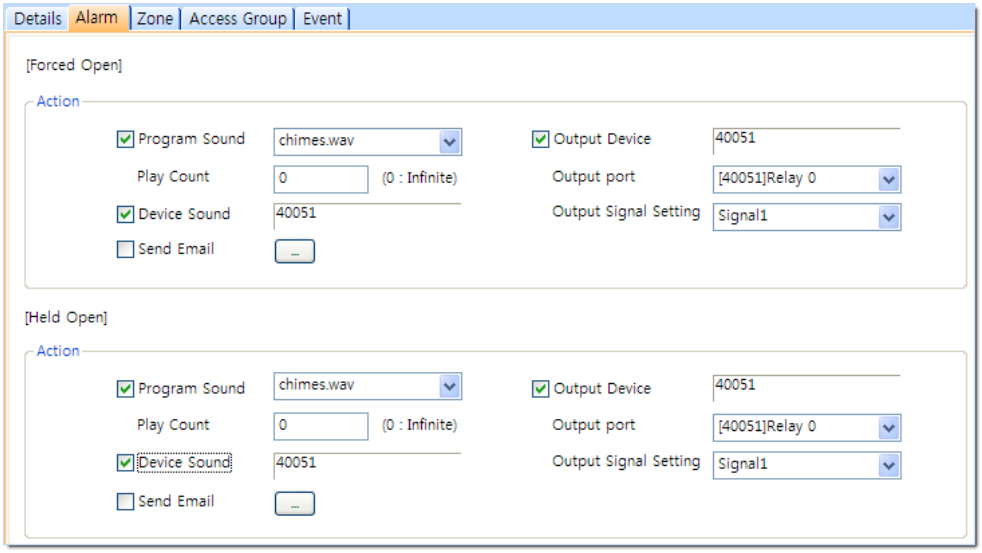
- **Inside Device** - select a device to use on the inside of the door.
- **Outside Device** - select a device to use on the outside of the door.
- **Unlock Time** - select a schedule when the door should normally be unlocked. During this time, door relays are active.
- **Lock Time** - select a schedule when the door should normally be locked. During this time, door relays are inactive.
- **IO Device** - when using two devices on a single door, specify which device's IO ports will be used.
- **Door Relay** - select a door relay.
- **Exit Button** - select a device input to use for an exit button (Disable or Input 0 and Input 1 for each device added).
- **(Switch Type)** - set the normal position of the input used for an exit button (*N/O-normally open* or *N/C-normally closed*).
- **Door Status** - set an input for a sensor that detects the current status of the door.
- **(Switch Type)** - set the normal position of the input used for a door status sensor (N/O-normally open or N/C-normally closed).

- **Door Open Period (sec)** - set the duration (in seconds) that a door relay should be activated when a door is opened. After this duration, the relay will stop sending the signal to open the door. The default is three seconds.
- **Door Open Alarm (sec)** - set the duration (in seconds) that a door can remain open before an alarm will sound.
- **Driven by** - select types of events that will trigger associated devices to open the door.
  - **All Events (default)** - associated devices will open the door on any successful authorization events.
  - **TNA + AUTH** - associated devices will open the door on successful T&A or credential authorization events or T&A authorization events. To use this option, you must select the Use Relay checkbox in the T&A tab. This option is only available for BioStation, BioLite Net, D-Station, X-Station, BioStation T2, and FaceStation devices. For more information about configuring T&A settings, see section 5.1.1.9, 5.1.3.8, 5.1.6.10, 5.1.7.9, 5.1.8.11, and 5.1.3.7.
  - **AUTH** - associated devices will open the door only on successful credential authorization events.
  - **TNA** - associated devices will open the door only on successful T&A authorization events. To use this option, you must select the Use Relay checkbox in the T&A tab. This option is only available for BioStation, BioLite Net, D-Station, X-Station, BioStation T2, and FaceStation devices. For more information about configuring T&A settings, see section 5.1.1.9, 5.1.3.8, 5.1.6.10, 5.1.7.9, 5.1.8.11, and 5.1.3.7.
  - **Disabled** - associated devices will not open the door, regardless of the attempted authorization events.
- **Closed by** - select an option for closing the door.
  - **Open period** - the BioStar system will close the door after the period specified in the *Door Open Period (sec)* field.
  - **Open period+Status** - the BioStar system will attempt to close the door based on door status (if you have connected door sensors and the system can detect that the door is open). If door sensors are not connected or the system is unable to detect the door status, the system will close the door after the period specified in the *Door Open Period (sec)* field. This setting is useful when used with revolving doors, for example, to prevent someone from following an authorized person through the door.
- **Anti-passback** - click the checkbox to activate the anti-passback feature (only available when using both an inside and an outside device).
  - **Device Name** - this field is populated automatically.

- **Device IP** - this field is populated automatically.
- **APB Type** - set the type of anti-passback restriction to use (Soft or Hard).
- **Reset Time (min)** - set the duration (in minutes) that must pass before the anti-passback status is reset. The default reset time is 0—at this setting, the anti-passback status will not be reset.

5.2.2 Alarm tab

The Alarm tab allows you to specify alarm actions for doors that are forced open or held open. A forced open alarm occurs when a door is forcibly opened without any authentication at the device. A held open alarm occurs when a door remains open longer than the duration specified in the system settings.



- **Action**
  - **Program Sound** - activate and select a sound from the drop-down list to be emitted by the BioStar program. Then, specify the duration ("play count") of the sound in seconds. If you set the Play Count to 0, the specified sound will play until someone with administrative privileges manually stops the sound via the Realtime Monitoring tab in the Monitoring pane. To add custom sounds to the list, see section 3.10.1.2.
  - **Device Sound** - activate and select a sound to be emitted by devices connected to the door.
  - **Send Email** - activate and setup emails to be sent by the system. For more information about sending alert emails, see section 3.10.2.
  - **Output Device** - activate and select a device to output an alarm signal.
  - **Output Port** - select an output port to use when sending the alarm signal.
  - **Output Signal** - select an output signal to send.

