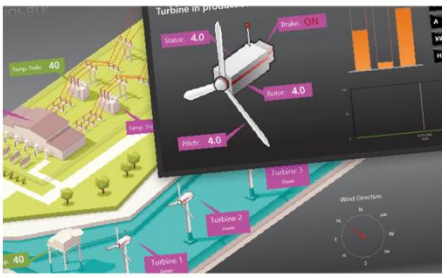
INDUSTRIAL AUTOMATION SOFTWARE

progea

Movicon.next™

Automation Platform.next generation



Movicon NExT

9.0 Security

Ver.3.4.268

Table of Contents

1. User and password management

1.1. Inserting Users and User Management

In order to utilize the User Management in your project you need to create a list of Users or Groups with profiles. When you insert Users and/or Groups in the project you can give them access rights and privilege levels that are needed for executing project commands.
Even though the Membership technology is used with the SQL repository to manage user authentication, the Users and Groups have to be created using the Platform.NExT project Users Editor. This is the only way possible to assign users with the specific information that is tied to the application that would not otherwise be assigned if using the Provider.

The Users or Groups Editor can be used in project edit mode, therefore while being programmed. It can also be used in runtime by authorized operators according to the preset modes and limits.

Users can be centralized in the **Domain of the Operating System** being used. In this case the Users Management has a profile managed by the Domain network of the Windows Operating System where the Platform.NexT project is run. Therefore users can be managed with both modes: if a user does not exist in the project, the domain can be asked to authenticate the user's existence among those in the Domain users.

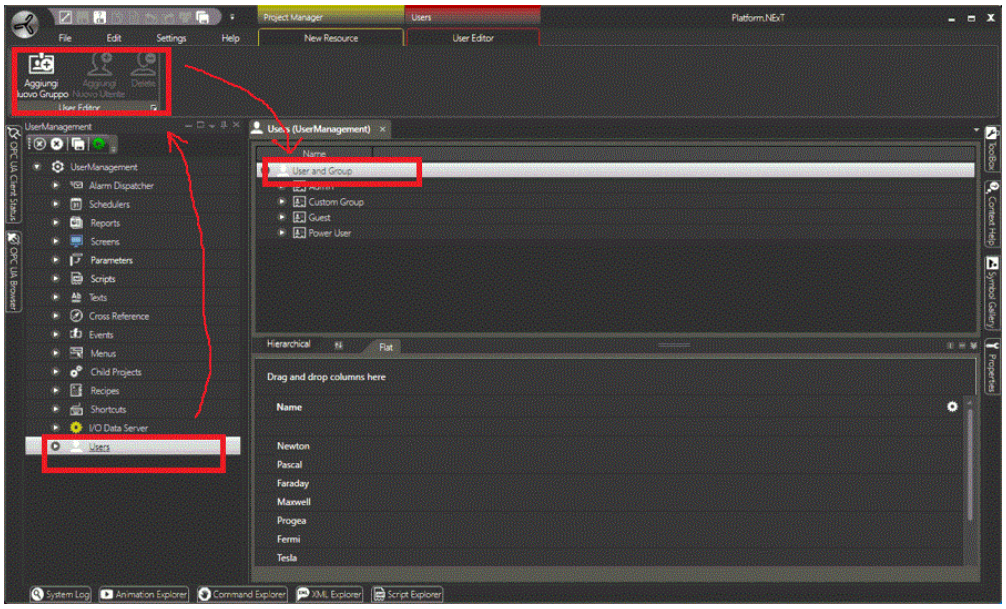
User authentication during runtime will be performed by the Provider by passing the credentials of the user, requesting the LogON, to the Platform.NExT.

A Windows user can also be authenticated without needing to insert a Group. When no folder is created containing a group name in the 'Users' resource, Movicon will create three predefined group folders as **Admin, Guest** and **Power User** when the project reopens. If these folders are cancelled, they will be automatically recreated at the next project startup unless at least one group already exists in the resource.
In cases when the 'Enable Windows Authentication' open has been selected, Movicon will attempt to authenticate a Domain User and associate this user to the group created in the 'User and Group' (i.e. 'Domain Users').
If the user is successfully authenticated, they will obtain access level rights of that same group.
If no user group exists, the user will obtain level 0. In cases where user groups exist without any domain users, the login will fail.

Project User Editor

The project's Users management Editor can be accessed from the "**Users**" resource from the project's tree structure. This editor is used for setting the User Manager's general properties, or for entering and configuring users and their access rights to project commands.

The users that are defined in the project will also be created automatically in the Membership Provider's SQL repository at the startup of Movicon in runtime if not already existing in the Provider's list of users. In this case the Provider Membership user settings will not be overwritten by the properties set in the project for local users.



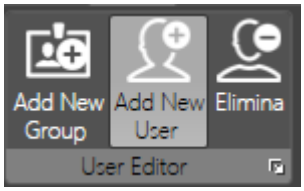
This image shows the programming environment and workspace of the User Manager.

Users Editor in Runtime

New users can be entered in the project during runtime as well , for example when new staff start while plant is already running a production process. The new users that are inserted in Runtime will be added to those previously inserted.
In order to insert users during runtime mode, the programmer should provide the necessary commands to display the Users Editor beforehand and as described in the topic on "User Manager Commands in Runtime".

User Editor commands

The commands used for editing Users and User Groups are located in the "User Editor - User Editor" Ribbon.



Ribbon containing the user editor commands.

Add New Group

This command is used for adding a new User Group to the project's user list. Once a new Group has been created, a pop-up window will automatically open containing the Group's properties (as described in previous paragraph).

Add New User

This command is used for adding a new User to the project's user list. The User must be inserted in a Group. Once a new User has been created a pop-up window will open containing the user properties (as described in previous paragraph).

Delete

This command is used for deleting the selected User or User Group. **The command is only available in Editing.**

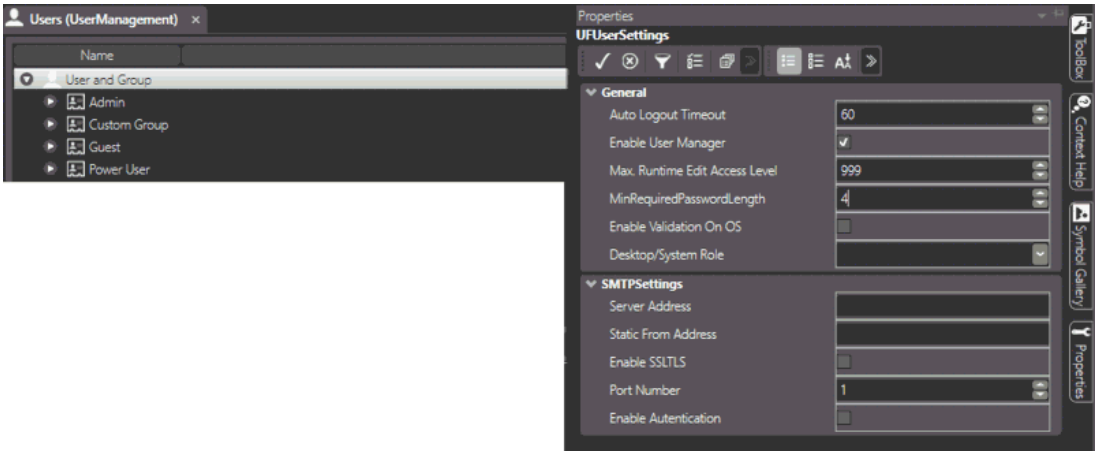
1.2. General User Management Settings

The User and Password management has a set of General Settings that can be displayed by means of using the Properties window after the User and Group Resource has been selected from the Users Editor.

Primarily, the general settings allow you to Enable or Disable the User Manager during runtime. In addition, there are a series of properties that concern the whole management and can be set as described below.

si sono

In order to activate the user manager in the project, you will need to enable the **"Enable User Manager"** property in the General User and Group Properties window.



General User Management Properties

Below are described the general properties of the project user management.

Auto Logout Timeout

This field is used to enter a time in seconds which will be used for logging out the active user automatically. The time in seconds refers to the inactive time. Therefore a logged in user that is inactive for the time set here will be automatically Logged Out for security reasons. If the user reassumes activity they will need to log on again.

Max. Invalid Password Attempts

This allows you to specify the maximum number of failed access attempts after which a user is blocked from using the system.

Setting the threshold criteria for user locks determines the number of failed login attempts that causes the system to block access of a specific user. When a user is locked, they will no longer be able to access the access even when using the correct credentials. The locked user will be denied access until reinstated by using the appropriate commands provided by Movicon.NExT.
This functionality requires you to set a failed login attempt value and to specify which users are to be locked using the "**User Lock Mode**" property.

User Lock Mode

This property gives you the possibility to specify which users are to be locked after attempting a certain number of failed logins.

This property come with the following options:

- None: the user lock mode is disabled (default value)
- OnlyEditableUser: Only those users with access levels lower or equal to the one set in the 'Max Runtime Edit Access Level' will be locked when exceeding the number of failed login attempts set in the 'Max. Invalid Password Attempts' property.
- All: In cases in which the number of failed login attempts is greater than the value set in the 'Max. Invalid Password Attemps' property, all users with different access levels will be locked out.

When needing to reinstate a locked user, use the commands contained in the 'Users' tab of any one of the Movicon.NExT objects.

Domain users are excluded from the lock users management as they are not managed directly by the Movicon.NExT membership provider.

Enable User Management

Enabling this property will activate the user manager during project Runtime. The programmer can then decide when to activate or deactivate the project's entire user management.

Login Control Visible

When the users management is enabled within the project, this property enables/disables the logo from displaying at the top right in screens used for logging in.

Max. Runtime Edit Access Level

This parameter is used to specify the maximum hierarchical level admissible for a user inserted or displayed in the project's Users Management at runtime.

Min. Password Length

This parameter is used to set the minimum number of characters allowed for a password to be associated to a user.

It is a good rule of the thumb to encourage strong passwords to increase security by using a mix of letters, number and special characters.

