

Manage Devices Access

With a Talk2M PRO Account

APPLICATION NOTE

AUG-0086-00 1.0 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
3	User and Device Rights Management	6
3.1	Overview	6
3.2	Default Configuration	6
3.3	Ewon Pools	7
3.4	User Groups	9
4	Examples	13
4.1	Machine Builder	13
4.2	Factory Owner	17

This page intentionally left blank

1 Preface

1.1 About This Document

This document explains how to configure correctly access to remote devices based on user groups and Ewon pools in 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	2019-05-30	First release

1.3 Related Documents

Document	Author	Document ID
Email & Text Messages(SMS) Relay using Talk2M	HMS	SSH-0046-00

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

Talk2M is a secure industrial connectivity service in the cloud allowing easy remote access and remote monitoring of industrial devices.

Talk2M is designed to securely allow users to connect to their remote assets for troubleshooting and monitoring.

On one side, an Ewon connected to a machine establishes a secure VPN connection to the Talk2M infrastructure.

On the other side, authorized users establish a secure connection to Talk2M which then acts as a relay between the user and the Ewon.

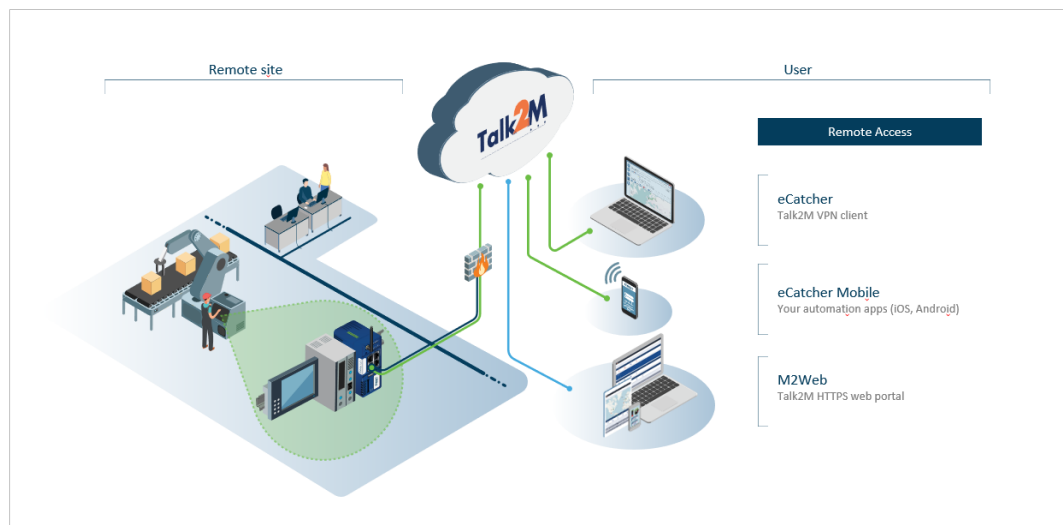


Fig. 1 Talk2M concept

With Talk2M's VPN client software, eCatcher, users can connect to their remote equipment for programming and troubleshooting.

Users can also use Talk2M's HTTPS web portal, M2Web, to view key performance indicators for their systems as well as monitor remote HMIs, PCs, and web servers from any device with a web browser.

For those users who need to interact with their equipment using mobile applications, the eCatcher Mobile app is available to create secure connections from their mobile devices.

While there are many benefits to remote access, there are security concerns associated with allowing remote access as well.

Talk2M account administrators can manage these concerns by controlling the access privileges granted to different users including restricting which devices a user can access, when the user has access, and the mechanisms by which a user is able to connect.

For example, a factory owner might wish to give remote access privileges to a machine builder for troubleshooting a machine.

With Talk2M PRO account, the factory owner can limit the machine builder's access to only those devices supported by the machine builder and grant access only when a machine needs to be serviced; during all other times, the machine builder's access is disabled.

Likewise, while a machine builder needs to be able to access all their machines for remote support, they might want to also give their customers the ability to monitor key values on their machines.

With Talk2M, the machine builder can grant different levels of access rights to their own service team and their customers so that the service team has full remote access to all machines and customers are limited to remotely monitoring their own machines through M2Web.

3 User and Device Rights Management

3.1 Overview

Talk2M Pro account administrators can define which users have access to which Ewons as well as what rights users have regarding user management and device management.

These access and management rights are controlled through **<User Groups>** and **<Ewon Pools>**.

<Ewon Pools>

<Ewon Pools> are collections of Ewons.

Users who have some level of access right to an Ewon in an Ewon pool will have that same level of access right to all Ewons in that same pool. Every Ewon must belong to at least one Ewon pool.

<User Groups>

<User Groups> define the access rights that member users have on different **<Ewon Pools>** as well as what administrative roles users have on the account, their own user group, and other user groups.

Every user must belong to at least one user group.

3.2 Default Configuration

Initially, a Talk2M Pro account includes a single Ewon pool, the **Device pool**, and two user groups, **Administrators** and **Users**.

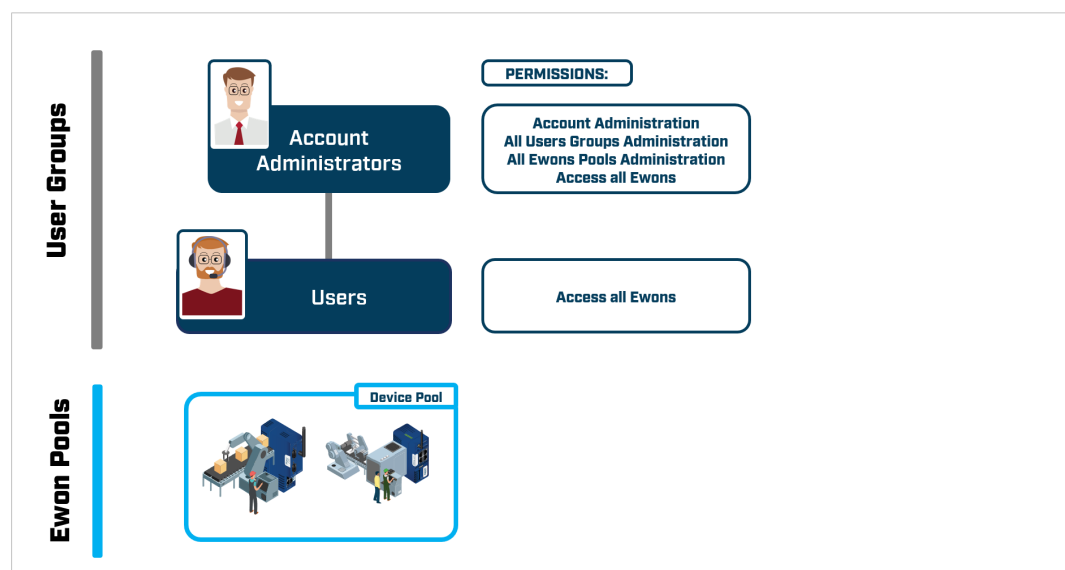


Fig. 2 Example of users rights

The **Administrators** user group has all permissions including managing all user groups, managing all Ewon pools, modifying the account settings, and access to all Ewons.

This group cannot be deleted, but it can be renamed. Its roles and permissions cannot be edited. The first user associated with the account creation is automatically a member of the Administrators group. It is strongly recommended to have more than one user in this group.

Members of the **Users** user group may connect to Ewons in the default **<Device pool>**.

They do not have administrator privileges on the <Device pool> or on any existing user groups. They also may not create new user groups or Ewon pools. The roles and permissions of the Users user group can be edited.

Modifying the user and device rights is performed through the eCatcher software.

3.3 Ewon Pools

Ewon pools are created or modified from the *Pools* window in eCatcher.

3.3.1 Creation

To create an Ewon pool, proceed as follows:

1. Click the **Add** button to create a new pool.
2. Enter a **Pool Name** and specify which **User Group** will manage this pool.

This user group will then receive automatically the **User can administer** rights on this pool.

The list of groups in the dropdown menu consist of the groups which you belong to that have the rights to create pools.

The default group is the Administrators group.

