Cybersecurity Behavior M262
网络安全行为 M262

06/2020

Cybersecurity_Behavior_M262.

www.schneider-electric.com

Schneider Electric

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

You agree not to reproduce, other than for your own personal, noncommercial use, all or part of this document on any medium whatsoever without permission of Schneider Electric, given in writing. You also agree not to establish any hypertext links to this document or its content. Schneider Electric does not grant any right or license for the personal and noncommercial use of the document or its content, except for a non-exclusive license to consult it on an "as is" basis, at your own risk. All other rights are reserved.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When devices are used for applications with technical safety requirements, the relevant instructions must be followed.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.

本文档中提供的信息包含有关此处所涉及产品之性能的一般说明和/或技术特性。本文档并非用于 (也不代替) 确定这些产品对于特定用户应用场合的适用性或可靠性。任何此类用户或设备集成商都有责任就相关特定应用场合或使用方面对产品执行适当且完整的风险分析、评估和测试。Schneider Electric 或其任何附属机构或子公司对于误用此处包含的信息而产生的后果概不负责。如果您有关于改进或更正此出版物的任何建议、或者从中发现错误、请通知我们。

本手册可用于法律所界定的个人以及非商业用途。 在未获得施耐德电气书面授权的情况下，不得翻印传播本手册全部或部分相关内容、亦不可建立任何有关本手册或其内容的超文本链接。施耐德电气不对个人和非商业机构进行非独占许可以外的授权或许可。 请遵照本手册或其内容原义并自负风险。与此有关的所有其他权利均由施耐德电气保留。

在安装和使用本产品时，必须遵守国家、地区和当地的所有相关的安全法规。出于安全方面的考虑和为了帮助确保符合归档的系统数据，只允许制造商对各个组件进行维修。

当设备用于具有技术安全要求的应用场合时，必须遵守有关的使用说明。

未能使用施耐德电气软件或认可的软件配合我们的硬件，则可能导致人身伤害、设备损坏或不正确的运行结果。

不遵守此信息可能导致人身伤害或设备损坏。

Table of Contents

Safety Information

Important Information

NOTICE

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

PLEASE NOTE

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

About the Book

At a Glance

Document Scope

This document describes the cybersecurity best practices in the context of user rights management.

Validity Note

This document has been updated for the release of EcoStruxure^{TM} Machine Expert V1.2.

User Rights Management - General Information

Overview

In order to meet constantly evolving cybersecurity requirements, with EcoStruxure Machine Expert V1.2 the user rights management is by default activated for Schneider Electric M241, M251, M262, PacDrive LMC Eco, PacDrive LMC Pro/Pro2 controllers. This has the effect that every Schneider Electric controller equipped with the latest EcoStruxure Machine Expert V1.2 firmware prompts you for user credentials whenever you attempt to gain access.

NOTE: The new user rights management does not apply for HMISCU controllers.

For general information regarding device user management, refer to the Programming Guide in the EcoStruxure Machine Expert *online help*, section **Software** → **Programming** → **Programming Guide** → **Configuration** → **Common Device Editor Dialogs** → **Device Configuration** → **Users and Groups** → **Users and Groups Management**.

First Login to Schneider Electric Controller with User Rights Management Activated Using Default Credentials

As user management is activated by default in the controllers, use the following default credentials for first login and modify them immediately.

Step	Action
1	At first login to a Schneider Electric controller, enter the default user credentials: ● **User name**: `Administrator` ● **Password**: `Administrator` **Result**: You are requested to change the default password.
2	Enter your individual **Password**.
3	Re-enter your individual **Password**.
4	Click **OK** to confirm. **Result**: Access to your controller is now protected by these new credentials. They are assigned the highest user rights level and allow you to manage access rights for users or user groups.

NOTE: For future login, the new **Password** will be required.

Controller Locked After Entering Incorrect Credentials

If you enter incorrect credentials for three times, the controller will be locked for 60 seconds. After this time, retry to connect by entering the correct credentials.

Logoff Procedure

After successful login to the controller, you can perform further online actions on the controller with EcoStruxure Machine Expert. As long as your project remains open, you will not be prompted to enter your credentials again.

In order to log off the present user from the controller, execute the command **Online → Security → Logoff current device user**.

After that you will be prompted for your credentials when you attempt to perform another online command on the controller.

Firewall Settings

Most of the communication services like FTP or OPC UA access the controller by using the settings of the user rights management. Therefore, make sure that the firewall settings on the controller allow the services to access the controller file system.

Controller - HMI Communication with User Rights Management Activated

With user rights management activated in the controllers, the connection between an HMI programmed with Vijeo-Designer and the controller will not be established.

The following solutions are available to solve this issue:

- In Vijeo-Designer, open the **Network Equipment Settings** dialog box of the **I/O Manager** and enter the **Username** and the **Password** to access the controller.
- Reset the device user rights of the controller *(see page 9)*.

