

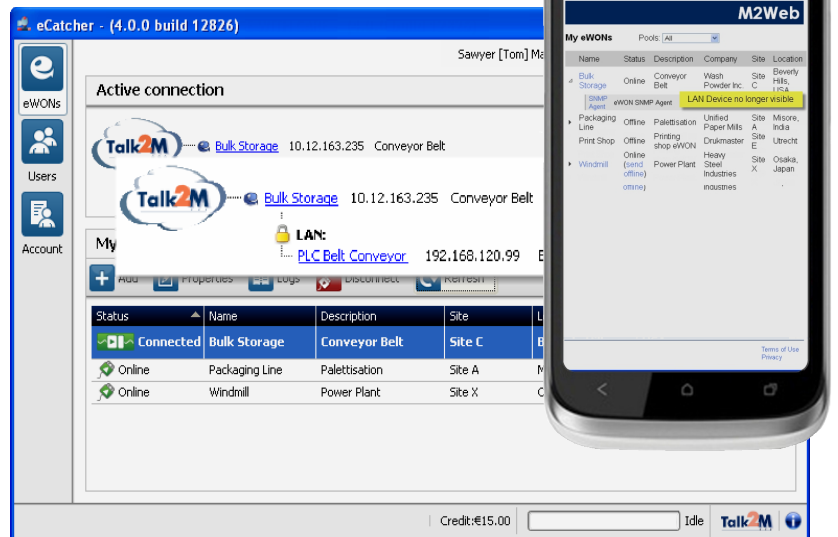


Application User Guide

AUG 056 / Rev. 1.1

eCatcher - Security Features with a Talk2M Free+ Account

This application guide describes the security features of eCatcher 5 with a Talk2M Free+ account.



The image shows a desktop browser window displaying the eCatcher (4.0.0 build 12826) interface. The interface includes a sidebar with 'eWONs', 'Users', and 'Account' sections. The main content area shows an 'Active connection' section with Talk2M logos and IP addresses (10.12.163.235) for 'Bulk Storage' and 'Conveyor Belt'. Below this is a 'My' section with a 'LAN' connection to 'PLC Belt Conveyor' (192.168.120.99). A table at the bottom lists device status:

| Status | Name | Description | Site |
|-----------|----------------|---------------|--------|
| Connected | Bulk Storage | Conveyor Belt | Site C |
| Online | Packaging Line | Palettisation | Site A |
| Online | Windmill | Power Plant | Site X |

Next to the desktop window is a smartphone displaying the 'Talk2M M2Web' app. The app shows a 'My eWONs' section with a table of devices:

| Name | Status | Description | Company | Site | Location |
|----------------|----------------------|--------------------|------------------------|--------|--------------------|
| Bulk Storage | Online | Conveyor Belt | Wash Powder Inc. | Site C | Beverly Hills, USA |
| Packaging Line | Offline | Palettisation | Unified Paper Mills | Site A | Mysore, India |
| Print Shop | Offline | Printing shop eWON | Drummaster | Site E | Utrecht |
| Windmill | Online (and offline) | Power Plant | Heavy Steel Industries | Site X | Osaka, Japan |



Table of Contents

- 1. General Information 3**
 - Scope 3
 - Reference documents 3
 - Software Requirements 3
- 2. Security is #1 Priority 4**
 - For Us 4
 - And for You! 4
 - Talk2M Free+ vs Pro Account 5
- 3. Security Policy 6**
- 4. Two Factor Authentication 8**
 - In practice, how does it work ? 8
 - What if the user does not receive the text message ? 10
 - Will the text messages be charged? 10
 - Backup mobile phone number ? 11
 - What is the "Remember this PC" option ? 11
- 5. Users and Permissions 13**
 - User Groups and Respective Permissions 13
 - Assigning Permissions and Groups 13
 - Disabling and Deleting a User 16
- 6. eWON Access Control 18**
- 7. LAN Device Access Control 19**
- Revision 23**
 - Revision History 23

1. General Information

Scope

The present manual addresses the security-related features of eCatcher 5 with a **Talk2M Free+** account.

Reference documents

Click on the hyperlink to download the relevant document.

- [R1] [AUG-034-0-EN-\(Talk2M – Getting started on Service Free+\)](#)
- [R2] [AUG-057-0-EN-\(eCatcher 5 - Security Features with a Talk2M Pro Account\)](#)

Software Requirements

- eCatcher version 5 or higher must be installed on your PC. You can download eCatcher 5 from our support website <http://support.ewon.biz>.
- You need to have created your Talk2M free+ account as explained in [R1].
- The eWONs you want to connect to need to have firmware version 6.1 s2 or higher.

