

Emerson Security Deployment Guide for ROC800-Series

System Training

A well-trained workforce is critical to the success of your operation. Knowing how to correctly install, configure, program, calibrate, and trouble-shoot your Emerson equipment provides your engineers and technicians with the skills and confidence to optimize your investment. Emerson Automation Solutions offers a variety of ways for your personnel to acquire essential system expertise. Our full-time professional instructors can conduct classroom training at several of our corporate offices, at your site, or even at your regional Emerson office. You can also receive the same quality training via our live, interactive Emerson Virtual Classroom and save on travel costs. For our complete schedule and further information, contact the Energy and Transportation Solutions Training Department at 800-338-8158 or email us at education@emerson.com.

Contents

Chapter 1. Introduction	1
1.1 New Product Features	1
1.2 New Firmware Versions	2
1.3 Rollout Procedure	2
Chapter 2. Configuring the New Features	3
2.1 Opting into Complex Usernames/Passwords	5
2.2 After Opting In: ROCLINK 800 Security	7
2.3 After Opting In: Device Security (IDs/Passwords)	8
2.4 After Opting In: Device Security (Comm Ports)	9

Emerson Security Deployment Guide for ROC800-Series

D301912X012

September 2022

Chapter 1. Introduction

The United States TSA (Transport Security Administration) released a Security Directive (Security Directive Pipeline-2021-02) to selected operators of critical US Pipeline Infrastructure. This directive requires that the recipients undertake various actions to protect the national security, economy, and public health and safety of the United States from the impact of malicious cyber intrusions affecting the nation's most critical gas and liquids pipelines.

As a supplier to the pipeline industry, Emerson has reviewed the RTU and Flow Computer products we provide and how those compare with the requirements for usernames and passwords in the directive. As a result of that review Emerson is releasing updated firmware for the ROC800 and ROC800L products that will help users meet the related requirements in that directive.

This security enhancement impacts both the ROCLINK 800 software's security settings and the security settings in the currently active devices ROCLINK 800 affects. Modifying the security settings on all the devices in a field will take time and may occur in several phases. This can result in some devices having the enhancement security and some not. To anticipate this scenario, the ROCLINK 800 Security Table can maintain both the older ID/password format and the new ID/password format. This enables you to continue to access those devices which have not yet been upgraded to the new security enhancement. Of course, once all devices in field have been upgraded, you can delete the old ID/passwords in the ROCLINK 800 Security Tables.

1.1 New Product Features

For **SCADA/Displays**:

- Modified the ROC Plus and Liquids protocols so that passwords are not transmitted as clear text



Important

Before opting into the longer IDs/password format, consult with your third-party SCADA/HMI vendors to determine if their products support the security-enhanced protocols.

For **ROCLINK 800**:

- Increased unique ROCLINK 800 users from 32 to 64 (PC/server specific)
- Included opt-in process for the new security features

For the ROC800 platform (**ROC800/800L**):

- Added opt-in features:
 - Username can be a maximum of 30 (minimum of 3) alphanumeric and special characters and is **not** case-sensitive

Note

“Special characters” includes any character on the ASCII table between 0x20 and 0x7E (such as !, (, (, [,], =, @, etc.)

- Password can be a maximum of 32 (minimum of 8) alphanumeric and special characters (see note above) and **is** case-sensitive

- Once opted-in, **cannot** change back to old security setup
- Once opted in, passwords are no longer passed in clear text via the ROC Plus protocol
- Increased unique users to 64 (from 32) for both the device and the ROCLINK 800 software
- Provided a new LCD PIN log-in option for the ROC800 Keypad Display

Note

A revision of the ROC Keypad Display user program is anticipated for release after the release of the ROC800 firmware.

