National Control Systems S.A.
Paepsem Business Park, Bat. 1
Blvd Paepsemlaan, 11B
1070 Bruxelles
Belgique
ncs.belgium@ncs-scaline.com
Tel : +32 2 245 22 39
Fax +32 2 245 16 25

National Control Systems S.A.R.L.
Centre d'affaires "Le Clos du Chêne au Loup », 1-3
Rue du Pic Cendré, 13
60520 La Chapelle-en-Serval
France
ncs.france@ncs-scaline.com
Tel. +33 3 44 63 07 10
Fax + 33 3 44 63 07 09

National Control Systems – NCS®

SCNET4 XPPLUG User Manual
Milestone Xprotect Access Plugin Integration

VERSION 1.0
21/01/2019

CONTENTS

1 INTRODUCTION

This document is the user manual of the XPPLUG option of the SCNET4 system. It provides information regarding the XPPLUG plugin (Milestone XProtect® Access plugin integration) for the SCNET4™ access control System by NCS. This plugin integration offers a bidirectional communication between both systems, allowing a direct control and monitoring of the SCNET4 access control system from the Milestone XProtect software interfaces. It also enables the user to benefit, within a single unified interface, from all other integrations accessible within Milestone XProtect.

This manual details the different operations (installation, configuration and basic user operations) required to interact with the Milestone XProtect Access plugin from the different software composing the Milestone XProtect solution (XProtect Management Client, Smart Client, …). For advanced user instructions for those products, we refer the user to the dedicated Milestone documentation.

1.1 Compatibility Note

The compatible version for software and equipment are the following:

Table 1: Software compatibility information

Software	Version
SCNET4	3.14.0
Milestone XProtect Express	2018R2/R3 (*)
Milestone XProtect Express +	2018R2/R3 (*)
Milestone XProtect Professional	2018R2/R3 (*)
Milestone XProtect Professional+	2018R2/R3 (*)
Milestone XProtect Expert	2018R2/R3 (*)
Milestone XProtect Corporate	2018R2/R3 (*)

(*) Version used for test and qualification of the solution.

1.2 Notes on licensing

1.2.1 SCNET4 Licensing

In order to ensure the correct installation and a reliable working environment for the Access plugin for Milestone XProtect, it is required to activate the **XPPLUG** license option on the SCNET4 system. If this option is not referenced on your license document or in the license activation tools of the SCNET4 system, please mention this to your software reseller in order to receive the appropriate commercial information on how this license option can be activated.

1.2.2 Milestone XProtect Licensing

A specific Milestone XProtect license option is required to activate the XProtect Access plugin. In addition, depending on the number of doors provisioned for your XProtect Access plugin, a limited number of doors relative to your access control software(s) can be controlled and monitored from within Milestone XProtect. For more information, please contact your Milestone software reseller.

1.3 Integration principles

The XPPLUG integration of the Milestone XProtect Access Plugin in the SCNET4 system is essentially a supervision and control integration allowing to view and control doors, alarms, relays and technical points. It does not allow the operator to define or manage users, identification tokens, access rights since those operations require to be achieved using the NET4-C clients for the SCNET4 system.

2 INSTALLATION PROCESS AND CONFIGURATION

The current section details the operations required to install and setup the configuration parameters for the plugin integration. These operation need to be achieved both for the SCNET4 system and for the target version of Milestone XProtect. The current section is therefore divided into two distinct subsections.

2.1 SCNET4 System

We detail here all the elements to be setup for the SCNET4 system.

2.1.1 Installation.

Not additional software is required.

2.1.2 Parameter setup

2.1.2.1 License

Regarding the license parameters, those need to be correctly configured within the system. Additionally, some specific parameters need to be put in place for the correct operation of the plugin integration.

2.1.2.1.1 License activation

As for all other optional functionalities of the SCNET4 system, the XPPLUG license activation is achieved using the “Distribution Wizard” software installed together with the NET4-S server software. You can find this utility in the target program folder of the NET4-S server. Required steps to access this utility are illustrated in Figure 1.

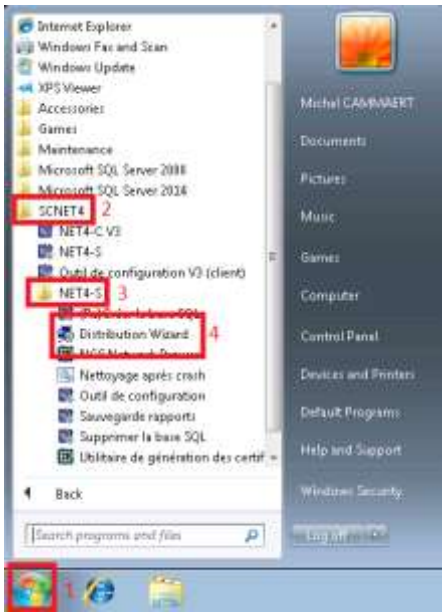

Figure 1: Accessing the “distribution wizard” (windows 7)

Once the “Distribution Wizard” launched, the “Options & Activation” menu needs to be selected. In this menu, the “XPPLUG” option needs to be correctly activated (overline in blue) in the “NET4 Options”. An activation code for the software version, corresponding to the license level and options need to be entered in the “Activation Code” field of this menu. This is illustrated in Figure 2.

Figure 2: XPPLUG activation in "Distribution Wizard"

2.1.2.1.2 License verification

Once your license correctly activated, it is possible the list all activated options from within the NET4-S server software interface (as illustrated in Figure 3):

1. Right-click on the icon located in the top left corner of the main window of the NET4-S server software GUI.
2. In the new window, click on “About NET4-S Server”
3. In the following screen, click on “Options”.
4. If the XPPLUG option is correctly activated, it appears as “XPPLUG” in the option list for the current configuration of the SCNET4 system.

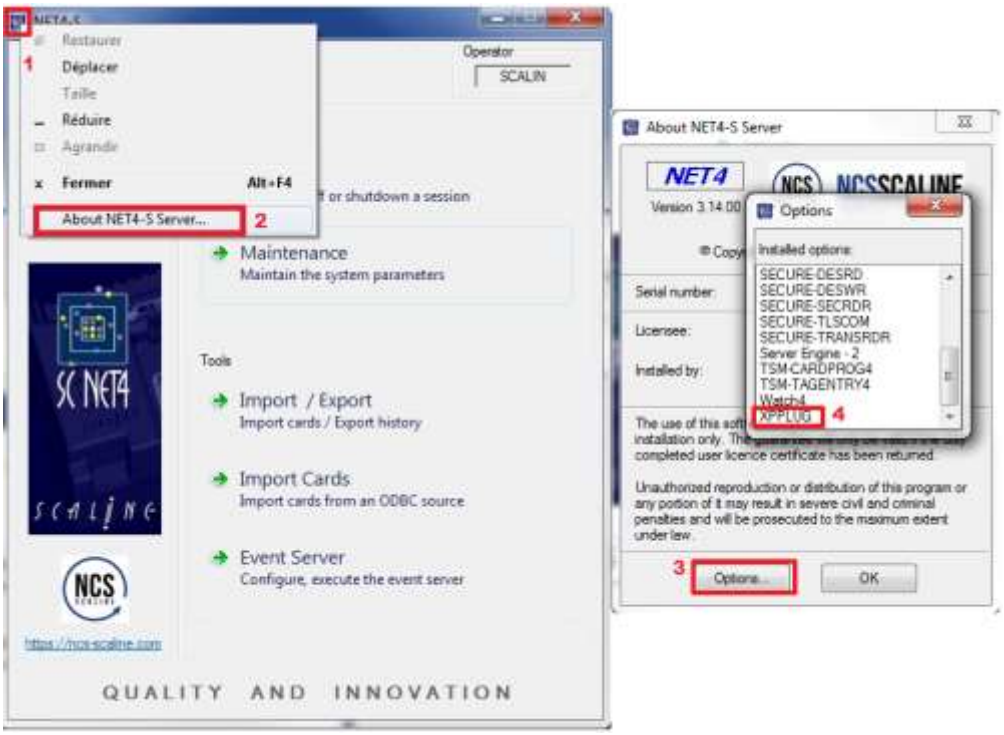

Figure 3: Validation of activated options for your SCNET4 system

2.1.2.2 Dedicated operator

In order to setup an authenticated communication between the XProtect Access plugin and the SCNET4 system, a dedicated operator must be created on the SCNET4 system. This definition can be achieved from within any NET4-C client software attached to your SCNET4 system, provided you own an operator profile with the appropriate access rights. The required operations are illustrated in Figure 4 :

1. Select the “Parameters” menu from the main window of the NET4-C software.
2. Develop the “Operator” sub-menu
3. Double-click the “Operators” configuration menu
4. In the new window, click on “New” to define a new operator
5. Input the appropriate parameters for this operator (name, initial (corresponding to the login)).
6. Validate that the associated schedule for this operator is “Always” and that all habilitations point to “All”.
7. Click on the “password” button to start the password definition process.
8. Type and confirm the password for this operator.
9. Click on “Save” in the password configuration window
10. Click on “Save” in the operator configuration window.

