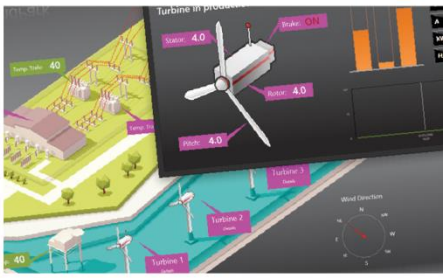
INDUSTRIAL AUTOMATION SOFTWARE
progea

Movicon.next™
Automation Platform.next generation



Movicon NExT

9.0 Sicurezza

Ver.3.4.268

Sommario

CONCETTI GENERALI DELLE SICUREZZE 1

MODELLO DI GESTIONE DELLE SICUREZZE 3

MEMBERSHIP PROVIDER 7

LA GESTIONE UTENTI E PASSWORD 9

Inserimento e Gestione Utenti 9
Impostazioni Generali Gestione Utenti 11
Proprietà Gruppi di Utenti 15
Proprietà Utenti 17
Comandi Gestione Utenti in Runtime 20
Autenticazione Utenti del Dominio 22

PROTEGGERE E CRIPTARE IL PROGETTO 23

Proteggere e Criptare il progetto ..... **Errore. Il segnalibro non è definito.**

CFR21 PART 11 25

Concetti Generali 25
Sicurezza 27
Validazione e Documentazione 30
Configurazione Progetto CFR21 32
Condivisione Utenti 39
Validazione dei dati di Backup 41

1. Concetti Generali delle Sicurezze

La gestione delle sicurezze nei progetti di Platform.NExT garantisce sia ai progettisti che agli operatori la massima protezione e la gestione in sicurezza dell'accesso al sistema secondo i requisiti e le norme più severe.
Il sistema di sicurezza della piattaforma prevede due criteri ben distinti nella protezione dei dati:

1. Protezione del progetto
2. Autenticazione ed accesso ai comandi ed ai dati in runtime

La protezione del proprio progetto

Un progetto di Platform.NExT può essere protetto e criptato, consentendo al progettista di impedire l'accesso in editazione ad altri, proteggendo il proprio know-how o evitando modifiche non autorizzate. La protezione del progetto in editazione è totalmente distinta dalla gestione degli utenti per l'accesso ai comandi in runtime. Infatti, ad esempio, un progetto potrebbe essere protetto e criptato, pur non avendo attivata la gestione degli utenti in runtime.

La Gestione Utenti e Password per gli operatori

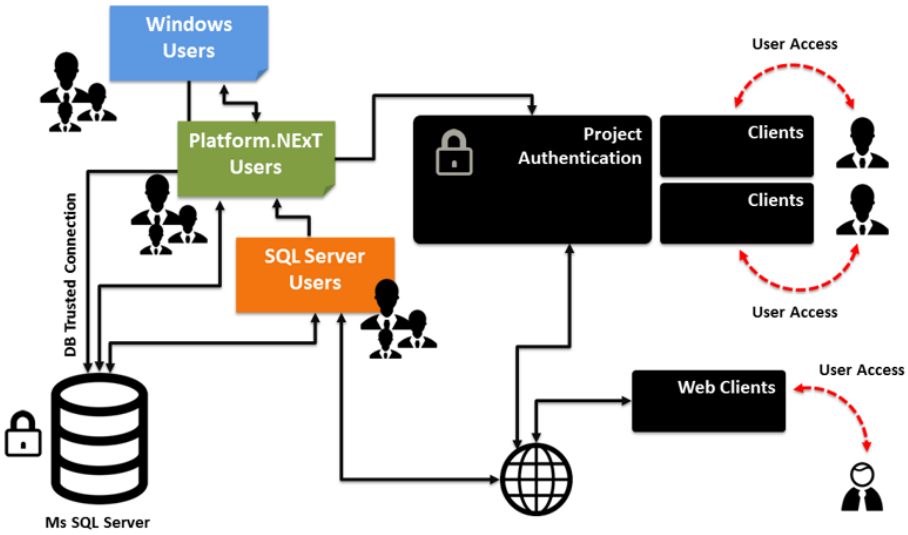
La gestione Utenti e Password offre la possibilità di gestire l'accesso ai comandi ed alle funzioni di progetto, durante l'esecuzione runtime, secondo gli standards di sicurezza più severi. Il progettista può quindi impostare, per tutte le funzionalità ed i comandi, ove necessario, la richiesta dell'autenticazione dell'Utente secondo il proprio livello di privilegio e/o area di accesso.

ATTENZIONE !! E' importante che progettisti o amministratori adottino gli opportuni accorgimenti per ricordare o recuperare la propria password. Una password di accesso persa non sarà più recuperabile!
Nel caso, contattare il Servizio di Assistenza Progea.

2. Modello di Gestione delle sicurezze

La gestione delle sicurezze nei progetti di Platform.NExT si basa sul modello delle Membership Providers di ASP.NET. Questa gestione, oltre a garantire i massimi criteri di sicurezza nella gestione degli utenti, offre il vantaggio utilizzare i "providers", per rendere indipendente il modello di sicurezza (data source) dal sistema di autenticazione.

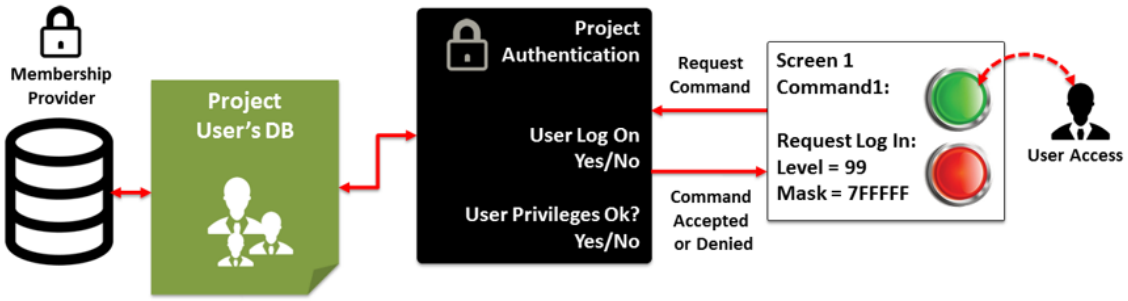
La Membership è un API per la gestione degli utenti all'interno di un'applicazione .NET che permette la gestione degli utenti per l'autenticazione. La configurazione di Membership, nell'ambiente Microsoft .NET, avviene grazie ai Providers, che sono in sostanza il mezzo di connessione tra l'applicazione ed il sistema di autenticazione. Grazie all'utilizzo dei Providers, quindi, un progetto di Platform.NExT garantisce lo stesso livello di sicurezza pur personalizzando il sistema di autenticazione, che potrebbe quindi essere basato su database diverso oppure su sistemi di autenticazione basati ad esempio su lettori biometrici, o identificazione RFID, Badge o altro.



L'illustrazione mostra un esempio di schema del concetto di sicurezza ed autenticazione utenti di default di Platform.NExT

Il Sistema di Autenticazione

Secondo il modello di sicurezza di Platform.NExT, ogni comando o funzione sensibile di un progetto, **qualora sia stata abilitata la Gestione Utenti e Password**, potrebbe richiedere l'autenticazione di un utente, quindi la verifica del suo livello di accesso per consentire o meno l'esecuzione di un comando. Questo tipicamente avviane sul lato Client, dove i comandi di esecuzione, le modifiche dei dati come set-pont, entry-point, ricette o altro, prevedono l'interazione con l'interfaccia utente. Ma la gestione delle sicurezze potrebbe essere prevista anche sul lato Server, dove potrebbe essere accettata o meno la modifica o la variazione di un dato.



L'illustrazione mostra un esempio di schema del concetto protezione all'accesso dei comandi e processo di autenticazione e consenso.

In ogni caso, i comandi o le funzioni di un progetto potrebbero quindi essere soggetti alla verifica del livello di privilegio di un utente, dopo la sua autenticazione.
Questo richiede pertanto che, oltre alla abilitazione della Gestione Utenti, siano stati inseriti, sia in editazione che in runtime, gli utenti che potranno eseguire i comandi in base al loro livello gerarchico.

Esiste quindi una anagrafica utenti di progetto, che viene automaticamente mappata sul database SQL Server che utilizzerà il Membership Provider per l'autenticazione. Il sistema di autenticazione della piattaforma, se abilitato, prevede pertanto che:

1. Siano state assegnate le proprietà di "Gestione Utenti" a tutti gli oggetti grafici o alle funzioni da proteggere, stabilendo il livello Utente ed eventualmente l'area di accesso.
2. Siano stati inseriti Utenti in anagrafica con le relative proprietà di Livello Utente (livello gerarchico) ed eventualmente area di accesso.
3. Sia correttamente configurato il Provider di autenticazione. Per default, il sistema è configurato con il provider Microsoft SQL Server.

Assegnazione dei criteri di accesso ai comandi

L'assegnazione dei criteri di accesso alle funzioni di un progetto avviene generalmente sul lato **Client**, ovvero negli oggetti o nelle funzioni di comando gestite dai sinottici. Ad esempio, un pulsante di "avvio" potrà prevedere, nelle sue proprietà, un livello di utenza ben preciso. Questo vale per qualsiasi oggetto, simbolo o funzione che permetta la gestione o l'esecuzioni di comandi.
Ma il criterio di sicurezza può anche essere definito sul **Server**, ed essere ereditato in modo generico da ogni oggetto associato.
Ad esempio, una variabile Tag potrebbe avere essa stessa definito, nelle sue proprietà, un livello di accesso. In tal caso, la modifica del valore del Tag, da qualunque parte provenga, richiederà l'autenticazione dell'utente.

E' compito del progettista definire dove associare la richiesta di autenticazione dell'utente. Normalmente ciò avviene sul lato Client, ma in architetture distribuite o complesse, potrebbe essere utile impostare la sicurezza sul singolo dato del Server.

In ogni caso, il criterio di sicurezza richiesto deve essere impostato nelle proprietà dell'oggetto desiderato, utilizzando le proprietà di "**Gestione Utenti**" (se sul lato Client) oppure le proprietà "**Livello di Accesso**" (se sul lato Server).

Riferirsi quindi alle specifiche proprietà descritte nei relativi capitoli.

Privilegi Utenti

Oltre all'autenticazione dell'utente, gestita dalle Membership, ogni utente dispone di specifici privilegi, stabiliti nelle proprietà di ogni singolo utente.
E' possibile quindi definire il Privilegio di un Utente in base ai seguenti criteri:

Livello

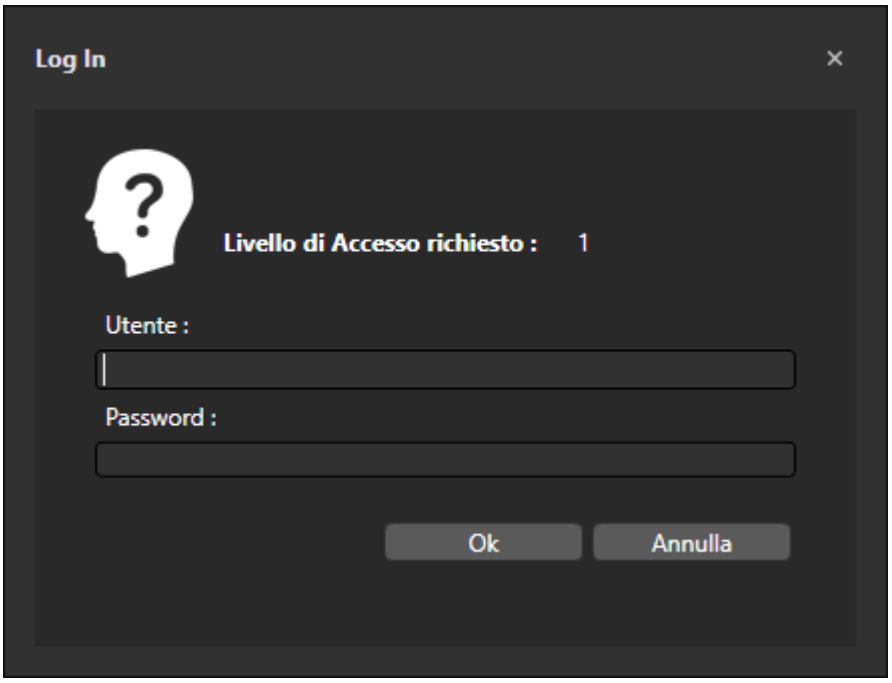
Definisce un livello gerarchico attraverso un valore numerico attribuito all'utente. Il livello numerico più basso definisce il privilegio minore. L'accesso al comando sarà quindi accettato se il livello numerico richiesto sarà uguale o superiore.

Maschera di Accesso

Oltre al livello gerarchico, gli utenti possono disporre anche di una "Maschera di Accesso", che rappresenta un'area di consenso alle operazioni. La maschera prevede la possibilità di selezionare fino a 31 aree (selezione di tutte, alcune o nessuna). Un comando quindi potrebbe essere condizionato in Lettura o Scrittura da una o più aree, per cui l'Utente che esegue il Log On, non solo dovrà avere il livello gerarchico uguale o superiore, ma anche l'eventuale abilitazione di area.
Per default, ogni utente ha sempre tutte le aree abilitate.

Log On Utenti.

Ove richiesto quindi, il sistema richiederà di eseguire l'accesso attraverso la procedure di Log On, richiesta attraverso l'apposita finestra come illustrato sotto. Il Log On viene registrato dopo l'avvenuta autenticazione con successo.



La figura sopra illustra la finestra di autenticazione utente, visualizzata dal sistema quando si tenta di eseguire un'azione che richiede un livello di utenza (indicato), e quindi una autenticazione. Se l'utente esegue l'autenticazione ed il livello di utenza è uguale o superiore, l'azione sarà consentita.

Il sistema traccia in ogni caso nel Log di Sistema la data e l'ora l'autenticazione dell'utente (eventi di Log On e Log Off)

Nei paragrafi successivi verranno descritte tutte le proprietà e le funzioni di Utenti e Gruppi di Utenti.

3. Membership Provider

Il modello di sicurezza di Platform.NExT è basato sui Membership Providers, per garantire la massima sicurezza e l'indipendenza dal tipo di autenticazione desiderata. Grazie ai Providers, infatti, è possibile personalizzare la gestione del sistema di autenticazione.
Platform.NExT utilizza per default, in modo totalmente automatico e sicuro, il Membership Provider Microsoft basato su SQL Server. L'utente quindi utilizza il provider di sicurezza in modo totalmente trasparente, in quanto durante l'installazione di Platform.NExT, se non già presente un'installazione SQL Server alla quale connettersi, viene installata automaticamente un'istanza di SQL Server Express 2012. Su questa istanza viene creato il database "Movicon.Membership" sul quale vengono create le tabelle per l'eventuale gestione utenti del progetto.

