eWON
MACHINES CAN TALK

Application User Guide

AUG 057 / Rev. 1.1

eCatcher - Security Features with a Talk2M Pro Account

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

support.ewon.biz

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 Pro vs Free+ Account 5

3. Password Policy 6

4. Two Factor Authentication 7
In practice, how does it work ? 7
What if the user does not receive the text message ? 9
Will the text messages be charged? 9
Backup mobile phone number ? 10
What is the "Remember this PC" option ? 10
How to enable/configure the two factor authentication on my account? 11

5. Users, Groups, Pools and Roles 13
Concept 13
Creating a New User 13
Disable and Delete User 16

6. eWON Access Control 17

7. Advanced Firewall Features 18
LAN Level Access Control 18
Gateway Level Access Control 20
Service Level Access Control 22

Revision 24
Revision History 24

1. General Information

Scope

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

Reference documents

Click on the hyperlink to download the relevant document.

- [R1] AUG-028-0-EN-(Talk2M Pro - Account Configuration)
- [R2] AUG-056-0-EN-(eCatcher 5 - Security Features with a Talk2M Free+ 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 Pro 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 priority number one. 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 all necessary tools to customize the level of security to the specific requirements of the infrastructure used to make remote connections to your equipment.

Talk2M Pro vs Free+ Account

The current document covers eCatcher 5 in combination with a **Talk2M Pro** account. Another document covers the features available with a Talk2M Free+ account, see [R2].

As compared to Talk2M Free+, **Pro** has a number of additional features allowing to:

- implement a highly secured access control policy for users, eWONs and devices
- establish concurrent secure VPN connections

- 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.

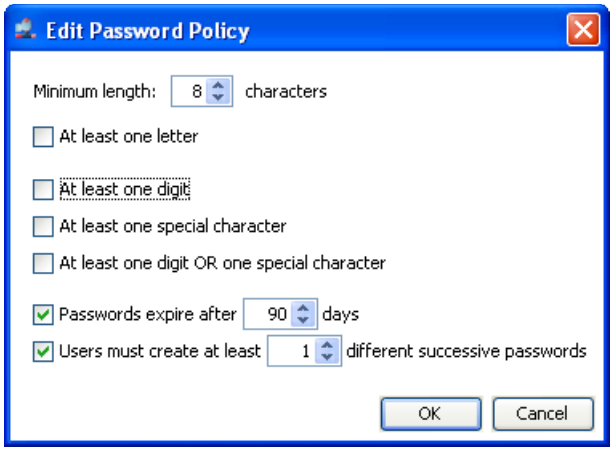
3. Password Policy

The Password Policy defines the password syntax requirements for all users of the account. Only members of the Administrators group can edit the Password policy.

The path to the Password Policy is:

```
Account > Show advanced properties > Password Policy > Modify...
```

The following popup appears:



The minimum length of the password is configurable between 6 an 45 characters

The user can be forced to have his password:

- having a minimum length [6..45]
- use at least one letter
- use at least one digit
- use at least one digit OR one special character
- at least one special character [%, $, @, etc.]
- expire every [10..999] days
- different than the [1..999] previous one(s)

- Important -

If the admin user changes the Password Policy while users have already been created, their existing passwords remain valid even if they do not meet the new policy. The new policy will apply only to new users or if the existing user changes his password.

4. Two Factor Authentication

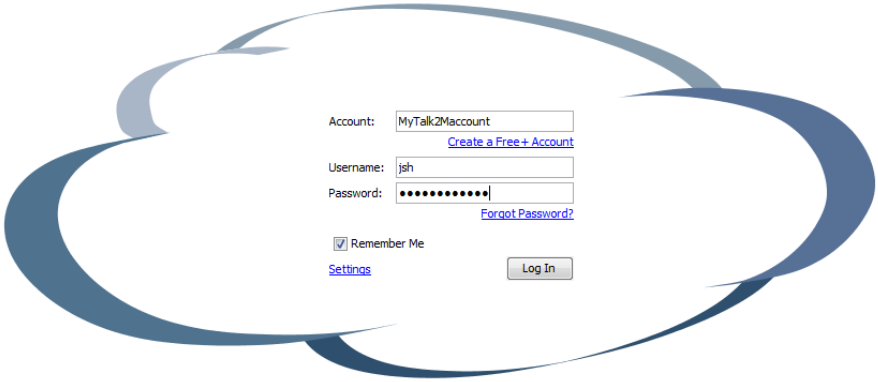
To increase the security of your Talk2M account, we strongly recommend to activate the two-factor authentication.

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).

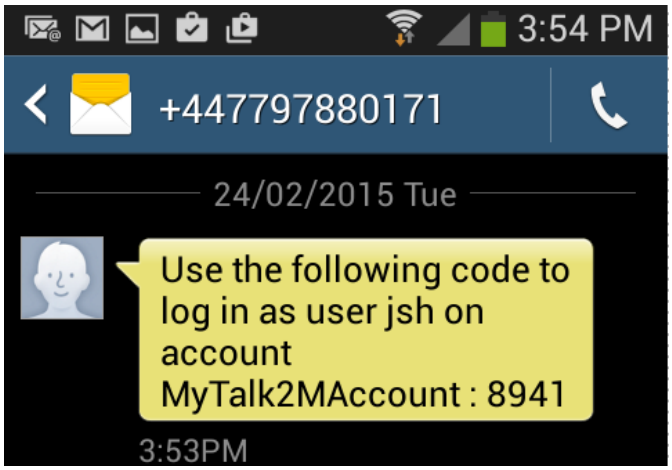
When it comes to eCatcher and M2Web connections, the second authentication factor will involve the mobile phone of the user. A text message that contains a one-time-valid, dynamic passcode consisting of 4 digits will be sent to the cell phone.

