APRO WEB

Software web di controllo accessi

MANUALE UTENTE

Le informazioni incluse nel presente documento sono di proprietà di A PLUS S.r.l. e possono essere soggette a modifica, senza necessità di autorizzazione da parte del cliente, che riceverà comunicazione della stessa secondo le modalità previste dal contratto.

A PLUS S.r.l. non è responsabile di eventuali danni, diretti o indiretti, che potrebbero essere causati dall'uso improprio del materiale a cui si riferisce la presente specifica tecnica.

È vietato riprodurre, tradurre, modificare o divulgare, in tutto o in parte, il contenuto del presente documento, senza preventiva autorizzazione scritta di A PLUS S.r.l.

Versione 2.2

Per informazioni e supporto contattare:

A PLUS S.r.l.
Via G.B. Vico, 45/B
50053 - Empoli (FI)
Tel. +39 0571 920442 - Fax +39 0571 920474
P.IVA: 06780430481 / REA: FI-655673

info@aplus.srl

Indice

1. Descrizione APRO WEB 5
1.1. Requisiti minimi 5
1.2. Installazione 5
1.2.1. Installazione Microsoft SQL Server 6
1.2.2. Installazione/Aggiornamento database 9
1.2.3. Installazione/Aggiornamento ADM, APRO WEB service e AxWin6 Client 11
1.2.4. Deployment di APROWEB come ISAPI module all'interno del web server IIS 15
1.3. Licenza 26
1.3.1. Licenza Hardware 26
1.3.2. Licenza software 27
1.3.3. Versionamento e specifiche licenza 28
1.3.4. Ampliamenti delle funzionalità caricate in licenza 29
1.3.5. Conversione da sistema AxWin6 a APRO WEB 30
1.4. Backup/Restore Database 31
1.4.1. Backup Database 31
1.4.2. Restore Database 32
2. Software per configurare i terminali: ADM 35
2.1. Creazione/Modifica terminali 36
2.1.1. Terminali LM2002, LMIP, LEGGO® 2000 e LMUP 36
3. Finestra eventi 58
4. Interfaccia WEB Utente: APRO WEB 59
4.1. Credenziali di accesso 59
4.2. Creazione Fasce Orarie 61
4.3. Creazione Gruppi 63
4.4. Creazione Profili 67
4.5. Creazione Utenti 68
4.5.1. Finestra utente: Dettagli 70
4.5.2. Finestra utente: Dettagli-Personal Profile 72
4.5.3. Finestra utente: Maggiori dettagli 73
4.5.4. Finestra utente: Storico operazioni 74
4.5.5. Finestra utente: Eventi 74
4.5.6. Utenti/Lettori e Utenti/Ascensori 74
4.6. Creazione Sedi 78
4.7. Creazione Aziende 79

4.8. Visualizzazione storico eventi 80
4.9. Visualizzazione storico operazioni 81
4.10. Presenti 82
4.10.1. Regole 82
4.10.2. Presenti 83
4.11. Account 84
4.11.1. Regole 84
4.11.2. Operatori 85
4.12. Modulo integrazione TrakaWEB 86
4.12.1. Caratteristiche 86
4.12.2. Abilitazione e configurazione 87
4.12.3. Disabilitazione e cancellazione codici 90

1. Descrizione APRO WEB

APRO WEB è un software per il controllo accessi WEB, l'utente finale/manutentore è in grado di accedere attraverso i comuni browser all'interfaccia WEB, senza la necessità di installare nessun tipo di applicazione sulla propria macchina (PC o dispositivo mobile).

APRO WEB rappresenta il nuovo client di configurazione e visualizzazione delle funzionalità di controllo accessi messe a disposizione dal sistema hardware e software fornito da A PLUS.
Il sistema APRO WEB si compone dei seguenti applicativi, da installare solo sul server centrale:

- APRO WEB Service: insieme di servizi e framework per l'esecuzione del web server a cui poter accedere dai client browser;
- ADM: software per la configurazione e la comunicazione con i terminali;
- Microsoft SQL Server, all'interno del quale viene creato il database "AxWinDB", installabile nella stessa macchina in cui risiede ADM, oppure su un'altra macchina.

1.1. Requisiti minimi

Di seguito sono riportati i requisiti per la macchina server.

<u>Requisiti Software</u>
Sistema operativo: Windows 10, Windows 11, Windows server 2016, Windows server 2019. Non compatibile con le starter edition.
Microsoft SQL Server versione Express o superiore, edizioni: 2008 R2, 2012, 2014, 2016, 2017.

<u>Requisiti Hardware</u>
Processore i5 (o equivalente), o superiore
8 GB di RAM
100 GB di spazio disponibile su hard disk
Risoluzione video minima: 1366x768 pixel
Risoluzione video consigliata: 1920 x 1080 pixel

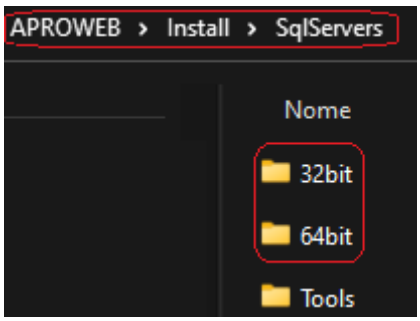
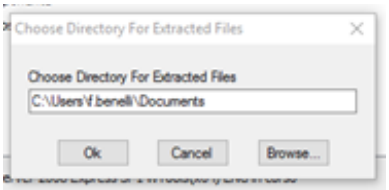
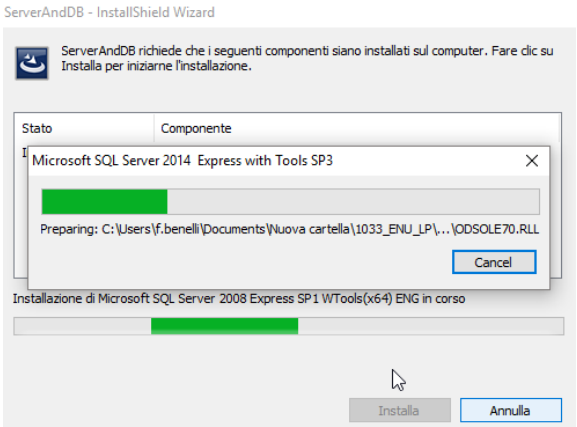
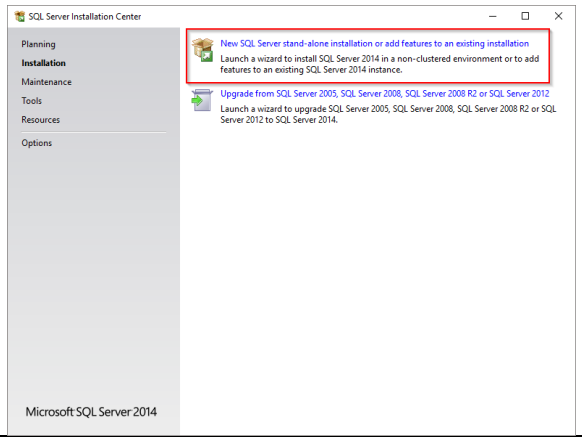
1.2. Installazione

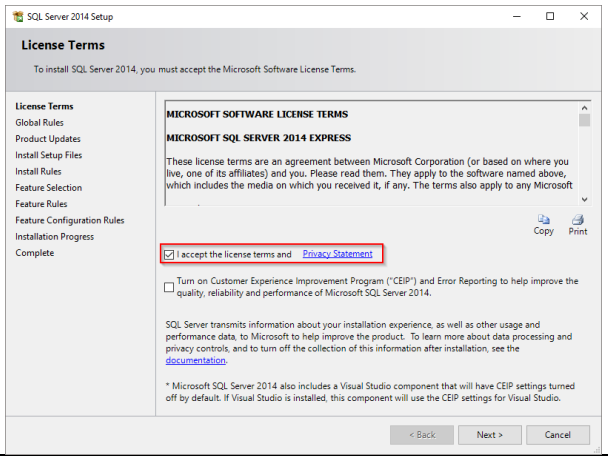
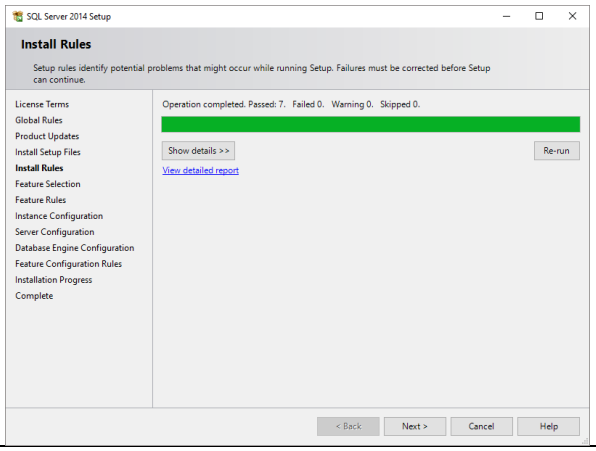
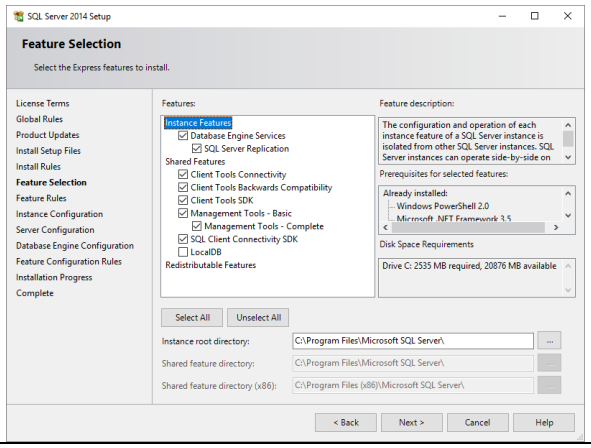
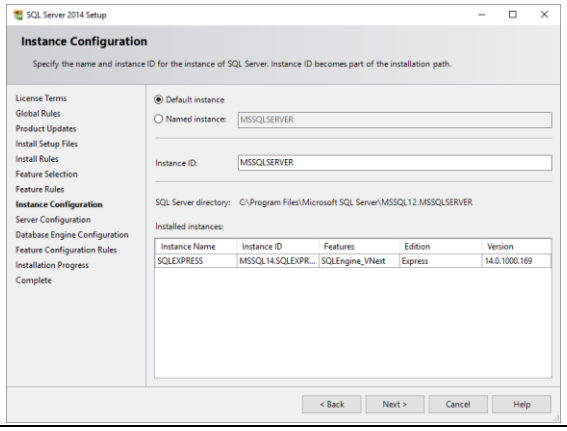
Per installare il programma seguire i seguenti passi:

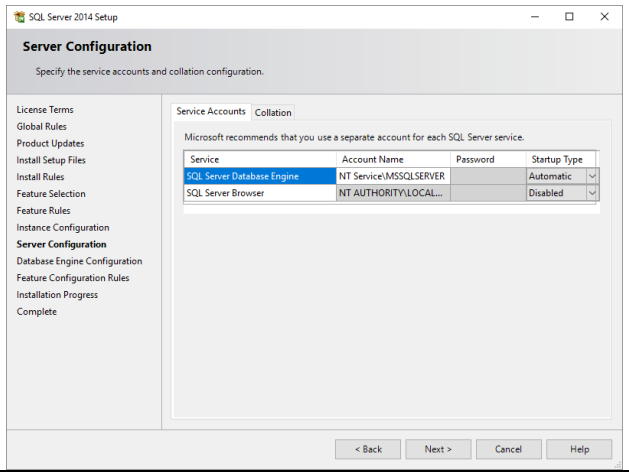
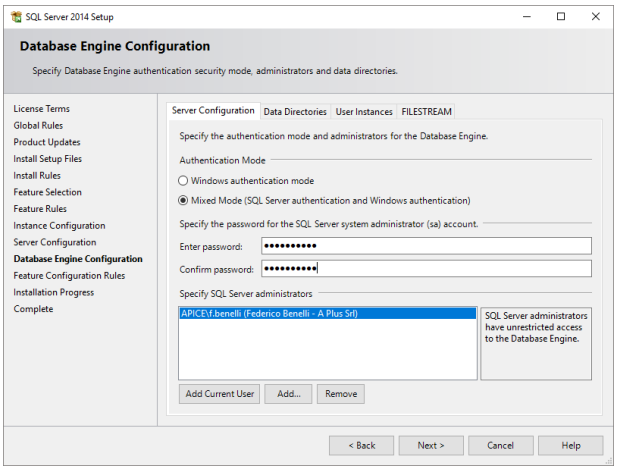
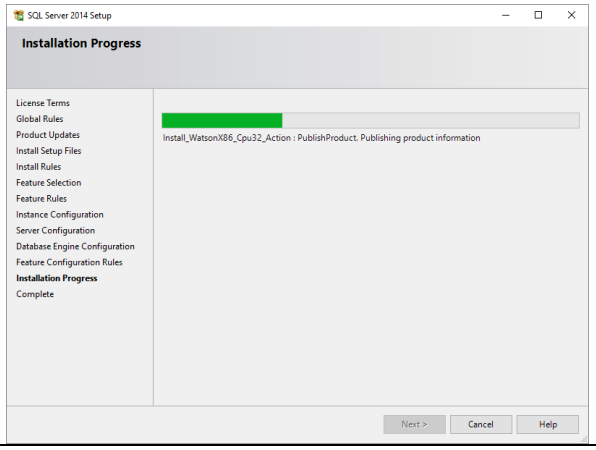
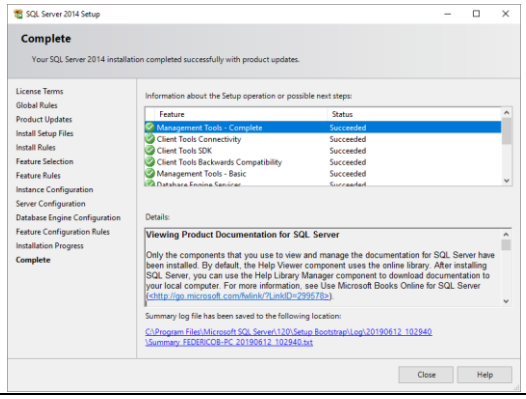
- installare Microsoft SQL Server;
- installare/aggiornare il database AxWinDB;
- installare il software per la configurazione e la comunicazione con i terminali ADM, APRO WEB Service e AxWin6 Client

Di seguito sono dettagliati i passaggi da seguire per la corretta installazione del software.

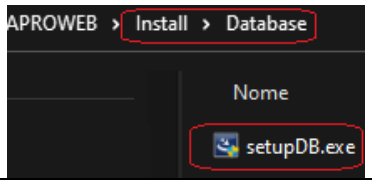
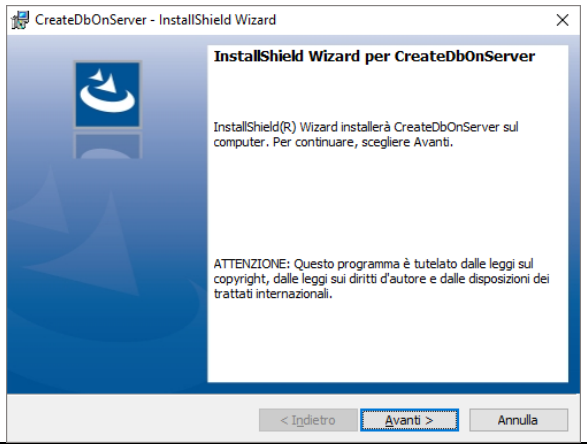
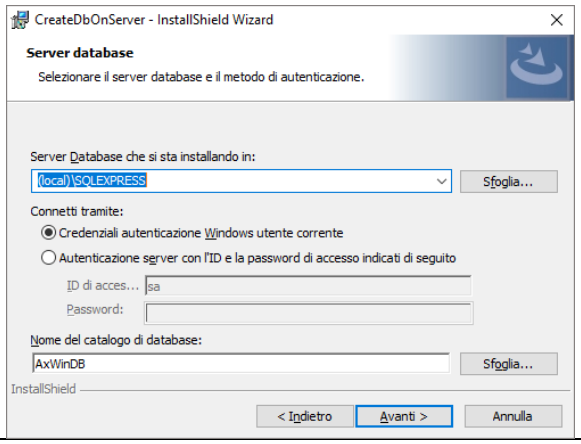
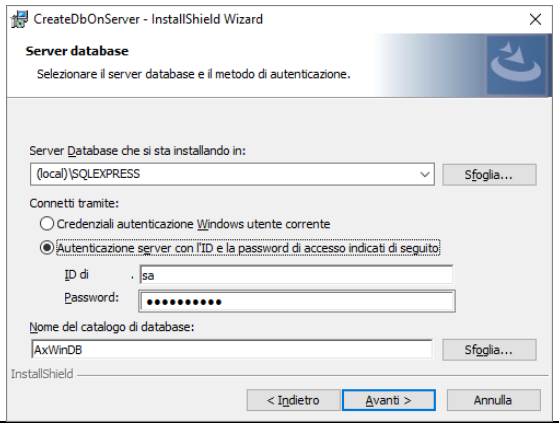
1.2.1. Installazione Microsoft SQL Server

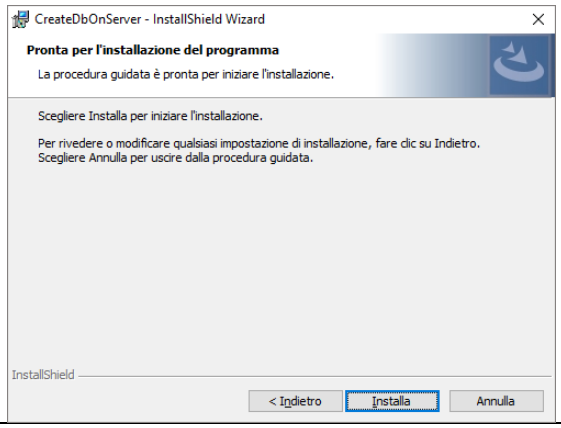
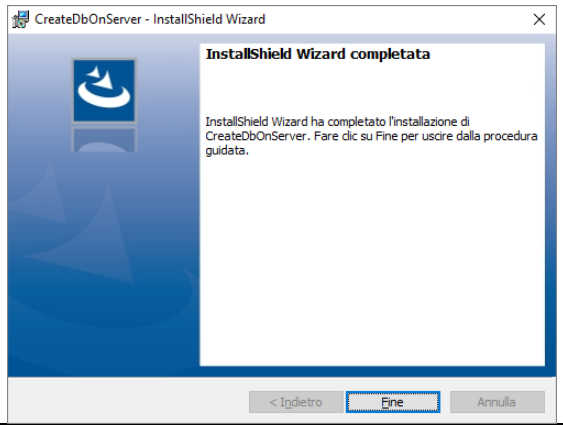
Nel caso di prima installazione, occorre installare il Server SQL e il database AxWinDB. Se si vuole utilizzare una versione di Microsoft SQL già presente, fare riferimento al paragrafo successivo "Installazione/Aggiornamento database". Nella cartella di installazione, aprire il percorso: \Install\SqlServers Lanciare il setup relativo alla versione di sistema operativo idonea.	
Scegliere il percorso dove estrarre i file.	
Attendere il completamento dell'estrazione.	
In seguito apparirà la console di installazione di SQL Server; selezionare "New SQL Server..." e seguire le indicazioni sotto riportate.	

Selezionare “I accept the license terms and Privacy Statement” e successivamente cliccare su “Next”.	
Cliccare su “Next”.	
Se non vogliamo cambiare il nome dell’istanza proseguire cliccando su “Next”.	
Se non vogliamo cambiare il nome dell’istanza, scegliere “Default instance” e proseguire cliccando su “Next”.	

Cliccare su “Next”.	
Configurazione del motore di database: Selezionare “modalità mista” ed inserire una password. Questa è la password associata all’account “sa” che è l’amministratore di default del server SQL. È importante non perdere questa password. Cliccando su “Add” è possibile aggiungere facoltativamente utenti del dominio o del computer.	
Attendere il completamento dell’installazione: l’operazione richiederà alcuni minuti.	
SQL Server è ora installato: cliccare su “Close”.	

1.2.2. Installazione/Aggiornamento database

Sia nel caso di una prima installazione del database, sia nel caso di un aggiornamento del database, nella cartella di installazione, Install\Database\setupDB.exe	
Cliccare su “Avanti”.	
Selezionare l’istanza del Server Database desiderata: es. (local)\ es. (local)\SQLEXPRESS es. NOME PC\ es. NOME PC\SQLEXPRESS es. IPADDRESS\ es. IPADDRESS\SQLEXPRESS	
Inserire le credenziali di accesso se si utilizza l’Autenticazione SQL. Lasciare il nome del database: “AxWinDB”. Cliccare su “Avanti”.	

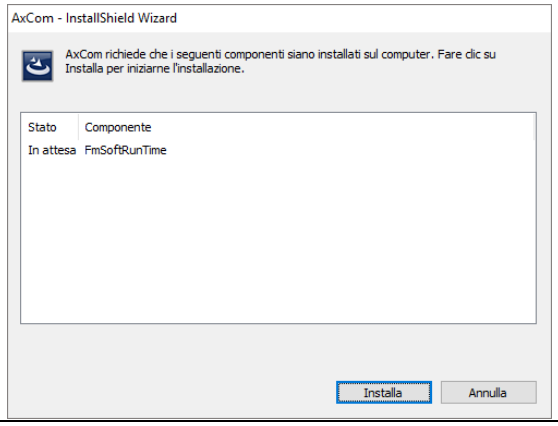
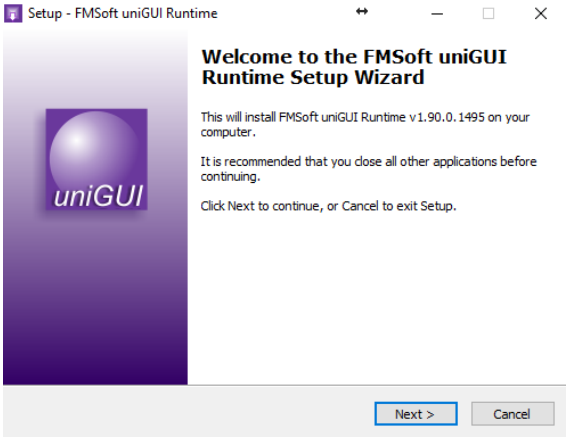
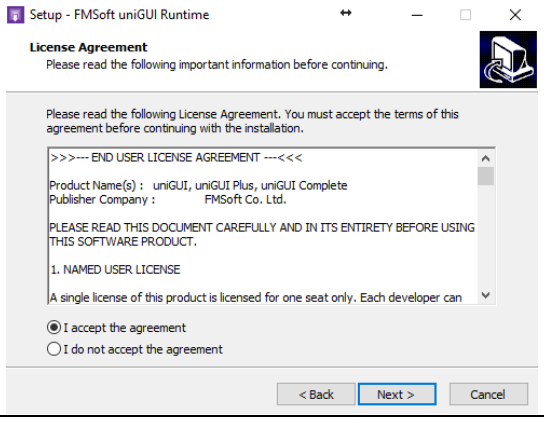
Cliccare su “Installa”.	
Il database è ora installato correttamente. Cliccare su “Fine”.	

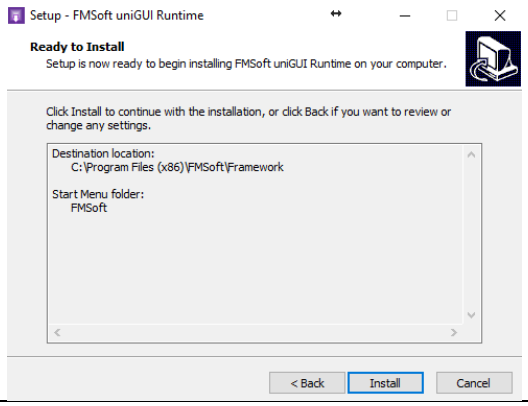
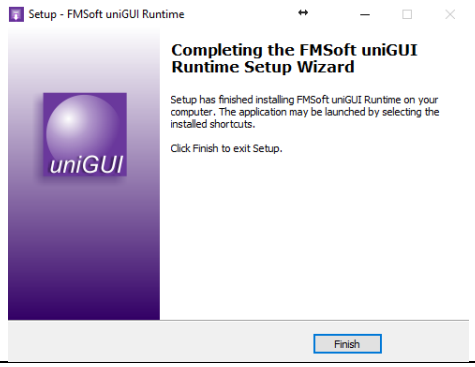
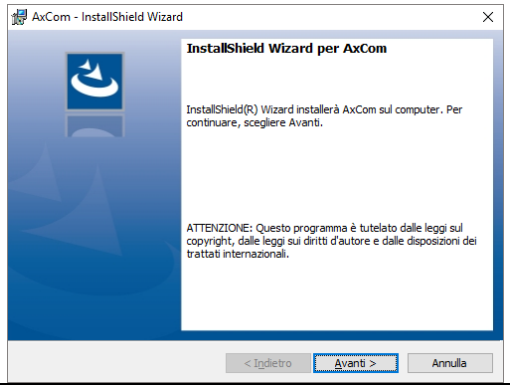
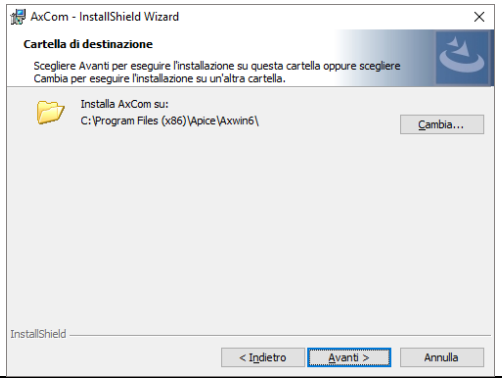
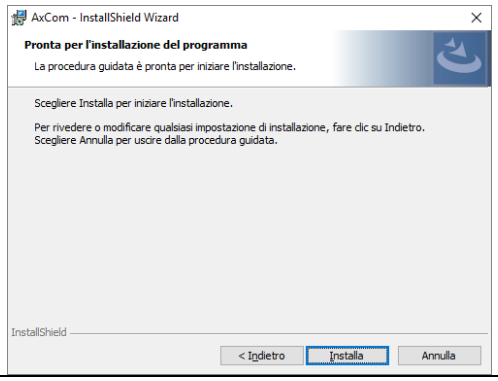
1.2.3. Installazione/Aggiornamento ADM, APRO WEB service e AxWin6 Client

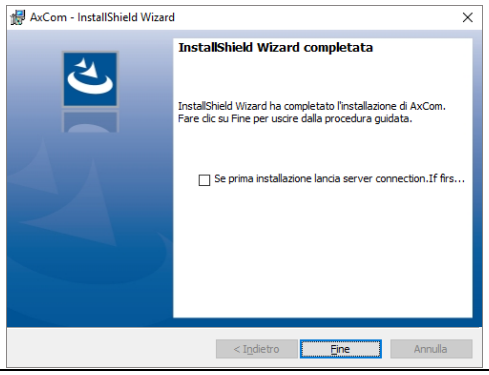
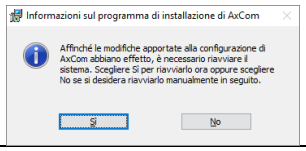
ADM è il nuovo software per la configurazione e comunicazione con i terminali che sostituisce AxCom.

