

R-CARD M5 with Unloc app control

Commissioning

Describes how to set up communication with Unloc to control doors in RCO's access control systems.

About Unloc and R-CARD M5 User API	3
Prerequisites	3
Activating IIS and installing the software	4
Overview.....	4
Activating IIS.....	5
Installing R-CARD M5 User API	6
Configuring IIS.....	6
Adjusting the firewall.....	8
Registering RCO licenses.....	9
Configuring logging.....	10
Logging via R-CARD M5 User API	10
Extended logging via RaServiceHost	11
Configuring R-CARD M5.....	12
Overview.....	12
Linking each door to a license	12
User identification and web password.....	13
Adjusting or checking the necessary system settings	13
Configuring an access profile for the “Unloc app” card	15
Adding a user named “Unloc app” or similar	16
Creating a card for the Unloc app user.....	17
Configuring an API operator.....	17
Creating a separate operator group	17
Creating an operator profile for the API operator	19
Providing information to Unloc.....	20
Important when changing or upgrading R-CARD M5 API.....	20
Troubleshooting	20
Failed upgrade	20
Checking the logs	21
Restarting IIS.....	21
APPENDIX: The configuration file rcoservers.config	22
Background.....	22
Editing rcoservers.config	23
Reference: Elements and attributes in rcoservers.config	24

About Unloc and R-CARD M5 User API

The Unloc mobile application allows you to open doors in RCO's access control system. The app can be downloaded from Google Play (Android) or the Apple AppStore (iOS) free of charge. Learn more at www.unloc.no.

The access control system is controlled by the R-CARD M5 program, and for the app to work, the additional program R-CARD M5 User API is required. The add-on is obtained by registering licenses for each database and for each door that users are to be able to open via the app.

Licenses are available in two variations:


- R-CARD M5 Access Door: Used for door environments with card readers.
- R-CARD M5 Access Virtual: Used for virtual doors.

After installation and license registration, configuration in RCO's R-CARD M5 software is required. That configuration is described in this manual.

When a door is opened via Unloc, you can see this in the event log in R-CARD M5. The user is registered as "Unloc app" (or other name that you enter – see page 16), and the telephone number of the Unloc user who was using the app is provided on the same line.

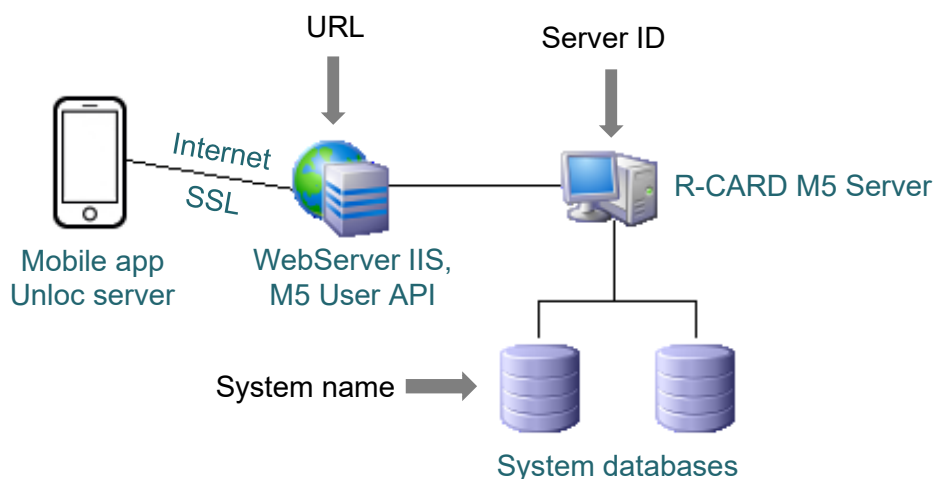
Prerequisites

- The access control system is commissioned and online.
- IP communication between internet / Unloc and R-CARD M5.
- License to use R-CARD M5 Access Door and / or R-CARD M5 Access Virtual (see above).
- License for R-CARD M5 User API
- Controller unit UC-50 version 2.84 F8 or later.
- R-CARD M5 version 5.42.1 or later.

 **Important:** Make sure your computer automatically installs security updates, or ensure your system is kept up-to-date in some other way.

Activating IIS and installing the software

Overview



Calls and communication with the IIS web server take place via HTTPS when an R-CARD M5 system is in operation.

By default, all access control systems on the local computer will be available for Unloc. No configuration required if:

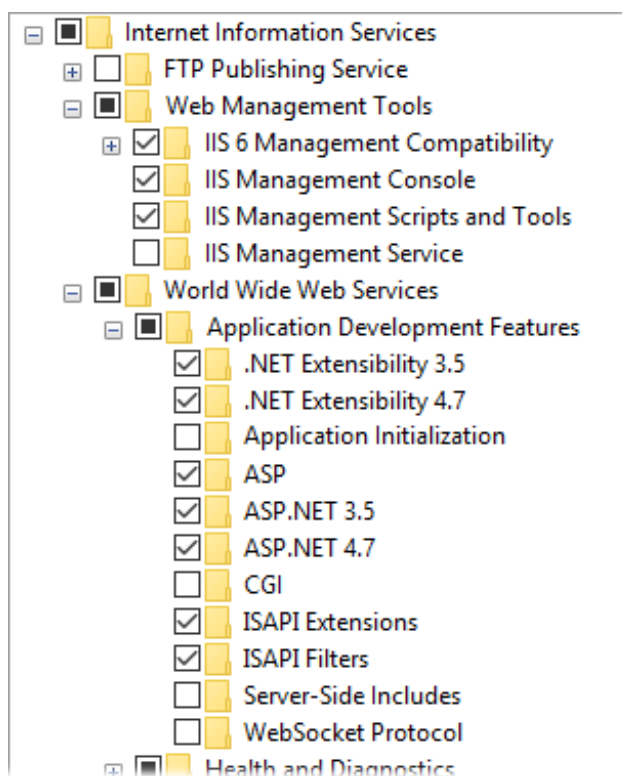
- All access control systems on the local computer (and no others) are to be available.
- The API operator(s) are created with the name “apitest” and password “1234”. (See instructions on page 19.)