2. Security is #1 Priority

For Us

Offering products featuring top-notch security is eWON's number one priority. That's why eCatcher 5, our Talk2M VPN connection utility, has tools that will help you to comply with your corporate IT security policies.

In addition to the security features described in this document at the eCatcher level, there are numerous security features included in the eWON itself :

- Password protected Web & FTP access
- Configurable user permissions (10 topics)
- Configurable WAN traffic control
- Configurable traffic forwarding
- Configurable allowed VPN source-IPs and target-IPs, including port definition
- Configurable IP-Services ports
- Encryption of sensitive data (option)
- Password protected reconfiguration of IP address (option)
- Configurable static routing
- Etc...

For more information about these eWON features, see <http://support.ewon.biz>

And for You!

Considering the ongoing challenge of keeping corporate IT security to the level that is appropriate to YOUR business, it is our duty at eWON to put the relevant toolbox at your disposal. eCatcher 5 and Talk2M provide you the tools to customize the level of security to the specific requirements of the infrastructure used to make remote connections to your equipment.

Talk2M Free+ vs Pro Account

The current document covers eCatcher 5 in combination with a Talk2M Free+ account. Another document covers the added features available with a Talk2M Pro account, see [\[R2\]](#). Additional security features include:

- More password policy options
- Restricted access at the gateway and service levels
- Access control for user groups and eWON pools

- Good to know -

The differences in features between the Free+ and Pro accounts are managed at the Talk2M level. The eCatcher application remains the same. Depending on the connected account, eCatcher shows or hides the corresponding features on the interface. This means you don't need to install new software when you upgrade your Free+ to a Pro account.

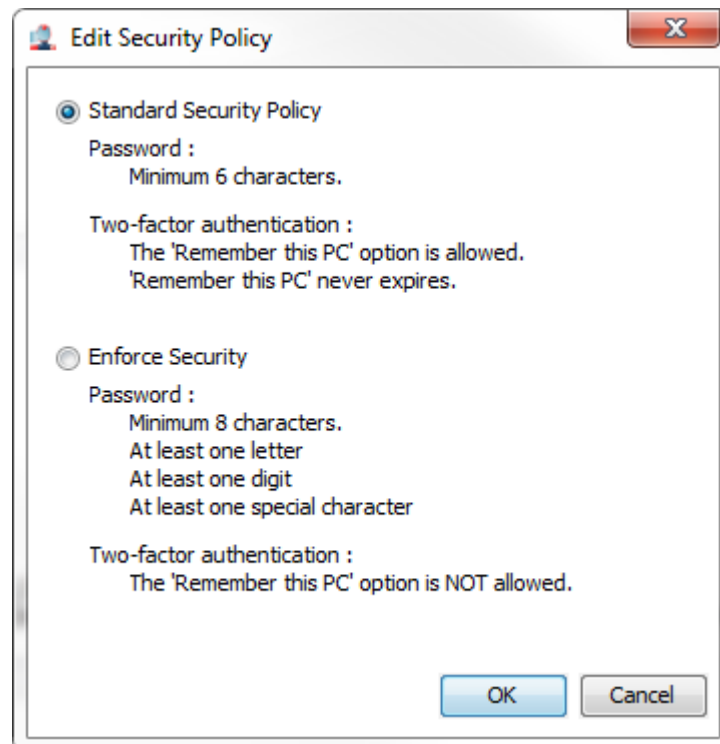
3. Security Policy

With a Talk2M Free+ account, an admin user can choose between a **Standard** or an **Enforced** security policy. This is defined at the account level for all users including admin user(s).

The path to the **Security Policy** popup is:

Account > Show advanced settings > Password Policy > Modify...

The following popup appears:



If **Standard** is selected, the sole constraint for the password, is that it must be at least 6 characters long. This (default) selection should be used only if the exposed risks in case of intrusion by a fake user are negligible.

Using the Standard Security Policy, the “Remember this PC”¹ option of the Two-factor authentication is enabled and does not expire automatically.

If **Enforced** is selected, all passwords of the account will have to meet 4 different criteria: length of minimum 8 characters including at least one letter, one digit and

¹ See the ['What is the “Remember this PC” option ?'](#) section for more information.

one special character. Example: `Brasil2014%` has 11 characters, out of which 6 letters, 4 digits and 1 special character.

Using the Enforced Security Policy, the “Remember this PC”² option of the Two-factor authentication is not allowed.

- Important -

If an admin user changes the Password Policy from Standard to Enforced while users have already been created under the Standard policy, their existing passwords remain valid in spite of the fact they do not meet the new policy. The new policy will apply only to new users or if the existing user wants to change his password.

The Talk2M Pro account offers more password policy management options. For more information, see [\[R2\]](#).

