

Security Features

For Talk2M PRO Account

APPLICATION NOTE

AUG-0057-00 1.2 en-US ENGLISH

Important User Information

Disclaimer

The information in this document is for informational purposes only. Please inform HMS Industrial Networks of any inaccuracies or omissions found in this document. HMS Industrial Networks disclaims any responsibility or liability for any errors that may appear in this document.

HMS Industrial Networks reserves the right to modify its products in line with its policy of continuous product development. The information in this document shall therefore not be construed as a commitment on the part of HMS Industrial Networks and is subject to change without notice. HMS Industrial Networks makes no commitment to update or keep current the information in this document.

The data, examples and illustrations found in this document are included for illustrative purposes and are only intended to help improve understanding of the functionality and handling of the product. In view of the wide range of possible applications of the product, and because of the many variables and requirements associated with any particular implementation, HMS Industrial Networks cannot assume responsibility or liability for actual use based on the data, examples or illustrations included in this document nor for any damages incurred during installation of the product. Those responsible for the use of the product must acquire sufficient knowledge in order to ensure that the product is used correctly in their specific application and that the application meets all performance and safety requirements including any applicable laws, regulations, codes and standards. Further, HMS Industrial Networks will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features or functional side effects found outside the documented scope of the product. The effects caused by any direct or indirect use of such aspects of the product are undefined and may include e.g. compatibility issues and stability issues.

Table of Contents

Page

1	Preface	3
1.1	About This Document	3
1.2	Document history	3
1.3	Related Documents	3
1.4	Trademark Information	3
2	Introduction.....	4
2.1	Security is the #1 Priority.....	4
2.2	Requirements.....	4
3	Password Management	5
4	Two-Factor Authentication.....	6
4.1	Process	6
4.2	Enable <i>Two-Factor Authentication</i>	8
4.3	Troubleshooting.....	10
5	Users and Permissions	12
5.1	User Rights Management	12
5.2	Permissions and Groups Assignment	12
6	Ewon Access Control	16
6.1	Ewon LAN Side	16
6.2	Gateway Level Access Control	18
6.3	Service Level Access Control	19

This page intentionally left blank

1 Preface

1.1 About This Document

This document addresses the security-related features of eCatcher with a Talk2M PRO account.

.

For additional related documentation and file downloads, please visit www.ewon.biz/support.

1.2 Document history

Version	Date	Description
1.0	2013-12-09	First release
1.1	2015-02-25	Added: 2 Factor Authentication
1.2	2020-05-29	Changed: General content

1.3 Related Documents

Document	Author	Document ID
Talk2m PRO account configuration	HMS	AUG-0028-00

1.4 Trademark Information

Ewon® is a registered trademark of HMS Industrial Networks SA. All other trademarks mentioned in this document are the property of their respective holders.

2 Introduction

The present manual addresses the security-related features of eCatcher with a Talk2M PRO account.

2.1 Security is the #1 Priority

Offering products featuring top-notch security is Ewon's number one priority.

That's why eCatcher, the Talk2M VPN connection utility, embeds tools helping you comply with your corporate IT security policies.

Considering the ongoing challenge of keeping corporate IT security to the level appropriate to your business, it is our duty at Ewon to put the relevant toolbox at your disposal.

eCatcher and Talk2M provide the tools to adapt the level of security to the specific requirements of the infrastructure necessary to establish remote connections to your equipment.

2.2 Requirements

The following requirements are mandatory:

- eCatcher version 5 or higher must be installed on your PC. You can download eCatcher from our www.ewon.biz/support.
- You need a Talk2M Pro account as explained on [Ewon elearning](#) platform.
- The Ewons you want to connect to must run the firmware version 6.1s2 or higher.

3 Password Management

With a Talk2M Pro account, password management is handled in the account's **<Password Policy>**.

The path to the **<Password Policy>** frame is **Account ► Show advanced settings ► Password Policy ► Modify**.

The following frame appears:

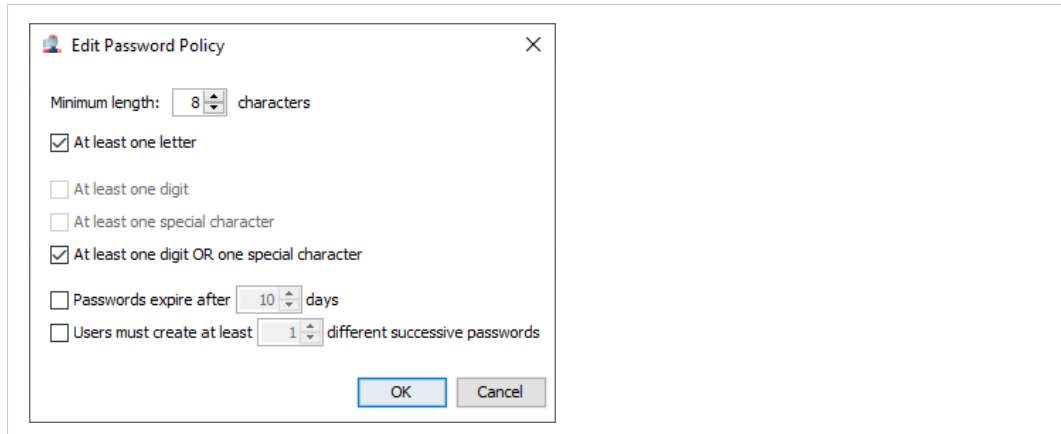


Fig. 1 Password management frame

The following criteria can be forced on a user's password:

- password minimum length (between 6 and 45),
- at least one letter,
- at least one digit,
- at least one special character,
- at least one digit or special character,
- password expiration after a chosen time period,
- number of different successive former passwords

If an administrator changes the password policy, the password of the already existing users remain valid even though the password doesn't meet the new policy.

The new policy applies in the following cases:

- creation of a new user;
- an existing user wants to change his current password;
- the administrator forces a user to change his password on next login.

4 Two-Factor Authentication

To increase the security of your Talk2M account, we strongly recommend activating two-factor authentication.