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.

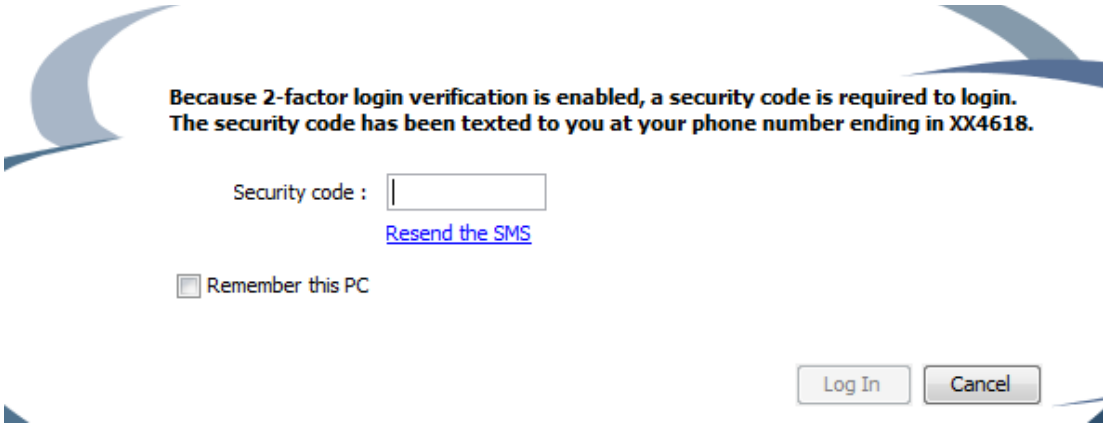


The Talk2M system will then send a text message to the mobile phone number encoded for this user.



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.

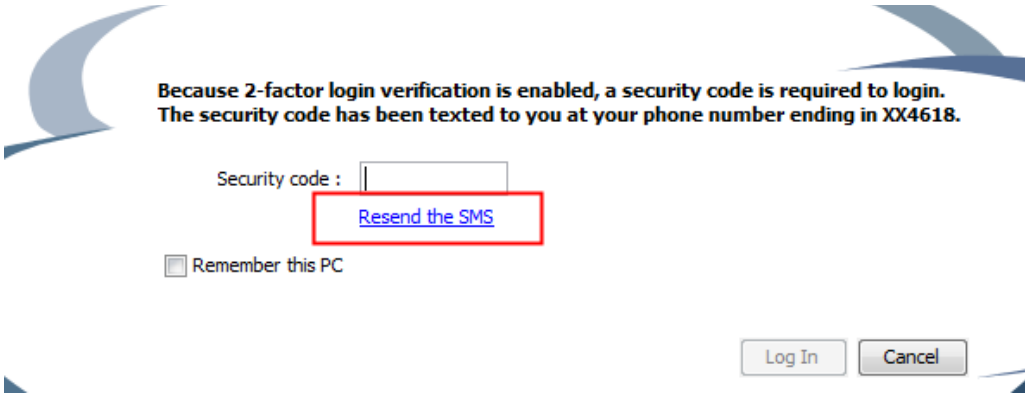


- Note -

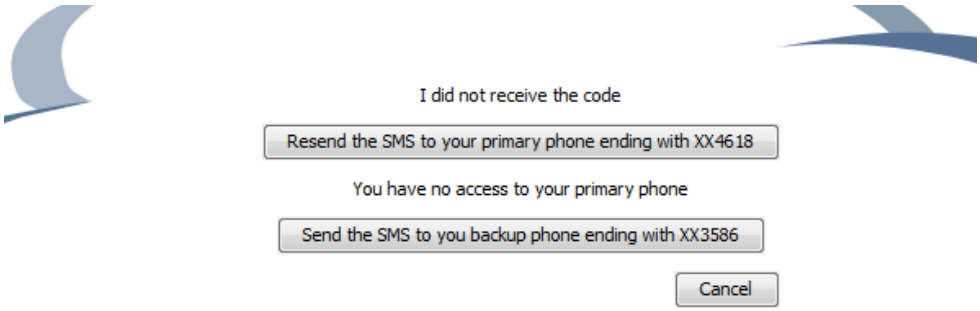
The user has 3 attempts to encode the correct passcode, otherwise the user login will be blocked for a certain period (30 minutes).

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.

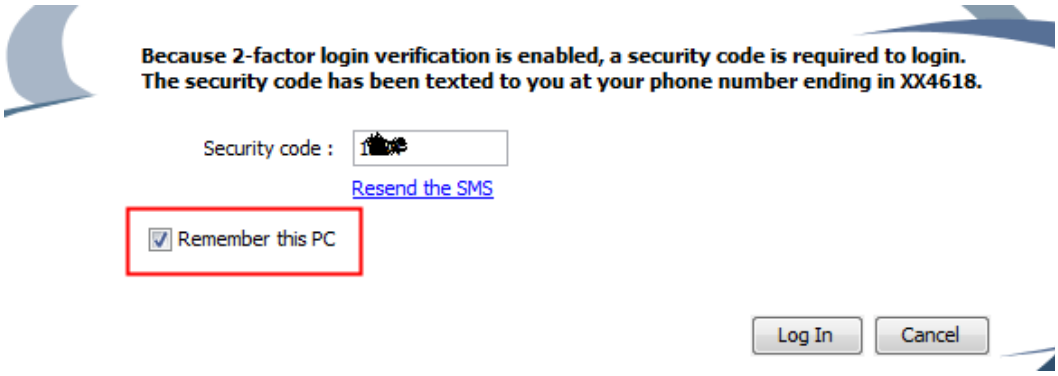
So it is strongly recommended to encode a backup mobile phone number for each user.