The use of numbers and special characters in passwords can be forced by modifying the "MoviconNExT.exe.config" system file by introducing the "minRequiredNonalphanumericCharacters" variable.
The value inserted in this property will be the minimum number of non-alphanumeric characters required in a 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>
```

Enable Windows Authentication

When this functionality is enabled, the User Management system will allow authentication of those users registered in the Domain of the Windows OS in which the project is run. In this way, if the user management cannot find a user in the project user list, it will ask the OS for user authentication using the LDAP protocol with the 'domain\user' format.
If the user is recognized, they will be authenticated from the Domain, and then validated for using the project. In this case their access rights will be determined by their **group** membership

Shared Connection Repository

Used to generate one table for all the projects containing all the various project users so that they can be shared.

The Movicon.NExT installations used for each project need to have memberships in common. It will therefore be necessary to modify the "Moviconnext.exe.config" and Platformnext.exe.config" files so that they use the same "membership".

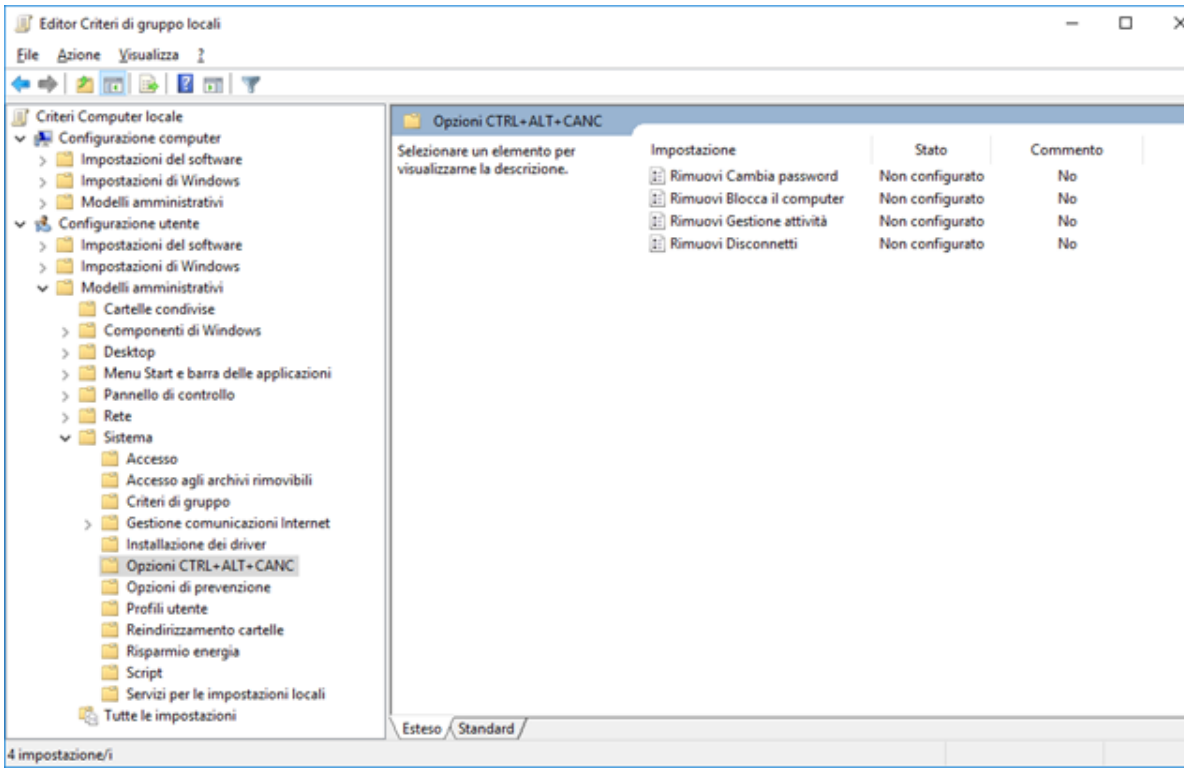
Desktop/System Role

This property is used to associate a "Group" and then the relative Users with rights for executing system operation commands. The system commands are those commands that are not linked directly to the project but to the operating system's functions which perform those operations. For example, closing the application window, reducing to icons, desktop access and closing the application.

The system commands are not managed by the application's objects but by Windows OS. To enable correct user management, it is important that the programmer decides which user has rights to use those operating system commands which are accessible.

Attention: this feature may, however, be fully compatible with Windows antimalware, which is constantly updated and therefore may be in execution and resetting certain system registry keys when Movicon is running whereby certain restrictions may be negated. In addition, the "CTRL+ALT+CANC" combo keys cannot be blocked using this

Movicon feature. In this case, the Windows' Local Group Policy Editor can be used to set these restrictions accordingly to prevent the antimalware from intervening. To startup the editor, digit "gpedit.msc" in Cortana's search bar and press enter:



The safest configuration to use rests on the use of the Movicon Server started up as service in combination with the Windows settings indicated above.

SMTP Property Settings

In addition to the general property settings, there is a **"SMTPSettings"** property group that allows you to set the report notification email functions.
Attention, these settings do not concern the Alarm Dispatcher Notifications which need an appropriate Server configuration.

Server Address
Sets the address of the SMTP server address.

Static from Address
If set, this allows the sender's address to be shown in the notification email to be generated by the system.

Enable SSL/TLS
When enabled, permits you to use the security certificates and encryption for authentication on the SMTP Server.

Port Number
This is used to set the SMTP output port's address.

Enable Authentication
Enabling this will activate the authentication on the SMTP server (when required).

User Name

This field is used to set the user name to be used when SMTP Server authentication is required.

Password

This is used to set the password to be used for the SMTP Server authentication when required.

1.3. User Group Properties

The User Groups are essential to the project's Users management. Users cannot be inserted individually unless the become members of a group first.
The Platform.NExT User Management offers these default groups: Admin, Guest, Power User. These groups can be modified, removed and new ones can be added. When a "Group" is selected within the workspace, its property window can be opened to defined the following settings:

Name

Defines the Group's name. The group must have its own unique name within the group list which must be no more than 64 characters long.

Default Access Level

This property is used to set the Group's hierarchical access level. This level will be used by those users who have not been set with an access level or who are authenticated by the operating system's domain.
The hierarchical level can be set a value from 0 to 9999. The value set here will determine the user's access rights. The higher the value the more access rights the user will have. For example, a user with level 10 will be able to activate controls requiring a level equal to or lower than this value (comprised between 1 and 10).
The Level -1 cannot be used for Groups, but can be used by the users to inherit the Group's level.

Default Access Mask

This property is used to define the access area using a bit mask for the Group. This mask will be inherited by those users who have not been set with one or who are authenticated by the operating system's domain.
Each bit corresponds to an access area where the user is permitted to interact with those controls that require an Access Area in addition to an Access Level. For example, When a control has been set with an Access Level and enabled with the Access Area 1, users who login with an Access level equal or higher than that of the command's but who so not have an Access Mask will not be able to use the control.
The Access Areas start from 1 to 31. They can all be selected or only those needed by using the selection window. All Access Areas are enabled for default.

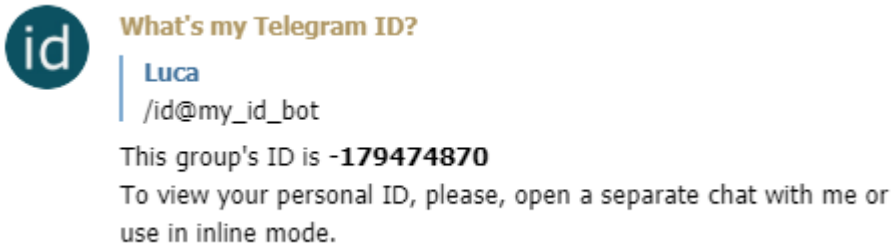
Default Language

This property is used to define the language to be associated to the Group in order to automatically activate the language, if included in the project's Text Table resource, to convert all the project texts and strings to the language desired.
Users who log in without a culture name will automatically be associated the one set for the Group they belong to.
When no language is defined in this property, no text language change will take place.

Telegram Group ChatID

This property identifies the Group ID of the Telegram user group to which the Alarm Dispatcher's Bot has been added.
To get the Group ID simply follow these procedures:

- startup the Telegram app
- define a user group
- add the Alarm Dispatcher Bot to group (use the magnifying glass icon to search for it)
- temporarily add "my_id_bot" user to group (use the magnifying glass icon to search for it)
- digit the "/id@my_id_bot" message in the group chat
- The Group ID to use in Movicon.NExT will show



- at this point you can remove the "my_id_bot" user from the group

When a group user has been defined in theTelegram Chat ID propriety, this user will have priority over the rest.

1.4. User Properties

The User properties are used for managing the user's personal data that is needed for user authentication in order to access project functions and controls which have been activated with the Users management. Apart from the necessary access rights and privileges, user must also have Group membership.
Each user can be configured with the following settings using the properties window:

General Properties

The General properties group are used to defined the main User settings.

User Name

Name of User. The name must be unique to that user on the list and can contain a maximum of 64 characters.

Password

This property is used to set a Password to associate to the User. The characters are hidden for reasons of privacy when entered. The minimum number of characters that can be used in the password can be set in the User Management's General Properties. The maximum number of characters allowed is 64.
All User password data are encrypted in the project therefore the right procedures must be taken to prevent passwords from being forgotten or lost!

Confirm Password

For security reasons, this field requires that the Password set in the above field be entered again and confirmed.

Electronic Signature

The value of this property must be unique in order to identify the user clearly. If inserted, It's value will be recorded in a UserName column row in the relative Trace table (UFUAAuditDataItem). If no value is inserted, the user's name will be inserted in this column instead. Electronic Signature uniqueness is handled by the system. In cases using Windows authentication, whereby no users Movicon.NExt project level are defined, Electronic Signatures are not defined and the user's name complete with dominion is reported in the Username column. To ensure Electronic Signature uniqueness, it is advisable not to have a mixed authentication model: Project User side and Dominion User side.

Language Activation

This property is used to associated a language to the user. If this field is left empty, the language defined in the Group of which the user is a member will be used. Therefore when the user logs in, the project will automatically activate with the language associate to the User in this field.

Execution Properties

The Execution property group allows you to define the settings the rights of a User Access.

Password Expires In Days

The password associated to the user can be set with an expiry time in days for security reasons. When the set time expires so will the validity of the password. Therefore when the user next logs in after their password has expired, they will be requested to enter and renew their password with a different one.
For reasons of regulation compliancy this procedure helps prevent the risk of the password being discovered and used by unknown parties.
The password will not be given an expiry time when this field is set at zero for default.

Force Password Change at First LogOn

When enabled,, this property will oblige the user to change their password with a different one after the first login.
For reasons of regulation compliancy, this procedure prevents the risk of the password being discovered and used by other users and unknown parties when assigned by the Administrator.

Access Level

Access Level

This property is used to define the User's hierarchical access level. This level can be set with a value from 0 to 9999. The value set here will determine the user's level of access. The higher the value the more the user will have access to the project. For example, when a user is set with a level 10, they will be able to access and execute those commands that require user level equal to or lower than 10 (between 1 and 10).
The user can inherit the Level associated to the Group he or she is a member of by entering the -1 value in this field.
In cases where user is authenticated by the operating system's Domain, they will receive the Group's hierarchical level.

Access Area Mask

This property is used to define the user with an access area by means of using a bit mask. Each bit corresponds to an access area which allows the user to interact with those controls which require, in addition to the Access Level, the same Access Area. For example, a control can be set with an Access Level as well as enabled with Area 1. When a user logs on with the same hierarchical level or higher but has not been enabled with Area 1, they will not be able to use the control.
The Access Areas start from 1 to 31 which can be all selected together or individually as required through the Access Area Mask Editor popup window. As with Access Levels, the User can also inherit Access areas of the Group they belong to. This can be done by using the "Inherited" command button at the bottom of the Access mask Editor popup window. New users are created with inherited Access Areas for default.

Notification

The properties in the Notification group are used to define the notification recipient addresses of each user. **These addresses are used for all notifications including those from the Alarm Dispatcher notification services.**

Email

This property is used for defining the User's email address. This address will be used by the Alarm Dispatcher to send the user notifications.

Phone Number

This property is used for defining the user's telephone number. This address will be used by the Alarm Dispatcher to send the user notifications. The number is displayed correctly, including the use of prefixes and national
International as provided by telephone operators.

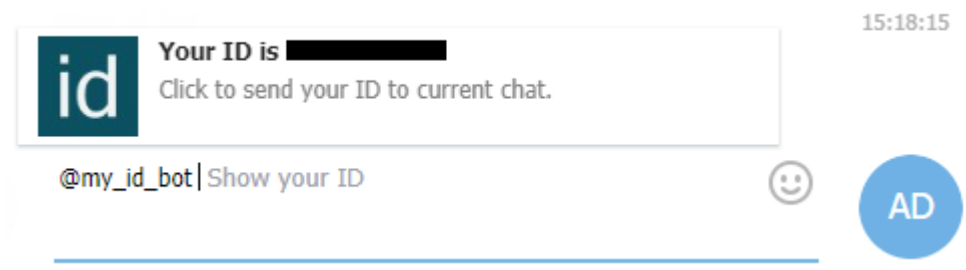
Mobile Phone Number

This property is used for defining the user's mobile phone number. This address will be used by the Alarm Dispatcher to send the user notifications. The number is displayed correctly, including the use of prefixes and national
International as provided by telephone operators.

Telegram Chat ID

This property identifies the Chat ID of the Chat Telegram to which the Bot of the Alarm Dispatcher has been added to.
To retrieve the Chat ID proceed as follows:

- open the Telegram app
- start a chat with the Alarm Dispatcher's Bot (use the magnifier icon to search for it)
- select "Send" to start chat
- digit the "@my_id_bot" message
- the Chat ID to use in Movicon.NExT will show

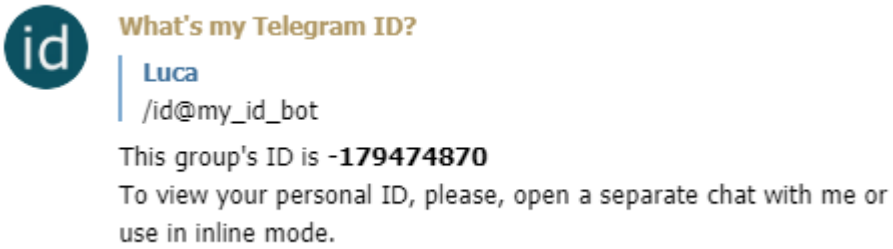


The Telegram Chat ID property, when set, always has priority over the Telegram Group ID property.

Telegram ChatID

This property identifies the Chat ID of the Telegram chat to which the Alarm Dispatcher's Bot has been added.
To recall the Chat ID simply follow these procedures:

- startup the Telegram app
- start a chat with the Alarm Dispatcher's Bot (use the magnifying glass icon to search for it)
- Select the command to start chat
