

TryggLogin

Multi-factor authentication for XProtect Smart Client



Table of Contents

How it works	3
Install	3
Requirements	3
Server	3
Included dependencies.....	3
Client.....	3
Included dependencies.....	3
Configuration	4
Add user	5
BankID specific.....	5
YubiKey specific	5
Add group	6
Client.....	7
BankID	7
YubiKey	8
Contact	9

How it works

TryggLogin is a Milestone XProtect plugin that enables the users to login to the system using multi-factor authentication. The product comes with two authenticators, [BankID](#) for Swedish residents and [YubiKey](#) OTP.

The system relies on having a “base” role, with rights to only log into the system. The users have no right to view any devices or view groups.

The admin configures all roles as usual but does not add any users or AD groups to them, instead they are connected in the TryggLogin configuration.

When the user initiates a log in to the XProtect system, the TryggLogin client plugin will intercept the login process and display the multi-factor authenticator’s user interface. The Smart Client plugin will communicate with the Event Server and when the multi-factor authentication is complete, the Event Server plugin will add the user to the role(s) defined in the TryggLogin configuration. The Event Server plugin will notify the Smart Client that the user is authenticated, and the Smart Client will proceed as usual. When the Smart Client window is opened, a configuration refresh will be performed to list the devices.

When the user logs out, the Event Server plugin will remove said user from the role(s) in the system.

Install

TryggLogin is split into two parts, one for the server(s) and one for the client.

Requirements

Both the client and the server package require .NET Framework 4.6 or later.

An active internet connection is required on the Event Server machine.

Server

This package is for the Management Client and the Event Server. The plugin needs to be installed on the machines running the Management Client and the Event server.

Install to “C:\Program Files\Milestone\MIPPlugins\TryggLogin Server”.

Included dependencies

- Newtonsoft.Json.dll
- VideoOS.ConfigurationAPI.dll
- YubicoDotNetClient.dll
- TryggLogin.Shared.dll
- TryggLogin.Server.dll

Client

This package is for the Smart Client. This needs to be installed on the user’s PC’s.

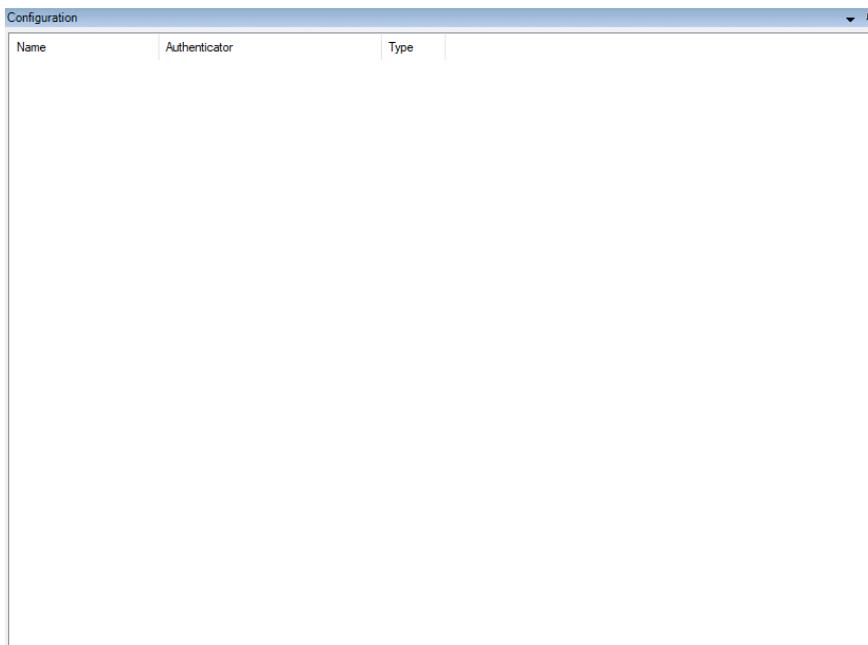
Install to “C:\Program Files\Milestone\MIPPlugins\TryggLogin Client”.

Included dependencies

- Newtonsoft.Json.dll
- TryggLogin.Shared.dll
- TryggLogin.Client.dll

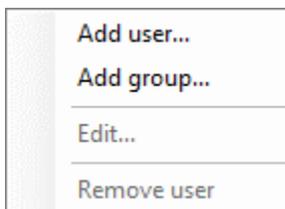
Configuration

The TryggLogin configuration page can be found at the bottom of the Site Navigation, under the MIP Plug-ins branch.