1.2 New Firmware Versions

New firmware and software versions support this functionality:

- ROC800 firmware: v. 3.90
- ROC800L firmware: v. 1.70
- ROCLINK 800 software: v. 2.70



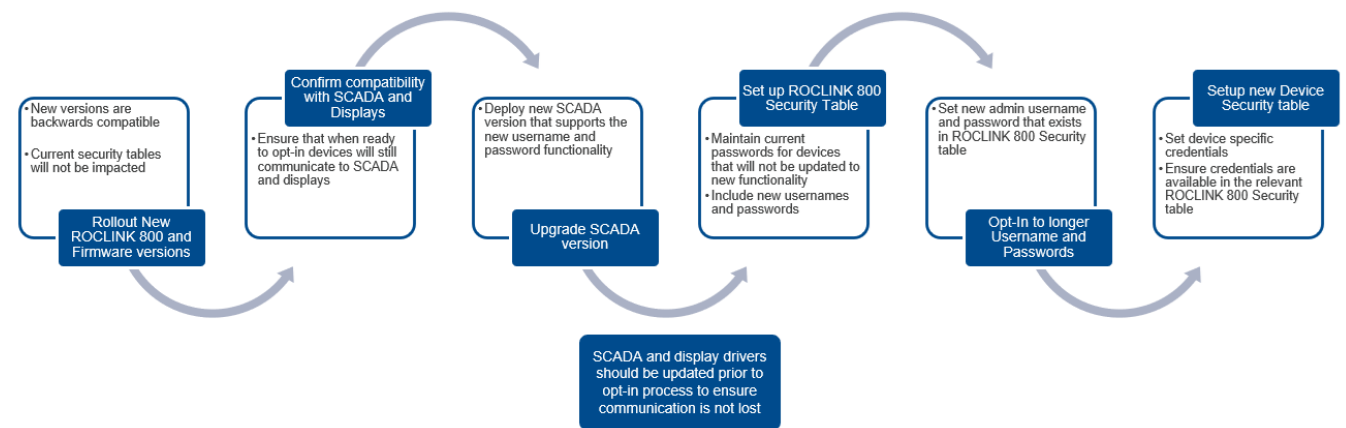
Important

Before opting into the new feature, confirm support in all software and devices communicating with the RTU or flow computer.

1.3 Rollout Procedure

The following graphic summarizes the required steps in the rollout:

Figure 1-1. Rollout Process



Chapter 2. Configuring the New Features

To configure the enhancements:

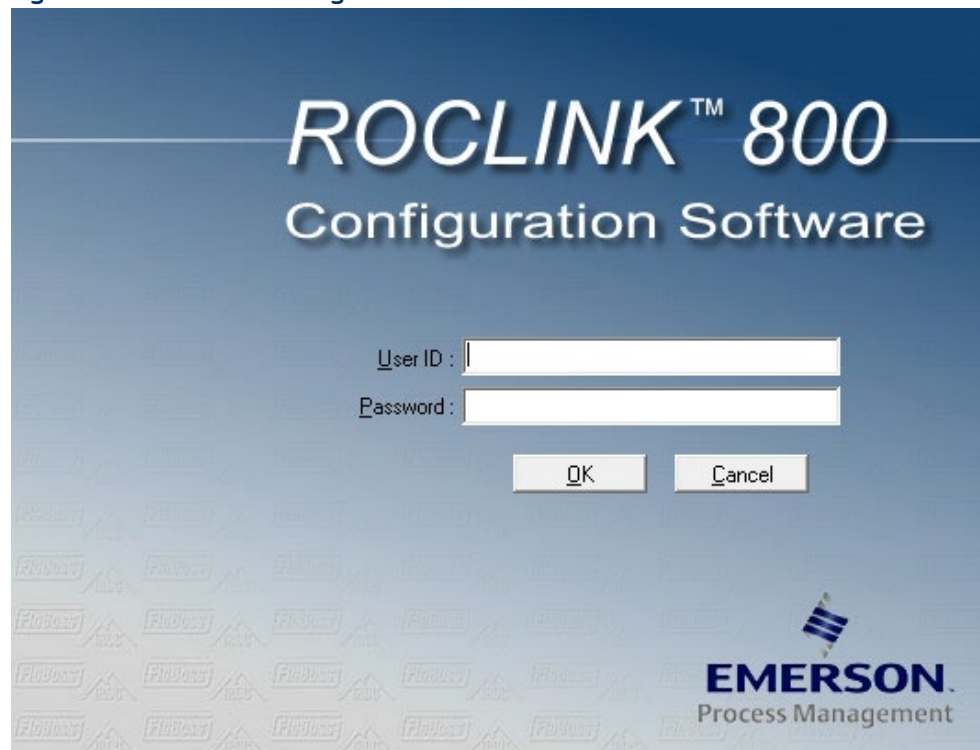
1. Install the new version of ROCLINK 800.
2. Install the new firmware version.