Two-factor authentication provides unambiguous user identification by means of a combination of two different components.

These two different components are generally something that the user knows and something that the user possesses or that is inseparable from the user.

When it comes to eCatcher and M2Web connections, the second authentication factor involves the mobile phone number of the user.

A text message that contains a one-time-valid, dynamic passcode of 4 digits is sent to the mobile phone.

4.1 Process

If a user has the two-factor authentication enabled, then to log into his account, the user will need to follow this process:

1. Enter the **account name, username** and **password**.

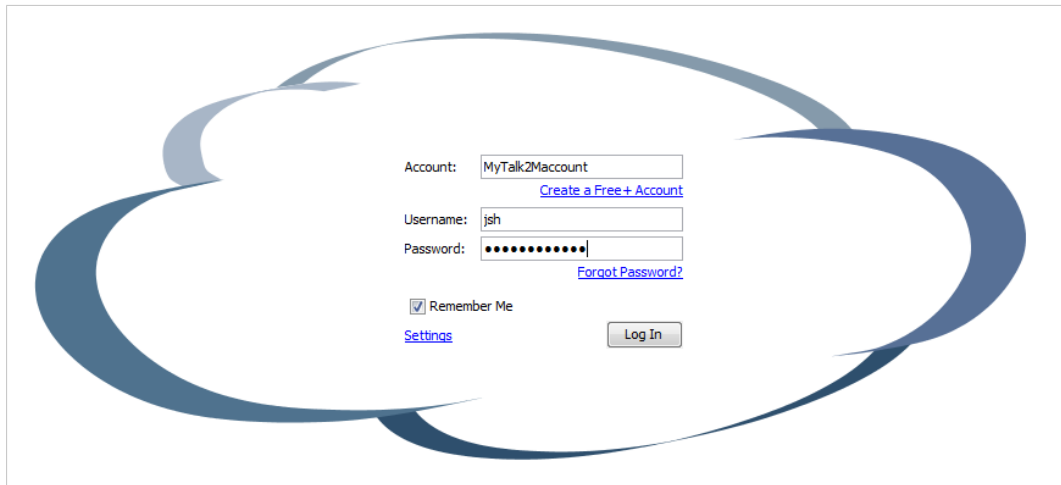


Fig. 2 Login window

The Talk2M system will then send a text message to the mobile phone number stored for this user.

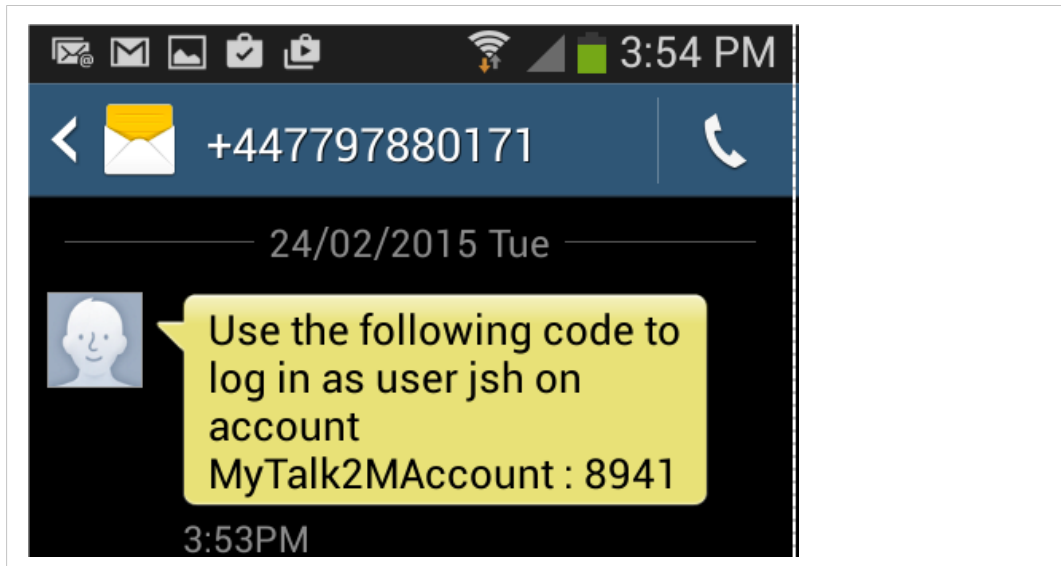


Fig. 3 SMS for 2FA

The text message contains the passcode required for the two-factor authentication.

2. Enter the passcode from the text message in the **Security code** field to complete the login process.

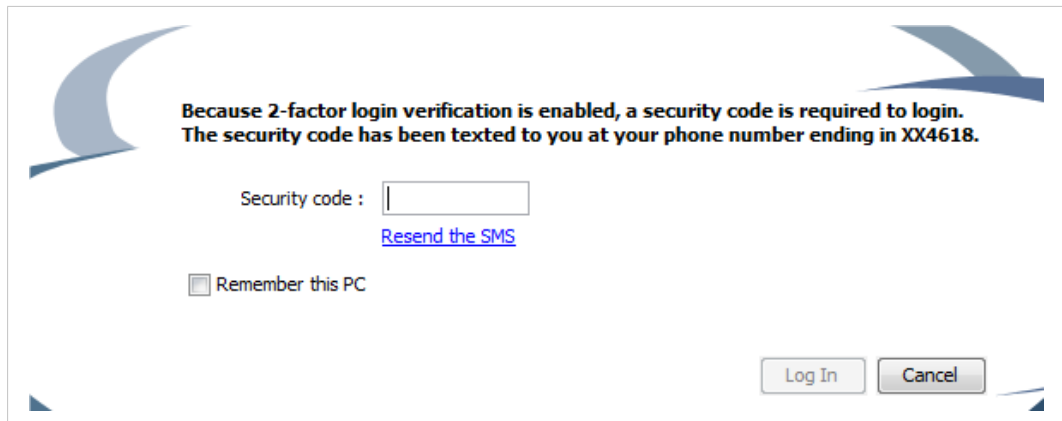


Fig. 4 Enter the security code

You have three attempts to enter the correct passcode otherwise the user login will be blocked for 30 minutes.