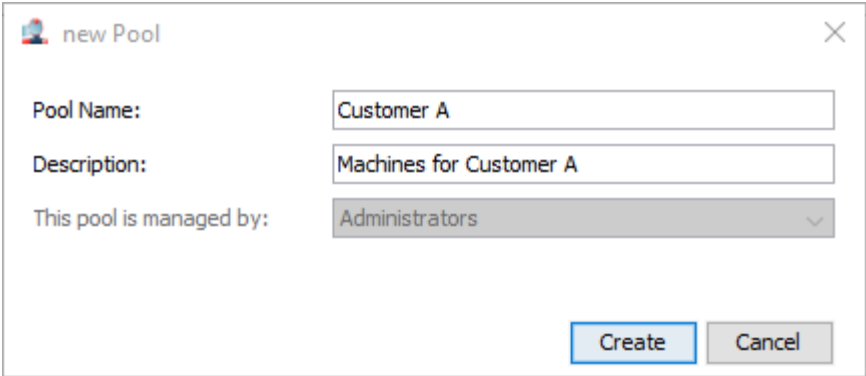


Fig. 3 New Pool creation

3.3.2 Modification

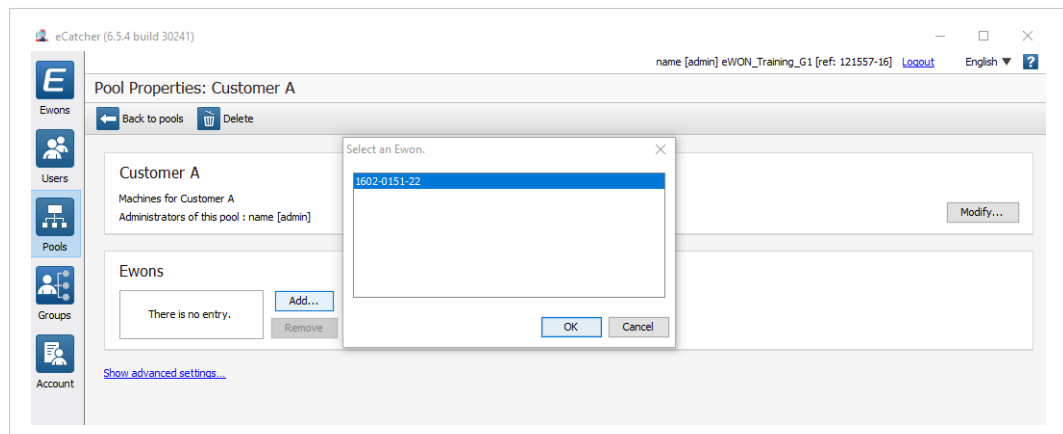
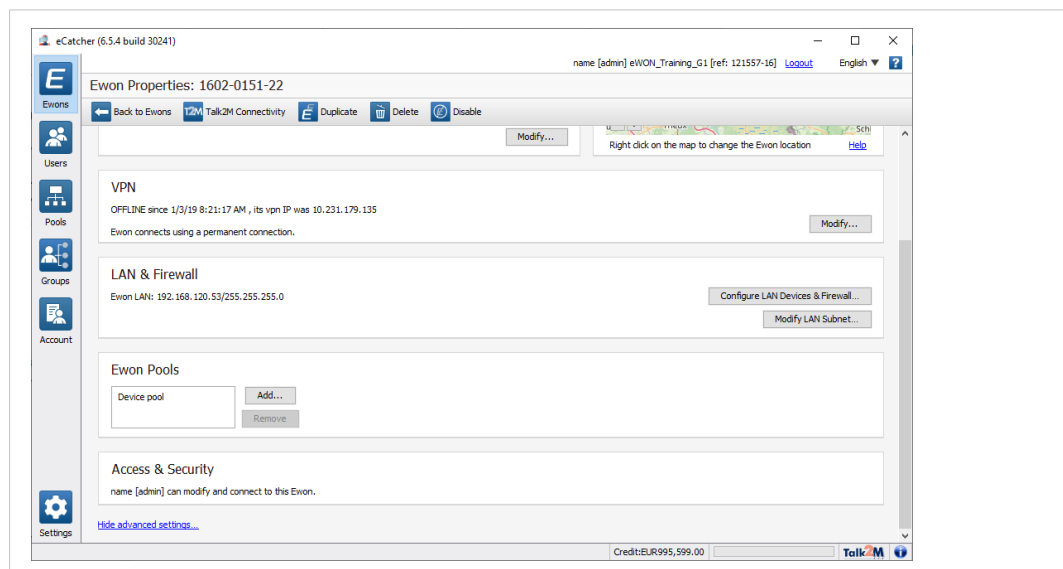
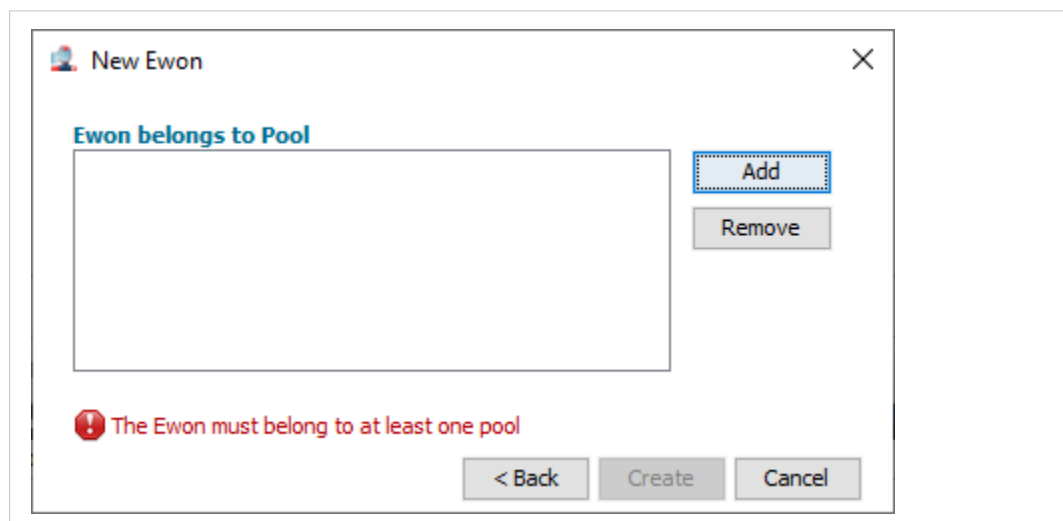
To modify or delete an existing pool:

- **Highlight** the pool.
- Click the **Properties** button.

Add or Remove Ewon(s)

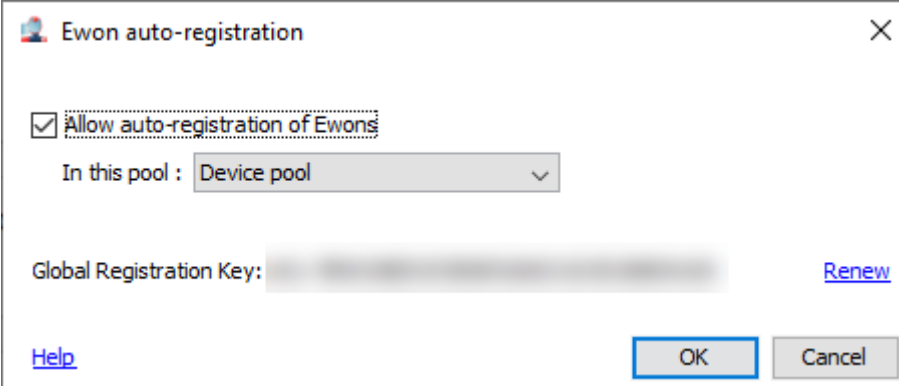
Ewons can be added or removed from an Ewon pool either:

- from the *Properties* page of the pool;
- from the *advanced settings* of the Ewon;
- from the **Add Ewon** button on the main view.

From the *Properties* page**Fig. 4** Add an Ewon through a pool**From the *advanced settings* of the Ewon****Fig. 5** Advanced settings of an Ewon**From the *Add Ewon*****Fig. 6** Add a new Ewon

For Ewons added to the Talk2M PRO account through the **Add Ewon** button, pool assignment occurs as part of the *Add Ewon* wizard.

If *Auto-Registration* is enabled for the account, you are allowing Ewons to be registered without the need to specify the Ewon first inside the Talk2M account. eCatcher will automatically assign Ewons to the pool indicated in the **<Account Properties>**.

A dialog box titled "Ewon auto-registration" with a close button (X) in the top right corner. It contains a checked checkbox labeled "Allow auto-registration of Ewons". Below this is a dropdown menu labeled "In this pool :" with "Device pool" selected. At the bottom left is a "Global Registration Key:" followed by a blurred text field. To the right of the key is a "Renew" link. At the bottom left is a "Help" link. At the bottom right are "OK" and "Cancel" buttons.