Note

The firmware and ROCLINK 800 are backwards-compatible; installing the new firmware **does not** break communications with the devices.

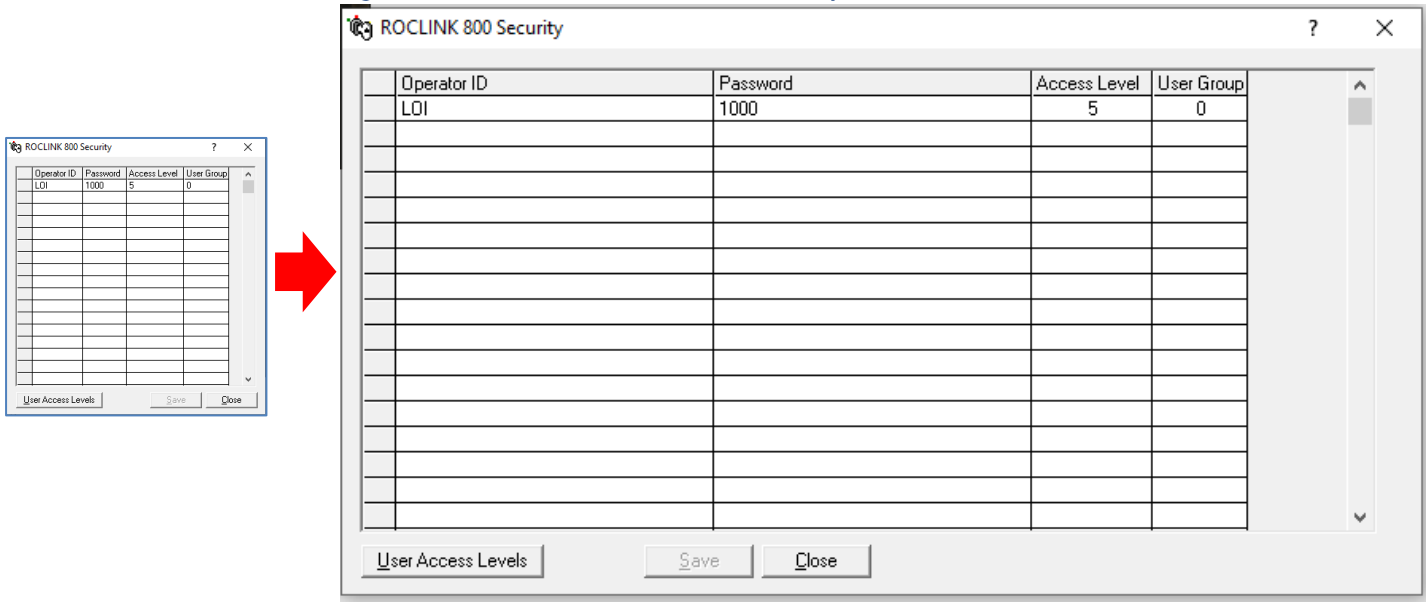
3. After the system performs a cold restart, the revised ROCLINK 800 log-in screen displays (note the longer User ID and Password fields).

Figure 2-1. ROCLINK 800 Log-in Screen



4. Access the enhanced ROCLINK 800 Security screen (**Utilities > ROCLINK 800 Security**) and configure new users.

Figure 2-2. Enhanced ROCLINK 800 Security Screen



With the new version of ROCLINK, you immediately access the larger user table, allowing you to define up to 64 operator IDs. These IDs can be a mix of the older username/password format and the new complex username/password formats. The ROCLINK 800 Security Table maintains both old and new IDs and passwords (see *Figure 2-7*).