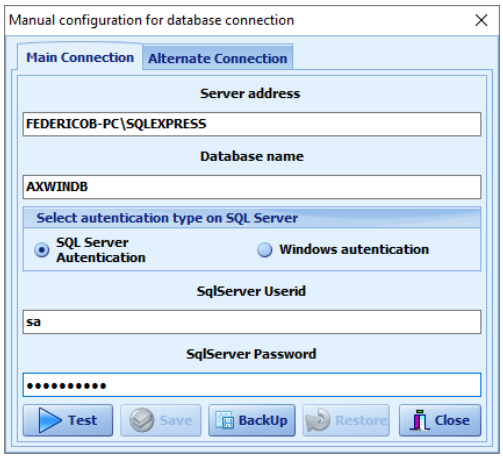
Sia nel caso di una prima installazione, che di un aggiornamento di ADM, di APRO WEB service e di AxWin6 Client, Install\AproWeb\setupAPROWEB.exe

Cliccare su “Sì”, nella prima maschera che appare.

Selezionare “Installa”.	
Cliccare “Next”.	
Scegliere “I accept the agreement”. Cliccare “Next”.	

Cliccare su “Install”.	
Cliccare su “Finish”.	
Cliccare su “Avanti”.	
Scegliere la cartella di installazione, consigliamo di lasciare quella di default	
Cliccare su “Installa”	

Cliccare su “Fine”	
Riavviare la macchina.	

Lanciare ADM, il percorso di default è: C:\Program Files (x86)\Apice\Axwin6\ADM.exe	
Al primo avvio apparirà la maschera di connessione al database. Inserire i dati del server SQL, del database e del modo di autenticazione. Nel campo “Server address” inserire l’indirizzo del server o il nome del server (completo dell’istanza) se nella rete esiste un server DNS che risolve i nomi. Nel campo “Database name” inserire il nome del database; di default il nome è AXWINDB. Scegliere il tipo di autenticazione: nel caso di SQL Server Authentication inserire “SQLServer Userid” e “SQLServer Password” così come impostate in fase di configurazione. Premere su “Test”. Se tutto è corretto apparirà la scritta “Connection successfully”, cliccare su “OK” e successivamente su “Save”. Può essere richiesto di fare la connessione al database anche in fasi successive, per vari motivi (il file “*Config.vtd*” contenente la stringa di connessione viene perso, l’indirizzo del server è cambiato, ecc.). In questi casi, per richiamare la maschera dove fare la stringa di connessione, scegliere il programma “Server Connection”, all’interno della cartella dei programmi C:\Program Files (x86)\Apice\Axwin6\	

1.2.4. Deployment di APROWEB come ISAPI module all'interno del web server IIS

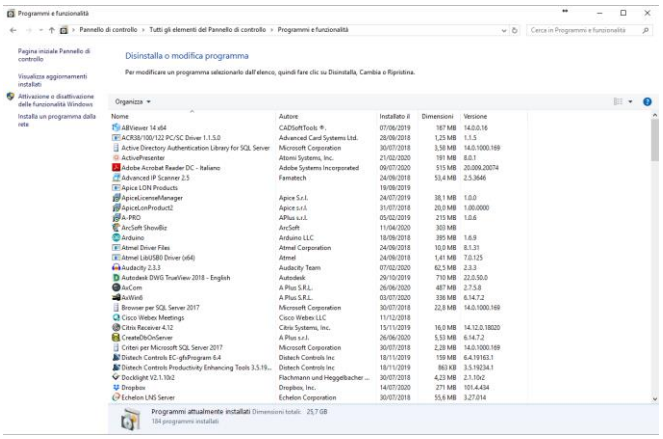
Il seguente paragrafo è da prendere in considerazione solo nel caso in cui il cliente voglia installare APROWEB in IIS. Nella cartella C:\Program Files (x86)\Apice\Axwin6\ è presente il modulo ISAPI di APROWEB: "**APROWebISAPI.dll**" da caricare nel web server IIS (Internet Information Services) di Microsoft.

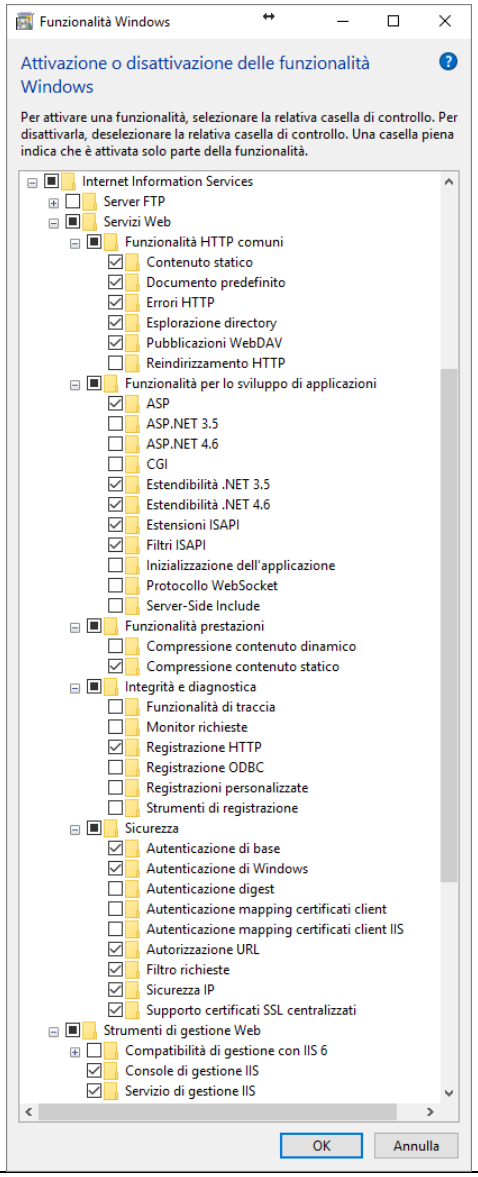
Installazione IIS:

Accedere in "Pannello di controllo" > "Programmi e Funzionalità" di Windows.

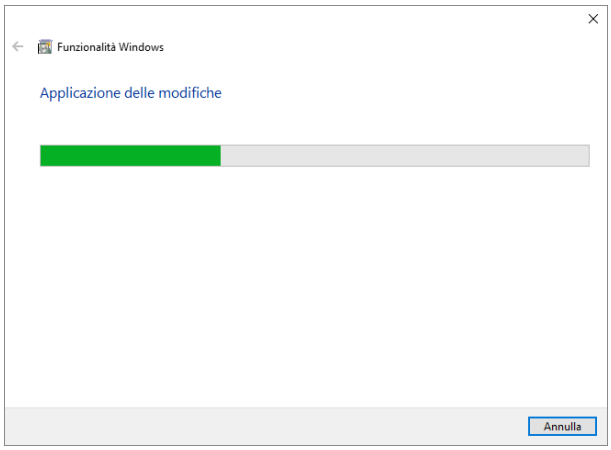
Cliccare su "Attivazione o disattivazione delle funzionalità di Windows".

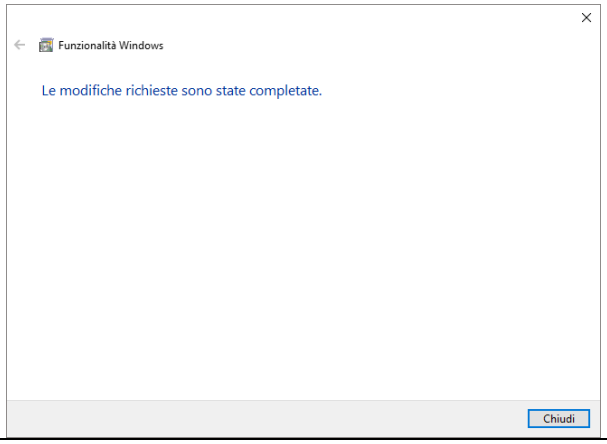
Verificare che siano già installate le seguenti funzionalità di Windows, in caso contrario selezionarle, cliccare su OK per installarle.





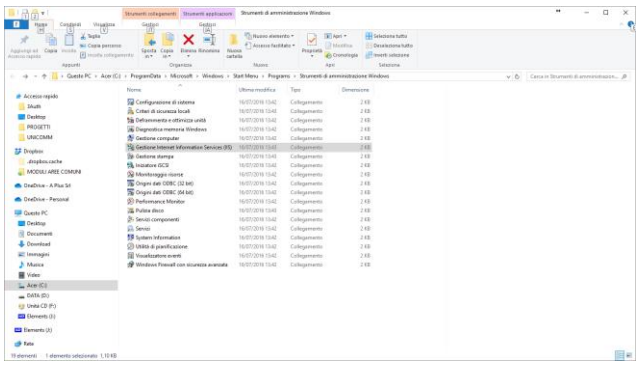
Attendere il completamento dell'installazione e cliccare su "Chiudi".

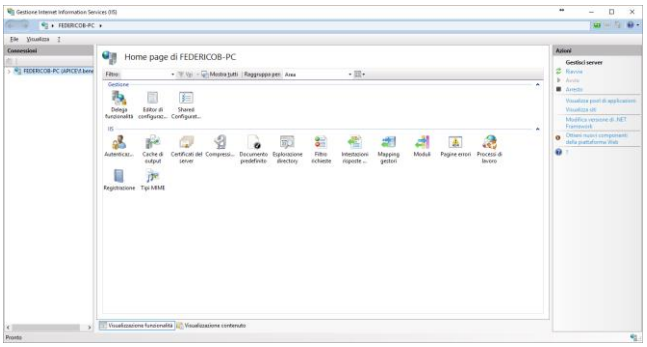


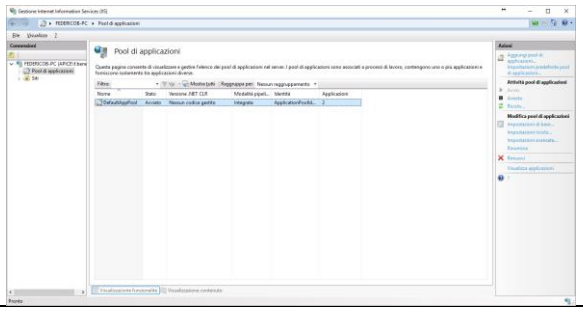
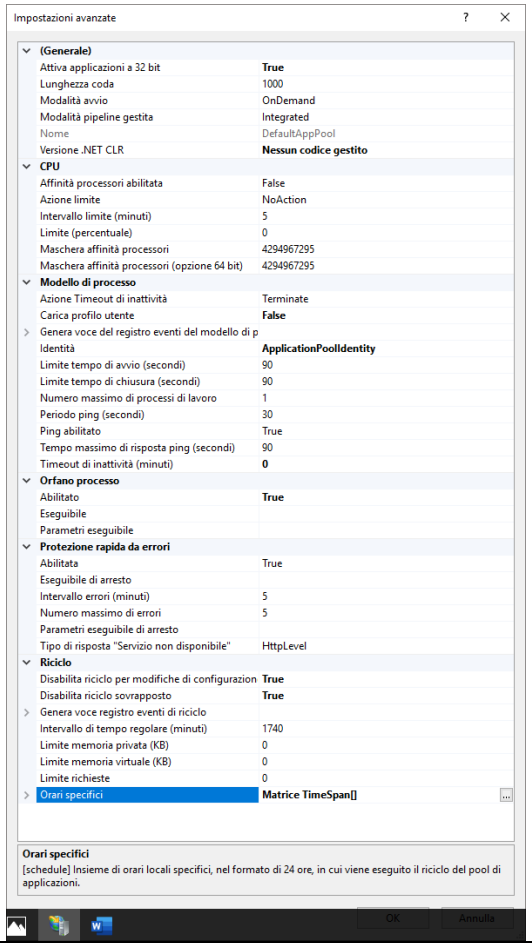
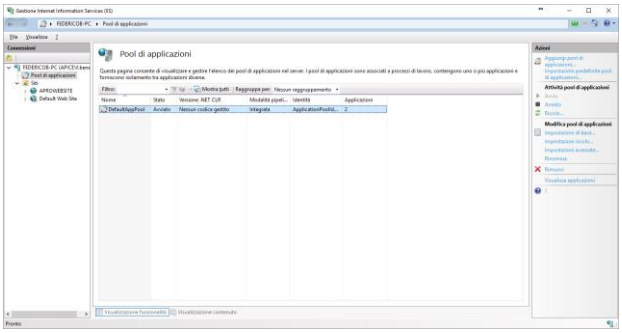
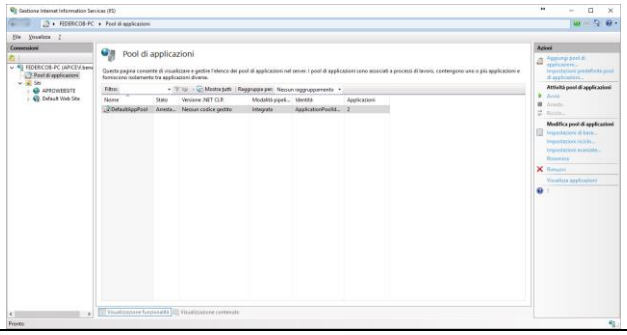


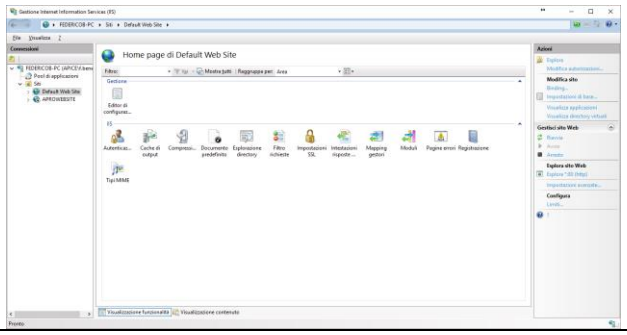
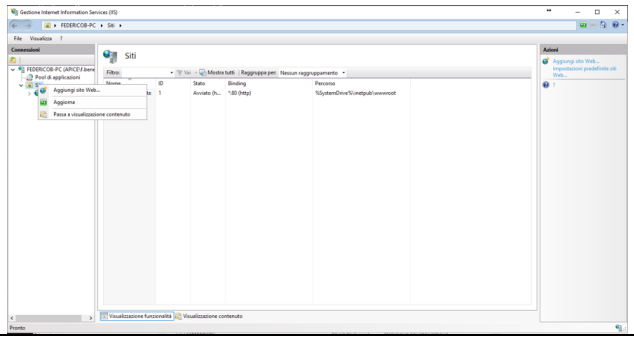
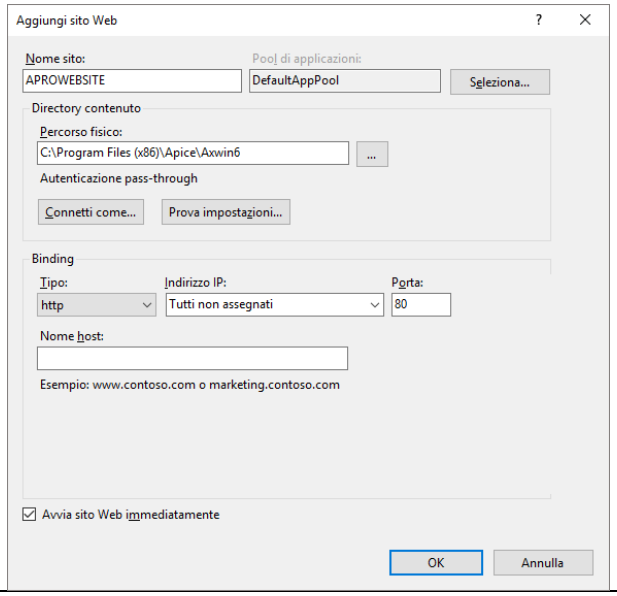
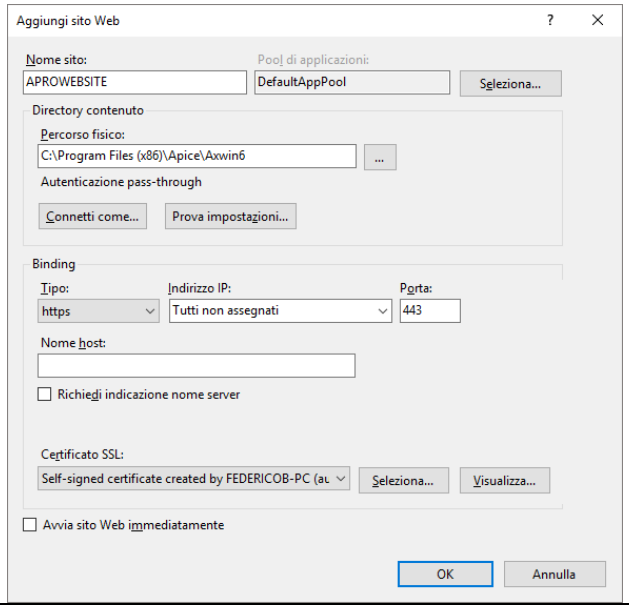
Deployment modulo ISAPI in IIS

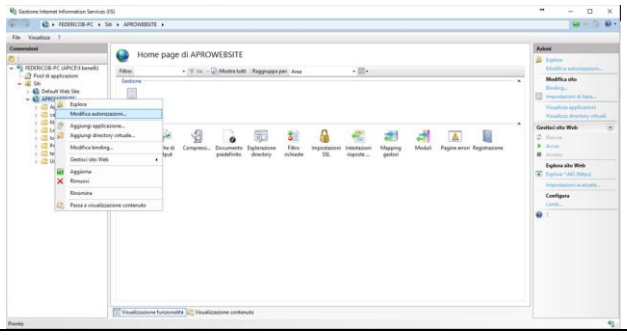
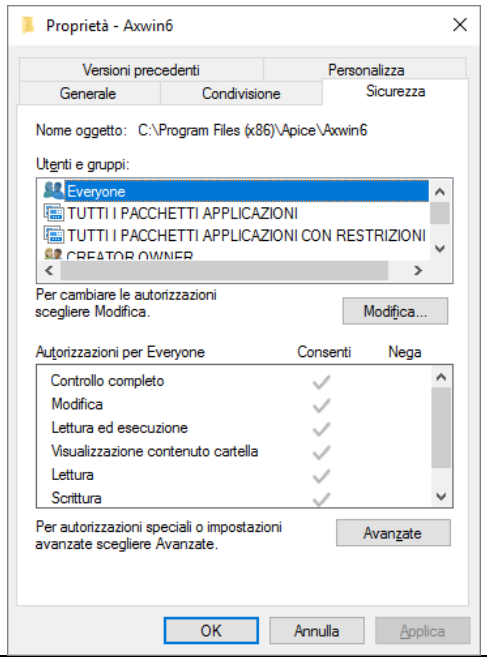
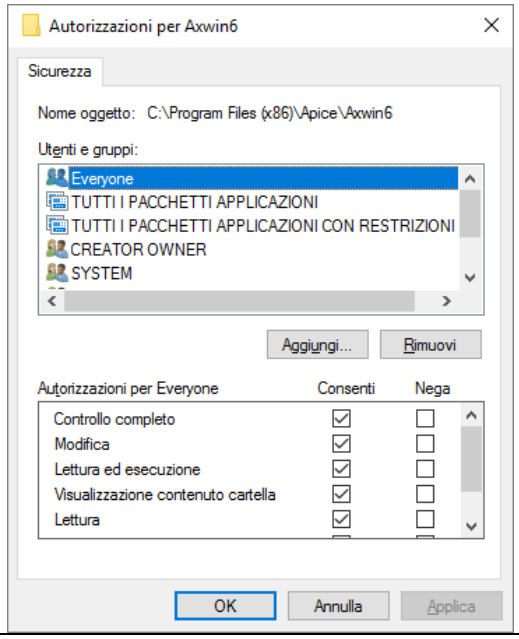
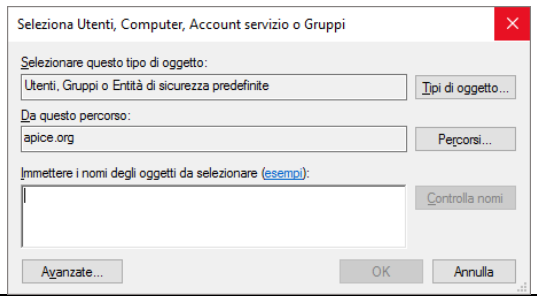
Aprire "Gestione Internet Information Service"

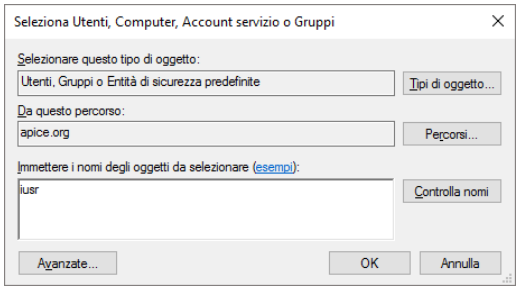


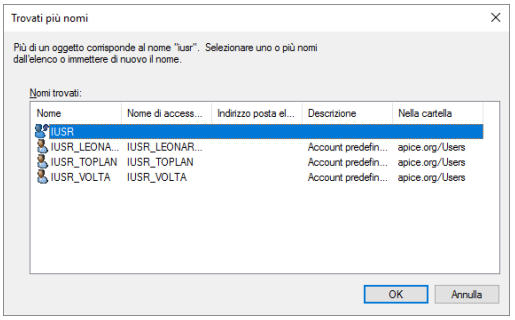


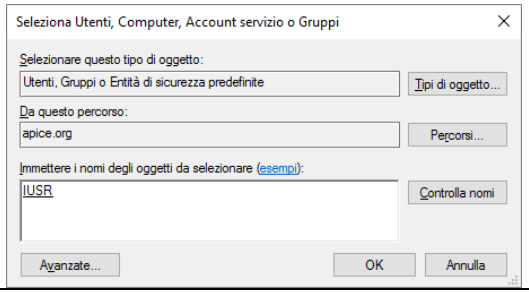
Selezione “Pool di applicazioni”, selezionare la riga “DefaultAppPool”. Cliccare su “Impostazioni avanzate”	
Impostare come in figura:	
Arrestare e ri-avviare il DefaultAppPool	 

Espandere “Siti”, doppio clic su “Default Web Site”. Cliccare su “Arresto”	
Tasto destro su “Siti”, scegliere Aggiungi sito Web...”	
Configurare il sito come di seguito, nel caso si scelga il protocollo http.	
Configurare il sito come di seguito, nel caso si scelga il protocollo https. In questo caso scegliere il certificato SSL	

Tasto destro su “APROWEBSITE”, cliccare su “Modifica autorizzazioni…”	
Nelle proprietà selezionare “Sicurezza”. Cliccare su “Modifica”.	
Cliccare su “Aggiungi”	
Immettere il nome “iusr” e cliccare su “Controlla Nomi”. Selezionare “IUSR” dalla lista che compare. Cliccare su “Ok”.	

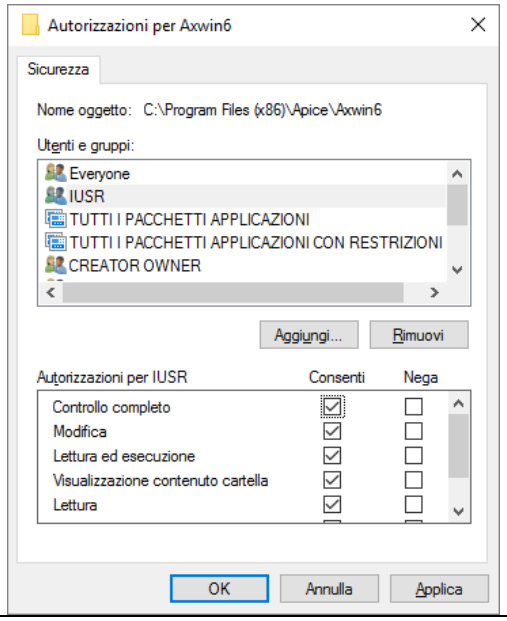




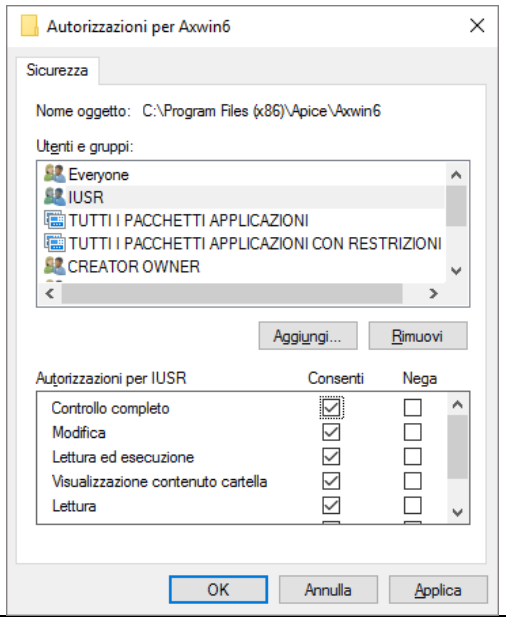


Selezionare tutte le caselle “Consenti” per l’utente IUSR.

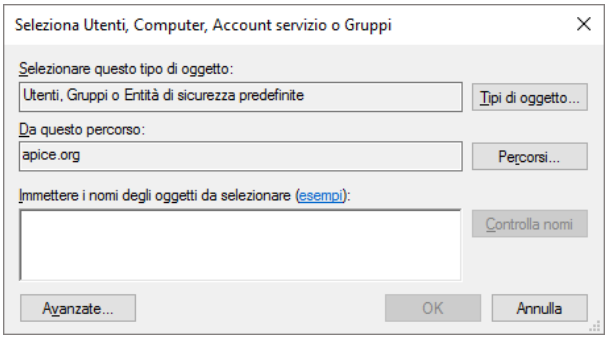
Cliccare su “Applica”.

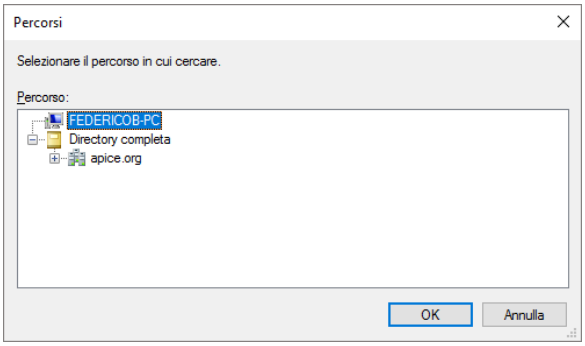


Cliccare nuovamente su “Aggiungi”



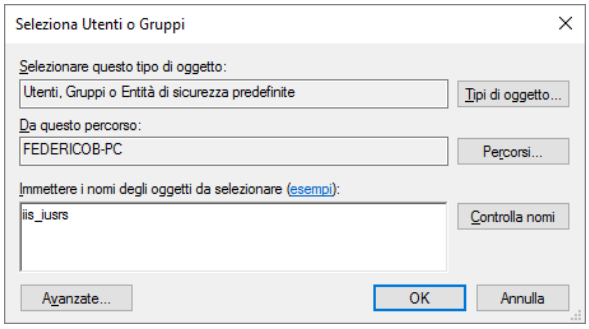
Aprire “Percorsi”.
Selezionare il nome del PC (o server).
Cliccare “Ok”.