Uno dei vantaggi dell'uso dei Providers è dato dal fatto che questo può essere condiviso da altri Clients, siano essi locali o remoti (es. Client Movicon.NExT o Web Clients).
Inoltre, il Provider può essere cambiato e configurato nei setting dell'applicazione, consentendo quindi l'utilizzo di sistemi di autenticazione diversi da quello di default basato su SQL Server.

Personalizzazione del Provider di autenticazione

Qualora lo si desideri, il progettista esperto può cambiare il Membership Provider di autenticazione, sostituendo il provider Microsoft SQL Server con quello desiderato.
Per impostare un nuovo Provider, occorre modificare il file XML di configurazione con estensione .config dell'applicazione (Movicon.NExT.exe come Client o PlatformNExTIOServer.exe come Server).
Qui occorrerà impostare il nome del Provider desiderato e i dati e parametri della stringa di connessione.
Per una corretta configurazione occorrerà quindi utilizzare la documentazione del Provider che si desidera utilizzare. Ove necessario, contattare il Supporto Tecnico per maggiori informazioni.

4. La Gestione Utenti e Password

4.1. Inserimento e Gestione Utenti

Per poter disporre di una Gestione Utenti nel progetto, è necessario gestire l'anagrafica, creando una Lista di Utenti o di Gruppi. Infatti, inserendo Utenti e/o Gruppi nel progetto, sarà possibile attribuire i diritti di accesso ed i livelli di privilegio necessari per potere eseguire i comandi del progetto.
Infatti, anche se viene utilizzata la tecnologie delle Membership con il relativo repository SQL degli utenti per gestire l'autenticazione, gli Utenti ed i Gruppi devono essere creati attraverso l'Editor Utenti del progetto Platform.NExT. Solo in questo modo è possibile assegnare agli utenti le informazioni specifiche legate all'applicativo, che nel Provider non verrebbero inserite.

L'Editazione degli Utenti, o dei Gruppi, può avvenire durante **l'editazione** del progetto, quindi in programmazione, oppure può essere eseguita in **runtime** dagli operatori autorizzati, secondo le modalità ed i limiti previsti.

Gli Utenti possono anche essere centralizzati nel **Dominio del Sistema Operativo** Utilizzato. In questo caso la Gestione Utenti prevede una anagrafica gestita dal Dominio di rete del sistema operativo Windows nel quale il progetto Platform.NexT è eseguito. Gli utenti comunque possono anche essere gestiti con entrambe le modalità: infatti, se un utente non è presente nel progetto, può essere richiesta l'autenticazione tra gli utenti del dominio. Riferirsi all'apposito paragrafo per le modalità di gestione dell'autenticazione degli utenti del Dominio.

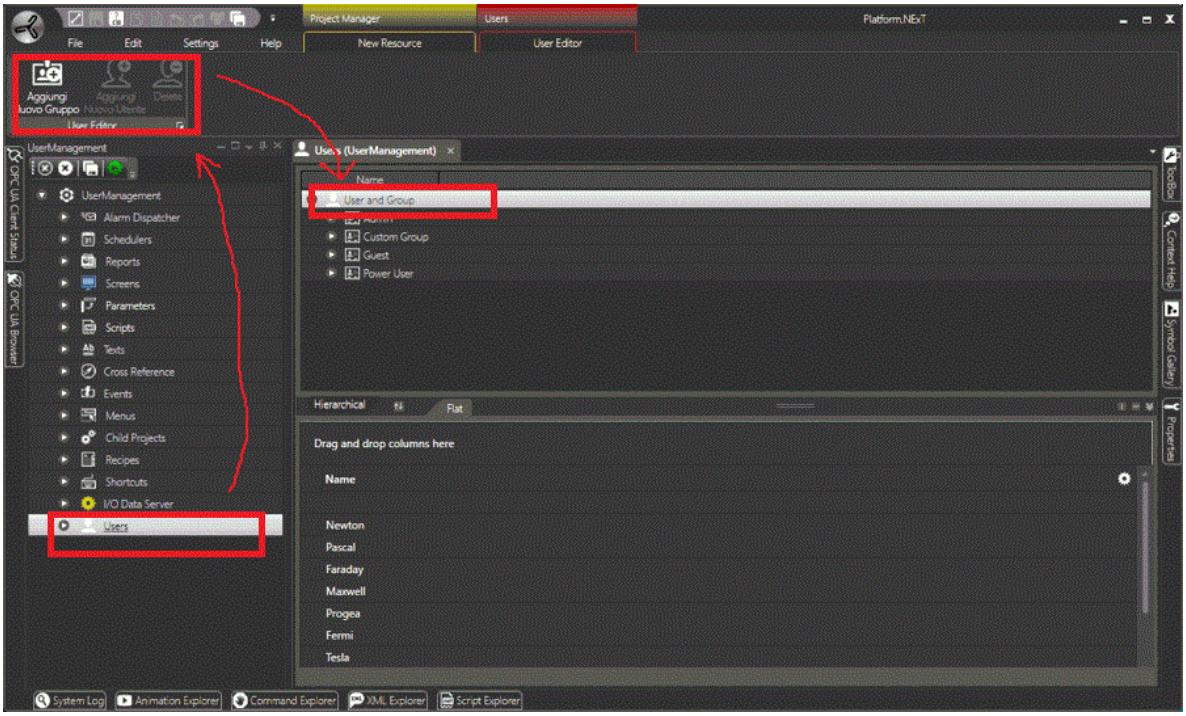
L'autenticazione di un utente durante la fase di runtime verrà quindi fatta dal Provider, che passerà al progetto Platform.NExT le credenziali dell'utente che ha richiesto il LogOn.

Un utente di Windows potrà essere autenticato anche senza dover inserire per forza un Gruppo. Nella risorsa 'Users', se non viene creata alcuna nuova cartella contenente un nome di gruppo, quando si apre il progetto, Movicon crea di default tre cartelle di gruppo predefinite che sono: **Admin, Guest e Power User.** Se questi vengono cancellati, alla riapertura del progetto verranno ricreati automaticamente, almenochè non sia presente almeno un gruppo all'interno della risorsa.
Nel caso sia stata selezionata l'opzione 'Enable Windows Authentication' Movicon tenterà di far autenticare un utente di Dominio e lo associerà al gruppo creato in 'User and Group' (es. 'Domain Users').
Se l'utente viene correttamente autenticato, questo avrà il livello di accesso del gruppo stesso.
Se non è presente nessun gruppo di utenti, l'utente avrà livello 0. Nel caso in cui ci siano gruppi di utenti di cui nessuno contiene l'utente di dominio, il login fallirà.

Editor Utenti del progetto

Utilizzando la Risorsa "**Utenti**" dalla struttura ad albero del progetto, si accederà all'Editor per la Gestione Utenti del progetto. Qui sarà possibile impostare le proprietà

generali della Gestione Utenti, oppure introdurre e configurare gli utenti ed i loro diritti di accesso ai comandi del progetto.
Gli utenti definiti nel progetto verranno creati automaticamente all'interno del repository SQL del Membership Provider all'avvio del runtime di Movicon, a meno che questi non siano già presenti nella lista utenti del Provider. In questo caso le impostazioni degli utenti del Membership Provider non verranno sovrascritte dalle proprietà impostate sugli utenti locali del progetto.



La figura mostra l'ambiente di programmazione e l'area di lavoro della Gestione Utenti

Editor Utenti in Runtime

Naturalmente è possibile inserire nuovi Utenti nella Gestione del progetto, anche durante l'esecuzione runtime, ad esempio per l'aggiunta di nuovo personale durante l'esercizio dell'impianto. I nuovi Utenti inseriti in Runtime andranno ad aggiungersi a quelli precedentemente inseriti.
Per inserire nuovi utenti durante l'esecuzione runtime, è necessario che il progettista abbia previsto gli appositi comandi per visualizzare l'Editor Utenti, secondo quanto descritto nell'apposito paragrafo "Comandi Gestione Utenti in Runtime".

Comandi per l'editazione utenti

Dopo avere selezionato la risorsa "Utenti" del progetto, sarà disponibile il Ribbon "Editor Utenti" dal quale sono disponibili i comandi per l'editazione degli Utenti e dei Gruppi.

Ribbon contenente i comandi di editazione utenti.

Aggiungi Nuovo Gruppo
Questo comando consente di inserire un nuovo Gruppo Utenti all'interno della lista utenti del progetto. Nel momento in cui si crea un nuovo Gruppo verrà automaticamente aperta la finestra pop-up contenente le proprietà caratteristiche di un Gruppo.

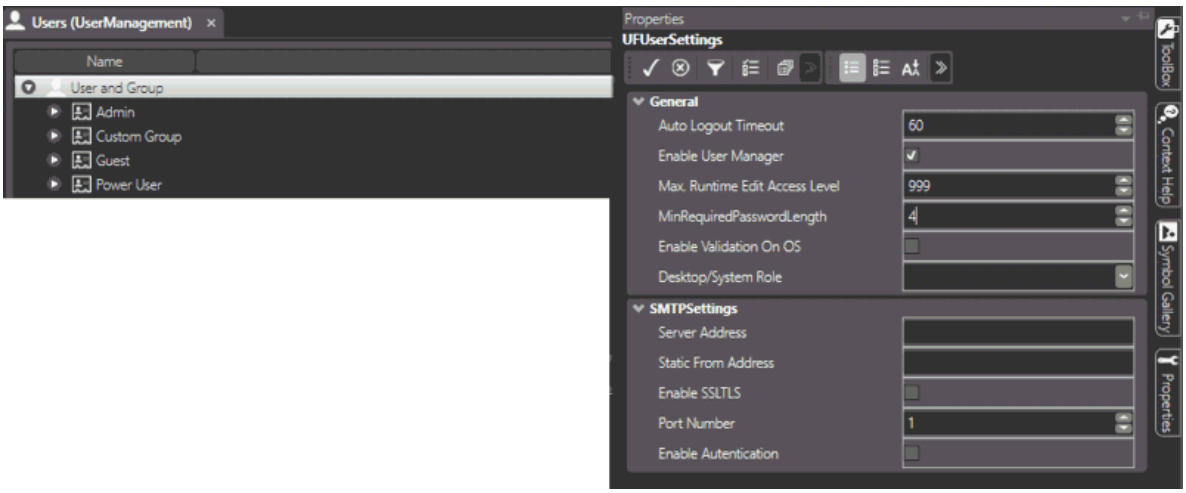
Aggiungi Nuovo Utente
Questo comando consente di inserire un nuovo Utente all'interno della lista utenti del progetto. L'Utente dovrà per forza essere inserito all'interno di un Gruppo. Nel momento in cui si crea un nuovo Utente verrà automaticamente aperta la finestra pop-up contenente le proprietà caratteristiche di un Utente.

Elimina
Questo comando consente di eliminare l'Utente o il Gruppo selezionato. **Il comando è disponibile solo in Programmazione**.

4.2. Impostazioni Generali Gestione Utenti

La Gestione degli Utenti e Password prevede una serie di Impostazioni Generali, che sono visualizzabili attraverso la Finestra delle Proprietà dopo avere selezionato la risorsa generale Utenti e Gruppi dall'Editor Utenti.
Le impostazioni generali consentono innanzitutto di Abilitare o Disabilitare la gestione della richiesta dell'autenticazione utente del progetto durante l'esecuzione runtime. Inoltre vi sono una serie di proprietà che riguardano l'intera gestione, e che vanno impostate come descritto di seguito.

⚠ Per poter attivare la gestione utenti all'interno del progetto è necessario abilitare la proprietà "**Abilita Gestione Utenti**", tramite la finestra delle Proprietà Generali degli Utenti e Gruppi.



Proprietà Generali Gestione Utenti

Di seguito vengono descritte le proprietà di carattere generale a tutta la gestione utenti del progetto.

Auto Logout Timeout

Utilizzando questo parametro è possibile inserire il tempo, espresso in secondi, per eseguire automaticamente l'operazione di LogOut dell'eventuale utente attivo. Il tempo in secondi si riferisce al tempo di inattività. Pertanto, un utente attivo, trascorso il tempo di inattività impostato, verrà disattivato eseguendo un LogOut di sicurezza automatico. In caso di ripresa dell'attività, quando richiesto, l'utente dovrà eseguire nuovamente l'accesso.

Max. Invalid Password Attempts

Permette di specificare il numero massimo di tentativi di accesso falliti dopo il quale un utente viene bloccato dal sistema

L'impostazione dei criteri di soglia per il blocco di un utente determina il numero di tentativi di accesso non riusciti che causano il blocco di accesso al sistema di un determinato utente.
Quando un utente viene bloccato non risulta più possibile accedere al sistema anche utilizzando le credenziali corrette finché non viene riabilitato utilizzando dei comandi specifici messi a disposizione da Movicon.NExT.
Questa funzionalità prevede l'impostazione di un valore di tentativi di accesso non riusciti ed inoltre tramite la proprietà "**User Lock Mode**" si potrà specificare quali utenti verranno bloccati

User Lock Mode

Tramite questa proprietà è possibile specificare se abilitare o meno la possibilità di bloccare determinati utenti nel caso di tentativi di accesso non validi.
Nella proprietà è possibile specificare le seguenti opzioni:

- None: La modalità di blocco utenti non è abilitata (Valore di default)
- OnlyEditableUser: Nel caso in cui il numero di tentativi di accesso non validi sia maggiore al valore della proprietà 'Max. Invalid Password Attemts' verranno bloccati solamente gli utenti con un livello di accesso inferiore o uguale alla proprietà 'Max. Runtime Edit Access Level'

- All: Nel caso in cui il numero di tentativi di accesso falliti sia maggiore al valore della proprietà 'Max. Invalid Password Attemps' verra bloccato l'utente di qualsiasi livello di access

Nel caso in cui un utente risultasse bloccato e si volesse procedere alla sua riabilitazione è possibile utilizzare i comandi contenuti all'interno della tab 'Users' di un qualsiasi oggetto di Movicon.NExT.

Gli utenti di dominio non vengono considerati nella gestione del blocco utenti in quanto non sono gestiti direttamente dal membership provider di Movicon.NExT.

Abilita Gestione Password

Abilitando questa proprietà verrà attivata la gestione utenti durante la fase di Runtime del progetto. E' possibile quindi, per il progettista, decidere quando attivare o disattivare l'intera gestione utenti del progetto.

Visualizza controllo Login

Se all'interno di un progetto viene abilitata la gestione utenti, questa proprietà permette di abilitare\disabilitare la visualizzazione del log in alto a destra nei sinottici, utilizzato per effettuare il log-in.