- 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.



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 Administrator of the Talk2M account can decide if the "Remember this PC" option is authorized or not for the Talk2M account.
The expiration time of the "Remember this PC" can also be configured. It can for example be set to 30 days. This means that the user will need to use, at least every month, the passcode received by text message as second authentication component.

- 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.

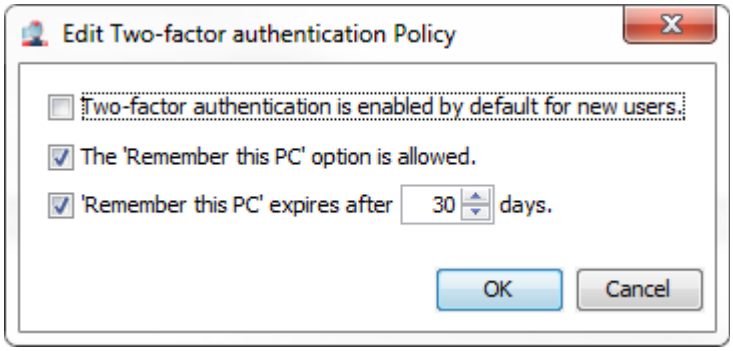
How to enable/configure the two factor authentication on my account?

Inside the account menu you can configure the general settings of the two-factor authentication.

The path to the Two Factor Authentication Policy is:

```
Account > Security Policy > Modify 2-Factor authentication policy...
```

The following pop-up appears:



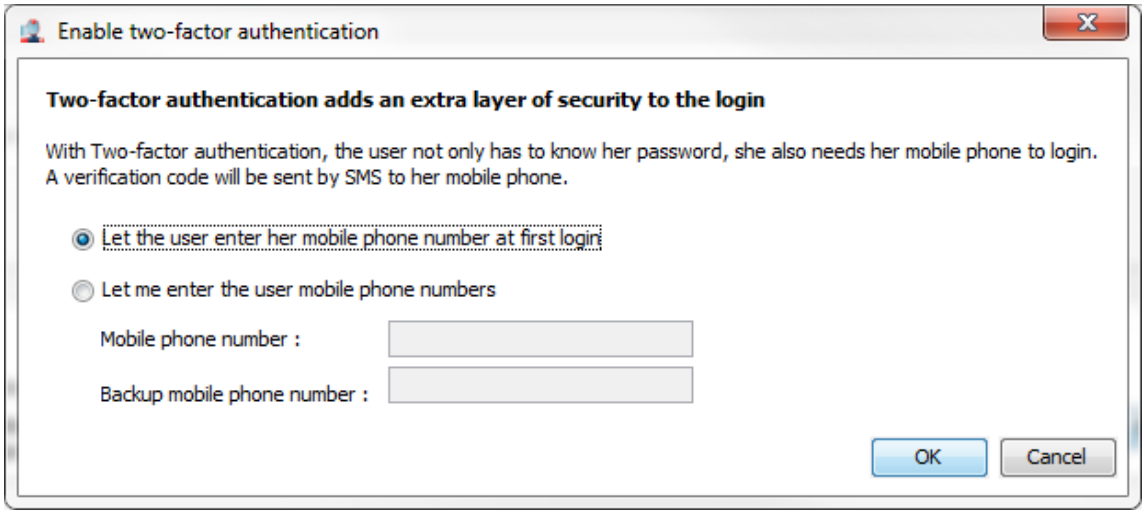
The options allow to enable the two-factor authentication for all new users and to enable and configure the "Remember this PC" option.

Then for each user of your Talk2M account, you 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...

The following pop-up appears:



Here you can decide either to encode the mobile phone number of the user or let the user encode and validate his phone number on next login.

5. Users, Groups, Pools and Roles

Concept

- 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*** included in this ***Group***.

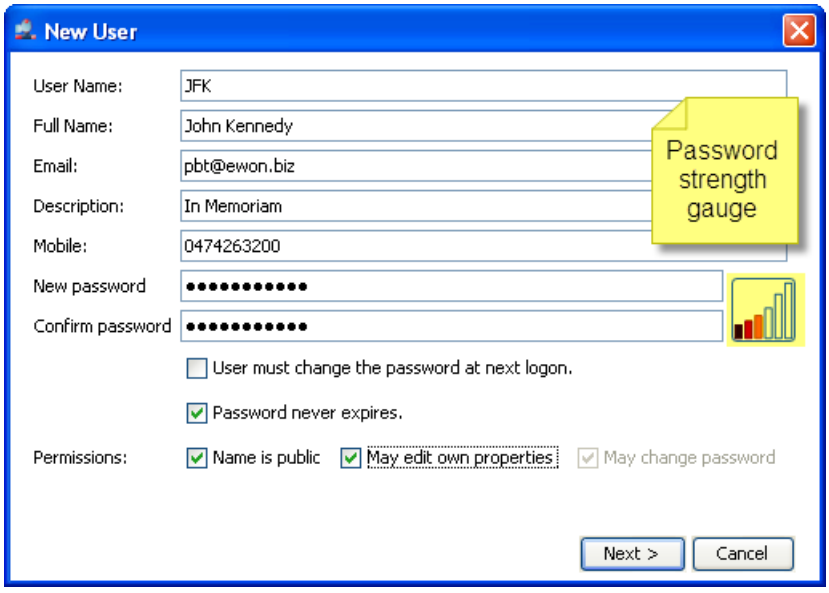
To create ***Groups***, ***Pools*** and assign ***Roles*** please refer to document [R1].

