



RFM

Router Fleet Manager

SETUP GUIDE

RFM product family is manufactured by

ETIC TELECOM
13 Chemin du vieux chêne
38240 MEYLAN
FRANCE

In case of difficulty in implementing the product, you can contact your reseller, or contact our support service:

TEL : + (33) (0)4-76-04-20-05
E-mail : hotline@eticlecom.com
web : www.eticlecom.com

TABLE OF CONTENTS

PRESENTATION.....	6
1 Aim of the document	6
2 Main characteristics of the RFM family.....	6
PREPARE CONFIGURATION	7
1 PC connection for configuration	7
1.1 Introduction.....	7
1.2 First configuration	8
1.3 Subsequent modification of the configuration	8
2 Return temporary to factory configuration	9
3 Return to factory configuration	9
4 Protect access to the configuration interface	9
5 Access to the fleet configuration interface	10
6 Configuration steps	12
ROUTER CONFIGURATION	13
1 Configure the LAN IP address.....	13
2 Configure the Internet connection	14
2.1 Access via the LAN interface.....	14
2.2 Access via the Ethernet WAN interface	14
3 Configure the connection to the M2Me service.....	15
FLEET CONFIGURATION.....	16
1 Operating principle.....	16
1.1 General principles	16
1.2 Synchronization modes.....	16
1.3 Sites and groups of sites	16
1.4 Users and user groups	16
1.5 Pairing / synchronization	17
2 Secure access to the fleet management interface.....	18
3 Add a site to the fleet.....	19
3.1 Configuration steps.....	19
3.2 Step 1: Create a site	19
3.3 Step 2: Activate synchronization	20
3.4 Step 3: Check the site	20
3.5 Open the RAS administration interface on M2Me (recommended)	22
4 Add a user to the fleet	23
4.1 Create a user	23
4.2 Create a temporary user.....	24
4.3 Create a user group	24
4.4 Assign the user to a group	26
4.5 Give specific access rights to the user	26
5 M2Me client configuration	28
6 Password policy definition	30
6.1 Add password complexity constraints.....	30

TABLE OF CONTENTS

6.2	Add password renewal constraints	30
7	Check the state of the fleet	31
8	Trace fleet modifications	32
9	Configuration management	34
9.1	Backup / restore	34
9.2	Encryption of configuration files	35
9.3	Automatic backup	36

PRESENTATION

1 Aim of the document

This document describes how to configure the products of the RFM family manufactured by ETIC TELECOM.

It is applicable from software version 1.1.0.

2 Main characteristics of the RFM family

RFM products allows a fleet of RAS routers to be configured remotely.

Main characteristics:

- Available in 220v table box
- Compatible with all our range of routers
- Management of a list of users and user groups
- Ephemeral users
- Fine configuration of access rights to each site or equipment
- Definition of a password policy
- Configuration & diagnostics via an html server
- Automatic configuration saving

PREPARE CONFIGURATION

1 PC connection for configuration

1.1 Introduction

The RFM is configured using a PC equipped with a web browser. No additional software is required. The RFM is a router on which is installed a management system for a fleet of routers. It therefore has an HTML configuration interface for the network part (administration server) identical to that of our range of routers as well as a configuration interface dedicated to fleet management (fleet management server).

Each configuration interface has a configuration file as well as its own configuration backup system.

Administration server Address:

On delivery, URL for accessing the administration web server is <http://192.168.0.128:8080>

RAS Fleet Management Server Address:

On delivery, URL for accessing the administration web server is <https://192.168.0.128:443>

The default identifiers of the RFM interface are:

User: etic

Password: etictelecom

Configuration:

The first configuration is preferably done by connecting the PC directly to the Ethernet LAN connector. Subsequent modifications can additionally be carried out remotely.

Restoration of the factory IP address:

The factory IP address 192.168.0.128 can be restored by pressing the push button on the back of the product.

Access protection to the administration server:

If you cannot access the administration server, access has probably been restricted for security or other reasons.

Network address format:

In the remainder of the text, we call "network address" the lowest value IP address of the network. For example, if the netmask is 255.255.255.0, the network address is X.Y.Z.0.

PREPARE CONFIGURATION

1.2 First configuration

Step 1: Create or modify the TCP / IP connection of the PC

Assign the PC a different IP address that is consistent with the factory IP address of the RFM; for example, the address 192.168.0.1 for the PC.

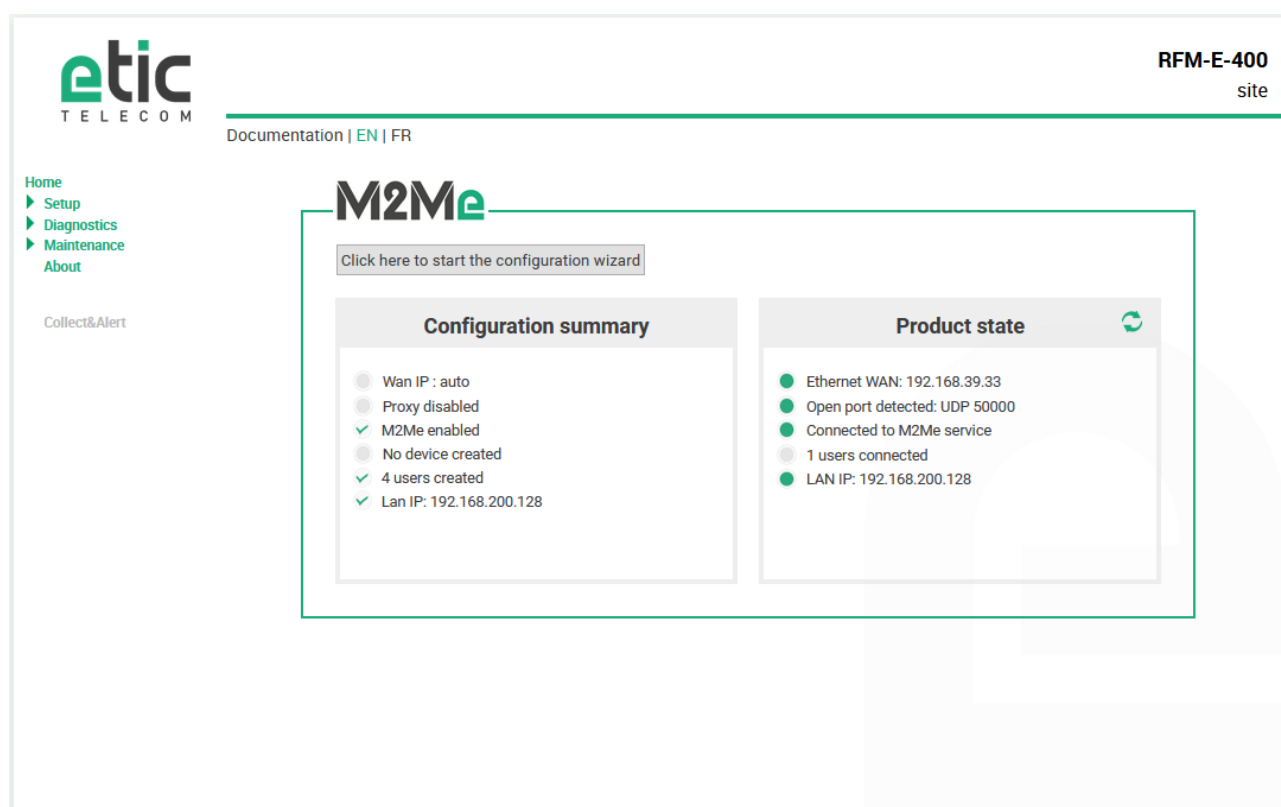
Step 2: Connect the PC to the RFM

Connect the PC directly to the RFM using a straight or crossover Ethernet cable.

Step 3: Launch the browser

Start the browser and enter the URL of the RFM administration server: <http://192.168.0.128>

The administration server home page is displayed.



Note: When configured for the first time, access to the administration server is not protected. It is strongly recommended that you [protect access to the configuration interface](#).


1.3 Subsequent modification of the configuration

Subsequently, the RFM administration server can be accessed from the Ethernet interface at the IP address assigned to the product.

- Open the html browser and enter the URL for accessing the RFM administration server.
- Enter the username and password, if applicable, programmed to protect access to the administration server.

2 Return temporary to factory configuration

If the IP address of the RFM cannot be identified, or if it is impossible to access the administration server following a configuration error, it is possible to restore the Factory configuration without losing the current configuration.