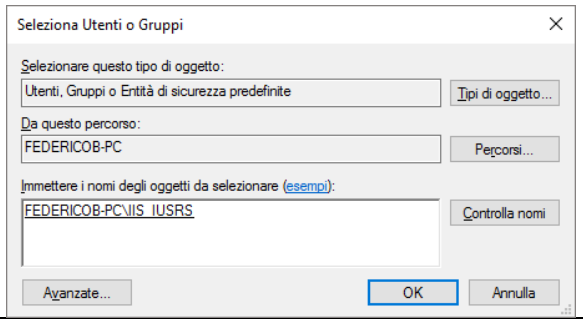
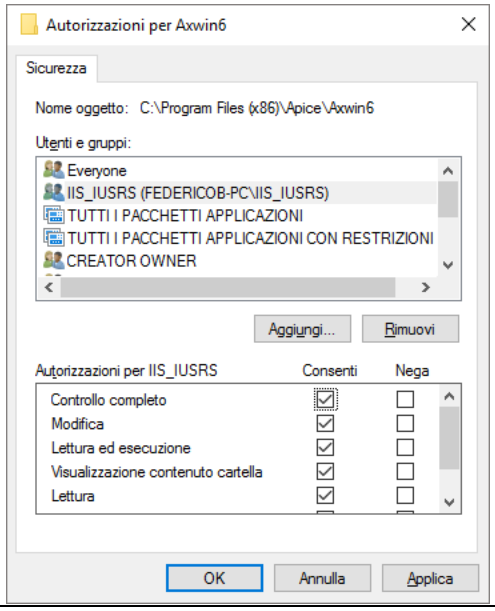
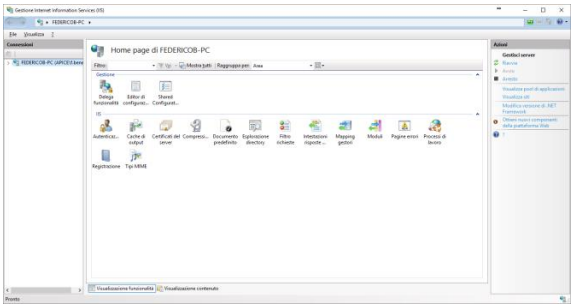


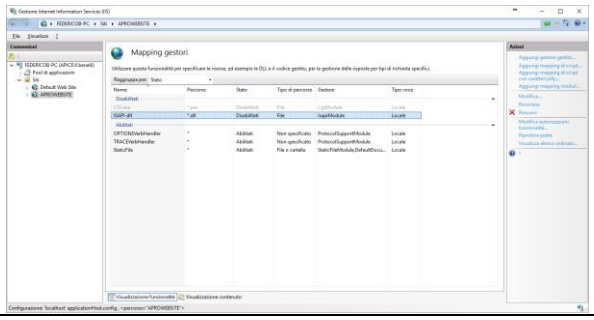


Immettere il nome “iis_iusrs” e cliccare su “Controlla nomi”.

Cliccare su “Ok”.



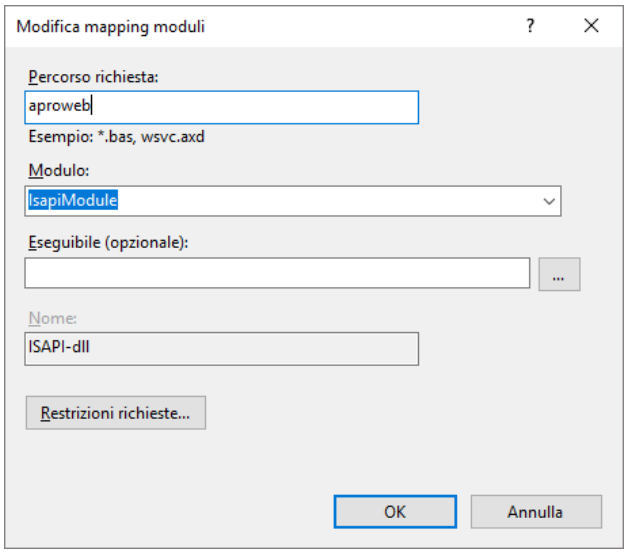
<table>
<tr><td></td><td> 
</td></tr>
<tr><td>Selezionare tutte le caselle “Consenti” per l’utente IIS_IUSRS.
Cliccare su “Applica”.</td><td> 
</td></tr>
<tr><td>Dalla pagina principale di gestione entrare nel menu “Mapping gestori”.
Doppio clic su “ISAPI-dll”.</td><td> 

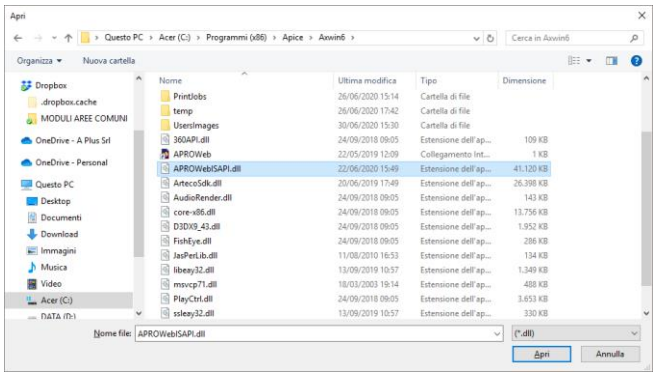

</td></tr>
</table>

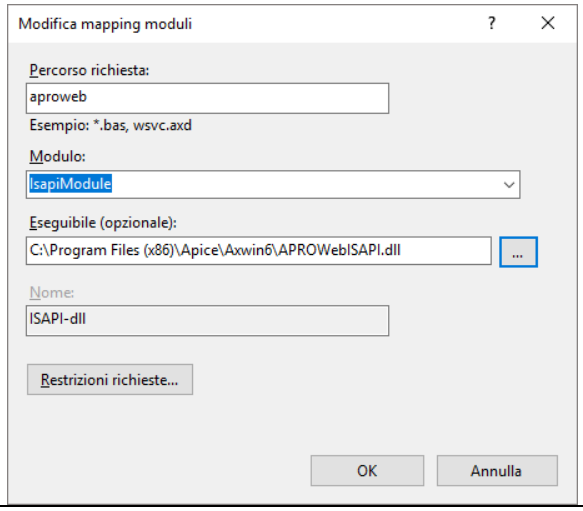
Compilare come di seguito.

L'eseguibile è "APROWebISAPI.dll" si trova in:

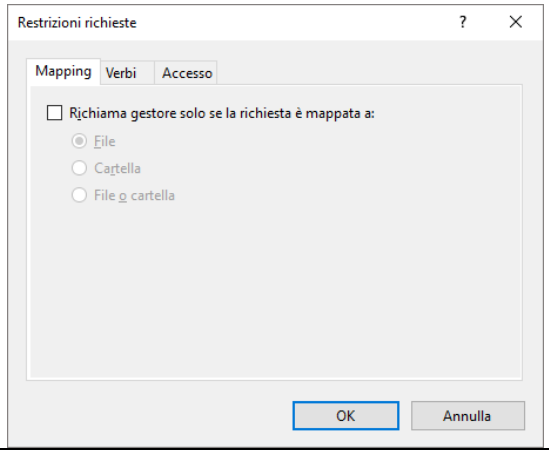
C:\Program Files (x86)\Apice\Axwin6

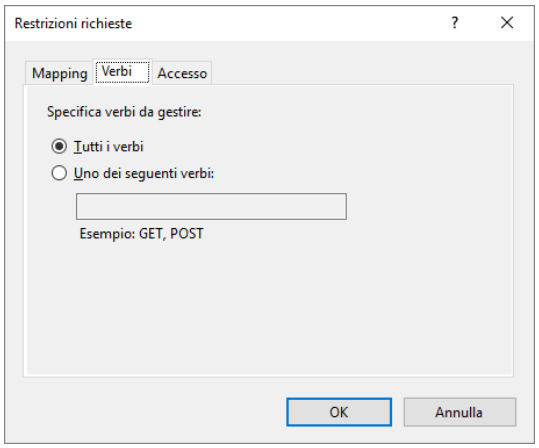
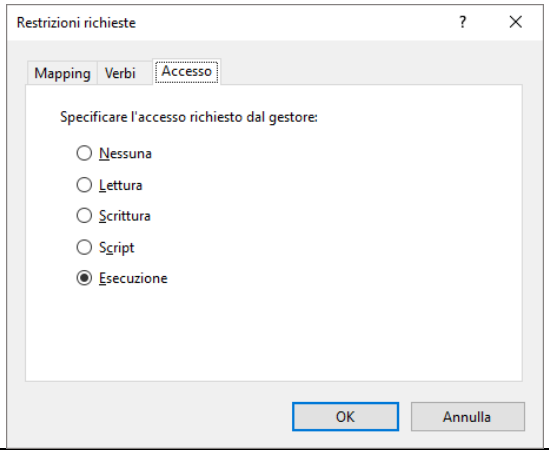
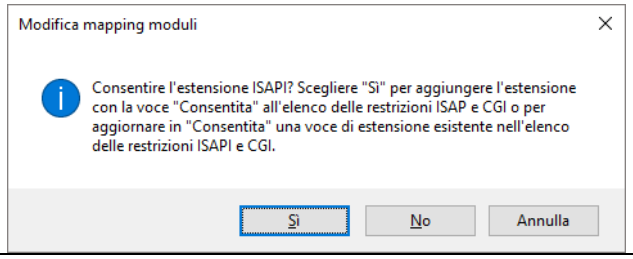
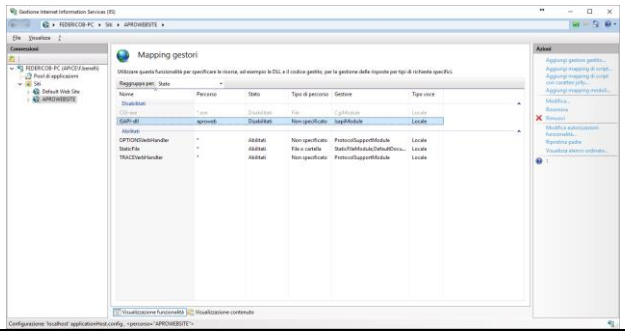
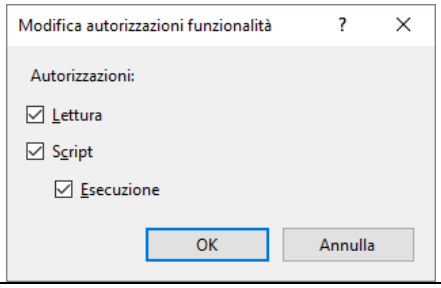


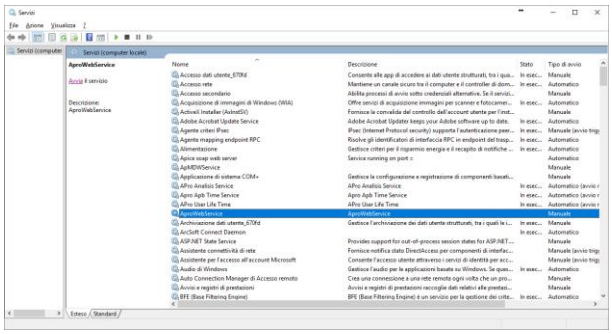
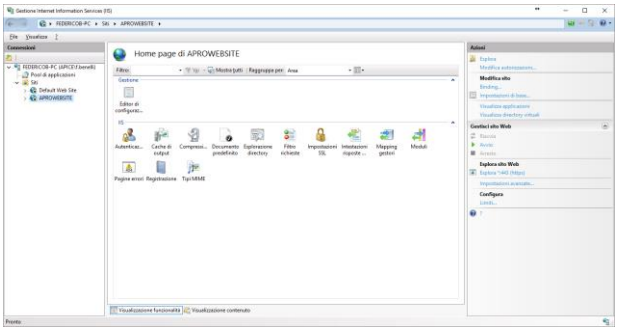
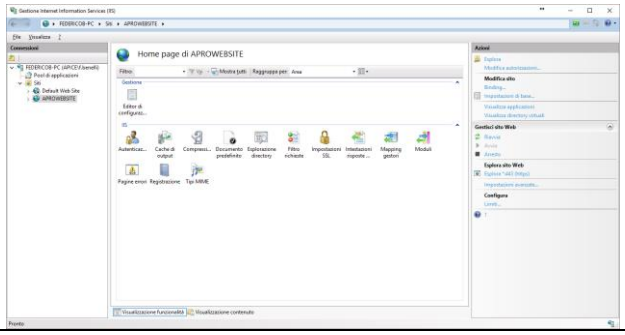
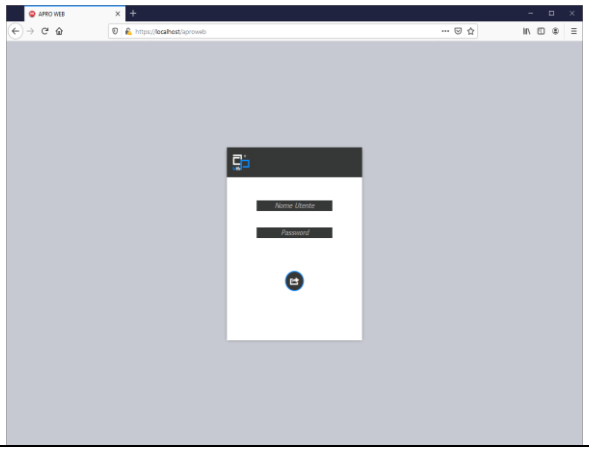




Cliccare su "Restrizioni richieste", impostare come in figura.



	 
Cliccare “Sì” al seguente form	
Scegliere “Modifica autorizzazioni funzionalità…”	
Abilitare tutto come in figura e scegliere “Ok”	

Prima di avviare “APROWEBSITE” assicurarsi che il servizio “AproWebService” sia fermo. Impostare nelle proprietà del servizio “avvio manuale”.	
Selezionare “APROWEBSITE” e cliccare su “Avvio”	 
Accedere al sito Es. https://localhost/aproweb	

1.3. Licenza

Per poter funzionare completamente la piattaforma APRO WEB ha bisogno di una licenza. La licenza può essere di tipo hardware, sotto forma di pendrive USB, oppure di tipo software.

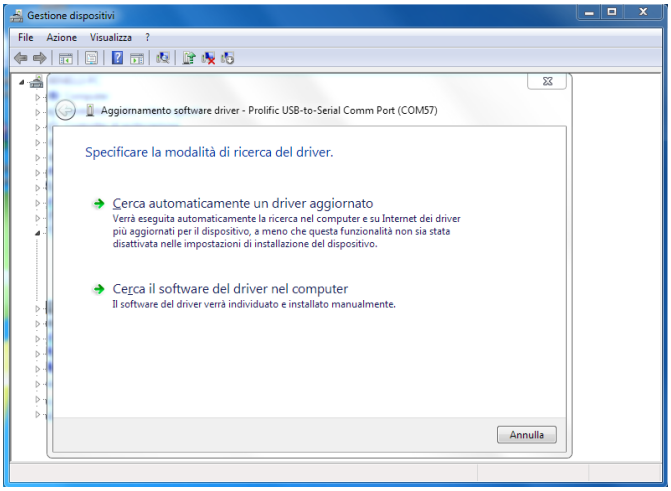
La licenza stabilisce i seguenti parametri:

- con quanti terminali (detti anche periferici) ADM può comunicare;
- quante sessioni di apertura di APRO WEB dal browser, con utente correttamente loggato, possono essere attive.

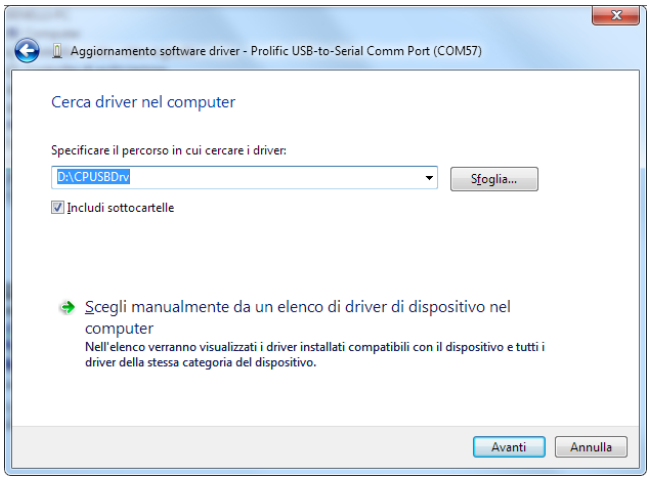
In qualunque momento è possibile richiedere ad A PLUS un ampliamento delle funzionalità abilitate nella licenza in proprio possesso.

1.3.1. Licenza Hardware

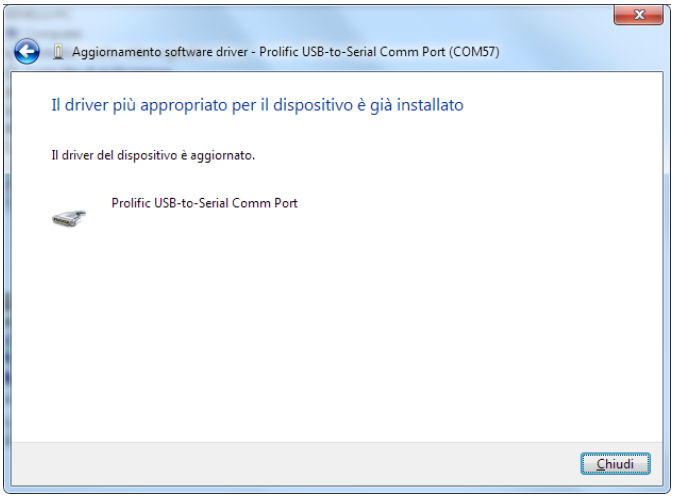
In caso di utilizzo di licenza hardware è sufficiente inserire la licenza USB in una presa USB della macchina dove è installato ADM. Nel caso in cui l'installazione automatica dei driver per la pendrive USB non vada a buon fine, è possibile aggiornare i driver della USB non riconosciuta dal pannello "Gestione dispositivi" di Windows:



Selezionare "Cerca il software del driver nel computer": i driver si trovano nella cartella di installazione, aprire il percorso: \Driver chiave USB\ oppure possono essere scaricati dal sito internet www.aplus.srl.



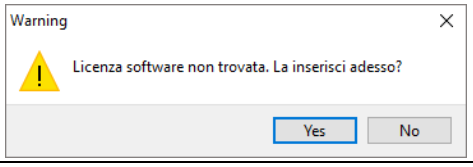
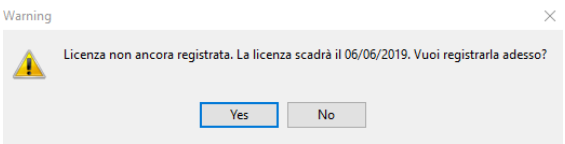
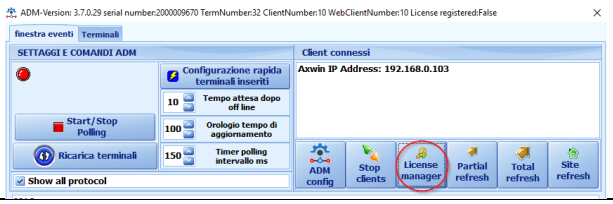
Cliccare su “Avanti” e attendere il messaggio di conferma di avvenuto aggiornamento del driver del dispositivo:

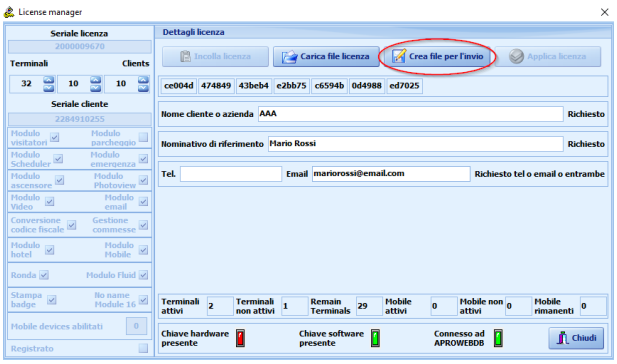
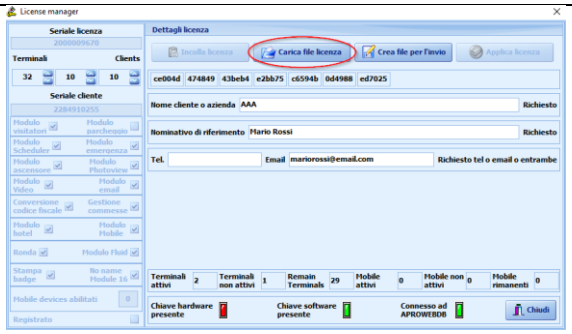
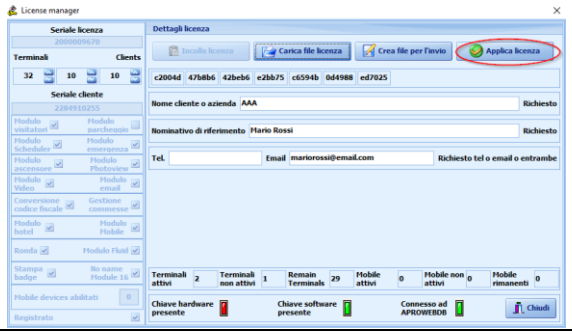


Cliccare su “Chiudi”.

1.3.2. Licenza software

Di seguito viene spiegato come caricare e registrare la licenza software.

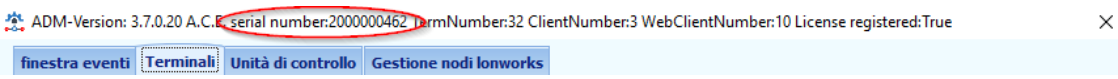
All’avvio di ADM verrà richiesta la licenza software. Cliccare su “Yes” e selezionare il file: “*LicenseFile.lic*”	
Una volta caricata una licenza valida, apparirà la seguente finestra, che informa che la licenza va registrata entro 15 giorni. Per registrarla subito cliccare su “Yes”. Per registrarla in seguito e lanciare ADM, cliccare su “No”.	
Per effettuare la registrazione della licenza cliccare su “Gestione licenza (License manager)” nella finestra eventi di ADM.	

Nella seguente finestra riempire tutti i campi richiesti: • nome cliente o azienda, • nome di riferimento, • telefono e/o mail. Cliccare su “Crea file per l’invio” e selezionare dove si desidera salvare il file “*LicenseFileToReg.lic*”. Cliccare su “Chiudi”.	
Inviare via mail il file appena generato a: produzione@aplus.srl.	
Tramite mail, A PLUS invierà un nuovo file “*LicenseFileReg.lic*” che contiene la licenza registrata.	
Per caricare il file di licenza registrata cliccare su “Gestione licenza (License manager)” nella finestra eventi di ADM. Cliccare su “Carica file licenza” e selezionare il file inviato da A PLUS tramite mail.	
Cliccare su “Applica licenza” e in seguito su “Chiudi”.	

1.3.3. Versionamento e specifiche licenza

A PLUS stabilisce un sistema di versionamento distinto per ciascun software che compone la piattaforma.

La versione di ADM si trova in alto, nell’intestazione della finestra principale di ADM:

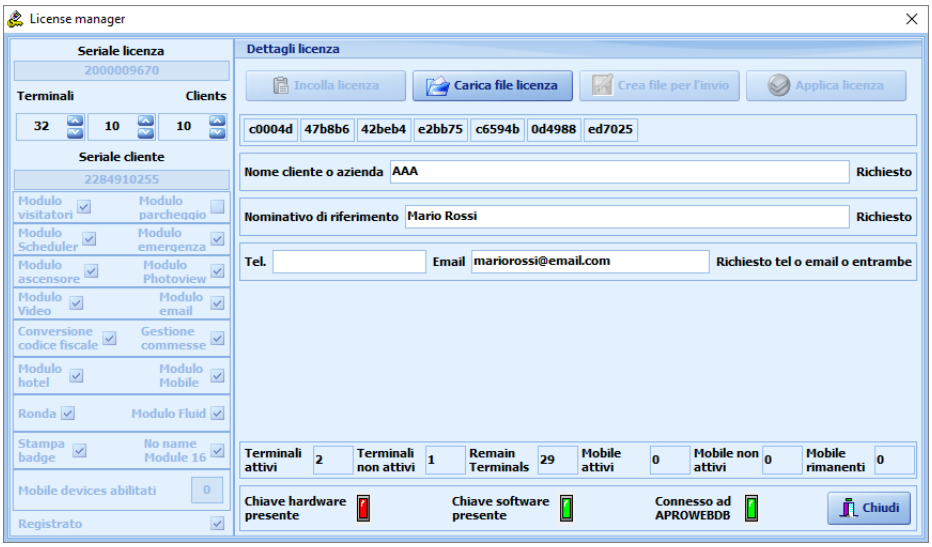


In questa stringa è presente:

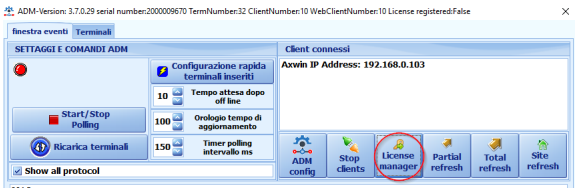
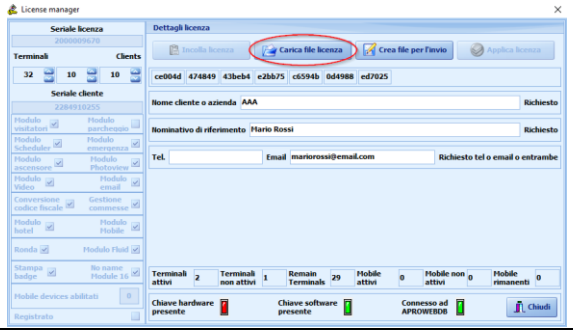
- la versione di ADM (ad esempio 3.7.0.20);
- il numero seriale del prodotto (ad esempio 2000000462);
- il numero di terminali (TermNumber), il numero di client (ClientNumber), il numero di sessioni web abilitate (WebClientNumber) nella licenza caricata

- se la licenza è registrata oppure no.

Per maggiori approfondimenti sul tipo di licenza utilizzata e sulle funzionalità abilitate, cliccare sul tasto “License manager” nella finestra eventi di ADM. Apparirà la seguente finestra dove, nella colonna a sinistra, sono riepilogate le funzionalità abilitate nella licenza:



1.3.4. Ampliamenti delle funzionalità caricate in licenza

Comunicare ad A PLUS il serial number attuale del prodotto.	
A PLUS invierà una nuova licenza con gli ampliamenti richiesti nel file “*LicenseFile.lic*”. Per caricare questa nuova licenza con gli ampliamenti, andare nella finestra eventi di ADM e cliccare su “License manager”.	
Nella finestra che appare cliccare su “Cerca file licenza” e selezionare il file “*LicenseFile.lic*”.	
Cliccare su “Applica licenza” e in seguito su “Chiudi”.	