Max. Livello Utente Editabile in Runtime:

Questo parametro permette di specificare quale deve essere il Livello gerarchico massimo ammissibile per un utente che viene inserito o visualizzato nella Gestione Utenti del progetto durante l'esecuzione runtime.

Min. Lunghezza Password Richiesta

Questo parametro permette di forzare il numero minimo di caratteri ammissibili per una password associabile ad un utente.

E' buona norma per ottenere password più sicure, utilizzare lettere, numeri e caratteri speciali.
Per forzare l'uso di numeri e caratteri speciali nelle password, è possibile modificare il file di sistema "MoviconNExT.exe.config". introducendo la variabile "minRequiredNonalphanumericCharacters".
Il valore inserito, risulterà essere il minimo numero di caratteri non alfanumerici richiesto nella password.

```
<membership defaultProvider="AspNetSqlMembershipProvider">
  <providers>
    <remove name="AspNetSqlMembershipProvider" />
    <add name="AspNetSqlMembershipProvider" type="System.Web.Security.SqlMembershipProvider, System.Web,
         connectionStringName="LocalSqlServer"
         enablePasswordRetrieval="false"
         enablePasswordReset="true"
         requiresQuestionAndAnswer="false"
         applicationName="/"
         requiresUniqueEmail="false"
         passwordFormat="Hashed"
         maxInvalidPasswordAttempts="5"
         minRequiredPasswordLength="1"
         minRequiredNonalphanumericCharacters="0"
         passwordAttemptWindow="10" passwordStrengthRegularExpression="" />
  </providers>
</membership>
```

Abilita Autenticazione Utenti Windows

Se si abilita questa funzionalità, il sistema di Gestione Utenti permette l'autenticazione anche di utenti registrati nel Dominio del sistema operativo Windows nel quale il progetto è eseguito. In questo modo la gestione utenti, se non trova un utente nella lista utenti del progetto, richiederà l'autenticazione tramite protocollo LDAP al sistema operativo, utilizzando la forma 'domain\user'.

Se l'utente verrà riconosciuto, verrà autenticato dal dominio, e quindi validato anche per la gestione del progetto. In questo caso, i diritti di accesso però sono determinati dal "**gruppo**" di appartenenza.

Connessione Repository condiviso

Permette di generare una tabella unica per tutti i progetti con all'interno tutti gli utenti dei vari progetti, in modo che essi possano essere condivisi.

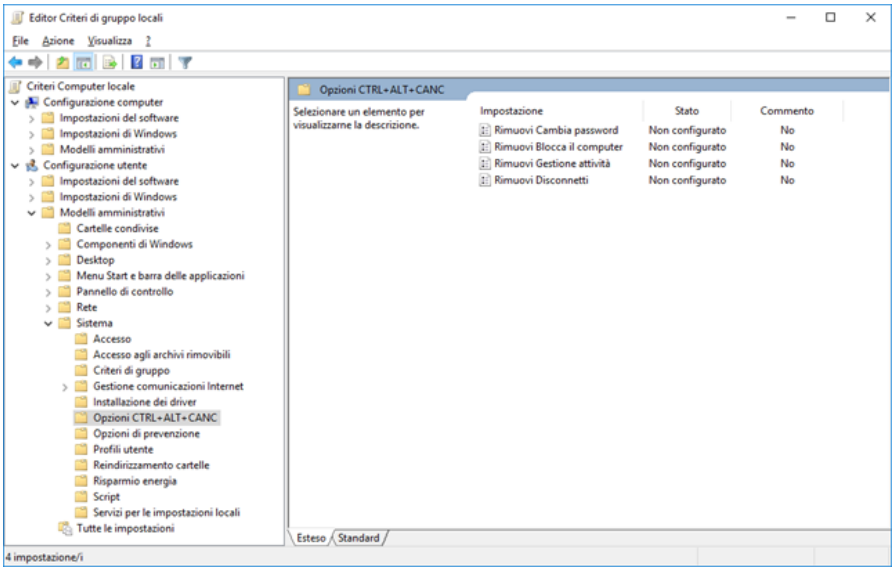
Le installazioni di Movicon.NExT utilizzate per i singoli progetti, necessiteranno del "membership" in comune. Sarà necessario quindi modificare i file "Moviconext.exe.config" e Platformnext.exe.config" affinchè utilizzino lo stesso "membership".

Ruolo Desktop/Sistema

Utilizzando questa proprietà, è possibile associare un "Gruppo", e quindi i relativi Utenti, con il diritto di eseguire i comandi operativi di sistema. I comandi di sistema sono quei comandi non direttamente legati al progetto, ma alle funzioni del sistema operativo che ne riguardano l'operatività. Ad esempio la chiusura della finestra dell'applicazione, la riduzione ad icona, l'accesso al desktop, la chiusura dell'applicazione, ecc.

I comandi di sistema non sono gestiti quindi dagli oggetti dell'applicazione, ma sono gestiti dall'operatività di Windows. In una corretta gestione Utenti, è importante che il progettista decida quali utenti possono avere il diritto di agire sui comandi del sistema operativo se questi sono accessibili.

Attenzione: questa funzionalità potrebbe comunque non essere pienamente compatibile con l'antimalware di Windows, che viene costantemente aggiornato, potrebbe essere in esecuzione e reimpostare certe chiavi della registry del sistema mentre Movicon è in esecuzione vanificando di fatto alcune restrizioni impostate. Inoltre la combinazione di tasti "CTRL+ALT+CANC" non può essere bloccata tramite questa funzionalità di Movicon. In questo caso è possibile usare l'"Editor Criteri di Gruppo Locali" di Windows per impostare queste restrizioni in base alle proprie esigenze evitando così che antimalware intervengano. Per avviare l'editor digitare "gpedit.msc" nella ricerca di Cortana e premere invio:



La configurazione più sicura da utilizzare resta l'uso del Server Movicon avviato come servizio in combinazione con le impostazioni di Windows sopra indicate.

Proprietà SMTP Settings

Oltre alle proprietà generali, è disponibile il gruppo **"SMTPSettings"** che consente di impostare le eventuali funzioni di notifica email di reportistica.
Attenzione, queste impostazioni non riguardano le Notifiche di Alarm Dispatcher, che prevedono un Server di configurazione apposito.

Indirizzo Server
Imposta l'indirizzo del server SMTP di posta

Indirizzo Mittente
se impostato, permette di visualizzare l'indirizzo del mittente nella mail di notifica che verrà generata dal sistema.

Abilita SSL/TLS
Se abilitata, permette di utilizzare i certificati di sicurezza e crittografia per l'autenticazione sul server SMTP.

Numero Porta
permette di impostare il numero della porta SMTP in uscita

Abilita Autenticazione Server
Se abilitata, permette di attivare l'autenticazione sul server SMTP (ove richiesta).

User Name
Se richiesta l'autenticazione Server SMTP, imposta il nome utente per l'autenticazione.

Password
Se richiesta l'autenticazione Server SMTP, imposta la password per l'autenticazione.

4.3. Proprietà Gruppi di Utenti

I Gruppi di Utenti sono fondamentali nella gestione Utenti del progetto. Infatti, non è possibile inserire un Utente se prima non si è definito il suo gruppo di appartenenza. Il Gestore Utenti di Platform.NExT prevede per default i gruppi: Admin, Guest, Power User. Ovviamente questi gruppi possono essere modificati, eliminati e se ne potranno comunque aggiungere dei nuovi. Selezionando un "Gruppo" nell'area di lavoro è possibile impostare, tramite la finestra delle proprietà, le seguenti impostazioni:

Nome
Definisce il nome del Gruppo. Il nome dovrà essere univoco nella lista, con la lunghezza massima di 64 caratteri.

Livello di Accesso Predefinito
Tramite questa proprietà è possibile definire il livello gerarchico di accesso del Gruppo. Questo significa che se un utente non ha impostato un proprio livello di accesso, oppure viene autenticato dal dominio del sistema operativo, riceve il Livello di Accesso dalle proprietà del gruppo.

Il Livello gerarchico prevede un valore numerico da 0 a 9999. Il valore associato determina il livello di privilegio, pertanto più alto è il valore e maggiori saranno le capacità di accesso dell'Utente. Ad esempio, un utente con il livello 10 potrà eseguire tutti i comandi che richiedono un livello uguale od inferiore (compreso tra 1 e 10).
Per un Gruppo non è ammesso il livello -1, che invece è ammissibile per un Utente che, in tal caso, erediterà il Livello del Gruppo.

Area di Accesso Predefinita

Tramite questa proprietà è possibile definire un'area di accesso, attraverso una "maschera di bit" per il Gruppo. Questo significa che se un utente non ha impostato una propria maschera di accesso, oppure viene autenticato dal dominio del sistema operativo, riceve la Maschera di Accesso dalle proprietà del gruppo.
Ogni bit corrisponde potenzialmente ad un'area di accesso, alla quale viene consentito all'utente di interagire per quei controlli che richiedono, oltre al Livello, la medesima Area di Accesso. Ad esempio, ad un comando può essere impostato un Livello di Accesso ed inoltre, l'abilitazione (ad esempio) dell'Area 1. Se un Utente che si autentica ha un livello gerarchico uguale o superiore, ma non ha abilitata anche l'Area 1, non potrà eseguire il comando.
Le Aree di accesso vanno da 1 a 31, selezionabili tutte o in parte a seconda delle necessità attraverso l'apposita finestra di selezione. Per Default, le Aree di Accesso sono sempre tutte abilitate.

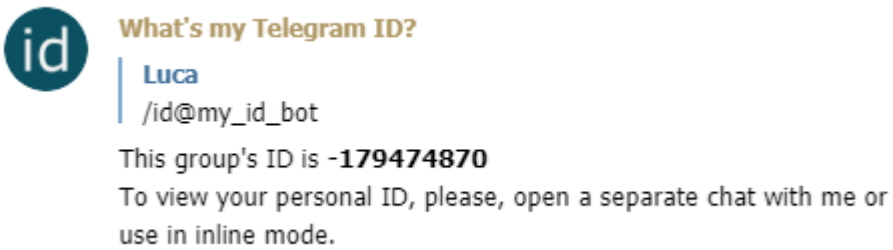
Lingua Predefinita

Tramite questa proprietà è possibile definire la Lingua associata al Gruppo, per consentire l'attivazione automatica della lingua se presente nella Risorsa Tabella Testi del progetto, allo scopo di convertire tutti i testi e le stringhe del proprio progetto nella lingua desiderata.
Questo significa che se un Utente non ha una propria lingua specifica associata, riceverà la Lingua associata al gruppo di appartenenza.
Se non è specificata una lingua, non verrà eseguito alcun cambiamento nei testi.

Telegram Group ID

Questa proprietà identifica il Group ID del gruppo di utenti Telegram nel quale il Bot dell'Alarm Dispatcher è stato aggiunto.
Per ricavare il Group ID è sufficiente seguire questi passi:

- avviare l'app Telegram
- definire un gruppo di utenti
- aggiungere al gruppo il Bot dell'Alarm Dispatcher (utilizzare l'icona lente di ingrandimento per trovarlo)
- aggiungere temporaneamente al gruppo l'utente "my_id_bot" (utilizzare l'icona lente di ingrandimento per trovarlo)
- nella chat di gruppo digitare il messaggio "/id@my_id_bot"
- verrà mostrato il Group ID da utilizzare in Movicon.NExT



- a questo punto è possibile rimuovere dal gruppo l'utente "my_id_bot"

Se un utente del gruppo ha specificata la proprietà Telegram Chat ID, questa avrà priorità sulla proprietà Telegram Group ID.

4.4. Proprietà Utenti

Gli Utenti, nella gestione delle sicurezze del progetto, permettono di gestire i dati personali necessari all'autenticazione ed all'accesso delle funzioni del progetto, se questo ha attivata la Gestione Utenti. Un Utente deve necessariamente appartenere ad un Gruppo, anche se possiede comunque tutte le proprietà specifiche di diritti e privilegi.
Per ogni Utente è possibile impostare, tramite la finestra delle proprietà, le seguenti impostazioni:

Proprietà Generali

Il gruppo di proprietà Generali permette di definire le impostazioni principali di un Utente.

Nome
Questa proprietà definisce il Nome dell'Utente, che dovrà consentire l'identificazione in modo univoco, con la lunghezza massima di 64 caratteri.

Password
Questa proprietà consente di impostare la Password associata all'Utente. I caratteri sono nascosti per la privacy durante la digitazione. Il numero minimo di caratteri della password può essere impostato nelle Proprietà Generali della Gestione Utenti. Il numero massimo è 64 caratteri.

- **Tutti i dati delle password Utenti nel progetto sono criptate, quindi è necessario adottare gli opportuni accorgimenti per non dimenticare o smarrire una password!**

Conferma Password
Per sicurezza, in questo campo viene richiesto di digitare nuovamente la Password impostata in precedenza a conferma dell'operazione.

Firma Elettronica
Il valore di questa proprietà deve essere univoco in modo da identificare con precisione un utente. Il suo valore, se inserito, viene registrato nella riga del Trace sulla tabella relativa (UFUAAuditDataItem) nella colonna UserName, mentre se non è inserito in tale colonna verrà riportato il nome utente. L'univocità viene gestita dal sistema. In caso di utilizzo dell'autenticazione Windows, non venendo definiti gli utenti a livello di progetto Movicon.NExT, la Firma elettronica non viene definita e, nella colonna di Username viene riportato il nome, completo di dominio, dell'utente. Per garantire l'univocità della Firma Elettronica è preferibile non avere un modello di autenticazione misto: parte utenti di progetto e parte degli utenti di dominio.

Lingua Utente
Tramite questa proprietà è possibile definire la Lingua associata all'Utente. Se il campo viene lasciato vuoto viene ereditata la Lingua eventualmente definita nel Gruppo di appartenenza. In questo caso quando l'Utente esegue il Login, la Lingua ad esso associata verrà automaticamente attivata nel progetto.

Proprietà di Esecuzione

Il gruppo di proprietà di Esecuzione permette di definire le impostazioni relative ai diritti di accesso di un Utente.

Nr. Giorni durata Password

Tramite questa proprietà è possibile impostare la validità massima (espressa in giorni) della password associata all'utente, per ragioni di sicurezza. Una volta terminato il periodo di validità, al successivo Login verrà visualizzata all'utente la finestra di richiesta per il re-inserimento ed il rinnovo della password, la quale dovrà essere differente dalla precedente.
In questo modo, secondo normative specifiche che lo richiedessero, è possibile limitare i rischi nel caso in cui qualcuno venga a conoscenza della password di un utente.
Lasciando il campo al valore zero di default, non verrà gestita la scadenza temporale della password.