Resetting Device User Rights

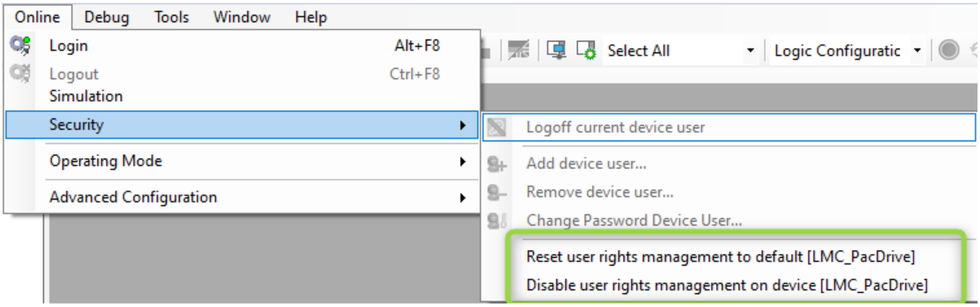
Overview

You can reset the device user rights to the default settings by using different software tools. Your individual credentials are required for this procedure. For further information on the default settings, refer to the *First Login to* Schneider Electric *Controller with User Rights Management Activated Using Default Credentials* paragraph *(see page 7)*.

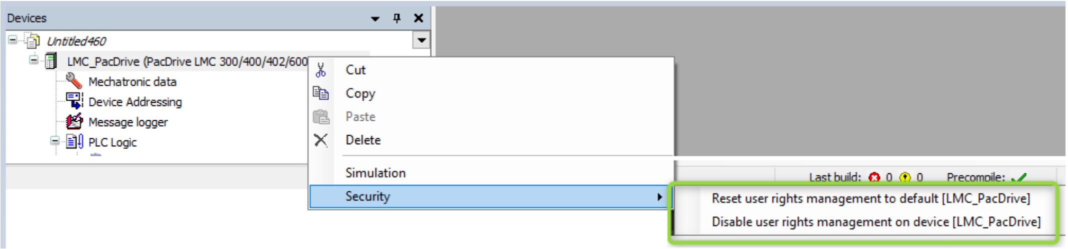
Reset via EcoStruxure Machine Expert Logic Builder

For PacDrive LMC Eco and PacDrive LMC Pro/Pro2 controllers, you can reset the device user rights using the **Reset user rights management to default** command that is available at two different locations:

Online → **Security** → **Reset user rights management to default** menu:



Contextual menu of the controller, **Security** → **Reset user rights management to default** command:



Devices
Untitled460
LMC_PacDrive (PacDrive LMC 300/400/402/600
Mechatronic data
Device Addressing
Message logger
PLC Logic
Cut
Copy
Paste
Delete
Simulation
Security
Last build: 0 0
Precompile:
Reset user rights management to default [LMC_PacDrive]
Disable user rights management on device [LMC_PacDrive]

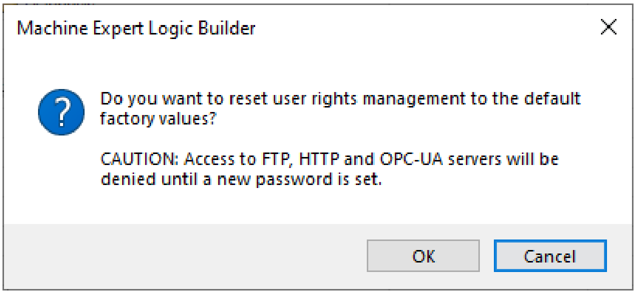
⚠ CAUTION

NO ACCESS VIA FTP, HTTP, OPC-UA

When you reset the user rights management to the default values, access to FTP, HTTP and OPC-UA servers is denied until you set your individual user name and password.

Failure to follow these instructions can result in injury or equipment damage.

Confirm the message with **OK**.



Machine Expert Logic Builder

Do you want to reset user rights management to the default factory values?

CAUTION: Access to FTP, HTTP and OPC-UA servers will be denied until a new password is set.

Reset via Controller Webserver

The Modicon M241 Logic Controller, Modicon M251 Logic Controller, and the Modicon M262 Logic/Motion Controller support the reset of device user rights management via the embedded webserver: **MAINTENANCE → USER MANAGEMENT → USER ACCOUNTS MANAGEMENT → RESET TO DEFAULT**

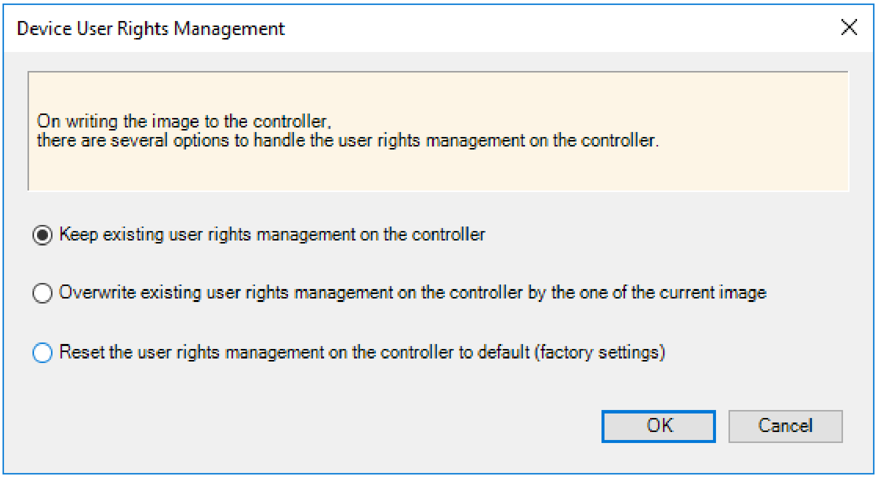
Consult the *Programming Guide* specific to your controller in the EcoStruxure Machine Expert online help for further information:

- Modicon M241 Logic Controller
  Machine Expert > V1.2 > Controllers > M241 Logic Controllers > M241 Logic Controller - Programming Guide > Ethernet Configuration > Ethernet Services > Web Server
- Modicon M251 Logic Controller
  Machine Expert > V1.2 > Controllers > M251 Logic Controllers > M251 Logic Controller - Programming Guide > Ethernet Configuration > Ethernet Services > Web Server
- Modicon M262 Logic/Motion Controller
  Machine Expert > V1.2 > Controllers > M262 Logic/Motion Controllers > M262 Logic/Motion Controller - Programming Guide > Ethernet Configuration > Ethernet Services > Web Server

Reset via Controller Assistant

With EcoStruxure Machine Expert V1.2, the service tool Controller Assistant supports user rights management of PacDrive LMC Eco and PacDrive LMC Pro/Pro2 controllers.