- digit the "@my_id_bot" message
- The Chat ID to use in Movicon.NExT will show



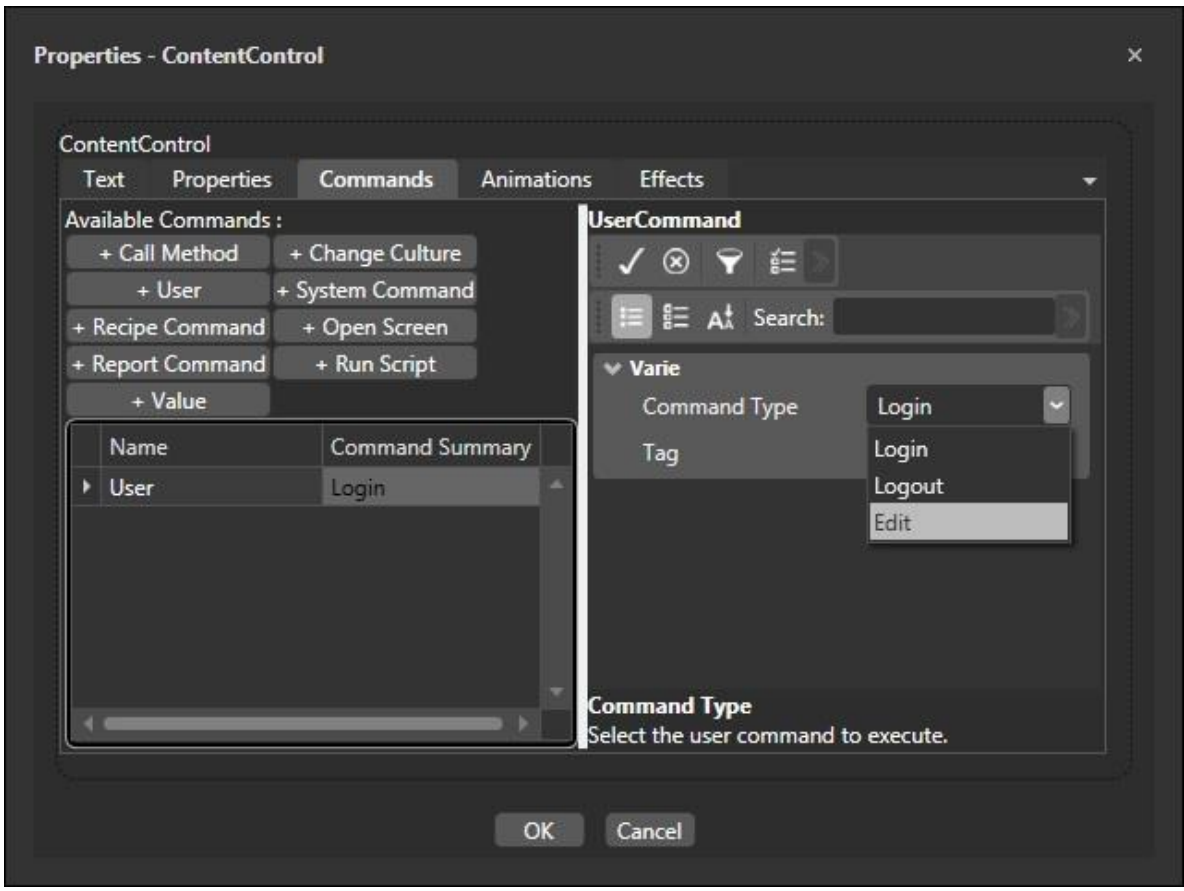
When set, the Telegram Chat ID property always has priority over the Telegram Group ID.

1.5. Runtime User Control Management

To allow those operators who have been given permission to use the Users Management during project runtime the developer must provide controls that can be associated to screen objects. For example, the following functions, that are opertive in runtime, can be associated to a button (or other control objects):

- **User Log In**
- **User Log Out**
- **User Editor**

The developer must decide whether a password should be associated to the commands that activate these functions.
The commands are set by using the normal procedures described in the **Assigning Commands to objects** topic.



This image shows the window used to assign 'User' commands to an object in edit mode.

User Log In Command

This command activates the User Log In request independently from user level. Once user has been authenticated by Logging in successfully, he or she will result active in the project users management.

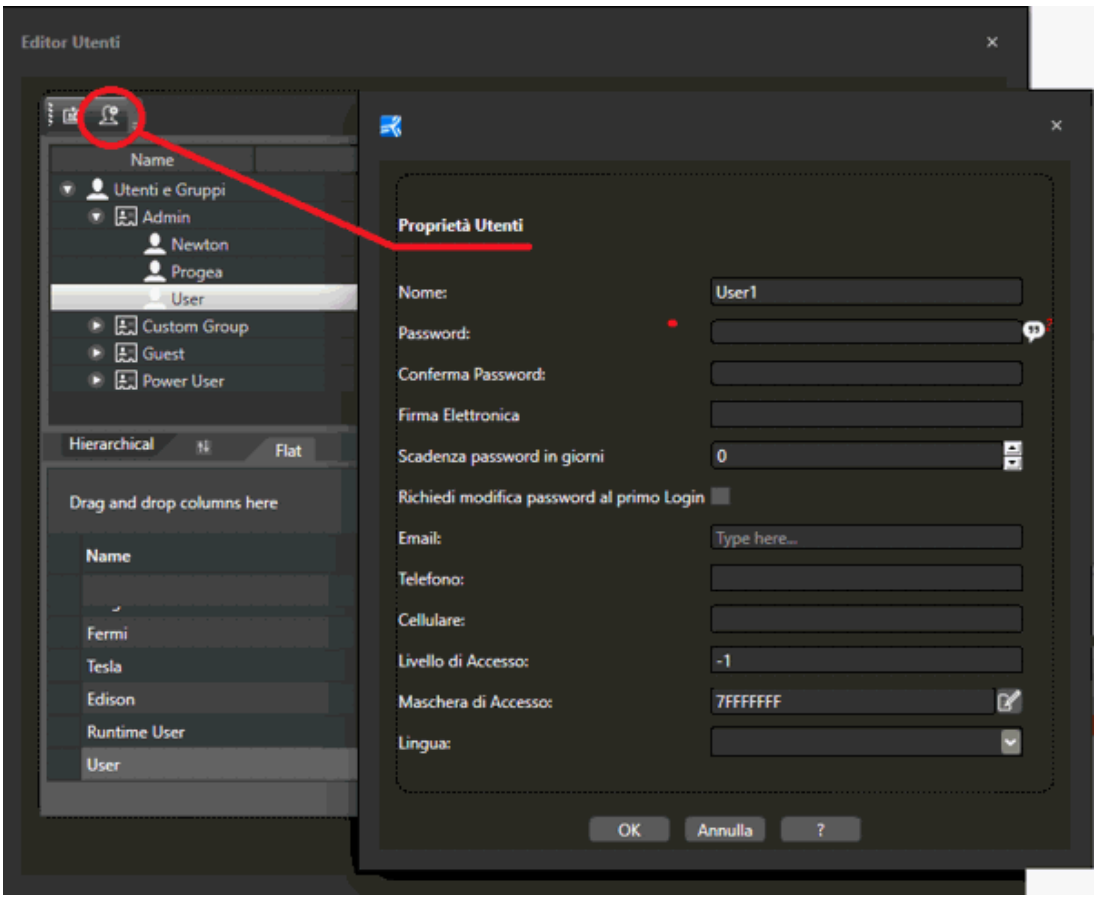
User Log Out Command

This command activates the Log Out procedure for the currently active user. After the user has completed this procedure, he or she will no longer result active.

Runtime User Edit Command

This command activates the window used for inserting users and user groups during runtime. This command opens a window where the Users and User Groups properties can be set.

In order to set the security criteria to request a specific user level for activating the command, you will need to use the User Management properties of the object to which the command is to be associated.



Those operators who have been enabled with the levels needed to insert Users in runtime, can use the window which is displayed for adding new users according to the functional modes and properties described in the User Management section in this topic.

Please take into consideration that Users added in runtime can only have one Access Level that has been preset by the developer in the Users Management property. In addition, users cannot be changed or removed once added. Only new ones can be added.

Note that if the project is started up in runtime with the user editor window open, it will not be possible to open the Users Editor window in runtime.

1.6. Domain User Authentication

When this functionality is enabled, the User Management system will permit access to users registered in the Domain of the Window OS in which the project is run, by using the login procedures. Therefore if the user wishing to access the project is not on the project user list, the user manager will ask the operating system for user authentication by means of using the LDAP protocol with the domain/User' format.

The user who launches Movicon.NExT (as service or as runtime) should belong to the Window Domain managed by the Active Directory (LDAP), otherwise this type of authentication will not function correctly.
When the user is acknowledged, they will then be authenticated by the domain and therefore authorized to manage the project. In this case, the access rights will however be determined by the group the user belongs to.

Once authorized, the user's group membership is then validated and if a match to a project user group is found, the user will be granted access with the same access levels of that group.

The names of standard User Groups created by Windows (as 'Administrators' or 'Users') is NOT supported by the validation procedure. If you wish to use this authentication method, you will need to create new User Groups with custom names, then create the same user groups within the project for setting the access levels.

1.7. General Security Concepts

The Platform.NExT project security management ensures both project developers and users the maximum protection with security system access management that complies to the strict regulations and standards.
The platform's security system has two precise data protection criteria:

1. Project Protection
2. User Authentication and access to controls and data in runtime

Protecting your project

A Platform.NExT project can be protected and encrypted to enable the developer to protect their know-how and prevent project access and modification by unauthorized persons. Project protection in edit mode is totally distinct from the user management to access controls in runtime. For example, a project can be protected and encrypted without activating the users management in runtime.

User and Password Management for Operators

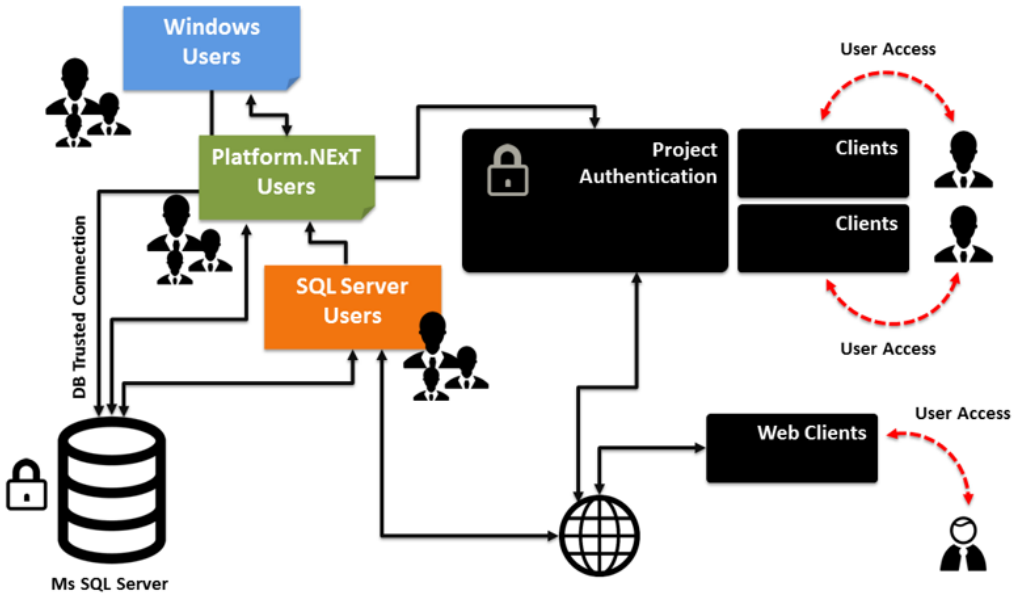
The User and Password management offers the option to manage access to project controls and functions during runtime according to the security standards. The developer can set for all the functions and controls, where necessary, with user authentication request by Logging in according to access level and/or area level.

ATTENTION!! It is important that the developer or administrator adopt ways to remember or retrieve a forgotten password. Once a password has been lost it will impossible to gain access!
If this should ever happen please contact the Progea Help Line.

1.8. Security Management Model

The project security management in Platform.NExT is based on the ASP.NET. Membership Providers model. In addition to ensuring the maximum security policies for managing users, it also offers the use of "providers", so that the security model (data source) is independent from the authentication system.

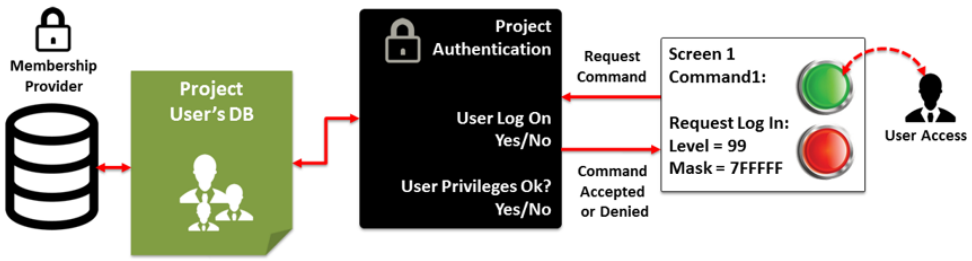
The Membership is an API used to manage users within a NET. application to permit user authentication management. The Membership configuration within the Microsoft .NET ambient is made possible due to the Providers which connect applications to authentication system. By using these Providers, a Platform.NExT project can guarantee the same level of security despite any authentication system customization that might be based on different databases or on authentication systems based on biometrics readers or scanners, RFID (Radio Frequency Identification), Badge or others for instance.



This diagram shows an example of the Platform.NExT default user security and authentication concept

Authentication System

According to the Platform.NExT security model **when the User and Password Management is enabled** each sensitive project control or function might require user authentication and access level verification in order to grant users permission to use them. This usually happens the Client side where command executions, data modifications such as set-points, entry-points, recipes or other require interaction with the user interface. However the security management may also be provided on the Server Side to accept or deny data modifications or variations.



This is an example of command access protection and the authentication and permission process

In whatever case, the project commands and functions may nevertheless be subject to user access level and privilege verification after the user has been authenticated.
In addition to enabling the Users Management, this also requires that users be entered either in edit or runtime mode to enable them to activate commands according to their hierarchical level.

Therefore there is a project user profile/credentials that is/are automatically mapped to the SQL Server database which used the Membership Provider for user authentication. when enable the platform's authentication system requires that:

1. the "Users Manager" properties be assigned to all graphical objects and functions to be protected by establishing User access level and area.
2. the User profiles have been entered with the relative User Level property (hierarchy level) and access area.
3. the Membership Provider has been configured correctly. The system is configured with the Microsoft SQL Server Provider for default.

Assigning command access criteria

Assigning the access policies to the project's functions is generally done on the **Client** side in control objects or functions managed in screens. For example, a "Start" button may set with a certain user level in its properties. This can be done for any object, symbol or function that is used for command executions.
However, security policies can also be defined on the **Server**, and inherited by each associated object hierarchically.
For example, a Tag in the Server can be set with an access level so that every time its value is changed by a user from elsewhere, the user will be asked for User authentication beforehand.

It is the job of the programmer to establish where the user authentication is to be associated. Normally such procedures are established on the Client side but it would be very convenient to use these procedures to protect Server data in distributed or more complex architectures.

Independently from where the security policy is used, it must be set in the interested object's properties which are those grouped under **"User Management"** if object is on the Client side or under **"Access Level"** if on Server side.
Therefore please refer to relevant topics describing the use of these properties.

User Privileges

In addition to user authentication, managed with Memberships, each user can be set with specific privileges by means of using their properties.
The settings of the user privileges are bases on the following criteria:

Level

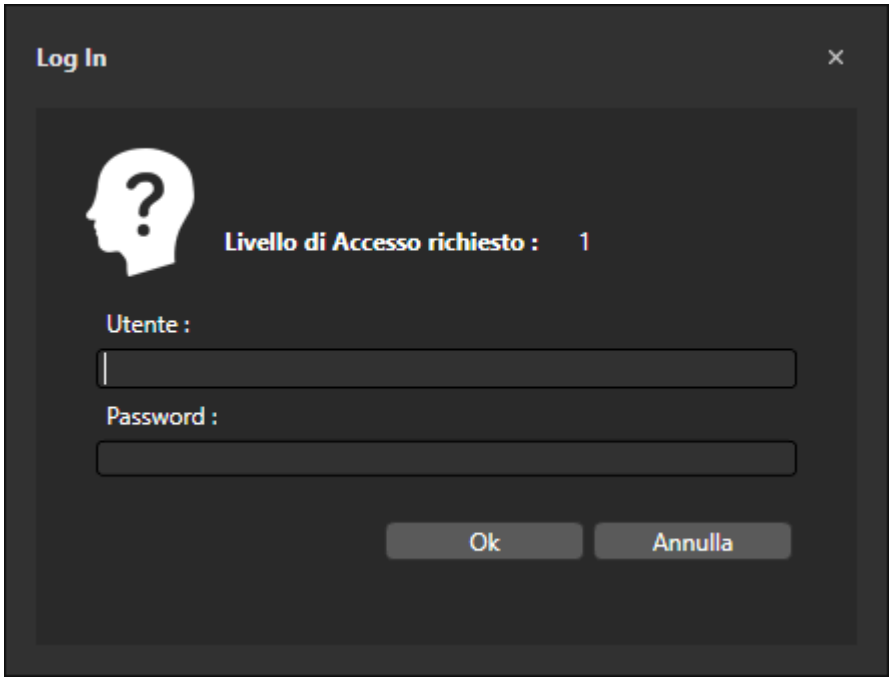
This is a hierarchical level which is defined by using a value to establish the user's level of access. The lowest level value indicates that the user has the least privileges. Access to the control will then be accepted if the level requested is equal to or higher.

Access Mask

In addition to the hierarchial level, users can also be assigned an "Access Mask" that represents the area of access to the operations. The Access Mask has a selection of up to 31 areas (Select all, some or none). Therefore controls can be conditioned in Read or Write by one or more areas for which the User, who Logs ON, must not only have a hierarchical level equal or higher than the one requested but also access to an area where the control can be used.
Users are enable with the areas for default.

User Log On

The system will ask users to Log On wherever data has been protected with user authentication. The window below shows when user log on is needed. All successful Log Ons are recorded.



This image above shows the user authentication window for logging on. It is displayed by the system when the user attempts an operation that requires a certain user level and therefore user authentication. When the user logs on with a user level equal to or higher than the one requested by the system, he or she will be granted access.

The system traces all user Log On/Off dates and times in the System Log.

The following topic describe all the User and User Group properties and functions.

1.9. Membership Provider

The Platform.NExT security model is based on Membership Providers to ensure maximum security and independency from the type of authentication desired. By using Membership Providers, you will be able to customize the type of authentication system management you prefer best.
Platform.NExT uses Microsoft Membership Provider based on the SQL Server for default in total automatic and safety. The user can use the security provider with compete transparency as the SQL Server Express 2012 instance is automatically installed while installing Platform.NExt if the SQL Server to connect to is not already installed. The "Movicon.Membership" database is created in the SQL Server Express 2012 instance along with tables to manage project users.

One of the advantages of using Providers is the possibility to share with other Clients, whether local or remote (e.g. Movicon.NExT Clients or Web Clients).
In addition, the Provider can be changed and configured in the application's settings to allow the use of authentication systems other than the one used for default based on SQL Server.

Membership Provider Customization

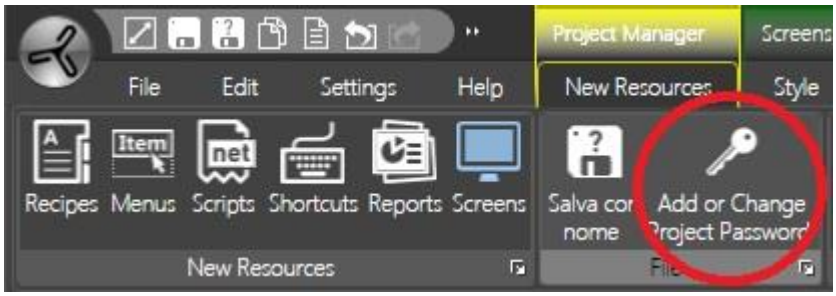
Whenever needed, the expert design engineer can change the Membership Provider they are using by replacing the Microsoft SQL Server provider with the one desired.
To setup a new Provider, you will need to modify the application's XML configuration file with the .config extension (Movicon.NExT.exe as Client or PlatformNExTIOServer.exe as Server).
In this file you will need to set the name of the Provider desired and the connection string data and parameters
In order to configure the desired Provider correctly, please refer to its documentation or, if necessary, contact Technical Support for further information.

2. Protect and encrypt the project

2.1. Project security

The Platform NExT development environment provides the developer a functionality that will enable them to protect their project against modifications by unauthorized users.
This functionality has been implemented using security password that must be entered and activated in the project using the appropriate Project Manager's taskbar ribbon.
After having activated the protection, the project will be protected and encrypted to prevent any unauthorized access to the project in edit mode. The developer will then be the only one to allowed access to the project in edit mode in order to protect the project from being modified by third parties.

ATTENTION!! It is important that the developer or administrator adopt ways to remember or retrieve a forgotten password. Once a password has been lost it will be impossible to gain access!