Otherwise, customizations are required in the configuration file **rcoservers.config**. See page 22 for instructions after installation.

Activating IIS

Internet Information Services (IIS) can be added to most Windows operating systems. Enable IIS on the computer on which the R-CARD M5 User API is to be installed:

1. Open **Programs and Features** in Windows Control Panel.
2. Click **Turn Windows Features On or Off** on the left side.
3. Select **Internet Information Services**.
4. In addition to the basic settings, expand the **Web Services > Application Development Features** folder and make sure the following settings are checked:
 - **.NET development** (also be called **.NET Extensibility** or similar, depending on the operating system)
 - **ASP**
 - **ASP.NET**



Installing R-CARD M5 User API

1. Download "R-CARD M5 User API" from [RCO's website](#).
(The API is also found in the **M5Web** folder on the R-CARD M5 installation media.)
2. Extract the file.
3. Right-click the **SetupM5UserAPI.exe** file and select **Run as administrator**.
4. Follow the on-screen instructions and complete the installation.

Configuring IIS

HTTPS means that the communication between client and web server is encrypted. Using a signed server certificate ensures that the client communicates with the specified server.

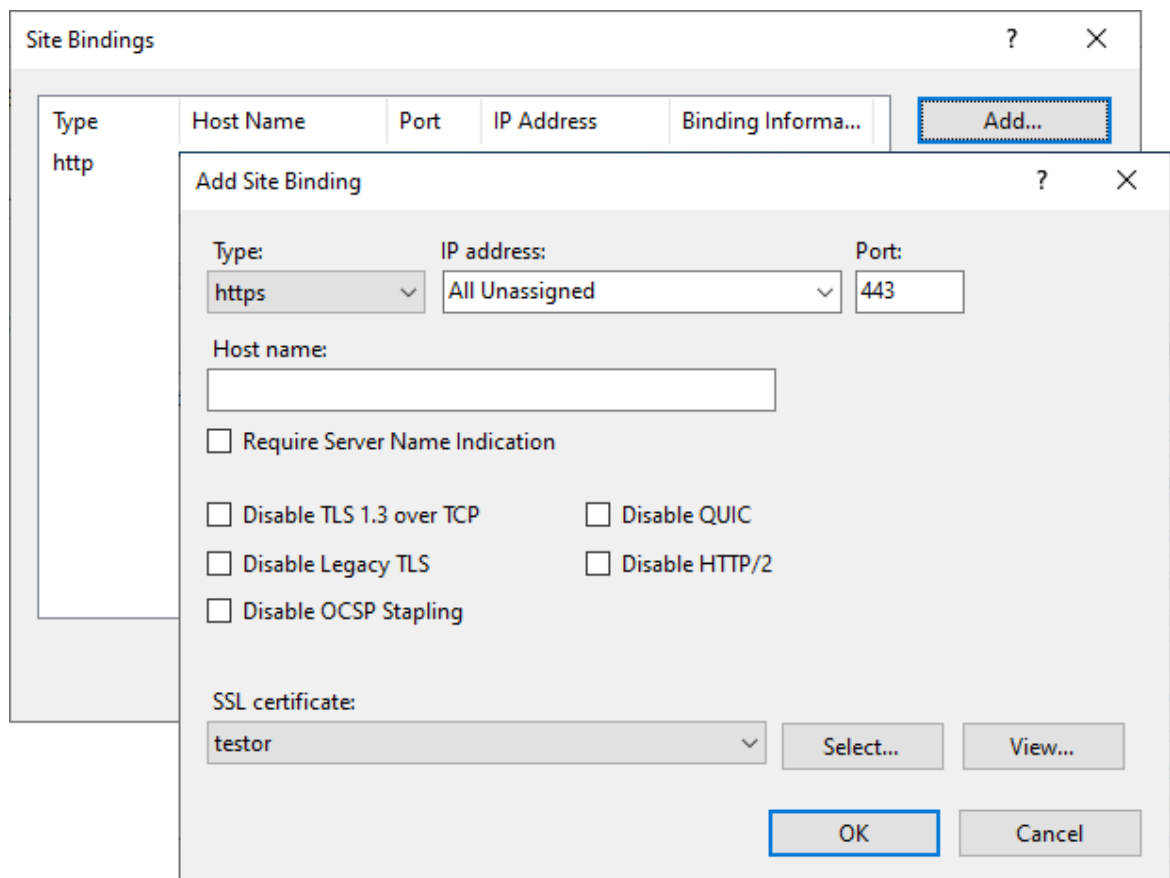


Use the following procedure to create a *self-signed* server certificate and enter it in the binding. Of course, if you have a certificate signed by a *certification authority*, use that instead.