5.3 Customize Zone Settings

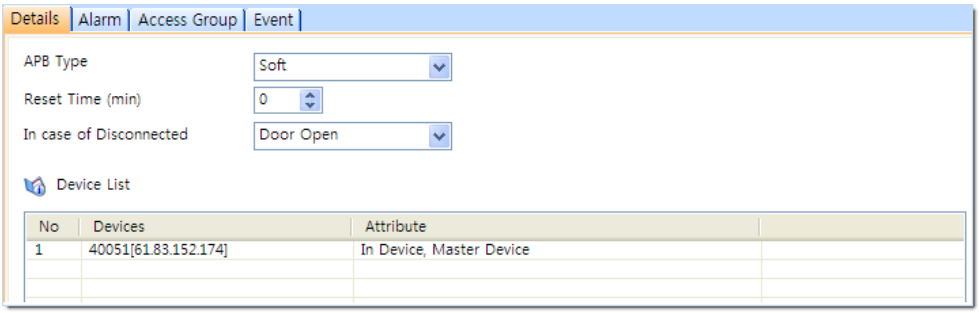
Customize the way zones function by changing the settings to suit your particular environment and operational needs. To access the tabs described below, click **Doors** in the shortcut pane, then click a zone name.

5.3.1 Customize Settings for Anti-Passback Zones

The sections below describe the settings available for anti-passback zones. Customize the way the zone functions by changing these settings to suit your particular environment and operational needs.

5.3.1.1 Details tab

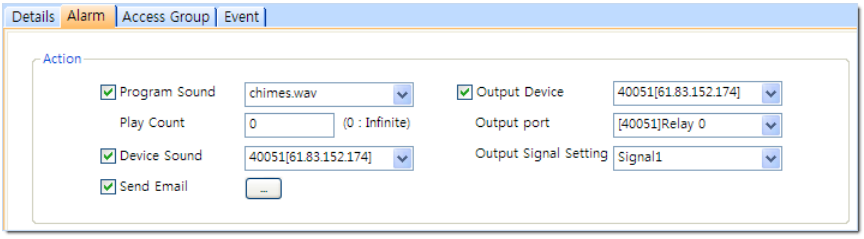
The Details tab allows you to specify which anti-passback type to use for a zone and the reset period for the anti-passback feature.



- **APB Type** - select a type of anti-passback restriction to apply (*Soft* or *Hard*).
- **Reset Time (min)** - set the duration (in minutes) that must pass before the anti-passback status is reset. The default reset time is 0—at this setting, the anti-passback status will not be reset.
- **In case of Disconnected** - set how doors in the zone should behave if communication is lost between the master and member devices.

5.3.1.2 Alarm tab

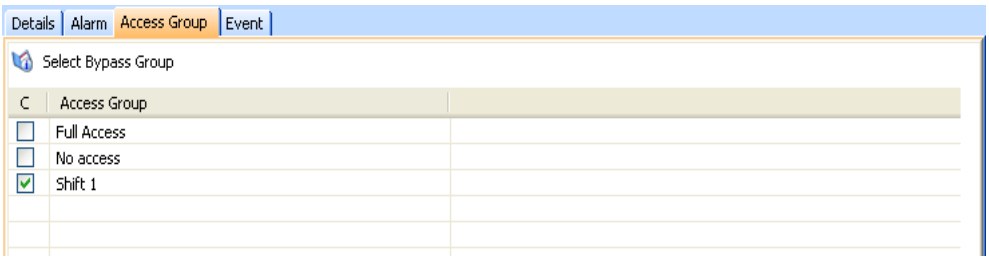
The Alarm tab allows you to specify alarm actions and an output device for an anti-passback zone.



- **Action**
  - **Program Sound** - activate and select a sound from the drop-down list to be emitted by the BioStar program. Then, specify the duration ("play count") of the sound in seconds. If you set the Play Count to 0, the specified sound will play until someone with administrative privileges manually stops the sound via the Realtime Monitoring tab in the Monitoring pane. To add custom sounds to the list, see section 3.10.1.2.
  - **Device Sound** - activate and select a sound to be emitted by devices connected to the door.
  - **Send Email** - activate and setup emails to be sent by the system. For more information about sending alert emails, see section 3.10.2.
  - **Output Device** - activate and select a device to output an alarm signal.
  - **Output Port** - select an output port to use when sending the alarm signal.
  - **Output Signal** - select an output signal to send.

5.3.1.3 Access Group tab

The Access Group tab allows you to specify access groups that can bypass normal restrictions for the zone. To grant bypass rights to an access group, select a group and click **Apply** at the bottom right of the Zone pane.

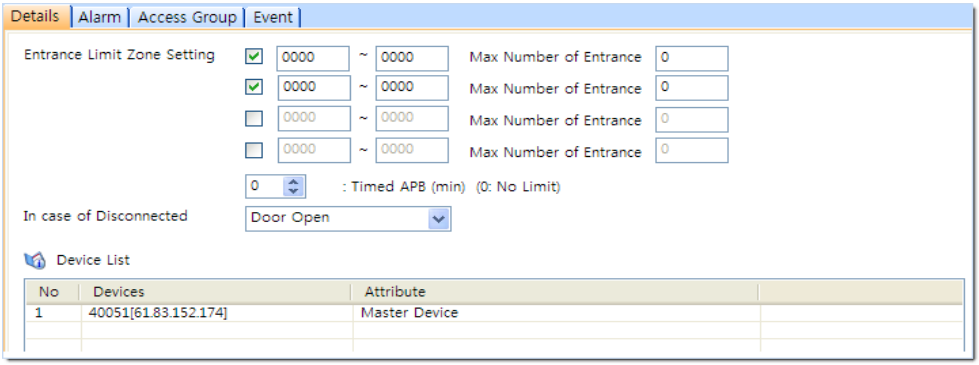


5.3.2 Customize Settings for Entrance Limit Zones

The sections below describe the settings available for entrance limit zones. Customize the way the zone functions by changing these settings to suit your particular environment and operational needs.

5.3.2.1 Details tab

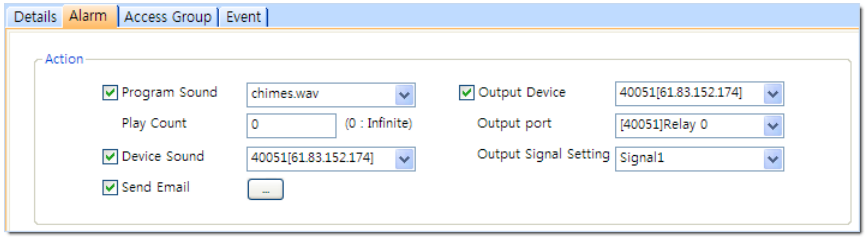
The Details tab allows you to specify entrance limits and a schedule for the zone restrictions.