² See the ['What is the “Remember this PC” option ?'](#) section for more information

4. Two Factor Authentication

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

Two-factor authentication provides unambiguous user identification by means of the combination of two different components. These two different components are generally something that the user knows and something that he possesses (or that is inseparable from him).

When it comes to eCatcher and M2Web connections, the second authentication factor will involve the mobile phone of the user. A text message that contains a one-time-valid, dynamic passcode consisting of 4 digits will be sent to the cell phone.

In practice, how does it work ?

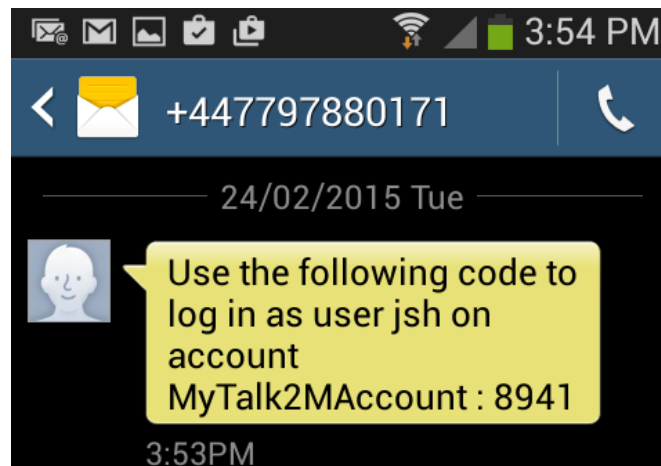
If the two-factor authentication is enabled for a user, then to log into his account, the user will first need to encode his username and password.



The image shows a login form for a Talk2M account, enclosed in a blue cloud-like shape. The form contains the following fields and elements:

- Account: MyTalk2Maccount
- Username: jsh
- Password: [masked with dots]
- Remember Me: Remember Me
- Buttons: [Settings](#), [Log In](#), [Create a Free+ Account](#), [Forgot Password?](#)

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



The text message contains the passcode required for the two-factor authentication. To complete the login process, the user will need to enter that passcode inside the Security code field.

Because 2-factor login verification is enabled, a security code is required to login. The security code has been texted to you at your phone number ending in XX4618.

Security code :

[Resend the SMS](#)

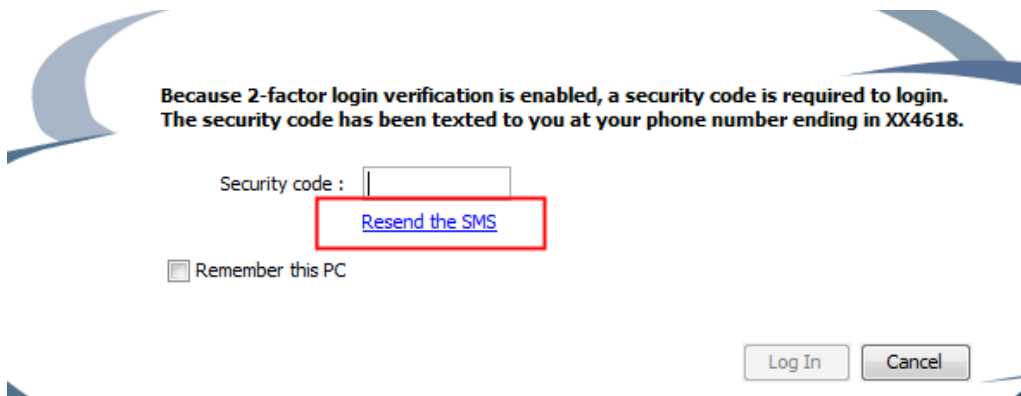
Remember this PC

- Note -

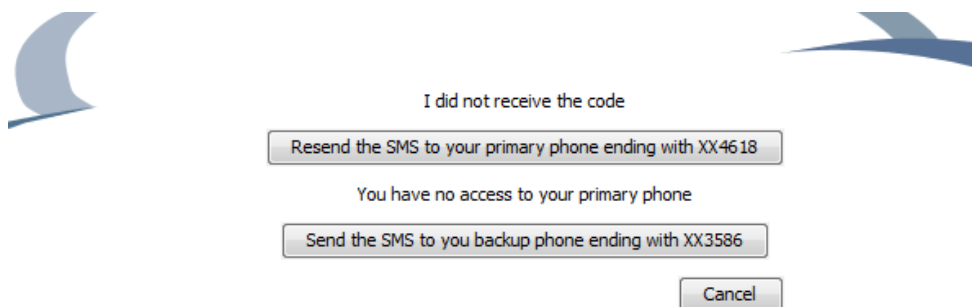
The user has 3 attempts to encode the correct passcode, otherwise the user login will be blocked for a certain period (30 minutes).

