Emerson Security Deployment Guide for ROC800-Series RTUs and FloBoss™ 107 Flow Computers

Energy and Transportation Solutions

EMERSON™

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

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/ROC800L and FloBoss™ 107 products that helps 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 the field have been upgraded, you can delete or retain the old ID/passwords in the ROCLINK 800 Security Tables.

1.1 Product Features

For **SCADA/Displays**:

- Modified the ROC andROC Plus 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 and Liquids protocols (for the ROC800 and ROC800L implementations) and are not stored in the ROCLINK 800 database or device memory
- 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.

For the **FloBoss 107**:

- Added opt-in features:
  - Username can be a maximum of 30 (minimum of 3) alphanumeric and special characters, (see note above) and is **not** case-sensitive
  - Password can be a maximum of 32 (minimum of 8) alphanumeric and special characters 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 Protocol and are not stored in the ROCLINK 800 database or device memory
- Maintains support for a maximum of 16 users for the device (same maximum as current firmware)
- Increased unique users for ROCLINK 800 (version 2.70 or newer) to 64
- Maintained current PIN log-in on FB107 LCD
- Supported through new FloBoss 107 Security user program (W68318X0012), a non-licensed program which **can only be** installed in previously unavailable slot **8**)

1.2 New Firmware Versions

New firmware and software versions support this functionality. For the ROC800:

- ROC800 firmware: v. 3.90
- ROC800L firmware: v. 1.70
- ROCLINK 800 software: v. 2.71

For the FloBoss 107:

- FloBoss 107 firmware: v. 2.00
- ROCLINK 800 software v. 2.71

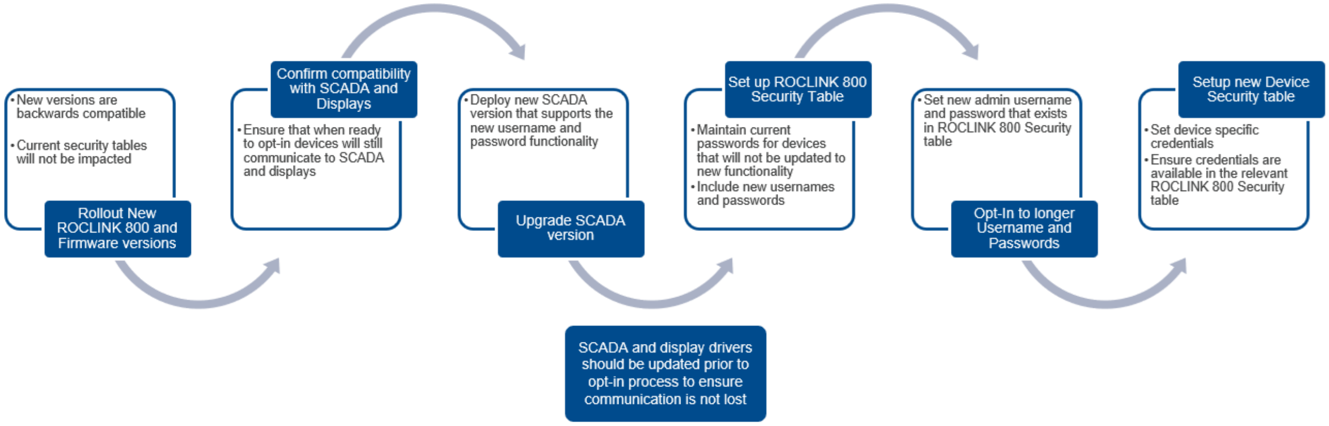
Important

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

1.3 Rollout Procedure

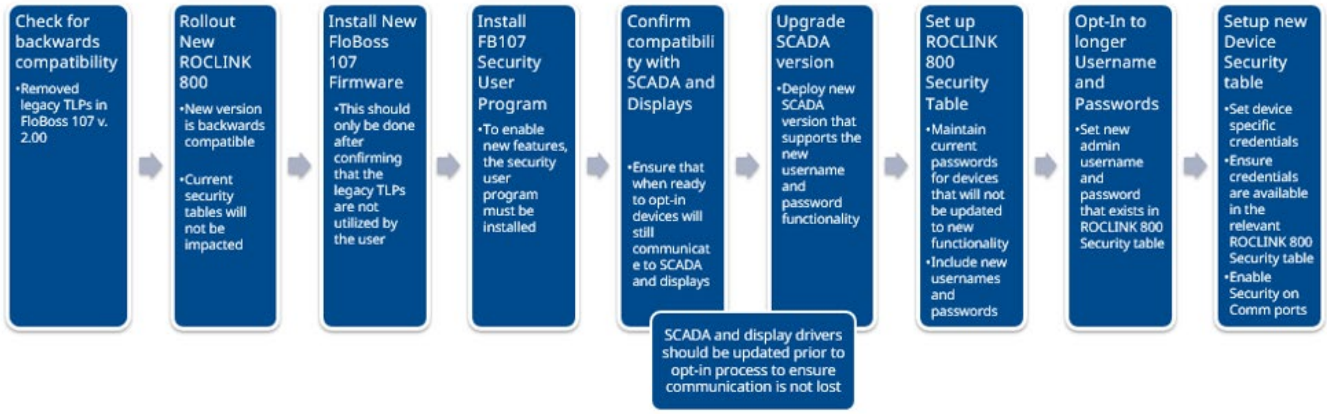
The following graphic summarizes the required steps in the rollout for the ROC800:

Figure 1-1. Rollout Process for ROC800


• New versions are backwards compatible
• Current security tables will not be impacted
Rollout New ROCLINK 800 and Firmware versions
Confirm compatibility with SCADA and Displays
• Ensure that when ready to opt-in devices will still communicate to SCADA and displays
• Deploy new SCADA version that supports the new username and password functionality
Upgrade SCADA version
SCADA and display drivers should be updated prior to opt-in process to ensure communication is not lost
Set up ROCLINK 800 Security Table
• Maintain current passwords for devices that will not be updated to new functionality
• Include new usernames and passwords
• Set new admin username and password that exists in ROCLINK 800 Security table
Opt-In to longer Username and Passwords
Setup new Device Security table
• Set device specific credentials
• Ensure credentials are available in the relevant ROCLINK 800 Security table

The following graphic summarizes the required steps in the rollout for the FloBoss 107 which, because of the installation of a user program, differs from the process for the ROC800:

Figure 1-2. Rollout Process for FloBoss 107


Check for backwards compatibility
•Removed legacy TLPs in FloBoss 107 v. 2.00
Rollout New ROCLINK 800
•New version is backwards compatible
•Current security tables will not be impacted
Install New FloBoss 107 Firmware
•This should only be done after confirming that the legacy TLPs are not utilized by the user
Install FB107 Security User Program
•To enable new features, the security user program must be installed
Confirm compatibility with SCADA and Displays
•Ensure that when ready to opt-in devices will still communicate to SCADA and displays
SCADA and display drivers should be updated prior to opt-in process to ensure communication is not lost
Upgrade SCADA version
•Deploy new SCADA version that supports the new username and password functionality
Set up ROCLINK 800 Security Table
•Maintain current passwords for devices that will not be updated to new functionality
•Include new usernames and passwords
Opt-In to longer Username and Passwords
•Set new admin username and password that exists in ROCLINK 800 Security table
Setup new Device Security table
•Set device specific credentials
•Ensure credentials are available in the relevant ROCLINK 800 Security table
•Enable Security on Comm ports

Chapter 2. Configuring Security for the ROC800

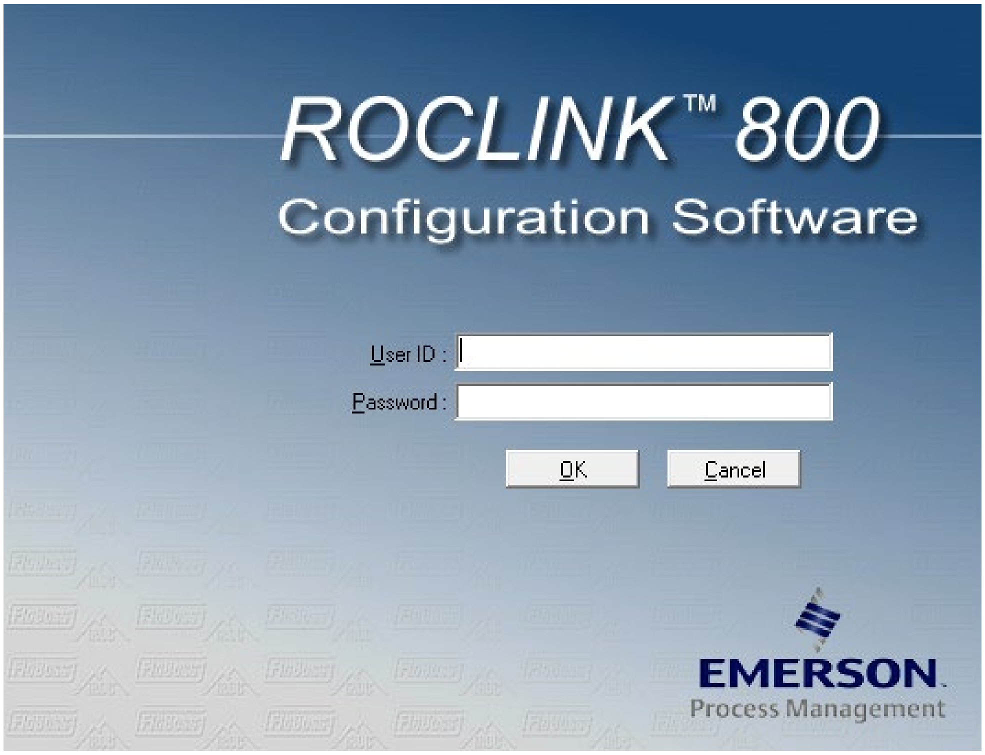
To configure the enhancements:

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.

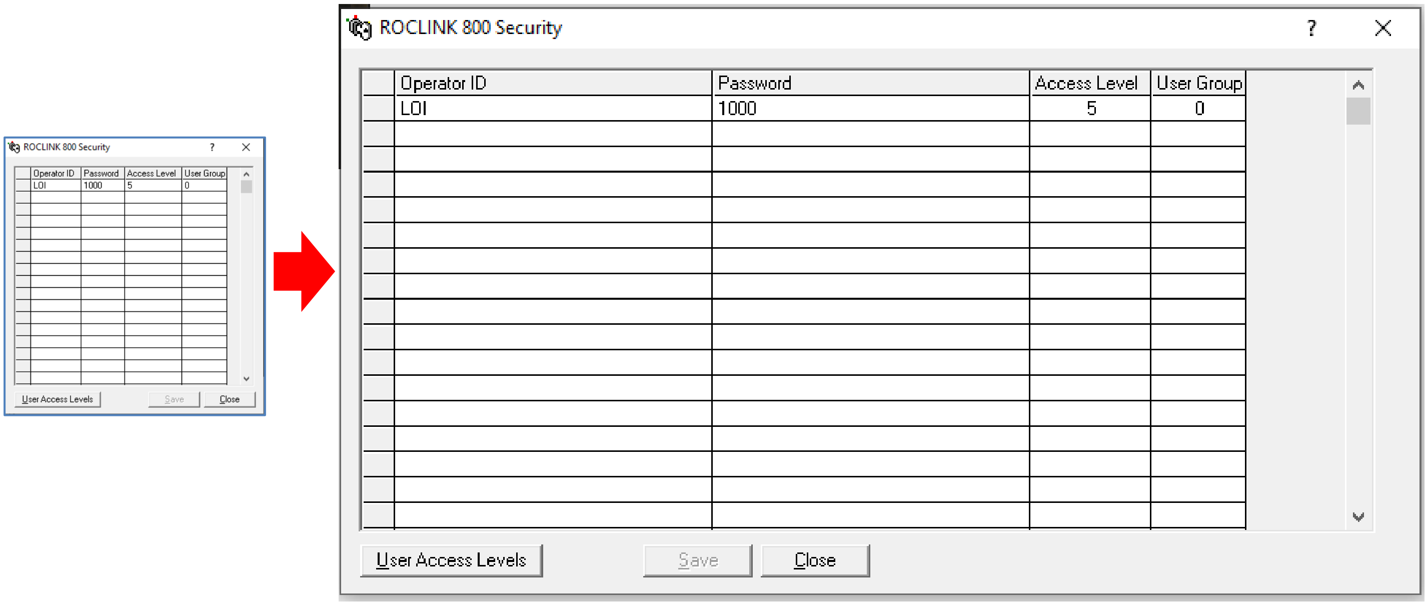
3. After the system performs a warm restart, the revised ROCLINK 800 log-in screen displays (note the longer User ID and Password fields).

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



Operator ID	Password	Access Level	User Group
LOI	1000	5	0

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.