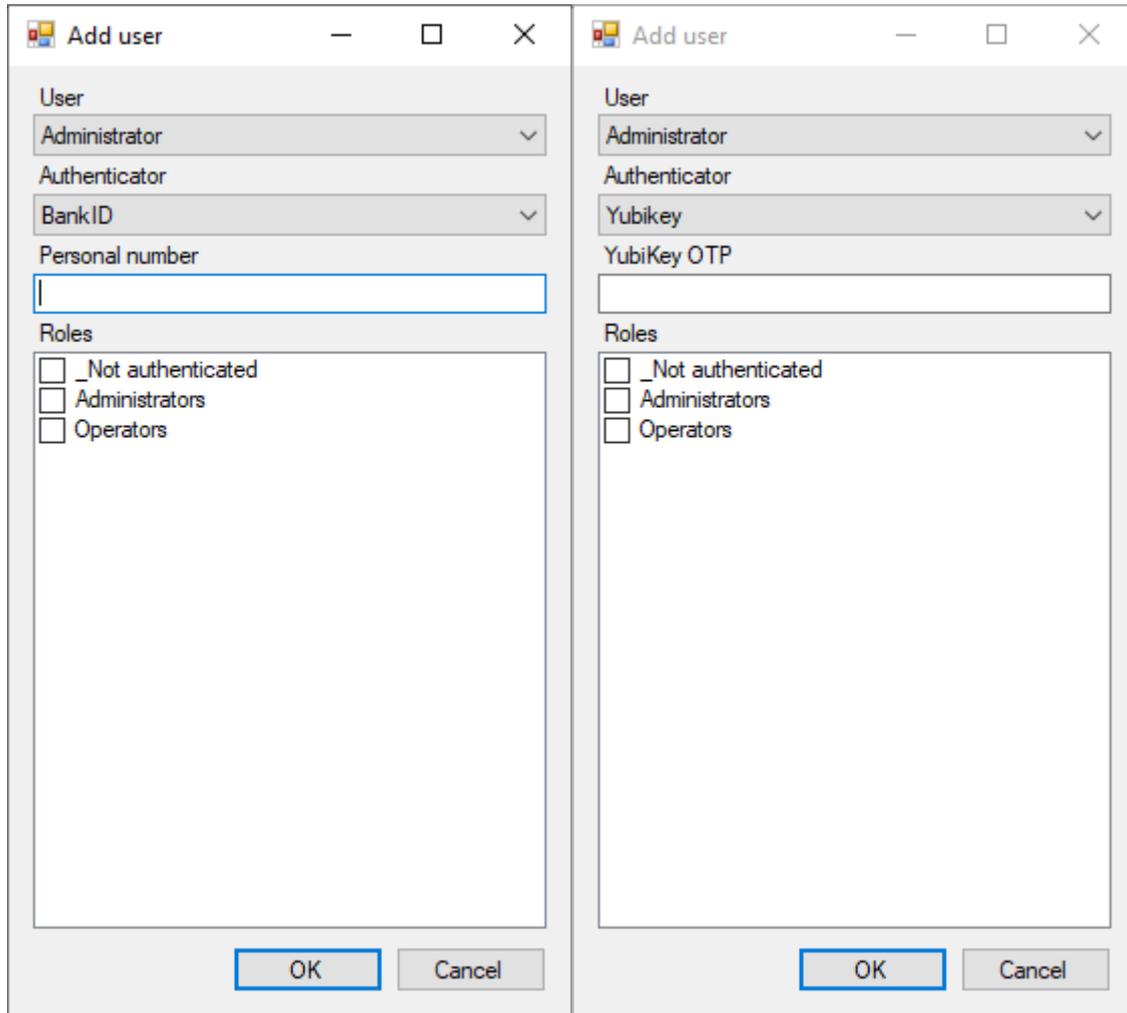
The fastest way to enroll users for **BankID** or **YubiKey** is to create a group in the active directory domain for each role in the XProtect system and have the users Personal Number(BankID) or YubiKey public id in an active directory user property, like "Employee Number" or similar.

To add a user or group to TryggLogin, right click anywhere in the list and choose an option.



Add user

This form adds a single user to the configuration. The Personal Number or YubiKey data is manually set here.