What if the user does not receive the text message ?

If for some reason the user did not receive the text message, he can click on the "resend the SMS" link.



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



Will the text messages be charged?

Security is a top priority for eWON and Talk2M. That's why the text messages for the two-factor authentication will be free of charge. However we reserve us the right to contact the administrator of the Talk2M account in case of abuse.

Backup mobile phone number ?

During the user configuration, you'll be asked to encode the mobile phone number of the user for the 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 phone is not accessible, was lost or is damaged.

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

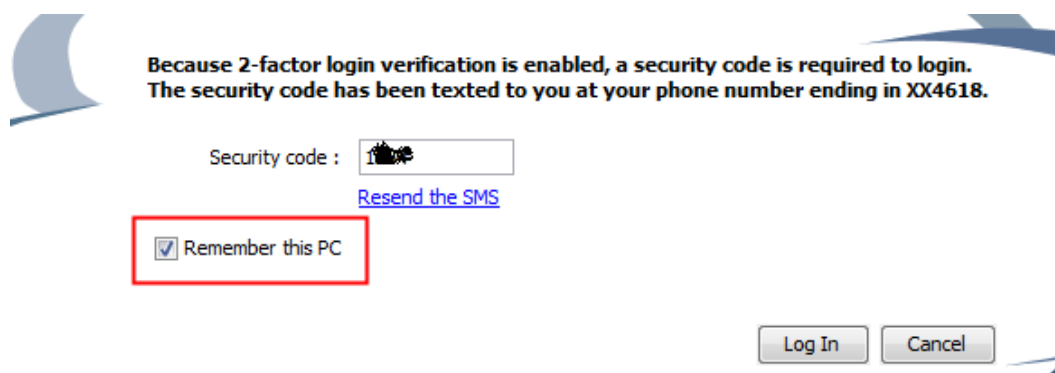
- Note -

For users with administrator rights it is a requirement to encode the backup mobile phone number.

What is the “Remember this PC” option ?

The “Remember this PC” option allows eCatcher to use the PC of the user instead of the text message for the second authentication factor.

During the two factor authentication login, the user can check the “Remember this PC” option when he writes the passcode received on his mobile phone.



Because 2-factor login verification is enabled, a security code is required to login.
The security code has been texted to you at your phone number ending in XX4618.

Security code :

[Resend the SMS](#)

Remember this PC

This will allow him to login the next time from this PC by entering only the username and password. The passcode reception by text message is not required anymore as his PC (a physical object only he possesses) is now the second authentication component.

- Important -

*Do NOT use the "Remember this PC" option, if you are not connected using your own PC or tablet.
The "Remember this PC" option is not available if the Enforced Security Policy has been selected for the Talk2M account.*

- Note -

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 once again the text message as second authentication component at the next logon. To revoke the authorizations click on the dedicated link on the user properties page.



5. Users and Permissions

User Groups and Respective Permissions

With a Talk2M Free+ account, the admin user creating a new user can assign this user either to the group **Administrators** or to the group **Users** depending on the operational role this user will have.

Members of the **Administrators** group can:

- View/edit the account information, including custom fields and security policy.
- Add/view/edit/delete/disable users
- Enable/disable the two factor authentication for each user.
- Add/view/edit/configure/delete/disable eWONs
- Connect to all eWONs created in the account

Members of the **Users** group can:

- View own user properties
- Edit own user properties (if granted permission by administrator)
- *Connect to all eWONs created in the account*

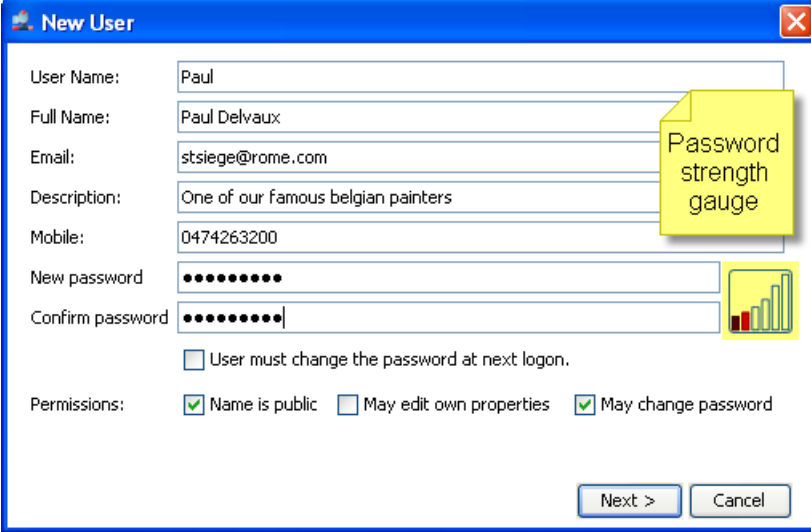
Assigning Permissions and Groups

These user properties are configured when adding a new user.