1. Start the Internet Information Services (IIS) Manager application.
2. Select the uppermost node in the left pane.
3. Double-click **Server certificates** in the middle pane.
4. In the menu on the right, click **Create Self-Signed Certificate**.
5. Specify a name and click **OK**.
6. In the left pane, click the plus sign (+) by **Sites** and select the node with the globe (🌐).
7. In the menu on the right, click **Bindings**. The **Site Bindings**

8. Add the binding:

a) Click **Add**.



Type, select **https**.

c) For **SSL certificate**, select the certificate that you created.

d) Click **OK** and **Close**.

9. In the left pane, click the plus sign (+) by **Default Web Site** and select **M5UserAPI**.

10. Double-click **SSL settings**

11. Select **Require SSL**. (Leave other settings unchanged.)

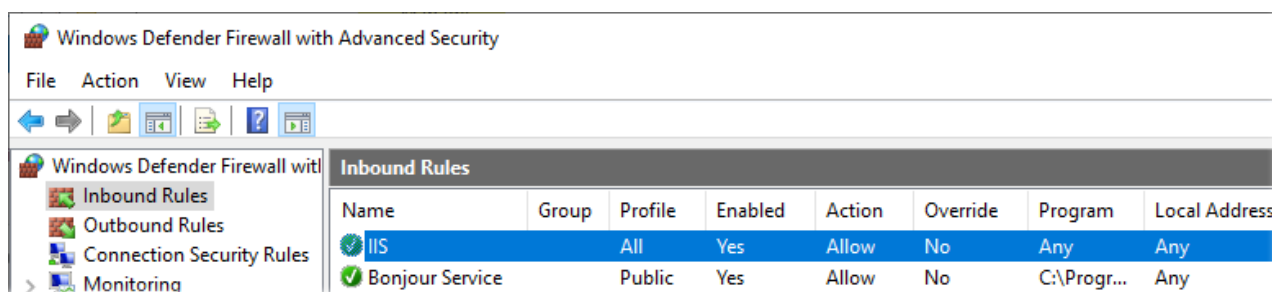
12. In the menu on the right, click **Apply**.

❗ **Tip:** Read more about IIS and SSL at <https://technet.microsoft.com>.

Adjusting the firewall

If the built-in firewall in Windows is used, you can turn it off temporarily for testing. For a production environment, the firewall must be open for incoming traffic on HTTPS port 443.

1. Open **Windows Defender Firewall** in the Control Panel.
2. Click **Advanced Settings** in the left pane.
3. Click **Inbound Rules**.
4. Verify that there is a rule for IIS. Otherwise, configure such a rule (open the firewall for incoming traffic on port 443).



Registering RCO licenses

The following licenses are required:

- R-CARD M5 Access Door: License for the number of *doors with card readers* that can be opened via the app.
- R-CARD M5 Access Virtual: License for the number of *doors without card readers* that can be opened via the app.
- R-CARD User API

Register the licenses in the same way as other RCO licenses. For detailed instructions, see the installation manual for R-CARD M5 or the online help¹ in R-CARD M5 (press **F1** while using the program or the license registration program).

How to start:

1. On the computer where the R-CARD M5 Server is to run (the computer that handles communication with the access control system), log in to Windows as a user with administrator privileges.
2. Start the R-CARD M5 Registration program. (Select **Start > All Programs > R-CARD M5 > R-CARD M5 Registration.**)

¹ The installation manual and the online help are available in Swedish, Norwegian and Finnish. Help in English, if it opens, is not current and does not contain the information you need. The other help files are **RAM5HLPSWE.CHM**, **RAM5HLPSWE.CHM** and **RAM5HLPSWE.CHM**. In a default installation the path to the files is **C:\Program (x86)\RCO Security AB\R-CARD M5**. If you need additional assistance, please contact RCO Technical Support.

Configuring logging

Logging via R-CARD M5 User API

R-CARD M5 User API handles logging using Apache Log4net. The configuration is found in the API's **web.config** file. The default path for this file is:

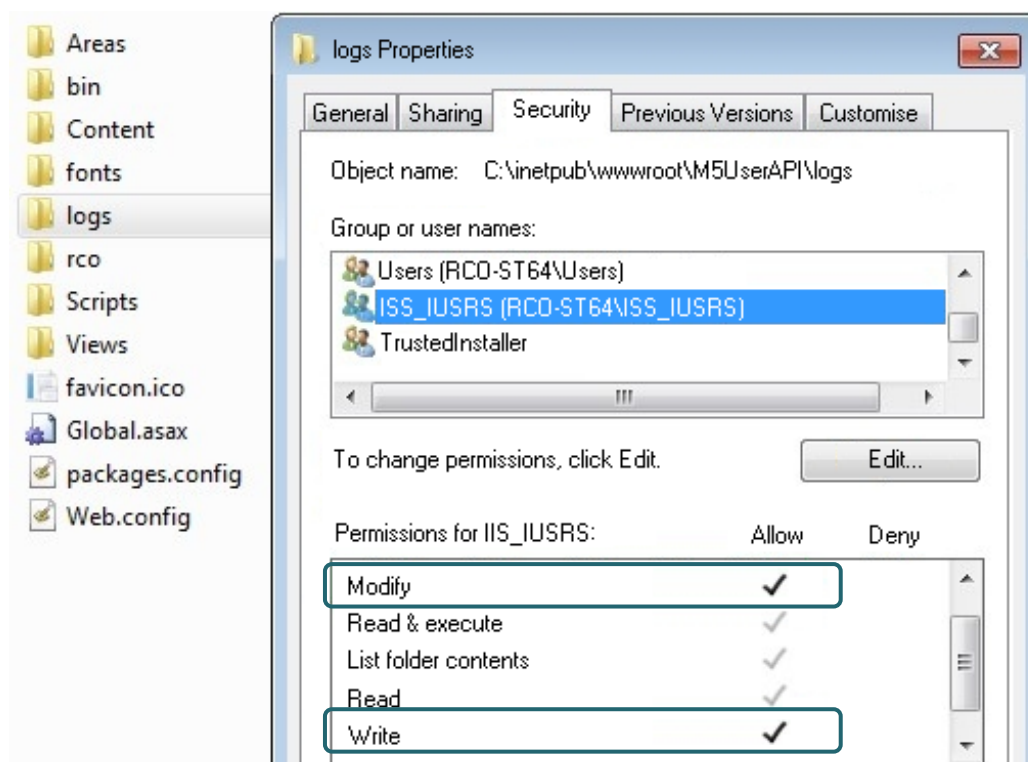
C:\inetpub\wwwroot\M5UserAPI

The **<level>** element controls which errors are to be logged. The value **INFO** (default setting) results in logging of application traffic, door events and errors.

```
<log4net debug="false">
  <root>
    <!-- ALL, DEBUG, INFO, WARN, ERROR, FATAL, OFF -->
    <level value="INFO" />
    <appender-ref ref="RollingLogFileAppender" />
  </root>
```

C:\inetpub\wwwroot\M5UserAPI\logs

For logging to take place, you must give the user IIS_IUSRS *write* and *modify* rights in the properties of the **log** directory:



Use this procedure:

1. Right-click on the **logs** folder and select **Properties**.
2. On the **Security** tab, select the user **IIS_IUSRS**.
3. Select **Modify** and **Write**.
4. Click **Apply**.

Extended logging via RaServiceHost

RaServiceHost, too, has logging via Apache Log4net. It is optional to activate this logging, which shows call errors.

The logging is controlled via the configuration file **log4net.config**. The default search path for this file:

C:\Program Files (x86)\RCO Security AB\R-CARD M5\RcardService

The logs are normally written to the following directory:

C:\Windows\SysWOW64\config\systemprofile\AppData\Local\RCO Security AB\R-Card M5\Logs

Configuring R-CARD M5

Overview

In order for Unloc to be able to control doors in the access control system:

- Each door that is to be controlled by the app must be linked to an RCO license. This is described under “Linking each door to a license” below.
- Unloc requires its own uniquely identified *user* (or flat) for its communication with R-CARD M5. Setup is described under “User identification and web password” on page 13.
- The API uses an *operator profile* to log in on R-CARD M5 Server. See “Configuring an API operator” on page 17.

Linking each door to a license

Each device that can be controlled via the app must be linked to a license of the type R-CARD M5 Access Door or R-CARD M5 Access Virtual. This is done via the device's settings:

1. Select **Units > System units**.
2. Select the desired device in the system tree.
3. Click the plus sign (+) next to **RCO Access app**.

+ Settings for offline units	
- RCO Access app	
Control from RCO Access app	<input checked="" type="checkbox"/>
+ Miscellaneous	


5. Click **Save** (📁).

User identification and web password

Unloc requires *one* unique R-CARD M5 *user or flat (apartment)* in order to communicate with the program. Recommendation: Name the user “Unloc app” or similar.

Instructions for adding that user or flat are given under “Adding a user named “Unloc app” or similar” on page 16. However, you may need to adjust some system settings first (see below).

Additionally, the user or flat must have a *card* defined for it – one that is authorised to open doors during the times when door control via the app is to be allowed. Authorisation is given via its access profile.

 **Note:** More specific end users and their access is defined in Unloc itself. The “user” referred to here is for communication between Unloc and R-CARD M5.

Adjusting or checking the necessary system settings

Required settings:

- You must specify which user data field will be used to identify the *user*. If no field is selected, the integration will not work.

(If you are going to define a *flat* for Unloc to use for communication, then you can skip this step, because flats are always identified by flat number.)

- The user or flat must have a *web password*. The **Web password** field is not visible in *user* properties by default, so you must activate this. (The **Web password** field is probably activated in flat properties.)

Use this procedure:

1. Select **Settings > Settings**.
2. Expand the **System** folder and select **User data fields**.

- For **Field for RCO Access user login**, select a *text field* that has unique information, such as **Email**. (Again, you can skip this step if you are going to define a **flat** for Unloc to user for communication.)

The screenshot shows the 'Settings' dialog box with the 'System/User data field' tab selected. On the left, a tree view shows 'System' expanded, with 'User data fields' selected. On the right, there are three dropdown menus: 'User field to be displayed in name:' (set to 'Last name:'), 'Extra field for identification (displayed after name):' (set to '(None)'), and 'Field for RCO Access user login (not apt.):' (set to 'Email'). A 'Configure user data fields...' button is at the top right.