- **Entrance Limit Zone Setting** - click the checkbox to enable an entrance limit setting, and then specify the effective hours for the entrance limit.
- **Max Number of Entrance** - set the maximum number of entries allowed during the specified time limit.
- **Timed APB (min)** - specify a time limit for re-entry into a zone.
- **In case of Disconnected** - set how doors in the zone should behave if communication is lost between the master and member devices.

5.3.2.2 Alarm tab

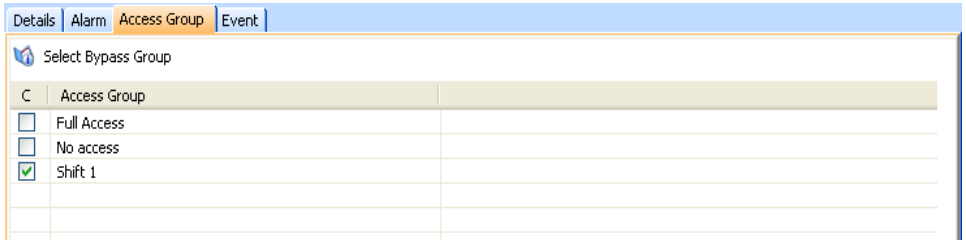
The Alarm tab allows you to specify alarm actions and an output device for an entrance limit zone.



- **Action**
  - **Program Sound** - activate and select a sound from the drop-down list to be emitted by the BioStar program. Then, specify the duration ("play count") of the sound in seconds. If you set the Play Count to 0, the specified sound will play until someone with administrative privileges manually stops the sound via the Realtime Monitoring tab in the Monitoring pane. To add custom sounds to the list, see section 3.10.1.2.
  - **Device Sound** - activate and select a sound to be emitted by devices connected to the door.
  - **Send Email** - activate and setup emails to be sent by the system. For more information about sending alert emails, see section 3.10.2.
  - **Output Device** - activate and select a device to output an alarm signal.
  - **Output Port** - select an output port to use when sending the alarm signal.
  - **Output Signal** - select an output signal to send.

5.3.2.3 Access Group tab

The Access Group tab allows you to specify access groups that can bypass normal restrictions for the zone. To grant bypass rights to an access group, select a group and click **Apply** at the bottom right of the Zone pane.

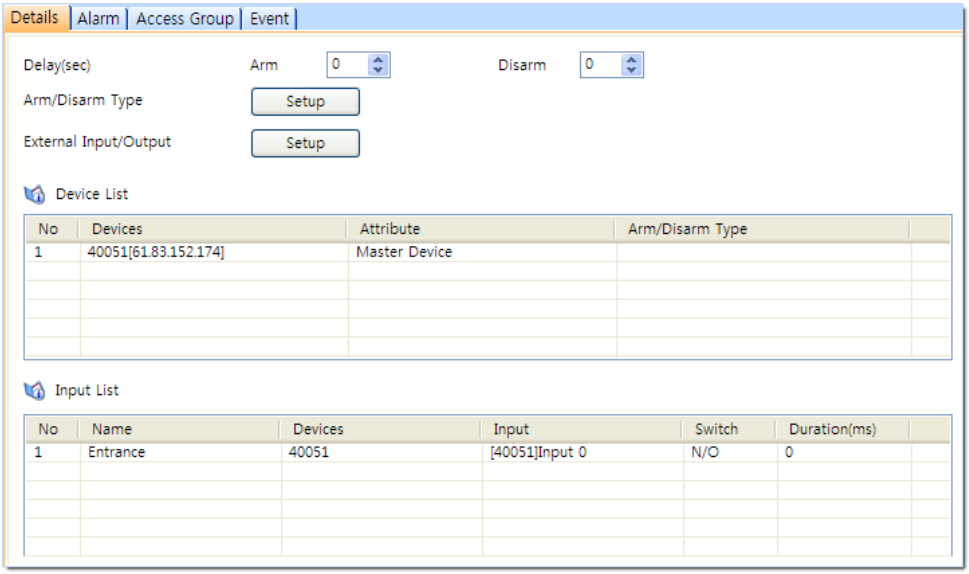


5.3.3 Customize Settings for Alarm Zones

The sections below describe the settings available for alarm zones. Customize the way the zone functions by changing these settings to suit your particular environment and operational needs.

5.3.3.1 Details tab

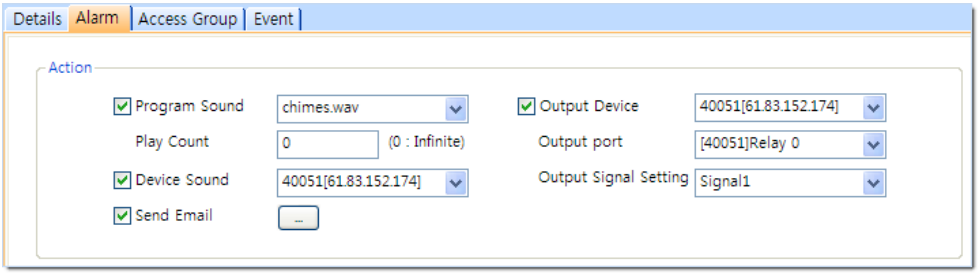
The Details tab allows you to specify alarm delays and arm/disarm types for alarm zones.



- **Delay (sec)**
  - **Arm** - set the length of time (in seconds) to delay before arming the zone.
  - **Disarm** - set the length of time (in seconds) to delay before disarming the zone.
- **Arm/Disarm Type** - specify settings for arming or disarming zones. For more information for configuring arm and disarm settings, see 3.5.2.5. For more information on setting up alarms, see section 3.10.
- **External Input/Out** - specify settings for enabling the BioStar system to antomatically arming or disarming zones. For more information on configuring external input/output settings, see 3.5.2.6. For more information on setting up alarms, see section 3.10.