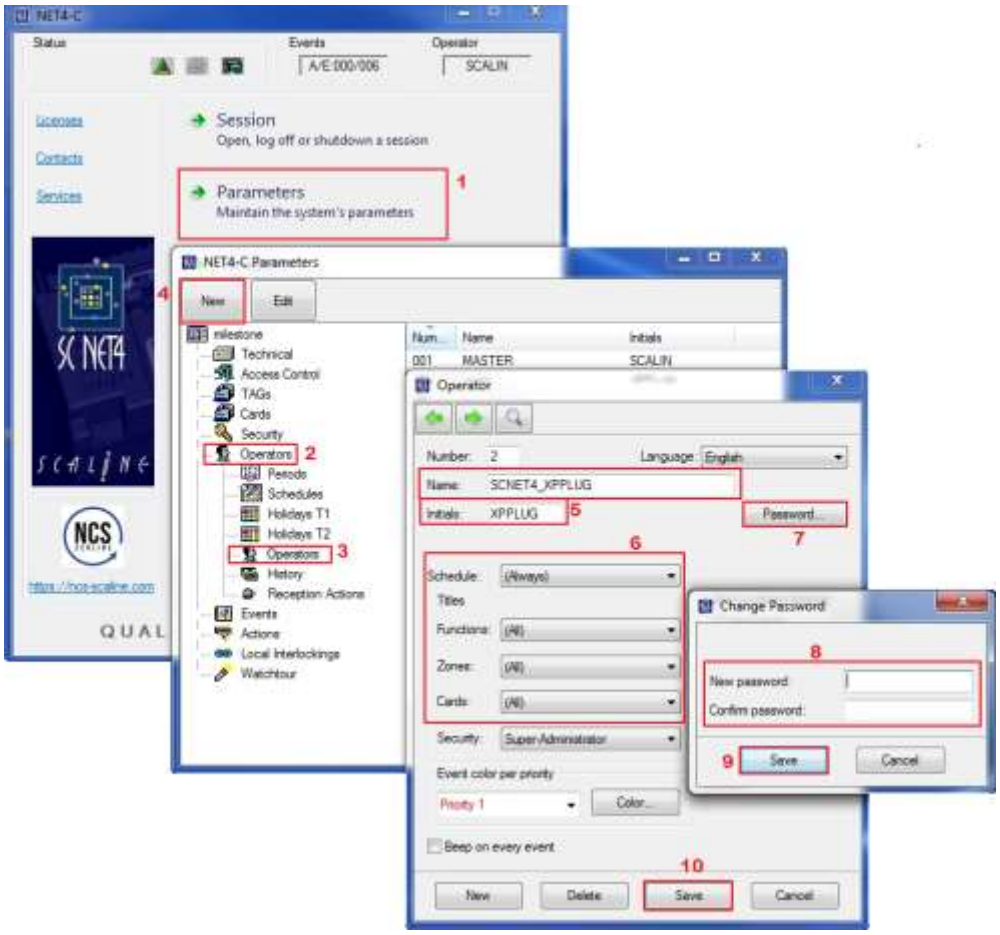

Figure 4: Configuration of a dedicated operator in the NET4-C interface.

Remark : This new operator can be used from any operator interface connected to your SCNET4 system, as long as no other valid session is using it. However, as soon as your XPPLUG plugin is started by the milestone server, this operator becomes unavailable for a session establishment on the SCNET4 system since it only allows a single active session per operator login. Please be careful to communicate these credentials only to the required people.

2.1.2.3 Dedicated client station

In order to establish the communication between the NET4-S server and the XPPLUG plugin, a dedicated station must be created. Indeed, as viewed from the NET4-S server, the XPPLUG plugin is only another station client receiving event information and providing parameter configuration. To configure this dedicated station, the NET4-S server menu needs to be used (as illustrated in Figure 5):

1. Go to the “Maintenance” menu of the NET4-S server
2. Select the “Client station” sub menu and double click on “Parameters” menu
3. In the new window, click on the “New” button
4. In the new window that appears, the name of the station can be defined.

Figure 5: Creating a dedicated client station for the XPPLUG plugin instance.

Once this new stations has been created, you must remember the name given to this station as it will be required for the XProtect Access plugin parameter configuration (see section **Erreur ! Source du renvoi introuvable.**). Please also ensure that the “Attributed” check box remains unchecked after you leave the configuration window. You can finalize the station definition by clicking on the “Save” button.

2.1.3 Validating the link between the NET4-S server and the Access plugin

Once the plugin is correctly configured and activated in Milestone XProtect, and once the XProtect event server has established a connection towards the NET4-S server, this connection appears in the list of active client connections. The dedicated station selected for the XProtect Access plugin is identified from the type received as it must show “XPPLUG” in the “Type” column of this window, as illustrated in Figure 6. In this figure, the same of the station is “XProtectAccessPlugin” and the operator Login is “XPPLUG”.

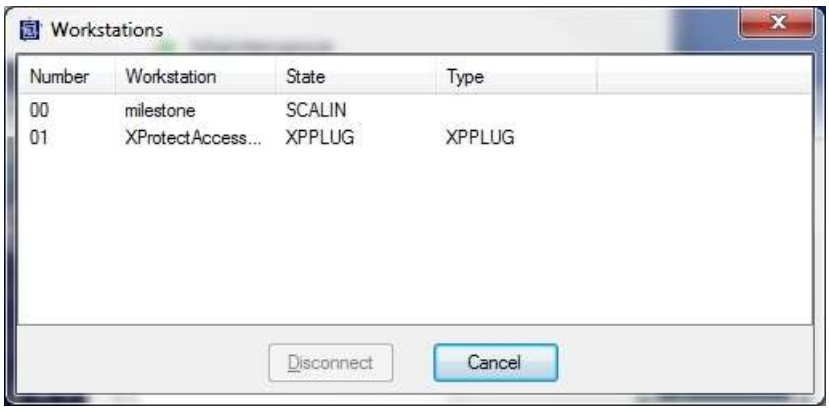

Figure 6: Illustration of connected client stations.

2.1.4 Controlled access management

If, in addition to the XPPLUG option, the SCNET4 license includes the ADACC4 option, it is possible to configure the controlled access mode on the different side of doors within the SCNET4 system in order to control this behavior directly from Milestone XProtect Smart Client.

As a reminder, when the controlled access is activated, an access requires is generated by a user when its access token (access card, ….) is presented on the reader of the target door. Once the card is read, and its credentials validated, an operator working on the target NET4-C station has a defined delay to grant the access. Passed this delay, the access is considered as refused.

2.1.4.1 Preliminaries

To enable the controlled access function within Milestone, it is required to:

- Have an established link between the NET4-S server and the Milestone XProtect event server (dedicated station and user correctly setup on both sides)
- Define a specific station display class on the SCNET4 system. This display class can be defined in the NET4-C → Parameters → Event → Station class menu.
  For the current case, we will chose the following configuration parameters:
  - Schedule : Always (the time schedule associated to the controlled access is “Always”)
  - Station : Name of the dedicated station used for the XProtect Access plugin (see Sections **Erreur ! Source du renvoi introuvable.** et **Erreur ! Source du renvoi introuvable.**).

  This is illustrated in Figure 7.