❗ The selected field must be a text field (not numerical). You can check whether a field is text or numerical in the **Settings for user fields** dialog box (see next step).

- Click **Configure user data fields**. The **Settings for user fields** dialog box is displayed.
- Ensure that the correct tab is selected – **User** or **Flat**.
- In the **Visible** column, select **Web password**.

The screenshot shows the 'Settings for user fields' dialog box. At the top, it says: 'Changing field names affects how they are displayed in the rest of the client. To restore the original name, clear the custom name.' Below this, there are four tabs: 'User' (selected), 'Flat', 'Företag', and 'Group'. A table lists various fields with columns for 'Field', 'Field name', 'Format', 'Visible', 'Required', 'Unique', and 'Searchable'. The 'Web password' field is circled in the 'Visible' column.

Field	Field name	Format	Visible	Required	Unique	Searchable
Personal data:	Personal data:					
Last name:	Last name:		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
First name:	First name:		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Employee number:	Employee number:	Numeric	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Department:	Department:		<input checked="" type="checkbox"/>	<input type="checkbox"/>		
Group:	Group:		<input checked="" type="checkbox"/>	<input type="checkbox"/>		
Telephone:	Telephone:	Numeric	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Web password:			<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
Address:	Address:					
Post address:	Post address:		<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
Postal code:	Postal code:		<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>

- Click **Apply** and **Close**.

Configuring an access profile for the “Unloc app” card

As stated on page 13, the app user’s card must be given access to relevant doors at the desired times. This is done via an *access profile*.

(These instructions assume that one access profile is used. However, you can use up to three different ones to provide access to different card readers at different times.)

In the access profile, the **Control from RCO Access app** setting must also be selected.

Use this procedure:

1. Select **Main menu > Access profiles**.
2. Right-click in an empty area under **Access profiles** and select **New > Access profile**.
3. Enter a name for the profile, to indicate what it is for.
4. Under **Usage**, select **User**.

The screenshot shows the configuration window for an access profile named "Unloc app access". The window has tabs for "Properties", "Card readers/Areas", and "Schedule".

Validity

- ☐ Blocked
- Start date: [dropdown]
- End date: [dropdown]


Usage

- ☒ User
- ☐ Functions
- ☐ Group codes

Time code

- Hours: [0] Minutes: [1]
- ☐ Door is unlocked
- ☐ Follow card access
- ☐ Temporary code
- ☐ Once only


Properties	Settings
Holiday controlled	<input type="checkbox"/>
Two-card function 1	<input type="checkbox"/>
Two-card function 2	<input type="checkbox"/>
Selectable PIN code from display reader	<input type="checkbox"/>
Arming	<input type="checkbox"/>
Disarming	<input type="checkbox"/>
Lock/reset door (*0*)	<input checked="" type="checkbox"/>
Day/night control manoeuvre *1*	<input checked="" type="checkbox"/>
Door opening for handicapped	<input type="checkbox"/>
Security guard access	<input type="checkbox"/>
Engineer access	<input type="checkbox"/>
Max. selectable time for arming delay (hours)	(Not used) [dropdown]
Ignore counter and lock in roll call areas	<input type="checkbox"/>
Janitor access	<input type="checkbox"/>
+ Offline units	
Control from RCO Access app	<input checked="" type="checkbox"/>

5. At the bottom of the settings, select **Control from RCO Access app**.
6. On the **Card readers/Areas** tab select the card readers that the Unloc app is to have access to. Do this by dragging each one from the left pane to the right.
7. On the **Schedule** tab, at the bottom, click **Create 24/7**.
(This assumes that the Unloc app should have access to doors all day, every day. Otherwise, create a custom time schedule.)
8. Click **Save** .

Unloc requires a unique R-CARD M5 user or flat in order to communicate with the program. It does not matter how many Unloc end users there are; only one R-CARD M5 user or flat is required.

1. Select **Main menu > Users**.
2. Select the **Name** tab so that existing users and flats are visible.
3. Right-click in an empty area under **Users** and select **New > User > Empty** or **New > Flat > Empty**.
4. If you are defining a user:
 - Enter a name such as “Unloc app” to signify what the purpose of the user or flat.
 - Enter a unique value for field you chose as the **Field for RCO Access user login** in step 3 on page 14.

If you are defining a *flat*, enter a unique value as the flat number.


5. In the **Web password** field, enter at least 4 characters.
6. Enter other required data, if any.
7. Click **Save** .



20.

Creating a card for the Unloc app user

The Unloc app user (or flat) must be given a virtual card with door access. The card does not need a card number, but you must give it access to all doors that are to be controlled by the Unloc app – and normally all day every day. This access is given using the access profile that you created according to instructions on page 15.

1. Right-click the Unloc app user **New card > Normal**.
2. If desired, enter a name for the card.
3. If required by system settings, enter a card number and PIN code.
4. Under **Permissions**, drag up to three access profiles from the left pane to the right.
5. Click **Save** (.


Unloc communicates with R-CARD M5 via “M5 User API”. The API, in turn, logs in to R-CARD M5 as an *operator*. Therefore, an *operator profile* must be defined in R-CARD M5.