- Keep the push-button pressed for about 3 seconds.
- The indicator light  flashes red rapidly.
- The administration server becomes accessible at the Factory IP address (192.168.0.128), in HTTP and without authentication. The configuration temporarily applied is the Factory configuration. However, the current configuration is not lost and is the one that is still visible in the pages of the administration server.
- After reading the IP address or changing parameters of the displayed configuration, press the push-button again or switch the product off and then on again.
- The product becomes reachable again at the registered IP address.

Note:


If the RFM's IP address is not known, the EticFinder software can also be used.

This software detects all ETIC brand products on a local network. After launching the software, click on the "Search" button, then, when the list of products is displayed, double-click on the product address to access its html server.

3 Return to factory configuration

To restore the Factory configuration using the push button,

- Switch off the RFM.
- Press the push button located at the rear of the box.
- Switch on while keeping the push button pressed.

The indicator light  turns red; RFM is initialized and the Factory configuration is restored.

Note: You can also restore the Factory configuration from **Maintenance > Configurations management** of the administration server.

4 Protect access to the configuration interface

- Select **> Setup > Security > Administration rights**.
- Enter the username and password that protect access to the administration server.
- Click on **Password protect the configuration interface**.
- In the field **Protocols to use for configuration** Select **HTTPs only**.

If you lost the administration interface credentials, you must temporarily return to the factory configuration. You can therefore change the password. Restart the router to apply the modified configuration.

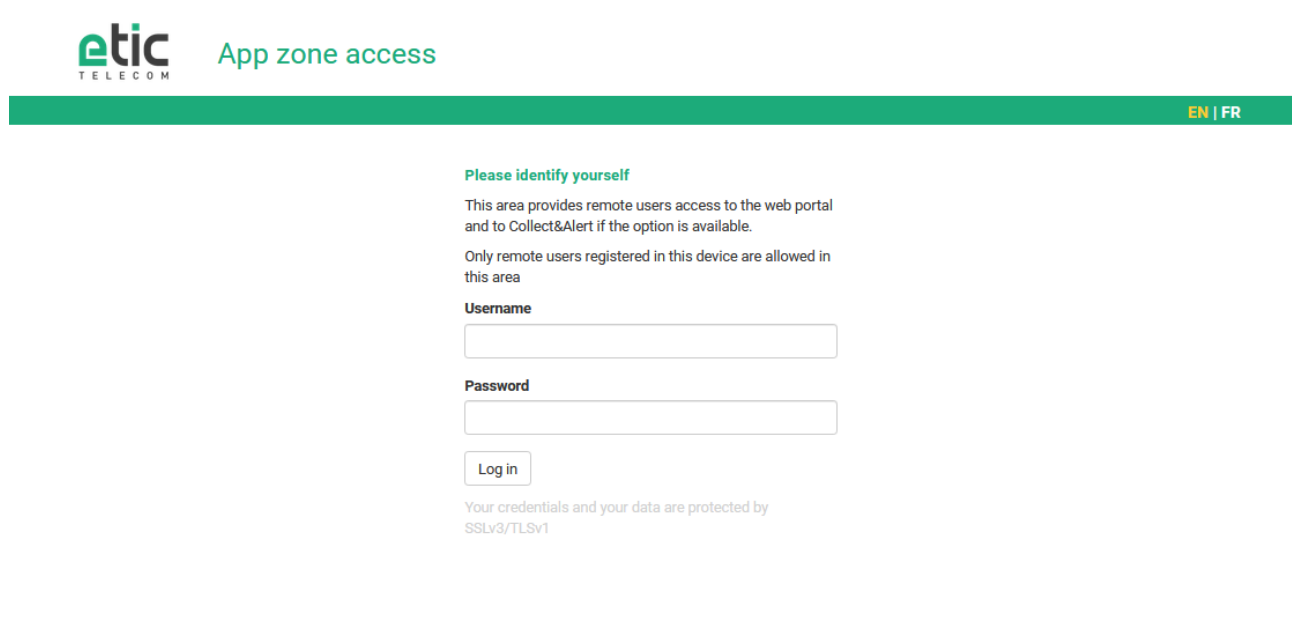
It is possible to disable the push button allowing return to factory configuration by checking **Disable the pushbuttons** in the **> Setup > Security > Administration rights** page.

5 Access to the fleet configuration interface

Access to the fleet configuration interface is also via a WEB browser.

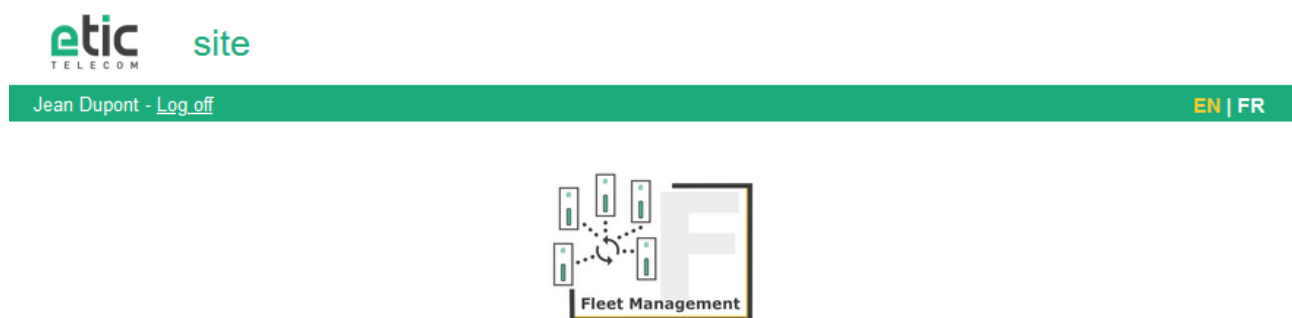
Launch the browser then enter the URL to access the fleet management interface: <https://192.168.0.128:443>

The operating server login page is displayed.



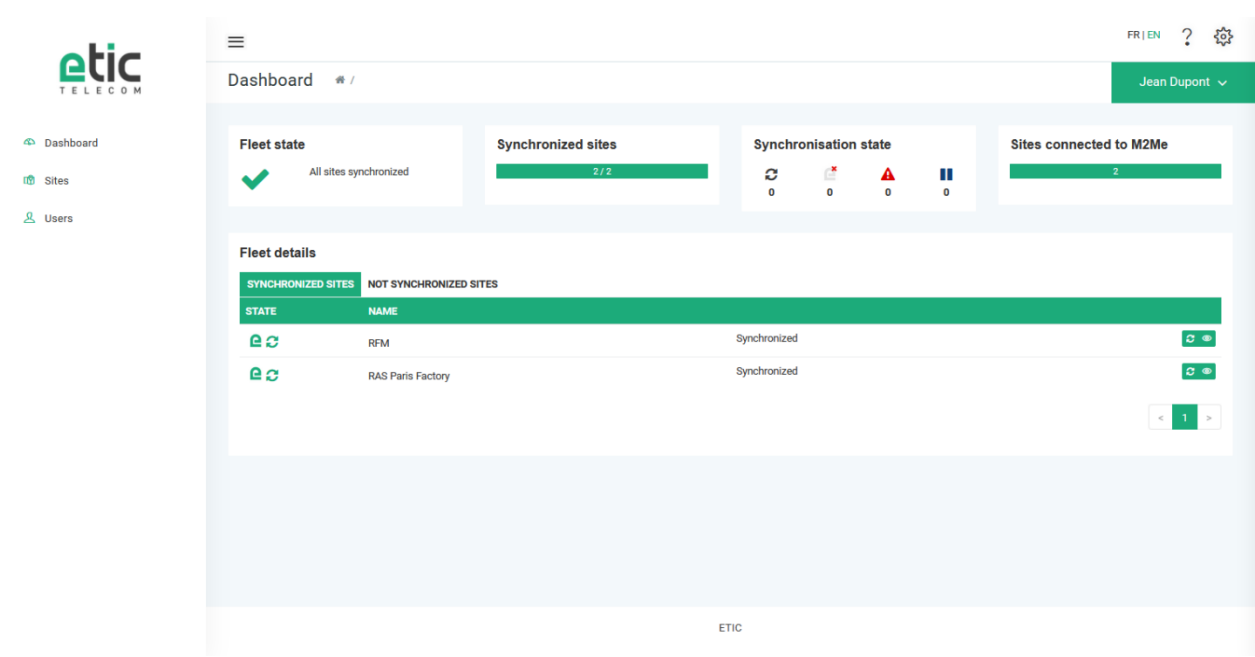
Enter the identifiers of a fleet user with administration rights (default user: etic / password: etictelecom).
The operating server home page is displayed.

To secure access to the fleet management interface, refer to the section [Secure access to the fleet management interface](#).



Click on the **Fleet Management** button.

The fleet management system home page is displayed.