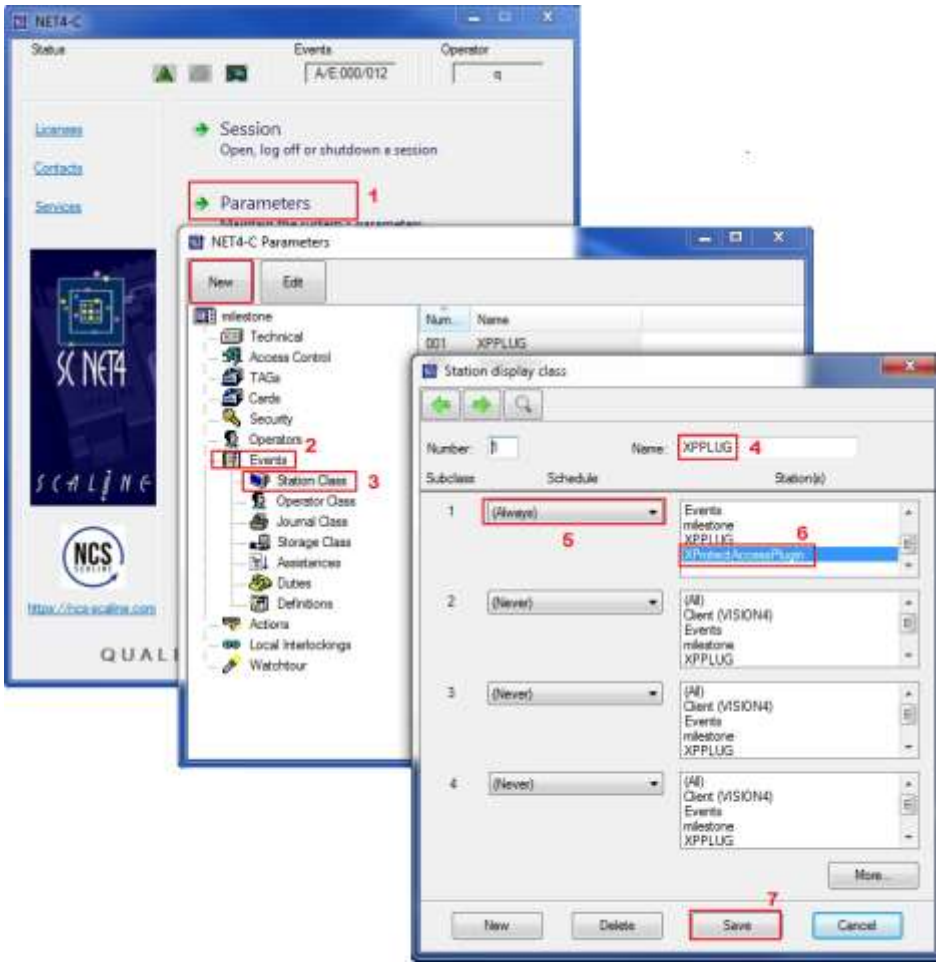

Figure 7: Station display class required in order to setup the controlled access with the XPPLUG plugin.

2.1.4.2 Access control setup on the doors

The correct setup of the controlled access functionality can be achieved for each door from within the NET4-C software. For each door of the system, it is possible to choose which side of the door shall benefit of such a behavior. For each door, in order to dedicate the controlled access behavior management to the XPPLUG plugin, it is required to check on the desired side(s) of the door the two check boxes:

- « Enabled to go to the A/B zone »
- « With operator validation »

After that, it is required to select the schedule during which the door must follow the controlled access behavior rules. Outside of the periods defined by this schedule, the door has a regular behavior. The, it is required to choose the station display class as defined in the above preliminaries.

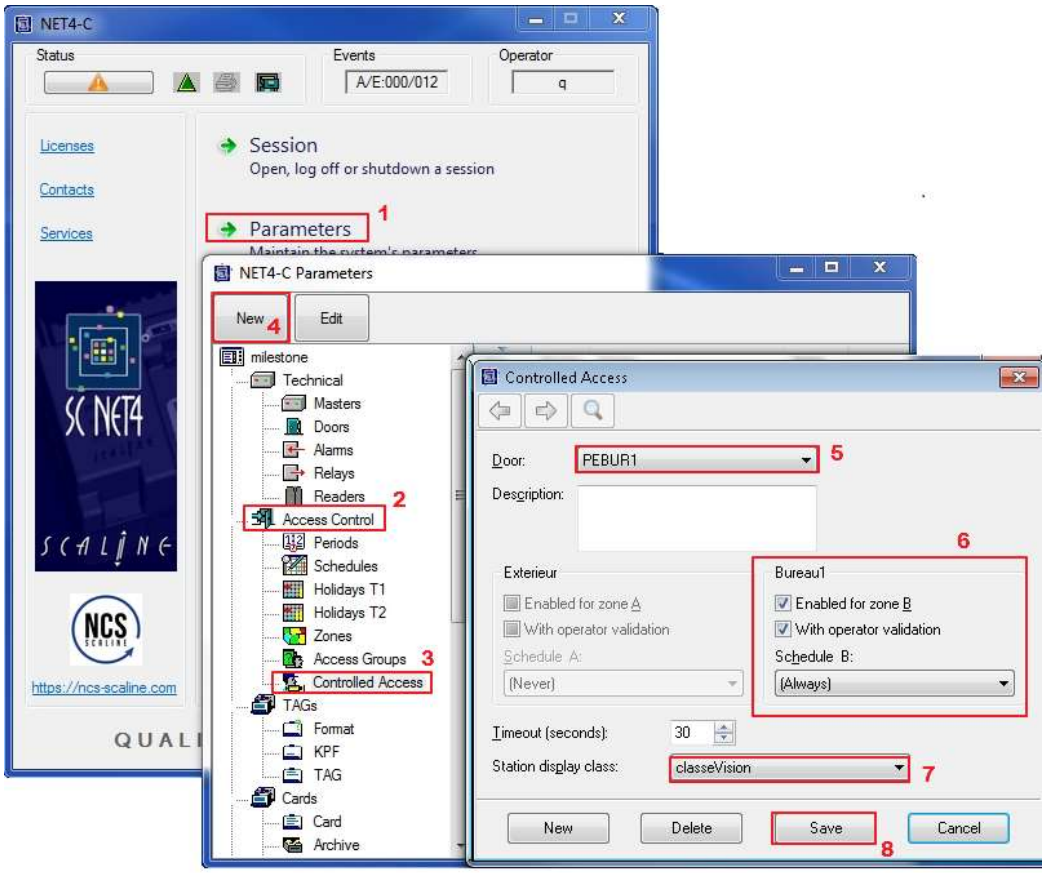

Figure 8: Controlled access setup to enable management from Milestone XProtect Smart Client.

2.2 Milestone XProtect

The current sub-section details the necessary elements to be configured on the Mistone XProtect side. Information are provided about the plugin installation, its generic configuration and the parameters required for its full exploitation.

2.2.1 Installation and license

2.2.1.1 XPPLUG plugin installation

The plugin installation must be achieved on the same computer where the Milestone XProtect server application is installed. The execution of the installation process is initiated using the “setup.exe” application icon you can find in the installation folder of the NET4-S server application. Chose first the folder corresponding to your desired installation language then double-click on the “setup.exe” file.

Caution, the installation process requires that you are logged in the current windows session using with administrator rights on the target PC/server.

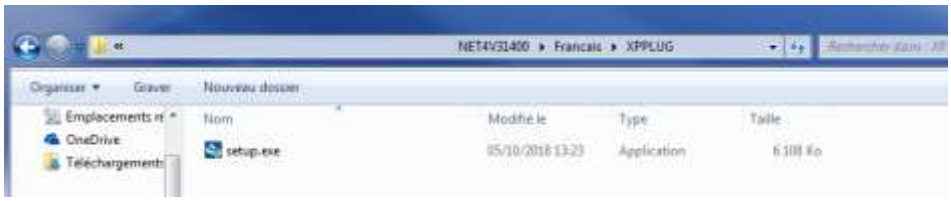

Figure 9: Illustration of the target file to be used for the XPPLUG plugin installation

At the beginning of the installation process, a window appears with a message about the preparation of the installation of the SCNET4 XPPLUG plugin for Milestone XProtect.

Figure 10: Launch of the XPPLUG plugin installation process

Once the installation preparation completed, a second window appears warning the user about the imminent installation and requesting a confirmation by clicking on the “Next” button.

Figure 11: Continuation confirmation

It is then necessary to confirm the license agreement to continue the installation process. (click “Next” after confirming the license agreement)

Figure 12: Plugin license agreement confirmation.

It is then required to confirm/select the destination folder for the XPPLUG plugin installation. A folder under the “MIPPlugins” sub-folder located under the installation root for the XProtect event server software must be selected. Once the right folder selected, click on the “Next” button to proceed with the installation process.

Figure 13: Installation folder selection

The last confirmation screen appears then to finalize the installation setup. To proceed, it is required to press the “Install” button.

Figure 14: XPPLUG plugin installation finalization

A progress bar is then displayed illustrating the installation process progress.

Figure 15: Progress of the installation process

A last window confirms the successful / failed installation of the plugin. To terminate the installation process, click on the button “Finish”.

Figure 16: Closing the installation process

2.2.1.2 Milestone License elements

Once you purchase a Milestone XProtect product, an email is generated providing a software license code (SLC) and a software license file (.lic extension). In the same way, if you purchase an XProtect Access plugin license, a license file containing its specific parameters is provided.

2.2.1.2.1 Information regarding the software license

The **Milestone XProtect Management Client*** application provides an interface to browse the information on the installed license elements, including the presence of a Milestone support contract. This interface can be accessed through « Basics > License information ».

Information on the installed products is provided in the section “Installed Products” with details on the activation code, the expiration date (if any), the validity date of the contract (if any). The information regarding the license usage are provided in the “License Overview – All sites” section. In the case of the Access plugin, the number of configured doors, together with the maximum number of usable doors are provided.

Other complementary license information are provided in the “License details –xxx” for each configured site. This is illustrated in Figure 17.