In addition, each operator profile is associated with an *operator group* that specifies which actions can be performed and which data (for example which users and access profiles) is available to act upon.

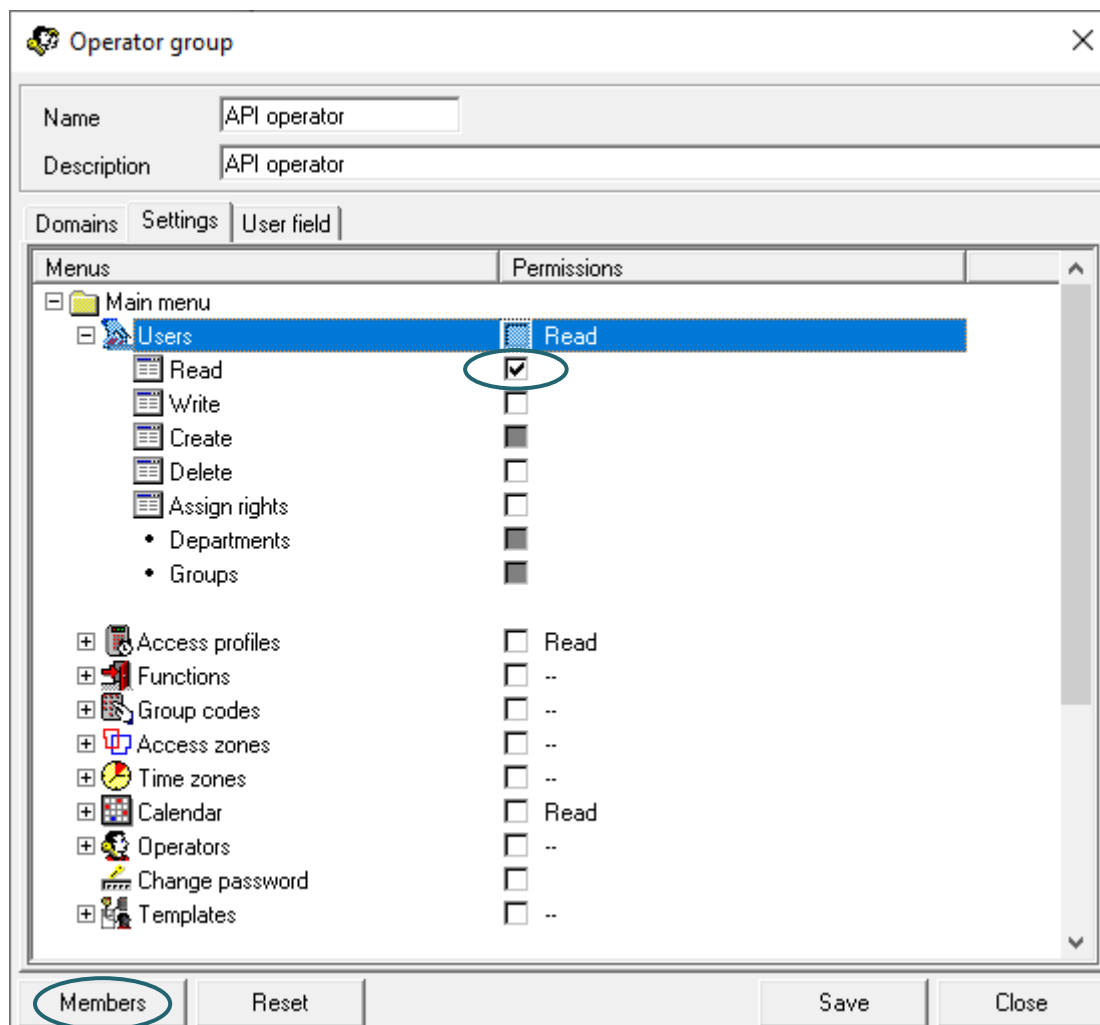
Creating a separate operator group

If there are already multiple operators with different operator groups managing users and cards in the system, *it is recommended to use the default operator group SystemAdmin for the API operator*.

If you instead want to create a separate operator group for the API operator, to restrict access, use this procedure:

1. Select **Main menu > Operators**.
2. Select **Operator groups** in the system tree.
3. Click the icon **Define a new operator group** (). The **Operator group** dialog box is displayed.
5. Configure the API operator access.

At the very least, the API operator's group must provide read access to **Main menu > Users**, for access to the Unloc user.



You can further restrict which users or flats (apartments) can control doors via this API operator. To do this, select **Users** and click **Members**.

Press **F1** to open online help² if you need further instructions.

- Click **Save** (📁).

² The online help is available in Swedish, Norwegian and Finnish. Help in English, if it opens, is not current and does not contain the information you need. The other help files are **RAM5HLPSWE.CHM**, **RAM5HLPSWE.CHM** and **RAM5HLPSWE.CHM**. In a default installation the path to the files is **C:\Program (x86)\RCO Security AB\R-CARD M5**. If you need additional assistance, please contact RCO Technical Support.

Creating an operator profile for the API operator

The R-CARD M5 User API uses an *operator profile* to log in to R-CARD M5 Server. Create an API operator profile for this purpose.