6 Configuration steps

To configure the product, we recommend proceeding as follows:

1. Router settings
 - Connect to the administration interface
 - Configure the Internet connection
 - Configure the connection to the M2Me service
2. Fleet configuration
 - Connect to the fleet management interface
 - Add sites to the fleet
 - Add users / user groups and their access rights

ROUTER CONFIGURATION

The routing functions are configured through the administration interface of the router.
The advanced routing functions are described in the configuration manual of our routers.

1 Configure the LAN IP address

- In the menu, select **Setup > LAN Interface > Ethernet and IP**

The screenshot shows the web-based configuration interface for an etic RFM-E-400 router. The breadcrumb trail at the top reads: **Home > Setup > LAN Interface > Ethernet and IP**. The left sidebar contains a navigation menu with options: Home, Setup (expanded), WAN Interfaces, LAN Interfaces (expanded), Ethernet and IP (selected), Devices list, DHCP Server, WEB portal, Remote access, Network, Security, Serial gateways, System, Diagnostics, Maintenance, and About. The main content area is titled 'LAN network' and contains three sections: 'LAN network' with input fields for IP address (192.168.0.128), Netmask (255.255.255.0), and Default gateway; 'Remote access' with a checkbox for 'Automatic management of the remote users IP addresses' (checked); and 'Advanced parameters' with a checkbox for 'Show advanced parameters' (unchecked). At the bottom are 'Save' and 'Cancel' buttons. The top right corner displays 'RFM-E-400 site' and 'Documentation | EN | FR'.

- Configure the **LAN network** parameters:

IP Address

This is the IP address assigned to the Ethernet interface of the RFM on the local network.
This is the IP address of the administration server.

Default: 192.168.0.128

Subnet mask

The subnet mask defines the structure of the IP addresses of all stations in an Ethernet segment of the local network.

Default value: 255.255.255.0

Default Gateway

This is the default router IP address on the local network. This gateway is only active when no WAN is connected.

2 Configure the Internet connection

2.1 Access via the LAN interface

- In the menu, select **Setup > LAN Interface > Ethernet and IP**

The screenshot shows the 'etic TELECOM' web interface for the 'RFM-E-400 site'. The breadcrumb trail is '> Home > Setup > LAN Interface > Ethernet and IP'. The left sidebar lists navigation options: Home, Setup (expanded), WAN Interfaces, LAN Interface (expanded), Ethernet and IP, Devices list, DHCP Server, WEB portal, Remote access, Network, Security, Serial gateways, System, Diagnostics, Maintenance, and About. The main content area is titled 'LAN network' and contains the following fields:

- IP address:** 192.168.0.128
- Netmask:** 255.255.255.0
- Default gateway:** (empty field)

Below these fields is the 'Remote access' section with a description: 'When a remote user connects to the product, an IP address is automatically assigned to his PC which becomes a part of the local network. Enter below the start and end address that can be assigned to a remote PC.' It includes a checkbox for 'Automatic management of the remote users IP addresses' which is checked.

The 'Advanced parameters' section has a checkbox for 'Show advanced parameters' which is unchecked. At the bottom are 'Save' and 'Cancel' buttons.

Fill the field **Default gateway** with the IP address of the Internet access router.

2.2 Access via the Ethernet WAN interface

- In the menu, select **Setup > WAN Interfaces > Ethernet**

The screenshot shows the 'etic TELECOM' web interface for the 'RFM-E-400 site'. The breadcrumb trail is '> Home > Setup > WAN Interfaces > Ethernet'. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Ethernet WAN port configuration' and contains the following fields:

- Speed / duplex:** Autonegotiation (dropdown menu)
- IP configuration of Ethernet WAN:** Connection type: Ethernet (dropdown menu)
- WAN interface: connection to an Ethernet network:**
 - Ethernet WAN priority: High (dropdown menu)
 - Obtain an IP address automatically: ☒
 - Obtain DNS servers addresses automatically: ☒
 - Enable address translation (NAT): ☒
 - Enable proxy ARP: ☐
- Ping control:**
 - Enable ping control: ☐

At the bottom are 'Save' and 'Cancel' buttons.

IP Address

This is the IP address assigned to the RFM Ethernet interface on the local network.

This is the IP address of the administration server.

Default: 192.168.0.128

3 Configure the connection to the M2Me service

- In the menu, select **Setup > Remote access > M2Me_Connect**

The screenshot shows the etic RFM-E-400 web interface. The breadcrumb trail is: Home > Setup > Remote access > M2Me_Connect. The configuration options are as follows:

Enabled	<input checked="" type="checkbox"/>
UDP ports	50000 <input checked="" type="checkbox"/> 1194 <input checked="" type="checkbox"/> 5000 <input checked="" type="checkbox"/> From 50001 to 51000 <input type="text"/>
TCP ports	50000 <input checked="" type="checkbox"/> 1194 <input checked="" type="checkbox"/> 5000 <input checked="" type="checkbox"/> 443 <input checked="" type="checkbox"/> 80 <input checked="" type="checkbox"/> From 50001 to 51000 <input type="text"/>
Direct access to the Internet (no proxy)	<input checked="" type="checkbox"/>
Show advanced parameters	<input type="checkbox"/>

Connection start parameters

Connect at power on	<input checked="" type="checkbox"/>
Connect when the digital input is on	<input type="checkbox"/>
Disconnect now	<input type="button" value="Disconnect"/>

Check the **Enabled** box.

Select the UDP / TCP ports you want to use to connect to the M2Me service.

FLEET CONFIGURATION

1 Operating principle

1.1 General principles

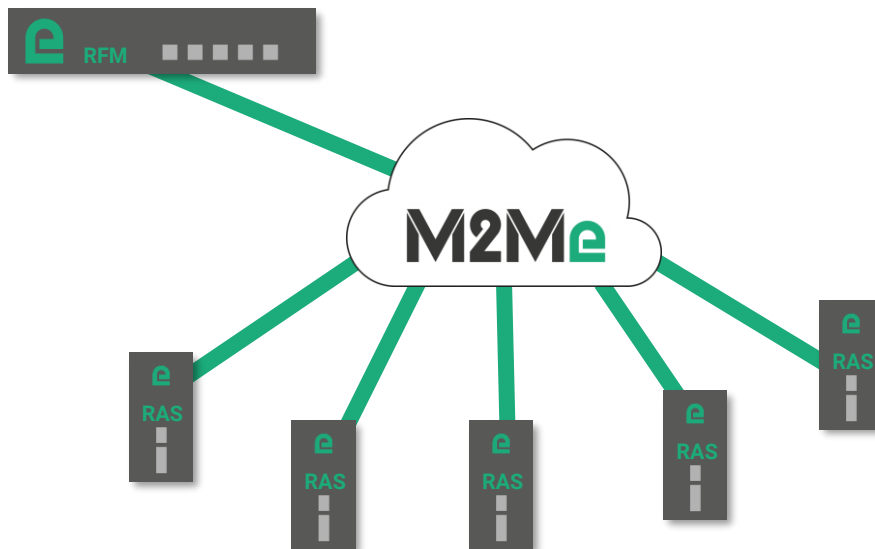


Diagram 1: How the solution works

RFM is a product for centralizing the configuration of a RAS fleet through M2Me. The RFM is compatible with the entire RAS range from Etic Telecom.

The RFM has a graphical interface allowing the configuration of fleet parameters.

1.2 Synchronization modes

To configure a RAS, the RFM uses the RAS configuration http API. He therefore needs to know the credentials of the RAS administrator.

For the RFM to be able to access this HTTP API for configuring the RAS, 2 scenarios arise:

- 1 RFM establishes a user connection to the RAS. It is therefore found in the RAS LAN network and can therefore access to the http configuration interface. **In this case, it is necessary to enter the identifiers of a remote RAS user in the RFM.**
- 2 The RAS has opened its HTTPs configuration interface in the M2Me service (see diagram 2 below). **In this case, the administrator's credentials are sufficient for the RFM to do the remote configuration.**

1.3 Sites and groups of sites


A site is a RAS product identified by its product key. To classify the sites, it is possible to group them.

1.4 Users and user groups

A user is a natural person identified by an identifier / password pair. It is possible to group users to apply access rights more globally. In fact, when a user is added to a group, he directly inherits the access rights defined for the group.

1.5 Pairing / synchronization

When a site is configured, the RFM performs a connection called pairing to verify the connection credentials entered during site configuration and retrieve the list of machines on the RAS. During pairing, no action is taken in the configuration of the remote RAS. It is therefore always possible to log in with the user identifiers created locally in the RAS.

When the administrator puts the site in synchronization mode ( button), the RFM connects to the RAS to write the new list of users and their access rights. It is therefore no longer possible to connect to the RAS with the user identifiers created locally in the configuration of the RAS.