Richiede Cambio Password

Se abilitata, questa proprietà richiederà all'utente, la prima volta che eseguirà l'autenticazione in runtime (Log In), a reimpostare la propria password, inserendone obbligatoriamente una nuova rispetto a quella che gli era stata attribuita nelle proprietà.
In questo modo, secondo normative specifiche che lo richiedessero, è possibile limitare i rischi quando un utente Amministratore inserisce gli utenti attribuendo, e quindi conoscendo, la relativa password di ciascuno.

Proprietà di Accesso

Livello di Accesso

Tramite questa proprietà è possibile definire il livello gerarchico di accesso dell'Utente. Il Livello gerarchico prevede un valore numerico da 0 a 9999. Il valore associato determina il livello di privilegio, pertanto più alto è il valore e maggiori saranno le capacità di accesso dell'Utente. Ad esempio, un utente con il livello 10 potrà eseguire tutti i comandi che richiedono un livello uguale od inferiore (compreso tra 1 e 10).
E' possibile non assegnare uno specifico livello, per ereditare il Livello associato al Gruppo di appartenenza. Per questo occorre inserire il valore -1, ed in tal caso l'Utente riceverà il Livello di privilegio del Gruppo.
Anche in caso di autenticazione dal Dominio del sistema operativo, se presente, un Utente riceve il livello gerarchico del Gruppo.

Area di Accesso

Tramite questa proprietà è possibile definire un'area di accesso, attraverso una "maschera di bit" per l'Utente. Ogni bit corrisponde potenzialmente ad un'area di accesso, alla quale viene consentito all'utente di interagire per quei controlli che richiedono, oltre al Livello, la medesima Area di Accesso. Ad esempio, ad un comando può essere impostato un Livello di Accesso ed inoltre, l'abilitazione (ad esempio) dell'Area 1. Se un Utente che si autentica ha un livello gerarchico uguale o superiore, ma non ha abilitata anche l'Area 1, non potrà eseguire il comando.
Le Aree di accesso vanno da 1 a 31, selezionabili tutte o in parte a seconda delle necessità attraverso l'apposita finestra di selezione. Come per i "Livelli di Accesso" anche le "Arre di Accesso" di un Utente possono essere ereditate dal Gruppo di appertenza. Nel Popup di impostazione delle "Aree di Accesso" è infatti presente il pulsante di comando "Inherited" con il quale si può decidere se l'Utente dovrà ereditare le "Aree di

Accesso" dal Gruppo oppure no. Alla creazione di un nuovo Utente il default è di ereditare le "Aree di Accesso".

Proprietà di Notifica

Il gruppo di proprietà di Notifica permette di definire le impostazioni relative agli indirizzi di destinazione delle Notifiche di ogni Utente. **Questi indirizzi valgono per tutte le notifiche, comprese quelle del servizio del server di notifica allarmi Alarm Dispatcher.**

Email

Tramite questa proprietà è possibile definire l'indirizzo E-Mail dell'Utente. Questo verrà poi ad esempio utilizzato dall'Alarm Dispatcher per l'eventuale invio delle notifiche.

Numero Telefono

Tramite questa proprietà è possibile definire il numero di telefonia fisso dell'Utente. Questo verrà poi ad esempio utilizzato dall'Alarm Dispatcher per l'eventuale invio delle notifiche.
Il numero va indicato correttamente, comprendendo l'uso dei prefissi nazionali ed internazionali secondo quanto previsto dai gestori di telefonia.

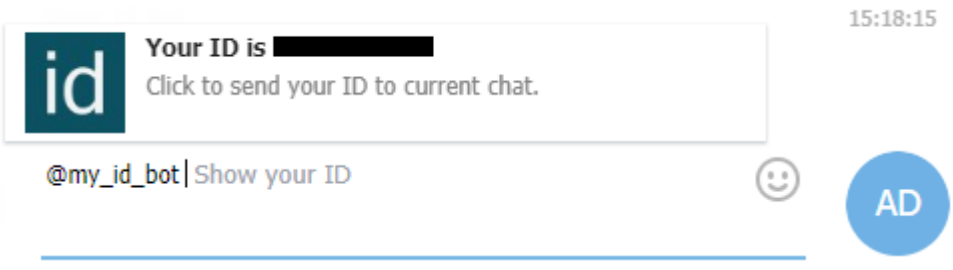
Numero Telefono Mobile

Tramite questa proprietà è possibile definire il numero di telefonia mobile dell'Utente. Questo verrà poi ad esempio utilizzato dall'Alarm Dispatcher per l'eventuale invio delle notifiche.
Il numero va indicato correttamente, comprendendo l'uso dei prefissi nazionali ed internazionali secondo quanto previsto dai gestori di telefonia.

Telegram Chat ID

Questa proprietà identifica il Chat ID della chat Telegram alla quale il Bot dell'Alarm Dispatcher è stato aggiunto.
Per ricavare il Chat ID è sufficiente seguire questi passi:

- avviare l'app Telegram
- avviare una chat con il Bot dell'Alarm Dispatcher (utilizzare l'icona lente di ingrandimento per trovarlo)
- selezionare "Avvia" per avviare la chat
- digitare il messaggio "@my_id_bot"
- verrà mostrato il Chat ID da utilizzare in Movicon.NExT



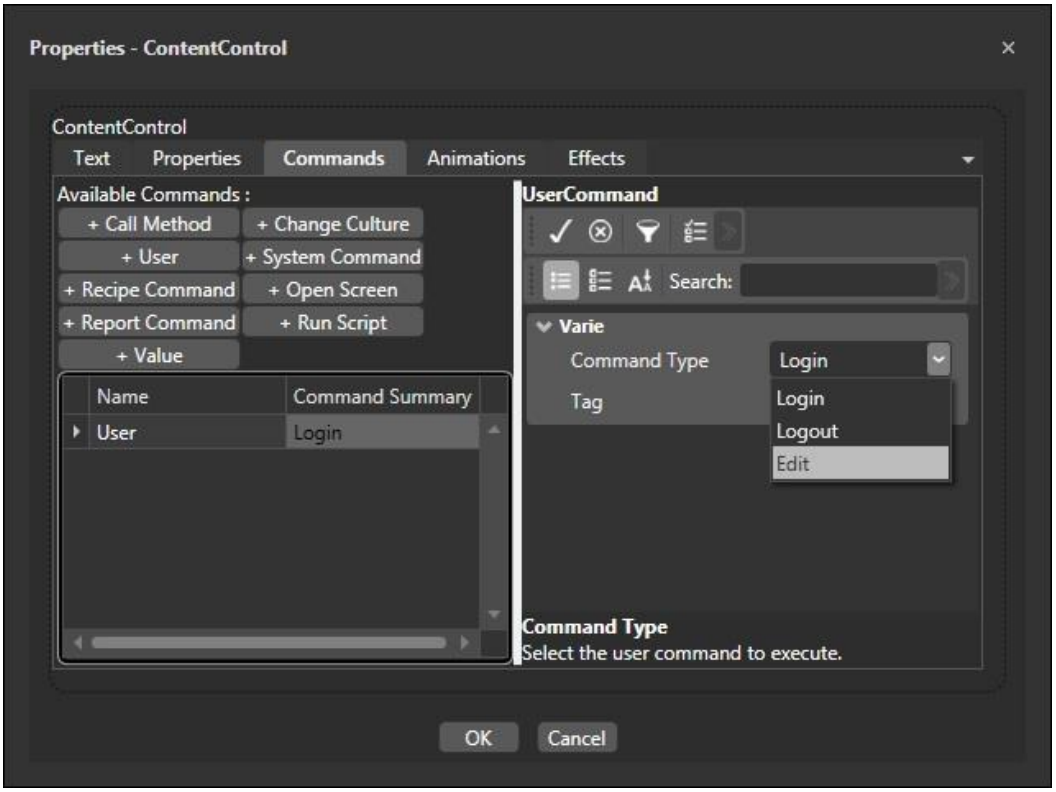
La proprietà Telegram Chat ID, se impostata, ha sempre priorità sulla proprietà Telegram Group ID.

4.5. Comandi Gestione Utenti in Runtime

Per consentire la gestione degli Utenti agli operatori preposti a questo, durante l'esecuzione runtime del progetto, il progettista dispone di appositi comandi associabili agli oggetti dei sinottici. Ad esempio, è possibile associare ad un pulsante (o altri oggetti di comando) le seguenti funzioni operative in runtime:

- **Log In Utente**
- **Log Out Utente**
- **Editazione Utenti**

Naturalmente, è compito del progettista decidere se associare ai comandi che attivano queste funzioni una eventuale password di accesso.
L'impostazione dei comandi avviene pertanto seguendo le normali procedure descritte nel capitolo relativo alla **Assegnazione di Comandi agli oggetti.**



La figura mostra la finestra per l'assegnazione dei comandi "Utente" ad un oggetto in programmazione.

Comando di Log In Utente

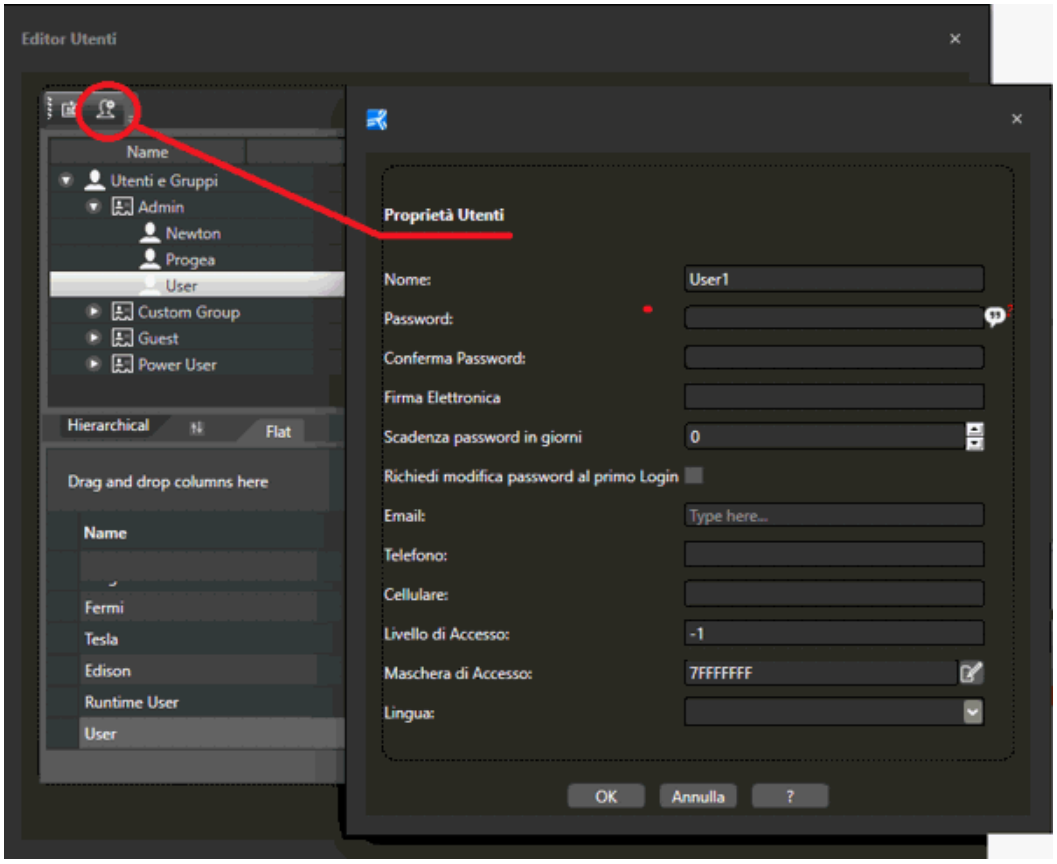
Questo comando esegue la richiesta di autenticazione di un Utente, indipendentemente dal suo livello. L'utente, se autenticato, avrà eseguito il Log In e sarà attivo nella gestione utenti del progetto.

Comando di Log Out Utente

Questo comando esegue la procedura di Log Out per l'utente eventualmente attivo. Dopo questa operazione non sarà più attivo quindi alcun utente.

Comando di Editazione Utenti Runtime

Questo comando attiva la finestra per l'inserimento degli utenti e dei gruppi di utenti, durante l'esecuzione runtime. Il Comando visualizza la finestra di Inserimento Utenti o Gruppi, consentendone di impostare le relative proprietà.
Per impostare i criteri di sicurezza per richiedere uno specifico livello di utenza per attivare il comando, occorrerà utilizzare le proprietà di Gestione Utenti dell'oggetto al quale si intende associare questo comando.



Gli Operatori che hanno il livello sufficiente per potere inserire gli Utenti in runtime, potranno utilizzare la finestra appositamente predisposta per aggiungere nuovi utenti, secondo le modalità funzionali e le proprietà descritte nel paragrafo della Gestione Utenti di questo capitolo.

Considerare che gli Utenti aggiunti in runtime potranno disporre solo di un Livello di Accesso il cui limite è prefissato dal progettista, nelle proprietà della Gestione Utenti. Inoltre, in runtime non è possibile modificare o rimuovere gli utenti, ma solo aggiungerne dei nuovi.

Notare che, se si avvia il progetto in esecuzione runtime con la finestra di programmazione utenti aperta nell'editor, non sarà consentito attivare la finestra di Editazione Utenti in runtime.

4.6. Autenticazione Utenti del Dominio

Se si abilita questa funzionalità, il sistema di Gestione Utenti permette l'autenticazione anche di utenti registrati nel Dominio del sistema operativo Windows nel quale il progetto è eseguito. In questo modo la gestione utenti, se non trova un utente nella lista utenti del progetto, richiederà l'autenticazione tramite protocollo LDAP al sistema operativo, utilizzando la forma 'domain\user'.
L'utente che effettuerà l'avvio di Movicon.NExT (sia come servizio che come runtime) dovrà quindi appartenere al Dominio Windows gestito dall'Active Directory (LDAP), altrimenti questo tipo di autenticazione non funzionerà correttamente.
Se l'utente verrà riconosciuto, verrà autenticato dal dominio, e quindi validato anche per la gestione del progetto. In questo caso, i diritti di accesso però sono determinati dal "gruppo" di appartenenza.