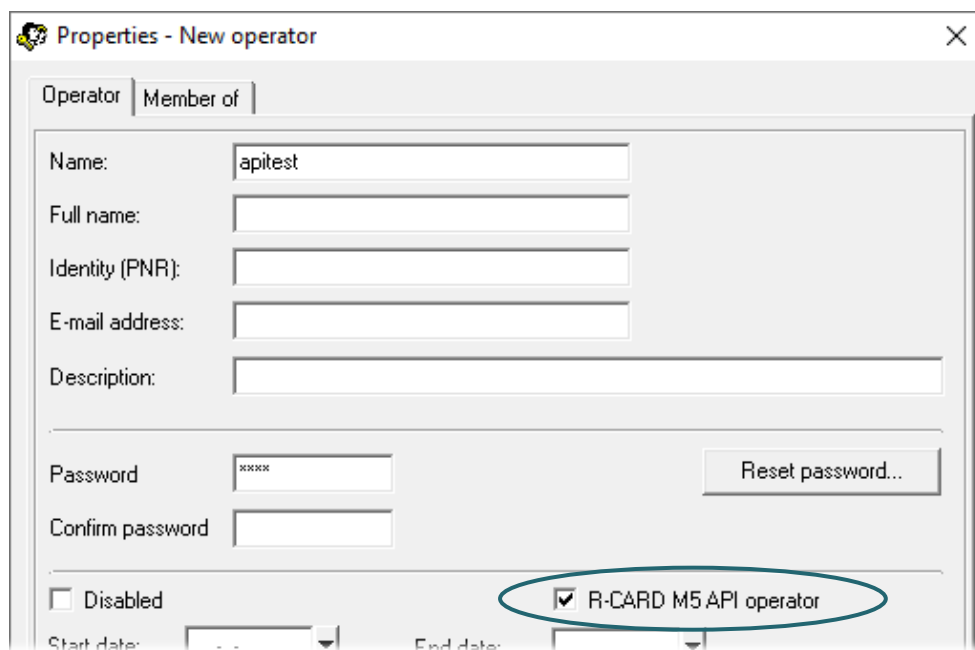
- ❗ If you use the default setting, which makes all systems are available, this operator must be logged in *on each system*.

Use this procedure:

1. Select **Main menu > Operators**.
2. Select **Operators** in the system tree.
3. Right-click an empty space under **Operators** and select **Create a new operator**.
4. Enter a name and password for the operator.

- ❗ The default name and password are *apitest* and *1234*. If you enter a different name or password, then changes are required in the configuration file **rcoservers.config**. See page 22 for instructions.

5. Select **R-CARD M5 API operator**.



- ❗ This operator will now be unable to log in on R-CARD M5 Workstation (client).

6. On the **Member of** tab, click **Change** and drag in one operator group (for example **SystemAdmin** or the one that you created in the previous section).
7. Click **OK** and **Save**.

Providing information to Unloc

End users download the Unloc app from the Apple AppStore (iOS) or Google Play (Android).

Unloc must receive the following information:

- **Name:** A descriptive name of the relevant facility.
- **DNS / IP address:** IP address, host computer name or domain name of the IIS server.
- **Server ID:** Must match **server.id** in **rcoservers.config** (usually “1”).
- **System name:** R-CARD M5 system name. Must match **system.name** in **rcoservers.config**. Alternatively (if no system is specified in the configuration file), must exactly match the name of a system located on the specified server.
- **User name** and **web password**. The unique user name you entered for the user in R-CARD M5, or the flat number to be used for communication, and the corresponding web password. (See page 20.)

Important when changing or upgrading R-CARD M5 API

Make a backup of the configuration file **rcoservers.config**. (The file is described on page 22.) *This file is deleted during uninstallation.*

The file is found in the IIS folder, default path **C:\inetpub\wwwroot\M5UserAPI\rco**.

Troubleshooting

Failed upgrade

After upgrading, check that the new version has actually been installed: Launch a web browser and enter the address <https://localhost/M5UserAPI>. Check the version number.

If the older version number is displayed, you need to uninstall R-CARD M5 User API via **Control Panel > Programs and Features**. Then reinstall a full version.

Checking the logs

The best general troubleshooting advice is to check the log. By default, API log files are found in the following folder:

C:\inetpub\wwwroot\M5UserAPI\logs

This assumes that the user IIS_IUSRS has write and edit rights in the **log** directory. (See page 10.)