2 Secure access to the fleet management interface

By default, the connection to the fleet management page is secured in HTTPs. From the first connection, it is recommended to create at least one fleet administrator.

To create a fleet administrator, you must create a user and check the box **Ras manager administrator** at the end of the form.

The screenshot shows a form for creating a user. It has two main sections: 'RAS usine Paris' and 'SITES'. The 'RAS usine Paris' section contains a text input field with 'RFM' entered. The 'SITES' section is empty. At the bottom, there is a checkbox labeled 'Administrateur du ras manager' which is checked with a green checkmark. Below the checkbox are two buttons: 'Appliquer' (green) and 'Annuler' (grey).

Once you have created one or more administrators, you must delete the default user.

You can get the list of RFM administrators in the menu **Settings > Security dashboard**.

The screenshot shows the 'Security' dashboard. The top navigation bar includes a menu icon, 'FR | EN', a help icon, and a settings icon. The user 'Jean Dupont' is logged in. The dashboard is divided into two main sections: 'Configuration log' and 'Administrator list'. The 'Configuration log' section has a table with columns 'Info', 'Warning', and 'Error', all of which are checked with green checkmarks. Below the table is a scrollable log of system events. The 'Administrator list' section has a search bar and a table listing administrators: Cornelle LePetit, Guy Lavarre, Jean Dupont, and Mike Dubois. A pagination bar at the bottom of the list shows '1' of 1 items.

NAME ▲
Cornelle LePetit
Guy Lavarre
Jean Dupont
Mike Dubois

3 Add a site to the fleet

This paragraph describes the steps to add a site to the fleet.

3.1 Configuration steps.

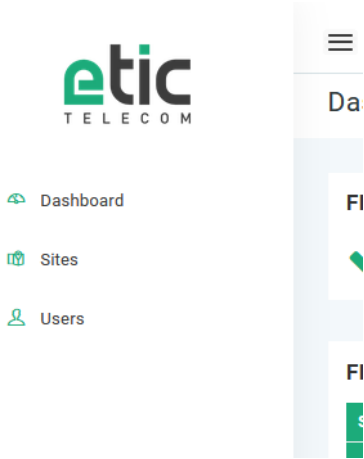
Step 1: Create a site

Step 2: Activate synchronization

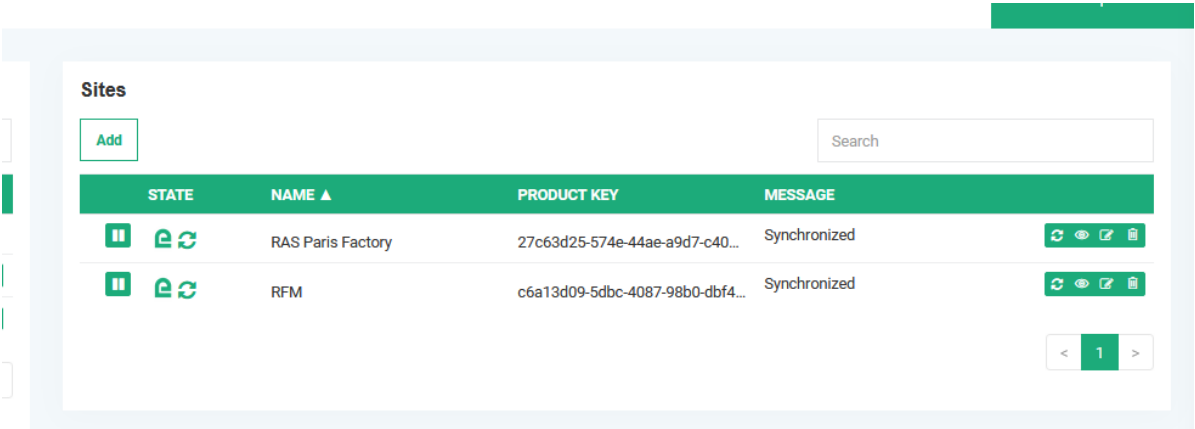
Step 3: Check the site

3.2 Step 1: Create a site

In the left menu select the menu Sites



In the Sites frame click on Add



ROUTER CONFIGURATION

A dialog box opens:

Add site

Name: Test site

Group: No group

Product key: 27c63d25-574e-44ae-a9d7-c40dafbd0713

Configuration access: Directly (with https on RAS firmware > 4.4.1)

Administration credentials

Enter here the identifiers of the Machine Access Box in the configuration menu (Home > Setup > Security > Administration rights)

Administrator: username password

Apply Cancel

Choose a site name then enter the product key.

Once the product key has been entered, if the site's RAS is connected to the M2Me service, the RFM analyses the equipment and adapts the rest of the form according to the configuration mode available on the RAS (see [Synchronization modes](#)).

Note: The product key is available in the menu **Setup > About** of the RAS.

Two scenarios:

- 1 The RAS has opened its administration interface on M2Me (For more reactivity in the synchronization process, it is advisable to configure the RAS in such a way as to use this mode cf. Open the administration interface of the RAS on M2Me)
 - Choose Access to configuration - Direct
 - Enter the credentials of the RAS configuration administrator.
- 2 The RAS has not opened access to its administration interface on the M2Me service.
 - Choose Access to configuration - Via a remote connection
 - Enter the credentials of a remote RAS user.
 - Enter the credentials of the RAS configuration administrator.

3.3 Step 2: Activate synchronization

Once the site is added, RFM performs [a pairing](#) to verify the login credentials. By default, the site is paused; That is to say, it performs a pairing to the site to check its availability as well as the login credentials but does [not synchronize](#) the list of users.



To activate synchronization, you must click on the button  on the line of the site.





3.4 Step 3: Check the site

The site status is shown in the left column of the sites table. The right column indicates the status of the site in text.

Sites

[Add](#)

STATE	NAME ▲	PRODUCT KEY	MESSAGE
 	RAS Paris Factory	27c63d25-574e-44ae-a9d7-c40...	Synchronition suspended The site will be tested in a few minutes



   





< 1 >

Once pairing is complete, activate synchronization. Please note that synchronization overwrites the list of RAS users and replaces it with the one defined by the access rights entered in the RFM.

Sites

[Add](#)

STATE	NAME ▲	PRODUCT KEY	MESSAGE
 	RAS Paris Factory	27c63d25-574e-44ae-a9d7-c40...	Synchronized

< 1 >

Once synchronization is complete, you can test the remote connection to your RAS with your M2Me client (see [M2Me client configuration](#)).

3.5 Open the RAS administration interface on M2Me (recommended)

To simplify the synchronization of the RAS with the RFM, it is possible to open the RAS administration interface on M2Me. When this interface is open to the M2Me service, the RFM no longer needs to establish a user connection to the RAS to perform its maintenance operation.

Activating this mode allows:

- Improved fleet synchronization speed
- Simplification of site configuration

For security reasons the mode is not enabled by default in the RAS configuration.

To activate it, check the box **Enable access by M2Me (HTTPs only)** in the menu **Setup > Security > Administration rights**.

> Home > Setup > Security > Administration rights

Administration credentials

List of administrators

Name	Password
azer	*****

Show Edit Delete Add ... Copy and edit ^ V

Configuration interface

The configuration web interface may be protected by a password. The above values will be used if this feature is enabled. The configuration over the WAN will be enabled only if the password is not the default one and the checkbox is checked.

Password protect the configuration interface ☒

Protocols to use for configuration HTTP and HTTPS

HTTP port for administration (8080) 8080 (1 to 32000, step 1)

HTTPS port for administration (4433) 4433 (1 to 32000, step 1)

Use the factory certificate ☒

Enable access through M2me (HTTPS only) ☒

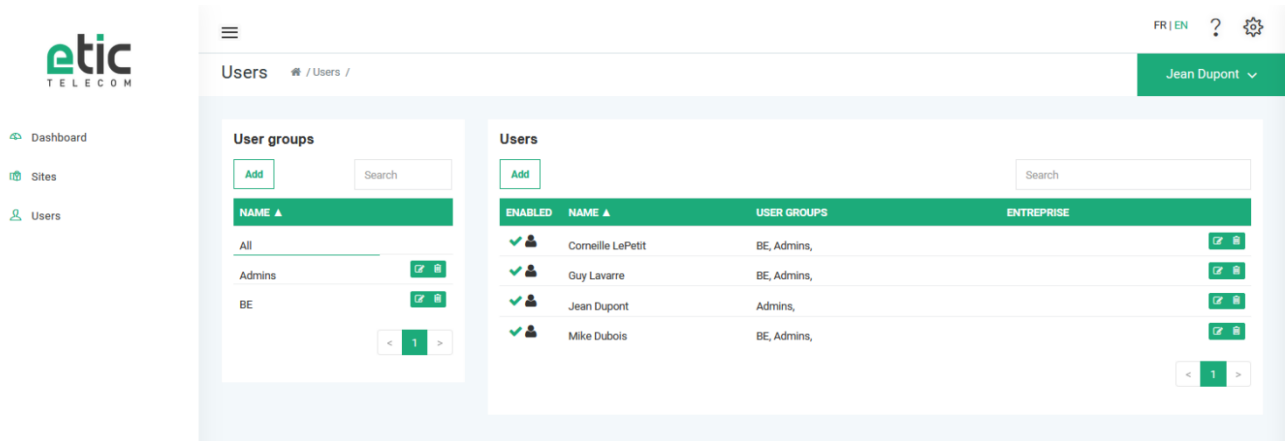
Enable access from the WAN (HTTPS only) ☐

4 Add a user to the fleet

This paragraph describes the steps to add a user.