5.3.3.2 Alarm tab

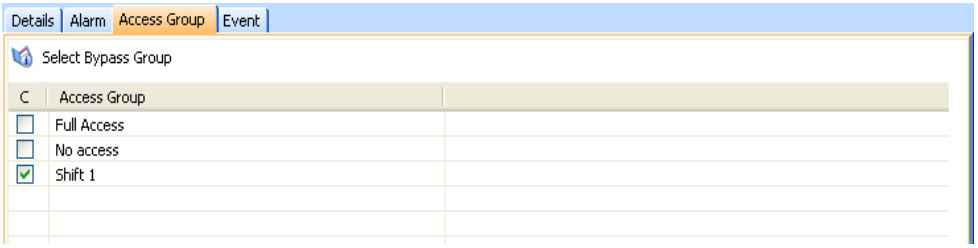
The Alarm tab allows you to specify alarm actions and an output device for an alarm zone.



- **Action**
  - **Program Sound** - activate and select a sound from the drop-down list to be emitted by the BioStar program. Then, specify the duration ("play count") of the sound in seconds. If you set the Play Count to 0, the specified sound will play until someone with administrative privileges manually stops the sound via the Realtime Monitoring tab in the Monitoring pane. To add custom sounds to the list, see section 3.10.1.2.
  - **Device Sound** - activate and select a sound to be emitted by devices connected to the door.
  - **Send Email** - activate and setup emails to be sent by the system. For more information about sending alert emails, see section 3.10.2.
  - **Output Device** - activate and select a device to output an alarm signal.
  - **Output Port** - select an output port to use when sending the alarm signal.
  - **Output Signal** - select an output signal to send.

5.3.3.3 Access Group tab

The Access Group tab allows you to specify access groups that can arm and disarm zones. To grant disarm authorization to an access group, select a group and click **Apply** at the bottom right of the Zone pane.

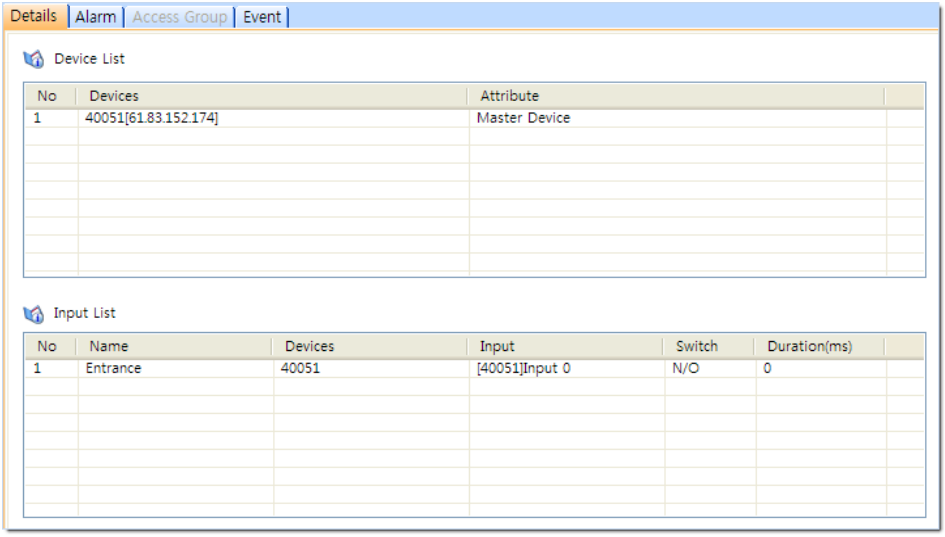


5.3.4 Customize Settings for Fire Alarm Zones

The sections below describe the settings available for fire alarm zones. Customize the way the zone functions by changing these settings to suit your particular environment and operational needs.

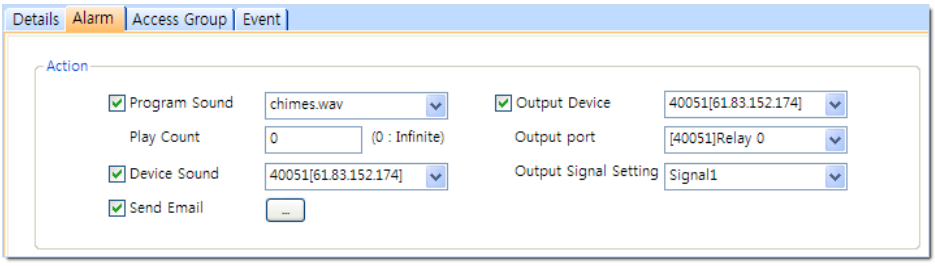
5.3.4.1 Details tab

The Details tab allows you to add or delete devices in the Device List and inputs to the Input List. To add or delete devices, see section 3.5.2.2.



5.3.4.2 Alarm tab

The Alarm tab allows you to specify alarm actions and an output device for a fire alarm zone.



- **Action**
  - **Program Sound** - activate and select a sound from the drop-down list to be emitted by the BioStar program. Then, specify the duration ("play count") of the sound in seconds. If you set the Play Count to 0, the specified sound will play until someone with administrative privileges manually stops the sound via the Realtime Monitoring tab in the Monitoring pane. To add custom sounds to the list, see section 3.10.1.2.

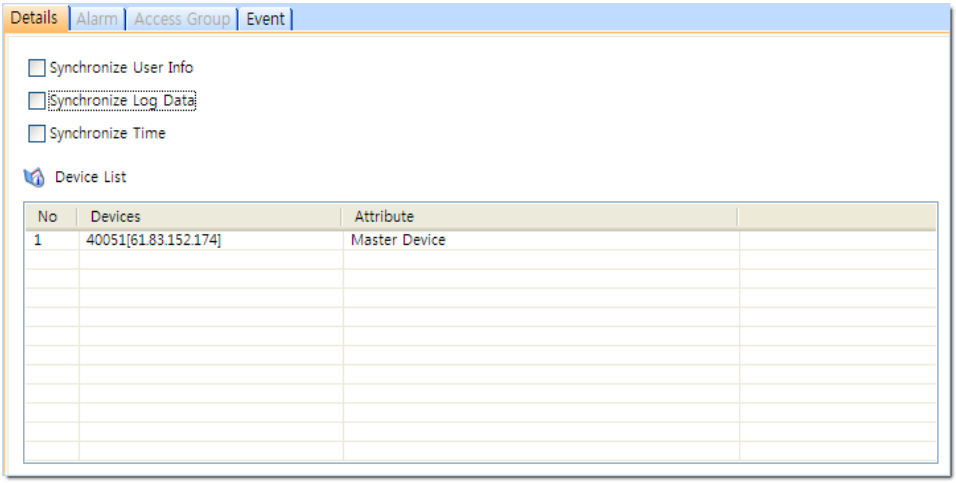
- **Device Sound** - activate and select a sound to be emitted by devices connected to the door.
- **Send Email** - activate and setup emails to be sent by the system. For more information about sending alert emails, see section 3.10.2.
- **Output Device** - activate and select a device to output an alarm signal.
- **Output Port** - select an output port to use when sending the alarm signal.
- **Output Signal** - select an output signal to send.