4.2 Enable *Two-Factor Authentication*

Inside the account menu, administrators can configure the general settings for two-factor authentication.

The path to the *Two-Factor Authentication* policy is: **Account** ► **Security Policy** ► **Modify 2-Factor authentication policy...**

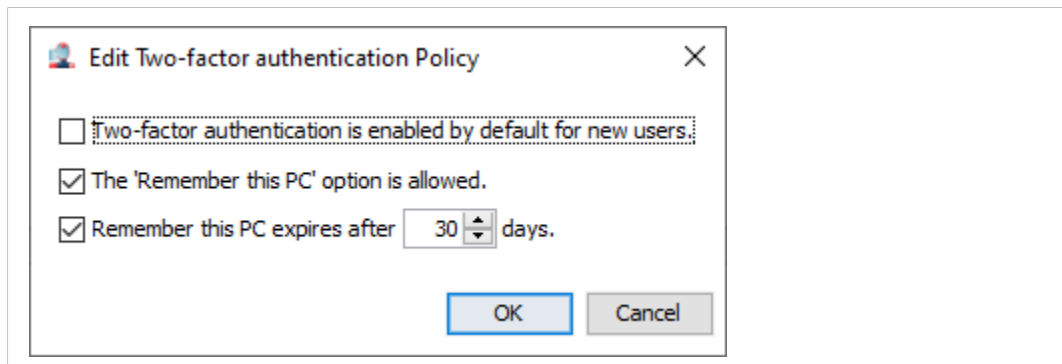


Fig. 5 2FA policy

The options allow you to enable the two-factor authentication for all new users. It also allows you to enable and configure the **<Remember this PC>** option.

For each user of the Talk2M account, administrators can activate and configure the two-factor authentication settings:

Select the user inside the user list and open the properties window: **Users** ► **Properties** ► **Security** ► **Enable Two-factor authentication**

Fig. 6 Configuration of the 2FA user policy

Administrators can decide to encode the mobile number of the user or let the user encode and validate the phone number on the next login.

4.2.1 Backup Number

During the user configuration, you will be asked to enter the mobile phone number of the user for two-factor authentication.

You will also have the possibility to put a backup mobile phone number, which could be used for example in case the first mobile number is not accessible, was lost, or is damaged.

It is strongly recommended to encode a backup mobile phone number for each user.

It is a requirement for users with administrator rights.

4.2.2 <Remember this PC> Option

The <Remember this PC> option allows eCatcher to use your PC instead of the text message as second authentication factor.

During the two-factor authentication login, you can check the <Remember this PC> option when you enters the passcode received on your mobile phone.

Fig. 7 Remember this pc

This allow you to log in the next time from this PC by entering only your username and password. The passcode reception by text message is not required as the PC (a physical object only the user possesses) is not the second authentication component.



DO NOT use the **<Remember this PC>** option if you are connected using another device than your own PC or tablet.

A revoke feature exists for the **<Remember this PC>** option.

An administrator of the account can revoke all **<Remember this PC>** authorizations of a user. This means that the user will need to use the text message as the second authentication component at the next logon.

To revoke the authorization, click the dedicated link on the user properties page.

The administrator of a Talk2M PRO account can decide if the **<Remember this PC>** option is authorized or not for the account.

You can also configure an expiration time for the **<Remember this PC>** feature. This expiration time represents how long before the user must use the passcode by text message again as the second authentication component. For example: if the expiration time is set to 30 days, then a user will need to use, at least every month, the passcode.

4.3 Troubleshooting

SMS not sent

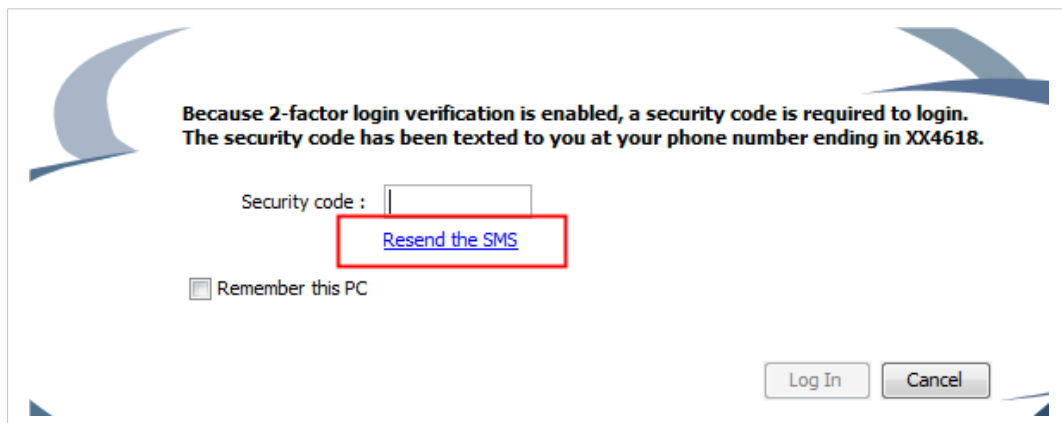


Fig. 8 Resend the passcode

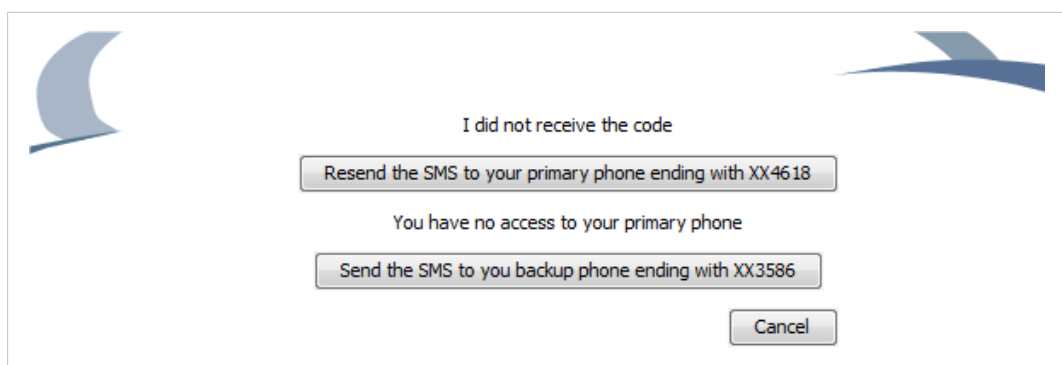


Fig. 9 Choose number to send the passcode

If for some reasons, you did not receive the text message, you can click the **<Resend the SMS>** link.