Creating a New User

The path to create a New User is:

```
Users  > Add
```

The following page appears (New User wizard page 1):



Security related items in this page are:

- Visual password strength gauge (see description below)
- Ability to force user to change password at first login
- Ability to force user to change password at configurable intervals (@ Account level)

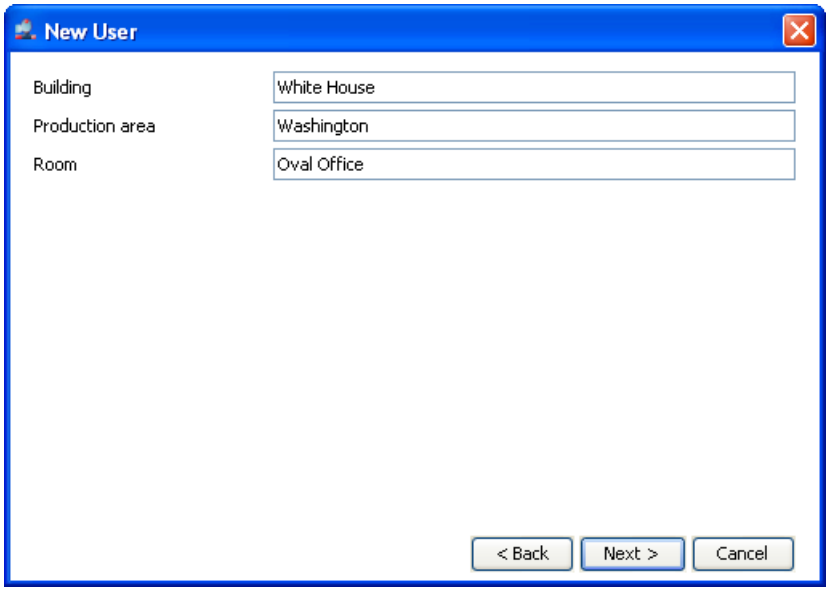
- Ability to make the name of the connected user public. This option, if checked, will make the user name visible to other logged users of the account in the "connected user" column of the eWON list.
- Ability for the user to change his own password

- 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 § 3 Password Policy.

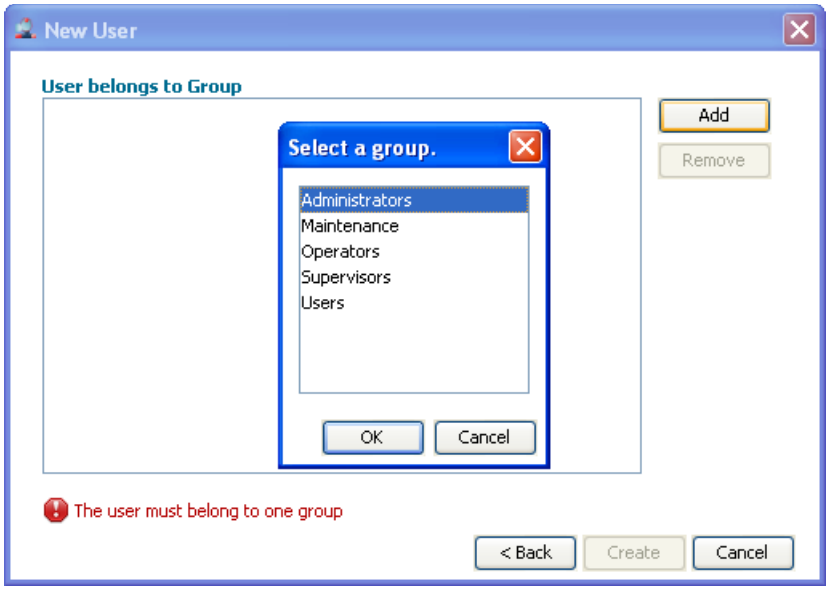
Click ***Next***

The following page appears (New User wizard page 2):



These custom fields are optional, click ***Next***

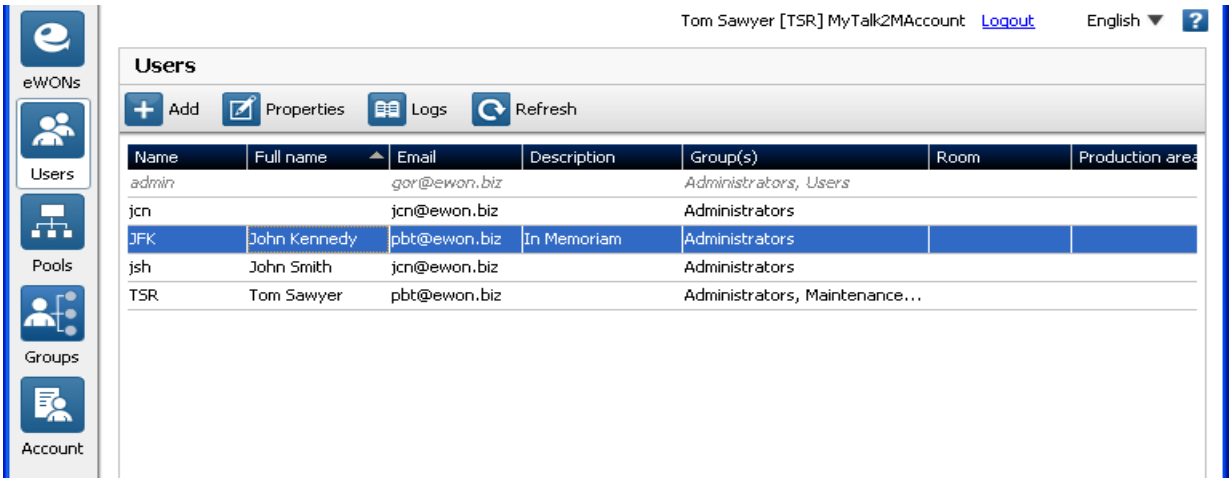
The following page appears (New User wizard page 3):