By attempting to write an image to the controller in online mode or to the SD card or flash disk, you will be prompted to decide how to handle user rights in the controller:



Device User Rights Management

On writing the image to the controller,
there are several options to handle the user rights management on the controller.

● Keep existing user rights management on the controller

○ Overwrite existing user rights management on the controller by the one of the current image

○ Reset the user rights management on the controller to default (factory settings)

The following options are available:

- **Keep existing user rights management on the controller**
  Activate this option to keep the existing user rights management as it is. This applies even if the user rights management is disabled.
  NOTE: If you attempt to write an EcoStruxure Machine Expert V1.2 or later firmware to a controller without user rights defined, the user rights management in the controller will be set to the default settings.
- **Overwrite existing user rights management on the controller by the one on the current image**
  The user rights management in the controller will be overwritten by the user rights management that is defined in the image you attempt to write.
  NOTE: If you attempt to write an EcoStruxure Machine Expert V1.2 or later firmware and if there is no user rights management defined in the image, the user rights management in the controller will be set to the default settings.
- **Reset the user rights management on the controller to default (factory settings)**
  The user rights management in the controller will be set to the default settings.

By default, the user rights management existing in the controller are preserved when writing to the controller in online mode.

Reset Without Credentials

If you have lost the credentials, you can reset the user rights management of the controller by using the service tool Controller Assistant to write the image to the SD card or flash disk.

From the message prompting you to decide how to handle user rights in the controller, select the option **Reset the user rights management on the controller to default (factory settings)**. If this option is not available, you can create a new firmware from scratch that comes with the default settings. Then you can restart the controller directly from this SD card or flash disk.

The Modicon M241 Logic Controller, Modicon M251 Logic Controller, and the Modicon M262 Logic/Motion Controller also allow you to modify a script.cmd file on the SD card to reset the user rights management. Consult the *Programming Guide* specific to your controller for further information.

Deactivating Device User Rights

Overview

In order to help prevent unauthorized access to your controller, keep the device user rights management function activated. If you ensure that your machine or process is not accessible to unauthorized personnel, you can deactivate the function as described in this chapter. Your individual credentials are required for this procedure.

Deactivating via EcoStruxure Machine Expert Logic Builder

For PacDrive LMC Eco and PacDrive LMC Pro/Pro2 controllers, you can deactivate the device user rights management using the **Disable user rights management on device** command that is available at two different locations:

- **Online** → **Security** → **Disable user rights management on device** menu
- Contextual menu of the controller, **Security** → **Disable user rights management on device** command

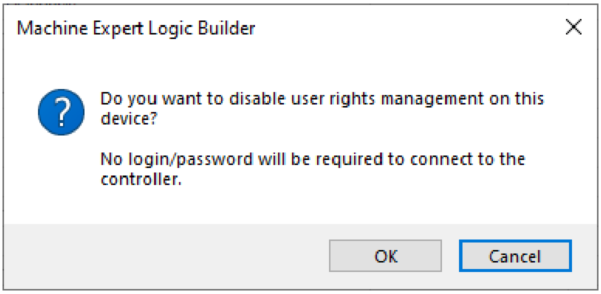
⚠ **WARNING**

UNAUTHENTICATED ACCESS AND MACHINE OPERATION

Do not disable user rights management if your machine or process is accessible to unauthorized personnel either directly or via a network.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

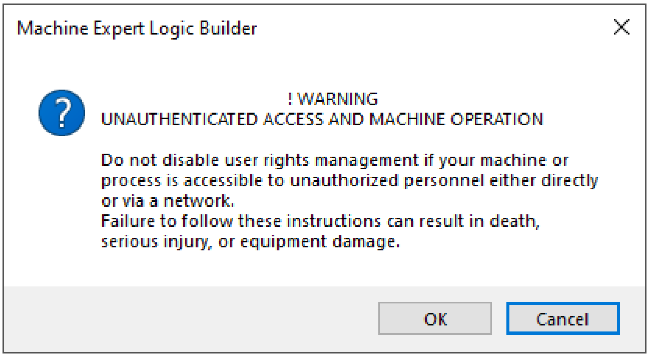
Confirm the two confirmation messages with **OK** if you are sure to deactivate the device user rights.



Machine Expert Logic Builder

Do you want to disable user rights management on this device?

No login/password will be required to connect to the controller.


Machine Expert Logic Builder

! WARNING
UNAUTHENTICATED ACCESS AND MACHINE OPERATION

Do not disable user rights management if your machine or process is accessible to unauthorized personnel either directly or via a network.
Failure to follow these instructions can result in death, serious injury, or equipment damage.

Result: Access the controller is now available without credentials.