You can then decide to resend the text message to the same phone number or to send the text message to the backup phone number that was also encoded for the user.

Fees

Security is a top priority for Ewon and Talk2M. That's why the text messages for two-factor authentication are free of charge.

However, we reserve the right to contact the administrator of the Talk2M account in case of abuse.

5 Users and Permissions

5.1 User Rights Management

With a Talk2M PRO account, user permissions are based on the user **Groups** which the user belongs to, the **Roles** associated with that **Groups** and the access rights granted to those **Groups** for different **Groups** of Ewons.

- A **User** always belongs to at least one **Group**.
- An **Ewon** is always included in at least one **Pool**
- Every **Group** has at least one **Role**
- The **Roles** assigned to a **Group** define the permissions of the **Users** belonging to this **Group**

To create **Groups** or **Pools** and assign **Roles**, please refer to Talk2m PRO account configuration from the [Related Documents, p. 3](#).

5.2 Permissions and Groups Assignment

5.2.1 New User

You can configure user properties when adding a new user.

The path to the New User wizard is: **Users >> Add**.

A wizard appears to help you create a user:

1. Enter the information of the user you want to create

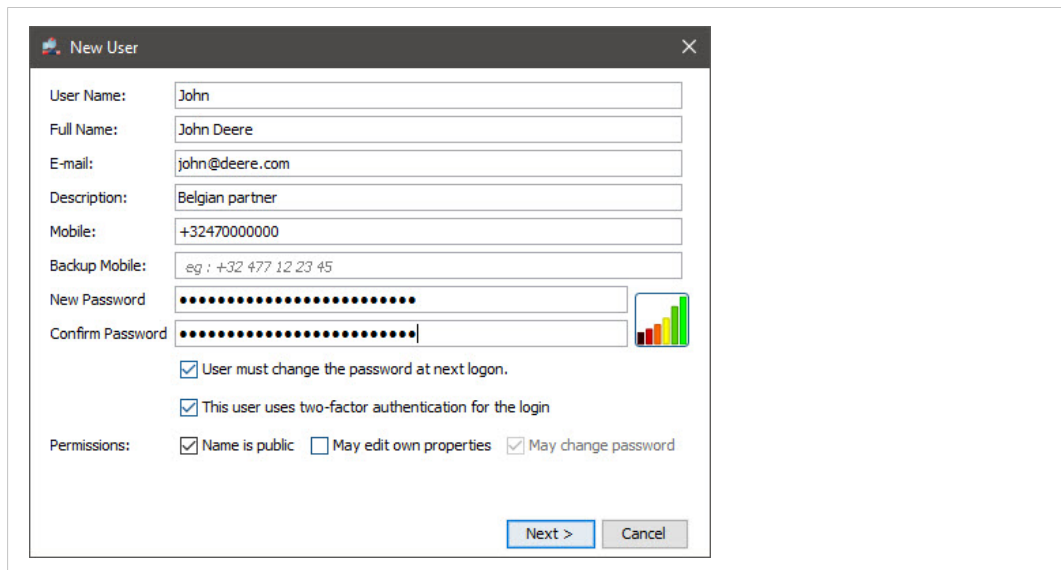


Fig. 10 User creation



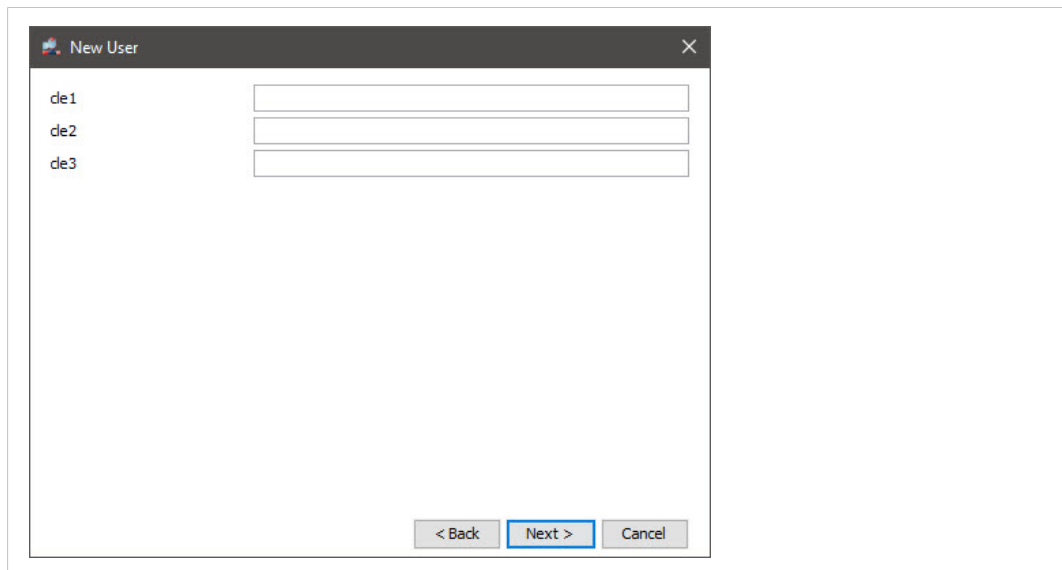
When entering your new password, a password strength gauge helps you rate the password you intend to use. This indicator is not linked with the password enforcement policy described earlier.