The path to the New User wizard is:

Users > Add

The following wizard appears (page 1):



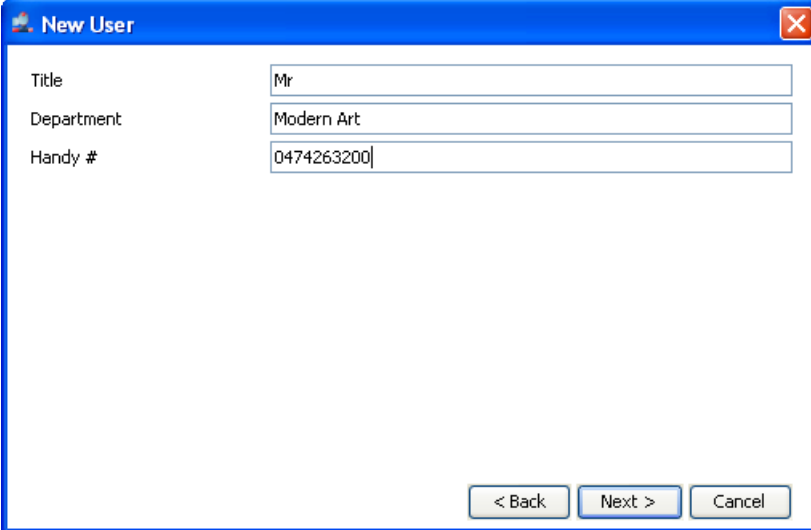
- Password strength gauge -

When entering your new password, a password strength gauge helps you to rate the password you intend to use. The gauge is presented under the form of a bar-graph of which the respective bars are progressively getting colored as you type. The closer to the highest bar, becoming green then, the safer your password is. This indicator is not linked with the password strength enforcement policy described in § [Error: Reference source not found](#) [Error: Reference source not found](#).

The admin user that creates a new user can check the following check-boxes:

- **User must change...** is usually checked when the admin user assigned a password for the user.
- **Name is public** 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 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.

Click **Next**, the following window appears (page 2):



New User

Title: Mr

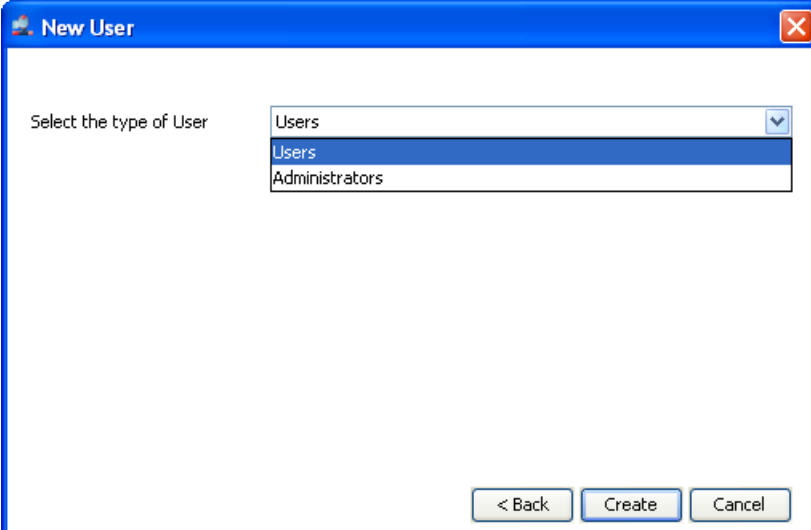
Department: Modern Art

Handy #: 0474263200

< Back Next > Cancel

Fill-out the custom fields (optional)

Click **Next**, the following window appears (page 3):



New User

Select the type of User: Users

Users

Administrators

< Back Create Cancel

The **Select the type of user** drop down assigns the user to one of the two groups.

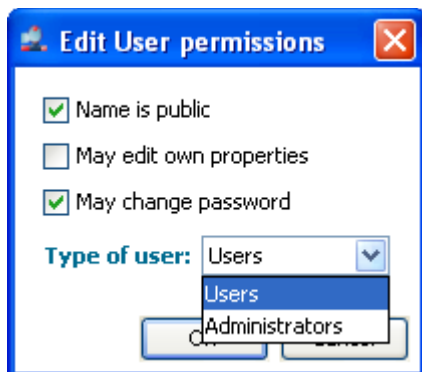
The Talk2M Pro account offers more user groups management options. For more information, see [\[R2\]](#).