2.1 Opting into Complex Usernames/Passwords



Important

You must log into ROCLINK using an administrator-level ID.

Opting into the new complex usernames/password format occurs at the device.

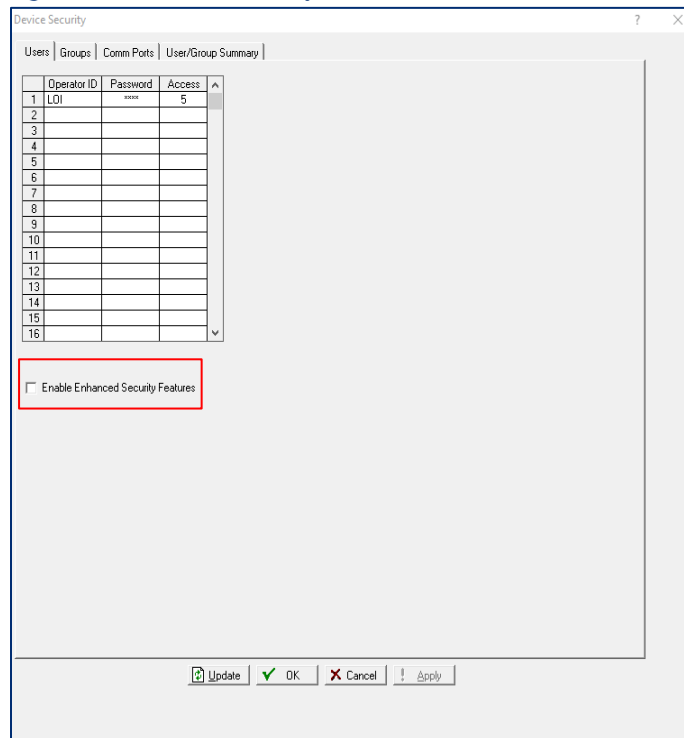


Important

Once you opt into the complex usernames/passwords format, you **cannot** change back to the previous security format.

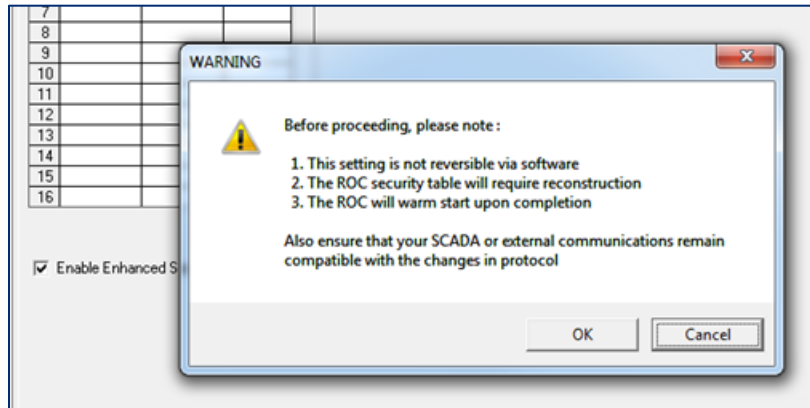
1. Access the device's security screen (**ROC > Security**).