The administrator creating a new user can check the following check-boxes:

- **User must change the password at next logon** is usually checked when the administrator assigned a password for the user.
- **This user uses two-factor authentication for the login** if the user must use the 2FA to log in to the Talk2M account.
- **Name is public** is the ability to make the name of the connected user public. This option, if checked, will make the user name visible to other logged users of the account in the **<connected user>** column of the Ewon list.
- **May edit own properties** allows the user to change properties such as his own name, email, and password. It does not give the user rights to modify his own permissions.
- **May change password** allows the user to change his password.

2. Click **Next** .

3. Complete the custom fields

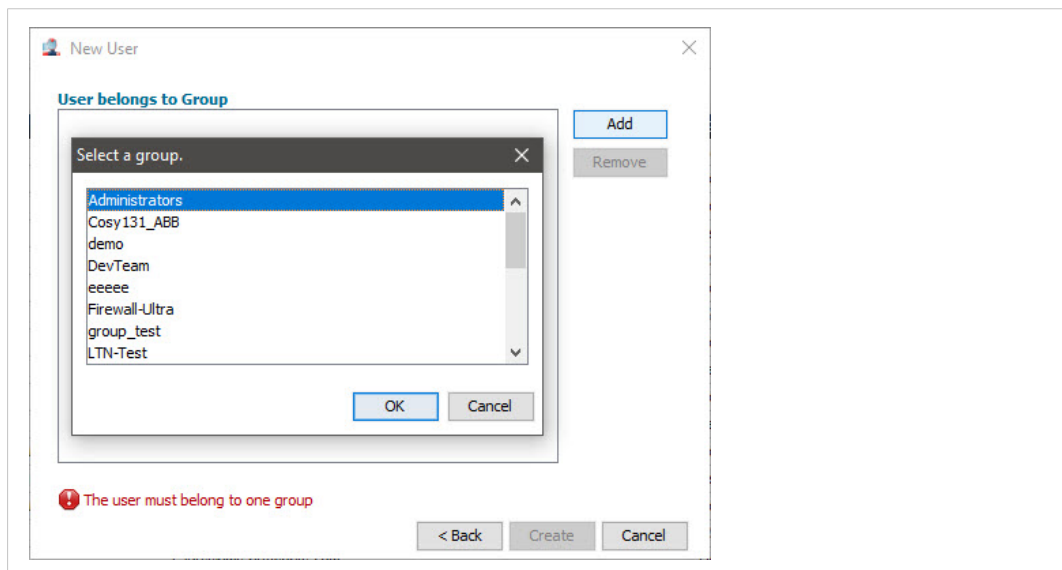


The screenshot shows a 'New User' dialog box with three input fields labeled 'de1', 'de2', and 'de3'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

Fig. 11 Custom Fields for a user

4. Click **Next**.
5. Assign a group to the user.

For a Talk2M PRO account, a user can be assigned to one or more groups. The user will assume the roles associated to those groups.



The screenshot shows the 'New User' dialog box with the 'User belongs to Group' section. A 'Select a group.' dialog box is open, displaying a list of groups: Administrators, Cosy131_ABB, demo, DevTeam, eeeee, Firewall-Ultra, group_test, and LTN-Test. The 'Add' button is highlighted. Below the dialog box, there is a red warning icon and the text 'The user must belong to one group'. At the bottom of the main dialog box, there are three buttons: '< Back', 'Create', and 'Cancel'.

Fig. 12 Group assignment for a user

6. Click **Create**.

5.2.2 Existing User

Administrators can modify an existing user's permissions from the [<Edit User Permissions>](#) frame.

The path is: **Users >> Properties ▶ Permissions and Groups ▶ Modify.**

5.2.3 Disable or Delete User

An administrator can temporarily block the access of a user with an existing profile and password without deleting the user, for example for a planned leave or during a job rotation.

The path to temporarily disable a user is: **Users ▶ Select user from list ▶ Properties ▶ Disable.**

The user properties background becomes dark gray to show that the user is currently disabled.

To re-enable a disabled user, simply repeat the process by clicking on **Enable**.

If the administrator wants to permanently block the access of a user, follow the path: **Users ▶ Select user from list ▶ Properties ▶ Delete..**

6 Ewon Access Control

Within a Talk2M PRO account, user permission to access an Ewon is managed indirectly by the **<Groups>** which a user belongs to.

<Groups> have (or don't have) access based on the Group's **<Roles>** (permissions) on a given **<Pool>**.

Please refer to Talk2m PRO account configuration from the *Related Documents, p. 3* for more information on **<Groups>**, **<Pools>**, and **<Roles>**.

This type of configurable protection offers an additional security-layer to the user permission management on the Ewon itself.

6.1 Ewon LAN Side

One of the key features in eCatcher is the ability to create LAN dependencies behind the Ewons and to protect the network including these dependencies through a firewall.

6.1.1 LAN Device Access Control

To configure the LAN dependencies and enable the firewall, the path is: **Ewons** ► **Select Ewon from list** ► **Properties** ► **LAN & Firewall** ► **Configure LAN devices**.

On the **Devices & Firewall** frame, the following appears:

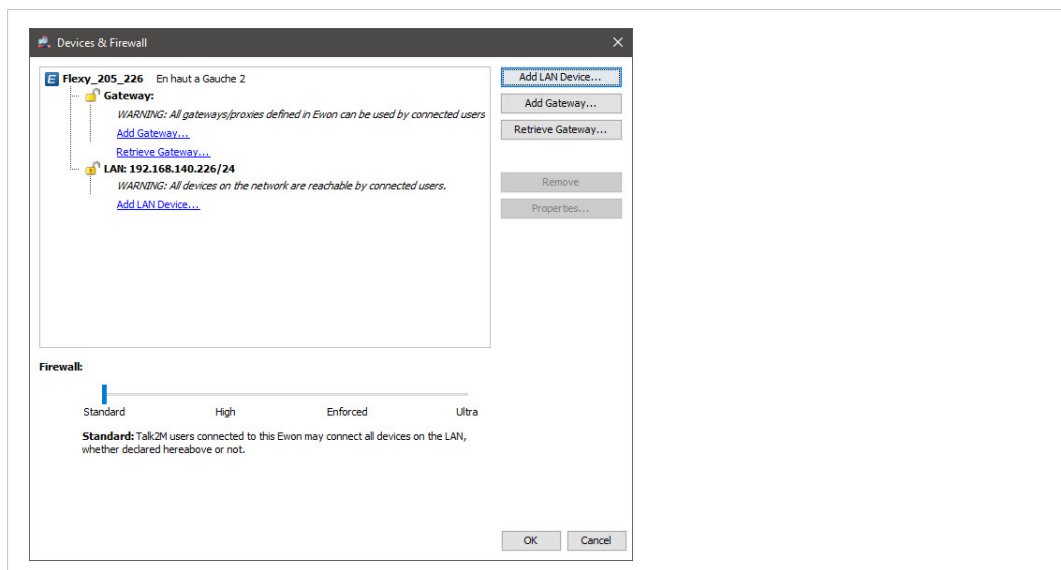


Fig. 13 Device & Firewall of an Ewon

Click on **<Add LAN device...>** to open the LAN Device page.

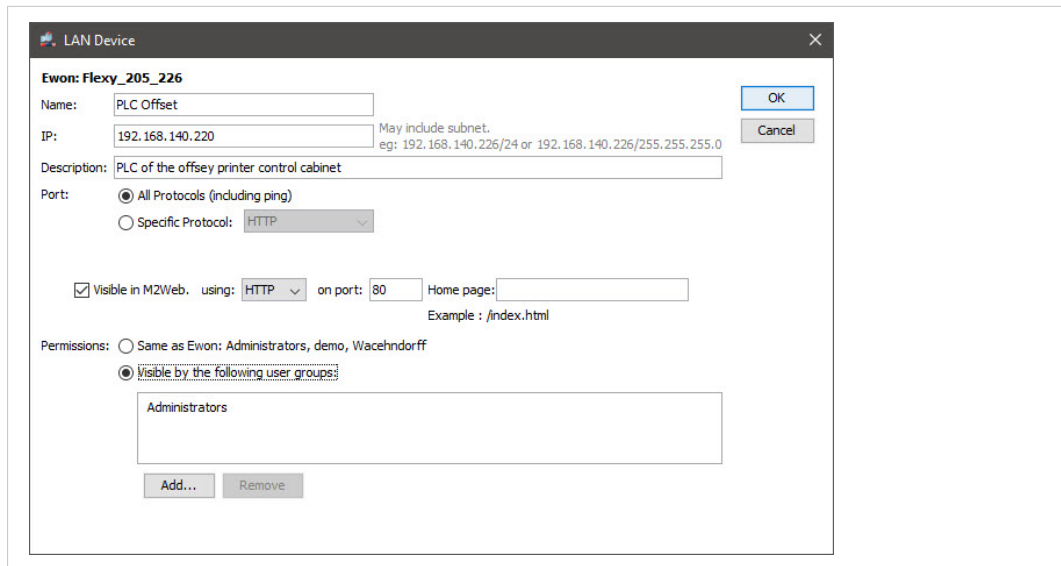


Fig. 14 Add a LAN device

Administrators can give a name to the LAN device, specify its IP address, provide a description and select if all ports are open or only protocol-specific ports.

Administrators can also define whether this particular LAN dependency will be **Visible in M2Web**. M2Web is the secure mobile web access using the Talk2M infrastructure. When the option is checked, the corresponding LAN device appears in the dependency list below the Ewon on the M2web platform.

In the **<Permissions>** area, administrators can define which user group(s) is/are allowed to connect to this device. For each LAN device configured, the user group permissions can be set at **Same as Ewon** or **Restrict to the following user groups**.

When you add a LAN device, the **<firewall slider>** automatically shifts to position **High**.

The new LAN device appears with a closed padlock under the structure of the relevant Ewon in the **<Active Connection>** zone when a user is connected through eCatcher.

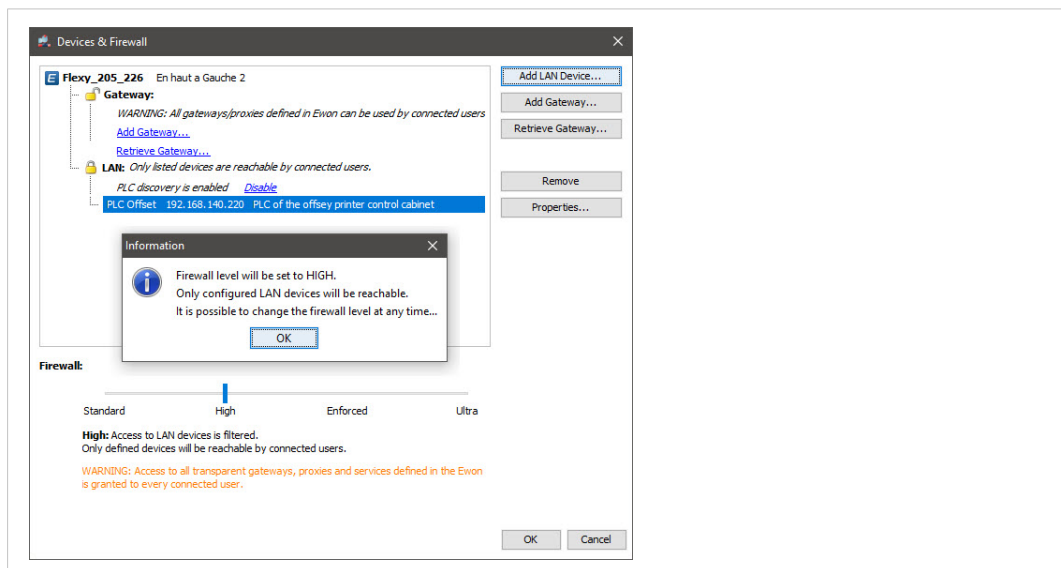


Fig. 15 Firewall state: high

6.2 Gateway Level Access Control

On a Talk2M PRO account, administrators can control which gateways are accessible.