If this should ever happen please contact the Progea Help Line.



To activate the project's protection simply use the "Add or change Project Password" ribbon. This will display a window through which the desired password can be entered and confirmed. After the password has been confirmed, the project will be protected and encrypted. The password must be used when you next want to access the project in edit mode.

Project password and encryption is disabled when the project is saved to the database. Saving a a protected project from a file to the Database requires that the protection be disabled before it can be saved.

When enabling the project security all the adhering files will be automatically encrypted and only accessible by using the password set in development mode.

Project security is not bound to user management activation and therefore the project can be protected without it having users.

3. CFR21 Part 11

3.1. General Concepts

CFR21 Part 11 General Concepts

The scope of the CFR21 Part 11 regulations issued by the Food & Drag Administration (FDA), is to obtain the legal equivalence of electronic documents (digital records and electronic signatures) to that of paper records and handwritten signatures executed on paper. This is due to the increasingly frequent use of automatic systems in managing production process systems subjected to FDA federal agency approval and revision. In order for the automation and control system to be in conformity with the CCFR21 Part 11 norm. it is necessary that recorded data are traced back to the responsible operator (Electronic Signatures). Furthermore, specific precautions must be taken to prevent falsifications or tampering of data recorded electronically, or that allow easy identification in cases of inappropriate use whether intentional or accidental.
Many pharmaceutical companies wish to take advantage of the benefits derived from the use of electronic signatures. It is astonishing how much paper, that has to be stored, accumulates over the years. In addition, the use of electronic records significantly reduces the time needed to retrieve and revise these documents before releasing medicine for sale on the market.
These companies should apply for equipment that have the necessary mechanisms to protect against accidental or malicious modification of data in electronic format.

General concepts for supporting this regulation

The following concepts relating to the 21 CFR Part 11 regulation define how it would be advantageous to use Movicon.NEXT to develop FDA CFR Part 11-ready projects.
The basic concepts, formed by Progea, have been listed below to give better clarity on the understanding that the user takes full responsibility to ensure that their application developed with Movicon.NEXT conforms with the relevant requirements.

Please remember that the hardware-software application is always to be validated in its entirety and not each individual product or component. It is the user's responsibility to create projects to conform to the 21 CFR Part 11 regulation.

Management to Trace Variable Modifications

Tracing variable modifications will be managed by Movicon.NExT using the Historian (historicals and data logger prototypes), therefore you must make sure the relevant option is activated on the license.
If this option is not activated you will still have use of the Audit interface's functions without being able to execute any traces.

Different properties will be involved in order to manage the Audit Trace of variable modifications. For further information please click the link relating to the topic of interest:

Objects
Data validation is performed using the 'Validatore Audit' control object from the Movicon. NExT toolbox.
The Data Source to be verified can be specified in the control's properties.

- Audit Trail Validator

Users and Passwords
All the application commands that can be executed by operators to interact on the process must be protected by passwords.
The password management must be enabled in the project's User Password resource's General Properties.

- Electronic Signature
- Name (ID) and Password
- Enable Password Management
- Password Expires in Days
- Force password change after first Login
- Minimum Password length
- Auto LogOut timeout

Tag
Movicon.NExT offers the possibility to trace all status variations and those of each variable value with significant relevance or that influence the production process. For example, an appropriate system to trace all significant process variables, such as set-points or process commands) should be ensured by using what is now as an Audit. Movicon.NExT offers an Audit property group to allow users to define how the Audit is to be managed for each individual variable concerned.

- Max Audit Age
- Access Level Required to Confirm
- Enter Comment On Audit
- Enable Audit Trace
- Force Password On Audit

Server
The audit-trail's role is to record all activities performed on variables by users during runtime. The recording of these activities is enabled by simply selecting the 'Enable Audit Trace' option in the variable properties. To validate a data set record in the database to ensure that it does not get altered externally, you will need to enable the 'Enable Data Protection' property found in the I/O Data Server's 'Settings' section. When this property is enabled, the I/O Server will startup with a certain user that is created by the Movicon Setup. This user, whose name for default is "NExT_IO_Server", and their password will be encrypted and will be used by the system to manage recordings in the Database. It is also the only user that can validate data by using by the "Validatore Audit Trail" object from the ToolBox.
- Default Audit Trace Connection
- Enable Data Protection in File

In certain procedures you will need to pay attention to the user with whom the Movicon.NExT I/O server is started up with. These procedures are:

- when deliberately changing the user in the Movicon.NExT server's 'Service Control Panel'.
- when installing the Movicon.NExT server's service using the 'Service Control Panel' before enabling the data protection option.
- when setting databases with a default connection string within which the authentication of a certain user is forced.

Historian

- Enable Data File Protection

Setting the database with a custom connection string (DB Connection String property) and specifying a certain user to access the DB will prevent data from being validated.

Datalogger

- Enable Data File Protection

Setting the database with a custom connection string (DB Connection String) and specifying a certain user to access the database will prevent data from being validated.

The document concerning the CFR21 Part 11 norm is downloadable from the Progea website.

3.2. Security

To ensure project security please take the following points into account:

- The Movicon.NExT project must be encrypted so that all the configurations and passwords used in the project cannot be accessed from the outside.
- Movicon.NExT ensures the uniqueness of user passwords inserted in the project. Each user is identified in the project by their UserID, Password, Description or unique printable Name (Electronic Signature).
- The Movicon.NExT server side must be executed as Windows OS Service. By doing this access to the operating system and the recorded records will require identification of users registered in the project according to the security requisites required by the norm.
- Movicon.NExT supports shared Windows operation system domain in order to utilise user passwords defined by the system administrator.
- Users who manage data recordings using Data Loggers must adopt the appropriate measures to prevent unauthorized access to registered databases to avoid any possible tampering or undesired modification of their contents. When using ODBC storage, use secure databases such as the Microsoft SQL Server and administer the correct Windows OS security procedures permitting access to records to system administrators or developers only.

- To restrict access to the developed application's functions and controls, the Movicon.NExT project must use User Password Profiles management correctly by entering the Password, UserID, User Name and Access Level. Movicon.NExT provides 1024 access levels and 32 areas.
- Users must have passwords that can be managed with top security. The insertion of new users by the administrator can result in the subsequent password re-entry by the user when they next Log On.
- All the passwords can be set with expiry times to make users re-enter their password periodically to contribute towards increasing security.
- To correspond correctly to the norms, the Auto LogOff function (enabled access timeout) must be used correctly in the Movicon password management to avoid unauthorized access to the system after a period of user inactivity.
- To ensure correct and valid data entries, users must make sure that the Movicon.NExT operating stations are allocated in safe workstations that are only accessible by authorized personnel.
- The use of the Movicon.NExt Auto LogOff function is compulsory in systems that are in continuous use.
- Movicon.NExT adopts tools and procedures that the Windows OS uses to discourage the continuation of unauthorized access attempts as required by the norm. After the forth failed attempt to Logon, Movicon.NExT will delay response time needed to re-enter the password to discourage attackers.
- System violation attempts. In the event of a fifth unauthorized LogOn attempt, Movicon.NExT will visualize and record the event in the Historical Log in order to control any further attempts of force entry into the system.

Miscellaneous

- All data must be stored in a relational database that meets the security requirements (eg. Encrypted IMDB or ODBC with protected access against tampering and unauthorized data access by also using the security functions of the Windows OS). Data must be stored in a filing system for an adequate period of time according to operation needs.
- To safeguard data of the project, images and recipes even further, the user should use third party software products that can ensure version maintenance (for example, Microsoft Source Safe can be sued to control versions).

Electronic Signature

The Control Systems must be capable of acquiring the status and behaviour of the process's variables in real time. The date and the product batch number must be entered along with the electronic signature of the operator and an eventual signature of approval from the process manager in the section relating to the product batch's working period. These procedures must be carried out without the threat of causing errors and that signatures are always unique and referable to their owners. The records must be filed in a save place and stored for an adequate time period. They must also be protected against unauthorized access.

Security

Security in systems subjected to validation is absolutely essential. There are two cases in which data is recorded in electronic format.

1. Handwritten Signature: when data is printed and signed for approval (the so called Hybrid solution: paper and electronic). In this case the file is to be considered an electronic record. Adequate measures must be implemented to ensure that the file and its data contents are not substituted or modified before being printed, identified, dated and signed. When signed manually, it may not be necessary to use electronic

signatures. Therefore, certain conditions must be setup to impede unauthorized manipulation of the data format and that such data is uniquely and automatically associated to a specific production batch or line. Furthermore, the original data file must be archived. It must also be stressed that a handwritten signature does not necessarily legitimize an electronic record inadequately protected.

2. Electronic Signatures: in this case everything is digital and all records are filed and stored in electronic format. In addition to ensuring that the file and its data contents cannot be substituted or modified, it must be also approved with an electronic signature. The data file should include information on the production batch it refers to and the name of the person who approved this data, being the person registered as logged on when data approval took place. All the file's original contents should then be protected from any unauthorized modification and manipulation.

Electronic Signature

The electronic signature can be created with a combination of at least two items such as an ID code and a password or a badge and a password etc., as required by the CFR21 part 11. The User ID and Password must be guaranteed that it is unique to that person with absolute certainty of identifying them. The ID code can be made public, meaning that it can be shown on screen. Since the password may not always be guaranteed as being unique to just one person, it is absolutely necessary that the ID code be original and personal to each user. These rules should be followed:

- A set minimum password length
- Change password periodically
- Carry out procedures to avoid any attempts of meddling or unauthorized access
- Record any attempts of unauthorized access
- The system administrator must not know the password of other users even when assisting them when they have forgotten their password.
- User Groups can share the same password only for reading data where the electronic signature is not required.

3.3. Validation and Documentation

The system used to validate data submitted to the Audit Trail is based on a maximum security model that involves the use of encrypted system users and SQL Server Transaction Log verification. All data submitted to the Audit Trail are recorded according to univocal security criteria and can be validated by means of using graphical objects, called "Validatore Audit Trail" available from the Movicon.NExT toolbox, that are used to view and timestamp data.