Deactivating via Controller Webserver

The Modicon M241 Logic Controller, Modicon M251 Logic Controller, and the Modicon M262 Logic/Motion Controller allow you to deactivate the device user rights management via the embedded webserver: **MAINTENANCE → USER MANAGEMENT → USER ACCOUNTS MANAGEMENT → DEACTIVATE**

Consult the *Programming Guide* specific to your controller in the EcoStruxure Machine Expert online help for further information:

- Modicon M241 Logic Controller
  Machine Expert > V1.2 > Controllers > M241 Logic Controllers > M241 Logic Controller - Programming Guide > Ethernet Configuration > Ethernet Services > Web Server
- Modicon M251 Logic Controller
  Machine Expert > V1.2 > Controllers > M251 Logic Controllers > M251 Logic Controller - Programming Guide > Ethernet Configuration > Ethernet Services > Web Server
- Modicon M262 Logic/Motion Controller
  Machine Expert > V1.2 > Controllers > M262 Logic/Motion Controllers > M262 Logic/Motion Controller - Programming Guide > Ethernet Configuration > Ethernet Services > Web Server

Deactivating User Rights for the Simulation Device in EcoStruxure Machine Expert Logic Builder

The simulation device in EcoStruxure Machine Expert Logic Builder has own user rights that can differ from those that are defined in the real controller.

NOTE: To help avoid account lockout (deadlocking), first disconnect EcoStruxure Machine Expert Logic Builder from the controller and make sure no other client, for example, an HMI, automatically attempts to connect using the previous user rights configuration.

In order to deactivate user rights in the simulation device, proceed as follows:

Step	Action
1	Close all instances of EcoStruxure Machine Expert Logic Builder.
2	Close all instances of Vijeo-Designer.
3	Remove the folder c:\ProgramData\CODESYS\Simulation. **Result**: The simulation device is reset to the default settings.

Managing Device User Rights by Call Parameters

Overview

The service tools Controller Assistant and Diagnostics provide command line arguments that are used to connect to a controller with the required credentials. For detailed information, refer to the Controller Assistant - User Guide and the Diagnostics - User Guide in the EcoStruxure Machine Expert online help.

The following arguments are available:

- `-username <Username>`
- `-password <Password>`
- `-renewalpassword <RenewalPassword>`

Examples

```
ControllerAssistant.exe -username Administrator -password
Administrator -renewalpassword MyNewPassword -getcontrollerinfo
etcp4://192.168.3.40
```

```
Diagnostics.exe -username Administrator -password MyPassword -save
ip etcp4://192.168.3.40 c:\Temp\MyDiagnosticsFile.pdi
```

`-renewalpassword` Argument

The argument `-renewalpassword` is used when a new password needs to be inserted. This is typically the case when the first login to a controller is performed and the default credentials (user name = `Administrator` and password = `Administrator`) are required.

The argument `-renewalpassword` cannot be used to change the password.

Starting Controller Assistant

Controller Assistant can also be started with graphical user interface using the command line arguments. In this case, you are not prompted to enter the credentials. They are retrieved from the values of the arguments.

Managing Device User Rights Using the Scripting API

Scripting for Using Online Services

EcoStruxure Machine Expert provides access to many of its online services via the scripting API. In order to establish a connection or to use an online service at a later time, valid credentials must be stored in the system.

Providing Specific Credentials for Online Services

You can store credentials via online device or online application in case of multi-controller projects. If there are specific credentials provided for the connection, they will be used by the system.

Example:

```
# create an "online device" to use online services
root_device = projects.primary.find("LMC_PacDrive", False)[0]
online_device = online.create_online_device(root_device)

# store credentials specific to this "online device"
online.set_specific_credentials(online_device, "my_user",
"my_password")

# use of any online service
online_device.connect()
```

Providing Default Credentials for Online Services

If no specific credentials are provided for the connection, the system uses the default credentials.

Example:

```
# create an "online device" to use online services
root_device = projects.primary.find("LMC_PacDrive", False)[0]
online_device = online.create_online_device(root_device)

# store default credentials
online.set_default_credentials("my_user", "my_password")

# use of any online service
online_device.connect()
```

Scripting for Enforced Password Renewal

The following scenarios require the password to be changed by the user after authentication:

- First login to a new controller.
- First connection after the user rights management has been reset to default.
- A password renewal is enforced for a specific user by an administrator of the device.

EcoStruxure Machine Expert V1.2 does not support the renewal of passwords using the scripting API. Perform this by using the service tool Controller Assistant.

You can call the latest version of Controller Assistant from command line as indicated in the following example:

```
"c:\Program Files (x86)\Schneider
Electric\EcoStruxureMachine Expert\Tools\ControllerAssistant\Controller
Assistant.exe" -username Administrator -password Administrator -
renewalpassword MyNewPassword -getcontrollerinfo etcp4://192.168.3.50
```

Including User Rights While Cloning the SD Card

Overview

The Modicon M241 Logic Controller, Modicon M251 Logic Controller, and the Modicon M262 Logic/Motion Controller provide a clone function that allows you to write the image of the controller to an SD card. By default, the user rights management is not written to the SD card with the image. If supported by your controller, you can activate the user rights management for the clone procedure in the **Clone management** on the webserver of the controller. Consult the *Programming Guide* specific to your controller for further information.

Additional Information

Cybersecurity Best Practices

Schneider Electric has incorporated cybersecurity best practices and solutions in our products.

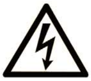
NOTE: To help keep your Schneider Electric products secure and protected, it is in your best interest that you implement the cybersecurity best practices as indicated in the *Cybersecurity Best Practices* document provided on the *Schneider Electric website*.