The path to the Gateway creation is the same as for LAN devices: **Ewons** ▶ **Select Ewon from list** ▶ **Properties** ▶ **LAN & Firewall** ▶ **Configure LAN devices**.

On the **<Devices & Firewall >** page, click on **Add gateway**.

The gateway page opens:

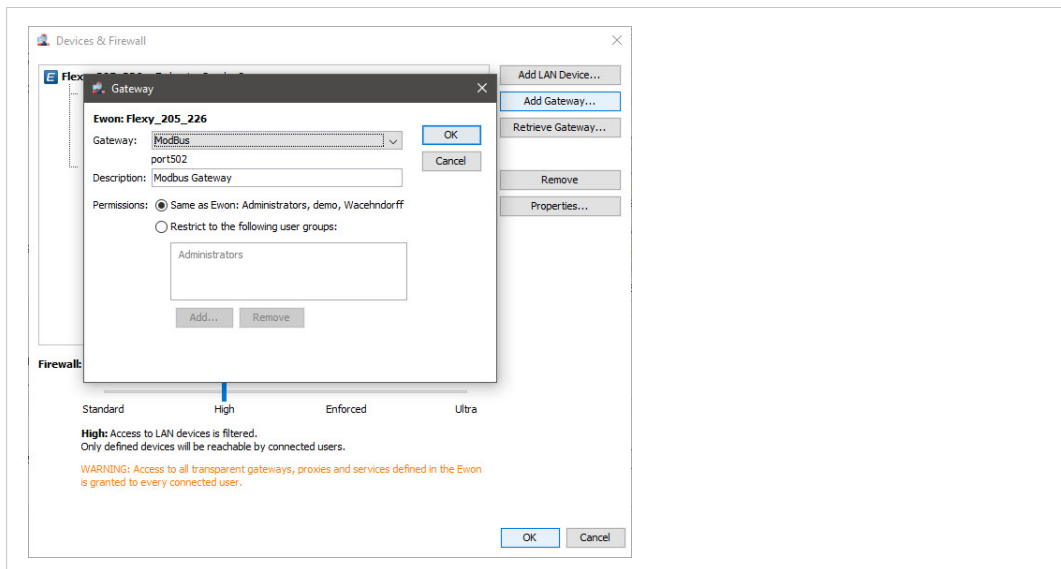


Fig. 16 Gateway addition

Select the relevant Gateway from the drop down list.

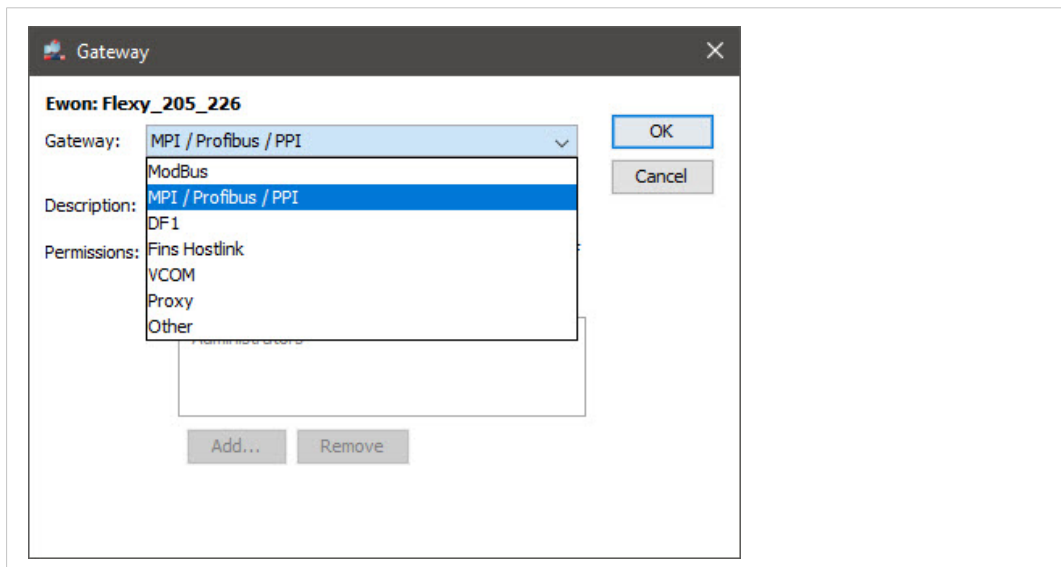


Fig. 17 Select gateway

Depending on the selected gateway, a **Customize** link may allow administrators to configure another port number than the default one.

If the gateway is a proxy, the interface is slightly different:

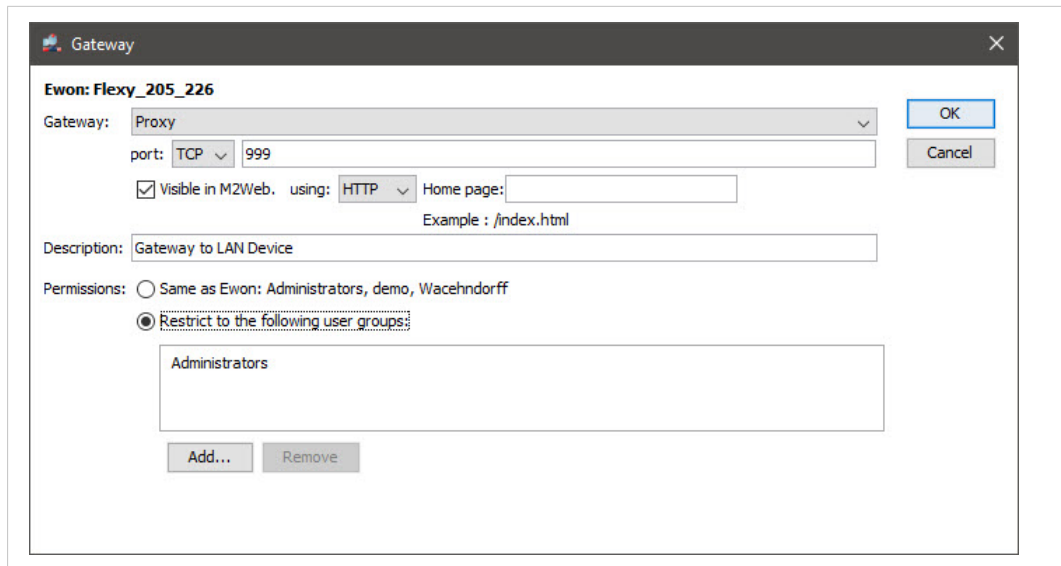


Fig. 18 Gateway is a proxy

The port can be set to either **UDP** or **TCP** and administrators can select whether the gateway should be visible in M2Web.