Ewon auto-registration

☒ Allow auto-registration of Ewons

In this pool : Device pool

Global Registration Key: [blurred text] [Renew](#)

[Help](#) **OK** Cancel

3.4 User Groups

User groups are created or modified from the *Groups* window in eCatcher.

3.4.1 Creation

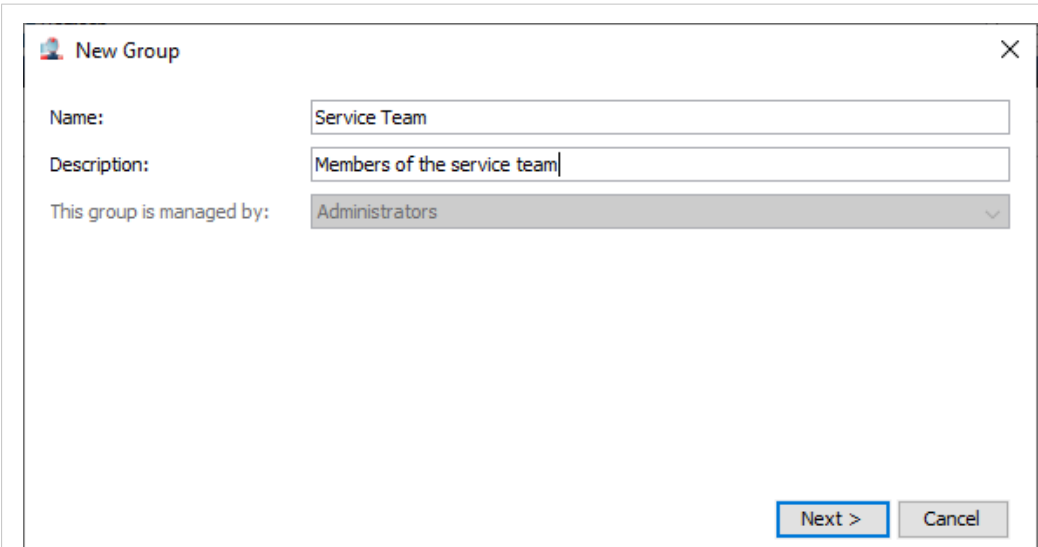
To create a new group, proceed as follows:

1. Click the **Add** button to create a new group.
2. Enter a **Group Name** and specify which **User Group** will manage this group.

This user group will then receive automatically the **User can administer** rights on this group.

The list of groups in the dropdown menu will consist of the groups to which you belong that have the right to create user groups.

The default group is the Administrators group.

A dialog box titled "New Group" with a close button (X) in the top right corner. It contains three input fields: "Name:" with "Service Team", "Description:" with "Members of the service team", and "This group is managed by:" with a dropdown menu showing "Administrators". At the bottom right are "Next >" and "Cancel" buttons.

New Group

Name: Service Team

Description: Members of the service team

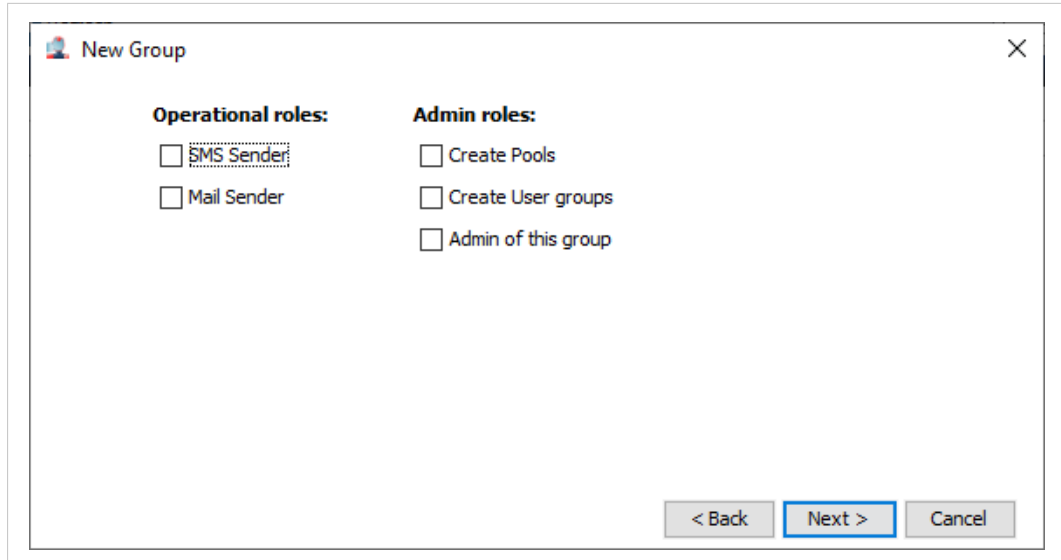
This group is managed by: Administrators

Next > Cancel

Fig. 7 New Pool creation

The **<Operational Roles>** specify the rights of users in this user group regarding the Talk2M email Relay. See Email & Text Messages(SMS) Relay using Talk2M from [Related Documents, p. 3](#) for more information about sending SMS and email through Talk2M.

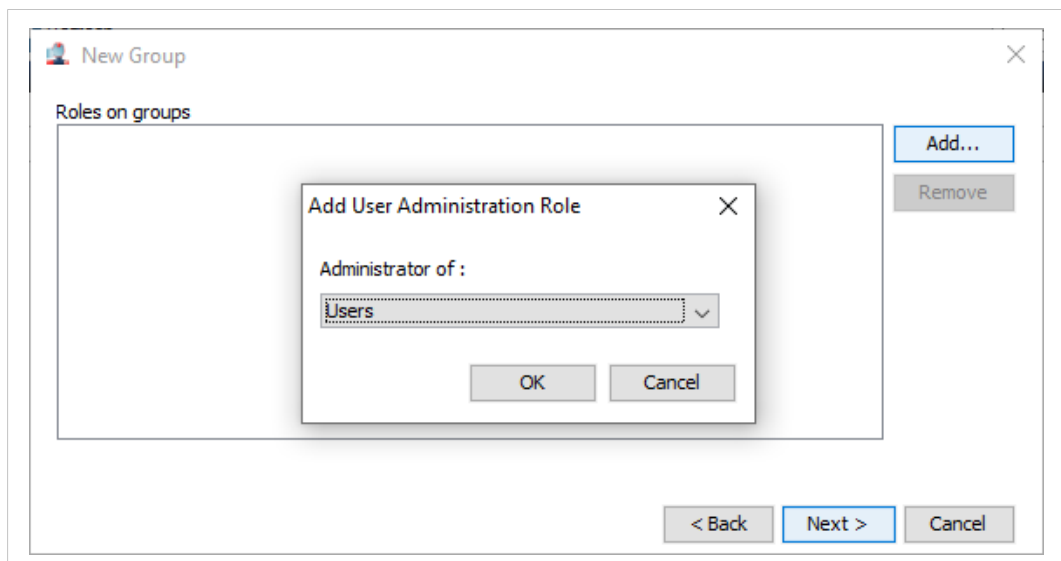
The **<Admin Roles>** describes whether members of this user group can create new Ewon pools, create new user groups, and add, delete, or modify other users belonging to this user group.



The screenshot shows a 'New Group' dialog box with a close button (X) in the top right corner. It contains two sections: 'Operational roles' and 'Admin roles'. Under 'Operational roles', there are two checkboxes: 'SMS Sender' and 'Mail Sender'. Under 'Admin roles', there are three checkboxes: 'Create Pools', 'Create User groups', and 'Admin of this group'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

Fig. 8 Roles inside a user group

If this user group can administer other user groups, add the groups to be administered in the **<Roles on Groups>** page.



The screenshot shows the 'New Group' dialog box with the 'Roles on groups' section selected. It features a large empty box for listing roles, with 'Add...' and 'Remove' buttons to its right. An 'Add User Administration Role' sub-dialog is open in the center. This sub-dialog has a title bar with a close button (X) and a label 'Administrator of :'. Below the label is a dropdown menu currently showing 'Users'. At the bottom of the sub-dialog are 'OK' and 'Cancel' buttons. The main dialog also has '< Back', 'Next >', and 'Cancel' buttons at the bottom right, with 'Next >' highlighted.

Fig. 9 Administrator permissions

On the next page, specify which Ewon pool(s) this user group can connect to or modify.