In order to get positive results, the validation process examines historical data to identify any tampering performed externally with Movicon. Each unauthorized variation will inevitably be detected by the Transaction Log analysis along with any user who is not a Movicon encrypted user ("NExT_IO_Server" user) but is responsible for performing the operations.

Please take the following points into account when dealing with the necessary validation and documentation concepts:

- Some of the CFR21 Part 11 regulation requirements demand activities and measures that are not based on the software application. To meet these demands required by the Part 11 standard, the customer must validate their application to ensure data recording accuracy, reliability and security in addition

to its capacity to prevent the mishandling, errors and cancellation of data. Movicon.NExT users should validate applications developed in accordance with the FDA regulation standards. Users can develop and/or run their own validation programs or protocols or delegate this process to other entities. The validation process should follow a methodology established according to the system's life cycle (SLC).

- In order to meet the control procedures required to obtain conformity with the CFR21 Part 11 regulations, the customer must adopt adequate procedures to verify the identification of the individual assigned an electronic signature.
- The customer must establish in writing and put into practice the procedures to give specific operators specific responsibility for executing operations assigned to them according to their electronic signature to further impede falsifications or mishandling of their signatures or user registration in accordance with the CFR21 Part 11 regulations.
- The customer must verify the true identity of the individual to whom they wish to assign an electronic signature. In addition, the customer is required to certify in writing to the Federal Agency (FDA) that they intend to use the electronic signature as and equivalent substitute for tradition paper documents and, if necessary, produce the required documentation as requested by the agency,
- The customer is responsible for producing documentation on system use or the application they have developed and details of the produced documentation's updates and distribution as well as personnel training. However, the customer is not responsible for any documentation of the platform being used (Movicon, Windows).
- When producing 'guaranteed' documentation, the customer must use the timestamp viewer tools provided by the Movicon.NExT platform which can validate and guarantee the veracity of recorded historical data as appropriately predisposed in the project properties.

Audit-Trail

The audit-trail records all operations carried out by users on process variables during runtime. The audit-trail is enabled to record by simply selecting the 'Enable Audit Trail' option found in each variable's Audit properties.

The 'Enable Data Protection' property, found in the I/O Data Server settings, protects both historical and Audit data so that they can be validated using the Audit Trail Validator object from the ToolBox.

When enabling this option, the ServerIO will startup with the “NExT_IO_Server” user created in the Movicon SetUp phase. This user, whose password is encrypted, will be used by the system to manage records on the DataBase and will be the only user permitted to valide data with the above mentioned object.

Below are listed some of the main columns or items that can be displayed within the "Audit Trail Validator" and "Historian Viewer" to keep track of eventual modifications to variables:

- **Name**: indicates variable name.
- **Description**: this is the description associated to the variable using the Tag's 'Description' property.
- **Value**: indicates the Tag's value after being changed.
- **ValueBefore**: indicates the tag's value before being changed.
- **Status:** indicates the Tag's quality.
- **RecordDateTime:** indicates the date and time of the event.
- **UserName**: indicates the name of the user who generated the event.
- **Reason**: Comment entered by the user while making change (This requires that the 'Force Comment On Audit' property be enabled beforehand).

Validating Data

Validating data is done by using the ' 'Audit Trial Validator' object from the Movicon.NExT toolbox.

Data validation in Movicon.NExT is essentially based on the SQL Server's Transaction Log. Basically, the logs of protected databases are monitored to see if any record sets have been modified by unauthorized users who are not registered with the Movicon.NExT I/O Server ("NExT_IO_Server" user).

When the project is started up for the first time, the first database backup is performed automatically after the first data recording in the SQL Server database has been executed (SQL Server installation backup folder). This first backup is **fundamental** for subsequent data validations. If this first backup is removed or deleted, it will not possible to validate data within the database. In addition, the validation of data in the Transaction Log is not based on the actual validation user's name (default "NExT_IO_Server"), but on their SID (the user's security ID). If the validation user (default "NExT_IO_Server") is eliminated by the operating system and then reinstated, their SID will change and therefore it will not be possible to validate data recorded with the previous user.

Time Stamp (date and time) Management

- The Time Stamp is managed by Movicon.NExT using the Windows operating system clock for both date and local time which is Universal Time Coordinated (UTC).
- In order to get the right time, the user should set the operating system to synchronize with the metrological servers that refer to the Network Time Protocol (NTP), or synchronize the client system date and time with the Server's for data recording consistency. These synchronizations can be managed directly using the Windows 7, Windows 8 and Windows 10 operating system functions or by using Basic Script code to synchronize the project times.

Validation User (NExT_IO_Server)

The encrypted and unique validation user ("NExT_IO_Server"), which is essential for the validation of Audit Trail data, is added to the operating system during the **Movicon Setup** phase. This user will be added as local user to the machine with the name of "NExT_IO_Server" when executing a Standard Setup. When executing a Custom Setup, a different user name can be specified or a Domain user can be created/selected if the PC belongs to a Domain.

The Domain user can only be created by accessing with a Domain user who has the necessary credentials for executing this operation.

The validation user ("NExT_IO_Server") will also be added to those of the SQL Server and added to the list of users authorized to start the Windows services.

If the validation user (default "NExT_IO_Server") is added as domain user, the Movicon client application should also be started up with a domain user that has the right credentials to retrieve the validation user's information (default "NExT_IO_Server").

When the Movicon.NExT I/O DataServer is run as service, the validation user (default "NExT_IO_Server") should be the same one with which the

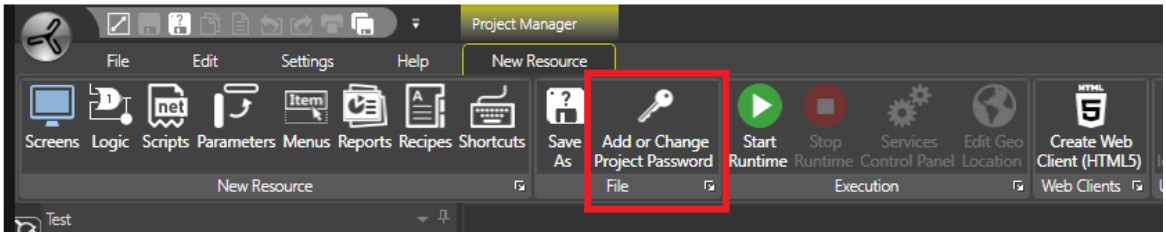
service was started up, unless the user is deliberately changed in the 'Services Control Panel' or the service is installed before enabling one of the data protection options.

3.4. CFR21 part 11 configuration

To get a Movicon.NExT project 21CFR Part 11 ready, you will need to configure it appropriately so that it is compactable with the FDA validation criteria. The necessary measures to take in doing this are indicated below:

Project Security

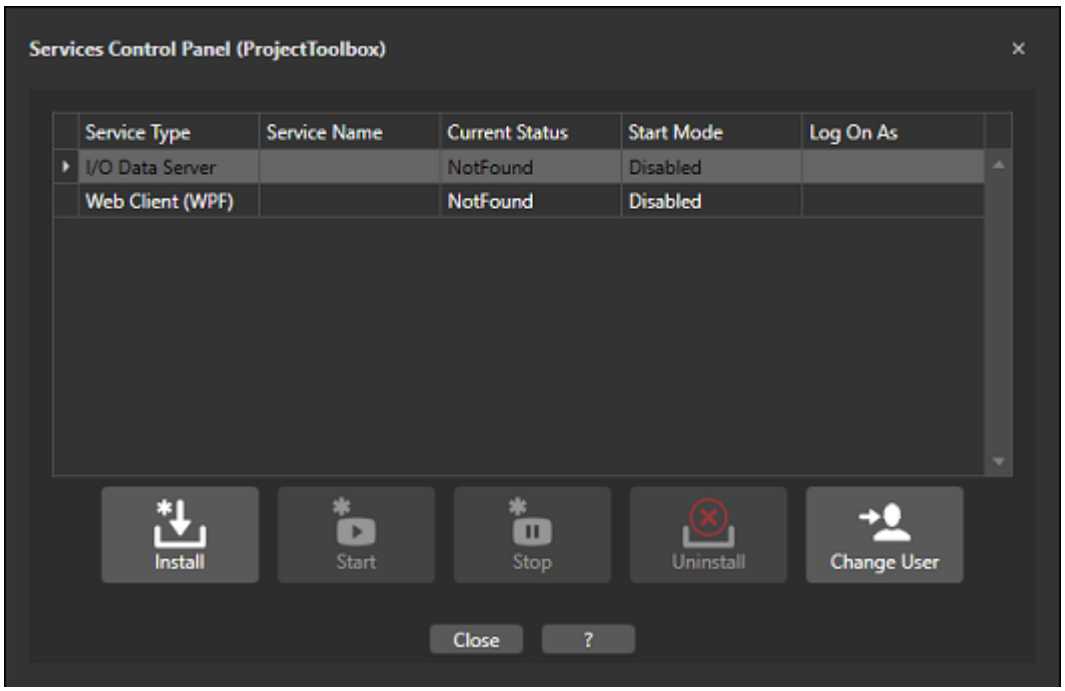
The project must be configured in its General Properties by selecting Project Password and setting a protection password. In this case, the project access in design mode will be protected and all the project's XML will be encrypted and inaccessible due to a proprietary algorithm.



Confirming this operation will save all the Movicon.NExT project files with encryption and protection when the project is next opened. It is important to remember that projects protected with passwords can be executed in runtime but cannot be modified or accessed in design mode without using a password to gain access.

System Startup

- When turning on the PC, the Windows operating system will startup together with the Movicon.NExT platform by automatically launching the project. For security purposes, these operations should be configured appropriately to ensure that the project is started up safely in protection mode.
- At Windows startup, all the Movicon.NExT project Server components should be run automatically using the Windows Services' functions. The Movicon.NExT project should therefore provide Services management using a control panel that can be accessed from the Movicon.NExT Editor. This Editor is used to install the Server parts (such as the I/O Server, Schedulers, Recipes and other) as Windows Services. In this way, they will all be run automatically when starting up the operating system independently from the Windows User Log On.



The Services Control Panel accessed by means of the Movicon.NExT Editor

- The Windows' user interface can only be accessed when Windows user has been authenticated. As a consequence, the Movicon.NExT user interface, known as the Client, will only be available after the Windows' User has Logged on successfully. There are several options to use for doing this:

    - Windows startup in normal mode by means of Windows user log on. The desktop interface will not be available until a Windows user has logged on. After a user has logged on with Windows, the startup applications can be run and then a command line can be executed to startup the Movicon.NExT Client. The Movicon.NExT Client project will then manage security and the project user management as well as consenting access to the Windows Desktop.
    - The Windows startup can be put into operation by setting the operating system to automatically log on a Windows user for default by means of using the operating system's startup command string. In this case, Windows will startup with an enabled 'standard' user, and as a consequence so will the Movicon.NExT Client startup automatically. The Movicon.NExT Client project will then manage the security and project users management as well as consent access to the Windows Desktop.
    - • The Windows and Movicon.NExT user management can be shared. Movicon.NExT permits shared Windows User Domain, and as a consequence the Windows user Log On will permit Windows authentication and the startup of the Movicon.NExT Client project. In this case, the Movicon.NExT project users will be shared with those of the Windows operating system domain.
    - Windows can also startup without the Desktop (including the resource explorer and management), and therefore by starting up the Movicon.NExT Client only by impeding any access to the Windows Desktop.

- In any case, access to the Windows desktop or its exclusion, and the configuration of Windows user privileges does not depend on Movicon.NExT, and must be managed by the system administrator.

Access to the Windows user interface (Desktop)

While in operation, therefore after the startup of Windows and the Movicon.NExT project application, it is important to manage the operating system's functions that consent access to the desktop from the application in the right way.
According to which mode the operating system was started up in, the user has the option to manage controlled Desktop access by means of the access level settings associable to the project user passwords.

- When the Movicon.NExT user interface (Client) is running, unauthorized access to the Windows user interface (Desktop) can be blocked by eliciting Movicon.NExT user authentication request for users with Desktop access privileges. User role requests can be assigned to users with Desktop access by means of using the Movicon.NExT General User Management properties.
- The operation system can also be configured to exclude the Windows Desktop in order to use the Movicon.NExT user interface functions only. This configuration must be done by a system administrator.

Passwords

All the application commands that can be executed by operators to interact on the process must be protected by passwords.
The password management must be enabled in the project's User Password resource's General Properties.

- Enable Password Management: the passwords will be activated according to the levels and access modalities to the preset commands.
- Auto Logoff: determines the time (sec.) for automatically deactivating the active user after a period of inactivity.
- Minimum Password length: sets the minimum password length allowed (4 characters for default).
- Electronic Signature Definition: the unique user Description of the user whose name is to be used as an Electronic Signature will be managed.

Movicon.NExT will automatically control correct authentications, the uniqueness of the Electronic Signatures and any attempts to force User Log On. Any further Log on attempts made after the fifth one fails, will be recorded in the Event Log and the response time will deliberately take longer to discourage further attempts.

The number of login attempts can be set in the Membership section found in the "MoviconNExT.exe.config" system file as shown below.