Here you can select the groups (and attached roles) you want the new user to be assigned. Repeat if you want the new user to be assigned to another group.

Click ***Create***.

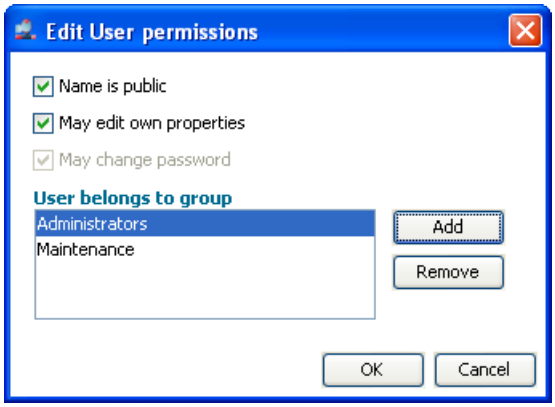
The new user appears in the ***Users*** list:



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:



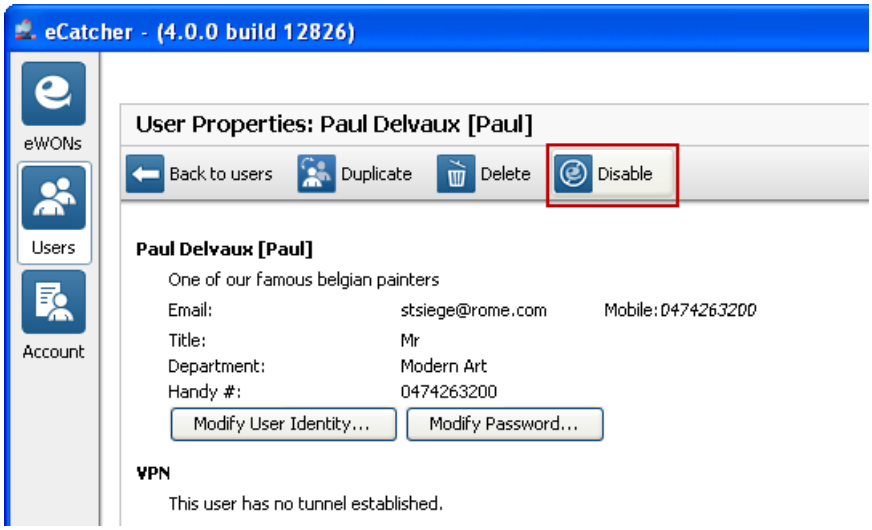
For the meaning of the options, you can refer to the explanations given for the new user creation here above.

Disable and Delete 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

With a Talk2M Pro account, the fact a given user has the permission to access an eWON or not is not managed at the ***eWON*** level, nor is it at the ***User*** level.

It is managed indirectly by the ***Group(s)*** to which that given user belongs to, Group(s) that have or not ***Roles*** (permissions) on given eWON Pools. Please refer to document [R1] for more information on ***Groups***, ***Pools*** and ***Roles***.

This type of configurable protection offers an additional security-layer to the user permission management at the eWON level itself.