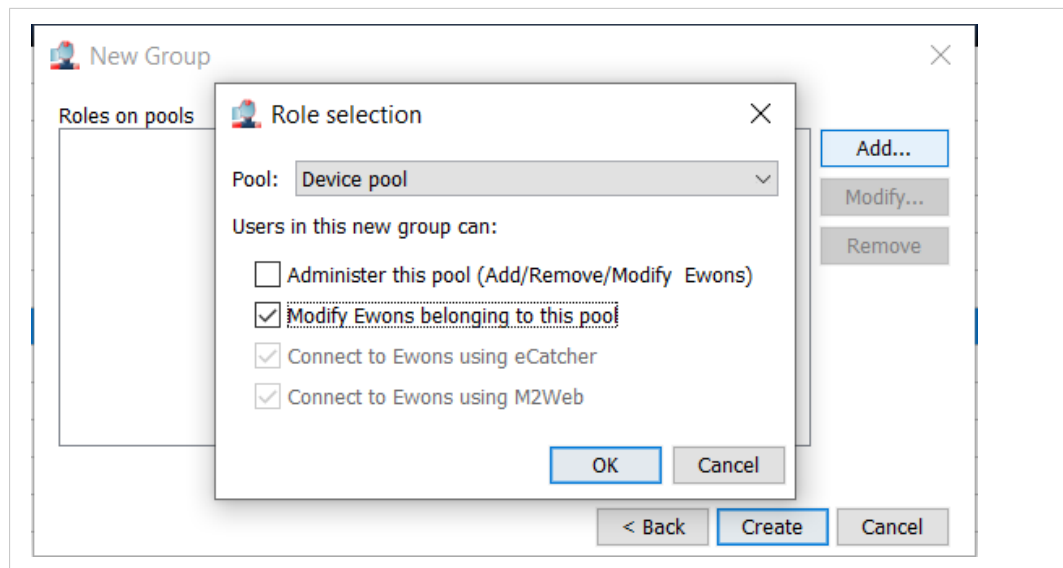


Fig. 10 Pool settings

3.4.2 Modification

To modify or delete an existing user group:

- **Highlight** the user group.
- Click the **Properties** button.

Add or Remove User(s)

Users can be added or removed from a user group either:

- from the *Properties* page of the group;
- from the *advanced settings* of the user;

From the *Properties* page

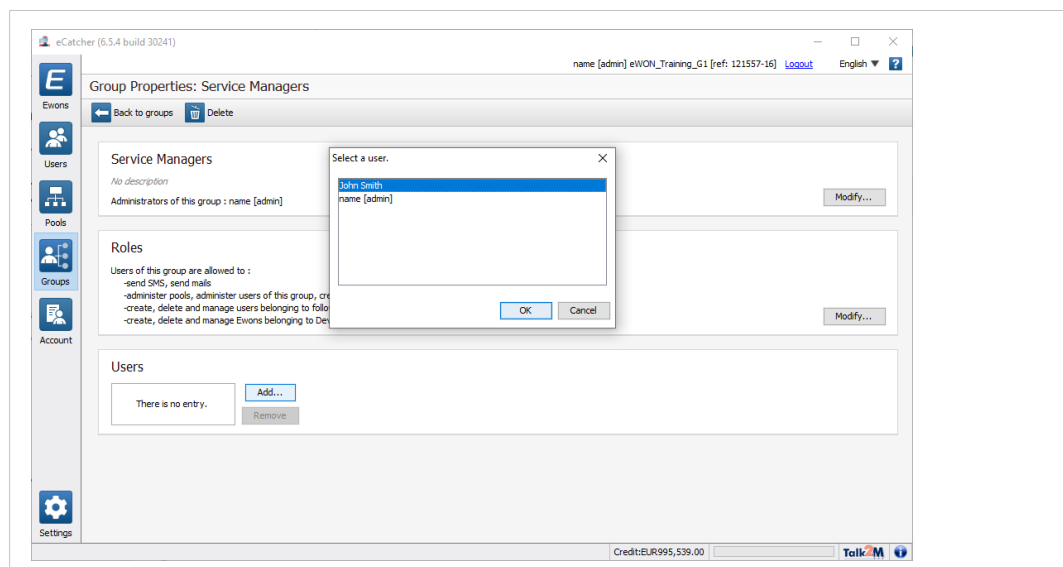
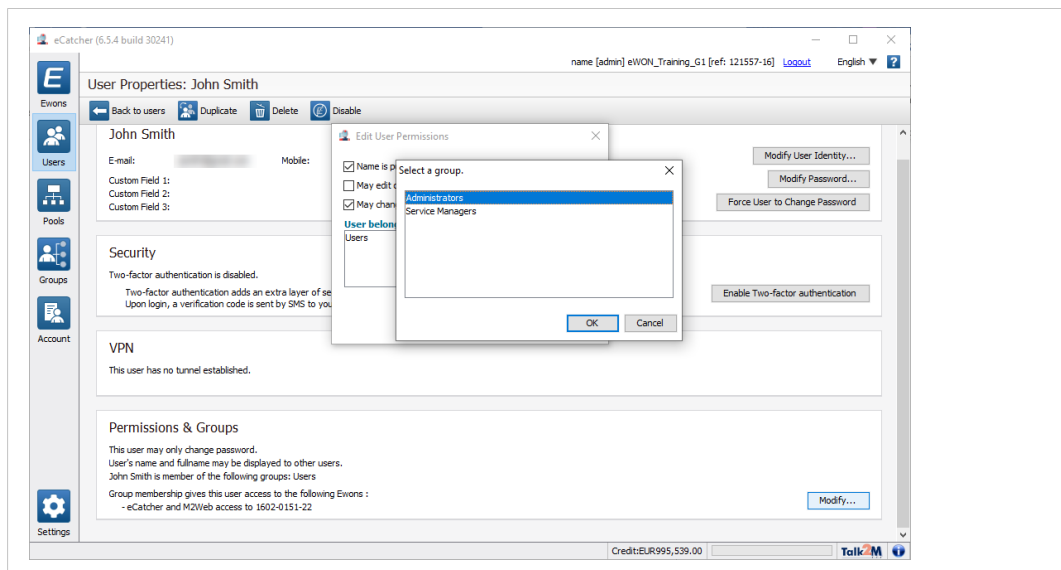


Fig. 11 Add a user through a user group

From the *advanced settings* of the Ewon**Fig. 12** Advanced settings of a user group

They can also be added or removed from a group in the *Permissions & Groups* section of the **<Properties>** page for the user.

4 Examples

For some organizations, the default user groups and Ewon pools are sufficient.

Typically, in cases like these, all users need to be able to access all equipment.

For example: a machine builder might want to grant their own service engineers access to all the machines since they might need to support them.

Similarly, a factory owner might want to grant their all of maintenance team access to all the machines within their own facilities. Access is limited to users with similar roles.

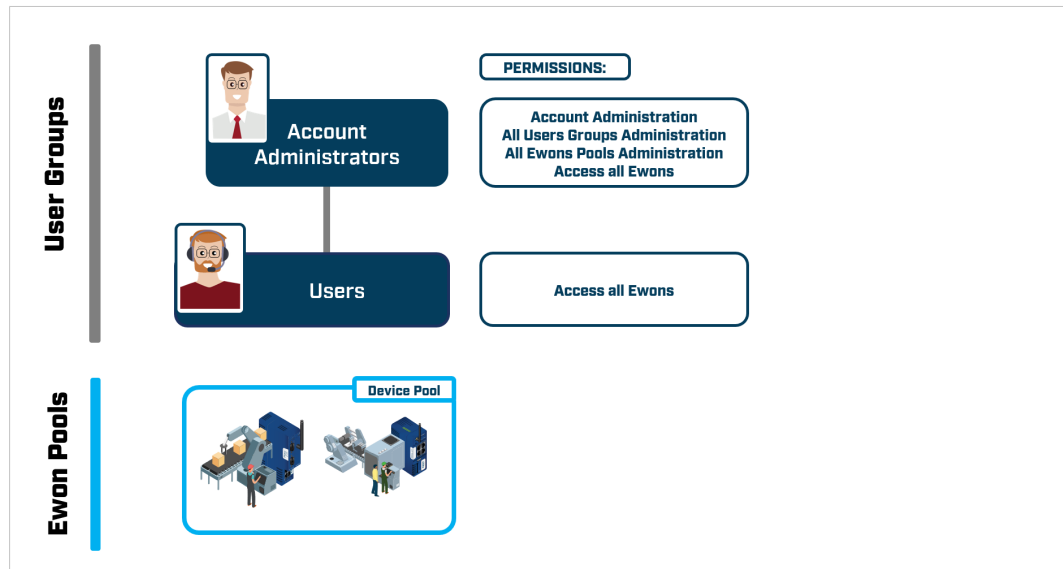


Fig. 13 User rights example

In this configuration all users on the Talk2M PRO account have full access to the connected equipment, but only members of the Administrator group, such as the service team managers or IT managers, have the right to add or delete users and Ewons.