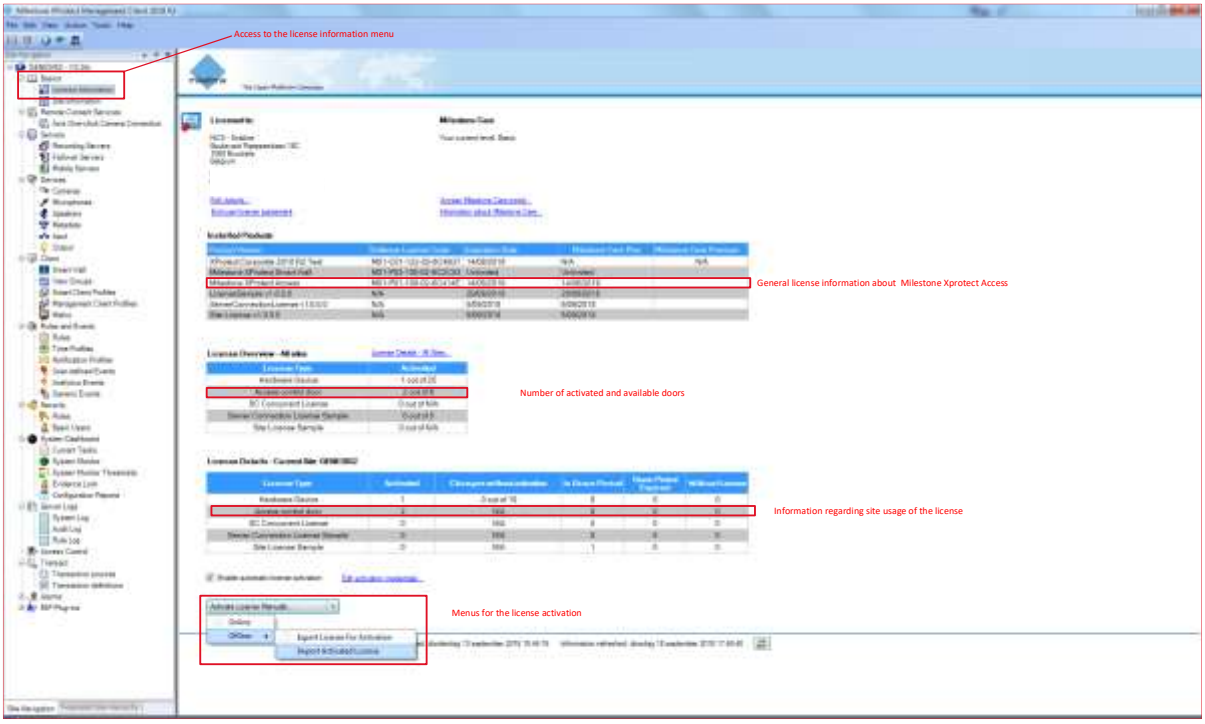

Figure 17: License information and activation for Milestone XProtect

* XProtect Express and XProtect Professional do not feature the Management Client but rather the Management Application which does not provide this information.

2.2.1.2.2 Installing the license (Management Client)

If your license file has been activated online, the installation process uses the following menu of the Milestone XProtect Management client: “Basic > License > Information”. At the bottom of the screen, in the “Activate License Manually”, choose the “Offline” option and then “Import Activated License”.

This is illustrated in Figure 17.

2.2.1.2.3 Other license activation mode

For all other license activation functions, please consult the Milestone documentation specific to XProtect:

https://www.milestonesys.com/support/help-yourself/manuals-and-guides/

2.2.2 Configuration

Once the XPPLUG access control plugin installed and the Milestone XProtect license correctly installed, it is possible to proceed with the technical configuration of the different parameters of the access control plugin within Milestone XProtect Management Client (or the Milestone XProtect Management Application for XProtect Express and Professionnal).

A generic configuration enables the communication between the XPPLUG plugin (within Milestone XProtect) and the SCNET4 access control system. Exploitation parameters can also be configured to select the doors of the access control system being mapped into Milestone XProtect, to associated them with cameras or configure other access control system objects mapped into Milestone XProtect.

2.2.2.1 Access control system generic mapping

The generic configuration enables the establishment of the communications between the XPPLUG plugin and the SCNET4 access control system.

A new communication link can be created by right-clicking on the “Access Control” menu in the list of accessible menus in the management program. A pop-up then opens allowing the creation of the new access control system. This is illustrated in Figure 18.

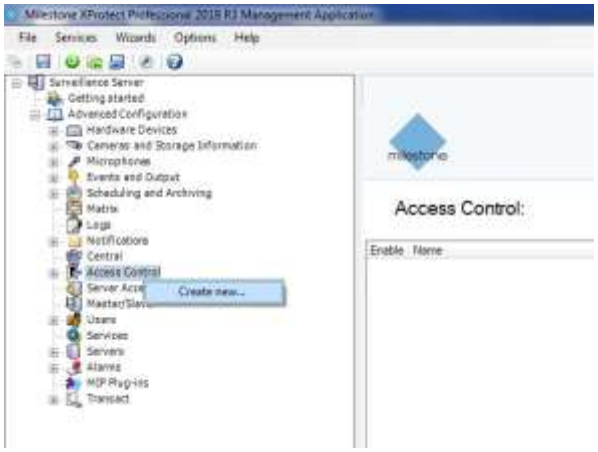

Figure 18: Communication link creation between the SCNET4 system and the XPPLUG plugin.

In this new window, we can configure a name for the activated plugin and select the target extension plugin: here select “SCNET4™ Access control plugin”.

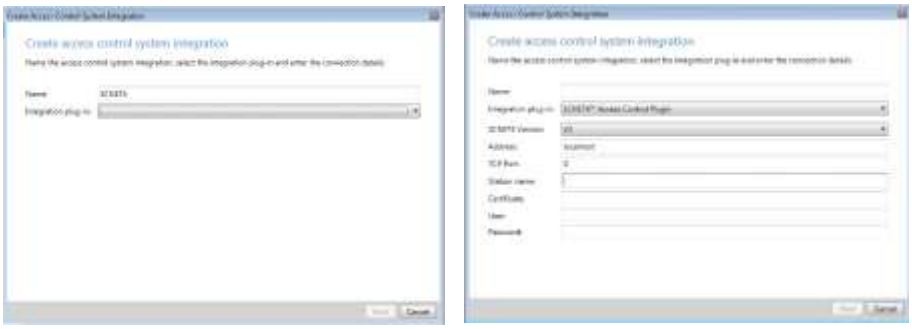

Figure 19: Selection of the target plugin and configuration of its generic parameters.

Once the SCNET4 module has been selected, it is possible to define the generic parameters necessary for the establishment of a communication between the two systems. The required parameters are the following:

Table 2: Required parameters for the communication establishment between Milestone XProtect and the SCNET4 system

Parameter	Details
Version SCNET4	Version of the selected SCNET4 system. Possible values are V2 or V3.
Address	IP address or target hostname of the computer hosting the NET4-S application.
TCP Port	TCP Port used for the connection. The default value is 0, indicating the usage of dynamic ports. If a specific port has to be used, a figure different than 0 corresponding to the target port shall be specified.
Station name	Name of the dedicated station configured in the NET4-S server (see section Erreur ! Source du renvoi introuvable.).
Certificate	Cryptographic certificate used to establish a TLS 1.2 connection with the NET4-S server (Only for V3 if the SECURE option is activated). The value that shall be specified here corresponds to the “Delivered to” value of the certificate. This certificate shall be installed following the method described in the SCNET4 Secure user manual in order to be correctly setup in the Windows certificate store.
User	Name of the dedicated user created to establish the connection with the NET4-S server (see section **2.1.2.2**). The target value corresponds to the Initials specified for the SCNET4 operator).
Password	Password related to the User selected above.

Once all parameters correctly set, click on the “Next” button to initiate the process reading the technical information (doors, inputs, outputs, …) from the SCNET4 system. Once the information read back, a creation menu signals that the configuration has been received and details all the elements received from the SCNET4 system as illustrated in Figure 20.

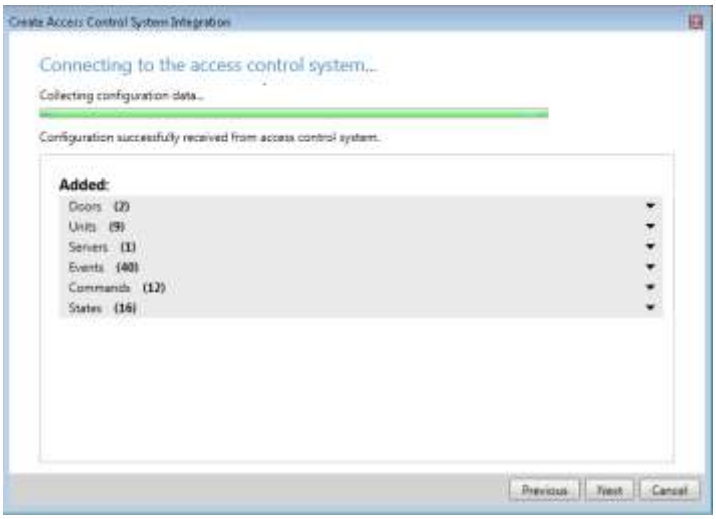

Figure 20: Recovery of information from the SCNET4 access control system.