5.3.5 Customize Settings for Access Zones

The sections below describe the settings available for access zones. These zones are used to synchronize user data, so the Alarm and Access Group tabs are unavailable. Customize the way the zone functions by changing these settings to suit your particular environment and operational needs.

5.3.5.1 Details tab

The Details tab allows you to add devices to the Device List.



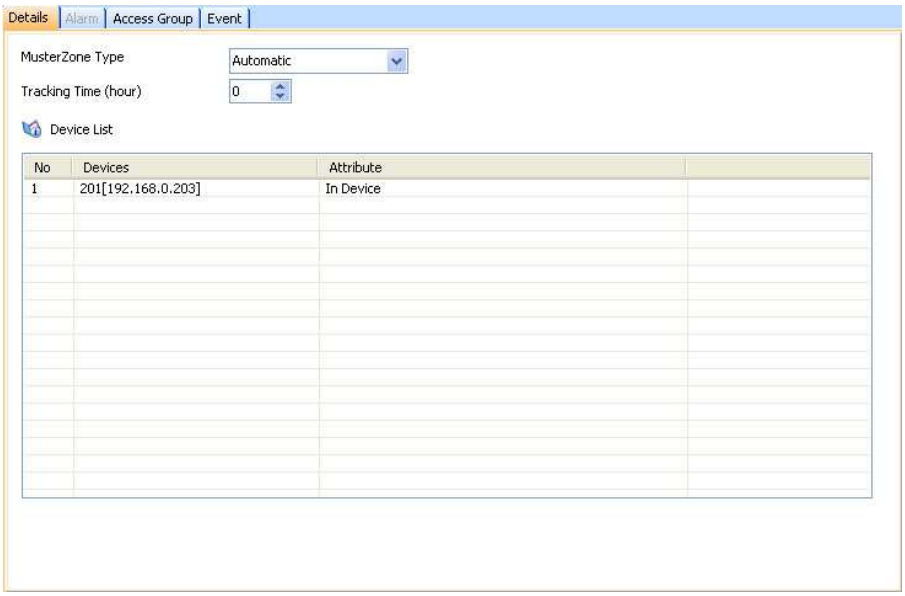
- **Synchronize User Info** - click this checkbox to automatically propagate user information to other devices.
- **Synchronize Log Data** - click this checkbox to automatically write all log records to the master device (for member devices in the zone).
- **Synchronize Time** - click this checkbox to synchronize the time of devices in the zone.

5.3.6 Customize Settings for Muster Zones

The sections below describe the settings available for muster zones. These zones are used to monitors user locations, so the Alarm tab is unavailable. Customize the way the zone functions by changing these settings to suit your particular environment and operational needs.

5.3.6.1 Details tab

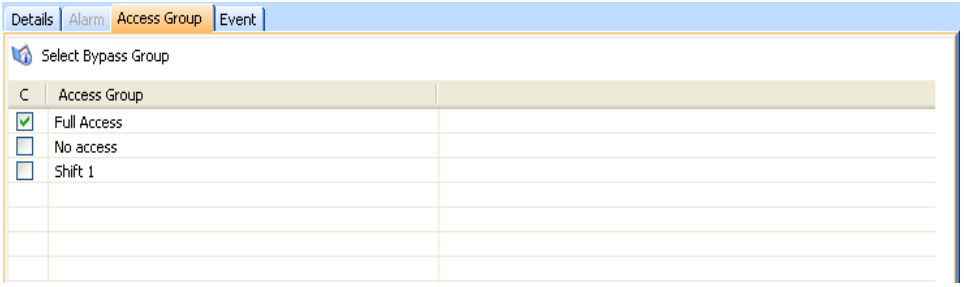
The Details tab allows you to add devices to the Device List.



- **Muster Zone Type** - set the type of monitoring to perform (*automatic* or *manual*).
- **Tracking Time (hour)** - set the number of hours to monitor the zone.

5.3.6.2 Access Group tab

The Access Group tab allows you to specify access groups that can arm and disarm zones. To grant disarm authorization to an access group, select a group and click **Apply** at the bottom right of the Zone pane.



5.3.7 Customize Settings for Interlock Zones

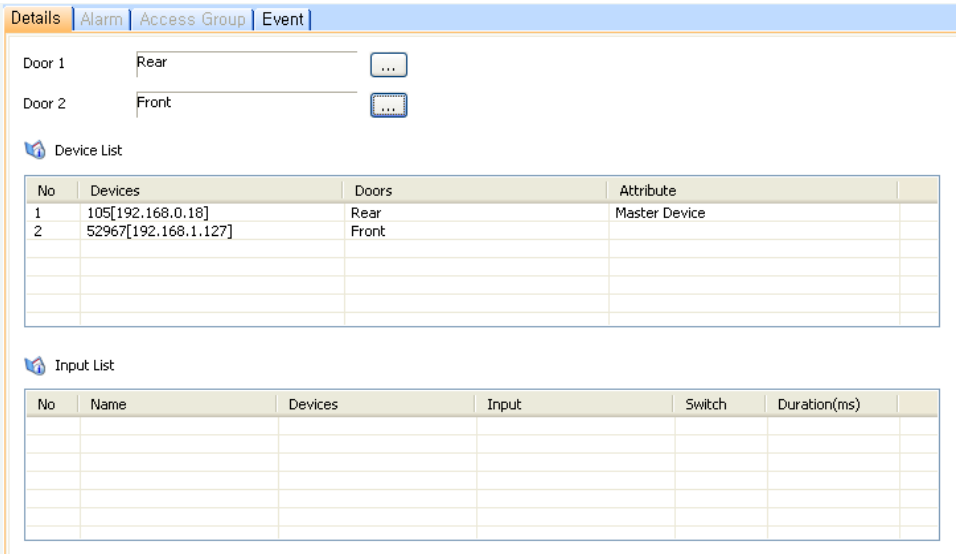
The sections below describe the settings available for interlock zones. Customize the way the zone functions by changing these settings to suit your particular environment and operational needs.