User = The Windows user.

Authenticator = The authenticator the user will use when logging in (max 1 per user).

Personal number/YubiKey OTP (Authentication data) = The data used to verify the multi-factor authentication.

Roles = The selected XProtect role(s) this user will be added to upon a successful log in.

BankID specific

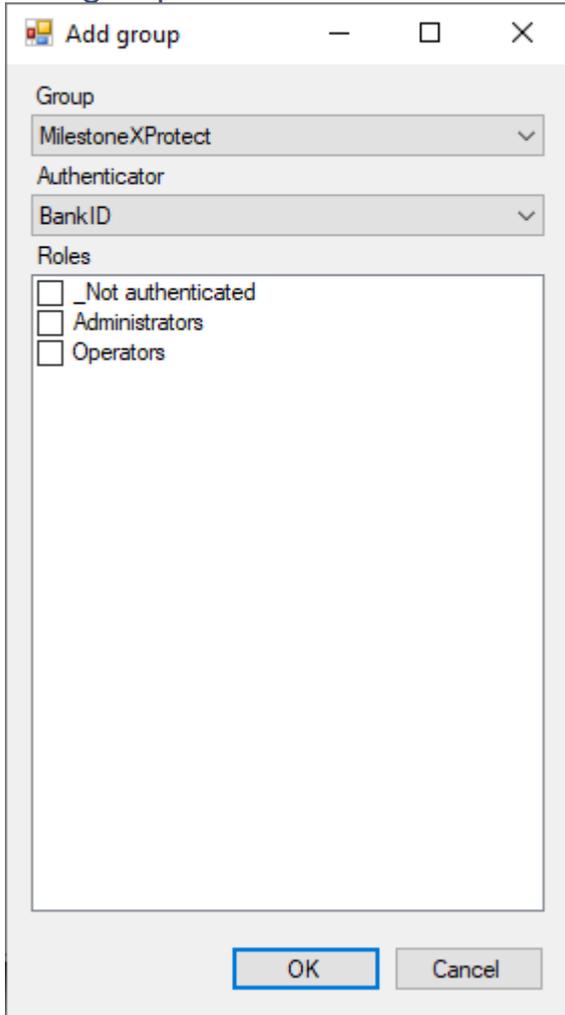
Personal number: The user's private personal number, format YYYYMMDDXXXX (196001011234)

YubiKey specific

YubiKey OTP: The YubiKey must be preconfigured and added to YubiKey servers, test here: <https://demo.yubico.com/otp/verify>

This field accepts the public id (12 characters) or a full OTP string. If a full OTP string is provided, it will be validated against Yubico servers. If the validation is successful, the public id will be saved.

Add group



The screenshot shows a dialog box titled "Add group". It has a title bar with a small icon, the text "Add group", and standard window controls (minimize, maximize, close). The dialog is divided into three sections:

- Group:** A dropdown menu with "MilestoneXProtect" selected.
- Authenticator:** A dropdown menu with "BankID" selected.
- Roles:** A list of three roles, each with an unchecked checkbox:
 - _Not authenticated
 - Administrators
 - Operators

At the bottom of the dialog are two buttons: "OK" and "Cancel".

Group = Windows group (from the local machines or domain if it exists).