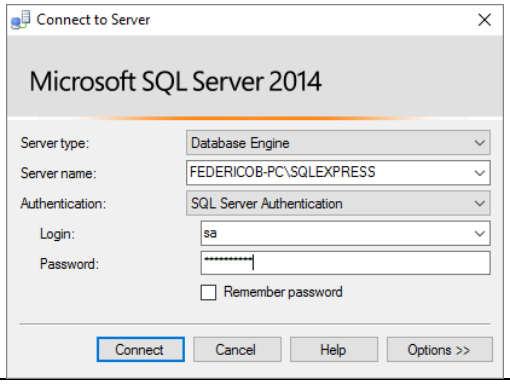
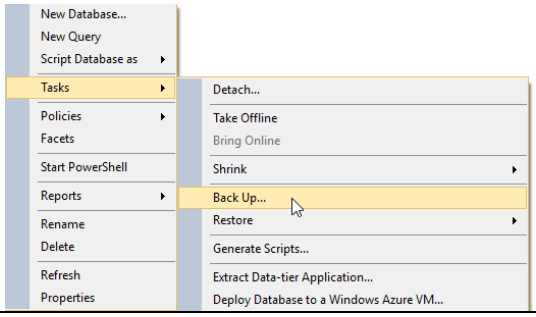
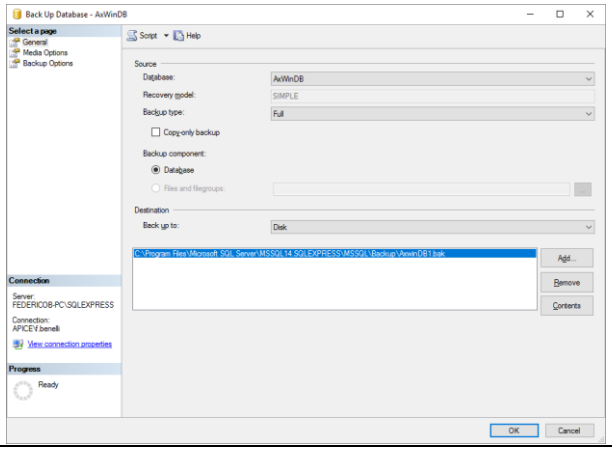
1.3.5. Conversione da sistema AxWin6 a APRO WEB

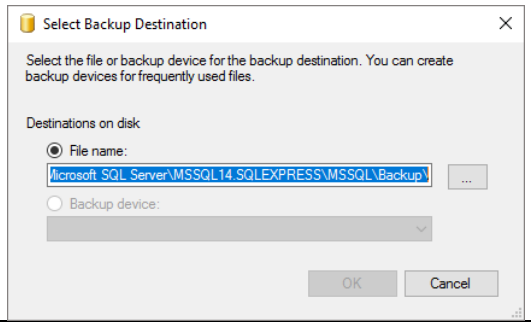
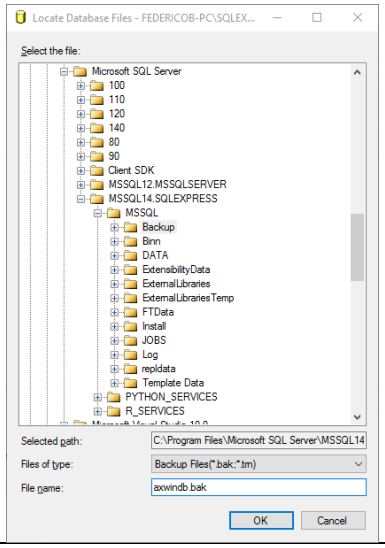
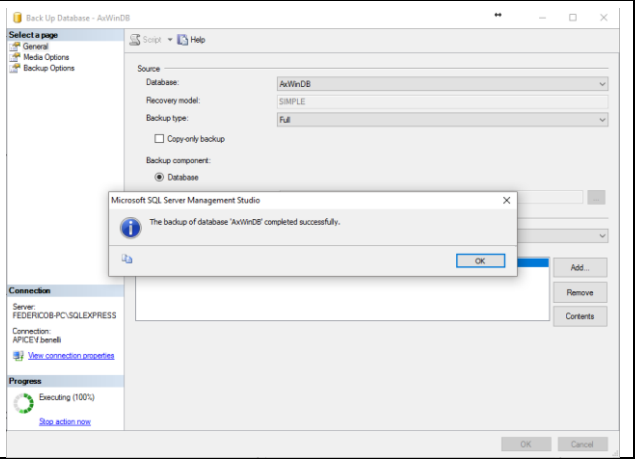
È possibile richiedere ad A PLUS la conversione completa dalla piattaforma software AxWin6 alla piattaforma APROWEB. Per svolgere questa conversione è necessario l'intervento del supporto tecnico di A PLUS.

1.4. Backup/Restore Database

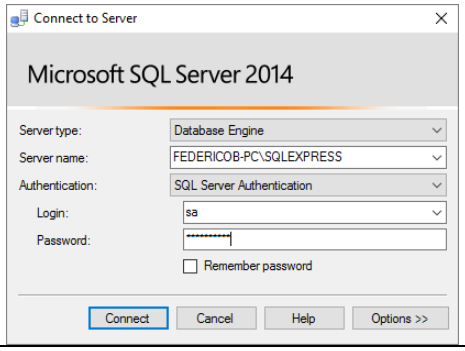
Si consiglia di effettuare periodicamente il backup del database e di salvarlo su una memoria di archiviazione esterna, in modo che, anche in caso di sostituzione del PC, è sufficiente reinstallare i software ed effettuare un restore dell'ultimo backup del database. Di seguito sono spiegati i passi da seguire per fare il backup e il restore del database, all'interno del software Microsoft SQL Server.

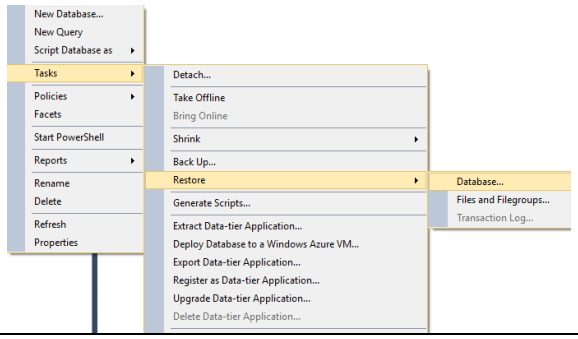
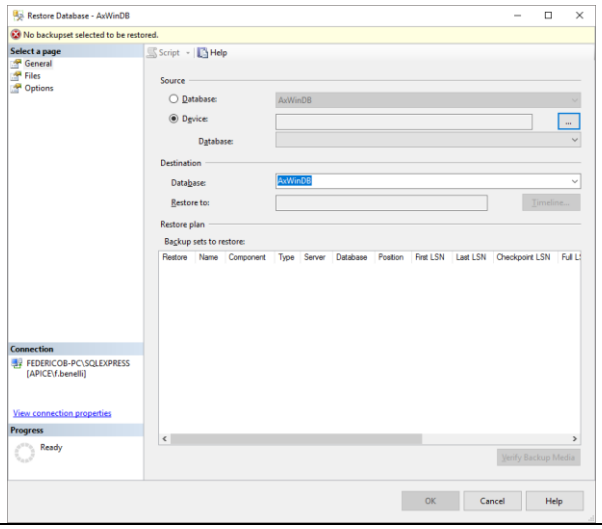
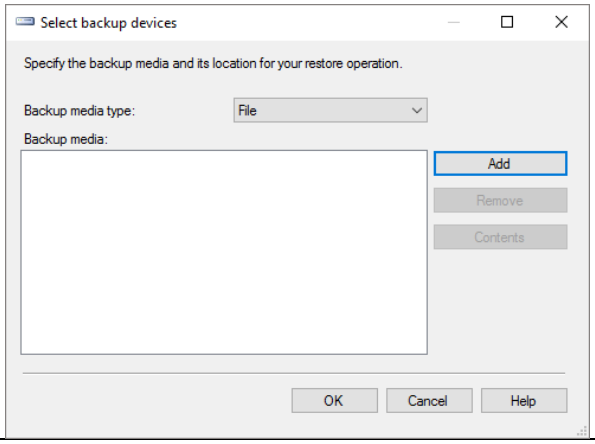
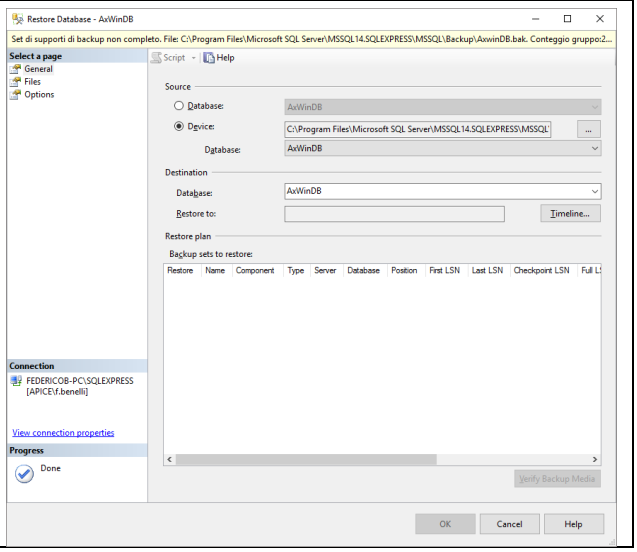
1.4.1. Backup Database

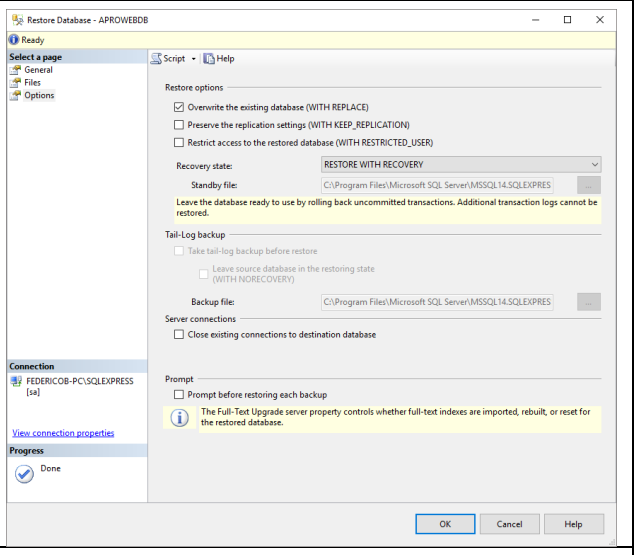
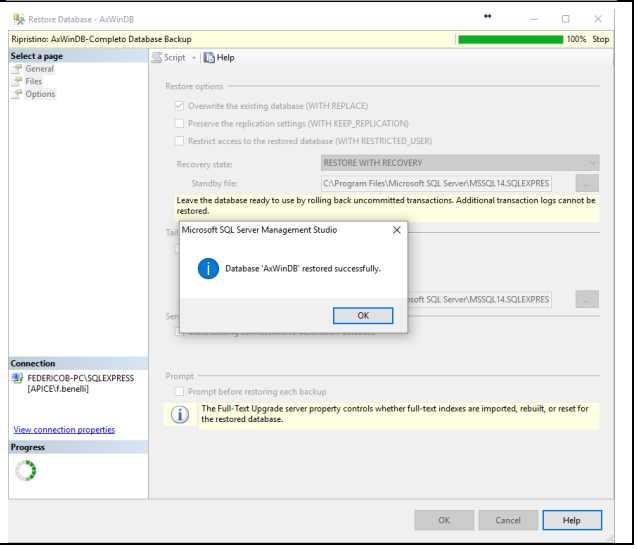
Lanciare il software "SQL Server Management Studio" da Programmi > Microsoft SQL Server 2014.	
Impostare i dati per l'accesso e cliccare su "Connect".	
Cliccare con il tasto destro del mouse sul database desiderato e selezionare Tasks > Back Up...	
Cliccare su "Remove" e successivamente su "Add...".	

Cliccare sui puntini per scegliere il percorso del file da caricare.	
Scegliere il percorso desiderato e specificare il nome del file, facendo attenzione a scrivere l'estensione "*.*bak*", ad esempio "*AxWinDB.bak*". Cliccare su "OK" e proseguire nella procedura.	
Cliccare su "Ok", attendere che la percentuale "Progress" sia al 100% e che compaia il messaggio "The backup of database 'AXWINDB' completed successfully".	

1.4.2. Restore Database

Lanciare il software "SQL Server Management Studio" da Programmi > Microsoft SQL Server 2008 R2.	
Impostare i dati per l'accesso e cliccare su "Connect".	

Cliccare con il tasto destro del mouse sul database desiderato e selezionare Tasks > Restore > Database…	
Selezionare come “Source”: “Device” e cliccare sui puntini.	
Selezionare “Add”, scegliere il file e cliccare su “OK”.	
Spuntare “Restore” e cliccare su “Options”.	

Spuntare “Overwrite the existing database” e cliccare su “OK”.	
Attendere che la percentuale “Progress” sia al 100% e che compaia il messaggio “The restore of database ‘AXWINDB’ completed successfully”.	

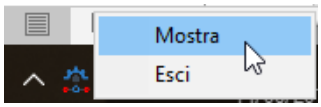
2. Software per configurare i terminali: ADM

Di seguito sono riportati i passi principali da seguire per rendere completamente operativo il sistema di controllo accessi.

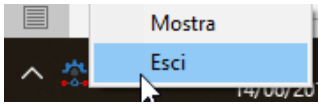
ADM non è un servizio, è un applicativo. Affinché il sistema comunichi costantemente con i terminali in campo è necessario che ADM sia attivo sulla macchina server e che un utente sia connesso (loggato) alla macchina. Questo significa che la sessione loggata, può essere “bloccata”, ma non “disconnessa”.

Per avviare ADM è sufficiente lanciare l’applicazione ADM installata, l’eseguibile è presente nella cartella C:\Program Files (x86)\A PLUS\APRO WEB.

Cliccando su ×, ADM non viene chiuso, il programma continua a funzionare, per ripristinare la sua visualizzazione cliccare con il tasto destro sull’icona presente in system tray (in basso a destra), scegliere “Mostra”.



Per chiudere ADM occorre cliccare con il tasto destro sull’icona presente in system tray (in basso a destra) e scegliere “Esci”.

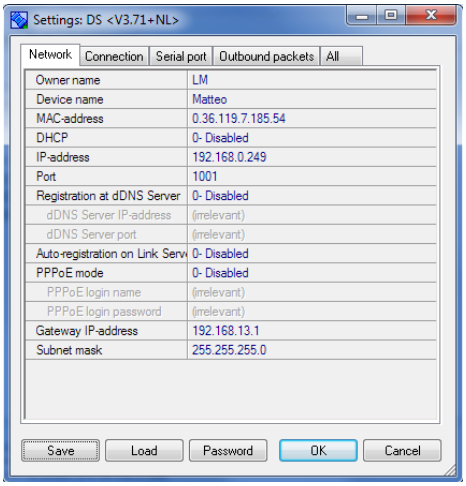


2.1. Creazione/Modifica terminali

Le metodologie di creazione/modifica di uno o più terminali sono diverse a seconda del tipo di terminale utilizzato.

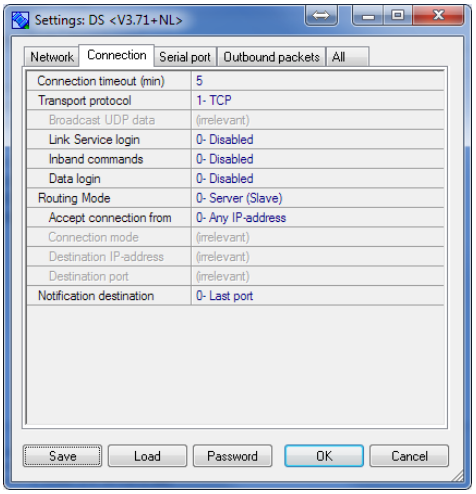
2.1.1. Terminali LM2002, LMIP, LEGGO® 2000 e LMUP

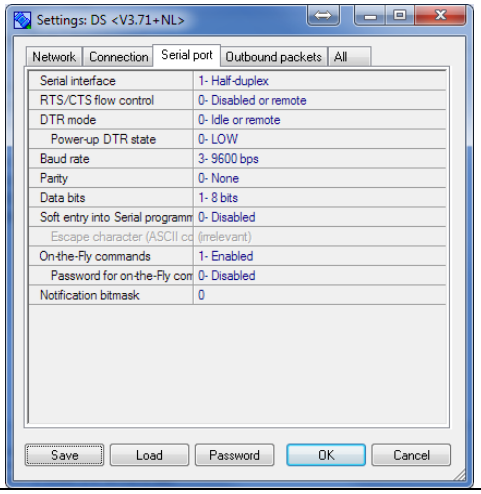
LM2002, LMIP, LEGGO® 2000

Se l'interfaccia è di tipo seriale il PC comunica con un terminale solamente attraverso un collegamento punto-punto di tipo RS232. In alternativa, il PC comunica con più terminali in rete RS485, attraverso un dispositivo di interfaccia USB/RS485: USB4. Il sistema operativo Windows assegnerà una porta COM per l'interfacciamento con i terminali in campo. Nel caso di comunicazione RS485 è necessario assegnare a ogni dispositivo un identificativo numerico univoco.	
Se l'interfaccia è di tipo IP lanciare il software Tibbo DS Manager (C:\Program Files\Tibbo\TDST\tdsman.exe): se non già installato, il programma è presente nella cartella "ComSrv_LMIP", oppure è scaricabile dal sito www.aplus.srl. Attraverso questo software è possibile: • effettuare una scansione di rete per individuare i terminali di rete in campo; • selezionare un terminale e variare i parametri di rete, cliccando su "Settings".	

I parametri di rete devono essere impostati come negli screenshot a fianco.

Rispetto ai parametri di default, assicurarsi di mettere un indirizzo IP statico raggiungibile dalla macchina su cui è installato ADM.





Una volta stabilito il canale di comunicazione (seriale o IP), utilizzare il software LSPY (C:\Program Files\Apice\Winleggo\lspy.exe).

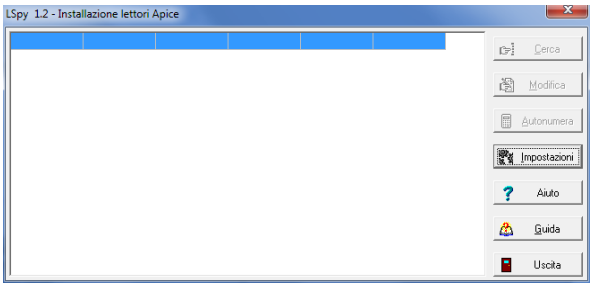
Se non già installato, il programma è presente nella cartella “Winleggo” oppure è scaricabile dal sito www.aplus.srl.

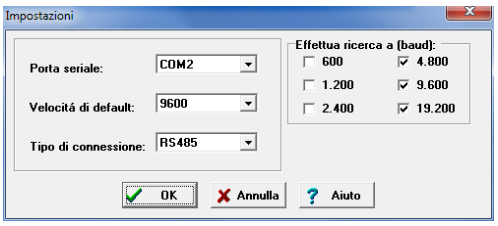
Cliccare su “Impostazioni” e scegliere il tipo di comunicazione.

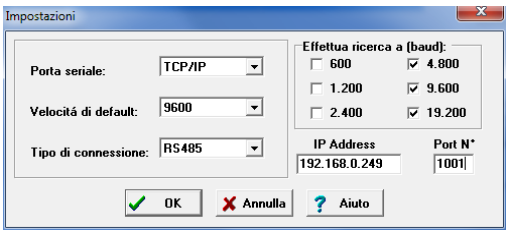
Per la <u>comunicazione seriale</u> impostare la porta COM assegnata dal sistema operativo e stabilire se il tipo di comunicazione è RS232 o RS485.

Per la <u>comunicazione IP</u>, scegliere “TCP/IP” e impostare “IP Address” e “Port N°”.

Cliccare su “OK”. Nella finestra principale cliccare su “Cerca”: verranno mostrati i terminali presenti sotto il canale di comunicazione impostato.



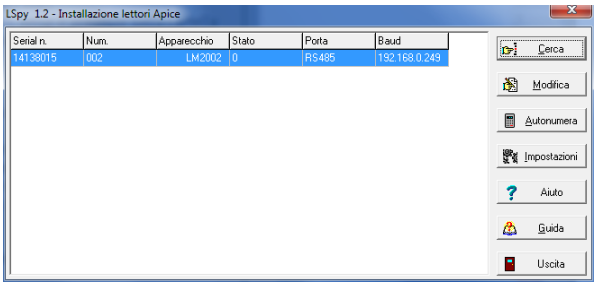


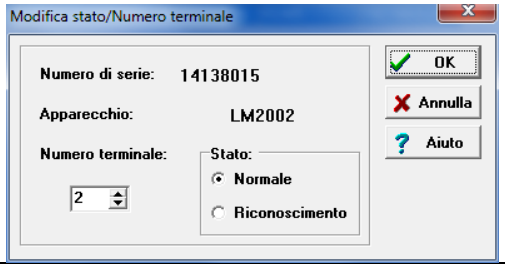


Nel caso in cui nell'impianto si abbia più di un terminale, è necessario assegnare a ciascuno di essi un numero identificativo univoco.

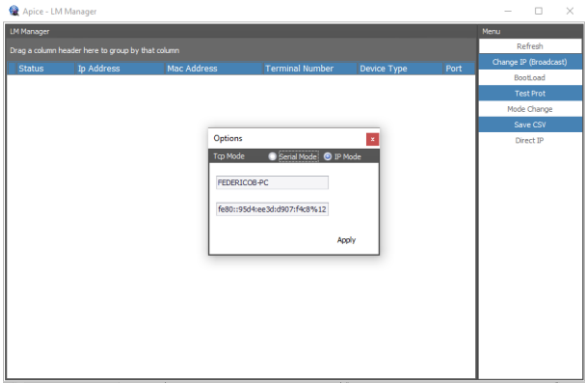
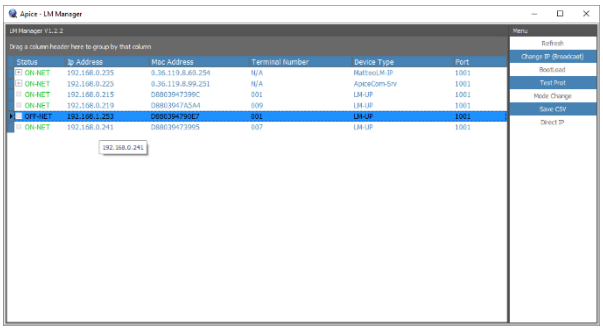
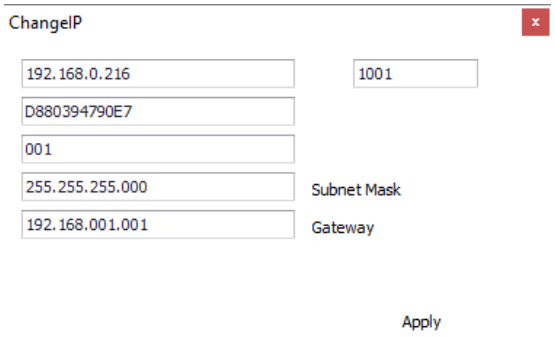
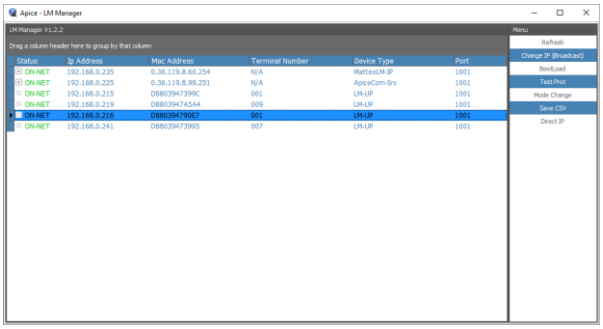
Per farlo selezionare la riga di un terminale e cliccare su "Modifica".

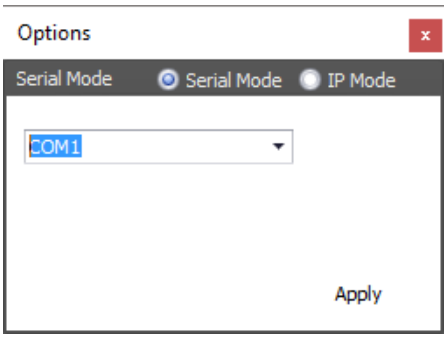
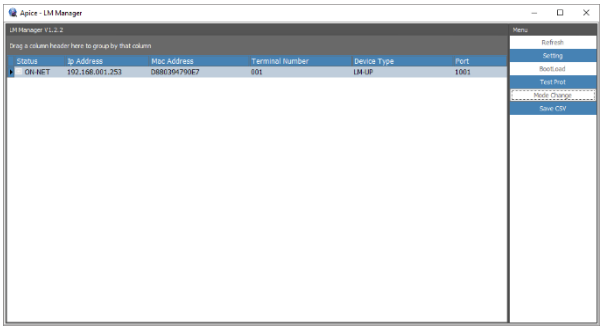
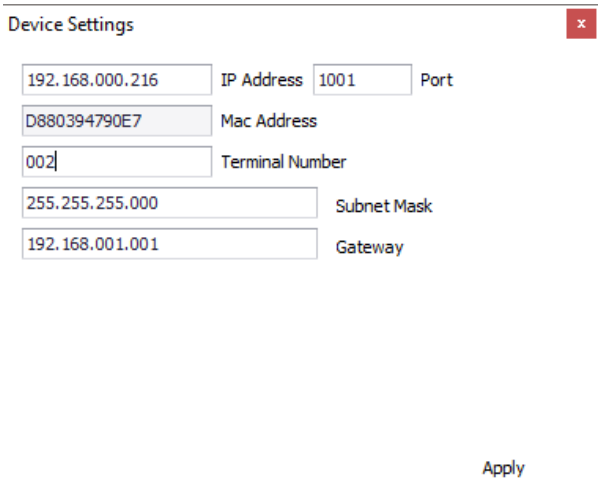
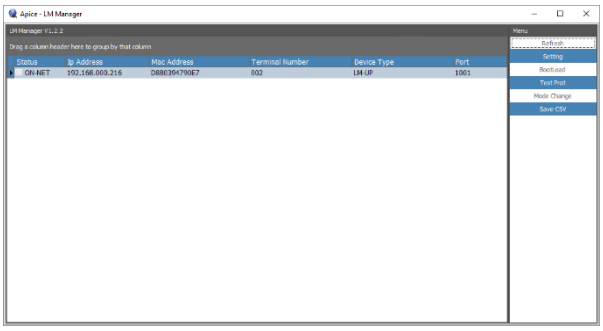
Cambiare il "Numero terminale" e cliccare su "OK".





LMUP

Lanciare il software LM Manager. Se non è già installato, è possibile scaricarlo dal sito www.aplus.srl. Selezionare il tipo di comunicazione tra il PC e uno o più terminali LMUP (IP o seriale).	
In caso di comunicazione IP il software effettuerà una scansione e individuerà i terminali collegati in rete. Ogni terminale LMUP ha la seguente configurazione di default: IP ADDRESS: 192.168.1.253 IP PORT: 1001 TERMINAL NUMBER: 001	
Cliccare su “ChangeIP” per cambiare i parametri di rete e il terminal number. Se nella rete sono presenti più terminali LMUP che verranno gestiti dal software, è necessario assegnare un terminal number diverso a ciascuno di essi. Cliccare su “Apply”. Effettuare un’altra scansione per verificare che il terminale abbia correttamente impostato i parametri.	 

Per cambiare il tipo di comunicazione con il terminale cliccare su “Mode Change”. In caso di comunicazione seriale (RS232 o RS485) con il terminale selezionare “Serial Mode”. Selezionare la COM del PC e cliccare su “Apply”.	
In caso di comunicazione seriale il software effettuerà una scansione e individuerà il terminale collegato (se utilizza la connessione RS232) oppure uno o più terminali collegati in rete (se si utilizza la connessione RS485). Ogni terminale LMUP ha la seguente configurazione di default: IP ADDRESS: 192.168.1.253 IP PORT: 1001 TERMINAL NUMBER: 001	
Cliccare su “Setting” per cambiare i parametri di rete e il terminal number. Se nella rete sono presenti più terminali LMUP che verranno gestiti dal software, è necessario assegnare un terminal number diverso a ciascuno di essi. Cliccare su “Apply”. Effettuare un’altra scansione per verificare che il terminale abbia correttamente impostato i parametri.	 