安全信息

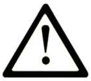
重要信息

声明

在试图安装、操作、维修或维护设备之前，请仔细阅读下述说明并通过查看来熟悉设备。下述特定信息可能会在本文其他地方或设备上出现，提示用户潜在的危险，或者提醒注意有关阐明或简化某一过程的信息。



在“危险”或“警告”标签上添加此符号表示存在触电危险，如果不遵守使用说明，会导致人身伤害。



这是提醒注意安全的符号。提醒用户可能存在人身伤害的危险。请遵守所有带此符号的安全注意事项，以避免可能的人身伤害甚至死亡。

⚠ 危险
危险表示若不加以避免，将**会导致**严重人身伤害甚至死亡的危险情况。

⚠ 警告
警告表示若不加以避免，可能**会导致**严重人身伤害甚至死亡的危险情况。

⚠ 小心
小心表示若不加以避免，可能**会导致**轻微或中度人身伤害的危险情况。

注意
注意用于表示与人身伤害无关的危害。

请注意

电气设备的安装、操作、维修和维护工作仅限于有资质的人员执行。施耐德电气不承担由于使用本资料所引起的任何后果。

有资质的人员是指掌握与电气设备的制造和操作及其安装相关的技能和知识的人员，他们经过安全培训能够发现和避免相关的危险。

关于本书

概览

文档范围

本文介绍了用户权限管理环境下的网络安全最佳做法。

有效性说明

本文档已随 EcoStruxure^{TM} Machine Expert V1.2 的发布进行了更新。

用户权限管理 - 一般信息

概述

为了满足不断提升的网络安全要求，在使用 EcoStruxure Machine Expert V1.2 的情况下，缺省为 Schneider Electric、M241、M251、M262、PacDrive LMC Eco、PacDrive LMC Pro/Pro2 控制器激活了用户权限管理。这样，每当要执行访问时，每个配有最新 EcoStruxure Machine Expert V1.2 固件的 Schneider Electric 控制器都会提醒您输入用户凭据。

注意： 新用户权限管理不适用于 HMISCU 控制器。

有关设备用户管理的一般信息，请参阅 EcoStruxure Machine Expert *online help* 中的编程指南的相关章节，即，**软件 → 编程 → 编程指南 → 配置 → 常用设备编辑器对话框 → 设备配置 → 用户和组 → 用户和组管理**。

藉由使用缺省凭据激活的用户权限管理首次登录到 Schneider Electric 控制器

由于控制器中缺省激活了用户管理，首次登录时，请使用以下缺省凭据，随即再对其加以修改。

步骤	操作
1	首次登录到 Schneider Electric 控制器时，输入缺省用户凭据： ● **用户名**：Administrator ● **密码**：Administrator **结果**：要求您更改缺省密码。
2	输入您自己的**密码**。
3	重新输入您自己的**密码**。
4	单击**确定**进行确认。 **结果**：对您控制器的访问现在便已受到这些新凭据的保护。它们被赋予最高用户权限级别，让您能够管理用户或用户组的访问权限。

注意： 将来登录时，将需要输入新**密码**。

输入的凭据错误时控制器锁定

如果连续三次输入的凭据不正确，控制器将锁定 60 秒。这之后，才能再次通过输入正确的凭据来连接。

注销操作

成功登陆到控制器后，可以使用 EcoStruxure Machine Expert 对控制器执行其他在线操作。只要您的项目保持打开状态，就不会再提醒您输入凭据。

如要从控制器注销当前用户，请执行命令**在线 → 安全 → 注销当前设备用户**。

然后，在对控制器执行另一个在线命令时，便会提示您输入凭据。

防火墙设置

大多数通讯服务（如 FTP 或 OPC UA）使用用户权限管理的设置来访问控制器。因此，确保控制器上的防火墙设置允许服务访问控制器文件系统。

在用户权限管理已激活的情况下进行控制器-HMI 通讯

在控制器中激活了用户权限管理的情况下，使用 Vijeo-Designer 编程的 HMI 与控制器之间将不会建立连接。

可以使用以下方案来解决这个问题：

- 在 Vijeo-Designer 中，打开 **I/O 管理器**的**网络设备设置**对话框，然后输入**用户名和密码**，即可访问控制器。
- 复位控制器的设备用户权限 (参见第 *26* 页)。

复位设备用户权限

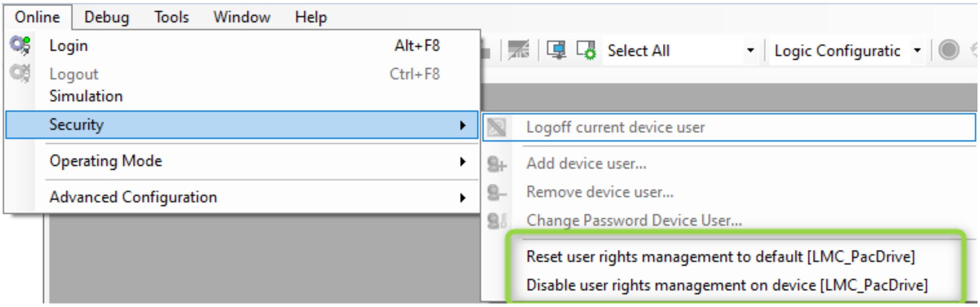
概述

您可以使用多种软件工具将设备用户权限复位至缺省设置。为此，您需要使用相应的凭据。有关缺省设置的更多信息，请参阅*藉由使用缺省凭据激活的用户权限管理首次登录到* Schneider Electric *控制器*文段 (参见第 *24* 页)。