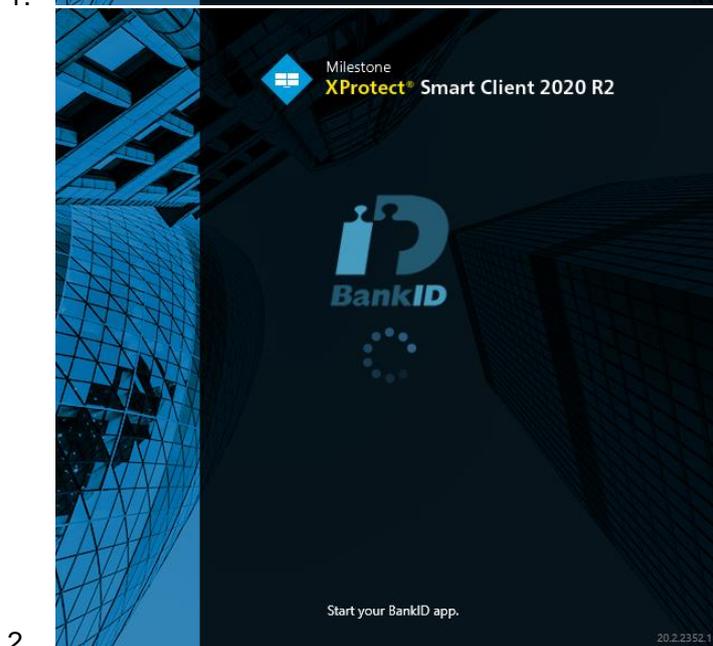
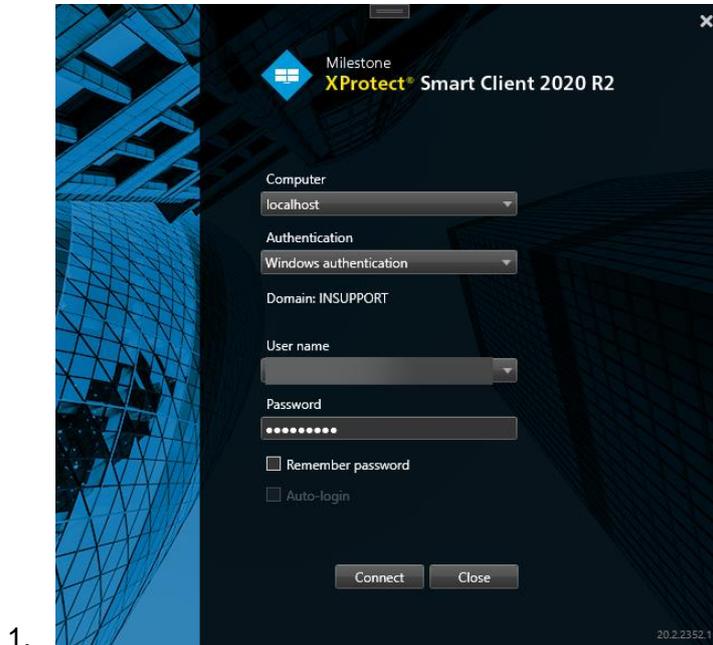
Authenticator = The used authenticator for the users in this group. The personal number or YubiKey OTP will be read from the EmployeeNumber property. This can be changed but [contact InSupport](#) first.

Roles = The roles authorized users will be added to.

Client

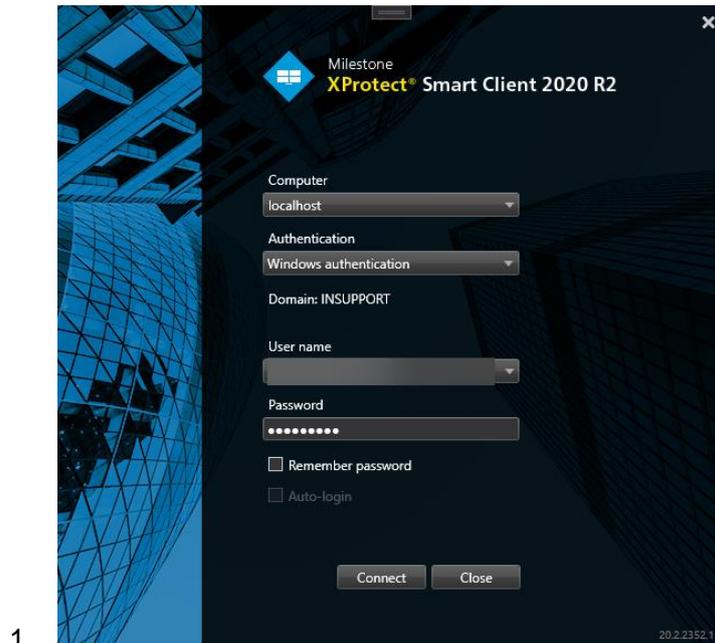
If the Windows user is added to the TryggLogin configuration and have the binary files installed, the Smart Client plugin will intercept the log in process.

BankID



3. The user performs the multi-factor authentication in the BankID app on the user's smartphone.
4. The Smart Client window opens and refreshes the configuration. The log in is complete.

YubiKey



-
-
3. The user inserts the YubiKey in the PC, selects the 'YubiKey OTP' textbox and tap the YubiKey OTP button.
4. The Smart Client window opens and refreshes the configuration. The log in is complete.

Contact

Sales: info@insupport.se

Support: support@insupport.se

Support (phone): +468 459 00 66, 08:00 – 17:00 CET.