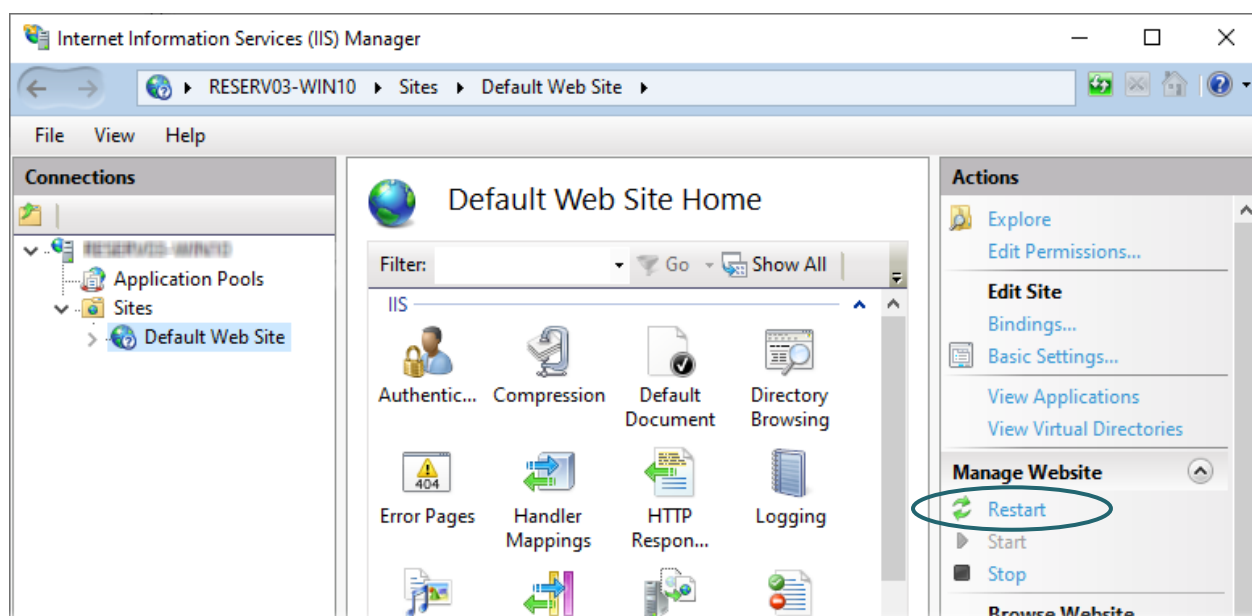
(Extended logging via RaServiceHost is also possible – see page 11.)

Restarting IIS

A reboot is usually required for changes to the web application's configuration files.

The image below is from 64-bit Windows 10. The actual appearance varies by operating system.

1. Start the Internet Information Services (IIS) Manager application.
2. Expand **Sites** and select **Default Web Site**.



3. Click **Restart** in the right pane.

APPENDIX: The configuration file rcoservers.config

Background

R-CARD M5 User API is installed on the R-CARD M5 server computer, or on any IIS server. The configuration file's default setting *localhost* gives Unloc access to all access control systems on the local computer:

```
<?xml version="1.0" encoding="UTF-8"?>
<rcoservers>
  <server id="1" url="net.tcp://localhost:8090/RcardServices/RcardService" identity="" username="apitest" password="1234">
  </server>
</rcoservers>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<rcoservers>
  <server id="1" url="net.tcp://localhost:8090/RcardServices/RcardService"
    identity="" username="rcard" password="1234">
    <systems>
      <system name="Fastighet A" username="apia" password="4444"/>
      <system name="Fastighet B" username="apib" password="6666"/>
    </systems>
  </server>
  <server id="987654321" url="net.tcp://server1:8090/RcardServices/RcardService"
    identity="" username="rcard" password="1234" />
</rcoservers>
```

❗ In an RCO access control system, properties can be divided up into multiple *domains* in order to keep hardware and certain functionality separate. Door control from the Unloc app and the R-CARD M5 User API is not domain-specific.

You can also limit or exclude access control systems on the local computer so that they are unavailable to Unloc.

Editing rcoservers.config

1. Open the **rcoservers.config** file in Notepad or other text or XML editor.

The file is located in the IIS directory. Default path:
c:\inetpub\wwwroot\M5UserAPI\rco

2. For each R-CARD M5 server that the R-CARD M5 User API is to have access to, add a **<server>** element.

Identify the server using the attributes **id** and **url**. (See next section. Also see the example on the previous page.)

3. The default setting is that the R-CARD M5 User API has access to all access control systems on specified servers. To *limit* which systems are available, specify them using **<systems>** elements.

Enter the system name in the **name** attribute. *The name must exactly match the system name displayed in R-CARD M5.*

4. Specify the login information that the R-CARD M5 User API will use when logging in to the R-CARD M5. Use the **server.username** and **server.password** attributes.

Alternatively, specify under each **system** which **username** and **password** to use.

5. Save and close the file.
6. **Important:** Configuration files may be lost when upgrading or reinstalling. If you modify a file, make a backup copy and save the copy somewhere else.

Reference: Elements and attributes in rcoseveres.config

XML Element.Attribute	Description
server	Points to an R-CARD M5 server instance.
server.id	Optional unique number for an R-CARD M5 server (max. 9 digits). Used when logging in. The default value is 1 (localhost).
server.name	Not used.
server.url	Address to the RaServerHost service. Used for access to R-CARD M5 Server ("localhost" or an IP address).
server.identity	Not used.
server.username	API operator that R-CARD M5 User API is to use for connection to all systems on this server (if not overridden per system). The default name is "apitest". The API operator must be added in each system manually. Instructions are provided on page 19.
server.password	The password for the API operator. Default: "1234".
systems	Specifies one or more systems (access control systems, alarm systems, installations) on the server. By default, R-CARD M5 User API has access to all systems on specified servers. To limit which systems are available, add the <systems> element. All systems below that – those which are specified with a correct name in a <system> element – will be available, and no others.
system	Points to a system on the server.
system.name	System name. Must exactly match the system name as displayed in R-CARD M5 (under Settings > Systems > General folder, Name field).
system.username	The API-operator used for system access. Optional. If specified, it overrides server.username (see above) for this system. The API operator must be added in each system manually. Instructions are provided on page 19.
system.password	The password for the API operator. Required if system.username is specified.