By clicking on the « Next » button, we can reach the menu from which doors from the SCNET4 system can be associated to doors in the XPPLUG plugin and linked to cameras. In this window, you can check/uncheck the “Activated” checkbox to associated doors from the SCNET4 system to doors within the XProtect Access plugin. For each associated door, the screen indicates the license usage “Pending” and if cameras are associated to either of the access points of the door. To link a camera to an access point, just select the camera from the lower left corner of the window, drag and drop it to the desired access point. A single camera can be associated with several access points. This is illustrated in Figure 21.

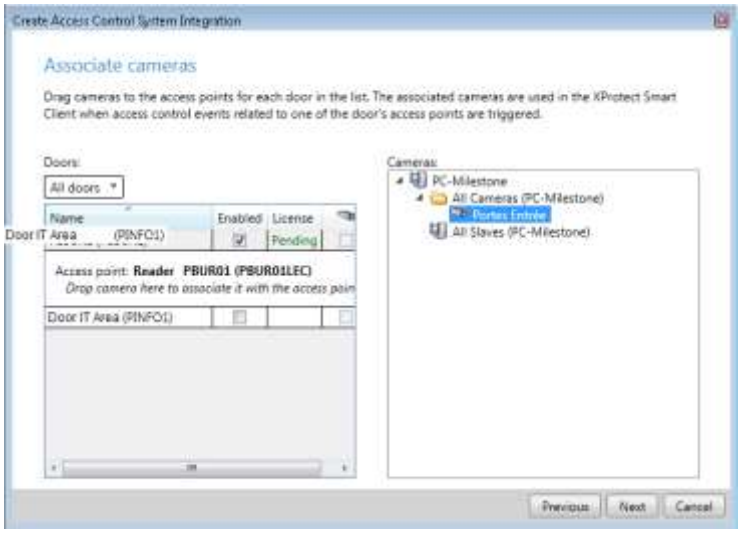

Figure 21: Association of cameras with doors/ access points of the XProtect Access Control plugin.

By clicking on the « Next » button, we reach the last window of the XPPLUG plugin. This window signals the end of the configuration process and that the access control system can now be used by operators of the XProtect Smart Client application. This is illustrated in Figure 22.

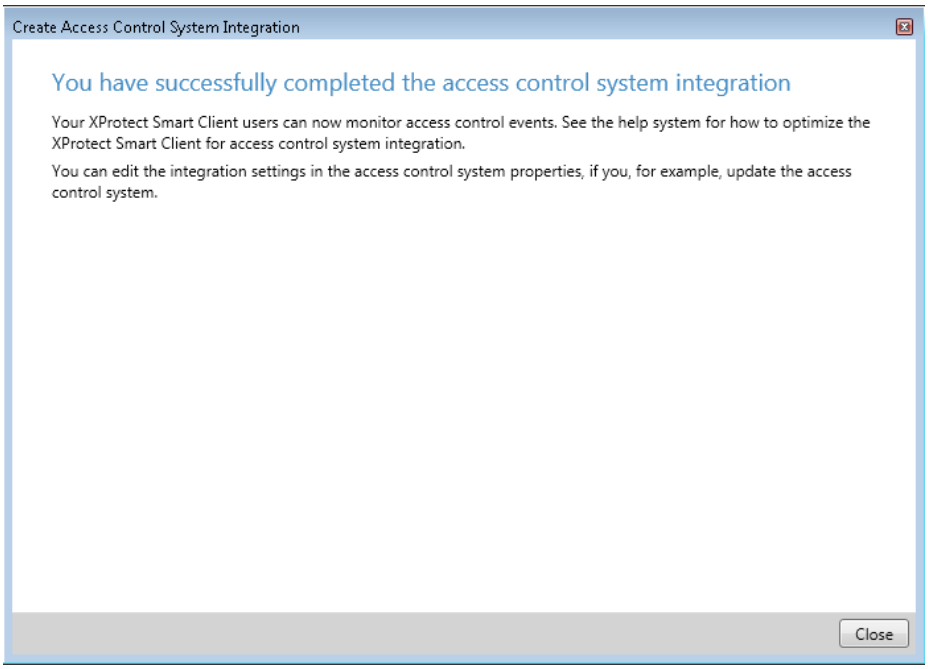

Figure 22: Configuration finalization of the XPPLUG plugin.

2.2.2.2 Generic configuration update

Once the generic configuration has been done for the first time, it is possible to modify those parameters. The Milestone XProtect Management Client or Management Application, can modify those by double-clicking on the desired access control system setup in the application. Once you do it, the management menu of the plugin is reached and can be used to modify the following configuration information:

- Generic parameters — Definition of the connection parameters used to establish the communication between both systems.
- Doors and associated cameras: — List of existing doors (can be updated), access points and their association with cameras.
- Access control events — Configuration of events generated by the access control system and their generic handling by the Milestone XProtect Access plugin (XPPLUG).
- Access control actions — Programming of the automatic actions generated by Milestone based on events generated by the access control system.
- Card holders : — Listing and details of user of the access control system (not operators)

Details regarding the above mentioned configurations are provided in the next sections.

2.2.2.2.1 Generic parameters

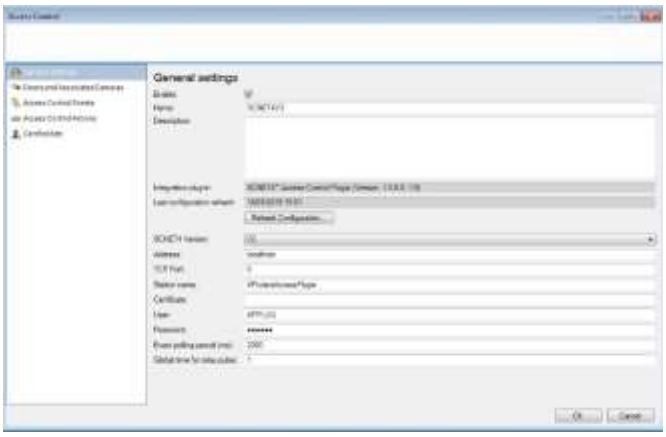

Figure 23: Plugin generic parameter

The generic parameter menu can be used to modify parameters configured during the system plugin creation (see Table 2). Additional parameters and functions can be accessed from this menu:

- Possibility to inert a description of the access control system
- Possibility to modify the events polling (in milliseconds) period. Indeed, in order to refresh the list of the events gathered from the access control system, the plugin implements a regular polling for which the frequency is defined by the present parameter.
- The global relay pulse time (in seconds) defines the duration of pulses applied to access control relays from the Milestone XProtect Plugin.

In addition, this menu informs the operator about the following system information:

- Plugin version
- Date and time of the last synchronization between the two systems.

Finally, by clicking on the « Refresh configuration » button, it is possible to initiate a resync of the technical information between the content of both databases.

Once changes in the access control system are detected by the plugin, those are summarized in a window similar to the one illustrated in Figure 24.

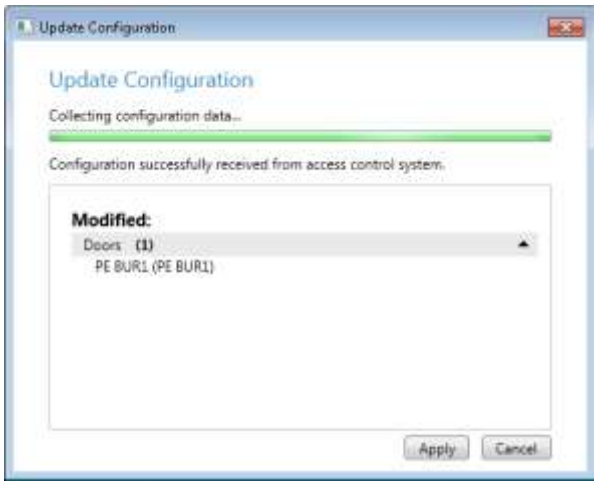

Figure 24: Illustration of the detection of an additional doors during the synchronization between the SCNET4 system and the XPPLUG XProtect Access plugin.

2.2.2.2.2 Doors and associated cameras.

Figure 25: Configuration of the door/access-point – camera association

The menu « Doors and associated cameras » provides a mean to configure or modify door/access-point association with cameras. This association is displayed by a checked checkbox in the column “activated”. The validity period of the license is given in the column “License”.

A camera listed in the right-hand side of the menu can be associated to either side of an access point by drag-and-dropping it on the target access-point associated with the door in the central part of the window.