4.1 Create a user

In the page **Users** click on the button add located on the **Users** frame



A user creation form opens.

Add user

Enable
☒

Temporary
☐

Name
Required

Username
Required

Password

Password must be at least 8 characters long with :

- At least one uppercase character
- At least one uppercase character
- At least one number
- At least one special character

Random

Required
Mismatch

weak

Company

E-mail

Phone

Fill in at least the mandatory fields.

Note: The complexity of the required passwords depends on the password strategy defined in the RFM (see [Password policy definition](#))

4.2 Create a temporary user

The RFM gives the possibility to create a temporary user. This user will be activated on the RAS on the user's start date of validity and then deactivated on the end of validity date.

To create a temporary user, click on the **Add** button in the Users frame, then in the user creation form select the **Temporary** box.

Add user

Enable ☒

Temporary ☒

04/03/2021 18/03/2021

Name
Required

Username
Required

Password Password must be at least 8 characters long with :
- At least one uppercase character
- At least one lowercase character
- At least one number
- At least one special character

Required Mismatch

Then choose a **Start validity** date and an **End validity** date.

4.3 Create a user group

To simplify the configuration of access rights, it is possible to create groups of users. A user group is a set of users with the same rights to access the fleet.

To create a user group, on the **Users** page, click the **Add** button in the **User groups** frame.

Add user group

Name

Required

Users

Users list

Add all

Search

Corneille LePetit

Guy Lavarre

Jean Dupont

Mike Dubois

Selected users

Remove all

Filter

Access rights

Sites list

Add all

Search

RFM

RAS Paris Factory

Selected sites

Remove all

Filter

Sites

Rights

Apply

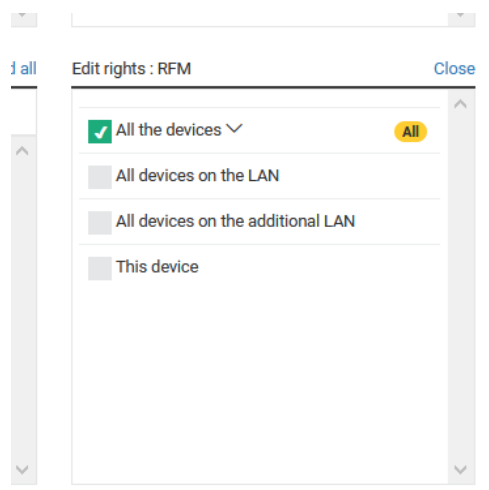
Cancel

Pick a name.

To add a user to the group, in the **Users list** frame click on the user to add. It then appears on the right in the list of **Selected Users**.

To add an access right, choose the sites that the group will be able to access in the **List of sites**. They will then appear under the **Selected Sites**.

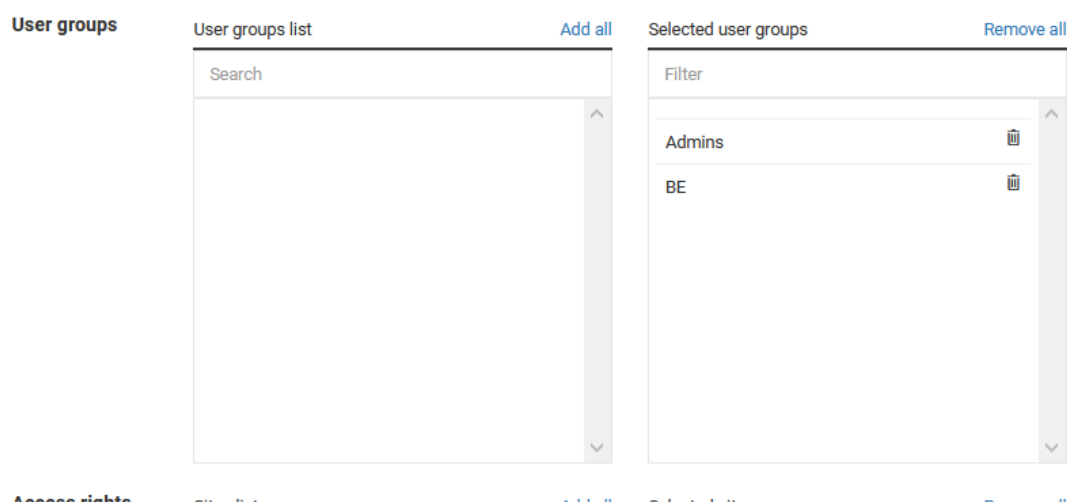
You can then select the rights more finely by clicking on the pencil to the right of the site name.



By default, a user has access to all the devices located in the LAN of the remote RAS.

4.4 Assign the user to a group

To add a user to a group, in the user creation form, select the user or groups to which this user must belong by clicking on the group name. The selected groups will then appear in the **Selected User Groups** frame.

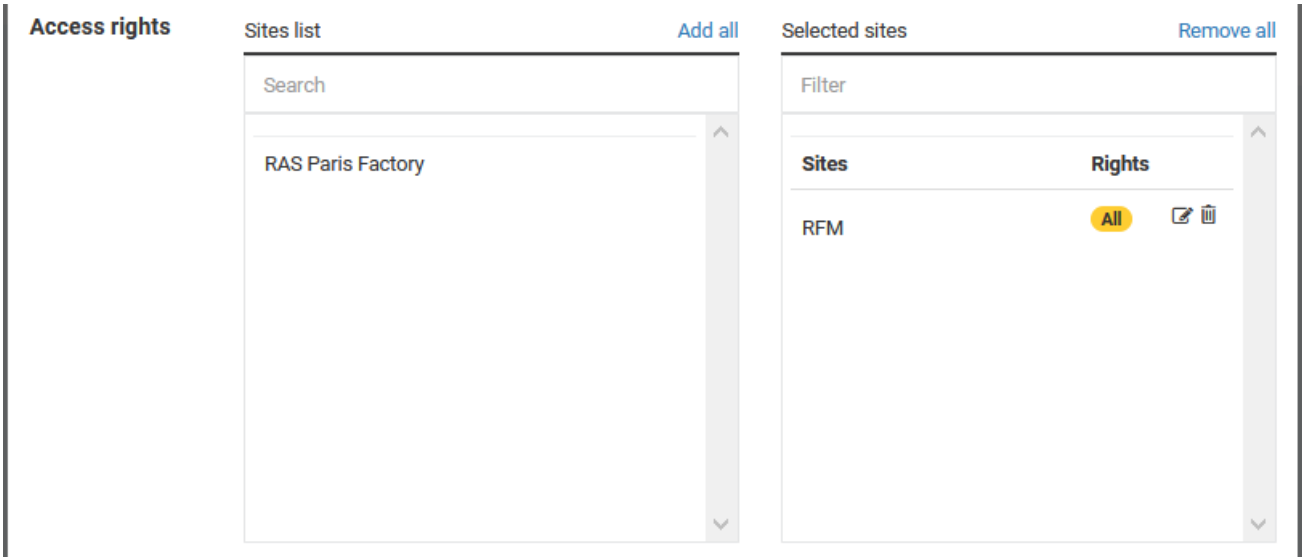


4.5 Give specific access rights to the user

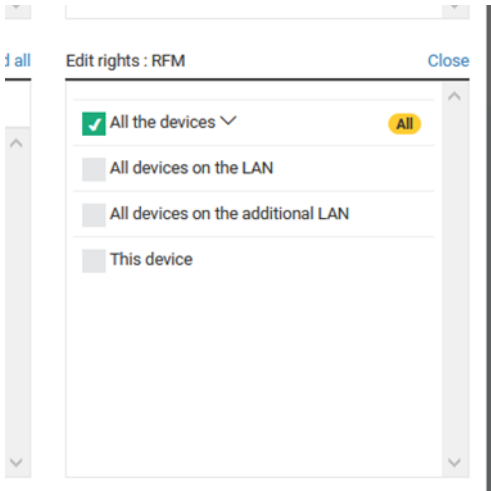
There are two ways to give access rights to a user:

- Assign the user to one or more groups. In this case, he will inherit all the access rights of the group (s) (see [Creating a user group](#))
- Assign specific rights to a user in the user creation form.