Once an organization wants to grant different levels of access to different types of users, more user groups and Ewon pools become necessary.

Below are some examples of how different organizations might configure their Talk2M PRO accounts.

4.1 Machine Builder

While a machine builder needs to be able to access all their machines for remote support, they might also want to give their customers the ability to monitor key values on their machines.

With Talk2M, the machine builder can grant different levels of access rights to their own service team from their customers.

The service team has full remote access to all machines and customers are limited to remotely monitoring their own machines through M2Web.

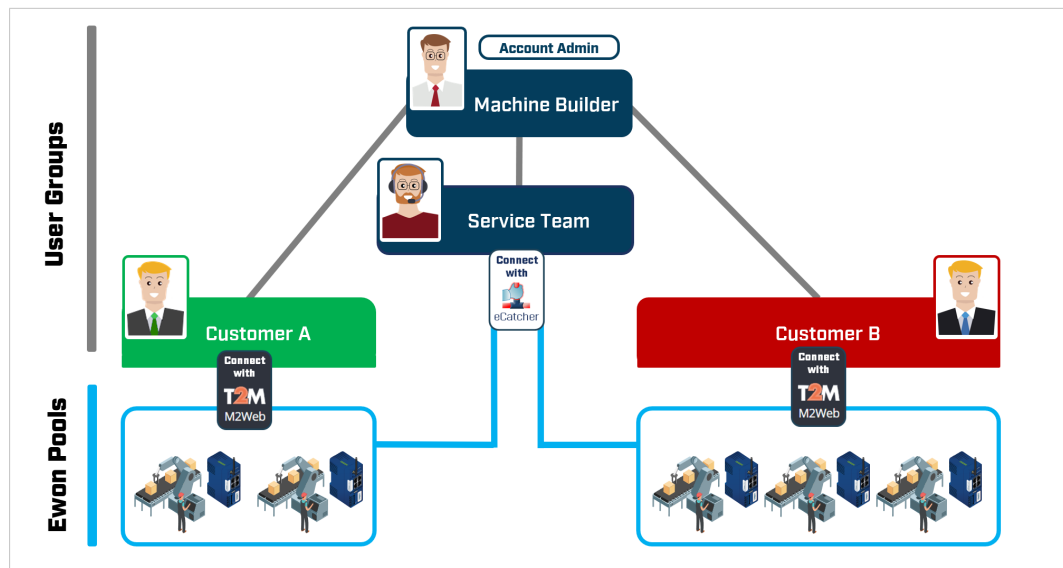


Fig. 14 Example 1 – user permission

To do this, the machine builder creates an Ewon pool for each of their customers.

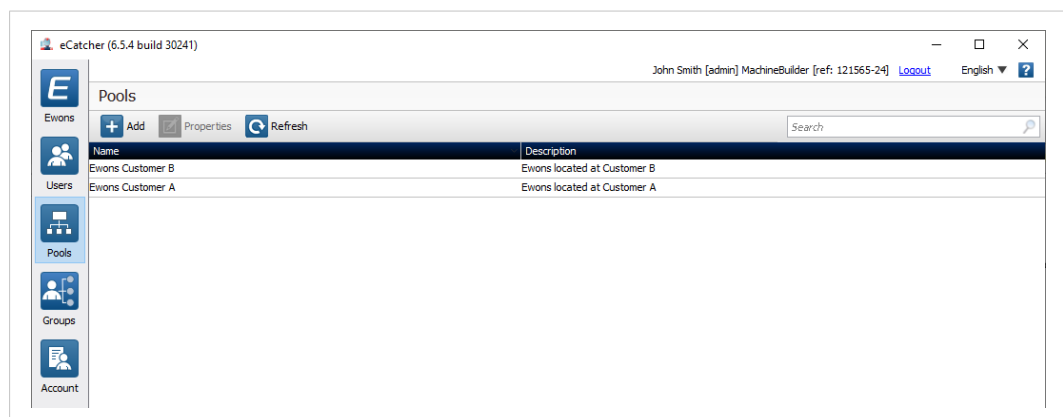


Fig. 15 Example 1 – Pools of Ewons

Then the machine builder makes a user group for each customer.

These user groups only have M2Web access to the Ewons in the pools.

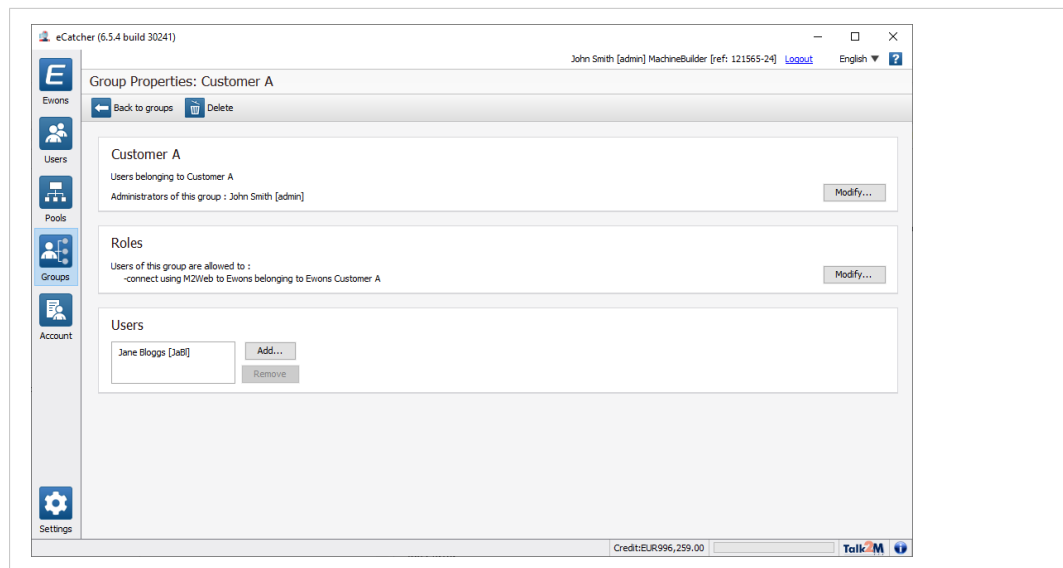


Fig. 16 Example 1 – Properties of group

The machine builder also makes a user group for their Service Engineers.

The members of this group can administer the Ewons in all the pools.

This means they can add, delete, and modify the Ewons in the pools as well as connect to them through eCatcher and M2Web.