Click **Create**.

You can modify an existing user's permissions from the **Edit User Permissions** popup. The path is

Users > Properties > Permissions and Groups > Modify...

The following popup appears:



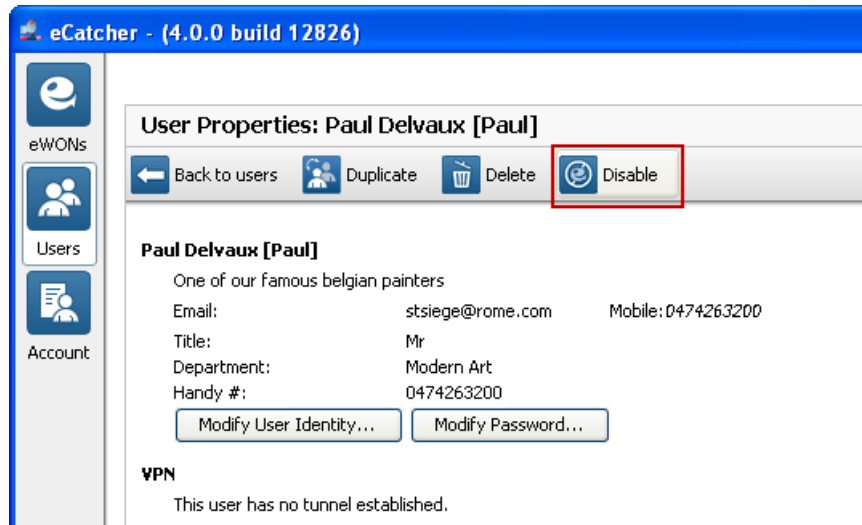
For the meaning of the options, you can refer to the explanations given for the new user creation here above.

Disabling and Deleting a User

An admin user can *temporarily* block the access of a user having an existing profile and password without deleting it (during a planned leave, a job rotation, etc.). The path to do this is:

Users > Select user from list > Properties > Disable

The user properties background becomes dark gray to show that this user is currently disabled. To re-enable this user, simply repeat the process clicking on **Enable**.



If the admin user wants to *permanently* block the access of a user, he clicks on **Delete**.



6. eWON Access Control

All users created in the Talk2M Free+ account can connect to all eWONs on this account. Access control to the eWON's web server or FTP server has to be managed by the user/password on the eWON itself.

Users of the Administrators group **can connect and can edit** the eWON properties in eCatcher. Users of the Users group **can only connect** to an eWON but not edit the eWON properties in eCatcher.

The Talk2M Pro account offers the ability to restrict the ability to connect to specified user(s) or group(s). For more information, see [\[R2\]](#).

7. LAN Device Access Control

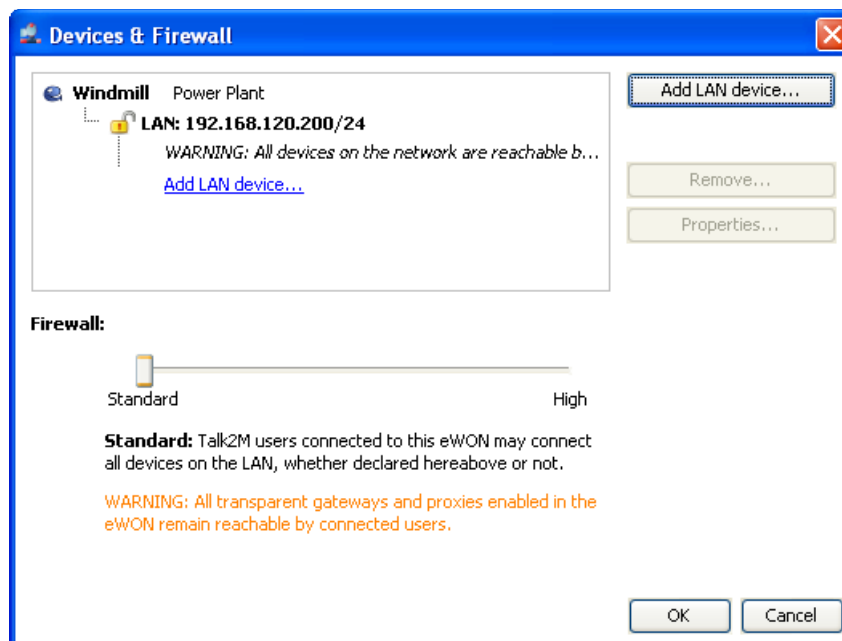
One of the key features in eCatcher is the ability to create LAN dependencies behind the eWONs and to protect the network including these dependencies by a firewall.