In the **<Permissions>** area, administrators can define which user group(s) is/are allowed to connect to this device. For each LAN device configured, the user group permissions can be set at **Same as Ewon** or **Restrict to the following user groups**.

When you add a LAN device, the **<firewall slider>** automatically shifts to position **Enforced**.

The new gateway appears with a closed padlock under the structure of the relevant Ewon in the **<Active Connection>** zone when a user is connected through eCatcher.

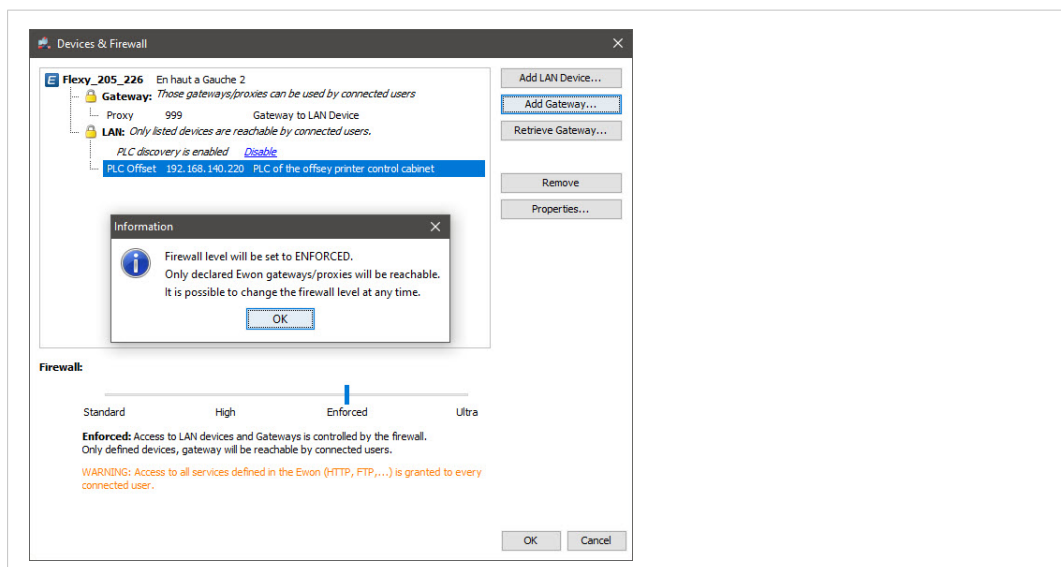


Fig. 19 Firewall state: enforced

6.3 Service Level Access Control

On a Talk2M PRO account, administrators can control which **Services** on the Ewon itself are accessible.

The path to the Ewon services creation is the same as for LAN devices or gateways: **Ewons ▶ Select Ewon from list ▶ Properties ▶ LAN & Firewall ▶ Configure LAN devices.**

Push the **<firewall slider>** to **Ultra** in order to show the **<Edit Services>** button.

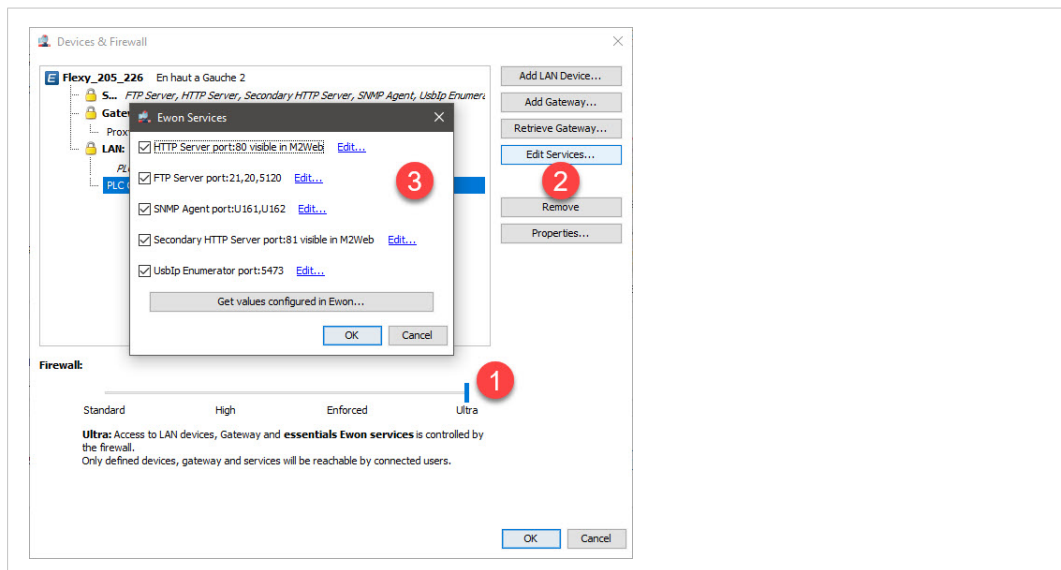


Fig. 20 Ewonservices modification

Click **Edit services** to display the Ewon services frame.

In this window, administrators can open single or multiple ports specifically for a service.

The available services include:

- Primary HTTP server
- FTP server
- SNMP agent
- Secondary HTTP server
- USB starting port number

The specific values that have been configured in the Ewon can be retrieved by clicking on the **Get values configured in Ewon** button.

However, to retrieve values from the Ewon, the Ewon must be online and you must have appropriate login credentials for the Ewon itself.

This page intentionally left blank