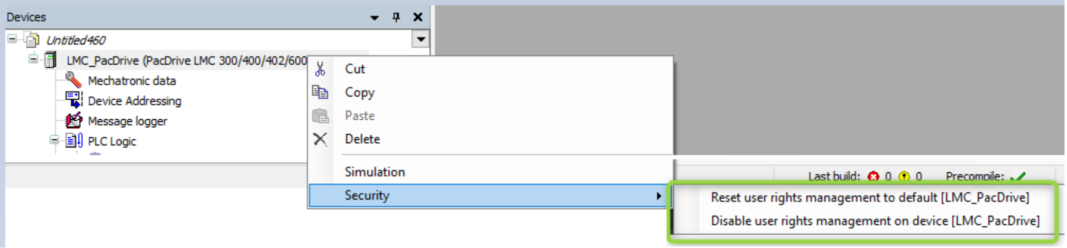
通过 EcoStruxure Machine Expert Logic Builder

对于 PacDrive LMC Eco 和 PacDrive LMC Pro/Pro2 控制器，可以使用 **Reset user rights management to default** 命令来复位设备用户权限，此命令在以下两个不同的位置均有提供：

在线 → 安全 → Reset user rights management to default菜单：



控制器的上下文菜单中的安全 → Reset user rights management to default命令：


Devices
Untitled460
LMC_PacDrive (PacDrive LMC 300/400/402/600
Mechatronic data
Device Addressing
Message logger
PLC Logic
Cut
Copy
Paste
Delete
Simulation
Security
Last build: 0 0 Precompile:
Reset user rights management to default [LMC_PacDrive]
Disable user rights management on device [LMC_PacDrive]

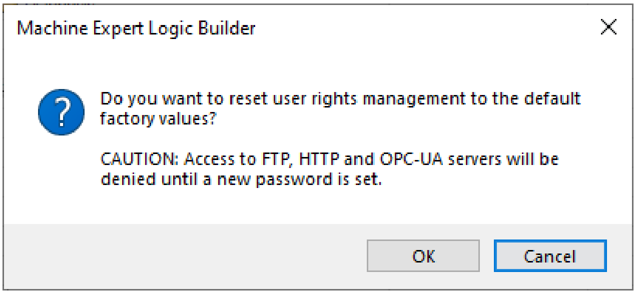
⚠ 小心

无法通过 FTP、HTTP、OPC-UA 进行访问

当复位用户权限管理至缺省设置后，在设置具体的用户名和密码之前，对 FTP、HTTP 和 OPC-UA 服务器的访问会遭到拒绝。

不遵循上述说明可能导致人身伤害或设备损坏。

单击**确定**确认消息。



Machine Expert Logic Builder

Do you want to reset user rights management to the default factory values?

CAUTION: Access to FTP, HTTP and OPC-UA servers will be denied until a new password is set.

通过控制器 Web 服务器复位

Modicon M241 Logic Controller、Modicon M251 Logic Controller 和 Modicon M262 Logic/Motion Controller 支持通过嵌入式 Web 服务器复位设备用户权限管理：**维护** → **用户管理** → **USER ACCOUNTS MANAGEMENT** → **复位到默认**

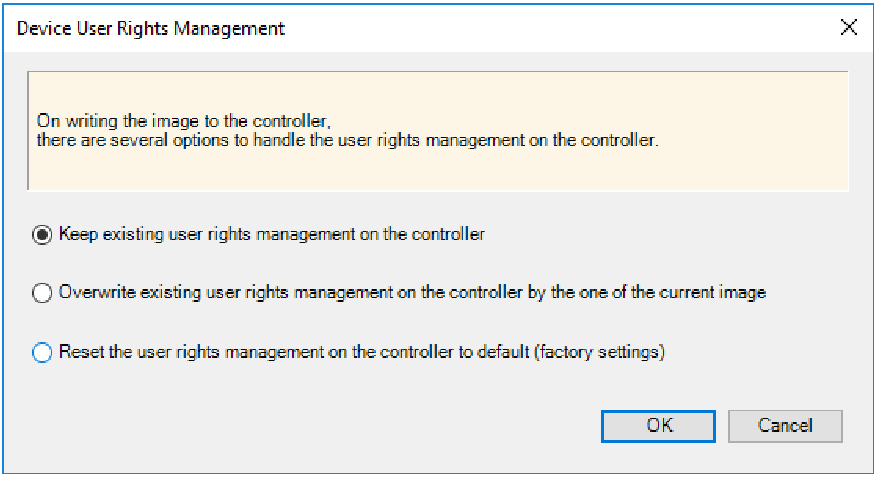
EcoStruxure Machine Expert 在线帮助中的 查询您的控制器对应的*编程指南*，以了解更多信息：

- Modicon M241 Logic Controller
  Machine Expert > V1.2 > Controllers > M241 Logic Controllers > M241 Logic Controller - Programming Guide > Ethernet Configuration > Ethernet Services > Web Server
- Modicon M251 Logic Controller
  Machine Expert > V1.2 > Controllers > M251 Logic Controllers > M251 Logic Controller - Programming Guide > Ethernet Configuration > Ethernet Services > Web Server
- Modicon M262 Logic/Motion Controller
  Machine Expert > V1.2 > Controllers > M262 Logic/Motion Controllers > M262 Logic/Motion Controller - Programming Guide > Ethernet Configuration > Ethernet Services > Web Server

通过 Controller Assistant 复位

使用 EcoStruxure Machine Expert V1.2，服务工具 Controller Assistant 可支持 PacDrive LMC Eco 和 PacDrive LMC Pro/Pro2 控制器的用户权限管理。

将映像写入到控制器（在线模式下）或者写入到 SD 卡或闪存盘时，会提示您决定如何处理控制器中的用户权限：



Device User Rights Management

On writing the image to the controller,
there are several options to handle the user rights management on the controller.