LM2002, LMIP, LEGGO® 2000 e LMUP

Lanciare ADM e scegliere il tab “Terminali” in alto.

Cliccare su “Nuovo” e inserire:

- Nome del terminale;
- Com. Type (tipo di comunicazione): scegliere Serial o TCP/IP;
- Term. Num., corrisponde al “Numero terminale” impostato in LSPY;
- Versione Firmware: scegliere il firmware appropriato per il tipo di terminale.

Esempio:

- per LM2002 o LMIP ultima versione scegliere LM2002/LMIP version >=5.10;
- per LEGGO® 2000 ultima versione scegliere version > 5.23;
- per TERP ultima versione scegliere TERP 2 version >= 5.20.

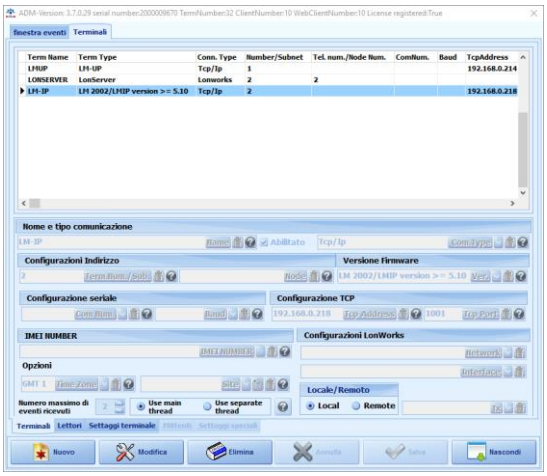
Nella lista sono presenti anche alcune versioni di firmware di vecchi terminali, per questioni di compatibilità con impianti esistenti.

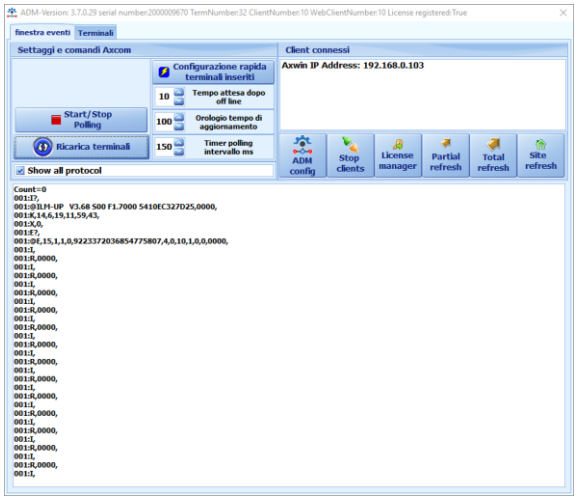
Se la comunicazione è IP, impostare Configurazioni TCP (TCP Address e TCP Port); in alternativa, se la comunicazione è seriale, impostare Configurazioni seriale (COM NUM e BAUD).

> Nota per la comunicazione seriale:
> - Baudrate per LM2002/LMIP è 9600;
> - Baudrate per LEGGO® 2000 e TERP è 19200 in RS232, 9600 in RS485;
> - Baudrate per LMUP è 9600 sia in RS232 che in RS485.

Cliccare su “Salva”.

Cliccare sul tab in alto “Finestra eventi” e cliccare sul tasto “Ricarica terminali”.





Dal tab in alto “Terminali”, selezionare la riga del terminale di cui si vuole completare la configurazione.

Cliccare su tab “Lettori”: di default è presente almeno un lettore, cliccare su “Modifica” per cambiarne le proprietà.

Cliccare su “Nuovo” per creare un nuovo lettore: i terminali LM2002/LMIP, LEGGO® 2000, TERP e LMUP sono in grado di gestire al massimo due lettori.

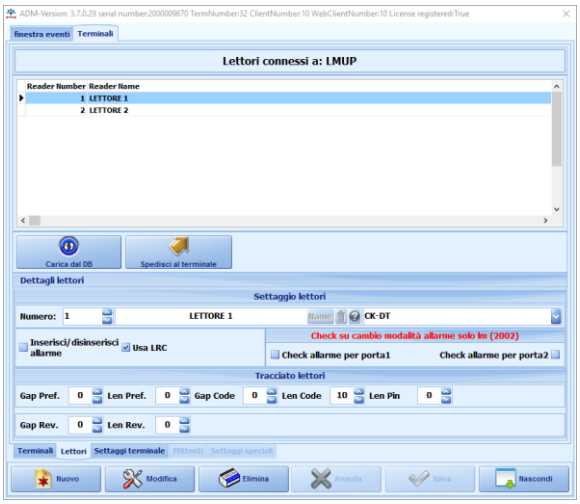
> Il “Numero” 1 o 2 che si associa al lettore corrisponde al connettore 1 o 2 per i lettori sulla scheda del terminale.

Impostare:

- nome del lettore,
- tipologia di lettore,
- tracciato lettori.

Per quest’ultimo parametro fare riferimento alla tabella sottostante, dove sono riportate le principali configurazioni a seconda del tipo di lettore utilizzato.

Cliccare su “Salva” e poi su “Spedisci al terminale”.



Si faccia riferimento alla tabella sottostante per impostare correttamente il tracciato lettori all'interno di ADM:

	Power Supply		Clock & Data			Wiegand		LED				Buzzer		Configurazioni standard	
	GND	+ VCC	CK	DT	CP	D0	D1	GREEN -	GREEN +	RED -	RED +	-	+	Tipo lettore	Tracciato lettura badge (GapPref. - LenPref. - GapCod. - LenCod.)
LA32		5												CK-DT	0 - 4 - 4 - 4 (con tessere standard Apice)
LA136		5												CK-DT	0 - 4 - 4 - 4 (con tessere standard Apice)
LA168		5												CK-DT	0 - 4 - 4 - 4 (con tessere standard Apice)
PROXY ONE		5/12												CK-DT	0 - 4 - 4 - 9
PROXY PRO		5/12												CK-DT	0 - 4 - 4 - 9
Proxy M (Mifare)		12												CK-DT	0 - 0 - 0 - 10
VKP/INOXC		12							12		12			CK-DT (no LRC)	0 - 0 - 0 - 8
BIOC		12												H10301 (prefisso 000)	non necessario
BIOXR	0	12				DT-LM*	CK-LM*							H10301 (prefisso 000)	non necessario
STID LXC-R11 (EM 125KHz)	0	12				DT-LM*	CK-LM*							LXC-R11	0 - 0 -1 -9 -LenPIN 4 (impostare usa PIN in memoria)
STID LXC-R31 (Mifare)	0	12				DT-LM*	CK-LM*							LXC-R31	0 - 0 -0 -10 -LenPIN 4 (impostare usa PIN in memoria)
STID UR1-URC	pin 1	pin 0	6	5										CK-DT	0 - 0 -4 -9
HID ProxPoint		12												Dipende dalla tessera	non necessario
HID R10		12												Dipende dalla tessera	non necessario

* DT o CK della morsettiera LMIP/LM2002

Selezionare la riga del terminale di cui si vuole completare la configurazione.

Cliccare su tab "Settaggi terminale".

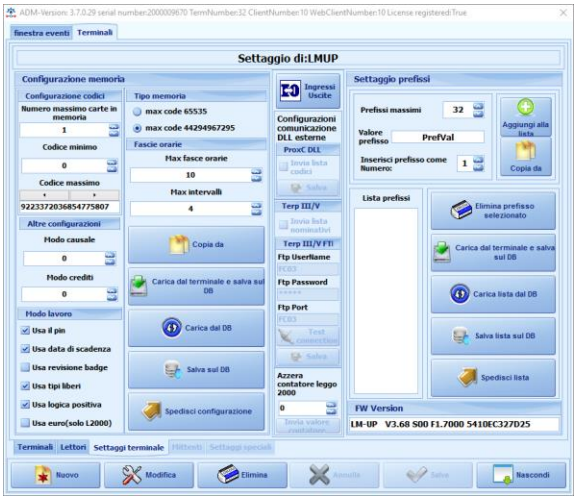
Impostare il "Numero massimo carte in memoria" (LMUP non considera questo campo).

Se si sta utilizzando un lettore con PIN, cliccare su "Usa il PIN".

Cliccare su "Salva sul DB" e successivamente su "Spedisci configurazione".

Se si utilizzano i prefissi, scrivere un prefisso in "Valore prefisso" e inserire un numero che identificherà quel prefisso ("Inserisci prefisso come Numero"); cliccare su "Aggiungi alla lista".

Cliccare su "Salva sul DB" e successivamente su "Spedisci configurazione".



Per impostare il funzionamento Ingressi/Uscite, cliccare su pulsante "Ingressi Uscite".

Per LM2002/LMIP e LMUP

Si aprirà la finestra a fianco dove è possibile impostare:

1 1 porta/relè, ovvero se il terminale deve gestire un unico varco con un solo lettore oppure con due lettori (uno in ingresso e uno in uscita);

- 2 porte/relè, ovvero se il terminale deve gestire due varchi con un lettore per ciascun varco;

2 se attivare relè 2 per codice non valido;

3 se attivare il relè se si verificano degli allarmi sul varco.

Per gestire gli allarmi sul varco (PORTA LASCIATA APERTA, INTRUSIONE, NON TRANSITO), occorre attivare il controllo dello stato porta.

È possibile avere:

- Nessuno controllo porta,
- Controllo porta 1,
- Controllo porta 2,
- Controllo porta 1 e 2.

Il controllo dello stato porta 1 va collegato fisicamente all'ingresso 1 del terminale LM2002/LMIP; nel terminale LMUP è etichettato ST1.

Il controllo dello stato porta 2 va collegato fisicamente all'ingresso 2 del terminale LM2002/LMIP; nel terminale LMUP è etichettato ST2.

È possibile interpretare questi due ingressi in due modi diversi a seconda della selezione:

- "Chiuso porta chiusa": se chiuso, significa che la porta è chiusa;
- "Aperto porta chiusa": se aperto, significa che la porta è aperta.

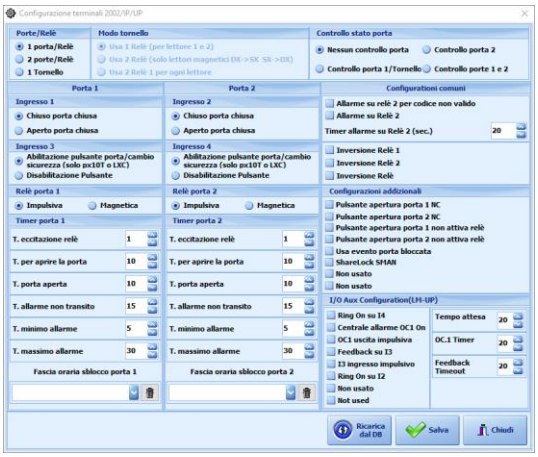
Il pulsante per aprire la porta 1 va collegato fisicamente all'ingresso 3 del terminale LM2002/LMIP; nel terminale LMUP è etichettato PB1.

Il pulsante per aprire la porta 2 va collegato fisicamente all'ingresso 4 del terminale LM2002/LMIP; nel terminale LMUP è etichettato PB2.

È possibile abilitare o disabilitare l'utilizzo del pulsante per il terminale.

È possibile impostare per i due relè un comportamento di tipo:

- impulsivo: il relè si eccita per i secondi stabiliti dal campo "T. eccitazione relè" (adatto per elettroserrature);
- magnetico: è necessario utilizzare il controllo dello stato del varco, il relè rimane eccitato



fintanto che la porta, dopo il transito, non viene richiusa.

È possibile far lavorare i relè 1 e 2 in maniera inversa, tramite i comandi “Inversione Relè 1”, e “Inversione Relè 2”: a riposo il relè è attivo, mentre si disattiva a seguito di un’abilitazione.

La funzione “Inversione Relè” scambia il relè 1 con il relè 2.

È possibile scegliere una “Fascia oraria di sblocco per la porta 1” e una “Fascia oraria di sblocco per la porta 2”, scegliendo tra le fasce orarie create. Se si imposta questa funzione, in quella determinata fascia oraria il relè è attivo e quindi permette l’apertura della porta.

Nei timer porta è possibile scegliere:

→ T. eccitazione relè

Stabilisce il tempo di attivazione dell’uscita del terminale che comanda l’elettroserratura del varco.

→ T. per aprire la porta

Tempo massimo che ha un utente per transitare dal varco, dopo la richiesta di accesso tramite badge o pulsante.

→ T. Porta Aperta

Stabilisce il tempo massimo per cui la porta può stare aperta. Terminato questo tempo, scatta l’allarme di “PORTA LASCIATA APERTA”.

→ T. Allarme non transito

Stabilisce il tempo per cui sta attivo l’allarme di “NON TRANSITO”.

→ T. Minimo Allarme

Stabilisce il tempo minimo per cui è attivo l’allarme “INTRUSIONE” o “PORTA LASCIATA APERTA”.

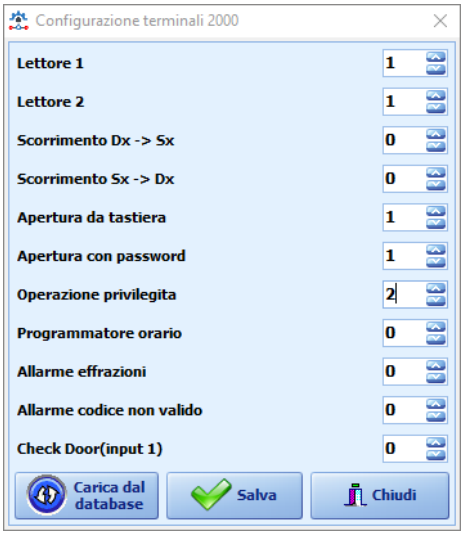
→ T. Massimo Allarme

Stabilisce il tempo massimo per cui è attivo l'allarme "INTRUSIONE" o "PORTA LASCIATA APERTA".

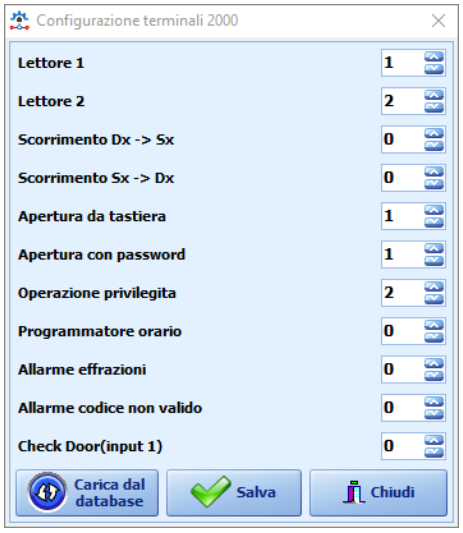
Cliccare su "Salva" e successivamente su "Chiudi".

Per LEGGO® 2000

Impostare come mostrato nella figura a fianco se vogliamo che entrambi i lettori attivino il primo relè.



Impostare come mostrato nella figura a fianco se vogliamo che il primo lettore attivi il primo relè, mentre il secondo lettore attivi il secondo relè.



Cliccare su "Salva" e successivamente su "Chiudi".

TERMINALE LONSERVER

Si suppone che l'utente che crea da zero un sistema con prodotti A PLUS in tecnologia LonWorks® abbia un minimo di conoscenza e dimestichezza con la terminologia e gli strumenti utilizzati in questa tecnologia.

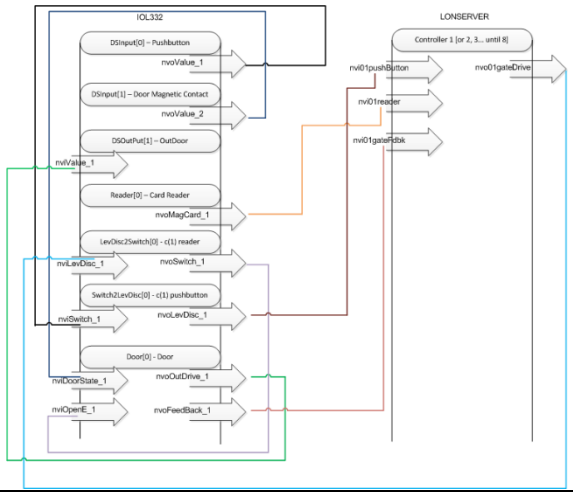
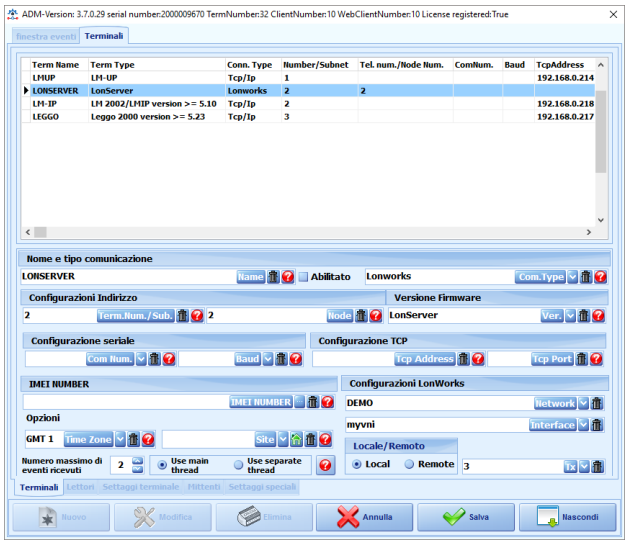
Prima di tutto occorre creare un progetto LonWorks®, tramite un software di gestione reti LonWorks® (ad esempio Open LNS di Echelon o NL220 di Newron System).

Nel progetto, oltre ad essere presenti uno o più LonServer, ci sono anche terminali IOL332 di A PLUS, in grado di gestire uno o più varchi.

Si tenga presente che ogni LonServer può gestire al massimo 8 varchi. Questi 8 varchi possono essere gestiti con un solo lettore di badge, oppure con doppio lettore di badge: pertanto ogni LonServer può gestire al massimo 16 lettori.

Un progetto LonWorks® stabilisce con che tipo di interfaccia il PC comunicherà con il campo:

- Interfaccia USB/FT-10;
- Interfaccia IP-RNI;
- Interfaccia IP-852.

Di fianco sono mostrati i binding tipici da realizzare nel progetto LonWorks tra LonServer e IOL332. Al LonServer inserito nell'impianto sarà assegnato un SUBNET ID e un NODE ID. Commissionare i nodi LonWorks creati nel progetto.	Binding tra IOL332 e un controller del LonServer 
Lanciare ADM e scegliere in alto il tab "Terminali". Cliccare su "Nuovo" e inserire: • Nome del terminale; • Com. Type (tipo di comunicazione): scegliere Lonworks; • Sub corrisponde al SUBNET ID, che viene assegnato nel progetto LonWorks; • Node corrisponde al NODE ID, che viene assegnato nel progetto LonWorks; • Firmware version; • scegliere il LonServer; • Network, ovvero il nome del progetto LonWorks; • Interfaccia utilizzata per connettersi ai terminali LonWorks in campo; • TX: 7s; • Local/Remote: Locale. Cliccare su "Salva". Cliccare sul tab in alto "Finestra eventi" e poi sul tasto "Ricarica terminali".	

Dal tab “Terminali” in alto, selezionare la riga del terminale di cui si vuole completare la configurazione.

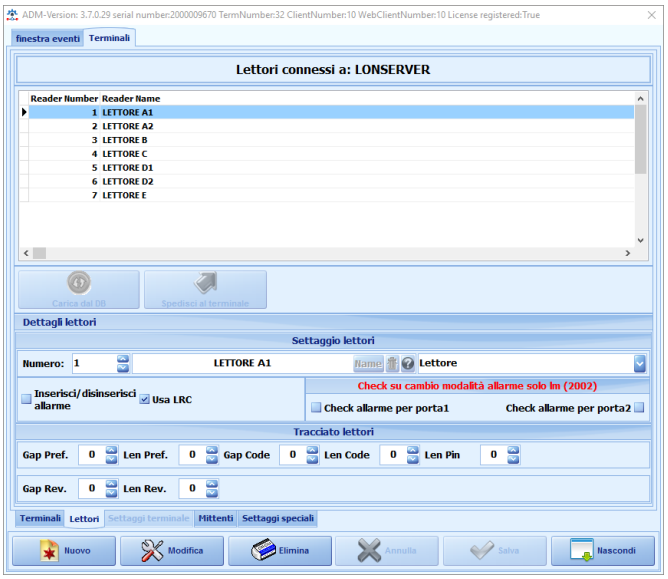
Cliccare su tab “Lettori”.

Almeno un lettore è già creato di default, cliccare su “Modifica” per cambiarne le proprietà.

Per ogni lettore riempire i campi:

- numero:
  - se un controller del LonServer gestisce un varco con un solo lettore inserire questo lettore con numero dispari, in maniera progressiva (1, 3, 5, 7, 9, 11, 13, 15);
  - se un controller del LonServer gestisce un varco con doppio lettore inserire il lettore di ingresso con numero dispari in maniera progressiva (1, 3, 5, 7, 9, 11, 13, 15) e il lettore di uscita con numero pari in maniera progressiva (2, 4, 6, 8, 10, 12, 14, 16);
- nome del lettore.

Gli altri campi non sono obbligatori.



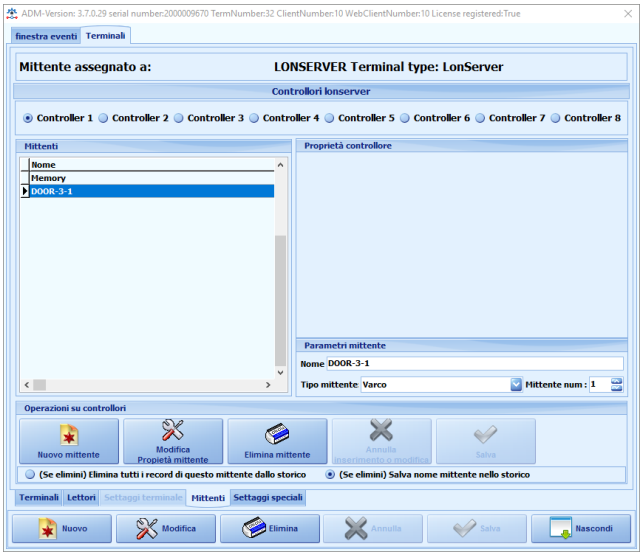
Dal tab “Terminali” in alto, selezionare la riga del terminale di cui si vuole completare la configurazione.

Cliccare su tab “Mittenti”.

Selezionare il primo Controller (l’elemento virtuale di controllo del varco).

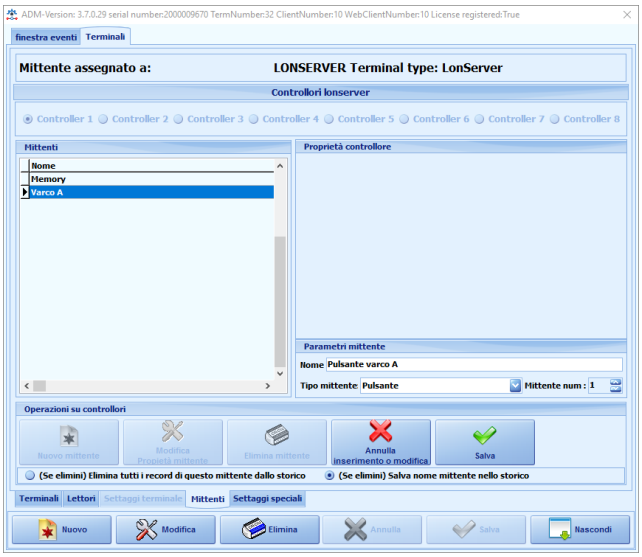
Selezionare la riga con il Tipo=Varco, cliccare su “Modifica Proprietà mittente”, inserire il nome desiderato per il varco controllato dal primo Controller del LonServer. Cliccare su “Salva”.

Se per questo varco si utilizza anche il pulsante cliccare su “Nuovo mittente”, scegliere il tipo di Mittente=Pulsante e inserire un nome per il pulsante. Cliccare su “Salva”.



Se per questo varco si utilizza un lettore a tastiera cliccare su “Nuovo mittente”, scegliere il tipo di Mittente=Tastiera e inserire un nome per la tastiera.Cliccare su “Salva”.

Ripetere le operazioni fatte per il controller 1, anche per gli altri controller che gestiscono i varchi.



TERMINALE TERP 3/4

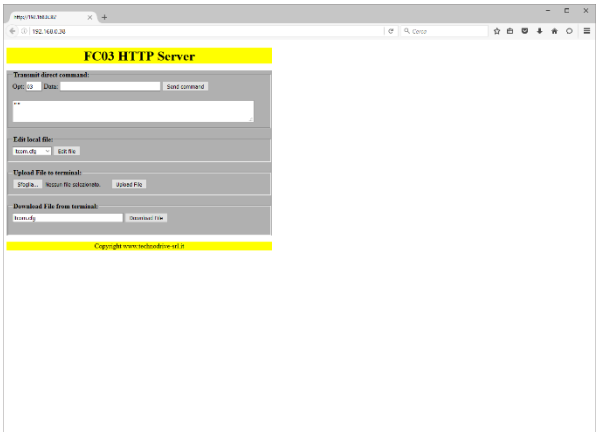
Dal display entrare nelle configurazioni con le seguenti credenziali:

Nome utente: FC03
Password: 12345

Configurare IP Address, Subnet mask e Gateway.

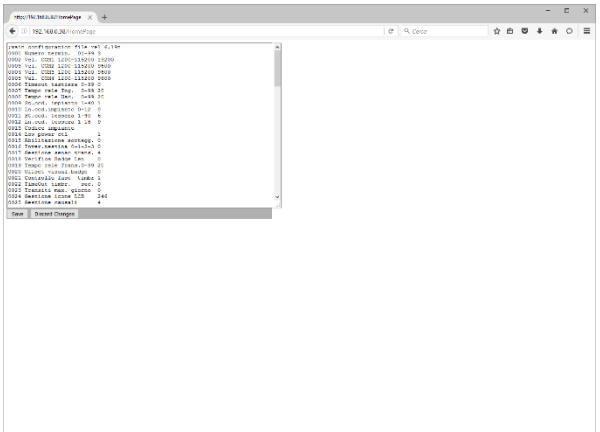
Continuare con la modifica dei parametri di configurazione direttamente da display, oppure accedere alla pagina web del terminale, digitando l'indirizzo IP configurato in un qualsiasi browser internet.

Verrà richiesto Nome utente e Password, una volta eseguito l'accesso apparirà la schermata mostrata a fianco.



In "Edit" > "Local File" selezionare "*ltcom.cfg*" e cliccare su "Edit file".

Nel file modificare il numero di terminale e i seguenti parametri a seconda del lettore integrato nel terminale:



125kHz

Parametro 11	5
Parametro 12	9
Parametro 53	0 di default (lettura come PROXY-ONE/PROXY-PRO) 16 se si vuole leggere il codice in 5 byte decimale dritto.