```
<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>
```

Each user or user group, who have access to commands or process interaction, must be inserted and configured in the project appropriately.
Users are inserted in the project's User Password Resource where they can be configured in their properties. These properties include those which conform to the FDA regulatory requirements:

- Name (ID) and Password. These are assigned to the user and are used for identification by the system.
- This is a unique text which corresponds to the user's electronic signature and is recorded as absolute user identification (the Electronic Signature management must be enabled in the User Password Resource)
- Auto Log Off: user disactivation time to be used after a period of inactivity.
- Expiring Password: The act stipulates that the user password expires after a certain preset time so that the user is obliged to change it periodically to increase system security.
- Change Password after first login: the normative requires that user be made to change their password once Logging in to prevent the administrator who inserted the original password from knowing it and thus contributing more to identification certainty.

It is a good rule of the thumb to encourage strong passwords to increase security by using a mix of letters, number and special characters.
The use of numbers and special characters in passwords can be forced by modifying the "MoviconNExT.exe.config" system file by introducing the "minRequiredNonalphanumericCharacters" variable.
The value inserted in this property will be the minimum number of non-alphanumeric characters required in a 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>
```

Comments on Alarm Acknowledgements (Audit Trail)

In many cases, before the operator is allowed to acknowledge an alarm, they may be required to make a comment, which will then be recorded in the historical together with the alarm ACK event.
Movicon.NExT provides a function where a severity level for each individual alarm is specified and in addition to which the Movicon.NExT Alarm window will ask the user to enter a comment on the acknowledgement operation.
Therefore, it will be necessary to define the alarm's severity level and threshold level that once reached will ask the operator user to enter a comment on the operation performed.