7. Advanced Firewall Features

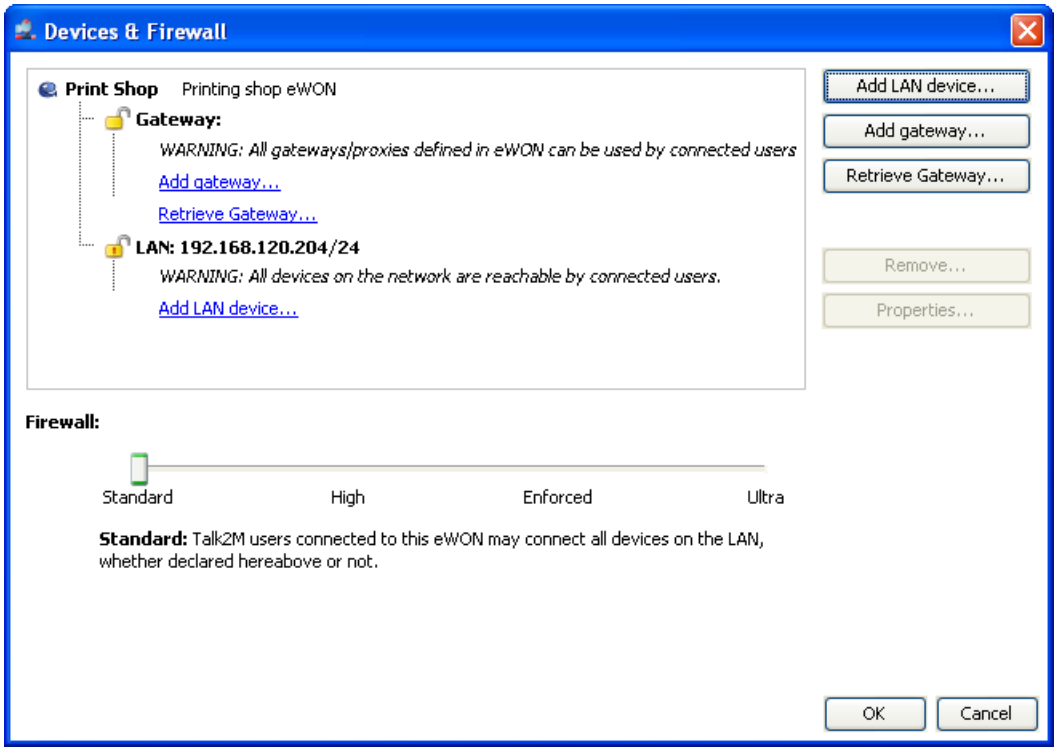
LAN Level Access Control

In order to protect the LAN network (machine network) you need to define the LAN addresses that need to be accessible.

The path to LAN-device creation is:

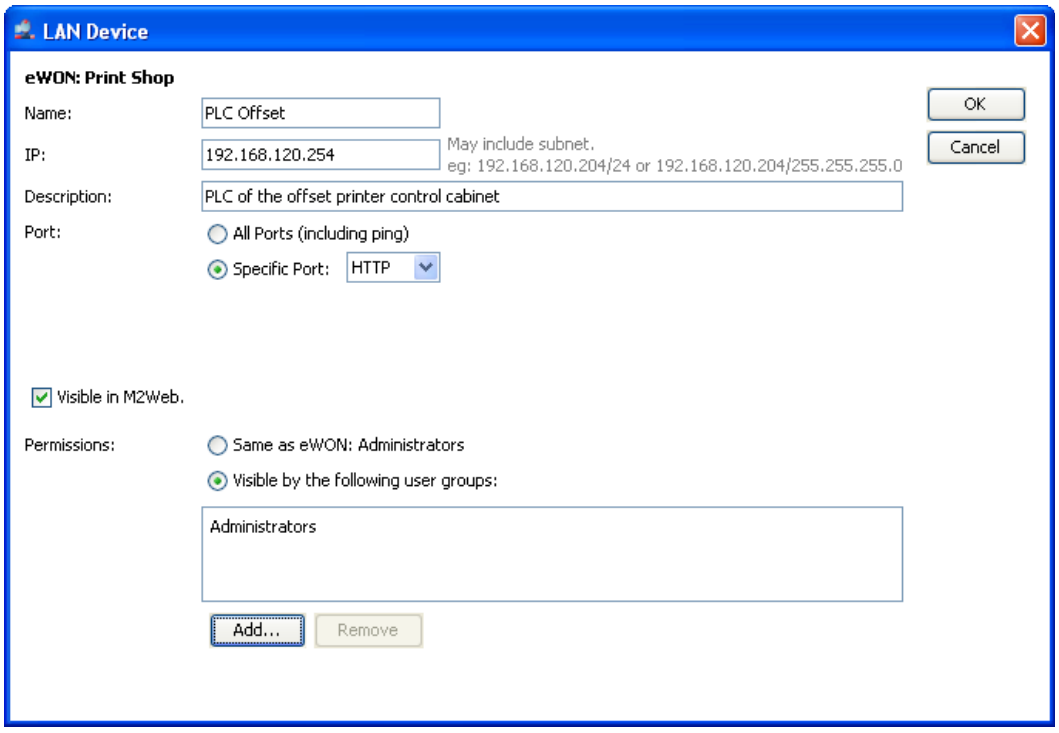
```
eWONs > select eWON from list > Properties > LAN & Firewall > Configure LAN devices & Firewall...
```

The ***Devices & Firewalling*** page opens



Click on ***Add LAN device...*** (link or button)

The LAN Device page opens.



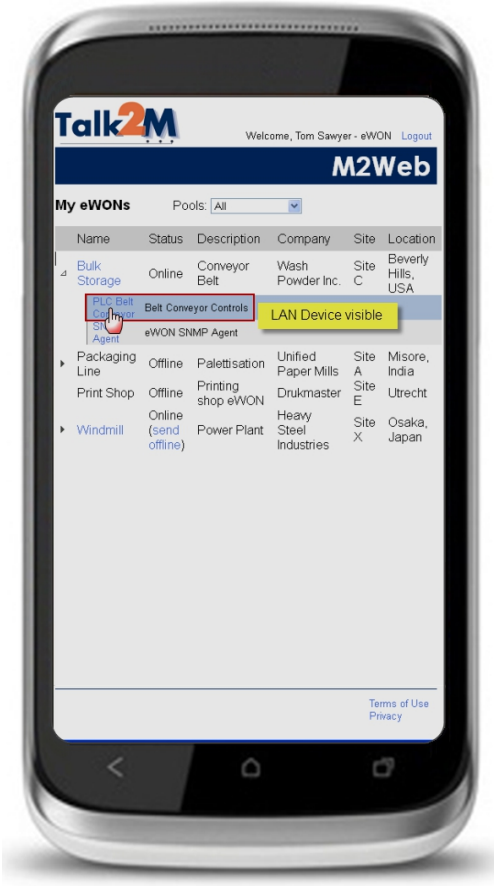
In this page you give a name to your LAN device, specify its IP address, give it a description (optional), select if all ports are open or only protocol-specific ports, whether you allow the device to be visible on M2Web (see description next page).