MAGNETICO IOS2

Parametro 11	5
Parametro 12	4
Parametro 17	1

Mifare

Parametro 11	1
Parametro 12	10
Parametro 77	3 (7 per TERP IIIs con lettore integrato)

Mifare + Bio

Parametro 11	1
Parametro 12	10 (dipende dal codice assegnato all'impronta)
Parametro 34	7
Parametro 77	1

Solo Bio

Parametro 11	1
Parametro 12	10 (dipende dal codice assegnato all'impronta)
Parametro 34	10
Parametro 77	0

Altri parametri per far funzionare il TERP 3/4 con ADM sono:

Parametro 34	**>0** **1** lista badge **2** lista badge + eventuale PIN **3** lista badge + fasce **4** lista badge + fasce + eventuale PIN
Parametro 43	**1** registra accesso negato **2** scatta relè 1 **4** scatta relè 2
Parametro 56	**56** (40 per mensa)

Cliccare su "Save".

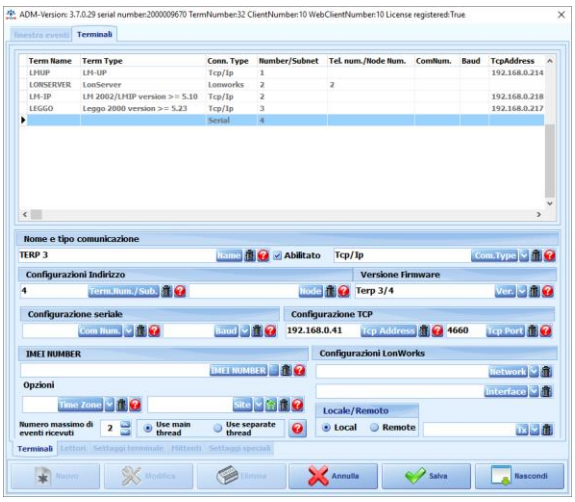
Lanciare ADM e scegliere il tab in alto “Terminali”; cliccare su “Nuovo”.

Inserire:

- nome del terminale;
- Com. Type (scegliere Tcp/IP);
- Term. Num. (corrisponde al “Numero terminale” impostato da Display oppure da pagina web);
- Firmware Version (scegliere il firmware TERP 3/4);
- impostare Settaggi TCP (TCP Address e TCP Port).

Cliccare su “Salva”.

Cliccare sul tab in alto “Finestra eventi” e cliccare sul tasto “Ricarica terminali”.



Dal tab in alto “Terminali”, selezionare la riga del terminale di cui si vuole completare la configurazione.

Cliccare su tab “Lettori”.

Almeno un lettore è già creato di default, cliccare su “Modifica” per cambiarne le proprietà.

Cliccare su “Nuovo” per creare un nuovo lettore.

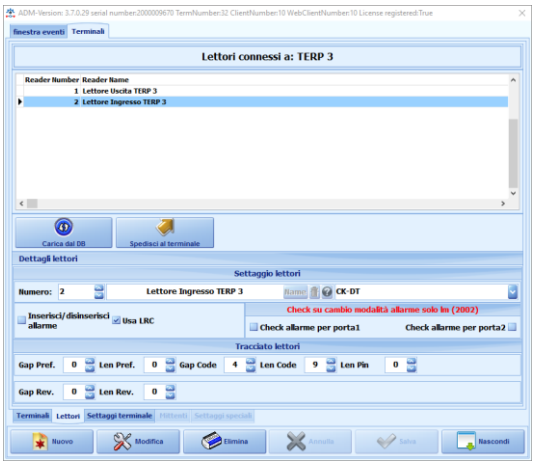
> “Numero” = 1 è riferito al LETTORE DI USCITA.
>
> “Numero” = 2 è riferito al LETTORE DI INGRESSO.

Anche se il lettore integrato è soltanto uno, cliccando sulle icone a display è possibile discriminare tra ingresso e uscita.

Impostare:

- nome del lettore;
- nel tracciato lettori è fondamentale impostare solo il campo “Len Code”, che deve essere esattamente uguale a quello impostato da display o pagina web.

Cliccare su “Salva” e poi su “Spedisci al terminale”.



Selezionare la riga del terminale di cui si vuole completare la configurazione.

Cliccare su tab “Settaggi terminale”.

Abilitare “Invia lista nominativi” se si vuole che sul display appaia, oltre al codice, il nome e il cognome della persona a cui appartiene il badge.

Impostare “FTP UserName” e “FTP Password”: sono le stesse usate per entrare nella pagina web.

FTP Port=21

Cliccare su “Test connection” per verificare la correttezza della connessione FTP.

Cliccare su “Salva”.

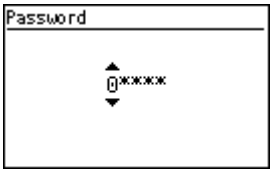
TERMINALE TERPV/TERPV UP

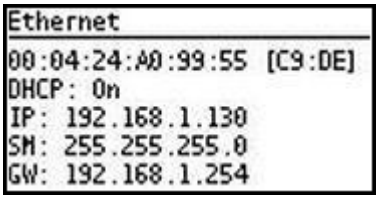
Premete .F + ▲ per visualizzare il prompt di richiesta password operatore:

- il primo valore mostrato per ciascuna cifra è sempre '0', per cui essendo "00000" la password di default è sufficiente premere Enter 5 volte per accedere al menù supervisore;
- il sottomenù "Ethernet" mostra l'indirizzo MAC, lo stato DHCP e gli attuali indirizzi IP, subnet e gateway. Impostare l'indirizzo IP desiderato al terminale (disattivare DHCP);
- configurare il terminale mediante un menù a interfaccia grafica disponibile alla pagina iniziale del web server HTTP del terminale (http://<Indirizzo_IP_Terminale>).

L'unico nome utente riconosciuto dal sistema è "admin" e la password assegnata inizialmente all'utente "admin" è "admin".

Una volta avuto accesso al menù HTTP con queste credenziali, è possibile modificare la password.





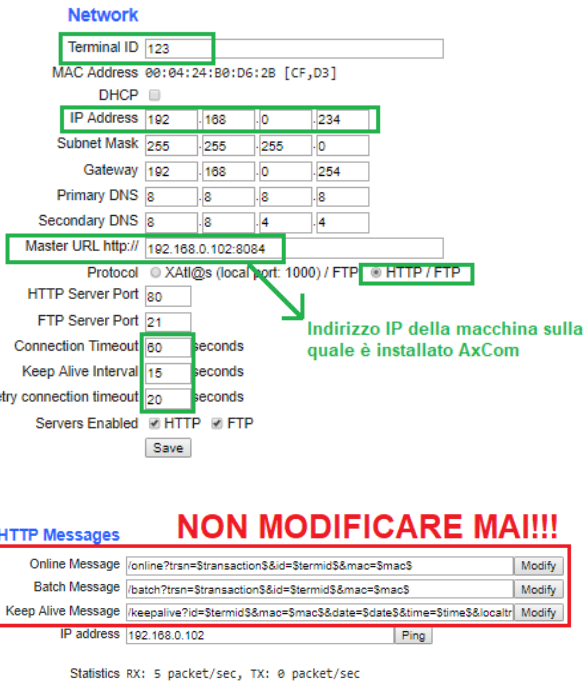
Entrando nelle configurazioni dal browser nella pagina "Network", impostare:

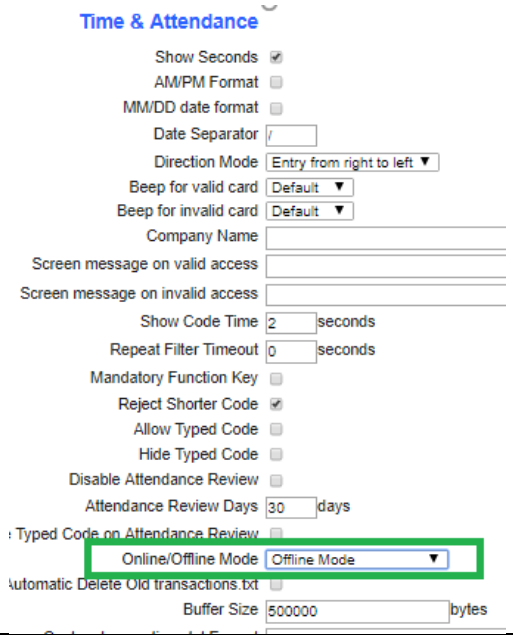
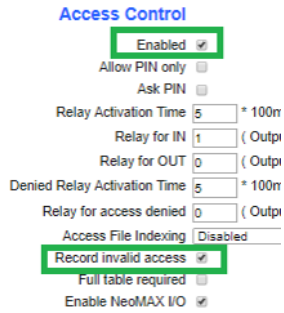
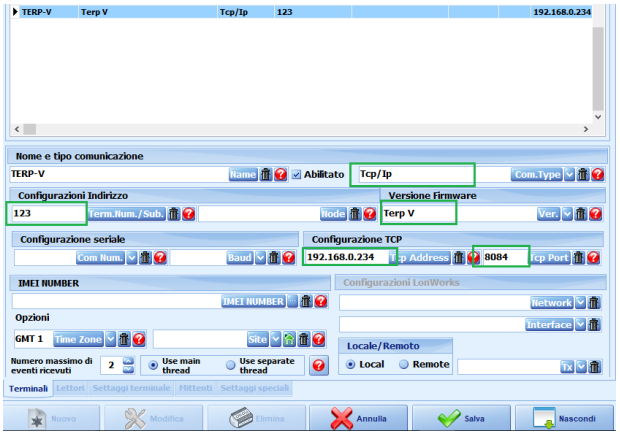
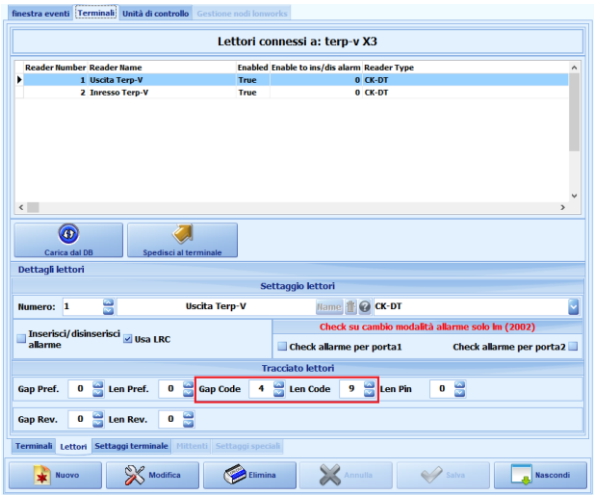
- "Terminal ID" = Numero del terminale (123);
- IP Address = indirizzo IP del terminale;
- Master URL = (indirizzo IP della macchina sulla quale è installato ADM: porta 8084);
- spuntare "HTTP / HTTPS / FTP";
- Connection Timeout = 60;
- Keep Alive Interval = 15;
- Retry connection timeout = 20.

Cliccare su "Save".

I primi due punti devono essere impostati allo stesso modo su ADM.

Non modificare/cambiare mai gli "Http Messages".

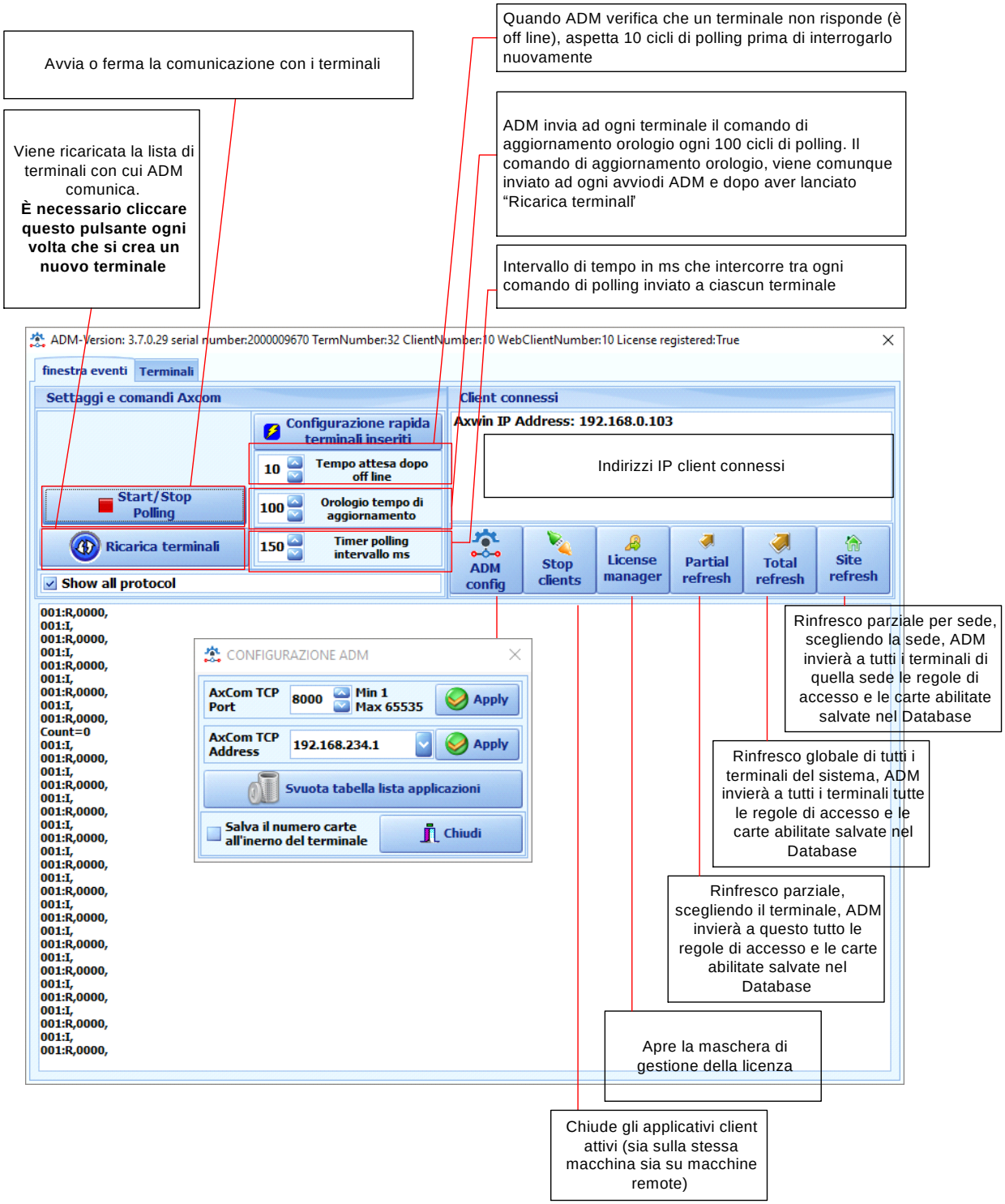


Entrando nelle configurazioni dal browser nella pagina “Time & Attendance” impostare “Offline Mode”. Cliccare su “Save”.	
Abilitare il “Controllo Accessi” e spuntare “Record invalid access” nella pagina “Access Control”. Cliccare su “Save” e poi su “Riavviare il dispositivo”.	
Avviare ADM e impostare come in figura accanto: • Com.Type = TCP/IP; • Term.Num = Numero del terminale impostato precedentemente (123); • Ver.Firm = TERPV; • Tcp Address = indirizzo IP del terminale; • Tcp Port = 8084. Cliccare su “Salva”.	
Configurazione dei lettori via HTTP nella pagina “Reader 1” e “Reader 2”: ***125 kHz*** Card Decode: 33.Generic Serial Reader Baudrate: 57600 Code Begin: 3 Code Lenght: 10 *oppure* Code Begin: 4 Code Lenght: 9	

MIFARE Card Decode: 33.Generic Serial Reader Baudrate: 57600 Code Begin: 0 Code Lenght: 10 I lettori si possono configurare anche da ADM.	

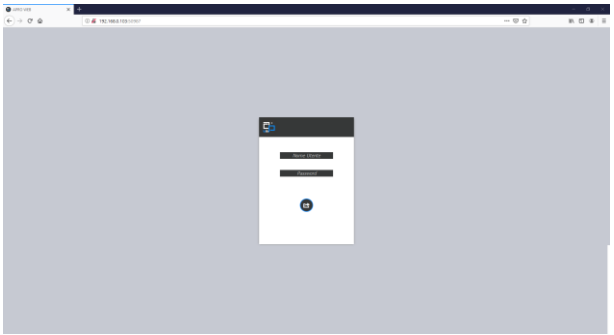
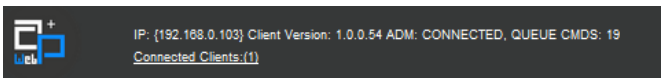
3. Finestra eventi

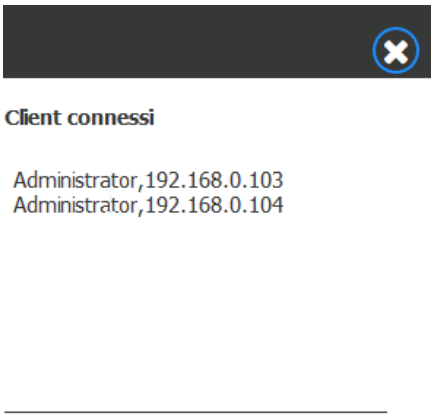
Nella figura sottostante vengono spiegate le funzioni che possono essere attivate dalla “Finestra eventi” di ADM:



4. Interfaccia WEB Utente: APRO WEB

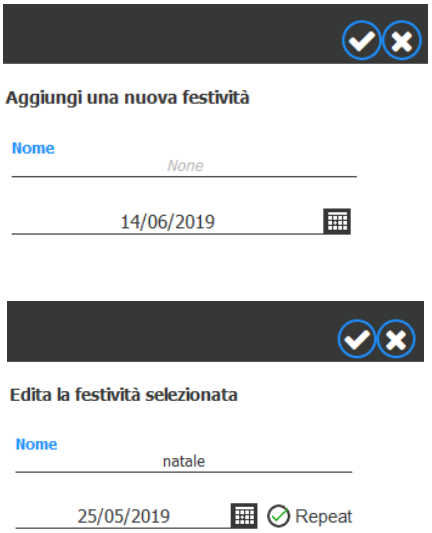
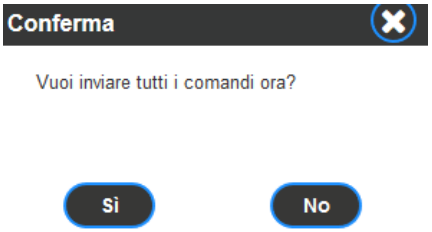
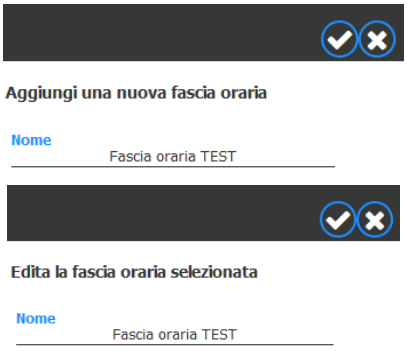
4.1. Credenziali di accesso

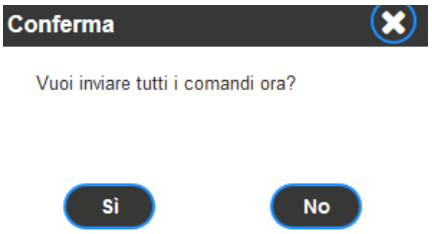
Per accedere all'interfaccia web del terminale, lanciare un browser internet da una macchina facente parte della stessa rete dove risiede il server. Nell'URL del browser digitare: xxx.xxx.xxx.xxx:50987 dove xxx.xxx.xxx.xxx è l'indirizzo IP del server. 50987 è la porta del server. Assicurarsi che ADM sia attivo sul server: ADM deve essere in esecuzione per far sì che le regole di accesso e i codici che vengono abilitati in APRO WEB siano immediatamente inviati ai terminali. Allo stesso modo, ADM è in grado di scaricare gli eventi dai terminali in campo. Per accedere, immettere nome utente e password, che sono, di default: Nome utente: admin Password: admin Al primo avvio verrà richiesto l'aggiornamento della password di accesso per l'utente "admin".	
In alto a destra è mostrato: • l'operatore loggato e il suo ruolo (es. ADMINISTRATOR) • il pulsante per la scelta della lingua: • il pulsante "Info": se il cerchio è verde significa che c'è comunicazione con ADM, se è rosso non c'è comunicazione:	
Cliccando sul pulsante "Info" vengono mostrate alcune informazioni utili: • l'indirizzo IP del server;	

• la versione del software APRO WEB; • se ADM è connesso o disconnesso; • i comandi in coda, che devono ancora essere inviati ai terminali in campo; • Connected Clients: indica il numero di sessioni attive. Se l'operatore ha un ruolo "TOTALE" sulla funzione "PRINCIPALE" (vedi menu "Account"), può cliccare su "Connected Clients", per avere il dettaglio delle sessioni connesse.	

Di seguito sono riportati, in sequenza, i passi da effettuare per creare uno o più badge di accesso da assegnare ad un utente.

4.2. Creazione Fasce Orarie

Se nel sistema è richiesto l'uso delle fasce orarie, seguire i passi seguenti. Prima di tutto occorre stabilire se si vogliono gestire delle festività. Scegliere "Configurazioni" e nel tab "Festività" cliccare su per aggiungere un nuovo giorno festivo, oppure selezionare un giorno festivo già creato e cliccare su . Impostare: • nome della festività, • data della festività.	
Viene richiesto se inviare tutti i comandi, si consiglia di cliccare "Sì".	
Se viene cliccato "No", ricordarsi successivamente di cliccare su . Se si utilizzano più sedi, selezionare per quale sede applicare la festività.	
Scegliere "Configurazioni" e nel tab "Fasce Orarie" cliccare su per aggiungere una nuova fascia oraria, oppure selezionare una fascia oraria già creata e cliccare su . Impostare: • nome fascia oraria.	

Per ognuno dei 4 intervalli temporali è possibile scegliere per quali giorni della settimana applicare l'ora di inizio e fine validità:	
Per rendere effettiva una modifica è necessario cliccare sul , per annullare cliccare su . Viene richiesto se inviare tutti i comandi, si consiglia di cliccare "Sì".	
Se viene cliccato "No", ricordarsi successivamente di cliccare su .	

4.3. Creazione Gruppi

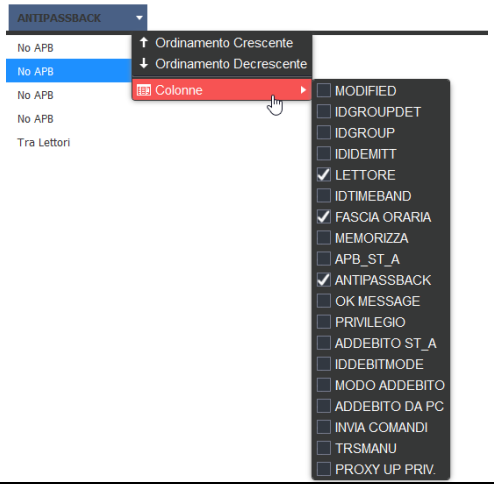
È necessario creare almeno un gruppo; di seguito i passi da seguire per la creazione/modifica di un gruppo.

Ogni gruppo contiene tutti i lettori del sistema ed è caratterizzato dalle modalità di transito che le persone appartenenti hanno per ogni lettore, ovvero:

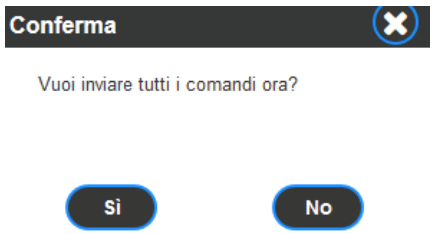
- se possono transitare solo in alcune fasce orarie;
- se i loro transiti devono essere memorizzati;
- se devono rispettare un antipassback associato;
- se il lettore deve mostrare un messaggio sul display al passaggio dell'utente e quale messaggio;
- se hanno un privilegio;
- se ogni transito comporta un certo addebito;
- se è necessaria la verifica della loro presenza in certe aree.

Il gruppo spiega in modo molto dettagliato tutte le modalità di transito, ma non specifica in quali lettori l'utente può transitare o meno, cosa che è possibile specificare con i profili.

Scegliere "Configurazioni" e nel tab "Gruppi" cliccare su per aggiungere un nuovo gruppo, oppure selezionare un gruppo già esistente e cliccare su .	
Impostare: • nome del gruppo.	
Per ogni lettore è possibile stabilire una serie di configurazioni di accesso, di default sono mostrate solo le colonne principali. Per modificare un parametro, fare doppio click.	
È possibile copiare la configurazione impostata per un lettore (di un gruppo), selezionando il lettore e cliccando su .	

Per incollare questa configurazione su uno o più lettori cliccare su .	
Per mostrare tutti i parametri disponibili, cliccare sul simbolo all'estremità dell'intestazione di una colonna , scegliere "Colonne", selezionare le colonne da visualizzare.	
Di seguito sono spiegati nel dettaglio i significati delle colonne e l'applicabilità ai vari terminali: → Fasce Orarie Per ogni lettore è possibile assegnare una fascia oraria, precedentemente creata. Applicabile per i terminali: LM2002, LMIP, LEGGO® 2000, TERP, LMUP, LonServer. → Antipassback Per ogni lettore è possibile stabilire se applicare una regola di antipassback nei confronti dell'altro lettore, o tra i due sensi di scorrimento in caso di lettore magnetico. Si tratta di un antipassback "Hardware", è il terminale stesso che si occuperà di abilitare/disabilitare il proprio lettore sotto regola antipassback. Applicabile per i terminali: LM2002, LMIP, LEGGO® 2000, TERP, LMUP (LMUP non supporta l'antipassback nei due sensi di scorrimento). → Memorizza Per ogni lettore è possibile stabilire se registrare i transiti oppure no per tutti gli utenti appartenenti al gruppo corrente. Applicabile per i terminali: LM2002, LMIP, LEGGO® 2000, TERP, LMUP.	

→ OK Message Se abilitato mostra sul display (per LEGGO® 2000 e TERP) il messaggio “Entrare prego carta valida”, quando viene passata una tessera valida sul lettore. Applicabile per i terminali: LEGGO® 2000, TERP. → Privilegio Se abilitato, considera il gruppo di utenti corrente come “privilegiato” a passare sul lettore. Il privilegio consente, per gli LM2002 e LMIP con firmware “allarmi”, di disattivare lo stato di allarme. Il privilegio consente, per il LonServer, di entrare in un varco in allarme o di disattivare lo stato di allarme a seconda delle configurazioni. → Addebito StA L’“Addebito Stand Alone” è applicabile solo per il LEGGO® 2000. Quando è > 0 il LEGGO® 2000 decrementa il suo credito a ogni passaggio dal lettore di un valore impostato. Il credito massimo addebitabile a ogni passaggio dal lettore è 254. Se si imposta 255, viene richiesto di inserire il credito da tastiera come una causale. È necessario attivare nelle configurazioni del LEGGO® 2000 il “Modo credito”. → Modo Addebito e Addebito da PC Riguarda l’abilitazione dell’addebito attravero il PC. Non appena il software riceve un evento legato a questo lettore e questo utente, applica l’addebito all’utente secondo quanto stabilito in “Modo Addebito”: • *Fisso*, addebiterà un valore fisso stabilito in “Addebito da PC” (Applicabile per LM2002, LMIP, LEGGO® 2000, TERP); • *Causale*, addebiterà il valore immesso come causale da tastiera del LEGGO® 2000 o TERP. È necessario attivare nelle configurazioni dei terminali, in ADM, il “Modo credito”.	