Figure 2-3. Device Security Screen



2. Select the **Enable Enhanced Security Features** option and click **Apply**. A warning dialog displays:

Figure 2-4. Warning Dialog

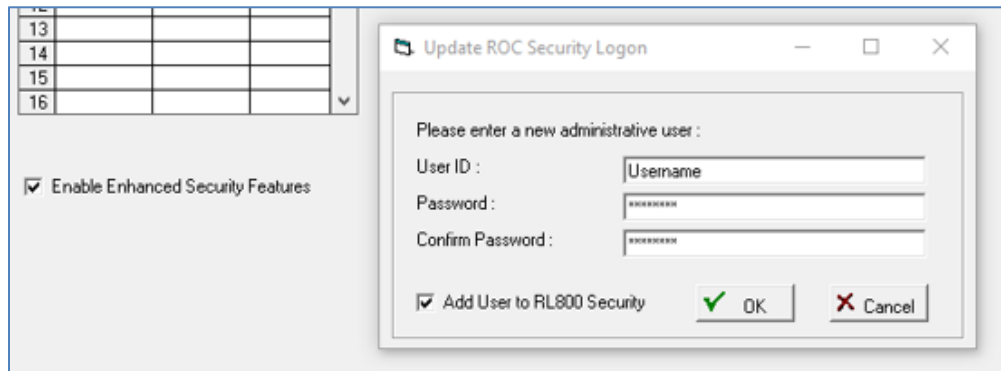


Important

Click **Cancel** (the default value) to exit this dialog and retain your current security table.

3. Click **OK** to opt into the new security enhancement. The Update ROC Security Logon dialog displays:

Figure 2-5. Update ROC Security Logon Dialog



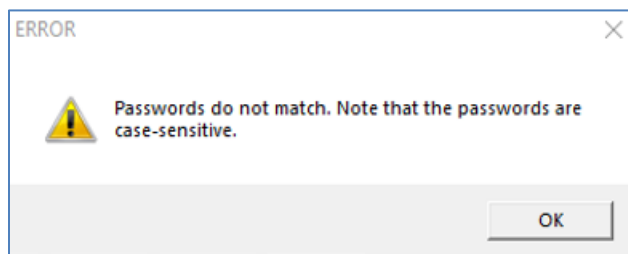
Important

Click **Cancel** to exit this dialog and retain your current security table.

4. Define a new User ID and password. This becomes is the **new administrative User ID**. Select the **Add User to RL800 Security** option to automatically add this administrative user ID to the ROCLINK 800 Security table.

Note

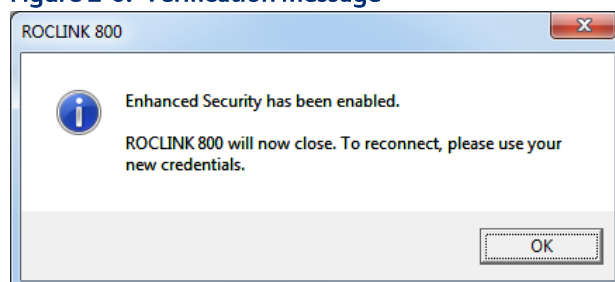
If the contents of the Password and Confirm Password fields do not exactly match (remember case-sensitivity), ROCLINK displays an error message:



Click **OK** to clear the message and re-enter the contents of both fields.