To add an access right, choose the sites that the user will be able to access in the List of sites. They will then appear under the **Selected Sites**.



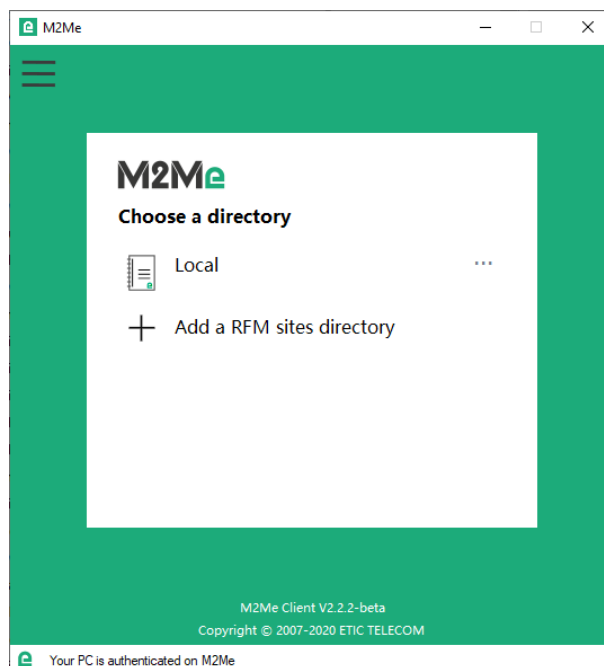
You can then select the rights more finely by clicking on the pencil to the right of the site name.



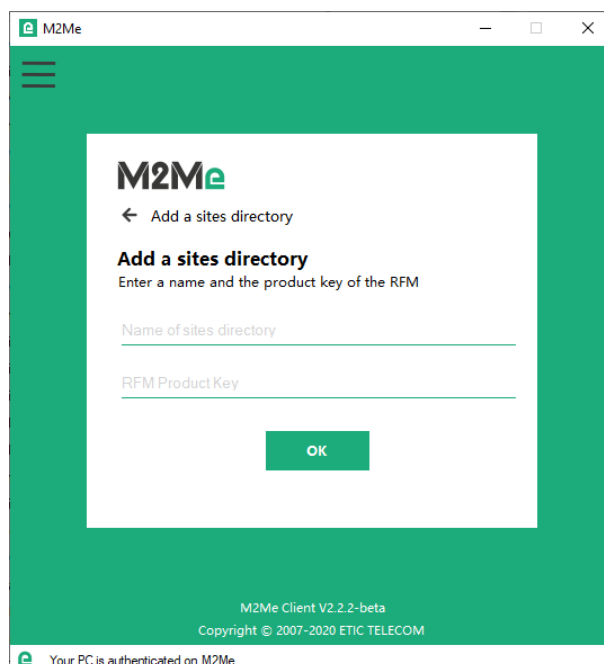
By default, a user has access to all the devices located in the LAN of the remote RAS.

5 M2Me client configuration

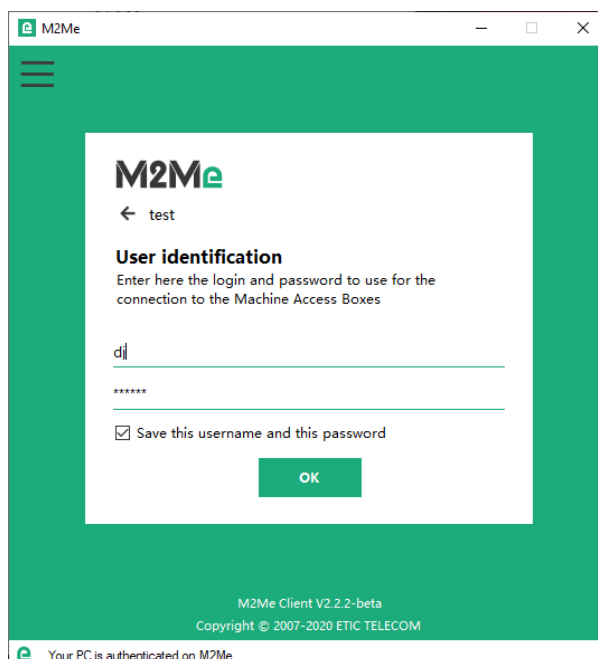
From version 2.2, the M2Me client integrates the synchronization of the site book with the RFM.



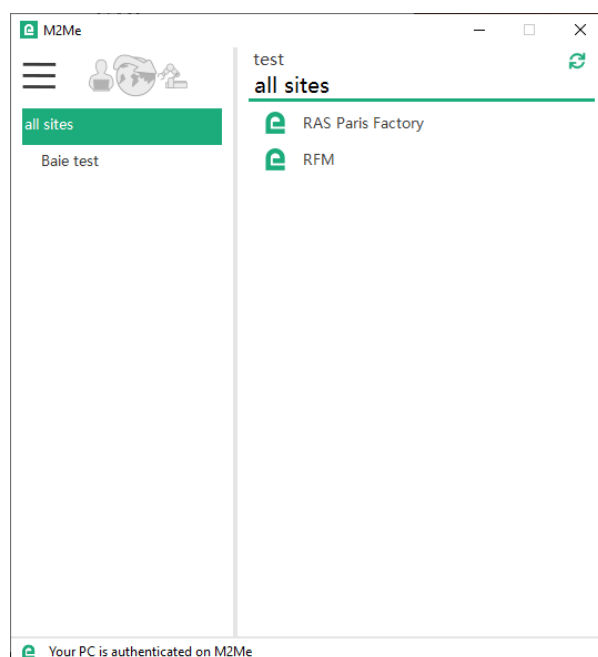
On the home page click on **Add a sites directory**.



Enter a name for the directory and enter the RFM product key (menu **Home > About**).



Fill in the identifiers of one of the users entered in the RFM.



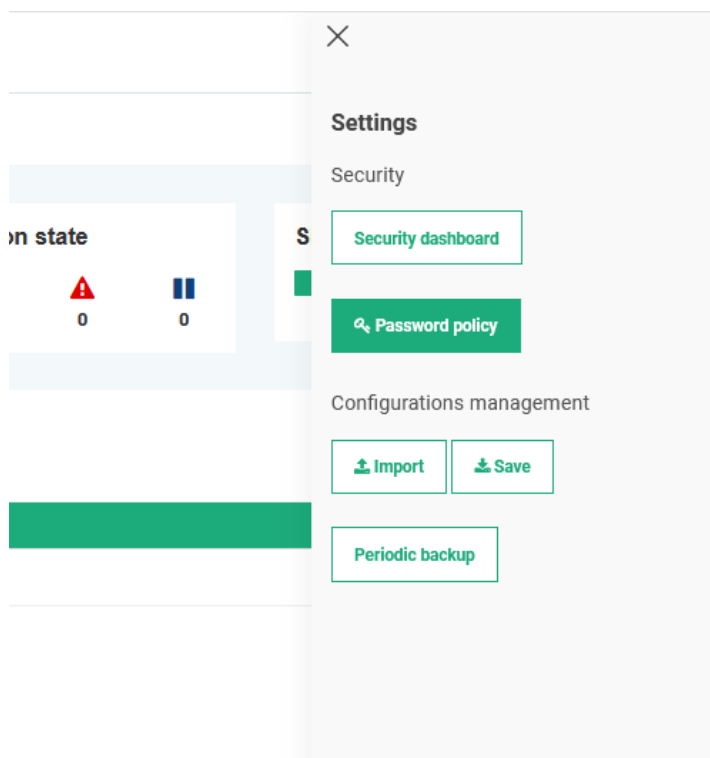
Your sites directory is synchronized with the RFM. Only sites and groups of sites that your user has permission to connect to are displayed.

If the user's password has expired (see [Password policy definition](#)) the M2Me client informs you and allows you to change it.

6 Password policy definition

For optimal security in a remote access system, it is recommended that passwords be chosen directly by end users. Under these conditions, it is necessary to be able to force the user to choose a strong password. To do this, you can define in the RFM a global password policy for your RAS fleet.

The password policy is configured from the settings (symbol  top right).