Interlock zones works only with the following device firmware versions:

- BioStation V1.9 or later, BioEntry Plus V1.5 or later, BioEntry W V1.0 or later, BioLite Net V1.3 or later, and Xpass V1.2 or later.
- BioStation T2 and X-Station devices do not support interlock zones.

5.3.7.1 Details tab

The Details tab allows you to specify which doors to use for either side of the interlock zone. Once added, the door names and device IDs will appear in the Device List.



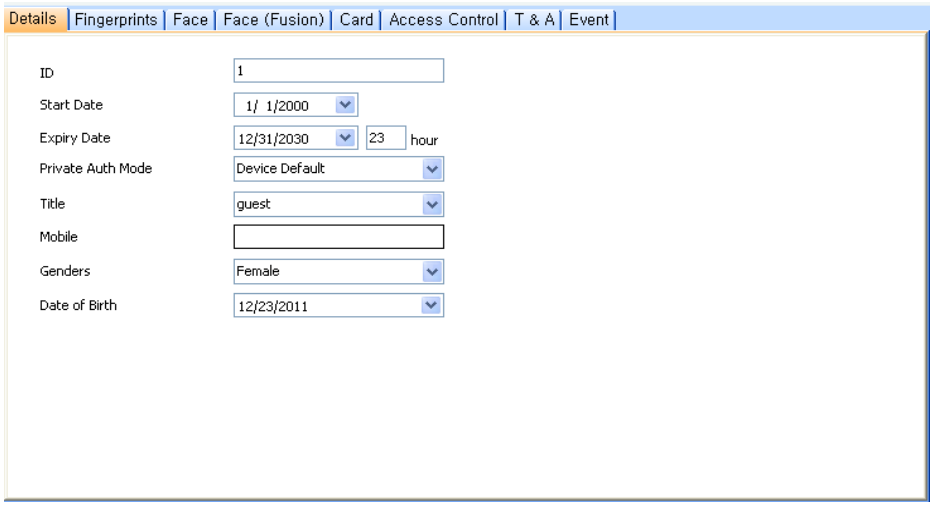
- **Door 1** - click the ellipsis (...) button to select door 1 of the interlock area. Doors without associated devices cannot be added to the interlock zone.
- **Door 2** - click the ellipsis (...) button to select the device on door 2 of the interlock area. Doors without associated devices cannot be added to the interlock zone.

5.4 Customize User Settings

Customize various settings for users, including personal details, fingerprint information, and access card information. To access the tabs described below, click **Users** in the shortcut pane, then click a user name.

5.4.1 Details Tab

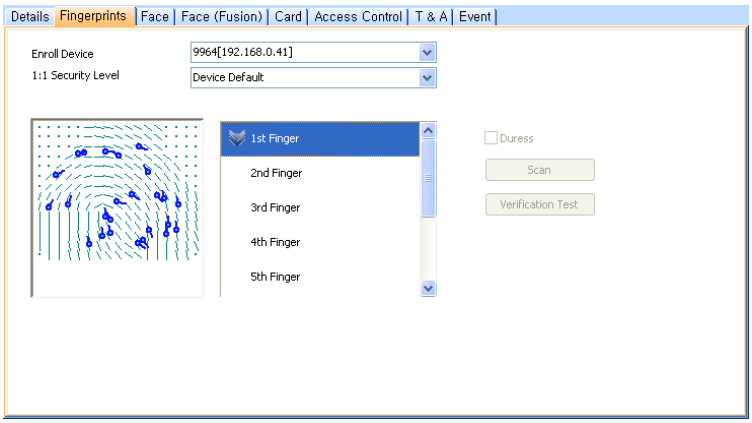
The Details tab allows you to specify personal information about a user and the valid dates of a user account. To edit these fields, see section 4.4.3.



- **ID** - enter an identification number for a user.
- **Start Date** - set a beginning date that the user can obtain authorization via the BioStar system.
- **Expiry Date** - set a date that the user's account will expire (you can also specify the hour that the account will expire).
- **Private Auth Mode** - set the authorization method for the user (*Device Default*, *Fingerprint*, *Fingerprint + Password*, *Card Only*, *Card + Fingerprint*, *Card + Password*, *Card + Fingerprint/Password*, *Card + Fingerprint + Password*, *ID + Fingerprint*, *ID + Password*, *ID + Fingerprint/Password*, *ID + Fingerprint + Password*). If you set the method to "Device Default," the authentication mode will be determined by operation mode settings of the device.
- **Title** - select a title for the user (*Guest*, *President*, *Director*, *General Manager*, *Chief*, *Assistant Manager*, or custom title).
- **Mobile** - enter a mobile telephone number for a user.
- **Genders** - select a user's gender.
- **Date of Birth** - select a user's date of birth from the drop-down calendar.

5.4.2 Fingerprints Tab

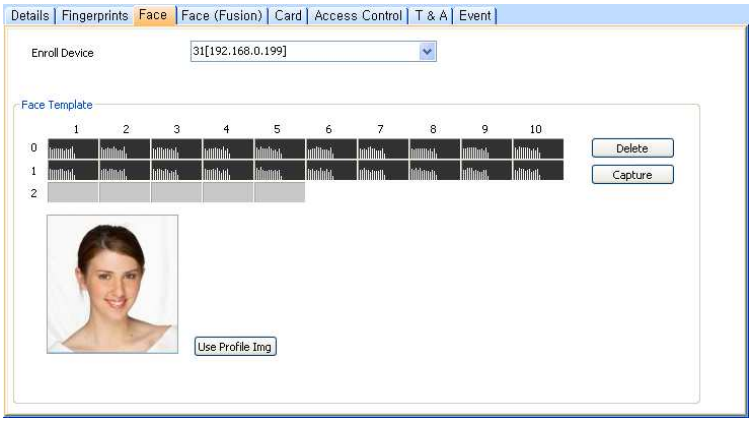
The Fingerprints tab allows you to specify which type of scanner to use for enrollment and the security level to apply. This tab can also be used to test for fingerprint matches and register duress fingerprints. For more information about registering fingerprints, see section 3.6.2.