With a Talk2M Free+ account, an admin user can, for each eWON independently, specify which devices are remotely accessible on the eWON's LAN network.

To configure the LAN dependencies and enable the firewall, the path is:

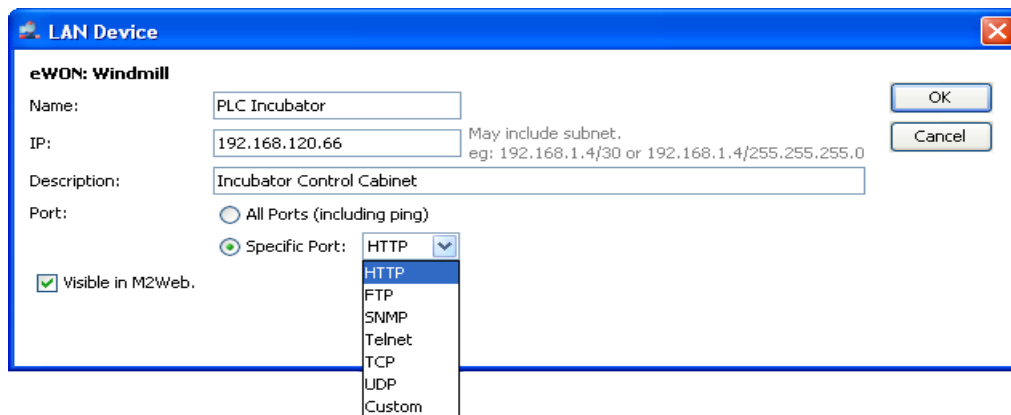
```
eWONs > Select eWON from list > Properties > LAN & Firewall > Configure LAN devices&...
```

The following page appears:



Click on **Add LAN device...**

The following page opens:



Fill-out the fields corresponding to the device behind the eWON. As you can see, you can restrict the access to service-specific ports. The service-specific ports are the standard ports for the corresponding protocol (ex: 80 for HTTP). The Talk2M Pro account offers more possibilities in this respect, would you want to specify port numbers other than the standard, see [\[R2\]](#).

You can also define whether this particular LAN dependency will be **Visible in M2Web** or not.

[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.

- Note -

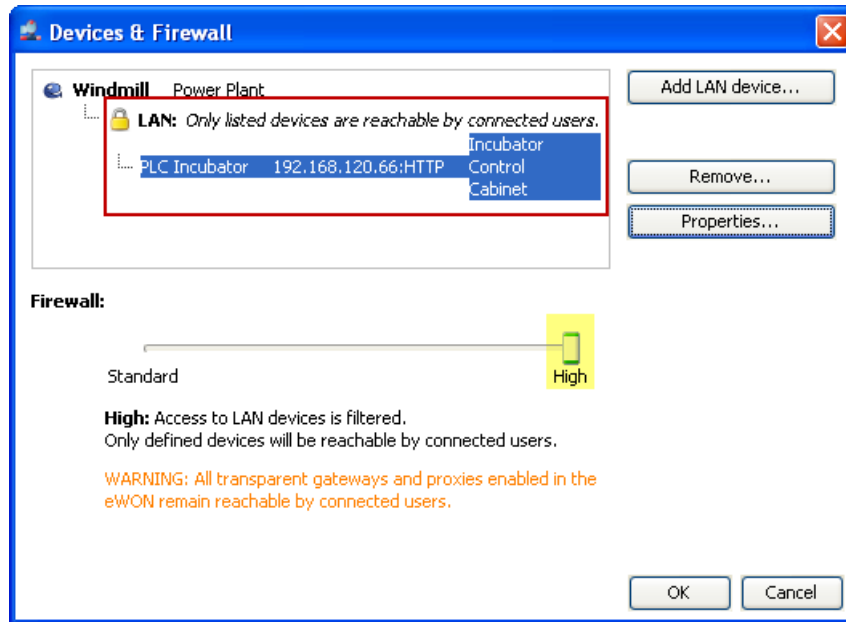
If you edit the LAN Device properties (i.e. change the status Visible in M2Web), you have to logout from M2Web and login again for the change(s) to be active.

Click **OK**

A warning message announces that the firewall setting will be set to **High**.