6.1 Add password complexity constraints

Enforce complex passwords:

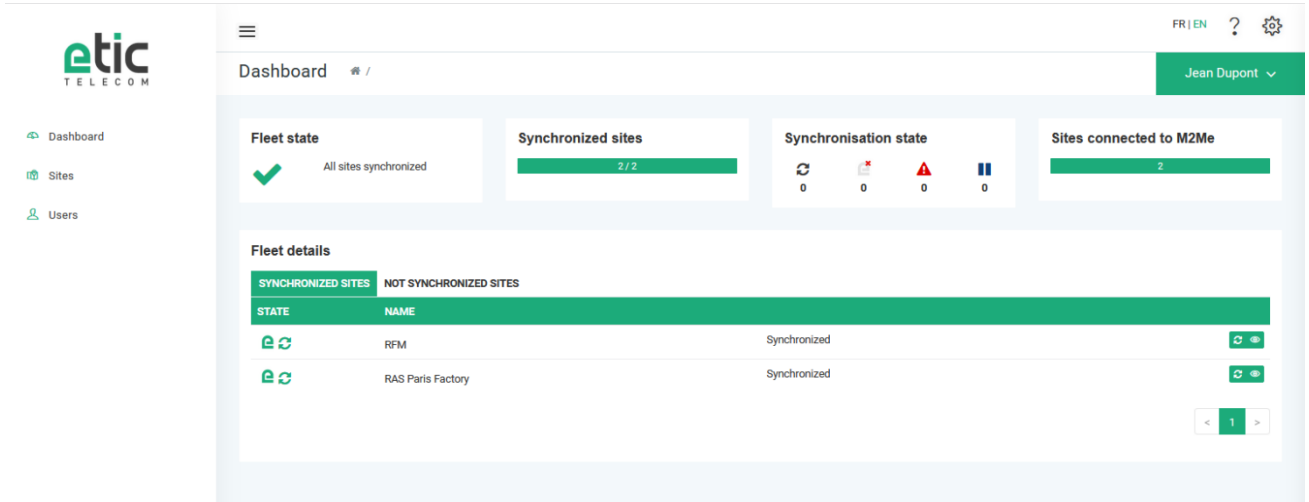
- Minimum number of characters
- Must have at least one lowercase character
- Must have at least one uppercase character
- Must have at least one number
- Must have at least one special character

6.2 Add password renewal constraints

- Allow renewal by users
- Force the renewal of the password at the first connection
- Set a password validity
- Minimum password age before renewal request (in days)
- Maximum age of the password before deactivation (in days)

7 Check the state of the fleet

Click on the menu and select **Dashboard**.

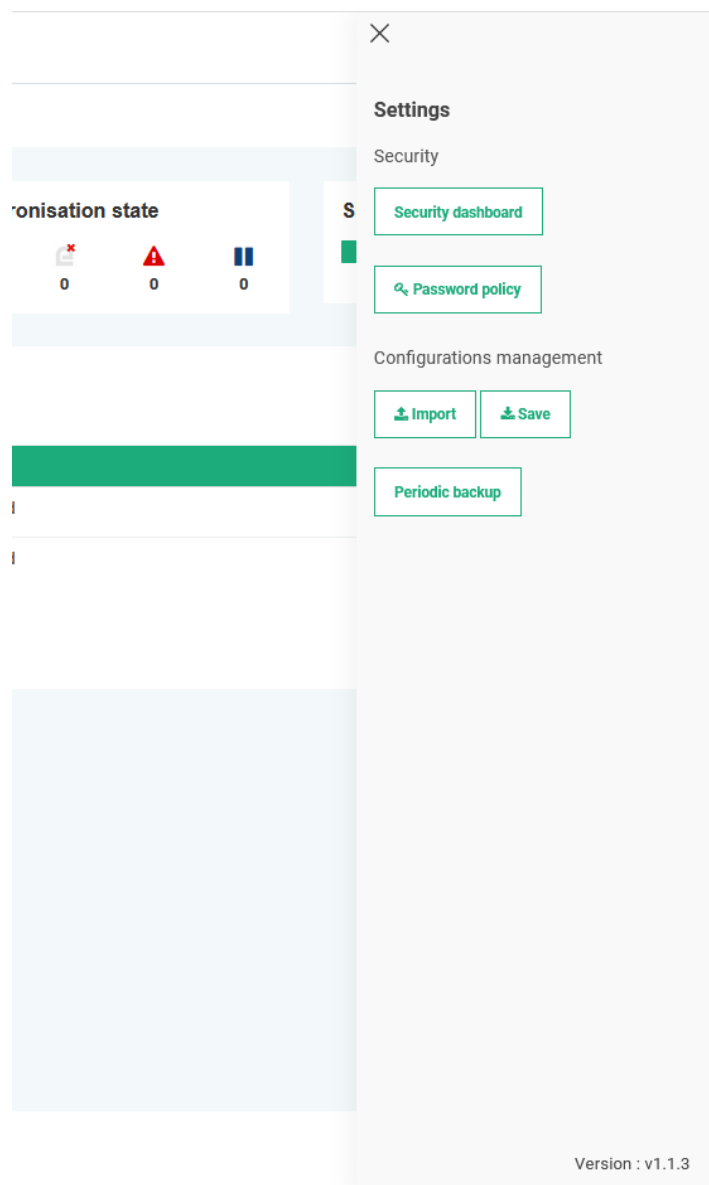


The overall state of the fleet is summarized on this page.

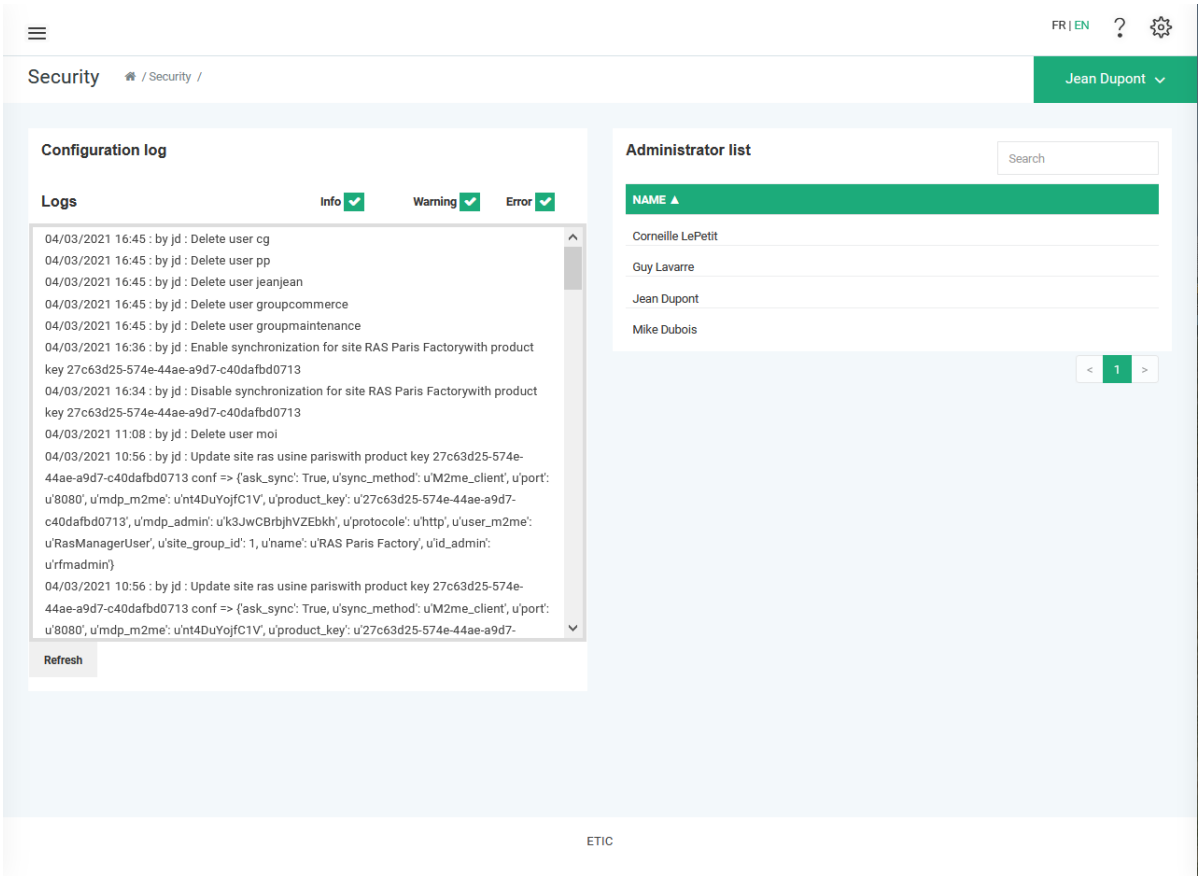
8 Trace fleet modifications

All changes made in the fleet configuration interface are tracked in a log. Each modification is recorded there as well as the user who made the modification. Thus, it is possible to trace each modification carried out on the fleet.