- **Enroll Device** - select a device to use for scanning fingerprints.
- **1:1 Security Level** - select a security level to use for fingerprint authorization (*Device Default* and *Lowest [1/ 1,000]* to *Highest [1/ 10,000,000]*). Keep in mind that as the security level is increased, so too is the likelihood of a false rejection.
- **Duress** - set a fingerprint template to be used as a duress finger (the duress finger will activate alarms when used to gain entry).

5.4.3 Face Tab

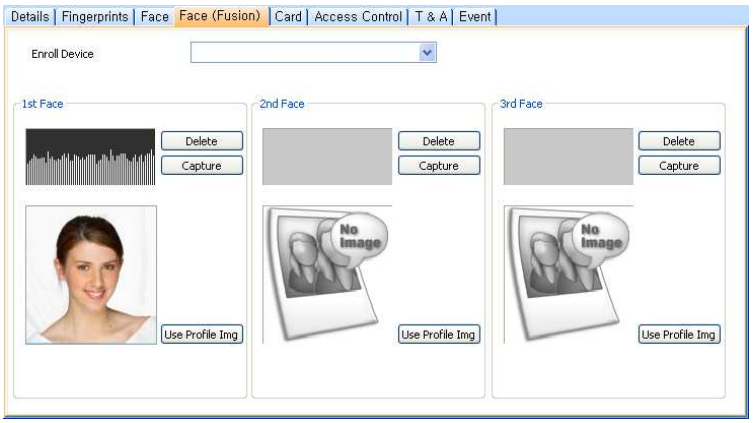
The Face tab allows you to specify a FaceStation device to use for storing face templates of users. When you sucessfully capture a face image, the FaceStation device transfers 25 face templates to the BioStar. During authentication, any face template that receives a higher score than one of the registered face templates will replace the old one. For more information about capturing face images, see section 3.6.3.



- **Enroll Device** - select a device to use for capturing face images.

5.4.4 Face (Fusion) Tab

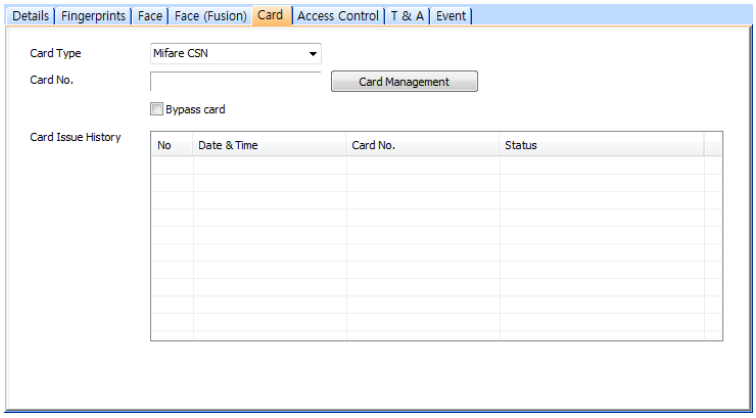
The Face tab allows you to specify a D-Station device to use for capturing face images of users. For more information about capturing face images, see section 3.6.3.



- **Enroll Device** - select a device to use for capturing face images.

5.4.5 Card Tab

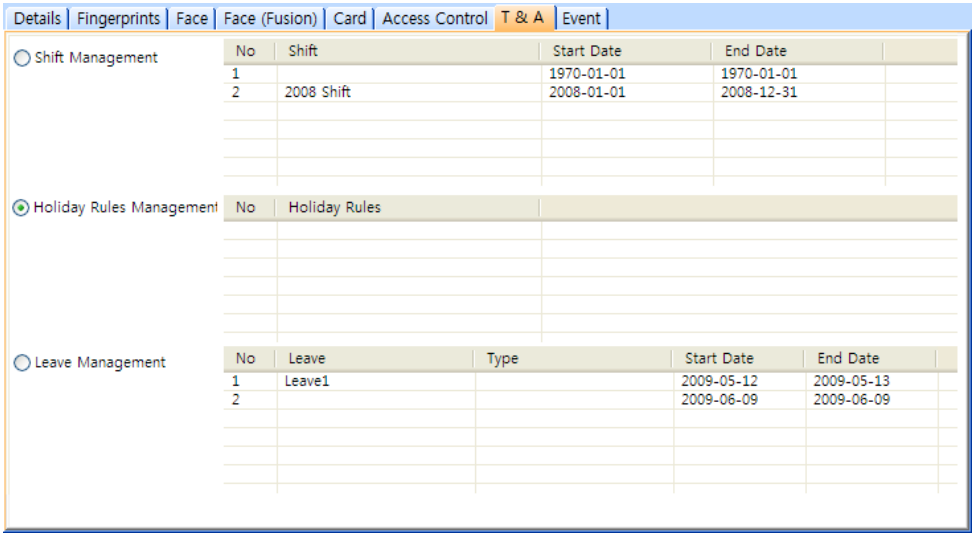
The Card tab allows you to specify card types and IDs and issue cards to users. For more information about issuing cards, see section 3.6.3.



- **Card Type** - select a type of access card to issue (*Mifare CSN*, *Mifare Template*, *EM 4100*, *HID Prox*, *iCLASS CSN*, or *iCLASS Template*).
- **Card ID** - displays the card ID number when a card is issued.
- **Custom ID** - enter a custom ID for the card.

5.4.6 T&A Tab

The T&A tab allows you to specify which shifts, holiday rules, and leave periods apply to a user. To add new details, click **Add** at the bottom of the tab. To save changes to time and attendance settings, you must click **Apply** at the bottom of the tab. You can also remove entries by highlighting the entry and clicking **Delete**. For more information about configuring time and attendance, see section 3.9.



- **Shift Management** - specify which shifts apply to the user.
- **Holiday Rules Management** - specify which holiday rules apply to the user.
- **Leave Management** - specify leave for the user.