5. Click **OK**. When ROCLINK accepts the new administrative ID and password, ROCLINK displays a verification message:

Figure 2-6. Verification Message

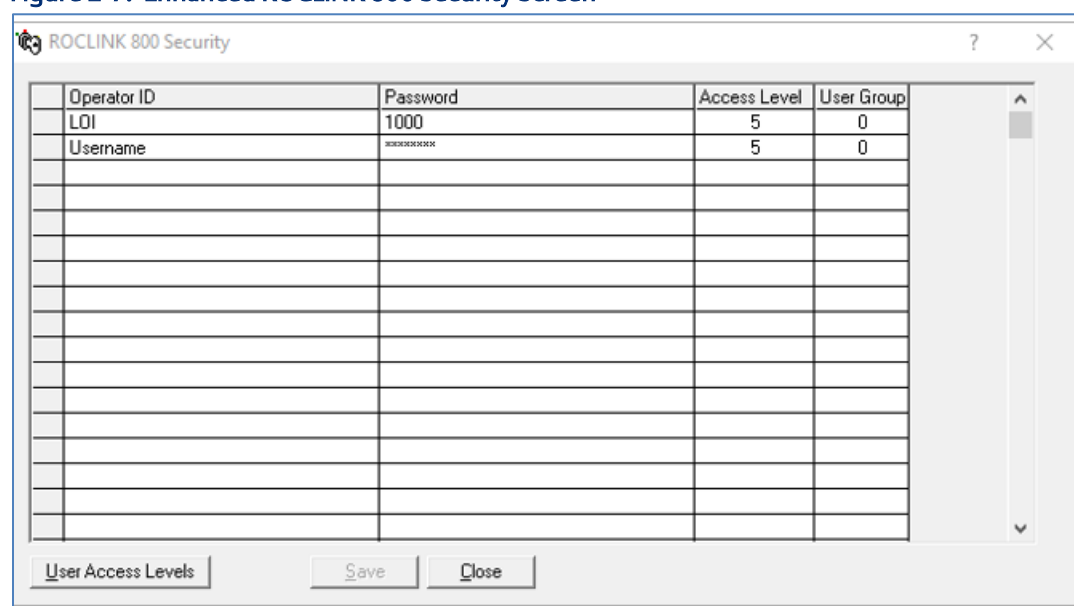


6. Click **OK** to close the message and exit ROCLINK 800.

2.2 After Opting In: ROCLINK 800 Security

1. Log into ROCLINK using the new **administrator** operator ID and password (defined in step 4 of section 2.1).
2. Access the ROCLINK 800 Security screen (**Utilities > ROCLINK 800 Security**).

Figure 2-7. Enhanced ROCLINK 800 Security Screen



3. Define any additional IDs/passwords for ROCLINK 800 users.



Important

When connecting to a device that still uses the older security format, you need to close ROCLINK and reconnect to that device using the corresponding operation ID/password.

2.3 After Opting In: Device Security (IDs/Passwords)

Once you implement the new enhanced security, you then need to modify the device security table for **each** device.



Important

Once you configure a device to use the longer operator IDs/passwords, you **cannot** log into that device using the old (short) IDs/passwords.

1. Log onto a device and access its security table (ROC > Security):

Figure 2-8. Enhanced Device Security Screen

	Operator ID	Password	Access	Keypad PIN	
1	Username	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	5	None	^
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					v

2. Define new operator IDs (of at least **3** and no more than **30** alphanumeric/special characters) and passwords (of at least **8** and no more than **32** alphanumeric/special characters).