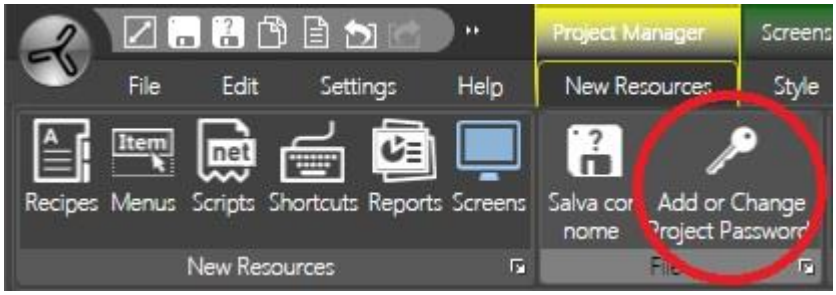
Una volta "validato" l'utente viene valutata la sua appartenenza ai gruppi utente e, nel caso in cui venga trovata una corrispondenza con un gruppo del progetto, allora verranno impostati i livelli di accesso di quel gruppo.

I nomi dei Gruppi Utente standard creati da Windows (come 'Administrators' o 'Users') NON sono supportati per la procedura di validazione. Nel caso in cui si volesse utilizzare tale metodo di autenticazione, sarà necessario creare nuovi Gruppi Utente con nomi personalizzati, quindi creare all'interno del progetto gli stessi gruppi utente per impostare i livelli di accesso.

5. Proteggere e Criptare il progetto

L'ambiente di sviluppo Platform NExT mette a disposizione del programmatore una funzionalità per proteggere il progetto da modifiche di utenti non autorizzati.
Questa funzionalità è stata implementata tramite l'utilizzo di una password di sicurezza che deve essere inserita ed attivata sul progetto, utilizzando il comando dell'apposito Ribbon del gruppo di comandi del Project Manager.
Dopo avere attivato la protezione, il progetto verrà protetto e criptato, ed impedirà il successivo accesso al progetto in editazione senza prima la relativa autenticazione. In questo modo il progettista sarà l'unico a poter accedere in editazione al progetto, evitando l'accesso e/o le modifiche a terze parti.

ATTENZIONE !! E' importante che progettisti o amministratori adottino gli opportuni accorgimenti per ricordare o recuperare la propria password. Una password di accesso persa non sarà più recuperabile!
Nel caso, contattare il Servizio di Assistenza Progea.



Per attivare la protezione del progetto occorre semplicemente utilizzare il relativo Ribbon "Aggiungi/Cambia Password Progetto". In questo modo verrà visualizzata una finestra che permette l'inserimento della password desiderata, con la verifica di conferma. Dopo la conferma, il progetto sarà protetto e criptato, ed il successivo accesso in editazione sarà consentito solo dopo l'inserimento della password inserita.

Abilitando la protezione del progetto , tutti i file inerenti ad esso verranno automaticamente criptati dal sistema, dopodiché sarà possibile accedervi soltanto tramite la password impostata in ambiente di sviluppo.

La protezione con password progetto e crittografia viene inibita quando il progetto è salvato su DataBase. Il salvataggio di un progetto da file a Database richiede di disabilitare la protezione, prima di effettuare il salvataggio, se questa era impostata.

La protezione del progetto non è vincolata alla abilitazione della Gestione Utenti. E' quindi possibile proteggere il progetto senza dover necessariamente inserire utenti nel progetto ed attivare le sicurezze runtime.

6. CFR21 Part 11

6.1. Concetti Generali

Concetti Generali CFR21 Part 11

Lo scopo della normativa CFR21 Part 11, redatta dalla FDA (Food & Drug Administration), è quello di ottenere l'equivalenza legale dei documenti elettronici (records digitali e Firma elettronica) rispetto a quelli cartacei tradizionali. Ciò è dovuto al sempre più frequente uso di sistemi automatici nella gestione dei processi produttivi in sistemi che devono essere sottoposti ad approvazione e revisione dell'ente federale FDA. Affinchè il sistema d'automazione e controllo realizzato sia conforme alla normativa CFR21 Part 11, è necessario far sì che i dati registrati siano sempre riconducibili all'operatore responsabile (Firma Elettronica), inoltre sono necessarie precauzioni specifiche che rendano impossibili falsificazioni o manomissioni dei dati registrati elettronicamente, o che consentano una loro agevole identificazione in caso di utilizzo inappropriato, sia esso intenzionale o casuale, di apparecchiature elettroniche che generano record elettronici.

Molte industrie farmaceutiche intendono approfittare dei benefici che derivano dall'uso dei record elettronici. Si pensi al solo ingombro di questi documenti in forma cartacea che devono essere conservati per anni. Inoltre usando dei record elettronici è possibile ridurre notevolmente i tempi di raccolta e revisione di questi documenti prima del rilascio delle medicine per la vendita.
Queste industrie devono richiedere apparecchiature che abbiano i necessari meccanismi di protezione da modifiche accidentali o malintenzionate dei dati in formato elettronico.

FDA
21 CFR Part 11

Concetti generali per il supporto alla norma.

I concetti esposti di seguito in relazione alla norma definiscono come sarebbe opportuno utilizzare Movicon.NEXT nello sviluppo di progetti applicativi compatibili con la normativa oggetto del documento.
Per spiegare meglio le indicazioni riportate, si elencano di seguito i concetti fondamentali assunti da Progea, fermo restando che rimane responsabilità dell'utente accertarsi che l'applicazione sviluppata in Movicon.NEXT sia conforme ai requisiti richiesti.

⚠ **E' importante ricordare che è sempre l'intera applicazione hardware-software ad essere validabile, non il singolo prodotto o componente. E' responsabilità dell'utente quindi realizzare progetti in conformità alle norme.**

Gestione Trace Modifiche Alle Varibili

Il Trace delle modifiche di una variabile verrà gestito da Movicon.NExT sfruttando gli Historian (prototipi storici e data logger), quindi dovrà essere attivata la relativa opzione in licenza.
In caso contrario rimarranno comunque le funzionalità dell'interfaccia dell'Audit, ma non verrà eseguita la tracciatura.

Allo scopo di gestire l'Audit Trail delle modifiche di una variabile saranno coinvolte diverse proprietà per maggiori informazioni, cliccare sul link relativo al capitolo interessato:

Oggetti

La validazione dei dati deve essere effettuata tramite l'oggetto 'Validatore Audit' presente nella toolbox di Movicon. NExT.
All'interno delle proprietà del controllo è possibile specificare la 'Sorgente Dati' da verificare.

- Validatore Audit Trail

Utenti e Password

Tutti i comandi dell'applicazione eseguibili dall'operatore che possono influire sul processo devono essere protetti opportunamente da password.
La gestione delle password deve essere abilitata nelle Proprietà Generali della risorsa Utenti Password del progetto:

- Firma Elettronica
- Nome (ID) e Password
- Abilita Gestione Password
- Giorni Durata Password
- Forza Password al primo Log On
- Lunghezza Minima Password
- Auto LogOut timeout

Tag

Movicon.NExT offre la possibilità di "tracciare" tutte le variazioni di stato o di valore di ogni variabile con significato rilevante o che influisce sul processo. Ad esempio, deve essere garantito un apposito sistema di tracciatura di qualsiasi variabile sensibile del processo (come set-point o comandi di processo), mediante quello che viene definito Audit di sistema.
Per ogni variabile Tag che si vuole sottoporre ad Audit, Movicon.NExT consente di definire un apposito gruppo di proprietà che consentono di specificare come deve essere gestito l'Audit di ogni singola specifica variabile.

- Periodo Storico di Dati
- Livello di Accesso Richiesto per Conferma
- Richesta di Commento su Audit
- Abilita Gestione Audit
- Forza Password su Audit

Server

L'audit-trail ha il compito di registrare tutte le attività che un utente compie sulle variabili di processo durante il runtime. L'abilitazione alla registrazione di queste attività avviene semplicemente selezionando l'opzione 'Abilita Gestione Audit' all'interno delle proprietà di una variabile.

Per far sì poi che un set di dati registrato possa essere validato, ovvero avere la certezza che in nessun modo il dato possa essere alterato esternamente nel Database, sarà necessario abillitare la proprietà 'Abilita Protezione Dati' all'interno della sezione 'Impostazioni' dell'I/O Data Server. Abilitando questa opzione il ServerIO verrà avviato con un utente particolare che verrà creato dal SetUp di Movicon. Tale utente, il cui nome di default sarà "NExT_IO_Server" e la cui password sarà criptata, verrà utilizzato dal sistema per gestire le registrazioni sul DataBase e sarà l'unico utente che potrà anche validare i dati tramite l'apposito oggetto della ToolBox "Validatore Audit Trail".

- Connessione di Default Audit Trail
- Abilita Protezione Dati su File

In certe casistiche occorre prestare attenzione all'utente con cui verrà avviato il server I/O di Movicon.NExT e sono:

- Si sceglie di cambiare utente volontariamente all'interno della finestra 'Pannello Controllo Servizi' del servizio del server di Movicon.NExT.
- Si installa il servizio del server di Movicon.NExT utilizzando la finestra 'Pannello Controllo Servizi' prima di abilitare l'opzione di protezione dei dati.
- Si imposta una stringa di connessione di default per i database ed all'interno di tale stringa si forza l'autenticazione di un particolare utente.

Historian

- Abilita Protezione Dati su File

Impostando una stringa di connessione al DB personalizzata (proprietà 'Stringa di connessione DB') e specificando un particolare utente per l'accesso al database si impedisce la validazione dei dati.

Datalogger

- Abilita Protezione Dati su File

Impostando una stringa di connessione al DB personalizzata (proprietà 'Stringa di connessione DB') e specificando un particolare utente per l'accesso al database si impedisce la validazione dei dati.

Il documento illustrativo riguardante la norma CFR21 Part 11 è scaricabile dal sito progea.

6.2. Sicurezza

Per garantire la sicurezza del progetto dovranno essere tenuti in considerazione i seguenti punti :

- Il progetto Movicon.NExT dovrà essere criptato affinchè tutte le configurazioni e password utilizzate nel progetto non siano accessibili dall'esterno.
- Movicon.NExT garantisce l'univocità degli utenti password inseriti nel progetto. Ogni utente viene identificato nel progetto con UserID, Password, Descrizione o Nome stampabile univoci (Firma elettronica).

- Per garantire l'integrità dei dati e per evitare la loro manomissione, la parte server di Movicon.NExT dovrebbe essere eseguita come Servizio del sistema operativo Windows. In tal modo l'accesso al sistema operativo ed ai records registrati richiederà l'identificazione di utenti registrati all'interno del progetto, secondo i requisiti di sicurezza richiesti dalla norma.
- Movicon.NExT supporta la condivisione del Dominio del sistema operativo Windows, al fine di utilizzare gli utenti password definiti dall'amministratore del sistema.
- Gli utenti che gestiscono registrazioni dati utilizzando i Data Logger dovranno adottare gli opportuni accorgimenti per evitare l'accesso non autorizzato ai database registrati, al fine di evitare ogni possibile manomissione o modifica indesiderata. In caso di utilizzo di archivi ODBC, occorre utilizzare database sicuri quali Microsoft SQL Server e gestire la corretta amministrazione delle sicurezza del sistema operativo Windows permettono l'accesso ai records solo all'amministratore di sistema oppure solo allo sviluppatore.
- Per limitare l'accesso alle funzioni ed ai comandi dell'applicativo sviluppato, il progetto Movicon.NExT deve utilizzare correttamente la gestione Profili Utenti Password con l'introduzione di Password, UserID, Nome Utente e Livelli di Accesso. Movicon.NExT prevede 1024 livelli di accesso e 32 aree.
- Gli utenti devono avere una password gestita in modo sicuro. L'inserimento di nuovi utenti da parte dell'amministratore può comportare il successivo reinserimento password da parte dell'utente al Log On successivo.
- Tutte le password possono avere impostata una scadenza per obbligare l'utente a reinserire una password periodicamente, contribuendo ad aumentare la sicurezza.
- Per una corretta corrispondenza alle norme, deve essere correttamente utilizzata la funzione di Auto LogOff (timeout di abilitazione accesso) nella gestione delle password di Movicon, al fine di evitare l'accesso non autorizzato al sistema dopo un periodo di inattività dell'utente.
- Per assicurare la validità e la corretta introduzione dei dati, gli utenti devono assicurarsi che le stazioni operative Movicon.NExT siano collocate in postazioni sicure ed accessibili solo al personale autorizzato.
- Nei sistemi con uso continuo, è obbligatorio utilizzare la funzione di Auto LogOff di Movicon.NExT.
- Movicon.NExT adotta strumenti e procedure per scoraggiare il perdurare di tentativi di accesso non autorizzati, allo stesso modo del sistema operativo Windows, secondo quanto previsto dalla norma. Dopo il quarto tentativo vano di accesso, Movicon.NExT provvede ad allungare sempre più i tempi di risposta per la reintroduzione della password, scoraggiando il malintenzionato.
- Il tentativo di violazione del sistema (Al quinto tentativo non autorizzato di Log On, Movicon.NExT provvede alla visualizzazione e registrazione nel Log Storico dell'evento, al fine di poter controllare tentativi di forzatura del sistema.

Varie

- Tutti i dati devono essere mantenuti in un database relazionale che soddisfi i requisiti di sicurezza (es. IMDB Criptato o ODBC con accessi protetti dalle manomissioni, anche tramite le funzioni di sicurezza proprie del sistema operativo Windows. I dati devono essere mantenuti in archivio per un adeguato periodo di tempo, in funzione delle necessità operative.
- Per soddisfare ulteriormente la salvaguardia dei dati, del progetto, delle immagini, delle ricette, l'utente dovrebbe utilizzare prodotti software di terze parti che garantiscano il mantenimento delle versioni (ad esempio Microsoft Source Safe può essere utilizzato per il controllo delle versioni).

Firma Elettronica

Un sistema di controllo deve essere in grado di acquisire lo stato reale e l'andamento delle variabili del processo. Sulla sezione relativa al periodo di lavorazione di un certo batch di prodotto devono essere indicati la data ed il numero di lotto del prodotto, inoltre deve essere apposta la firma elettronica dell'operatore responsabile ed eventualmente la firma di validazione del responsabile del processo. Le procedure devono assicurare che non avvengano degli errori e che le firme siano sempre riconducibili in maniera univoca al loro proprietario. I record devono essere archiviati in posto sicuro e mantenuti per un periodo adeguato, e devono essere protetti da accessi non autorizzati.

La sicurezza

La sicurezza, nei sistemi sottoposti a validazione, è fondamentale. Quando i dati vengano registrati in formato elettronico, vi sono due casi.