06 Solve Problems

If you experience problems with the BioStar software, contact Suprema's technical support by email: **support@supremainc.com**. When composing an email to technical support, please include the following:

- Which BioStar version you are using.
- Which Suprema devices are affected by the problem, if any.
- The error message you are receiving, if any.
- A complete (but concise) description of the problem you are experiencing.
- Your name and title.
- Your contact information.
- The best time and method to reach you

Glossary

access card - A card that can be used to grant or restrict access to a specific area. BioStar supports MIFARE®, EM4100, HID proximity, iCLASS®, and FeliCa® cards. See also: proximity card.

access control system - A system of physical mechanisms and controls that permit or deny access to a particular resource or physical area. BioStar is an IP-based biometric access control system.

alarm zone - A grouping of devices that is used to protect a physical area. BioStar monitors input points in an alarm zone and triggers alarms when intrusion or tampering is detected.

anti-passback - A security protocol that prevents a user from providing unauthorized entrance to another user via an access card or fingerprint. See also: timed anti-passback.

biometrics - Biometrics refers to the use of physical characteristics for verification or authorization. BioStar incorporates Suprema's award-winning fingerprint recognition technology to provide biometric authentication of a user's identity and authorization to gain access to restricted areas.

bypass group - A group of users that can bypass normal restrictions for a zone.

client - BioStar client software allows an operator to connect remotely to the BioStar server and control connected devices. An operator ID and password are required to access the system via a client.

department - A division of an organization used to group employees. The use of departments is not necessary, but may be helpful to organize large numbers of employees.

device - In this guide, the word "device" refers to any Suprema product supported by the BioStar system. Supported devices include BioStation, BioStation Mifare, BioStation HID, DStation, BioEntry Plus/BioEntry W, BioEntry Plus Mifare/BioEntry W Mifare, BioEntry

Plus iCLASS, BioEntry Plus HID, BioLite Net, Xpass, and BioMini USB terminals, as well as the Secure I/O device.

distributed intelligence - In the BioStar system, the authorization database is distributed to each terminal, so that authorization is faster and can continue even when other parts of the system are offline.

door - Doors are the physical barriers that provide entry into a building or space. At least one device must be connected to a door to provide access control, but two devices can be connected to support anti-passback and other features, such as door relays, alarm relays, exit switches, and sensors.

duress finger - This term refers to an enrolled fingerprint that will activate silent alerts when a candidate is under duress. In the typical duress scenario, a perpetrator forces the candidate to gain access by force or threat of harm. The candidate gains access by means of his or her "duress finger," which allows access and simultaneously triggers the alarm or alert actions you specify.

enrollment - The process of creating a user account and capturing images of fingerprints or issuing access cards.

entrance limit - The maximum number of times a user can gain authorization to a specific area. The entrance limit can be related to a time period so that users are limited to certain number of entries during office hours, for example.

ESSID - Extended Service Set ID. The ESSID is the name of a wireless network access point. It allows one wireless network to be clearly distinguishable from another. ESSID is one type of SSID (the other being BSSID).

face recognition -The automated process of validating a claimed identity based on the image of a face. BioStar extracts and analyzes the facial features such as the skin texture and the shapes of the face, eyes, nose and mouth from a captured face image and compares them with those of all the registered persons.

false acceptance rate - The false acceptance rate (FAR) is a measure of the likelihood that a biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR typically is stated as the ratio of the number of false acceptances to the number of identification attempts.

false rejection rate - The false rejection rate (FRR) is a measure of the likelihood that a biometric security system will incorrectly reject an access attempt by an authorized user. A system's FRR is typically stated as the ratio of the number of false rejections to the number of identification attempts.

fingerprint recognition -The automated process of matching two human fingerprints: one previously recorded and one being provided by a user for authentication. BioStar incorporates Suprema's award-winning algorithms for recognizing fingerprints.

Glossary

fingerprint sensor - A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for fingerprint recognition.

fire alarm zone - A zone that is used to interface with fire alarms and control doors when a fire is detected.

host - A host is the device that serves as the master in a RS485 network. The host device relays data packets between external devices (or a larger network) and slave devices connected to the RS485 network.

input signal - The signal sent to a device by an external object, such as an exit button.

operator - Operators are personnel who have rights to use BioStar clients. BioStar includes three pre-defined classes for operators: administrators, operators, and managers. BioStar also supports a maximum of 16 custom operator classes.

output signal - The signal sent to an external device, such as an alarm siren or electronic door strike.

proximity card - Proximity cards (or "prox" cards) are contactless integrated circuit devices used for security access. BioStation, BioEntry Plus, and BioLite Net devices support EM4100 cards; BioStation Mifare, BioEntry Plus Mifare, BioEntry W Mifare and BioLite Net, and DStation devices support MIFARE and iCLASS cards; and BioStation HID and BioEntry Plus HID devices support HID proximity cards.

RF device - Short-range radio frequency devices used to gain access to doors. The BioStar system allows 3rd party RF devices to be added to the system to incorporate existing hardware into the access control configuration

security level - see: *false acceptance rate.*

time and attendance (T&A) - This designation refers to the processes and functions that monitor and report check-in and check-out activities by employees and allow administrators to define time slots and schedules. The information collected by the BioStar system can be used in conjunction with external systems for time reporting and payroll capabilities.

timed anti-passback - A security protocol that prevents reauthorization of a user for a specified period of time. See also: *anti-passback.*

timezone - A customizable schedule that can be used to allow or restrict access during specified hours. Timezones can combined with doors to create access groups.

user - A user is any person who has access rights. A user's access rights are comprised of individual rights (user level), membership in access groups, and time restrictions.

Glossary

Wiegand interface - The Wiegand interface is a wiring standard used to connect a card swipe mechanism to the rest of an electronic entry system. The interface uses three wires, one of which is a common ground and two of which are data transmission wires usually called DATA0 and DATA1, but sometimes also labeled Data High and Data Low.

zone - A zone consists of two or more devices that are grouped together. BioStar includes seven types of zone classifications.

Index

Index

Index

Index

U

V

W

X

Z

suprema
BioStar

Suprema Inc.
16F Parkview Office Tower, Jeongja, Bundang, Seongnam, Gyeonggi, 463-863 Korea
Tel: +82-31-783-4502 **Fax**: +82-31-783-4503
Email: sales@supremainc.com **Homepage**: www.supremainc.com