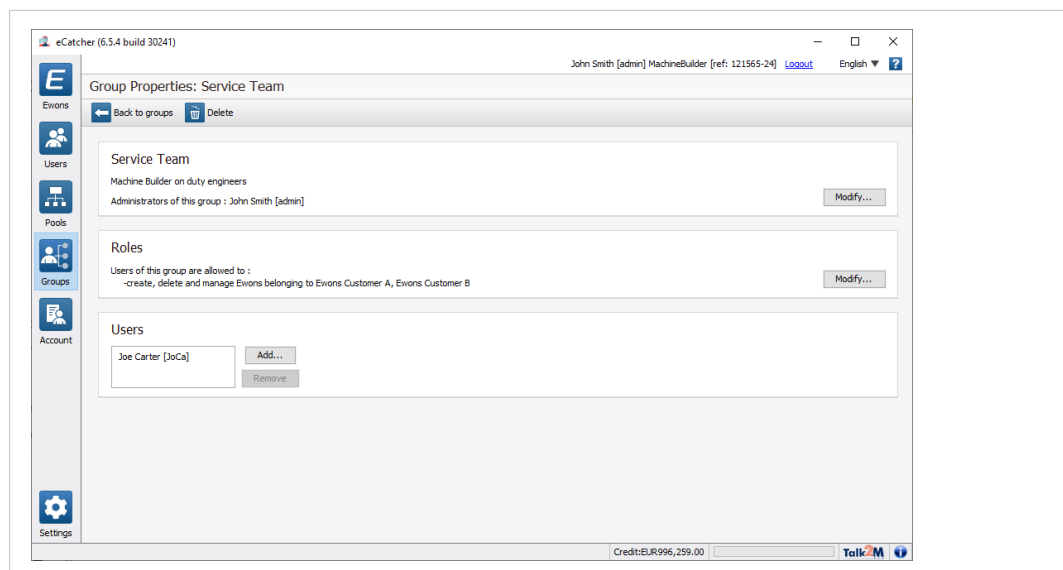


Fig. 17 Example 1 – Group properties

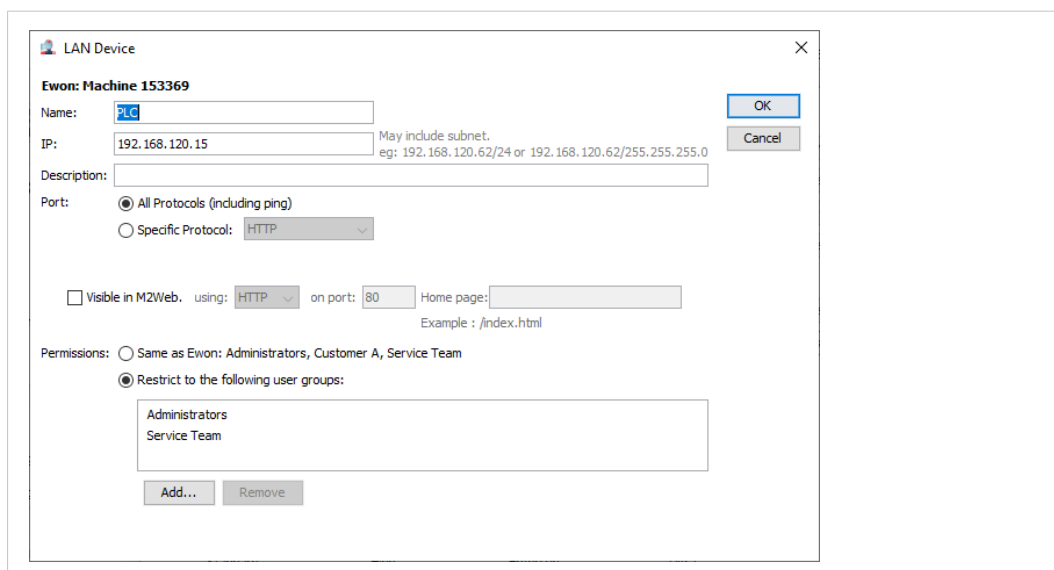
The default Administrator group maintains the rights to create new pools and groups and administer all Ewons and users. The managers of the service team would be members of the Administrator group.

Once the Ewon pools and user groups are created, each user can only see and connect to the Ewons for which they are authorized.

However, to restrict what each group can access on and behind an Ewon, the *LAN Devices and Firewall* settings must be configured for each Ewon.

In the *LAN Devices and Firewall* section of the **<Properties>** page for each Ewon, the machine builder sets the firewall setting to **Ultra** to restrict access to the LAN devices and to the Ewon's gateways and services.

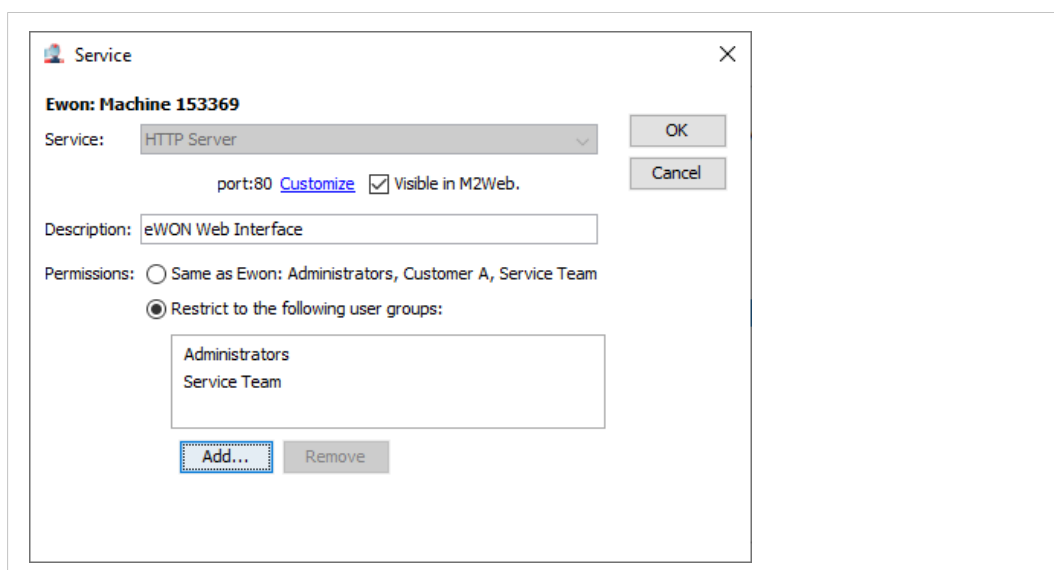
Since the Service Engineers need to access the devices behind the Ewon and the customers should not, the LAN Devices, such as the machine's PLC and HMI, are defined and only the Administrators and Service Team are granted access.



The screenshot shows the 'LAN Device' configuration window for 'Ewon: Machine 153369'. The 'Name' field is set to 'PLC'. The 'IP' field is '192.168.120.15' with a note 'May include subnet. eg: 192.168.120.62/24 or 192.168.120.62/255.255.0'. The 'Description' field is empty. The 'Port' section has 'All Protocols (including ping)' selected. There is a checkbox for 'Visible in M2Web' which is unchecked, with 'using: HTTP on port: 80' and a 'Home page' field with an example '/index.html'. The 'Permissions' section has 'Restrict to the following user groups:' selected, with a list containing 'Administrators' and 'Service Team'. 'Add...' and 'Remove' buttons are at the bottom.

Fig. 18 Example 1 – LAN device

The Ewon's services are similarly restricted to prevent unauthorized access of the Ewon's webserver by the customers.



The screenshot shows the 'Service' configuration window for 'Ewon: Machine 153369'. The 'Service' dropdown is set to 'HTTP Server'. Below it, 'port:80' is shown with a 'Customize' link and a checked 'Visible in M2Web' checkbox. The 'Description' field is 'eWON Web Interface'. The 'Permissions' section has 'Restrict to the following user groups:' selected, with a list containing 'Administrators' and 'Service Team'. 'Add...' and 'Remove' buttons are at the bottom.

Fig. 19 Example 1 – Service

When the account is configured like this, the members of the Service team can see and access their machines for remote programming and troubleshooting through eCatcher.

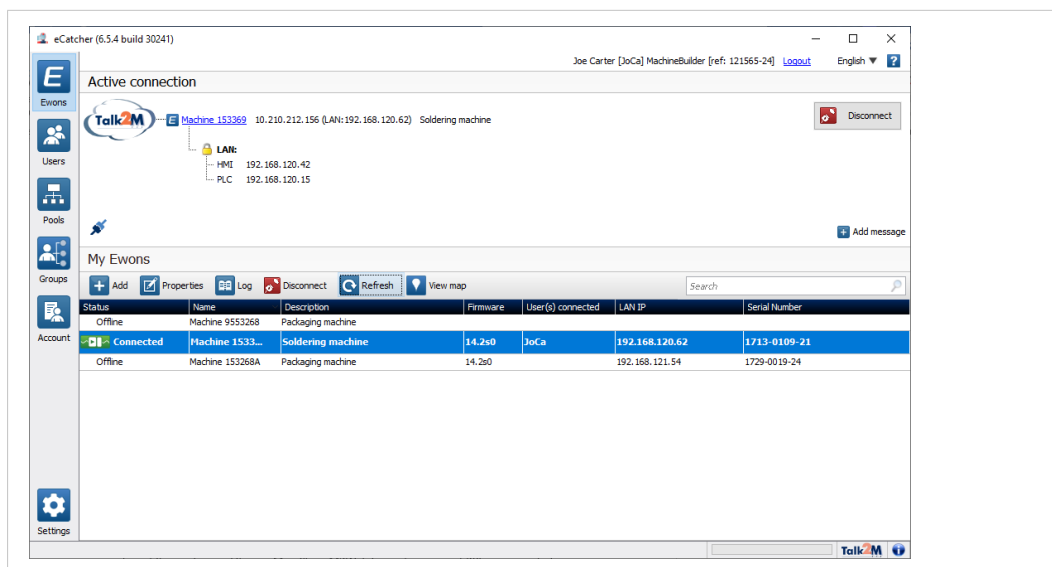


Fig. 20 Example 1 – eCatcher window

At the same time, the customers can see the KPIs that the machine builder configured to display for them (using M2Web), but they cannot connect to anything to make changes.