1. A severity level must be defined in the properties of each alarm.

2. The priority threshold level must be defined the Alarm Window properties that once exceeded will force the operator to enter a comment on the acknowledgement operation for Auditing purposes.

   Comments will be recorded in the Events log with the acknowledgement operation. An User Access Level can also be set for executing operations in alarms.

Data Storage Security and Validity

Protecting the storage of recorded data against manipulation of Electronic Records is absolutely essential to obtain validation and conformity with the CFR21 regulations and their application.

Data recorded by Movicon.NExT (Audit, Historian, Data Loggers) are physically created with database file archives. In order to ensure an effective data validation system, Movicon requires the use of the Microsoft SQL Server as a database for recording data. Projects can use other types of databases for storing data but if you need to have a FDA CFR21 Part 11 compliant, the Movicon.NExT stored data integrity validation system is based on secure control mechanisms that the require the exclusive use of the Microsoft SQL Server. It is therefore absolutely crucial that you comply with the system configurations and project design constraints described in the product documentation.

Succinctly, Movicon.NExT validation system provides a mechanism to record data on databases using a data uniqueness criterion based on the encrypted Movicon.NExT User system and specific controls from the SQL Server system's Transaction Log. Therefore, Movicon will record data using a unique and encrypted Windows System User in association with the database's Transaction Log to control and detect any undesired manipulations.

This pre-validated database containing information on the process and each Logged transaction will safeguard stored files submitted for validation from any undesired manipulation or modification.

This ensures that the file is analyzed in its original form and validated through a Viewer designed to detect and alert any manipulation to data upon which validation of such file will be withheld.

In addition to the above mentioned content, it is the responsibility of the user to implement the necessary data security and integrity criteria by configuring the database with the most adequate data access protection and retention systems that can ensure data availability for an appropriate period of time with reliable redundancy and backup systems as stipulated by the regulations.

Electronic Records

By Electronic Records we mean all production process information (data, values, events) electronically recorded in archives that ensure data integrity and protection against undesired manipulation.

All the information that Movicon.NExT records in database archives can be defined as 'Electronic Records'.

In order for the Movicon.NExT Electronic Records to be compliant with the regulations, you will need to follow the indications and guide lines contained in this document and in the user manual to ensure data integrity and security and prevent unauthorized data access or manipulation.