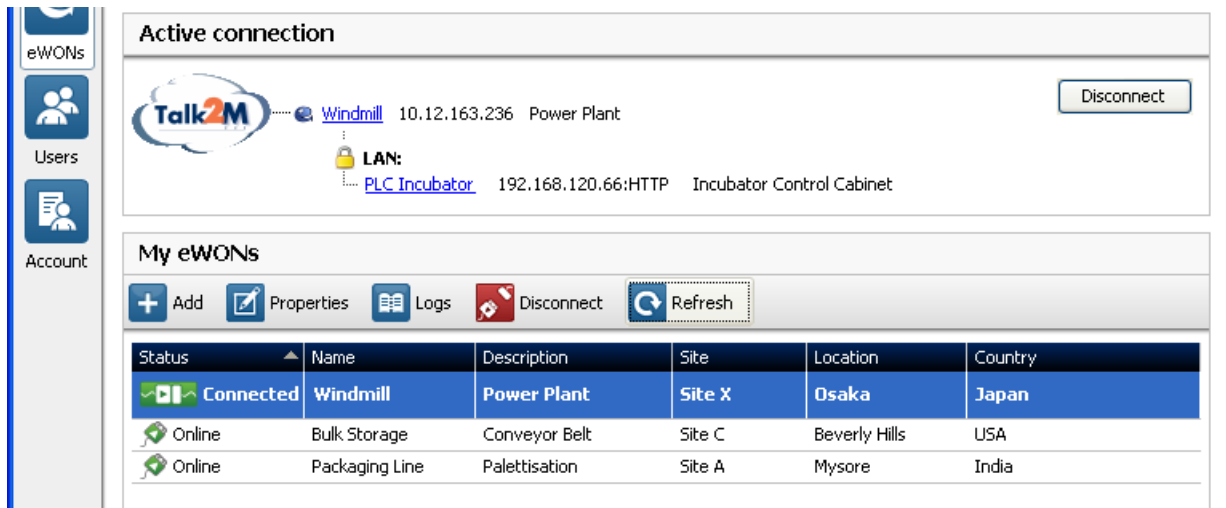
Click **OK**



The newly created LAN device appears under the eWON. The closed padlock next to the LAN instance indicates that the firewall has been enabled (also confirmed by the slider position **High**).

Click **OK**

Now when a user is connected to the eWON using eCatcher, the LAN device instance also appears in the **Active Connection** zone.



Clicking on the eWON (Windmill) opens the eWON web page in your Internet browser. Clicking on the LAN device (PLC Incubator) opens the target device in your Internet browser. The :HTTP suffix after the LAN device IP address indicates that the traffic is restricted to HTTP services on port 80.

- Reminder -

With Talk2M Free+, the access to the eWON itself is not restricted. Access to the eWON and permissions control have to be managed at the eWON user management level.

- Note -


Would the firewall be set to Standard, the padlock next to the LAN instance would appear open and the access to the LAN network behind the eWON would no longer be restricted to the specified LAN device IP address.

Devices

Users

Account

Active connection



[Packaging Line \(1\)](#) 10.237.153.103 Palettisation line



LAN: All devices on network are reachable by connected users.

- [HMI Wrapping Machine](#) 192.168.120.4:HTTP Palettisation Wrapping Machine
- [PLC Control Room](#) 192.168.120.233:HTTP Palettisation Control Room PLC

Disconnect

My eWONs

+ Add
🔗 Properties
📄 Logs
🛑 Disconnect
🔄 Refresh

| Name | Status | Description | User(s) conn... | Location | Site | Company |
|-------------------------|-----------------------------------------------------------------------------------------------------|---------------------------|-------------------|-----------------|---------------|--------------------------|
| Packaging Lin... |  Conne... | Palettisation line | eWON_guest | Misor... | Site A | Unified Paper ... |
| Bulk Storage | Offline | Conveyor Belt | | Beverl... | Site C | Wash Powder Inc. |
| Windmill (6) |  Online | Power Plant | | Osaka... | Site X | Heavy Steel Ind... |



Revision

Revision History

| Revision Level | Date | Description |
|----------------|------------|---------------------------------|
| 1.0 | 09/12/2013 | Initial version |
| 1.1 | 25/02/2015 | Two-factor authentication added |

Document build number: 21

Note concerning the warranty and the rights of ownership:

The information contained in this document is subject to modification without notice. Check <http://wiki.ewon.biz> for the latest documents releases.

The vendor and the authors of this manual are not liable for the errors it may contain, nor for their eventual consequences.

No liability or warranty, explicit or implicit, is made concerning the quality, the accuracy and the correctness of the information contained in this document. In no case the manufacturer's responsibility could be called for direct, indirect, accidental or other damage occurring from any defect of the product or errors coming from this document.

The product names are mentioned in this manual for information purposes only. The trade marks and the product names or marks contained in this document are the property of their respective owners.

This document contains materials protected by the International Copyright Laws. All reproduction rights are reserved. No part of this handbook can be reproduced, transmitted or copied in any way without written consent from the manufacturer and/or the authors of this handbook.

eWON sa, Member of ACT'L Group