2.2.2.2.3 Access control events

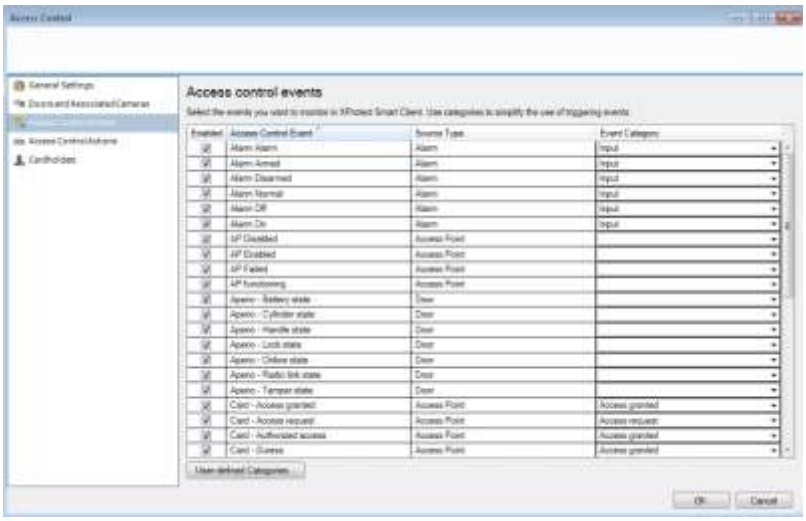

Figure 26: Configuration of the access control events and link between specific events from the SCNET4 system and generic access control events in the plugin.

With this menu, it is possible to configure which events coming from the access control systems are reported in Milestone XProtect through the XPPLUG plugin. In addition, it provides a mean to map access control specific events to generic XProtect Access events. Once events are mapped, they can then be used to trigger automatic behavior in Milestone XProtect (see Section **Erreur ! Source du renvoi introuvable.**).

Activated Column

A checked checkbox in the « Activated » Column in front a given event activates the selection of this particular event.

Source type

The source type specifies the type of source associated to this event. Source types can be:

- A door
- An access-point (for the SCNET4 access control system, this usually corresponds to a specific side of the door or, at least, to a specific reader or keypad).
- The NET4-S (the SCNET4 access control system server).
- An input (alarm, push-button, or any other source connected to a controller input).
- An output/relay (enabling the command-control of a siren or any actionnable mechanism connected to the access control system through a relay and not linked to a proper door).

Category

The event category relates to a type of access control event. This notion provides a mean to achieve advanced filtering on the event during the regular use of the system. The possible categories that can be associated to events are the following (it is possible to select more than one category for a specific event):

- Access granted — Event related to an access authorization successfully given to a cardholder.
- Access refused — Event related to a failed access authorization for a cardholder.
- Alarm — Alarm generated by the access control system.
- Warning — Warning generated by the access control system.
- Access request — Access request requiring an operator confirmation on the Milestone system that shall be forwarded to the access control system. By default, with the XPPLUG plugin, only the "Card – Access request" is linked to such kind of event and can be used only if the "controlled access" option is available on the target SCNET4 system. It is always possible to link such an event category to any other event defined in the SCNET4 system.
- Input — Event related to an input of the access control system (push button, detector, door contact, …).
- Error — System error or technical error coming from the access control system.
- Relay — Event related to a relay of the access control system.

In addition, it is possible to define custom event categories using the « User defined categories » button. We refer the user to Milestone XProtect documentation for the definition and usage of this menu.

The different event types coming from the access control system and accessible from the XPPLUG plugin are listed in the following table.

Table 3: Description of the different SCNET4 events accessible from the XPPLUG plugin.

Event	Description
Aperio – Tamper state	State change of the tamper sensor of an Assa-Abloy Aperio lock connected to the SCNET4 system.
Aperio – Battery state	State change of the battery sensor of an Assa-Abloy Aperio lock connected to the SCNET4 system.
Aperio – Online state	State change of the logicial connection between the SCNET4 system and an Assa-Abloy Aperio lock connected to the SCNET4 system.
Aperio – Handle state	Activation or return to normal state of the handle associated with an Assa-Abloy Aperio lock connected to the SCNET4 system.
Aperio – Lock state	Activation or return to normal state of the lock associated with an Assa-Abloy Aperio lock connected to the SCNET4 system.
Aperio – Cylinder state	Activation or return to normal state of the cylinder associated with an Assa-Abloy Aperio lock connected to the SCNET4 system.
Aperio – Radio link state	State change of the connection between the Aperio communication hub and one of its paired Assa-Abloy Aperio lock.
Card – Access granted	Access one of side of the door has been granted to an access control system user. This means that one of its credential was presented to a reader connected to the door while the user is register with access authorization on the associated system zone during a time period including the event time.

Card– Duress	Access one of side of the door has been granted to an access control system user. This means that one of its credential was presented to a reader connected to the door while the user is register with access authorization on the associated system zone during a time period including the event time. The user has entered a confirmation code indicating that he was forced to present his/her credential on the target door.
Card – Authorized access	The access has been granted to an access control system user following the presentation of a valid identifier while the door is in “free access” mode.
Card – Local passback	The access to one side of the door has been refused because the user attempted to pass a second time on the same access without having passed on another door and the local anti-passback has been configured on this door to prevent such a behavior.
Card – Access request	The access has been requested on a door for which the « Controlled access » has been configured. It requires an action from the operator to authorize the access. (The Milestone event “Access Request” has to be associated in relation to this event).
Card – Invalid schedule	The access to one side of a door has been refused to the user sinc he/she does not own an access right to the associated door at the time of which his/her credential was presented.
Card – Key error	Acces refused because the site-code associated to the credential (if defined in the card format) is invalid.
Card – Format error	Access refused because the format of the presented credential is invalid or does not correspond to any format configured on the target reader.
Card – Invalid number	The access was refused because the credential number used is not present in the database of the controller associated to the door or not mentionned has « Activated ».
Card – Invalid Period	The access has been refused for one of the following reason: - For a permanent user, he is supposed to be on holiday at the time of the event. - For a temporary user, the validity period of this user does not correspond to the time at which the event has occurred.
Card – zone	L’accès a été refusé parce que la zone de sécurité associée au côté de la porte où le badge a été présenté n’est pas reprise dans les droits d’accès de l’usager.
Server connection lost	The connection with the SCNET4 server has been lost
Alarm Normal	The input of a controller of the system has come back to its normal state.
Alarm Armed	An input of a controller is now armed. Any change of state on this input will be signaled.
Alarm Disarmed	An input of a controller has been disarmed. « Input at Normal state » and technical alarms (auto-protection, short/open circuit, instable state) will be signaled but no “regular” alarm will be transmitted.
Alarm Alarm	An input of a controller is now in alarm. Consult the alarm description to identify the alarm type.
Alarm On	An input of a controller has been put in service. Depending on its arming mode, events will be transmitted or not.
Alarm Off	An input of a controller has been put off service. No event of any kind will be transmitted regarding this specific input.
PIN code error	The keypad confirmation code entered by a user is wrong.
AP (Access point) Disabled	The reader/keypad associated to a specific side of a door is now activated.
AP Enabled	The reader/keypad associated to a specific side of a door is now deactivated.
AP functionning	The reader/keypad associated to a specific side of a door is now back to its normal state (after a failure).
AP failed	The reader/keypad associated to a specific side of a door has failed.
Door unlocked	A door of the system is unlocked (if a bolt bottom contact is configured on the door).
Door Alarm	Une porte du système a été forcée
Door Locked	A door has been switched to blocked mode. No credential will be read on none of the access points.
Door free access	A door has been switched to free access mode. No credential needed to enter the door.
Door Secured	A door has been switched to under sureillance mode. It is required to pass a valid credential to open it.

Door Normal	A door has been correctly closed.
Door Ajar	A door remais open after the configure open duration.
Relay On	A relay has been switched ON (on the NC contact of the relay).
Relay off	A relay has been switched OFF (on the NC contact of the relay).
Server connected	The connection to the SCNET4 server has been (re)established.

2.2.2.2.4 Controlled access actions

The “access control actions” menu provides a configuration interface for the interactions between access control events and functions or actions within Milestone XProtect. It is, for example, possible to configure the recording of the video stream generated by a camera when a specific doors enters an alarm state.