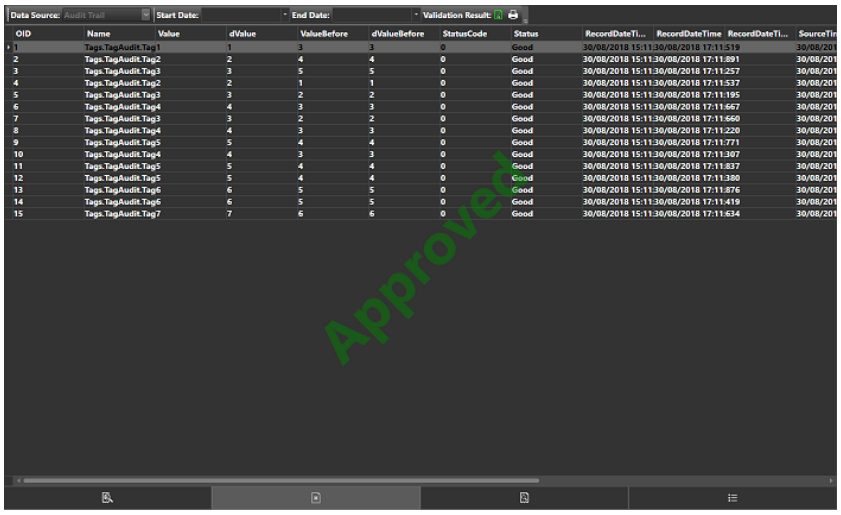
Data recorded on the SQL Server database within the constraints of project design and application and with the relative intrinsic security criteria, are submittable for validation and authentication in order to ensure the originality of data and therefore to impede any type of unwanted manipulation.

Movicon.NExT manages a recorded data validation system that can be activated by means of using the historical data management property settings configuration. This is

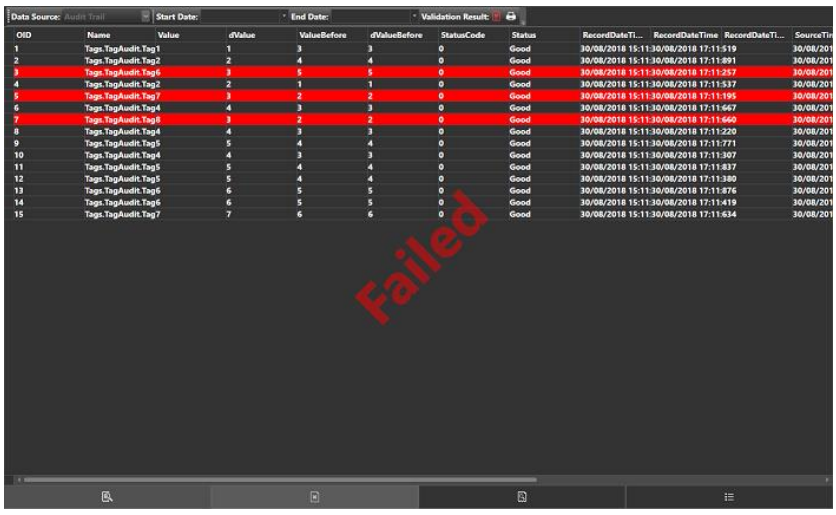
done by checking the Enable Event Data Protection property in the Database Settings properties of the recording engines managed by the Movicon.NExT Server.
When enabling this function, Movicon.NExT will use an encrypted System User ID and Transaction Log combination to ensure the integrity of each individual data recorded (records) on DB.
Aided by this control, Movicon.NExT can ensure users that the data recorded is genuine and impede any possible manipulation to alter or cancel the data.

Each historical data storage system can therefore be subjected to validation controls in Movicon.NExT, to confirm data authenticity or detect any data tampering.

Users operating in systems subjected to CFR21 validation, will be able to ensure data authenticity by implementing it where needed using data protection management or data visualization or print validation checks.
When enabling the data protection management, it will be impossible for anyone to tamper with historical data recorded by Movicon.NExT as validation checks are run to validate data authenticity or highlight any alterations due to unauthorized tampering.



This screen shot shows Historical database subjected to validation with positive results. Instead, the screen shot below shows the same check on a tampered and unauthentic historical database.



Data Retention

Historical data must be made available in storage for an adequate period of time according to the process managed. The period of time can be defined as needed in the Movicon.NExT recording engine and independently from the time of databased being used. Object properties, in effect, allow the number of days (e.g. 730 days can be set to cover 2 years) for which the application will ensure data availability. Once this period has been reached, the oldest data will be overwritten by the most recent to ensure that data is retained for availability for the period of time desired.

Data backup can be manages as desired in the project using the script functions to manage the data sources and destination backup files, or third party backup tools can also be used instead.

Redundancy

Movicon.NExT totally supports the multi-server redundancy function, not just for archive synchronization but also for any operating functionality automatically and transparently. The Redundancy function should be applied and managed in a way that complies to the regulations and in function with the process type.

The Redundancy function allows Movicon.NExT to synchronize the historical archives in a number of servers to ensure both maximum data and operation reliability.

External Security for DB archives

By means of using the Movicon.NExT Server functions, process data are recorded on the configured database.

These data therefore physically reside in files and tables that can be recorded locally on hard disk or in mass archives that physically reside in several servers, or in the Cloud. With the aid of safe relational databases, such as the SQL Server, Movicon.NExT uses protected connections (accounts) for accessing files. It is the responsibility of the user to configure the system so that no one can access files, by removing access rights to files both in the actual database and in the access privileges to folders by the operating system (Movicon.NExT run as service).

It is necessary to ensure data security by using this procedure:

- Movicon.NExT supports any type of relational database for storing data. However, to ensure that the right validation mechanisms are used, you must use the Ms SQL Server.
- To avoid unauthorized access to files, User Account protection will need to be setup by using the access criteria explicitly for system administrators or program designers only (eg. With the same project protection password). This will impede access to data tables where authorization has not been provided.
- Use the operating system's access lock (Locked by Movicon.NExT) or access rights to operating system by using Movicon.NExT as Service. By doing this, file access through the operating system will be physically denied.
- Do not share folders or disks when the station is operating in net, except for system administrator access.
- Remove all rights to modify database records (Updates). Movicon.NExT lets new records to be inserted whose data cannot be accessed for altering no matter what the reason is.

3.5. Users Sharing

Windows User Sharing

Movicon.NExT offers the possibility to share users from the operating system's Domain or that of Windows (Win7/Win10).
This will enable security system managers to use one defined point of network users by using the Window Domain Users in alternative or together with the users defined in the project. Movicon.NExT accepts mixed configurations of users inserted in the project list and user from the Win7/Win10 domains, whose log on and management is delegated to the operating system. When using Windows users, the electronic signature field in the electronic records will assume the value given by the name of the user qualified by the domain they belong to: i.e. Domain Name/User Name. Mixed configurations do not ensure the uniqueness of information inserted in the Electronic Signature field due to the fact that Movicon.NExT does not have control over information relating to domain users. Therefore, we suggest you avoid using mix configurations even if technically permissible.

When authentication of a User is requested in Movicon.NExT by means of the Log On window, the user will first be verified with those of the project, and if the 'Share Windows Users' property has been activated, Movicon.NExT will ask the operating system to authenticate the User Name and Password to access the operating system's Domain. The criteria that establishes the project's Access Level is defined in the User Group, as described below:

- The users defined in the Windows Domain (Primary Domain Controller) can also be authenticated in Movicon.NExT and be given a custom user level by means of using a common User Group definition. The Windows Domain Users need to be inserted in the Windows User Group whose name is identical and present in the Movicon.NExT User Group. Each Movicon.NExT User Group can be defined with an Access Level and Access Area in its properties. Therefore, when a User is authenticated by Windows, Movicon.NExT will receive authorization and assign the User Level defined in the name of the Group to which the user belongs. It is, therefore, possible to assign the desired password level and access area to each Domain User by means of using the Groups.

For example:

- Windows has defined the 'R_Waters' user in the 'Machine_Operators' group.
- The Movicon.NExT project also contains a User Group with the identical "Machine_Operators" name.
- The desired Access Level and Area properties are assigned to users of the Movicon.NExT Group including "R_Waters".
- The project should also enabled with the Share Windows Domain Users property.
- When the user Logs On to Movicon.NExT, their access credentials will be passed over to Windows for authorization to then return back to Movicon.NExT positive. Movicon.NExT will then grant access to the user assigning them the access level defined in the Group.
- The same operation can be performed for any other user by sharing Groups or creating new ones as needed.
- This mechanism is also valid for users configured directly during runtime with the Movicon.NExT user editor window.
- The user's Electronic Signature and Name (User ID) that Windows manages uniquely, preceded by the name of the Domain.

Biometrics Systems

Using Biometrics Systems is highly recommended in application validity according to the regulations.
In this case, you need to choose the right recognition system among those available on the market that can be easily integrated into your application.
The most popular biometrics systems are ultimately those that use digital fingerprints. These systems are simple to use and integrate perfectly with operating systems and software applications.

3.6. Data Backup Validation

It is very important that any restoration of backed-up data be done using procedures that ensure their integrity otherwise, even though original, it will not be possible to validate them.

Data Backup

The CFR21 Part 11 norm explicitly stipulates that data restored from backup involve procedures that ensure their integrity for validation purposes. This requires that data subject to validation be backed-up and restored together with data of the Windows operating system user.
The inclusion of the Windows operating system user data is vital for validating data with the Movicon Audit Trail Validator which is based on the security identifiers (SID) of the operating system user contained in the backup data.
Data will not be validated if the process data is restored without the operating system user data.
Please refer to the Microsoft documentation on operating system image back procedures to consider when backing up data.

The validation of data is based on the SQL Server's TRANSACTION LOG using SID (user security ID) unique to each validation user ("NExT_IO_Server" User).
This means that if the validation user ("NExT_IO_Server") is cancelled from the operating system and regenerated later, the SID will change. This is done to ensure that maximum security is maintained when validating data. Therefore, when the SID is changed, it will not be possible to validate data recorded by a previous user !

Therefore, in addition to backing up data contained in the SQL Server database (which includes the Transaction Log), you will also need to configure operating system backup in the part regarding Windows Users.
For more information on using the best backup strategy, please refer to the Microsoft SQL Server and Windows backup and restoration documentation.

Data Restoration

In the even of a "Disaster Recovery", it will be necessary to proceed with restoring the previously created operating system's image.
Please refer to the Microsoft documentation for Restoration procedure of system image.

As regards to restoring the database, it is **essential** to restore backups based on the order in which they were created. Before restoring a specific transition log backup, you will need to restore all the previous backups that took place without executing a

transition rollback by using the SSMS's 'WITH NO RECOVERY' option within the database restore window.

Please refer to the Microsoft documentation for the SQL Server database backup restore procedure.

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