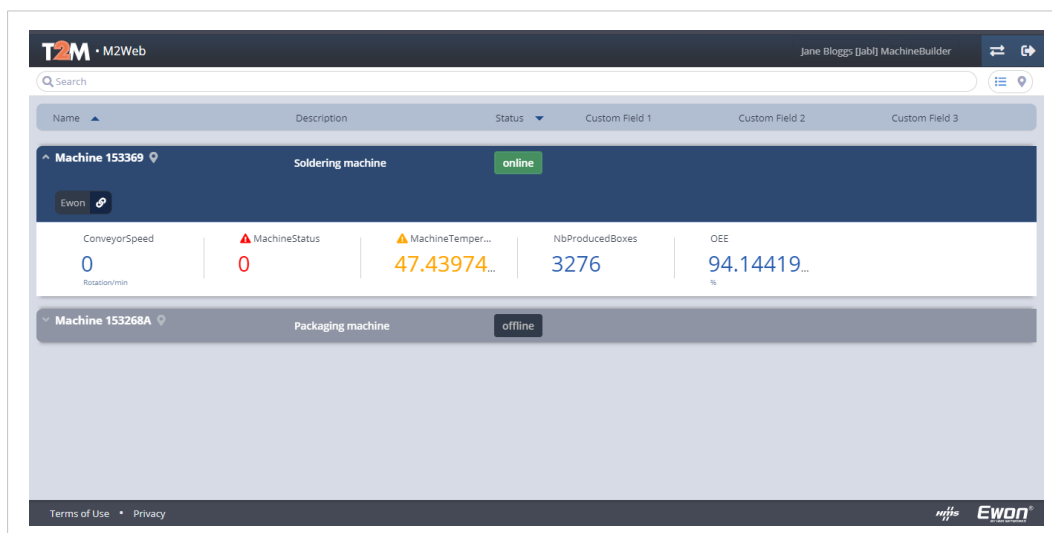


Fig. 21 Example 1 – M2Web platform

4.2 Factory Owner

A factory owner might have machines from many different machine builders.

From time to time, the machines have problems and the factory owner needs the machine's builder to provide support.

With a Talk2M Pro account, the factory owner can give remote access privileges to the machine builder for troubleshooting and support.

Using user groups and Ewon pools, the factory owner can limit the machine builder's access to only those devices supported by the machine builder and grant access only when a machine needs to be serviced; during all other times, the machine builder's access is disabled.

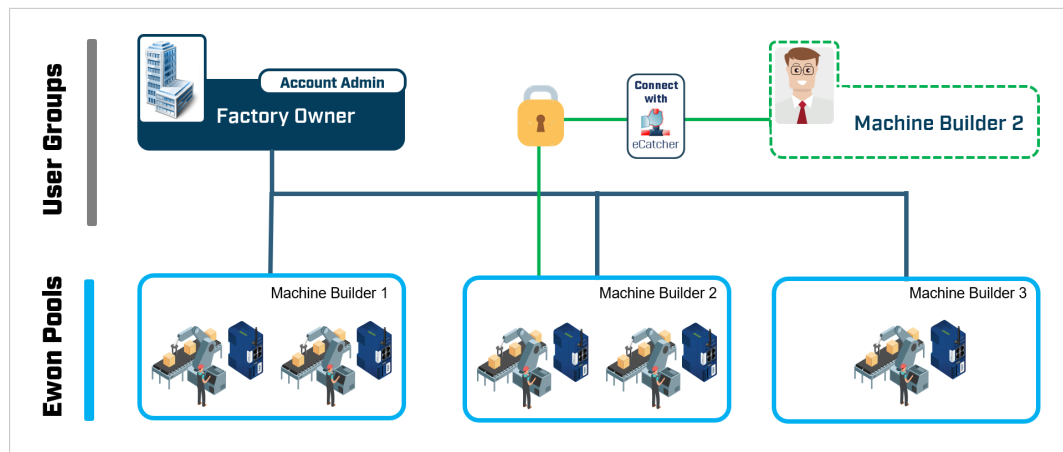


Fig. 22 Example 2 – Scheme of example

In this example, the factory owner creates an Ewon pool for each of their machine builders.

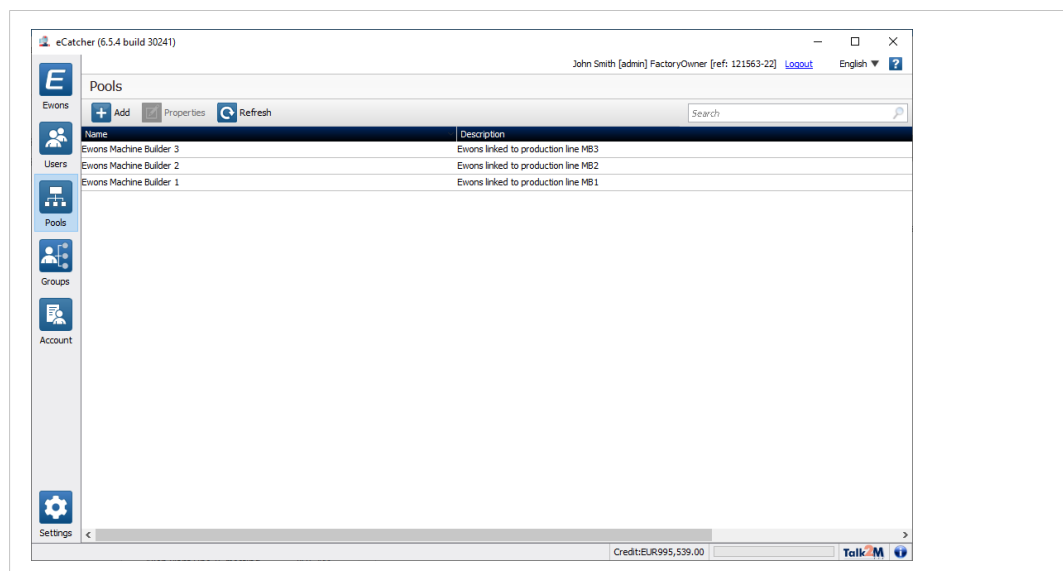


Fig. 23 Example 2 – Pools

Then the factory owner makes a user group for each machine builder.

These user groups can connect to the Ewons associated with their machines through eCatcher and M2Web, but they cannot administer those Ewons.

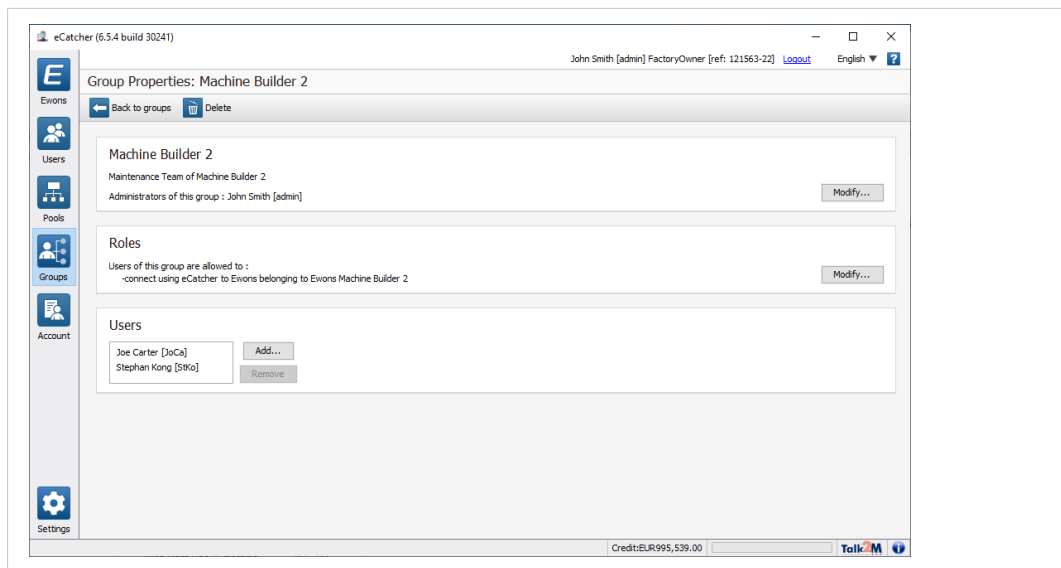


Fig. 24 Example 2 – Group properties

The default Administrator group maintains the rights to create new pools and groups and administer all Ewons and users.