1. **Firma Manuale**: Quando i dati vengono sempre stampati e firmati per approvazione (i cosiddetti sistemi ibridi: carta ed elettronico). In questo caso il file è da considerare un record elettronico: occorre assicurare che il file con i dati non possa essere sostituito né manipolato prima di essere stampato, identificato, datato e firmato. Invece la firma elettronica può non essere necessaria in quanto viene apposta manualmente. Quindi ad esempio una condizione necessaria è che il formato dei dati non sia manipolabile, e che venga univocamente ed automaticamente associato ad una linea o al lotto di produzione. Inoltre il file dei dati originari va conservato. Potremmo sintetizzare questo caso ricordando che una firma autografa non "nobilita" un record elettronico non adeguatamente protetto.
2. **Firma Elettronica**: In questo caso tutto avviene in forma digitale, e tutti i dati (record) verranno archiviati in formato elettronico. Qui, oltre a garantire che il file con i dati non possa essere sostituito né manipolato, qualora sia necessaria una firma di approvazione, nasce l'esigenza di avere anche la firma elettronica. In pratica bisogna fare in modo che all'interno del file dei dati siano anche presenti delle informazioni che lo riferiscano univocamente al lotto di produzione e alla persona che ha approvato questi dati, cioè chi si era registrato al momento dell'approvazione dei dati. Tutto il file deve essere poi protetto da eventuali manomissioni o alterazioni dei dati originali.

La firma elettronica

La firma elettronica può essere realizzata per mezzo di una combinazione di almeno due elementi ad esempio un codice identificativo ed una parola chiave o un badge ed una parola chiave ecc., come richiesto dal CFR21 part 11. Deve essere assicurata l'univocità della combinazione identificativo - parola chiave in modo che sia possibile identificare con certezza ciascun individuo. Il codice identificativo può essere pubblico, cioè può essere mostrato sullo schermo. Dato che l'unicità della parola chiave non può essere assicurata, sarà il codice identificativo a dover essere univoco per ogni utente.

Anche le seguenti regole sono consigliate:

- Lunghezza minima della password;
- Modifica periodica della password;
- Procedure per evitare i tentativi di manomissione o di accesso non autorizzati;
- Registrazione dei tentativi di accesso non autorizzati;
- L'amministratore di sistema non deve poter conoscere le passwords degli altri utenti, anche se deve poter assistere chi dimentica la sua password;
- Gruppi di utenti possono eventualmente condividere la stessa password solo per la lettura di dati, non per la firma elettronica;

6.3. Validazione e Documentazione

Il sistema di Validazione dei dati sottoposti ad Audit Trail si basa su un modello di massima sicurezza che prevede l'uso di un utente di sistema criptato e sulla verifica del Transaction Log di SQL Server. Tutti i dati sottoposti ad Audit Trail vengono registrati secondo criteri di sicurezza univoca e potranno essere validati attraverso la visualizzazione e la stampa gestita dall'apposito oggetti grafico denominato "Validatore Audit Trail", disponibile nella toolbox di Movicon.NExT.
La validazione, per riportare esito positivo, deve esaminare i dati storici e individuare ogni eventuale manomissione eseguita esternamente a Movicon. Ogni variazione non autorizzata sarà quindi inevitabilmente rilevata mediante l'analisi del Transaction Log e dell'utente diverso dall'utente criptato di Movicon (utente "NExT_IO_Server") che ha eseguito le operazioni.

Per quanto riguarda il concetto di validazione e la documentazione necessaria dovranno essere tenuti in considerazione i seguenti punti :

- Alcuni dei requisiti della norma richiedono attività ed accorgimenti che non sono basati sul software applicativo. Per soddisfare i requisiti della normativa Part 11 il cliente deve validare la sua applicazione per garantire accuratezza, affidabilità e sicurezza nella registrazione dei dati, oltre alla capacità di impedire manomissioni, errori, cancellazioni di dati. Gli utenti Movicon.NExT devono convalidare le applicazioni realizzate in conformità alla norma FDA. Gli utenti possono sviluppare e/o eseguire la convalida di programmi e protocolli essi stessi o demandare a altri enti queste attività. La convalida dovrebbe seguire una metodologia stabilita del ciclo di vita del sistema (SLC).
- Per soddisfare i controlli richiesti dall'ottenimento della conformità alla normativa, il cliente deve adottare adeguate procedure per verificare l'identità dell'individuo al quale è stata assegnata una firma elettronica.
- Il cliente deve stabilire per iscritto e mettere in pratica le procedure per responsabilizzare gli operatori sulle operazioni eseguite sotto la loro firma elettronica, impedendo falsificazioni o manomissioni di firme o di registrazioni, in conformità ai requisiti della norma.
- Il cliente deve sempre accertarsi dell'identità dell'individuo al quale assegna una firma elettronica. Inoltre il cliente è tenuto a certificare per iscritto all'Ente Federale preposto (FDA) che intende utilizzare la firma elettronica come sostituto equivalente dei documenti cartacei tradizionali e, se necessario, produrre la documentazione necessaria richiesta dall'ente.
- Il cliente è responsabile nel produrre la documentazione sull'uso del sistema o dell'applicativo realizzato, sulla distribuzione e sull'aggiornamento della documentazione prodotta, nonché sull'addestramento del personale. Tuttavia il cliente non è responsabile sulla documentazione delle piattaforme utilizzate (Movicon, Windows).
- La produzione di documentazione "garantita" deve utilizzare gli strumenti di visualizzazione stampa previsti dalla piattaforma Movicon.NExT, che sono in grado di validare e garantire la veridicità dei dati storici registrati, secondo quanto opportunamente predisposto nelle proprietà del progetto.

Audit-Trail

L'audit-trail ha il compito di registrare tutte le attività che un utente compie sulle variabili di processo durante il runtime. L'abilitazione alla registrazione di queste attività

avviene semplicemente selezionando l'opzione 'Abilita Gestione Audit' all'interno delle proprietà di una variabile.
La proprietà 'Abilita Protezione Dati' permette di proteggere i dati storici e quelli di Audit in modo tale da
poterli poi validare tramite l'apposito oggetto della ToolBox "Validatore Audit Trail".
Abilitando questa opzione, inoltre, il ServerIO verrà avviato con l'utente "NExT_IO_Server", creato in fase di SetUp da Movicon. Tale utente, la cui password è criptata, verrà utilizzato dal sistema per gestire le registrazioni sul DataBase e sarà l'unico utente che potrà anche validare i dati con l'oggetto sopra menzionato.
Di seguito alcune delle principali colonne o "voci" che potranno essere visualizzate all'interno degli oggetti "Validatore Audit" e "Visualizzatore Storico" per tenere traccia di eventuali modifiche alle variabili:

- **Name**: indica appunto il nome della variabile.
- **Description**: descrizione associata alla variabile tramite la proprietà "descrizione" della Tag.
- **Value**: indica il valore della tag successivo alla modifica.
- **ValueBefore**: indica il valore della tag precedente alla modifica.
- **Status:** qualità della tag.
- **RecordDateTime:** indica la data e l'ora dell'evento.
- **UserName**: nome utente che ha generato l'evento
- **Reason**: Commento imputato dall'utente durante la modifica (se abilitata precedentemente la proprietà Forza Commento su Audit)

Validazione dei dati

La validazione dei dati deve essere effettuata tramite l'oggetto 'AuditViewer' presente nella toolbox di Movicon.NExT.
La validazione dei dati in Movicon.NExT si basa essenzialmente sul Transaction Log di SQL Server. In pratica vengono monitorati i log relativi al database protetto e si ricercano eventuali modifiche ai recordset effettuate da utenti non autorizzati che non siano quello previsto dall'I/O Server di Movicon.NExT (utente "NExT_IO_Server").

Al primo avvio del progetto, dopo la prima registrazione di dati all'interno del database su SQL Server, viene effettuato un primo backup del database in automatico (cartella backup dell'installazione di SQL Server). Questo primo backup è **fondamentale** per la successiva validazione dei dati. Nel caso in cui questo venga rimosso o cancellato non sarà più possibile validare i dati presenti all'interno del database.
Inoltre la validazione dei dati su Transaction Log non si basa sul nome dell'utente di validazione (default "NExT_IO_Server"), ma sul suo SID (ID di sicurezza dell'utente). Questo significa che nel caso in cui l'utente di validazione (default "NExT_IO_Server") venga cancellato dal sistema operativo e successivamente rigenerato il SID cambia. Al cambio del SID non sarà più possibile validare i dati registrati con l'utente precedente.

Gestione Data e Ora

- La gestione della Data e Ora dei dati (time stamp), è gestita da Movicon.NExT utilizzando l'orario del sistema operativo Windows, sia come data e ora locale che come UTC (Universal Time Coordinated).
- Per avere coerenza e veridicità degli orari, l'utente dovrebbe impostare il sistema operativo affinchè utilizzi la funzione di sincronizzazione dell'orario del sistema verso i server metrologici di riferimento NTP (Network Time Protocol), oppure gestire la sincronizzazione della data di sistema dei Client rispetto al Server, affinchè le

registrazioni siano coerenti. Tali sincronizzazioni possono essere gestite direttamente con le funzioni del sistema operativo Windows 7, Windows 8, Windows 10 oppure tramite codice Basic Script per sincronizzazioni orari di progetto.

Utente di Validazione (NExT_IO_Server)

L'utente criptato ed univoco di validazione ("NExT_IO_Server"), che è fondamentale per la validazione dei dati di Audit-Trail, viene aggiunto nel sistema operativo in fase di **Setup di Movicon**. Tale utente verrà aggiunto come utente locale alla macchina con il nome "NExT_IO_Server" eseguendo un Setup Standard. Se si esegue invece un Setup Personalizzato sarà possibile specificare un nome utente diverso ed eventualmente creare/selezionare un utente di Dominio (nell'eventualità che il PC appartenga ad un Dominio).

L'utente di Dominio potrà ovviamente essere creato soltanto facendo l'accesso con un utente di Dominio in possesso delle credenziali necessarie all'esecuzione dell'operazione.

L'utente di validazione ("NExT_IO_Server") verrà inoltre aggiunto tra le sicurezze di SQL Server e verrà aggiunto nella lista degli utenti che possono avviare i servizi di Windows.

Se l'utente di validazione (default "NExT_IO_Server") viene aggiunto come utente di domino anche l'applicazione Client di Movicon dovrà essere avviata con un utente di dominio che abbia le credenziali per recuperare le informazioni dell'utente di validazione (default "NExT_IO_Server").

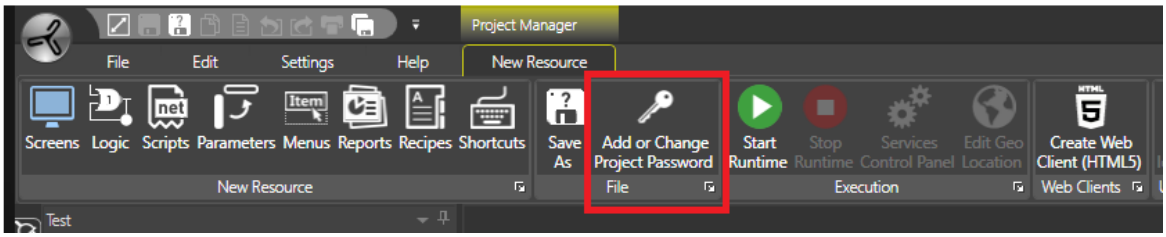
Se l'I/O DataServer di Movicon.NExT viene eseguito come servizio, l'utente di validazione (default "NExT_IO_Server") dovrà essere il medesimo con il quale si avvia il servizio, a meno che non si scelga di cambiare utente volontariamente nel 'Services Control Panel' oppure venga installato il servizio prima di abilitare una delle opzioni di protezione dei dati.

6.4. Configurazione Progetto CFR21

Per ottenere un progetto Movicon.NExT validabile ai sensi della norma 21CFR Part 11, occorre configurare opportunamente il progetto, per renderlo compatibile con i criteri di validazione FDA. Riportiamo di seguito le caratteristiche di configurazione necessarie:

Sicurezza

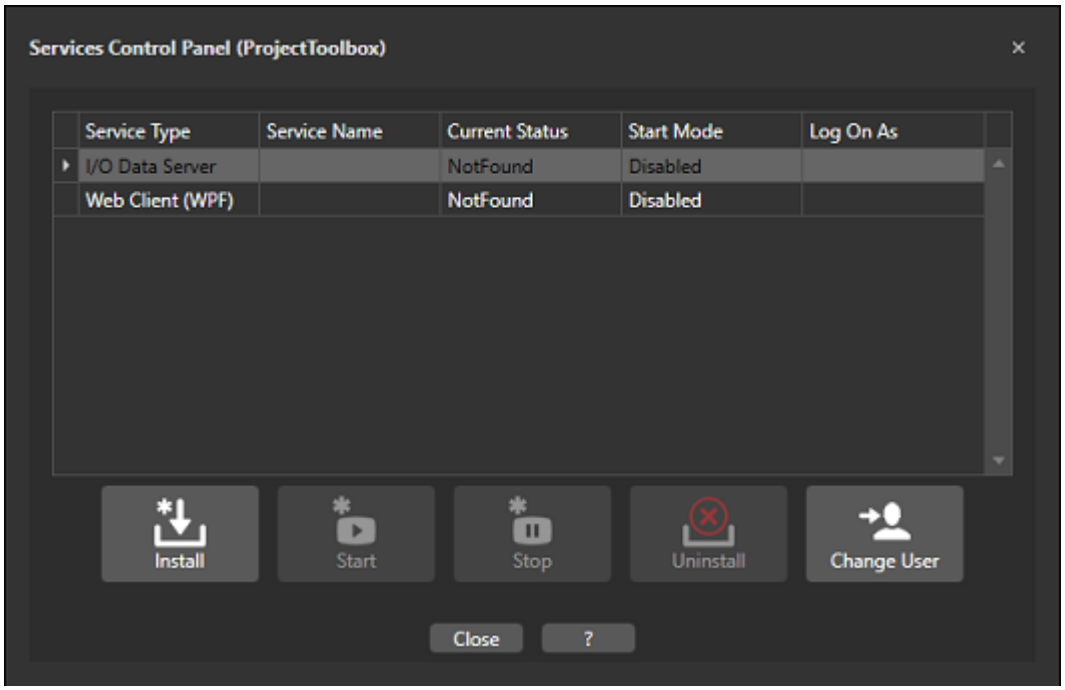
Il progetto deve essere configurato nelle sue Proprietà Generali selezionando "Progetto con Password" ed impostando la password di protezione. In tal caso l'accesso in programmazione al progetto sarà protetto e tutte le informazioni XML del progetto saranno criptate ed inaccessibili grazie ad un algoritmo proprietario di cifratura.



La conferma dell'operazione prevede il salvataggio di tutti i files del progetto Movicon.NExT con criptazione e protezione alla successiva apertura del progetto. E' importante ricordare che un progetto "protetto da password" potrà essere eseguito in runtime ma non sarà più modificabile o accessibile in programmazione senza password di accesso.