→ Invia Comandi Non utilizzato. → Priv. Proxy-UP Applicabile al terminale LMUP connesso in RS485 o RS232 con un lettore PROXY-UP. Se abilitato consente all'utente del gruppo corrente che passa sul lettore PROXY-UP di inserire o disinserire l'allarme (un'uscita del LMUP si attiva o disattiva, questa uscita è connessa all'ingresso di una centrale di allarme).	
Per rendere effettiva una modifica è necessario cliccare sul , per annullare cliccare su . Viene richiesto se inviare tutti i comandi, si consiglia di cliccare "Sì".	
Se viene cliccato "No", ricordarsi successivamente di cliccare su .	

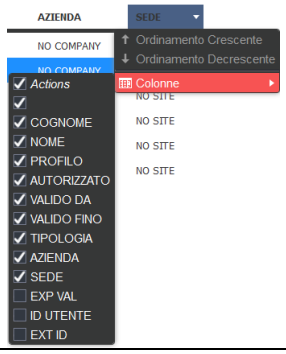
4.4. Creazione Profili

Un profilo è un sottoinsieme di lettori. Al momento della sua creazione occorre associarlo a un gruppo precedentemente creato: in questo modo eredita direttamente tutte le modalità di accesso stabilite dal gruppo. L'entità "Profilo", alla fine della sua configurazione, rappresenta tutte le regole di accesso che verranno successivamente assegnate a uno o più utenti e definiscono dove, quando e come avere accesso.

Scegliere "Configurazioni" e nel tab "Profili" cliccare su per aggiungere un nuovo gruppo, oppure selezionare un gruppo già esistente e cliccare su .	
Impostare: • nome profilo, • gruppo, • sede (opzionale).	
Per ogni profilo occorre stabilire quali lettori devono far parte del profilo, cliccando su , oppure su per escluderli.	
Per rendere effettiva una modifica è necessario cliccare sul , per annullare cliccare su .	

4.5. Creazione Utenti

Una volta stabilite le regole di accesso è possibile creare uno o più utenti a cui associare tali regole e il codice di badge con cui fare gli accessi.

Scegliere “Utenti” . Di seguito la visualizzazione dell’archivio degli utenti. È possibile visualizzare **tutti** gli utenti nel Database e impostare dei filtri per colonna.	
Per estendere le colonne visualizzate, cliccare sul simbolo all’estremità destra dell’intestazione di una colonna , scegliere “Colonne”, selezionare le colonne da visualizzare.	
In generale, per rendere effettiva una modifica è necessario cliccare su , per annullare cliccare su .	

Di seguito sono dettagliate alcune icone:

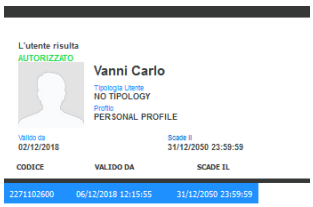
“Filtri”, attiva/disattiva la visibilità dei filtri sulle colonne.

“Esporta”, la lista visualizzata è esportata in formato “*.xls*”.

Icona di notifica “Valido”, indica se l’utente è non scaduto e “AUTORIZZATO”.

Icona di notifica “Non valido”, indica se l’utente è scaduto o “NON AUTORIZZATO”.

“Informazioni”, viene mostrata la scheda in sintesi dell’utente:



“Modifica”, equivale a fare il doppio click sulla riga. Si apre la finestra di creazione/modifica utente.

“Nuovo”, per creare un nuovo utente. Si apre la finestra di creazione/modifica utente.

“Elimina”, per eliminare l’utente selezionato.

“Refresh”, per aggiornare la visualizzazione della lista degli utenti.

“Utenti-Lettori”, finestra per la visualizzazione a matrice del legame Utenti/Lettori e Utenti/Ascensori

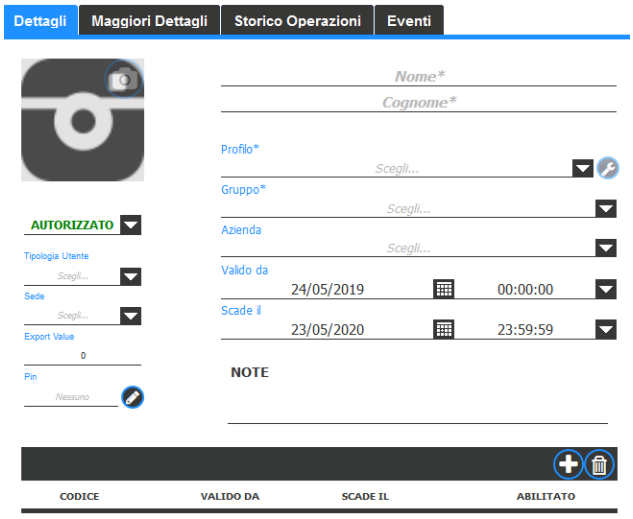
4.5.1. Finestra utente: Dettagli

Entrando nella finestra di creazione/modifica utente, tab “Dettagli” è possibile creare, modificare o eliminare un utente.

Compilare i campi seguenti:

- campi obbligatori:
  - ABILITATO/NON ABILITATO,
  - nome,
  - cognome,
  - profilo (da scegliere tra i profili precedentemente creati). Tra i profili è possibile scegliere “PERSONAL PROFILE”, il profilo è personalizzabile per ogni utente, composto come insieme di più profili già creati o come insieme di lettori,
  - gruppo, solo nel caso in cui in Profilo si è scelto di usare “PERSONAL PROFILE”, negli altri casi, il gruppo è già un’informazione contenuta nel profilo scelto.

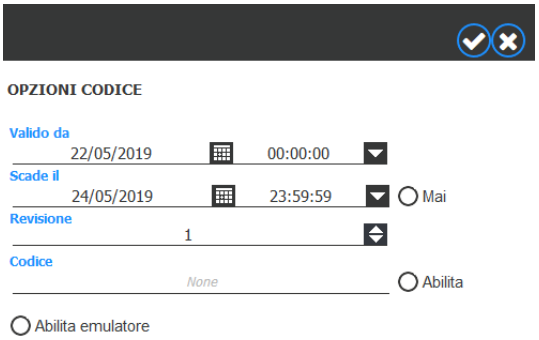
- campi facoltativi:
  - azienda,
  - tipologia utente,
  - sede,
  - PIN,
  - Export Value (valore alfanumerico, utilizzato tipicamente per inserire una matricola o il codice fiscale),
  - Valido da…,
  - Scade il …,
  - note,
  - foto, cliccando sopra l’icona è possibile caricare una foto.



In basso, è possibile aggiungere uno o più codici, cliccando su . Per cancellare un codice, selezionare la riga e cliccare su .

Compilare i campi seguenti:

- Valido da...,
- Scade il...,
- Revisione,
- Codice (campo numerico),
- Abilita/Disabilita.



Un codice può essere immesso manualmente oppure avvalendosi di un emulatore, in tal caso selezionare "Abilita emulatore".

L'emulatore è un lettore USB da connettere al PC dove si sta usando APRO WEB: passando il badge sull'emulatore, questo automaticamente riempie il campo di testo su cui il mouse sta puntando con il codice del badge.

Oltre ad aver messo il flag su "Usa emulatore", è necessario avere connesso al PC un emulatore APICE/A PLUS (ad esempio EPR o EMU-P) e avere avviato il software "Multi Prox Reader".

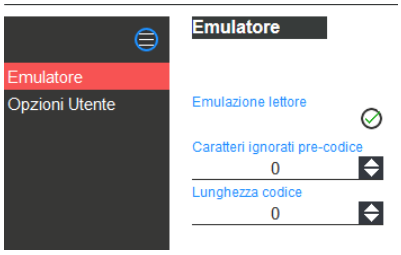
Se si utilizza l'emulatore è inoltre necessario configurare i seguenti parametri.

Scegliere "Opzioni di sistema" , "Emulatore":

- Abilitare "Emulazione lettore";
- Impostare "Caratteri ignorati pre-codice";
- Impostare "Lunghezza codice".

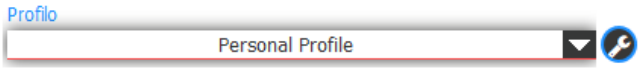
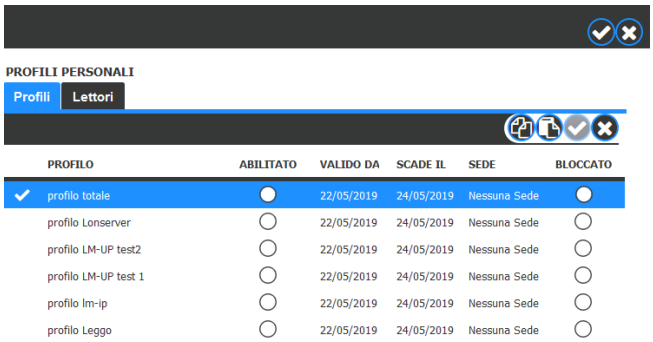
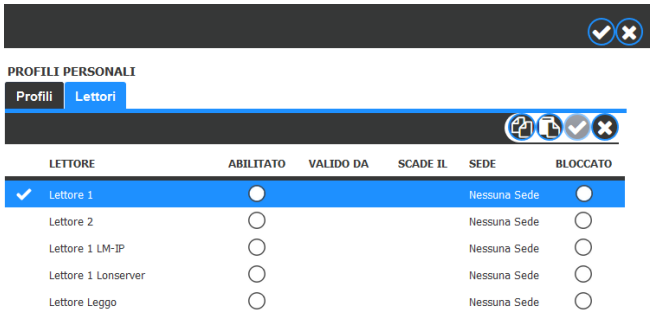
Ad esempio se il terminale in campo ha connesso un lettore PROXY-PRO, è configurato con il seguente tracciato badge: Gap Prefisso:0 ; Len Prefisso: 0; Gap Code: 4; Len Code: 9; significa che scarterà 4 caratteri e considererà 9 caratteri del codice. Occorre dunque impostare:

- Caratteri ignorati pre-codice: 4
- Lunghezza codice: 9



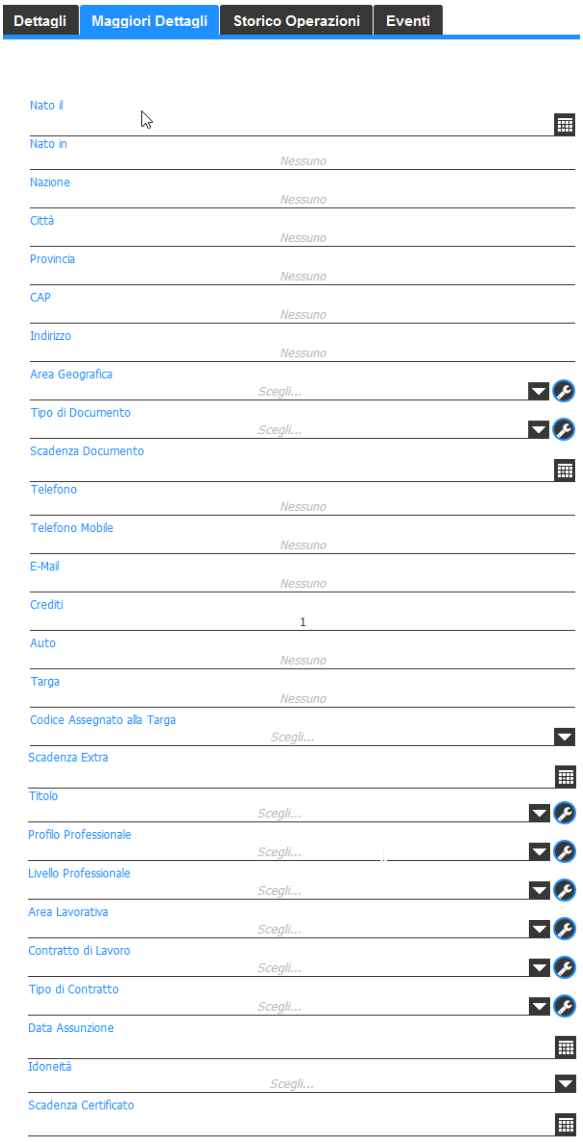
Le date di validità dell'utente hanno rilevanza maggiore rispetto alle date di validità dei singoli codici. Vale a dire che se un utente scade, scadono automaticamente anche i suoi codici.	

4.5.2. Finestra utente: Dettagli-Personal Profile

Nella configurazione di un utente è possibile assegnare "PERSONAL PROFILE":	
In caso di Personal Profile, è necessario assegnare anche il Gruppo, che porta con sé le informazioni su fasce orarie e antipassback (e altro). Cliccare su per impostare il profilo personalizzato per questo utente: • è possibile scegliere un insieme di profili, cliccando per ciascuno su "ABILITATO", e opzionalmente mettendo una validità (VALIDO DA, SCADE IL) e legando una sede: • è possibile scegliere un insieme di lettori, cliccando per ciascuno su "ABILITATO", e opzionalmente mettendo una validità (VALIDO DA, SCADE IL) e legando una sede: In entrambe le finestre è presente il parametro "BLOCCATO", che ha il seguente significato: se abilitato le date di validità immesse per lettore o profilo, queste restano bloccate ovvero non seguono le date di validità dell'utente.	 

4.5.3. Finestra utente: Maggiori dettagli

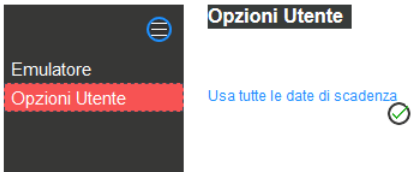
Nel tab “Maggiori Dettagli”, è possibile impostare una serie di informazioni aggiuntive all’utente.



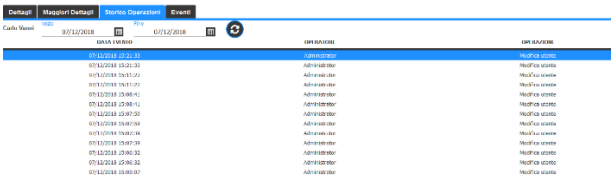
Si ponga attenzione alle tre date di scadenza aggiuntive dell’utente:

- “Scadenza Documento”,
- “Scadenza Extra”,
- “Scadenza Certificato”.

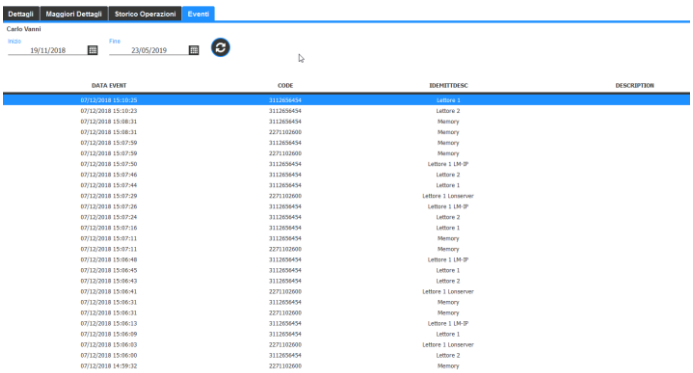
Queste tre scadenze insieme alla scadenza principale (Valido... - Scade il ...), presente nella pagina “Dettagli”, concorrono alla scadenza globale dell’utente se in “Opzioni di sistema”, “Opzioni Utente”, “Usa tutte le date di scadenza” è abilitato.



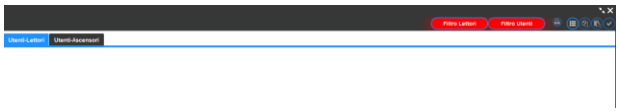
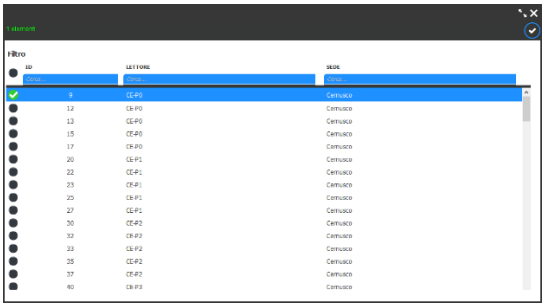
4.5.4. Finestra utente: Storico operazioni

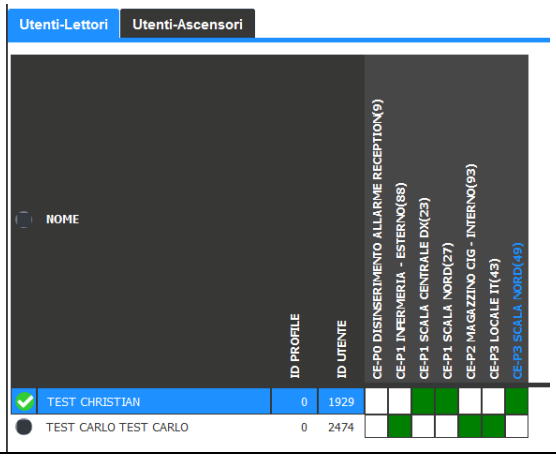
In questa finestra sono mostrate le operazioni che sono state fatte su questo utente, in un intervallo temporale impostabile a piacere.	

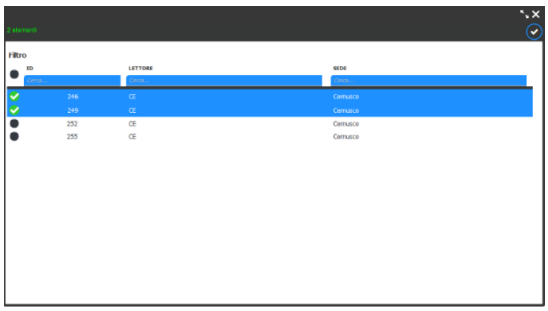
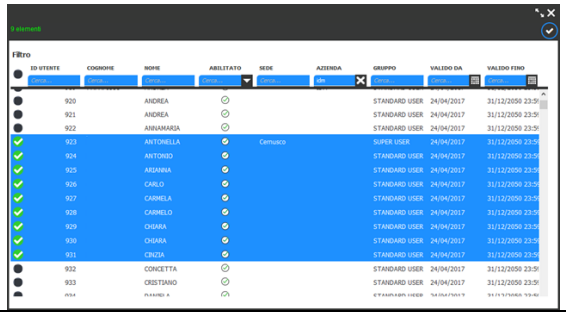
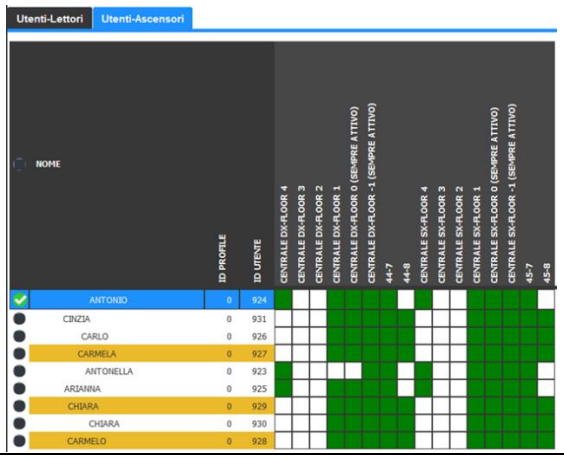
4.5.5. Finestra utente: Eventi

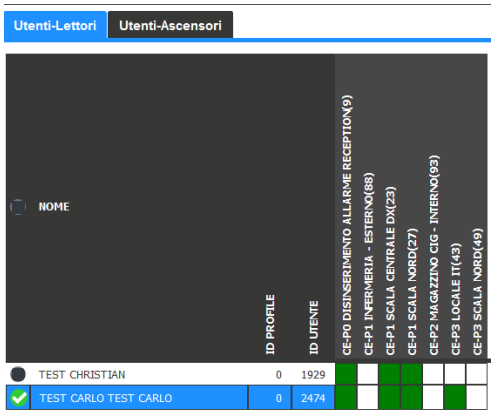
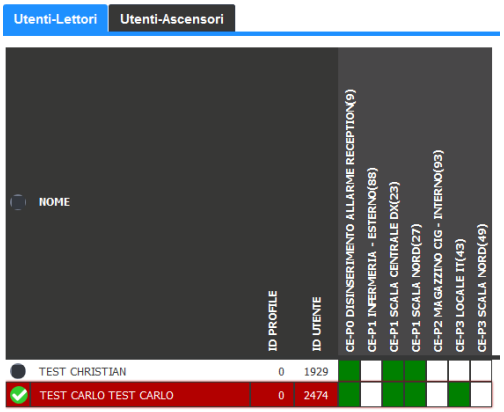
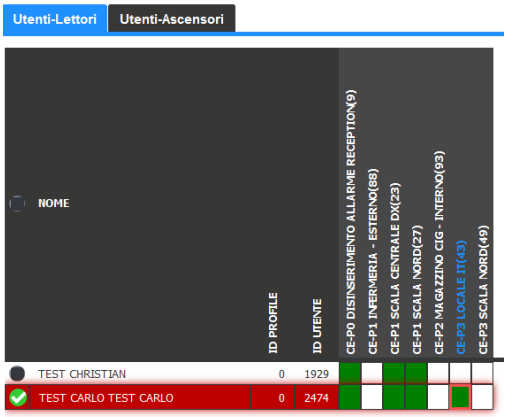
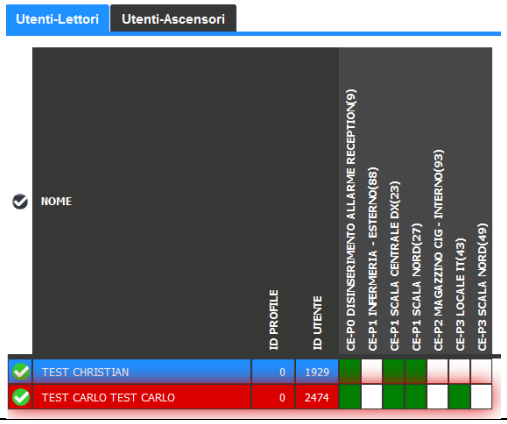
In questa finestra sono mostrati gli eventi compiuti da questo utente, in un intervallo temporale impostabile a piacere.	

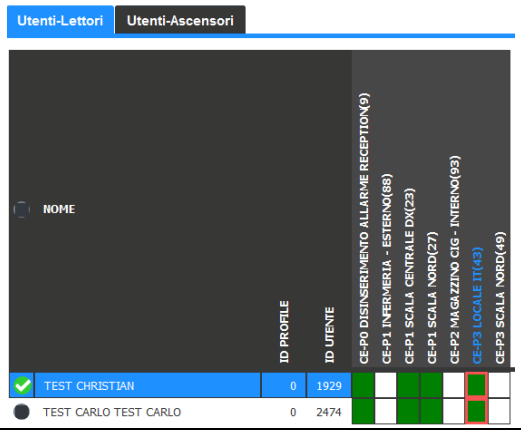
4.5.6. Utenti/Lettori e Utenti/Ascensori

Cliccando su , si entra in una pagina speciale dove è possibile visualizzare/modificare il legame tra ogni utente e i lettori associati e il legame tra ogni utente e i piani accessibili gestiti da un terminale ascensore.	
Utenti/Lettori Importante: è necessario che i terminali abbiano associata una Sede, operazione da fare in ADM nella maschera di configurazione dei terminali. Cliccare su “Filtro Lettori” e scegliere quali lettori mostrare, è possibile filtrare la ricerca per Sede:	

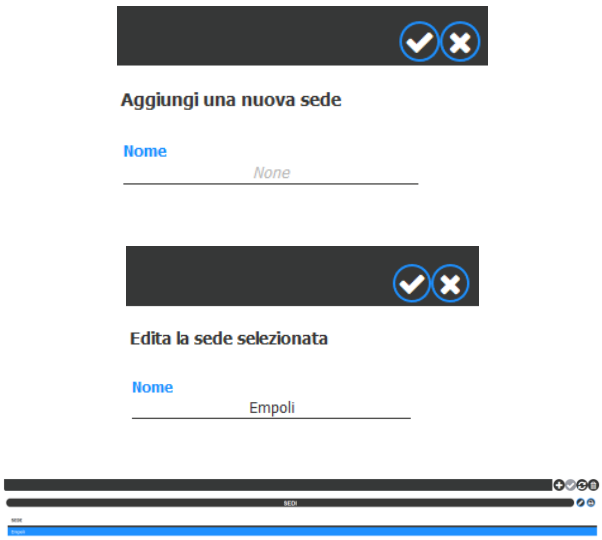
Cliccare su “Filtro Utenti”, scegliere quali utenti mostrare, è possibile applicare filtri di ricerca:	
Viene visualizzata sottoforma di matrice l’associazione tra Utenti e Lettori scelti, facendo doppio clic su una casella è possibile abilitare/disabilitare l’utente per quel lettore.	
Per rendere effettive le modifiche cliccare su .	

Utenti/Ascensori Per configurare i terminali che gestiscono un ascensore utilizzare il client AxWin6: cliccare su “Sistema” > “Configurazioni di sistema” > “Configurazioni database” > “Configurazioni moduli” > Sezione “Ascensori”: selezionare “Usa terminali per modalità ascensori”. Cliccare su “Seleziona/deseleziona terminali per ascensori” per stabilire quali terminali gestiscono gli ascensori e in seguito su “Configurazione nomi piani” per dare i nomi ai piani. Cliccare su “Filtro Ascensori” e scegliere quali lettori mostrare, è possibile filtrare la ricerca per Sede:	
Cliccare su “Filtro Utenti”, scegliere quali utenti mostrare, è possibile applicare filtri di ricerca:	
Viene visualizzata sottoforma di matrice l’associazione tra Utenti e Ascensori scelti, facendo doppio clic su una casella è possibile abilitare/disabilitare l’utente per quel lettore.	
Per rendere effettive le modifiche cliccare su .	

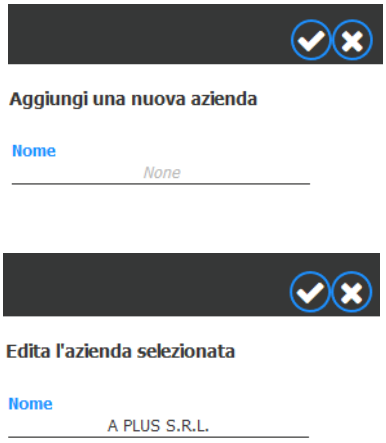
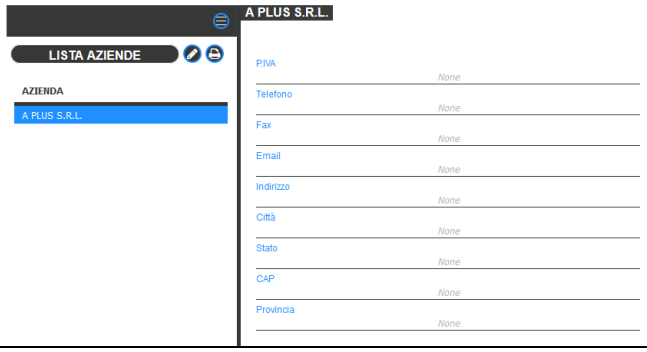
Operazione di copia e incolla Sia per Utenti/Lettori che Utenti/Ascensori è possibile applicare le abilitazioni stabilite per un utente per più utenti. Selezionare l'utente:	
Cliccare su . La riga selezionata diventa rossa:	
Selezionare una o più caselle di associazione, che si vuole copiare. Cliccare su .	
Selezionare uno o più utenti, per selezionarli tutti cliccare su "NOME".	