Since the factory owner only wants to allow the machine builder access when there is a problem, users are set to disabled until needed.

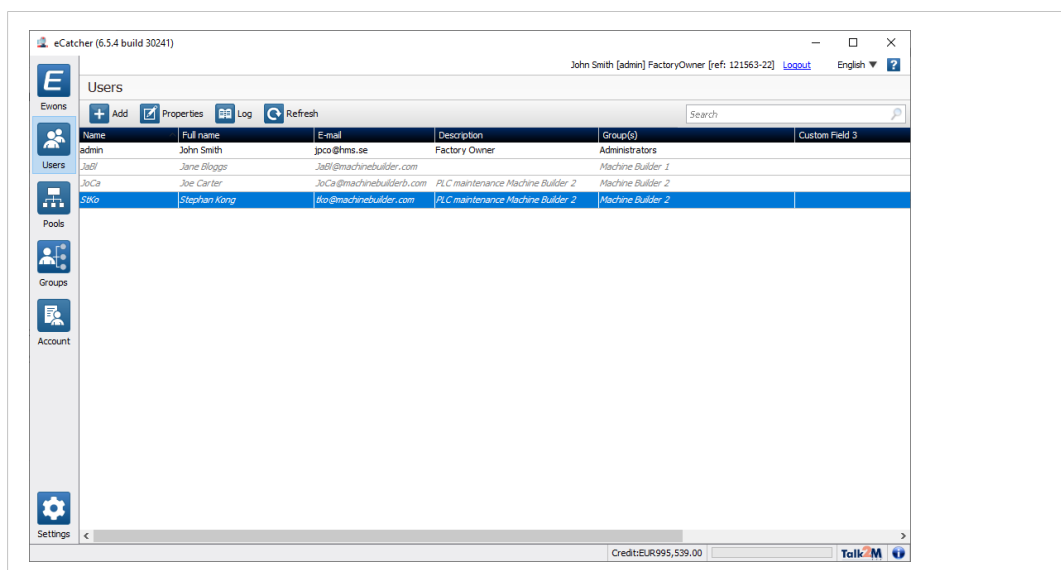


Fig. 25 Example 2 – eCatcher window

When a problem occurs and the factory owner needs support, he can enable the appropriate user.

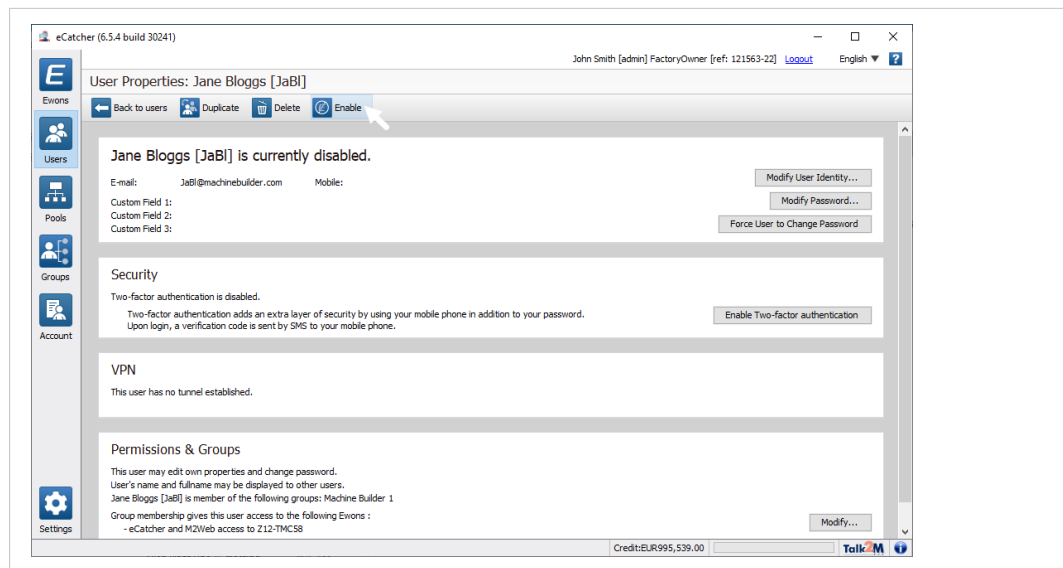


Fig. 26 Example 2 – Enable a user

Once the user is enabled, the user can log in, connect to the Ewon, and troubleshoot the problem.

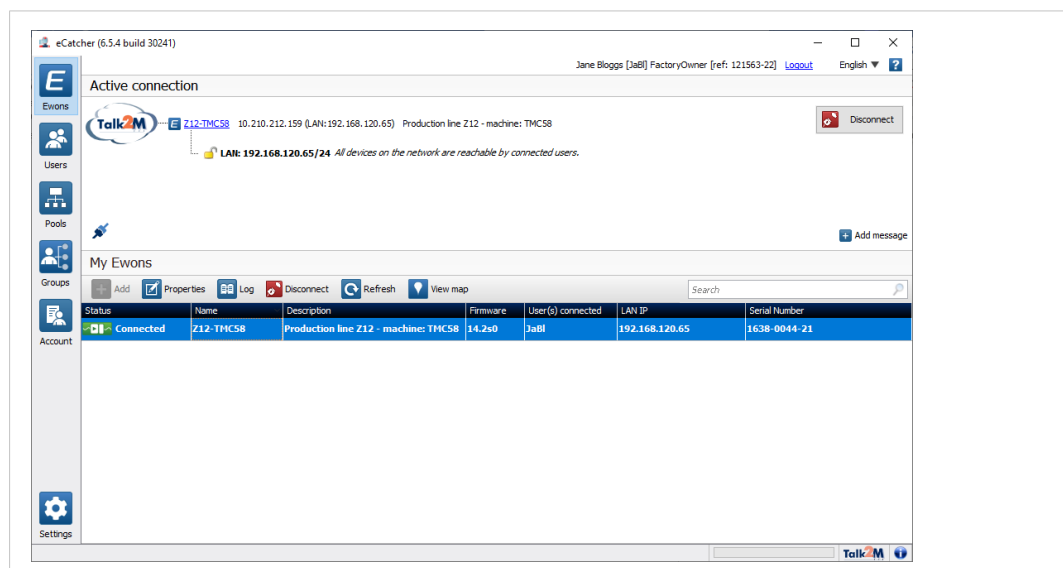


Fig. 27 Example 2 – Active connection

When the problem is resolved, the user can again be set to disabled and can no longer access any machines.

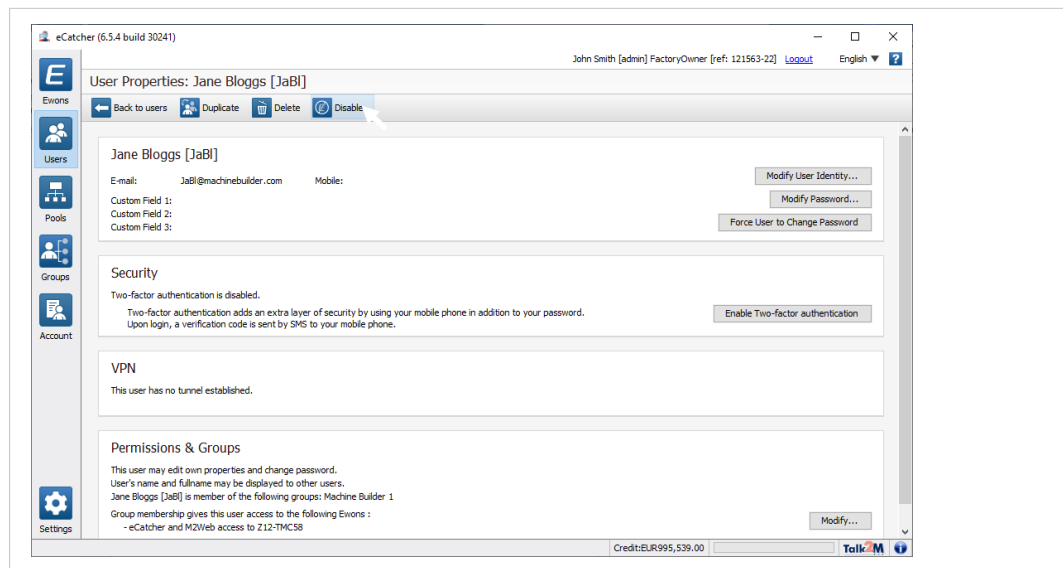


Fig. 28 Example 2 – User properties