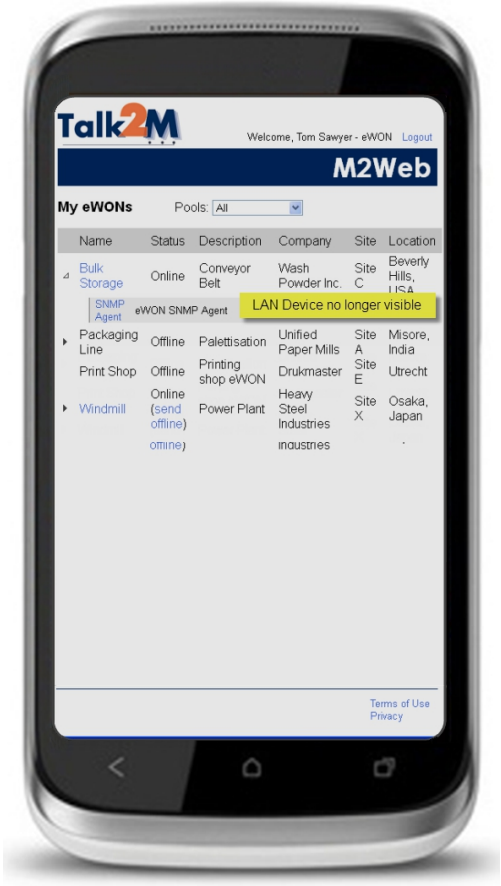
In the ***Permissions*** area you can define which user group(s) is/are allowed to connect to the device. Click ***OK*** when you are ready.

After this, the ***Firewall*** slider is automatically shifting to position ***High*** while this is the position required to activate the firewall protection at the LAN side.

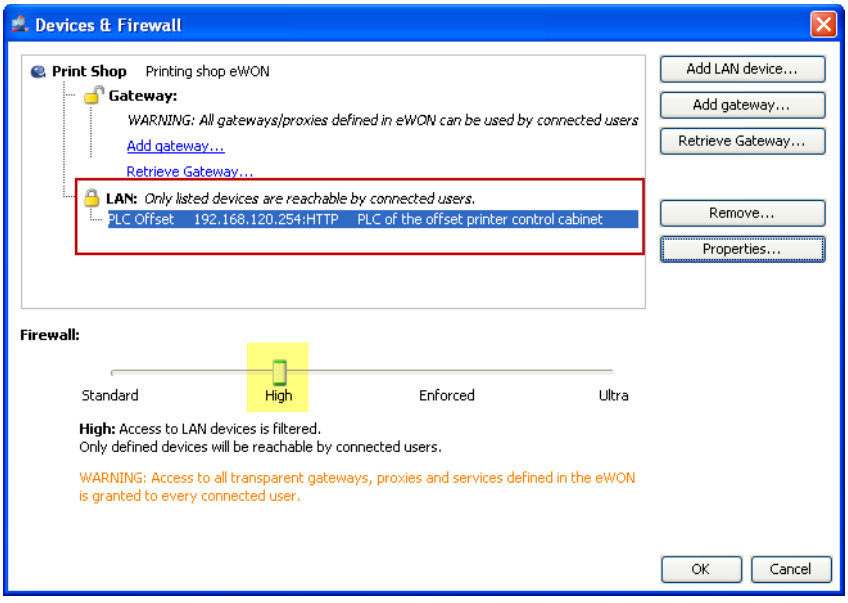
You can also define whether this particular LAN dependency will be ***Visible in M2Web*** or not.

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.





The new LAN device appears with a closed padlock under the structure of the relevant eWON:



The properties of the LAN device can be edited afterward by clicking ***Properties***.

Gateway Level Access Control

In order to protect the Gateway(s) you need to define the gateway(s) that need to be protected. As for the LAN network, we first need to create the relevant gateway(s).

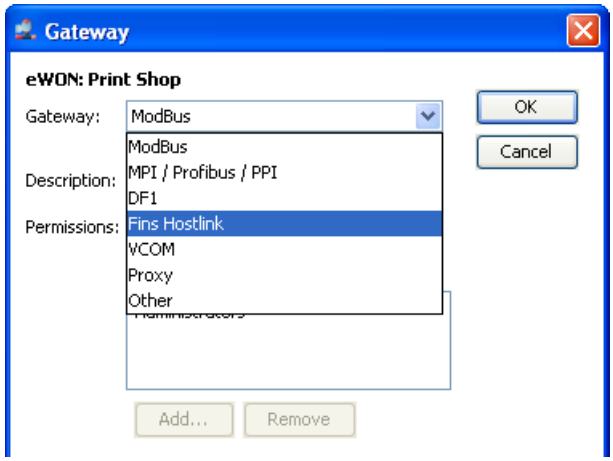
The path to Gateway creation is the same as for LAN devices:

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

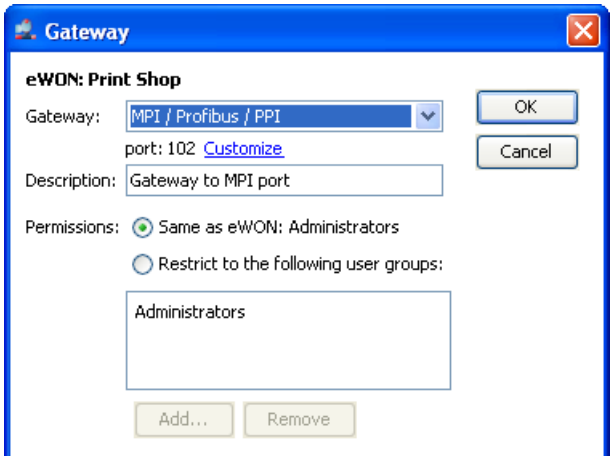
The Devices & Firewall page opens.