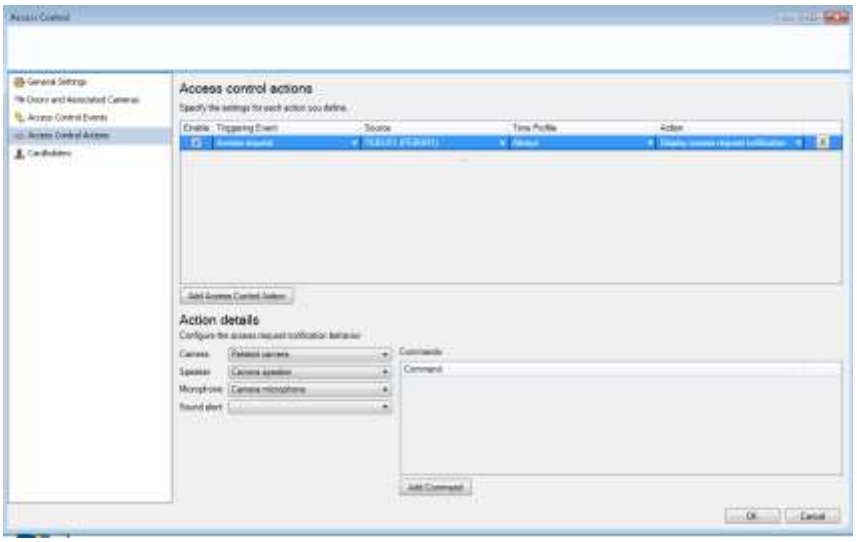

Figure 27: Configuration of access control functions in Milestone XProtect

The configuration of a specific action regarding the access control system requires the definition of the following elements:

- Triggering Event : One of the event type defined in Table 3
- Source System object from the access control sytem on which the trigger event occurs. It is possible to select :
  - A specific object
  - All objects of the same type
  - Different distinct objects (through the selection menu which appears when left-clicking on button « Other »).
- Time profile One of the time profile configured in the « Alarms → Time profile » of the management program of your Mileston XProtect install.
- Action One of the actions defined in the Milestone XProtect (see below sub-sections).

2.2.2.2.4.1 Action – Display a notification

Enables the configuration of a specific display of a given event notification.

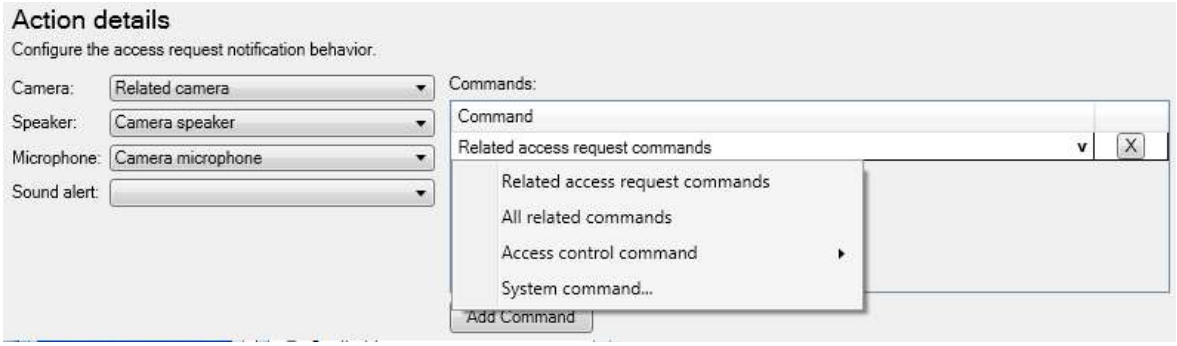

Figure 28: Configuration of the Display notification action

By clicking on the « Add a command » button, it is possible to add additional commands when the given notification arises and is displayed. The associable commands are:

- Commands of Access request on associated accesses
- All associated commands
- Access control commands (specific to the SCNET4 system):
    - Switch a door / access point to “controlled access” mode (normal mode)
    - Switch a door to the « free access » mode
    - Switch a door to the « blocked » mode
    - Trigger a temporary opening sequence of a door
    - Switch the door mode to automatic management (if specific schedules are configured they will be executed)
    - Arming an input
    - Disarming an input
    - Set an input off
    - Set an input on
    - Activate a relay
    - Deactivate a relay
    - Pulse a relay (duration of the pulse is programmed as a global parameter for all relays)
- System command (command related to Milestone XProtect and some of its configured options).

2.2.2.2.4.2 Go to predefine PTZ positions

Enables the definition of the triggering of a movement of a specific camera towards predefined PTZ positions and the time after which the camera shall come back to its default position.

2.2.2.2.4.3 Start recording

Enables the definition of the recording of one more specific video stream and the duration of this recording.

2.2.2.2.4.4 Specific system action

Enables the definition of the triggering of an action / command specific to the Milestone XProtect system and of some of its configured options.

2.2.2.2.5 Cardholders

Figure 29: Display menu of the cardholders of the SCNET4 system connected to Milestone XProtect through the XPPLUG plugin

The cardholder menu displays the main information (name, first name, type, category, photo, ….) of the users imported in Milestone XProtect from the SCNET4 system.

2.2.2.3 Operation settings

The operation settings can be configured using Milesotne XProtect SmartClient. We suggest that the reader consults the XProtect SmartClient user manual for a detailed explanation of the procedure. The section “XProtect Access” provides details on the generic principle of the configuration and usage of this software together with all the compatible XProtect Access plugins such as the XPPLUG pluging for the SCNET4 system.

2.2.2.3.1 Session management

The XPPLUG plugin does not require a second login to the access control system once an operator is in session. A session is automatically established to the SCNET4 system as soon as the Milestone Event Server is launched. When XProtect SmartClient is launched, the screen indicates a valid connection with the access control system as illustrate in Figure 30.

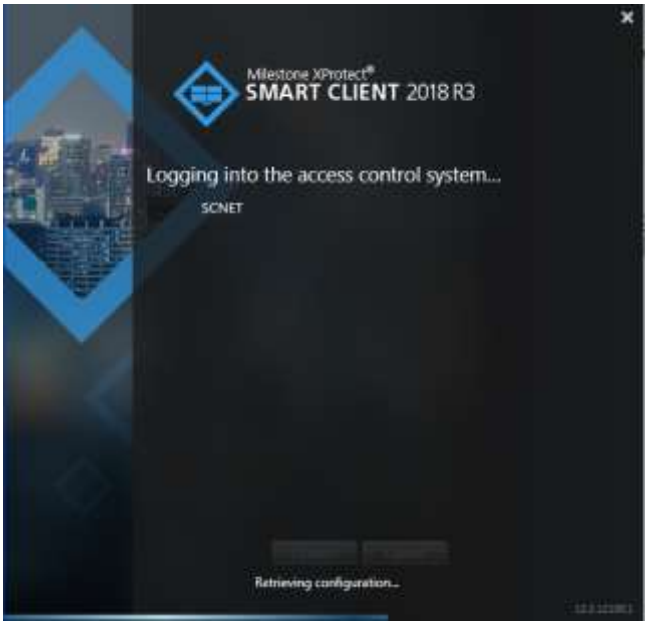

Figure 30: Illustration of a valid connection between Milestone XProtect and the access control system during the XProtect SmartClient initialization process.

2.2.2.3.2 Configuration of live access control events monitoring

It is possible to setup views specifically for the access control system by adding, in “Configuration mode”, one or more “Access monitor” to the “Live” thumbnail.

In order to do so, once in the “Live” thumbnail (1), ensure that the “Configuration” mode (2) is active. Then drag and drop the input “Access monitor” (3) to the part of the window where a display can be placed. This is illustrated in Figure 31.

Once this operation achieved, a window is open to precisely define the content of the access control view. It is first required to select the event source (4) then to select the camera (if several are linked to the source), the events, the commands and the order followed by the display of events as illustrated in Figure 32.

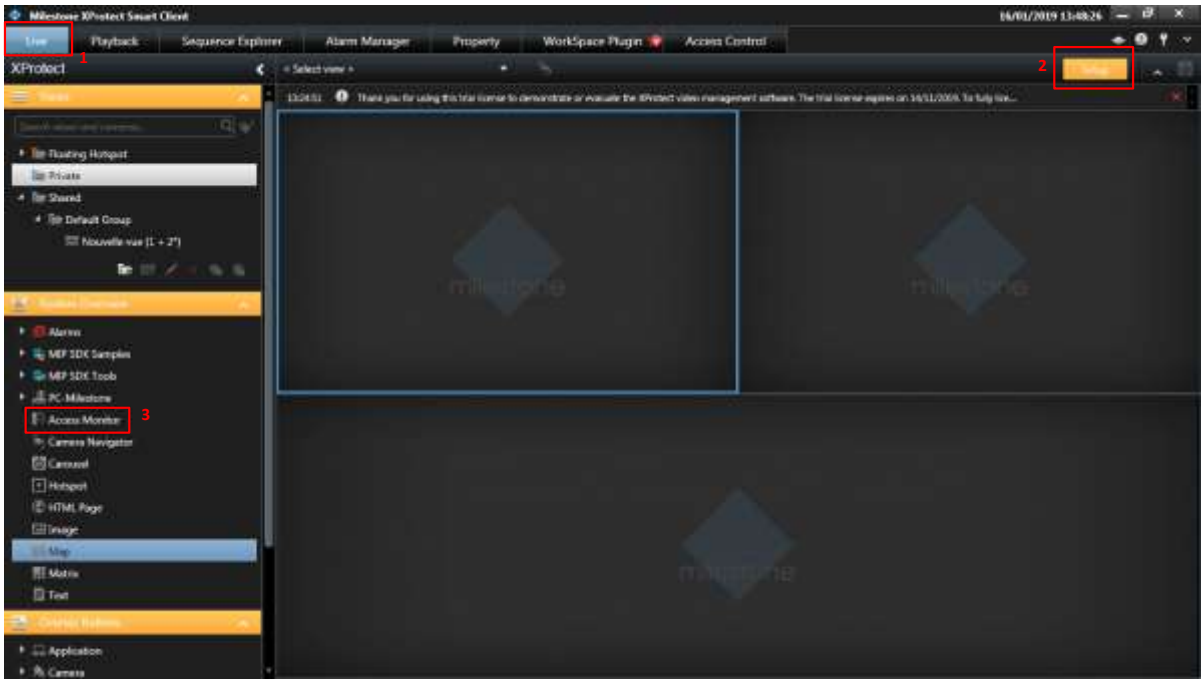

Figure 31: Access control view setup.