Click on the gear located on the right of the menu bar.



Click on the **Security dashboard** button.

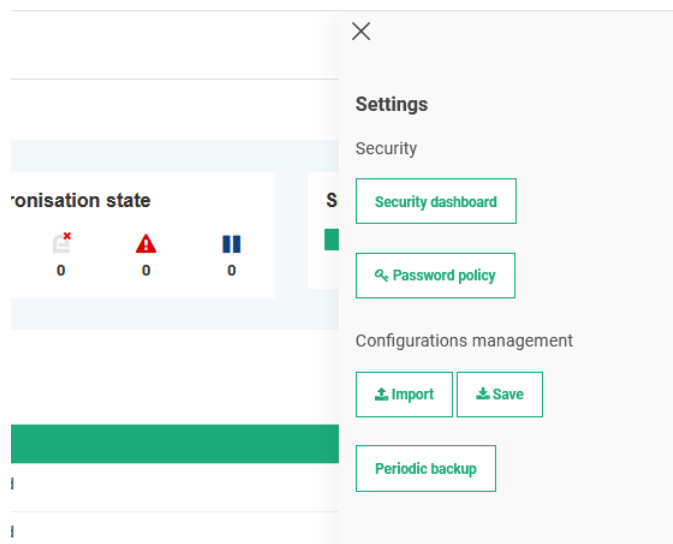


The **Configuration log** stores all the modification done to the fleet configuration.

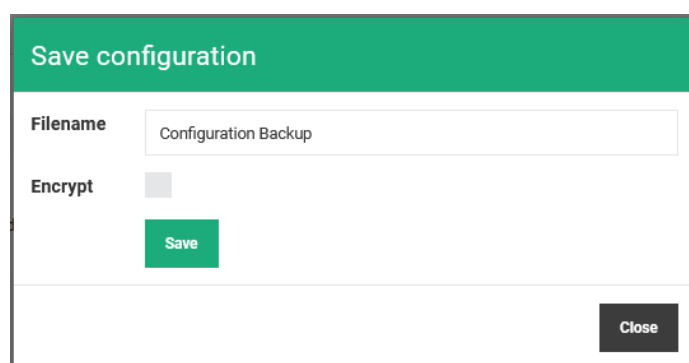
9 Configuration management

9.1 Backup / restore

Click on the gear located on the right of the menu bar.

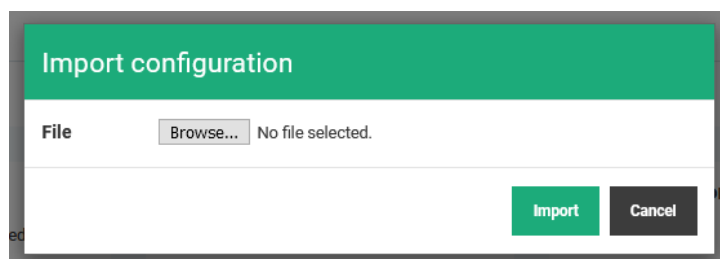


In the **Configurations management** section, click on **Save**.



Choose a file name and click **save**. The download of the configuration file begins.

To restore the configuration, click **Import**, click **Browse** and choose your configuration file, then click **Import**.

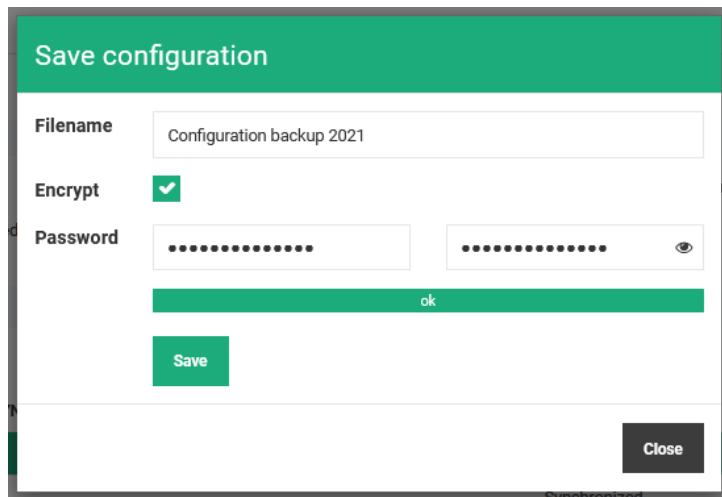


Your configuration is immediately loaded on the RFM.

9.2 Encryption of configuration files

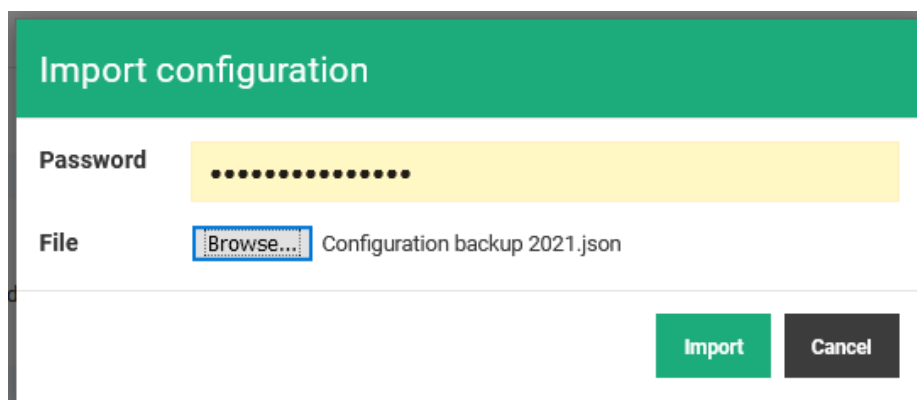
The configuration file contains the secrets for connecting to your RAS fleet; it is therefore sensitive. To store the configuration file securely, it is possible to encrypt the configuration file with a password when it is exported from the RFM.

In the **Configurations management** section, click on **Save**.

A dialog box titled "Save configuration" with a green header. It contains a "Filename" field with the text "Configuration backup 2021". Below it is an "Encrypt" checkbox which is checked with a green checkmark. Under "Encrypt" are two password fields, each filled with dots, and a small eye icon to the right of the second field. At the bottom right is a "Close" button. A green "ok" button is visible above a green "Save" button.

Check the **Encrypt** box and enter a configuration encryption password. You will be asked for this password when importing a configuration into the RFM.

To restore an encrypted configuration, click **Import**, click **Browse** and choose your configuration file. A **Password** field appears. Enter the password chosen during the backup and click on **import**.

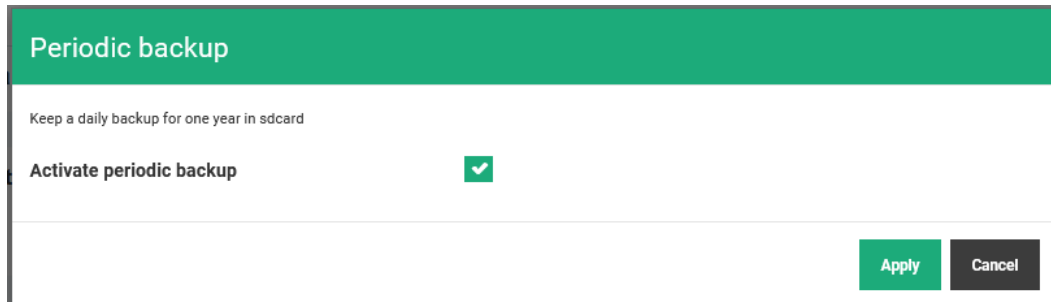
A dialog box titled "Import configuration" with a green header. It contains a "Password" field with a yellow background and dots. Below it is a "File" field with a "Browse..." button and the text "Configuration backup 2021.json". At the bottom right are "Import" and "Cancel" buttons.

Configuration is immediately loaded into the RFM.

9.3 Automatic backup

It is possible to save the RFM configuration daily on the SD card. When this option is enabled, the RFM performs a daily backup of the configuration on the SD card. Files are kept for 1 year.

In the **Configurations management** section, click on **Periodic backup**.



Periodic backup

Keep a daily backup for one year in sdcard

Activate periodic backup ☒

Apply Cancel

Check the box **Activate periodic backup** to enable this feature.



13, Chemin du Vieux Chêne
38240 Meylan - France

Tel : +33 (0)4 76 04 20 00

contact@etictelecom.com

www.etictelecom.com