Avvio del sistema

- All'accensione del PC, viene avviato il sistema operativo Windows e di conseguenza la piattaforma Movicon.NExT con l'avvio automatico del progetto. Queste operazioni, ai fini della sicurezza, dovrebbero essere configurate opportunamente per garantire l'avvio del progetto in modo sicuro e protetto.
- All'avvio di Windows, tutte le componenti Server di un progetto Movicon.NExT dovrebbero essere eseguite automaticamente, mediante le funzioni dei Servizi di Windows. Il progetto Movicon.NExT quindi dovrebbe prevedere la gestione dei Servizi, utilizzando l'apposito pannello di configurazione accessibile dall'Editor di Movicon.NExT, che consente di installare le parti Server (come ad esempio l'I/O Server, gli Schedulatori, le Ricette, ecc.) come Servizi di Windows. In questo modo verranno avviati automaticamente all'avvio del sistema operativo in modo indipendente dal Log On dell'Utente di Windows.



Pannello di Installazione Servizi dall'Editor di Movicon.NExT

- L'interfaccia utente di Windows è accessibile solo dopo l'autenticazione dell'utente di Windows. Di conseguenza, l'interfaccia utente (Client) di Movicon.NExT sarà disponibile solo dopo avere eseguito il Log On dell'utente di Windows. Vi sono diverse possibilità di gestione in tal senso:

    - L'avvio di Windows può avvenire normalmente, mediante la richiesta di autenticazione di un utente di Windows. Fino a che un utente di Windows non esegue il Log, nessuna interfaccia desktop è disponibile. Dopo che un utente ha eseguito il Log On di Windows, le applicazioni di startup possono essere eseguite, e quindi si può eseguire una riga di comando che prevede l'avvio del Client di Movicon.NExT. Il progetto Client di Movicon.NExT gestirà quindi le

sicurezze e la gestione utenti del progetto, incluso il consenso all'accesso al Desktop di Windows.

- L'avvio di Windows può avvenire impostando il sistema operativo in modo tale che avvenga automaticamente l'autenticazione di un utente Windows di default, mediante stringa di comando di avvio del sistema operativo. In tal caso, Windows si avvia con un utente "standard" abilitato, e di conseguenza può essere automaticamente avviato il Client di Movicon.NExT. Il progetto Client di Movicon.NExT gestirà quindi le sicurezze e la gestione utenti del progetto, incluso il consenso all'accesso al Desktop di Windows.
- La gestione degli utenti di Windows e di Movicon.NExT può essere condivisa. Movicon.NExT infatti permette la condivisione degli Utenti del Dominio di Windows, di conseguenza il Log On di un Utente Windows non solo permetterà l'autenticazione di Windows ma anche l'avvio del progetto Client di Movicon.NExT. In questo caso, gli utenti di progetto Movicon.NExT saranno ereditati dal quelli del dominio del sistema operativo Windows.
- E' possibile avviare Windows senza rendere disponibile il Desktop (compresa la gestione ed esplorazione risorse), ed avviare quindi solo il Client di Movicon.NExT impedendo ogni accesso al Desktop di Windows.
- In ogni caso, l'accesso al desktop di Windows o la sua esclusione, e la configurazione dei privilegi degli utenti di Windows non dipende da Movicon.NExT, e dovrà essere gestita dall'amministratore del sistema.

Accesso all'interfaccia utente (Desktop) di Windows

Durante il contesto operativo, quindi dopo l'avvio di Windows e l'avvio dell'applicazione del progetto Movicon.NExT, è importante gestire in modo corretto le funzioni del sistema operativo che consentono l'accesso al desktop dall'applicazione.
L'utente ha la possibilità di gestire in modo controllato l'accesso al Desktop, in funzione di come è stato avviato il sistema operativo, mediante l'impostazione di un livello di accesso associabile agli utenti di password del progetto.

- Quando l'interfaccia utente di Movicon.NExT (Client) è in esecuzione, è possibile impedire l'accesso non autorizzato all'interfaccia utente di Windows (desktop), mediante la richiesta di autenticazione degli utenti di Movicon.NExT che hanno ricevuto il privilegio di avere la possibilità di accedere al Desktop. Nelle Proprietà Generali del Gestore Utenti di Movicon.NExT è possibile quindi assegnare un ruolo richiesto agli utenti che possono accedere al Desktop.
- E' possibile configurare il sistema operativo per escludere il Desktop di Windows ed utilizzare quindi solo le funzionalità dell'interfaccia utente di Movicon.NExT. Per ottenere ciò il sistema operativo deve essere opportunamente configurato da un amministratore di sistema.

Passwords

Tutti i comandi dell'applicazione eseguibili dall'operatore che possono influire sul processo devono essere protetti opportunamente da password.
La gestione delle password deve essere abilitata nelle Proprietà Generali della risorsa Utenti Password del progetto:

- **Abilita Gestione Password:** verranno attivate le password secondo i livelli e le modalità di accesso ai comandi impostate.
- **Auto Log Off:** determina il tempo (sec.) per disattivare automaticamente l'utente attivo dopo il periodo di inattività.
- **Lunghezza Minima Password**: verrà impostata la minima lunghezza ammessa nell'impostazione della password (per default è 4 caratteri).

- **Definizione Firma Elettronica**: nelle proprietà di ogni singolo Utente verrà gestita l'univocità della Descrizione dell'utente quale nome da utilizzarsi come Firma Elettronica.

  Movicon.NExT gestirà automaticamente il controllo delle corrette autenticazioni, la gestione dell'univocità della Firma Elettronica, i tentativi di forzatura nel Log In Utenti registrando il messaggio di tentativo di intrusione negli eventi di Log dopo il 5 tentativo fallito di Log In, e scoraggiando i tentativi successivi mediante opportune tecniche di allungamento dei tempi di risposta.

  Il nr. di tentativi di log-on è impostabile nel file di sistema "MoviconNExT.exe.config" nella sezione delle Membership come riportato nell'immagine sottostante.

```
<membership defaultProvider="AspNetSqlMembershipProvider">
  <providers>
    <remove name="AspNetSqlMembershipProvider" />
    <add name="AspNetSqlMembershipProvider" type="System.Web.Security.SqlMembershipProvider, System.Web,
         connectionStringName="LocalSqlServer"
         enablePasswordRetrieval="false"
         enablePasswordReset="true"
         requiresQuestionAndAnswer="false"
         applicationName="/"
         requiresUniqueEmail="false"
         passwordFormat="Hashed"
         maxInvalidPasswordAttempts="5"
         minRequiredPasswordLength="1"
         minRequiredNonalphanumericCharacters="0"
         passwordAttemptWindow="10" passwordStrengthRegularExpression="" />
  </providers>
</membership>
```

  Ogni Utente o Gruppo di Utenti che avranno accesso ai comandi o che potranno influenzare il processo, devono essere opportunamente inseriti e configurati nel progetto.
  La gestione degli utenti prevede il loro inserimento nella Risorsa Utenti Passwords del progetto, quindi la configurazione delle loro proprietà. Tra le proprietà degli utenti, ricordiamo quelle richieste dalla norma FDA:

- **Nome (ID) e Password:** sono assegnati all'utente e ne consentono l'identificazione dal sistema.
- **Firma Elettronica:** è il testo, univoco, che corrisponde alla firma elettronica e che verrà registrato come identificativo assoluto utente (nelle proprietà della Risorsa Utenti Passwords deve essere abilitata la gestione della Firma Elettronica).
- **Auto Log Off:** può essere specificato il tempo di disattivazione dell'Utente attivo dopo un periodo di inattività.
- **Durata Password**: la norma richiede che le password degli utenti possano "spirare" dopo un tempo prefissato, affinchè l'utente sia obbligato a cambiarla periodicamente, incrementando la sicurezza.
- **Modifica Password Obbligatoria**: la norma richiede che l'utente sia obbligato ad introdurre la propria password la prima volta che esegue il Log In, evitando che l'amministratore che l'ha inserito possa conoscerla, contribuendo alla certezza dell'identificazione.

  E' buona norma per ottenere password più sicure, utilizzare lettere, numeri e caratteri speciali.
  Per forzare l'uso di numeri e caratteri speciali nelle password, è possibile modificare il file di sistema "MoviconNExT.exe.config". introducendo la variabile "minRequiredNonalphanumericCharacters".
  Il valore inserito, risulterà essere il minimo numero di caratteri non alfanumerici richiesto nella password.

```
<membership defaultProvider="AspNetSqlMembershipProvider">
  <providers>
    <remove name="AspNetSqlMembershipProvider" />
    <add name="AspNetSqlMembershipProvider" type="System.Web.Security.SqlMembershipProvider, System.Web,
         connectionStringName="LocalSqlServer"
         enablePasswordRetrieval="false"
         enablePasswordReset="true"
         requiresQuestionAndAnswer="false"
         applicationName="/"
         requiresUniqueEmail="false"
         passwordFormat="Hashed"
         maxInvalidPasswordAttempts="5"
         minRequiredPasswordLength="1"
         minRequiredNonalphanumericCharacters="0"
         passwordAttemptWindow="10" passwordStrengthRegularExpression="" />
  </providers>
</membership>
```

Commento sul Riconoscimento Allarme (Audit Trail)

In molti casi, prima che l'utente proceda ad eseguire il riconoscimento di un allarme, potrebbe essere richiesto l'inserimento di un commento da parte dell'utente stesso che verrà poi registrato nello storico insieme all'evento di ACK dell'allarme.
Movicon.NExT permette di gestire questa funzionalità mediante la specifica di un livello di priorità per ogni singolo allarme, oltre il quale la finestra Allarmi di Movicon.NExT richiederà all'utente di specificare un commento sull'operazione di riconoscimento.
E' necessario quindi definire il livello di priorità dell'allarme, e definire la soglia di priorità per la quale sarà richiesto l'inserimento del commento all'operazione.

1. Nelle proprietà di ogni allarme quindi dovrà essere specificato il livello di priorità (severity).
2. Nelle proprietà della Finestra Allarmi dovrà essere specificato il livello di priorità oltre il quale il sistema richiederà all'operatore di forzare l'inserimento di un commento (Audit) per l'operazione di riconoscimento.
   Il commento verrà registrato nello storico eventi con l'operazione di tacitazione.
   Naturalmente, potrà essere impostato un Livello di Accesso utente per eseguire le operazioni sugli allarmi.

Sicurezza e Validità dei dati di archivio

Garantire la sicurezza dei dati storici registrati, al fine di impedire manipolazioni dei Record Elettronici, è fondamentale per ottenere la validazione e la conformità alla direttiva CFR21 della propria applicazione.
I dati registrati da Movicon.NExT (Audit, Historian, Data Loggers) sono costituiti fisicamente da archivi su file database. Per garantire un efficace sistema di validazione dei dati, Movicon richiede obbligatoriamente l'utilizzo di Microsoft SQL Server come base dati per le registrazioni. I progetti possono utilizzare altri tipi di database per i propri archivi storici, ma se si desidera ottenere un progetto conforme alla normativa FDA CFR21 Part 11, il sistema di validazione dell'integrità dei dati storici di Movicon.NExT si basa su meccanismi di controllo sicuri che richiedono obbligatoriamente l'utilizzo di Microsoft SQL Server.
Occorre pertanto attenersi obbligatoriamente alle configurazioni di sistema ed ai vincoli di progetto previsti, descritti nella documentazione di prodotto.
In sintesi, il meccanismo di validazione di Movicon.NExT prevede che i dati registrati su database utilizzino un criterio di univocità dei dati, basato sull'utente di sistema criptato Movicon.NExT User, e su opportuni controlli del Transaction Log del sistema SQL Server. Movicon pertanto registrerà i dati utilizzando un Utente di Sistema Windows univoco e criptato, basandosi sul Transaction Log del DB per controllare ed evidenziare eventuali manomissioni.
Il database validabile quindi disporrà di informazioni di processo e di informazioni di Log di ogni transazione, in modo tale che gli archivi sottoposti a validazione non possano in alcun modo essere manomessi o modificati.

Un archivio originale pertanto verrà analizzato e validato dall'apposito Visualizzatore, ed in caso di manomissioni, il Visualizzatore evidenzierà che i dati sono stati manomessi e pertanto non saranno validabili.
Oltre a quanto sopra, gli utenti hanno la responsabilità di gestire comunque in modo opportuno il criterio di sicurezza all'integrità dei dati, gestendo i database mediante le opportune protezioni di accesso e impostando in modo appropriato un sistema che garantisca la disponibilità dei dati per un periodo di tempo adeguato secondo i requisiti della norma, gestendo funzionalità di ridondanza o backup dei dati.

Records Elettronici

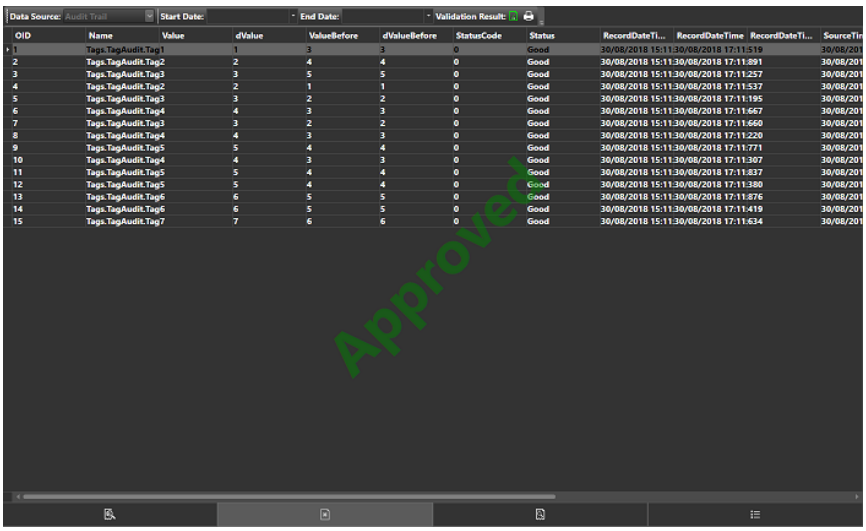
Per Record Elettronici si intendono tutte le informazioni di processo (dati, valori, eventi) registrate elettronicamente in archivi che devono garantire l'integrità del dato e prevenirne la manipolazione.
Tutte le informazioni che Movicon.NExT provvede a registrare in archivio possono essere definite "Record Elettronici".
Affinchè i Record Elettronici di Movicon.NExT possano essere conformi alla norma, occorre seguire le indicazioni e le linee guida contenute in questo documento e nel manuale tecnico per garantire sicurezza nell'integrità dei dati e prevenire accessi non autorizzati o manipolazioni.