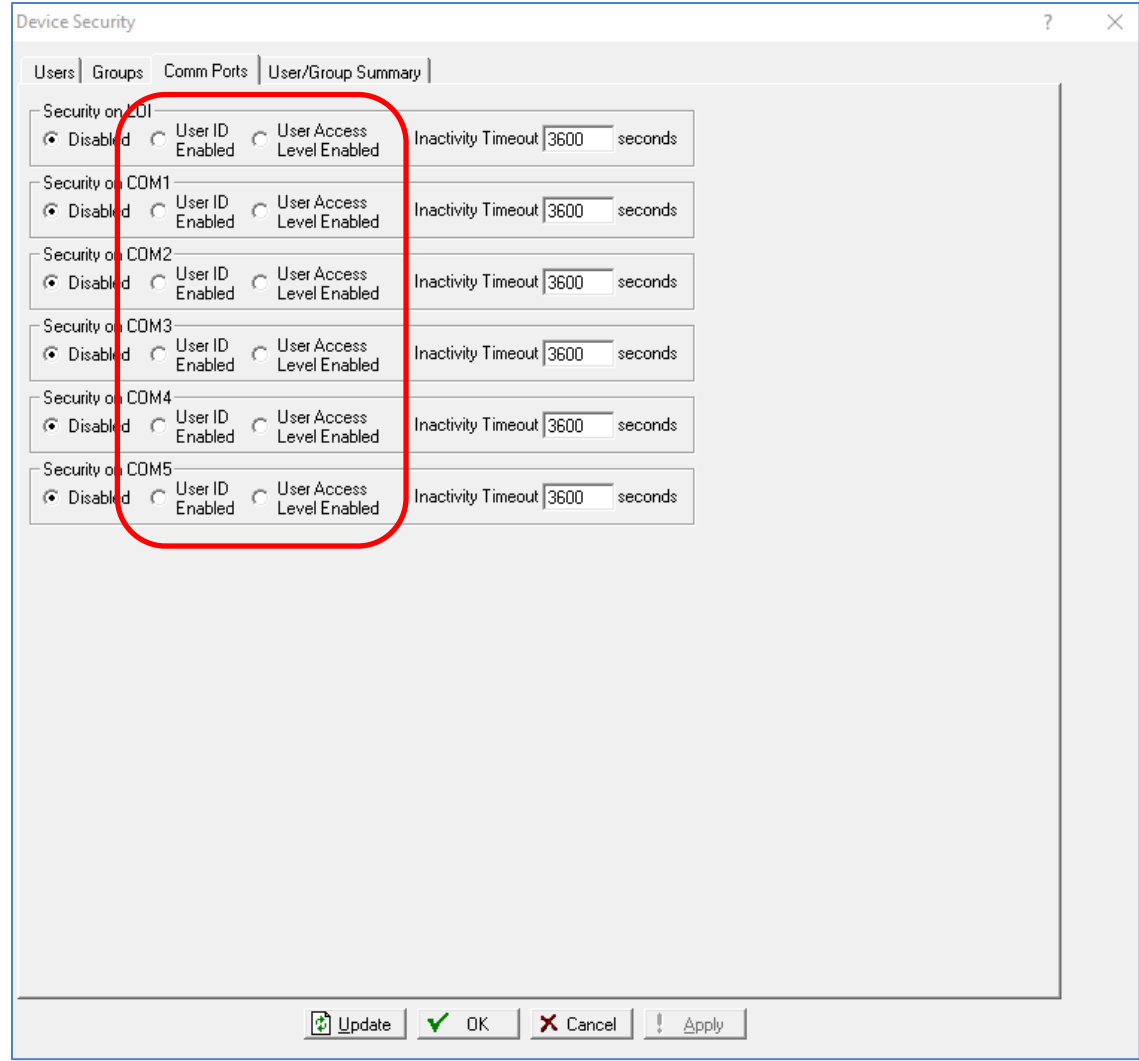
Note

Ensure that you define IDs and password for individual users in ROCLINK 800 security to enable them to easily log onto their device.

2.4 After Opting In: Device Security (Comm Ports)

This feature is unchanged from previous versions of ROCLINK 800, but to comply with the security directive you **must** enable security (either by User ID or User Access Level) for each comm port.

Figure 2-9. Enhanced Device Security Screen



Emerson Security Deployment Guide for ROC800-Series

D301912X012

September 2022

For customer service and technical support, visit www.Emerson.com/SupportNet.

Global Headquarters,

North America, and Latin America:

Emerson Automation Solutions
Remote Automation Solutions
6005 Rogerdale Road
Houston, TX 77072 U.S.A.
T +1 281 879 2699 | F +1 281 988 4445
www.Emerson.com/RemoteAutomation

Europe:

Emerson Automation Solutions
Remote Automation Solutions
Unit 1, Waterfront Business Park
Dudley Road, Brierley Hill
Dudley DY5 1LX UK
T +44 1384 487200

Middle East/Africa:

Emerson Automation Solutions
Remote Automation Solutions
Emerson FZE
P.O. Box 17033
Jebel Ali Free Zone – South 2
Dubai U.A.E.
T +971 4 8118100 | F +971 4 8865465

Asia-Pacific:

Emerson Automation Solutions
Remote Automation Solutions
1 Pandan Crescent
Singapore 128461
T +65 6777 8211 | F +65 6777 0947

© 2022 Energy and Transportation Solutions, an affiliate of Emerson Electric Co. All rights reserved.

This publication is for informational purposes only. While every effort has been made to ensure accuracy, this publication shall not be read to include any warranty or guarantee, express or implied, including as regards the products or services described or their use or applicability. Energy and Transportation Solutions (ETS) reserves the right to modify or improve the designs or specifications of its products at any time without notice. All sales are governed by ETS terms and conditions which are available upon request. ETS accepts no responsibility for proper selection, use or maintenance of any product, which remains solely with the purchaser and/or end-user. Emerson Automation Solutions, Emerson, and the Emerson logo are trademarks and service marks of Emerson Electric Co. All other marks are the property of their respective owners.