Click on ***Add gateway...*** (link or button).

The LAN Device page opens:

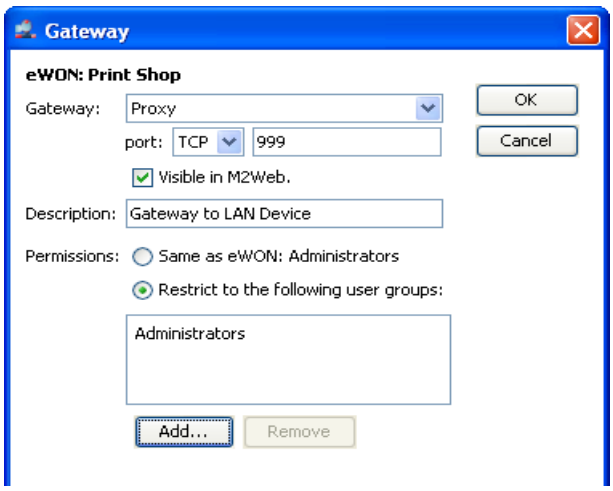


Select the relevant ***Gateway*** from the drop down list.



Depending on the selected gateway, a ***Customize*** link may allow you to configure another port # than the default one. In the example above, the default MPI port is 102 but you can configure whatever port you want.

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



You can select the port to be UDP or TCP. Also whether it may be visible on M2Web. For each gateway configured, the user group permissions can be set at ***Same as eWON*** *or* ***Restrict to the following user groups.*** Click ***Add*** if you want to add group(s). Groups first have to be created & configured. Please refer to document [R1] for more information on ***Groups***, ***Pools*** and ***Roles***.

After this, the ***Firewall*** slider is automatically shifting to position ***Enforced*** while this is the position required to extend the firewall protection to gateway(s). The new gateway appears with a closed padlock under the structure of the relevant eWON.

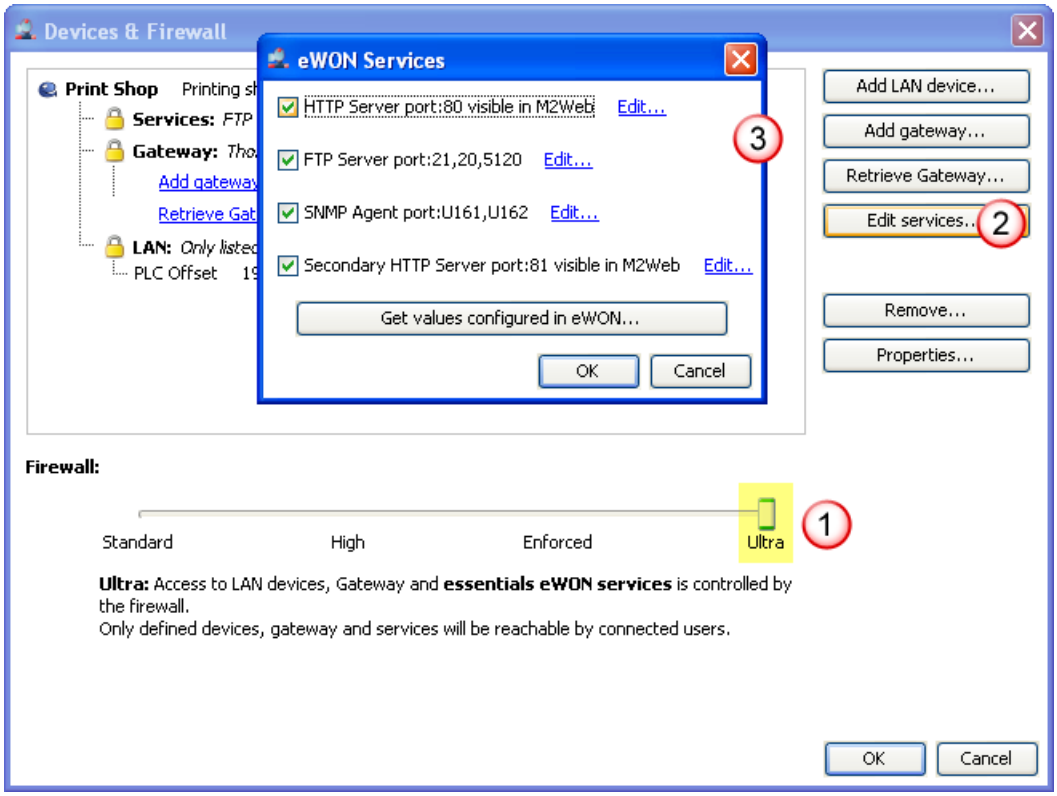
Service Level Access Control

In order to control the access at the ***Services*** level, you need to define to which services(s) the ports can be opened.

The path to the selection of services to open creation is the same as to create LAN devices:

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

Push the ***Firewall*** slider to ***Ultra*** (1) in order to have the ***Edit services*** button shown.



Click ***Edit services...*** (2), the eWON services popup appears (3):
In this window you can open single or multiple ports specifically for this service.

The available services include:

- Primary HTTP server
- FTP server
- SNMP agent
- Secondary HTTP server

- Important note -

*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 do this, your eWON must be online and you must have appropriate login credentials for the eWON itself.*

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: 34