Il sistema di Validazione Dati di Movicon.NExT

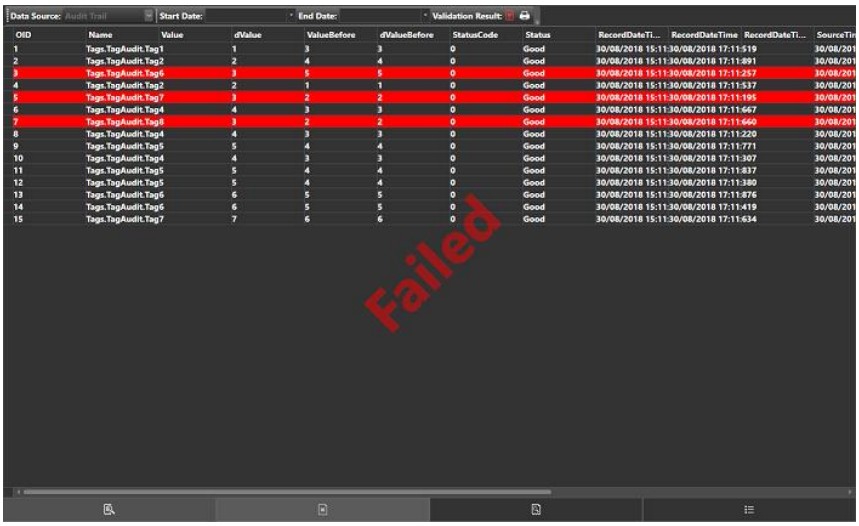
I dati registrati secondo i vincoli progettuali su database SQL Server, con le relative caratteristiche intrinseche di sicurezza, saranno sottoponibili a validazione ed autenticazione, in modo da poter garantire l'originalità dei dati e quindi ad impedire ogni tipo di manomissione.
Movicon.NExT gestisce un sistema di validazione dei dati registrati, attivabile mediante le opportune proprietà di configurazione impostabili nelle configurazioni della gestione degli storici.
Pertanto, nelle proprietà di Impostazione Database dei motori di registrazione gestiti dal Server di Movicon.NExT, è possibile abilitare la proprietà Abilita Protezione Dati.
Se si abilita questa funzione, Movicon.NExT utilizzerà la combinazione di User ID di sistema (criptato) e Transaction Log, garantire l'integrità di ogni singolo dato registrato (record) registrato sul DB.
Grazie a questo controllo, Movicon.NExT sarà in grado di garantire gli utenti sull'originalità dei dati registrati, impedendo quindi ogni possibile manipolazione o cancellazione di dati.

Ogni archivio storico potrà quindi essere sottoposto a controllo di validazione in Movicon.NExT, riportando l'autenticità dei dati o evidenziandone l'eventuale manomissione.

Gli utenti, in un sistema sottoposto a validazione CFR21, potranno quindi garantire l'autenticità dei dati predisponendo ove necessario sia la gestione della protezione dei dati, sia il controllo di validità in visualizzazione o stampa.
Risulterà pertanto impossibile manipolare dei dati storici registrati da Movicon.NExT quando è abilitata la gestione della protezione dei dati, in quanto il controllo di validazione sarà in grado di validare l'archivio o di evidenziarne la manomissione.



La figura sopra illustra un archivio storico sottoposto a validazione con risultato positivo. Sotto invece si illustra lo stesso controllo su un archivio storico manomesso.



Periodo di mantenimento dei dati

I dati storici devono essere disponibili in archivio per un periodo di tempo idoneo ed appropriato al tipo di processo gestito. Il periodo di tempo gestito è liberamente specificabile nelle proprietà dei motori di registrazione di Movicon.NExT, a prescindere dal tipo di database utilizzato.

Le proprietà degli oggetti consentono infatti di definire il numero di giorni (ad esempio, impostare 730 giorni per definire due anni) per i quali l'applicazione garantirà la disponibilità dei dati. Raggiunto tale periodo, il dato più vecchio in archivio sarà sovrascritto dal dato più nuovo, garantendo così sempre il periodo di archivio desiderato.

Eventuali backup dei dati potranno essere liberamente gestiti dal progetto mediante funzioni script che ne gestiranno la sorgente e la destinazione dei files di backup, oppure potrebbero essere gestiti con appositi strumenti di terze parti.

Ridondanza

Movicon.NExT supporta completamente la funzionalità di ridondanza multiserver, non solo per la sincronizzazione degli archivi ma anche per ogni funzionalità operativa, in modo completamente automatico e trasparente.

La funzione di Ridondanza dovrebbe essere applicata e gestita, in ottemperanza con le richieste della norma, in funzione della caratteristiche del processo.

Grazie alla Ridondanza, Movicon.NExT sarà in grado di gestire in modo sincronizzato gli archivi storici su più server, garantendo non solo l'alta affidabilità dei dati, ma anche delle operazioni.

Sicurezze esterne per gli archivi DB

Tramite le funzionalità del Server di Movicon.NExT, i dati di processo sono registrati sul database configurato. Tali dati quindi risiedono fisicamente in file e tabelle che possono essere registrati localmente sull'hard disk o su archivi di massa residenti fisicamente su server diversi, o sul Cloud. Grazie all'uso di database relazionali "sicuri" come SQL Server, Movicon.NExT utilizza connessioni protette (account) per l'accesso ai file. E' cura dell'utente configurare il sistema affinchè nessuno possa accedere ai file, rimuovendo i diritti di accesso ai file sia nel database stesso che nei privilegi di accesso alle cartelle da parte del sistema operativo (eseguendo Movicon.NExT come servizio).
E' necessario garantire la sicurezza dei dati attraverso le seguenti procedure:

- Movicon supporta ogni tipo di database relazionale per gli archivi. Tuttavia, per garantire i meccanismi di validazione, è obbligatorio utilizzare Ms SQL Server.
- Per evitare accessi non autorizzati ai file, occorre impostare la protezione alla connessione (User Accounts) utilizzando criteri di accesso noti solo all'amministratore di sistema oppure al progettista dell'applicazione (es. con la stessa password di protezione del progetto). Questo permette di impedire l'accesso alle tabelle dati se sprovvisti di autorizzazione.
- Utilizzare il blocco dell'accesso al sistema operativo (blocchi da Movicon.NExT o diritti di accesso al sistema operativo utilizzando Movicon.NExT come Servizio). In tal caso sarà impedito fisicamente l'accesso al file tramite il sistema operativo.
- Non condividere le cartelle o il disco in caso di stazione presente in rete, salvo l'accesso eventuale all'amministratore di sistema.
- Rimuovere i diritti di modificare i record del database (Update). Infatti Movicon.NExT provvede solo ad inserire nuovi record e per nessun motivo deve essere possibile accedere ai dati per alterarli.

6.5. Condivisione Utenti

Condivisione degli Utenti di Windows

Movicon.NExT offre la possibilità di condividere, nel progetto applicativo, gli Utenti del Dominio del sistema operativo o di un server Windows (Win7/Win10).
Questo permette al gestore del sistema di sicurezza di utilizzare un unico punto di definizione degli utenti di rete, utilizzando gli Utenti del Dominio di Windows, in alternativa o insieme agli utenti definiti nel progetto. Movicon.NExT quindi ammette configurazioni miste, ovvero sia utenti inseriti nella lista del progetto, sia utenti provenienti dal dominio Win7/Win10, la cui autenticazione e gestione è demandata al sistema operativo. In caso di utilizzo di utenti Windows il campo firma elettronica nei record elettronici, assumerà il valore dato dal nome utente qualificato dal dominio di appartenenza: Es. Nome dominio\Nome Utente. La configurazione mista, non garantisce quindi l'univocità delle informazioni inserite nel campo Firma elettronica, perché Movicon.NExT non può avere il controllo sulle informazioni relative agli utenti di dominio, è quindi una configurazione sconsigliata, seppur ammessa tecnicamente.
Quando viene richiesta l'autenticazione di un Utente in Movicon.NExT, mediante la richiesta di Log On, l'utente verrà verificato prima all'interno degli utenti di progetto, e se attivata la proprietà di "Condivisione Utenti di Windows", Movicon.NExT chiederà quindi al sistema operativo di autenticare il Nome Utente e la sua Password al Dominio

del sistema operativo. Il criterio che stabilirà il Livello di Accesso di progetto è definito tramite i Gruppi di Utenti, come vedremo di seguito.

Gli utenti definiti nel Dominio di Windows (Primary Domain Controller) possono essere autenticati anche in Movicon.NExT e ricevere associato un livello di utenza personalizzato, mediante la comune definizione di Gruppi di Utenti. Occorre infatti che gli Utenti del Dominio di Windows siano inseriti in Gruppi di Utenti di Windows il cui nome sia identico e presente nei Gruppi di Utenti di Movicon.NExT. Infatti, ogni gruppo di Utenti di Movicon.NExT permette di definire il Livello di Accesso e L'Area di Accesso nelle sue proprietà. Quindi, quando un Utente viene autenticato da Windows, Movicon.NExT riceverà l'autorizzazione ed assegnerà il Livello di Utenza definito nel nome del Gruppo di appartenenza.

E' quindi possibile assegnare ad ogni Utente di Dominio il livello di password e l'Area di accesso desiderata, mediante l'utilizzo dei Gruppi.

Ad esempio:

- Windows ha definito l'utente "R_Waters" nel gruppo "Machine_Operators".
- Il progetto Movicon.NExT dovrà anche lui contenere un Gruppo di Utenti con l'identico nome "Machine_Operators".
- Al Gruppo di Movicon.NExT vengono assegnate le proprietà desiderate di Livello di Accesso ed Area per gli utenti del Gruppo, come ad esempio "R_Waters".
- Nel progetto dovrà essere attiva la proprietà di Condivisione Utenti del Dominio di Windows.
- Quando l'utente eseguirà in Movicon.NExT l'operazione di Log On, passerà in modo sicuro le credenziali di accesso a Windows, che ne eseguirà l'autenticazione dando esito positivo a Movicon.NExT. Quindi Movicon.NExT attiverà con successo l'Utente, assegnandogli il livello di accesso definito nel Gruppo.
- La stessa operazione può essere eseguita per qualsiasi altro utente, condividendo i Gruppi o creando nuovi gruppi a piacere.
- Questo meccanismo è valido anche per gli utenti configurati direttamente in runtime con la finestra di editazione utenti di Movicon.NExT.
- La Firma Elettronica dell'utente è il Nome (UserID) che Windows gestisce in maniera univoca, preceduto dal nome del Dominio.

Sistemi Biometrici

L'uso di sistemi biometrici è incoraggiato in applicazioni validabili secondo la norma. In tal caso occorre scegliere il sistema di riconoscimento più idoneo e quello più facilmente integrabile nel proprio applicativo, tra quelli presenti sul mercato.
Movicon.NExT è concepito per utilizzare i sistemi di autenticazione secondo il modello delle Membership, in modo indipendente dal Provider.
E' quindi possibile sostituire il provider di autenticazione utenti di default di Movicon.NExT, basato sulle Membership di ASP.NET, per utilizzare un altro provider, come ad esempio i sistemi di autenticazione biometrici.
I sistemi biometrici più diffusi sono sicuramente i sistemi di identificazione tramite impronta digitale. Questi sistemi hanno raggiunto una semplicità di utilizzo ed una perfetta integrazione con il sistema operativo e le applicazioni software.
Utilizzando le funzionalità ad esempio di Windows Passport, è possibile integrare nell'applicazione Movicon.NExT il sistema di autenticazione biometrico di Windows.

6.6. Validazione dei dati di Backup

E' importante sottolineare che la validazione dei dati eventualmente ripristinati da un backup deve tenere in considerazione le corrette procedure di ripristino, diversamente i dati di backup, seppure originali, non potranno essere validati.

Backup dei dati

La norma CFR21 Part 11 richiede espressamente il corretto uso del backup dei dati. Tuttavia, i dati da sottoporre a validazione devono necessariamente seguire un Backup che tenga conto anche del ripristino dei dati utente del sistema operativo Windows. Questo è necessario in quanto la validazione dei dati da parte del Validatore di Audit Trail di Movicon.NExT si basa sul security identifiers (SID) dell'utente del sistema operativo contenuto nei dati di backup.
Un eventuale ripristino parziale dei soli dati di processo, senza il necessario ripristino dell'utente del sistema operativo comporterebbe la mancata validazione dei dati di processo ripristinati.
Si rimanda comunque alla documentazione Microsoft per la procedura di backup dell'immagine di sistema operativo, da considerarsi alla procedura di backup dei dati.

La validazione dei dati si basa sul TRANSACTION LOG di SQL Server, ed utilizza il SID (ID di sicurezza dell'utente) univoco dell'utente di validazione (Utente "NExT_IO_Server").
Questo significa che nel caso in cui l'utente di validazione ("NExT_IO_Server") venga cancellato dal sistema operativo e successivamente rigenerato il SID cambia. Ai fini di garantire la massima sicurezza nella validazione, cambiando il SID non sarà più possibile validare i dati registrati con l'utente precedente!

Quindi, oltre al backup dei dati contenuti nel database di SQL Server (che include il Transaction Log), è necessario pianificare il backup del sistema operativo perlomeno nella parte riguardante gli Utenti di Windows.
Per altre info riguardo l'implementazione di una buona strategia di backup si rimanda alla documentazione Microsoft di SQL Server e del backup e ripristino di Windows.

Ripristino dei dati

In caso di "Disaster Recovery" sarà necessario procedere al ripristino dell'immagine del sistema operativo precedentemente creata.
Si rimanda comunque alla documentazione Microsoft per la procedura di Restore dell'immagine di sistema.
Per quanto riguarda il ripristino del database è **fondamentale** ripristinare i backup in base all'ordine in cui sono stati creati. Prima di ripristinare un determinato backup del log delle transizioni è necessario ripristinare tutti i backup precedenti senza eseguire il rollback delle transizioni, ovvero è necessario utilizzare (tramite SSMS) l'opzione WITH NORECOVERY all'interno della finestra di ripristino del database.

Si rimanda comunque alla documentazione Microsoft per la procedura di ripristino dei Backup del DB di SQL Server.

INDUSTRIAL AUTOMATION SOFTWARE

progea

Progea Srl
Via D'Annunzio, 295
I-41123 Modena
info@progea.com
Tel +39 059 451060

Progea International SA
via Sottobisio, 28
6828 Balerna (CH)
international@progea.com
Tel +41 91 96 76 610

Progea Deutschland GmbH
Marie-Curie Str., 12
D-78048 VS Villingen
info@progea.de
Tel +49 (0)7721 99838 0

Progea North America Corp.
2380 State Road 44, Suite C
Oshkosh, WI 54904
info@progea.us
Tel. +1 (888) 305-2999