Figure 32: Access control view fine tuning

2.2.2.3.3 Map surveillance of the access control events

It is also possible to add access control linked objects in the map view. In order to so, in the “Live” thumbnail(1), activate the “Configuration” mode (2) and then extend the “Global view of the system”. The map selection (3) can then be dragged and dropped in the desired display corner.

A background map compatible with Milestone XProtect can then be added, resized, zoomed or re-centered to the view. By clicking on the right button on the map, a menu appears in which a toolbox can be selected. In this tool box, by clicking the  (3) icon, an edition menu appears providing specific tools for the access control plugin. In this menu, it is possible to list all the object that can appear on a map. Each object can then be selected and dragged to the map. Its symbol is then placed above the background map together with its name.

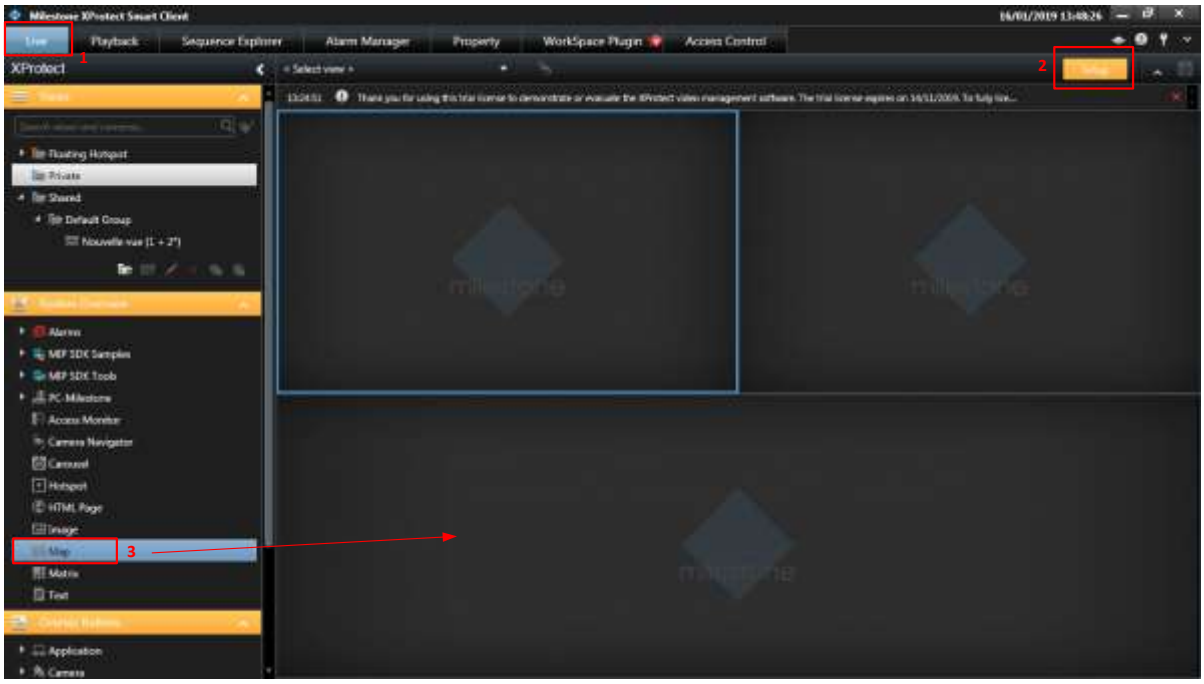

Figure 33: Initialization of the map setup for access control objects

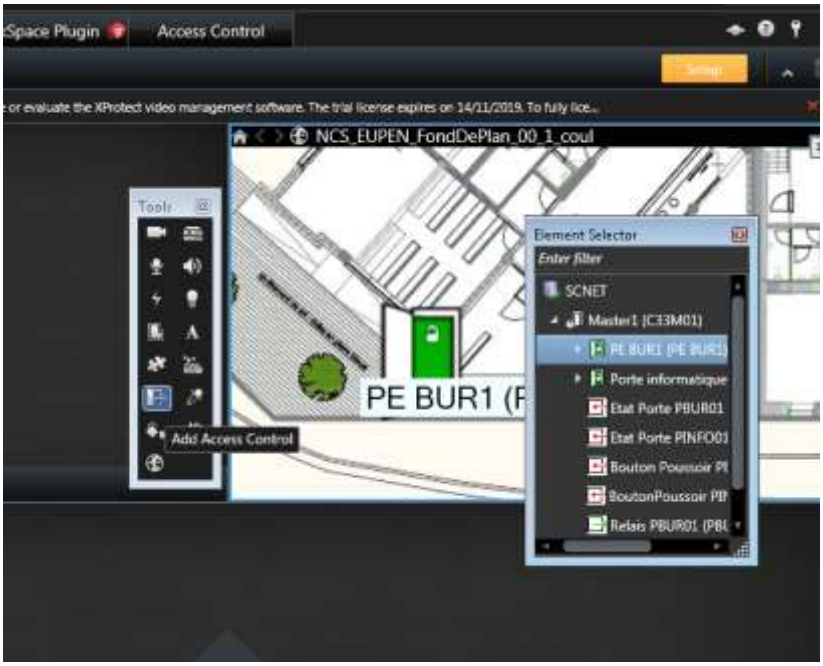

Figure 34: Adding an access control object to the map.

3 PLUGIN OPERATION

The operation of the plugin is directly achieved within Milestone XProtect SmartClient. We refer the reader to the user manual of this tool for information regarding its usage. Le “XProtect Access” section of the manual details the different usage possibilities of access control plugins compatible with Milestone XProtect (such as the XPPLUG addressed in the current manual).

DETAILS REGARDING LICENSE AND TRADEMARKS

NCS®, the NCS® and Scaline® logos are registered trademarks NATIONAL CONTROL SYSTEMS S.A. Scaline® International is a division of NATIONAL CONTROL SYSTEMS S.A. SCNET4™, NET4™, NET4-S™, NET4-C™, SC4x5™, NCDI™, XPPLUG™ and Scabus™ are trademarks of NATIONAL CONTROL SYSTEMS S.A.

XProtect Corporate, XProtect Expert, XProtect Enterprise, XProtect Professional, XProtect Express, XProtect Essential, XProtect NVR, XProtect Go, XProtect clients, XProtect Smart Client, XProtect Web Client, Milestone Mobile, XProtect Analytics, XProtect Access Control Module, XProtect Access, XProtect Retail, XProtect Screen Recorder, XProtect Smart Wall, XProtect Transact, Milestone Husky M10, Milestone Husky M20, Milestone Husky M30, Milestone Husky M30 Hybrid, Milestone Husky M50, Milestone Husky M50 Hybrid, Milestone Husky M50 Advanced, Milestone Husky M500A, Milestone Husky M550A, Milestone Care, SVQR and all associated logos and designs are trademarks or registered trademarks of Milestone Systems.

Aperio is a registered trademark of Assa-Abloy AB.

Microsoft®, Windows® are registered trademarks of Microsoft Corporation in the USA and other countries in the world.

This document is rather and extended view of the functionalities developed in the XPPLUG plugin. NCS® has brought its best attention to the redaction of the document and to the precision of the information it contains. However, this documentation is provided as is and without any guarantee.

NCS® makes no warranties or representations regarding the use or results of this documentation as to its accuracy, reliability, timeliness or otherwise. In the event of a defect in the documentation, it is the holder, and not NCS®, who will bear all the costs necessary for the repair, repair or correction. NCS® cannot be held responsible for any direct, indirect, secondary or incidental damage resulting from the use or inability to use this documentation.

NCS® reserves the right to modify this document without prior notice. Some functions described here are only available in specific models or licenses.
Conformity of the products mentioned in the standards is ensured only if the installation of these products is carried out in compliance with these standards and with the recommendations of NCS®. National rules and standards prevail over these recommendations.

DOCUMENT REVISION HISTORY

Date	Version Doc	Version Plugin	Description
21/01/2019	1.0	1.0	Initial version of the document