Cliccare su L'associazione è incollata per tutti gli utenti:	

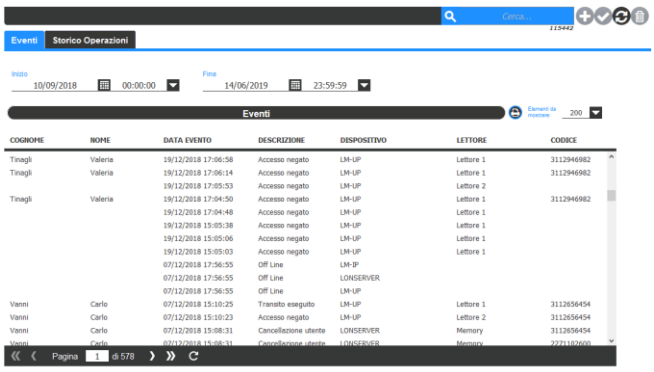
4.6. Creazione Sedi

Scegliere "Sedi" . Cliccare su per aggiungere una nuova sede, oppure selezionare una sede già esistente e cliccare su .	
"Esporta": la lista di sedi visualizzata è esportata in formato .xls	

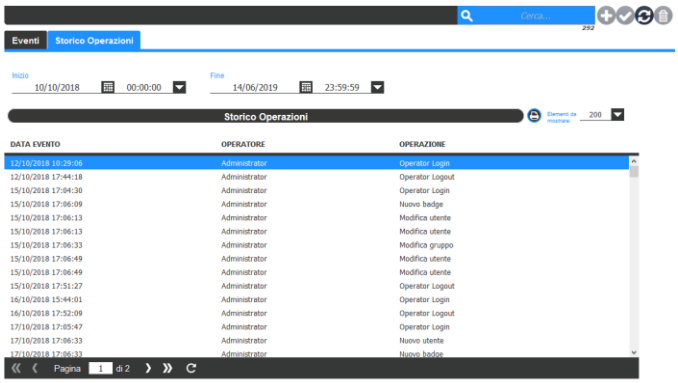
4.7. Creazione Aziende

Scegliere “Aziende” . Cliccare su per aggiungere una nuova azienda, oppure selezionare un’azienda già esistente e cliccare su .	
Compilare i dettagli dell’azienda (sono tutti campi facoltativi).	
Per rendere effettiva una modifica è necessario cliccare sul , per annullare cliccare su . “Esporta”: la lista di sedi visualizzata è esportata in formato .xls	

4.8. Visualizzazione storico eventi

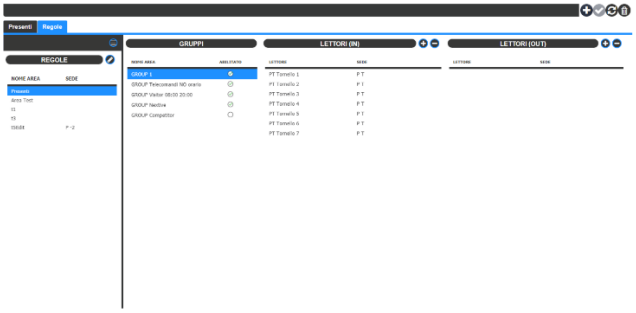
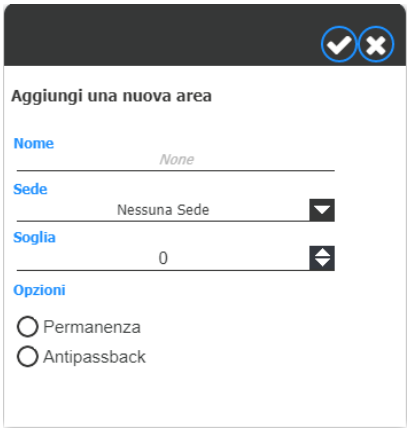
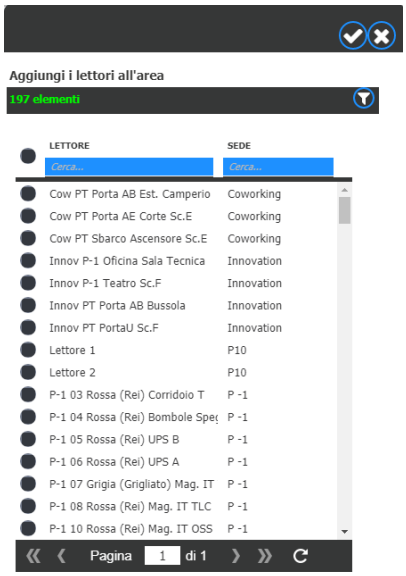
Le regole di accesso e i badge abilitati vengono automaticamente inviati ai terminali, se questi risultano correttamente on-line per ADM. Una volta che i terminali sono stati programmati, è possibile effettuare gli accessi. ADM durante il suo polling, oltre a verificare che i terminali siano online, scarica gli eventi di transito che si sono verificati; l'interfaccia APRO WEB si preoccupa di visualizzarli in maniera chiara e filtrabile. Scegliere "Storici" , nel tab "Eventi" impostare un intervallo temporale e cliccare su , per visualizzare gli eventi.	
Per mostrare solo le colonne di interesse, cliccare sul simbolo all'estremità dell'intestazione di una colonna , scegliere "Colonne", selezionare le colonne da visualizzare.	
"Esporta": la lista di eventi visualizzata è esportata in formato .xls	

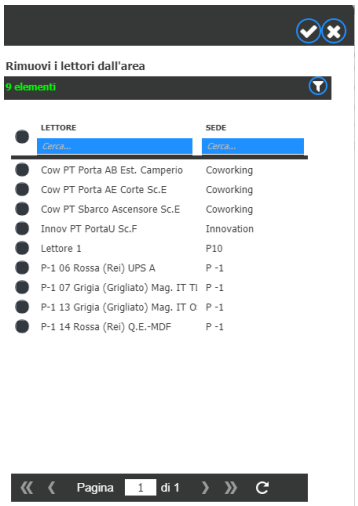
4.9. Visualizzazione storico operazioni

Scegliere “Storici” , nel tab “Operazioni” impostare un intervallo temporale e cliccare su , per visualizzare le operazioni che sono state effettuate sul software.	
“Esporta”: la lista di operazioni visualizzata è esportata in formato .xls	

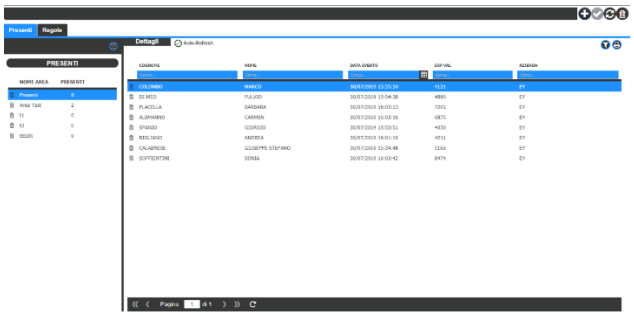
4.10. Presenti

4.10.1. Regole

Scegliere “Presenti” . Per prima cosa accedere al tab “Regole”, per verificare se le aree già crete sono sufficienti o si vuole apportare modifiche.	
Cliccare su per aggiungere una nuova area, oppure selezionare un’area già esistente e cliccare su .	
Dopo aver selezionato un’area è possibile configurare i lettori di ingresso e di uscita da questa area e per quali gruppi applicare il controllo dei presenti nell’area: Cliccare su per aggiungere oppure per togliere lettori dalla colonna LETTORI (IN) e dalla colonna LETTORI (OUT).	

	
Selezionare infine uno o più gruppi da associare a questa area.	

4.10.2. Presenti

Scegliere "Presenti" . Dopo aver selezionato un'area è possibile visualizzare i presenti in tempo reale (se la comunicazione con i terminali è attiva) all'interno dell'area, cliccando su , oppure selezionando la funzione "Auto-Refresh".	
Cliccando su è possibile attivare/disattivare la visibilità dei filtri sulle colonne. Cliccando su è possibile esportare la lista visualizzata in formato .xls. Cliccando sull'icona vicino al nome dell'area è possibile svuotare tutti i presenti. Cliccando sull'icona vicino al nome di una persona presente nell'area, questa sarà tolta dalla lista dei presenti.	

4.11. Account

4.11.1. Regole

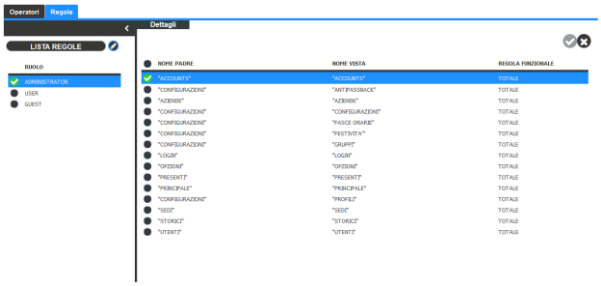
Scegliere “Account” . Per prima cosa, accedere al tab “Regole”, per verificare se i ruoli già presenti sono sufficienti.

Ogni ruolo ha delle proprietà sulle varie funzionalità del sistema. Queste proprietà indicano come può agire sulle funzionalità del sistema:

- **TOTALE**: proprietà più alta, l’operatore è in grado di creare/modificare/eliminare elementi di una specifica funzionalità a cui tale proprietà è assegnata;
- **CREAZIONE**: l’operatore è in grado di creare/modificare elementi di una specifica funzionalità a cui tale proprietà è assegnata;
- **LETTURA/SCRITTURA**: l’operatore è in grado di modificare elementi di una specifica funzionalità a cui tale proprietà è assegnata;
- **LETTURA**: l’operatore può solo leggere gli elementi di una specifica funzionalità a cui tale proprietà è assegnata;
- **DISATTIVATO**: l’operatore non può accedere agli elementi di una specifica funzionalità a cui tale proprietà è assegnata.

I ruoli di default sono:

- ADMINISTRATOR;
- USER;
- GUEST.

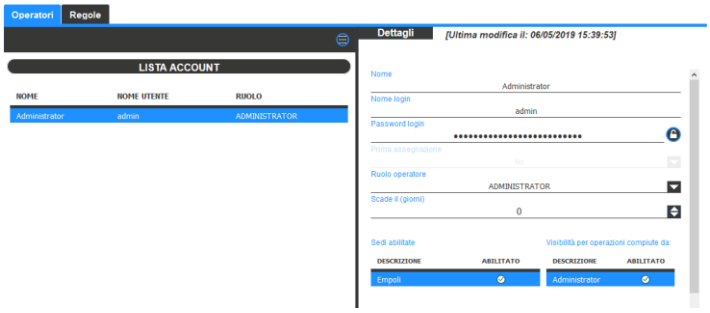


È possibile aggiungerne altri. Cliccare su per aggiungere un nuovo ruolo, oppure selezionare un ruolo già esistente e cliccare su . I ruoli di default non possono essere modificati.

4.11.2. Operatori

Scegliere “Account” . Accedere al tab “Operatori”, cliccare su per aggiungere un nuovo operatore, oppure selezionare un operatore già esistente e cliccare su . Compilare tutti i dettagli della finestra:

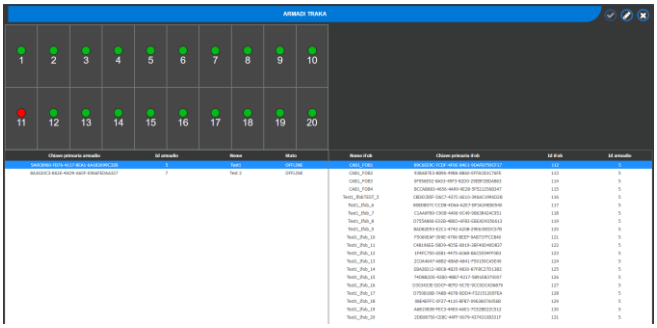
- Nome: nome che identifica l’operatore;
- Nome login: nome con cui effettuare il login;
- Password login: password con cui effettuare il login;
- Conferma password: ripetere la password di login;
- Prima assegnazione: stabilisce che la password immessa dovrà essere cambiata al primo accesso;
- Ruolo operatore: dalla lista è possibile scegliere un RUOLO pre-creato;
- Sedi abilitate: l’operatore è in grado di visualizzare gli utenti appartenenti alle sedi selezionate, l’operatore è in grado di visualizzare gli eventi provenienti da terminali a cui sono assegnate le sedi selezionate;
- Visibilità per operazioni compiute da: l’operatore è in grado di visualizzare le operazioni compiute anche da altri operatori, selezionati nella lista sottostante.



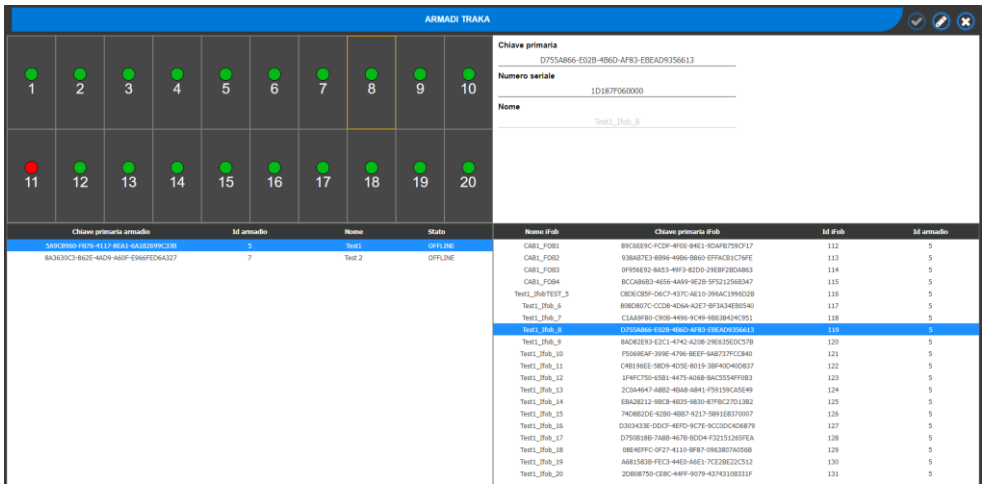
4.12. Modulo integrazione TrakaWEB

L'integrazione *APRO WEB – TrakaWEB* permette di controllare e gestire gli armadi Traka direttamente da APRO WEB.

Il sistema permette la gestione di più armadi, varie credenziali utenti e garantisce la completa visibilità di accesso ed utilizzo di ogni chiave (*iFob*).



L'interfaccia di gestione armadio permette di vedere in tempo reale lo stato completo dell'armadio e della singola chiave.



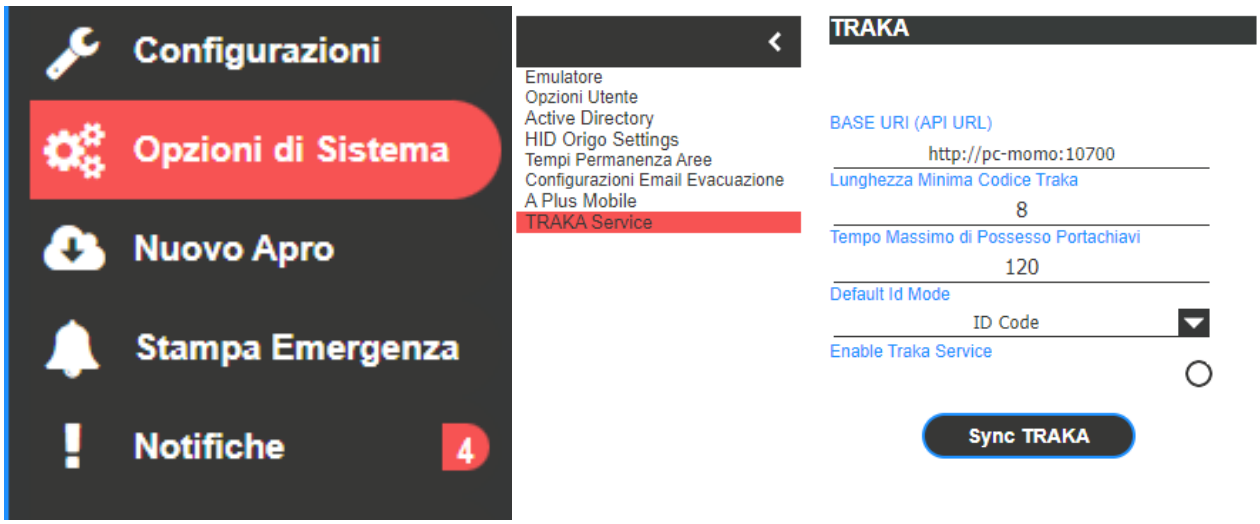
4.12.1. Caratteristiche

La gestione degli armadi e chiavi iFob permette di:

- Controllare in tempo reale lo stato degli iFob e degli armadi;
- Assegnare iFob specifici a utenti specifici mediante il profilo personale;
- Assegnare restrizioni anche a determinati iFob/utenti;
- Assegnare un tempo di permanenza entro il quale un iFob deve tornare al suo posto e dopo il quale scatterà un allarme;
- Inviare email di notifica se un tempo di permanenza non viene rispettato.

4.12.2. Abilitazione e configurazione

L'abilitazione avviene nell'apposita sezione **Traka Service** presente nel modulo **Opzioni di Sistema**

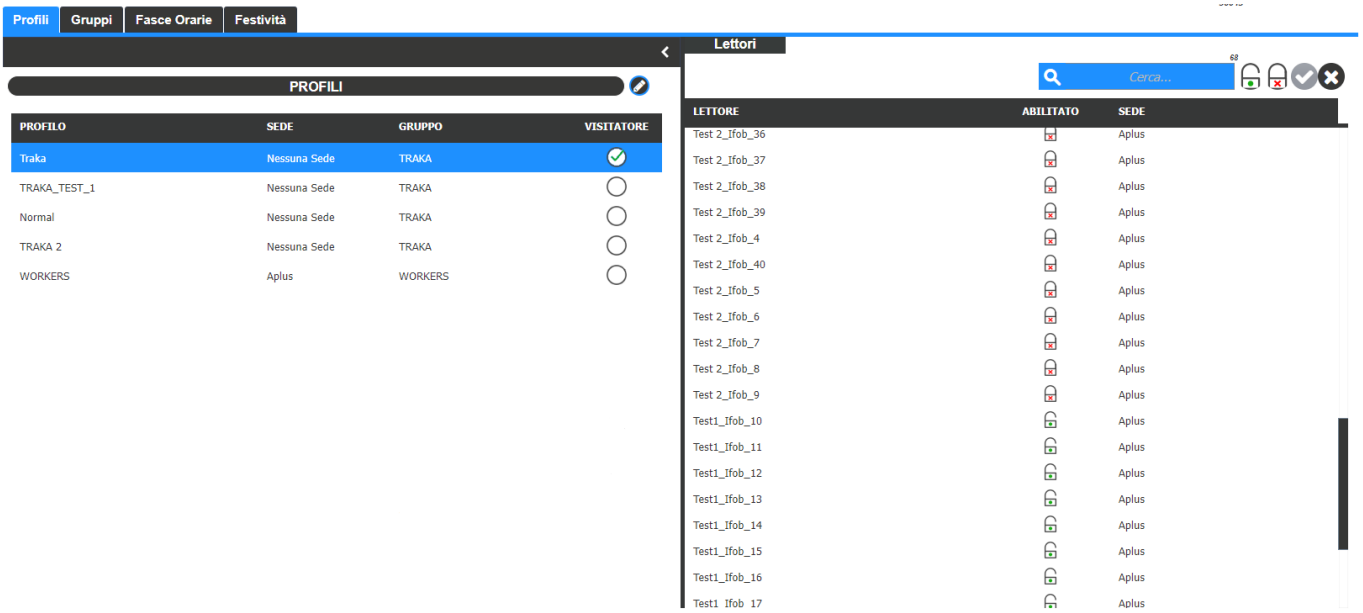


- Il campo *Base URI* indica l'indirizzo su cui sono installati i servizi Traka
- Il campo *Tempo massimo di possesso portachiavi* indica il tempo massimo per cui un iFob può essere restituito; allo scadere del tempo verrà inviata una notifica; È possibile disabilitare la funzione usando il valore "0".
- Il campo *Default Id Mode* indica il metodo di riconoscimento utente (passaggio badge o codice pin) per poter aprire l'armadio.
- Il campo *Enable Traka Service* abilita o disabilita tutto il servizio, inclusa la visione del modulo interfaccia.

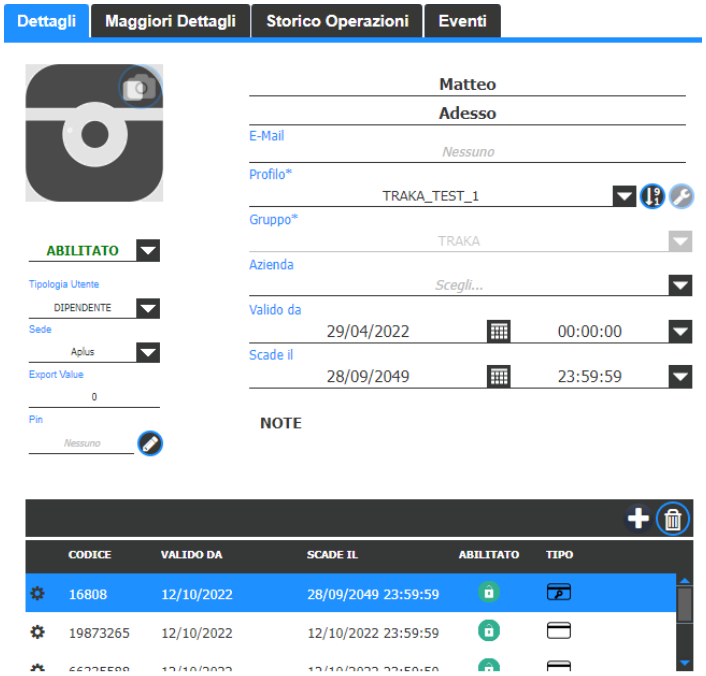
N.B. è necessario premere il pulsante "salva" presente in alto a destra della schermata per effettuare le modifiche

Tramite modulo **Configurazioni** è possibile gestire profili, in particolare creare profili nuovi Traka o modificarne esistenti ed integrarci le apparecchiature traka.

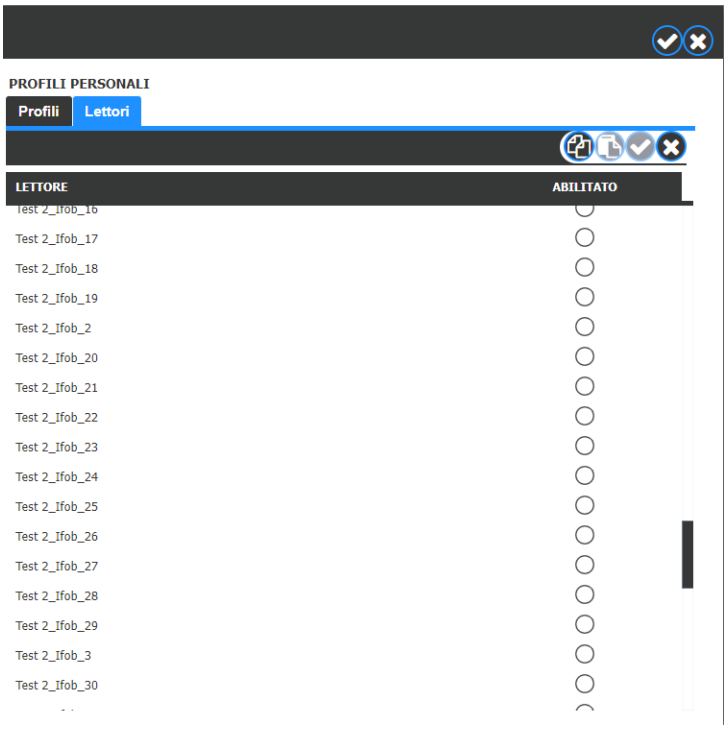
La configurazione permette, inoltre, di poter associare ad ogni profilo solo determinati iFob (o tutti), garantendo il completo controllo sulla gestione dell'armadio e delle sue chiavi.



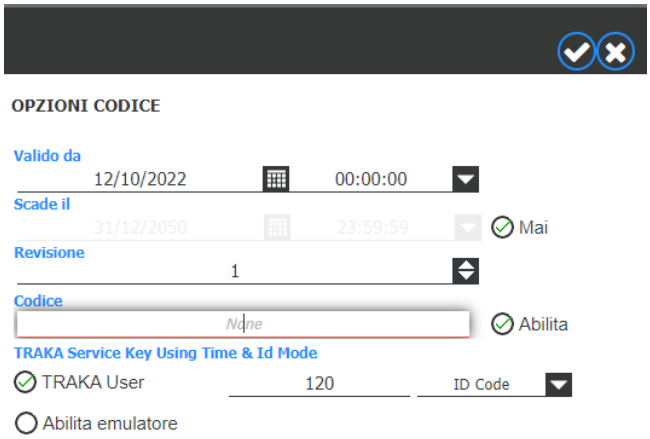
Una volta completata la configurazione di un profilo, per applicarlo basta andare sulla pagina dettaglio di un singolo utente ed assegnare il profilo appena creato:



Inoltre, è possibile usare la funzione “Profilo Personale” e assegnare le singole apparecchiature Traka:

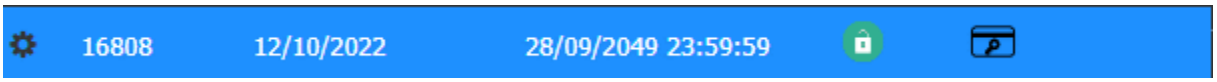


L’assegnazione del codice badge/pin segue il funzionamento standard di Apro Web, con l’aggiunta di una spunta “Codice Traka”; il numero che esegue fa riferimento al *Tempo massimo di possesso portachiavi* e prende come valore standard quello precedentemente specificato nel modulo **Configurazioni**

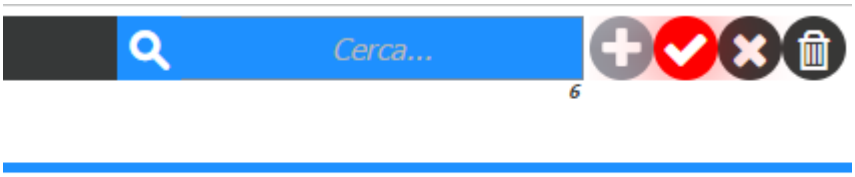


N.B. Ogni utente può avere uno e un solo codice Traka assegnato

Il nuovo codice Traka avrà un simbolo differente sotto al campo “tipo”:

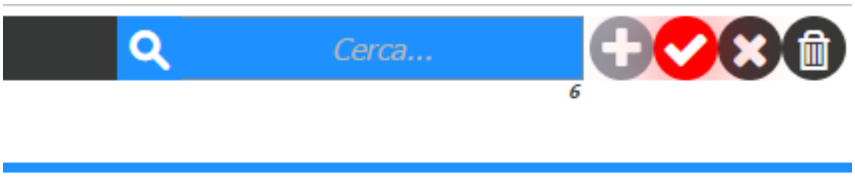


N.B. è necessario premere il pulsante “salva” presente in alto a destra della schermata per effettuare le modifiche



4.12.3. Disabilitazione e cancellazione codici

È possibile disabilitare un codice Traka tramite apposita spunta su pagina utente: in questo modo il codice badge continuerà il suo ordinario funzionamento, ma **non** sarà più riconosciuto come codice Traka.

Per la cancellazione si può fare affidamento alla funzione ordinaria “elimina”.

N.B. è necessario premere il pulsante “salva” presente in alto a destra della schermata per effettuare le modifiche