● Keep existing user rights management on the controller

○ Overwrite existing user rights management on the controller by the one of the current image

○ Reset the user rights management on the controller to default (factory settings)

有以下选项可供使用：

- **Keep existing user rights management on the controller**
  激活此选项可保持原有用户权限管理不变。即使禁用了用户权限管理，也适用此操作。
  注意： 如在未定义用户权限的情况下将 EcoStruxure Machine Expert V1.2 或更高版本写入到控制器，控制器中的用户权限管理将被设置为缺省设置。

- **Overwrite existing user rights management on the controller by the one on the current image**
  控制器中的用户权限管理将被在要写入的映像中定义的用户权限管理覆盖。
  注意： 如果试图写入 EcoStruxure Machine Expert V1.2 或更高版本的固件并且如果映像中未定义用户权限管理，则控制器中的用户权限管理将被设置为缺省设置。

- **Reset the user rights management on the controller to default (factory settings)**
  控制器中的用户权限管理将被设置为缺省设置。

缺省情况下，于在线模式下写入到控制器时，会保留控制器中原有的用户权限管理。

不使用凭据的复位

如果凭据丢失，可以使用服务工具 Controller Assistant 将映像写入到 SD 卡或闪存盘，以此来复位控制器的用户权限管理。

在提示您决定如何处理控制器中的用户权限的消息中，选择选项 **Reset the user rights management on the controller to default (factory settings)**。如果此选项不可用，可以通过缺省设置附带的 scratch 创建新固件。然后您就可以直接通过此 SD 卡或闪存盘来重启控制器。

Modicon M241 Logic Controller、Modicon M251 Logic Controller 和 Modicon M262 Logic/Motion Controller 还允许您修改 SD 卡上的 script.cmd 文件以复位用户权限管理。查询您的控制器对应的*编程指南*，了解详细信息。

禁用设备用户权限

概述

为了帮助防止对您控制器的未授权访问，应保持设备用户权限管理功能处于激活状态。如果能够确保未授权人员无法访问自己的机器或过程，则可以按照本章所述，禁用此功能。为此，您需要使用相应的凭据。

通过 EcoStruxure Machine Expert Logic Builder

对于 PacDrive LMC Eco 和 PacDrive LMC Pro/Pro2 控制器，可以使用 **Disable user rights management on device** 命令来禁用设备用户权限管理，此命令在以下两个不同的位置均有提供：

- **在线** → **安全** → **Disable user rights management on device** 菜单
- 控制器的上下文菜单中的**安全** → **Disable user rights management on device** 命令

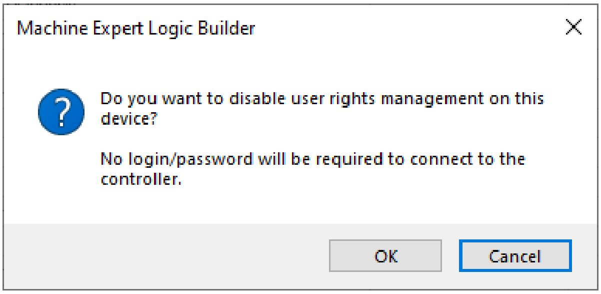
⚠ 警告

非法访问以及机器操作

如果未授权人员能够直接或通过网络访问您的机器或过程，则不要禁用用户权限管理。

不遵循上述说明可能导致人员伤亡或设备损坏。

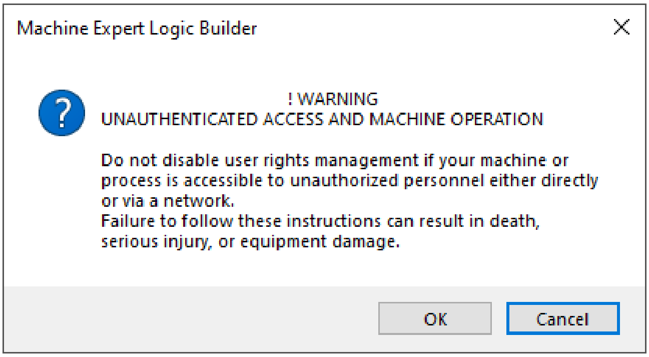
如果确定要禁用设备用户权限，则按**确定**确认两个确认消息。



Machine Expert Logic Builder

Do you want to disable user rights management on this device?

No login/password will be required to connect to the controller.



Machine Expert Logic Builder

! WARNING
UNAUTHENTICATED ACCESS AND MACHINE OPERATION

Do not disable user rights management if your machine or process is accessible to unauthorized personnel either directly or via a network.
Failure to follow these instructions can result in death, serious injury, or equipment damage.

结果：现在能够在不使用凭据的情况下访问控制器。

通过控制器 Web 服务器禁用

Modicon M241 Logic Controller、Modicon M251 Logic Controller 和 Modicon M262 Logic/Motion Controller 支持通过嵌入式 Web 服务器禁用设备用户权限管理：**维护 → 用户管理 → USER ACCOUNTS MANAGEMENT → 禁用**

EcoStruxure Machine Expert 在线帮助中的 查询您的控制器对应的*编程指南*，以了解更多信息：

- Modicon M241 Logic Controller
  Machine Expert > V1.2 > Controllers > M241 Logic Controllers > M241 Logic Controller - Programming Guide > Ethernet Configuration > Ethernet Services > Web Server
- Modicon M251 Logic Controller
  Machine Expert > V1.2 > Controllers > M251 Logic Controllers > M251 Logic Controller - Programming Guide > Ethernet Configuration > Ethernet Services > Web Server
- Modicon M262 Logic/Motion Controller
  Machine Expert > V1.2 > Controllers > M262 Logic/Motion Controllers > M262 Logic/Motion Controller - Programming Guide > Ethernet Configuration > Ethernet Services > Web Server

为EcoStruxure Machine Expert Logic Builder中的仿真设备禁用用户权限。

EcoStruxure Machine Expert Logic Builder 中的仿真设备拥有自己的用户权限，这些权限可能不同于实际控制器中定义的那些权限。

注意： 为了有助于避免账户锁闭（锁死），应先断开 EcoStruxure Machine Expert Logic Builder 与控制器的连接，并确保没有其他客户端（如 HMI）会自动使用先前的用户权限配置进行连接。

如要禁用仿真设备中的用户权限，请执行以下步骤：

步骤	操作
1	关闭 EcoStruxure Machine Expert Logic Builder 的所有实例。
2	关闭 Vijeo-Designer 的所有实例。
3	删除文件夹 c:\ProgramData\CODESYS\Simulation。 **结果**：仿真设备复位到缺省设置。

通过调用参数来管理设备用户权限

概述

服务工具 Controller Assistant 和 Diagnostics 提供在使用要求的凭据连接到控制器时需用到的命令行参数。有关详细信息，请参阅 EcoStruxure Machine Expert 在线帮助中的 Controller Assistant - 用户指南和 Diagnostics - 用户指南。

有以下参数可供使用：

- -username <Username>
- -password <Password>
- -renewalpassword <RenewalPassword>

示例

```
ControllerAssistant.exe -username Administrator -password Administrator -
renewalpassword MyNewPassword -getcontrollerinfo etcp4://192.168.3.40
```

```
Diagnostics.exe -username Administrator -password MyPassword -save
ip etcp4://192.168.3.40 c:\Temp\MyDiagnosticsFile.pdi
```

-renewalpassword 参数

需要插入新密码时，会用到参数 -renewalpassword 。这通常发生在首次登录到控制器且需要输入缺省凭据（用户名 = Administrator，密码 = Administrator）时。

参数 -renewalpassword 无法用来更改密码。

启动 Controller Assistant

也可以使用命令行参数以图形用户界面启动 Controller Assistant。在这种情况下，系统会提示您输入凭据。这些信息来自参数值。

使用脚本 API 管理设备用户权限

使用在线服务时所用的脚本

EcoStruxure Machine Expert 让您能够通过脚本 API 访问其多项在线服务。为了建立连接或稍后使用在线服务，系统中必须存储有效的凭据。

为在线服务提供特定凭据

对于多控制器项目，您可以通过在线设备或在线应用程序存储凭据。如果为连接提供了特定凭据，则系统将使用这些信息。

示例：

```
# create an "online device" to use online services
root_device = projects.primary.find("LMC_PacDrive", False)[0]
online_device = online.create_online_device(root_device)

# store credentials specific to this "online device"
online.set_specific_credentials(online_device, "my_user", "my_password")

# use of any online service
online_device.connect()
```

为在线服务提供缺省凭据

如果没有为连接提供特定凭据，系统会使用缺省凭据。

示例：

```
# create an "online device" to use online services
root_device = projects.primary.find("LMC_PacDrive", False)[0]
online_device = online.create_online_device(root_device)

# store default credentials
online.set_default_credentials("my_user", "my_password")

# use of any online service
online_device.connect()
```

用于强制密码更新的脚本

在以下情形下，在验证身份后，用户需要更改密码：

- 首次登录到新控制器。
- 将用户权限管理复位到缺省设置后首次连接。
- 设备管理员针对特定用户强制执行了密码更新。

EcoStruxure Machine Expert V1.2 不支持使用脚本 API 来更新密码。请使用服务工具 Controller Assistant 来执行此操作。

您可以通过以下示例所示的命令行来调用 Controller Assistant 的最新版本：

```
"c:\Program Files (x86)\Schneider
Electric\EcoStruxureMachine Expert\Tools\ControllerAssistant\ControllerAssistant.exe"
-username Administrator -password Administrator -renewalpassword MyNewPassword -
getcontrollerinfo etcp4://192.168.3.50
```

克隆 SD 卡时包含用户权限

概述

Modicon M241 Logic Controller、Modicon M251 Logic Controller 和 Modicon M262 Logic/Motion Controller 提供了一种克隆功能，让您能够将控制器的映像写入到 SD 卡。缺省不将用户权限管理写入到包含映像的 SD 卡。如果您的控制器支持，可以在控制器的 Web 服务器上，在**克隆管理**中激活克隆操作的用户权限管理。查询您的控制器对应的*编程指南*，了解详细信息。

附加信息

网络安全最佳做法

Schneider Electric 在我们的产品中纳入了网络安全最佳做法和解决方案。

注意： 为了有助于保持和保护 Schneider Electric 产品的安全，强烈建议您采取 *Schneider Electric website* 上提供的 *Cybersecurity Best Practices* 中所述的网络安全最佳做法。