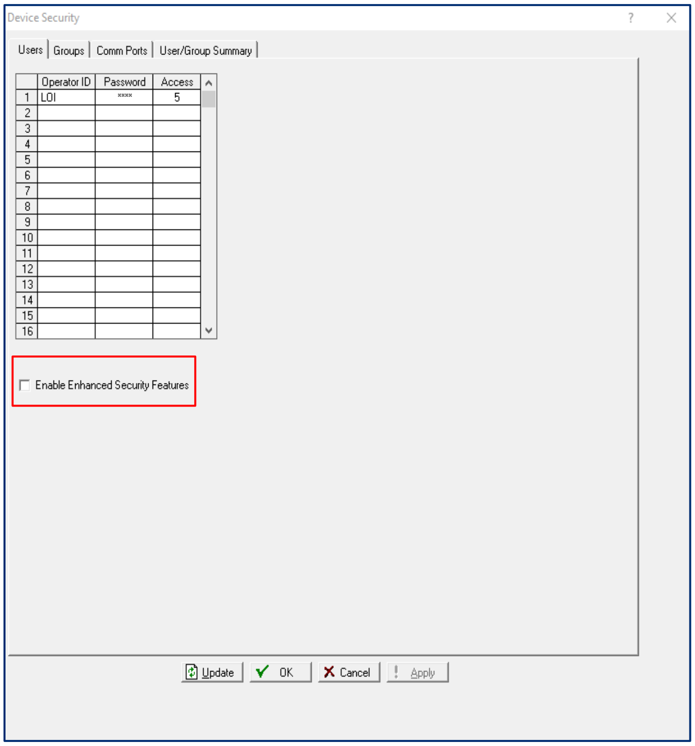
Opting into the new complex usernames/password format occurs at the device.

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

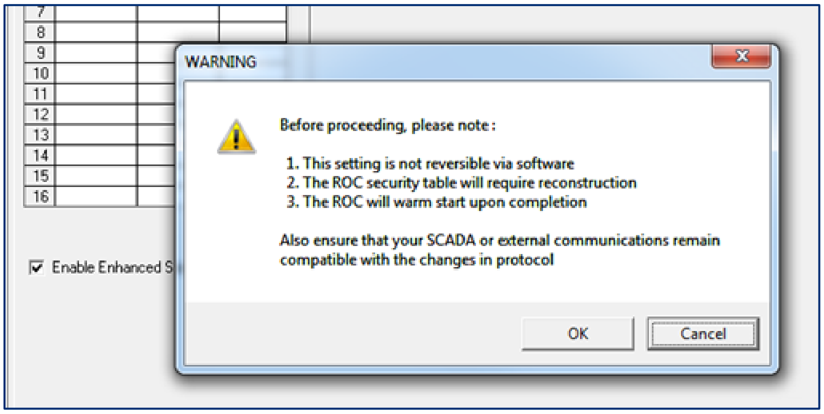


	Operator ID	Password	Access
1	LOI	****	5
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			

□ Enable Enhanced Security Features

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

Figure 2-4. Warning Dialog



Before proceeding, please note :

1. This setting is not reversible via software
2. The ROC security table will require reconstruction
3. The ROC will warm start upon completion

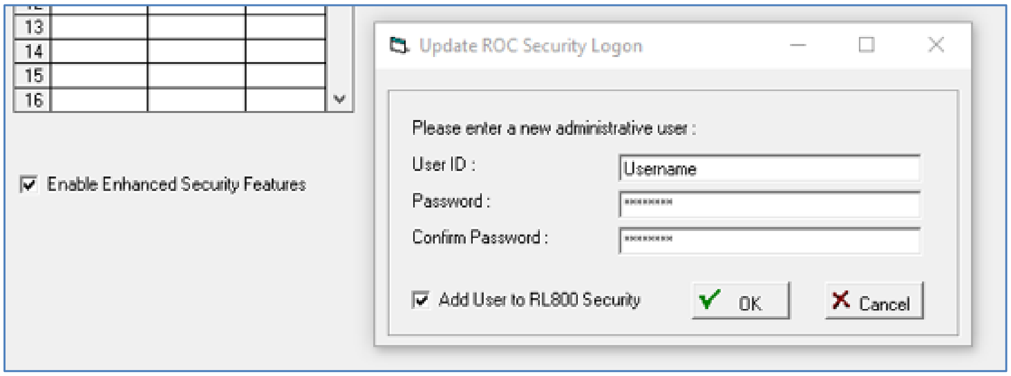
Also ensure that your SCADA or external communications remain compatible with the changes in protocol

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



☑ Enable Enhanced Security Features

Please enter a new administrative user :

User ID : Username

Password : ********

Confirm Password : ********

☑ Add User to RL800 Security

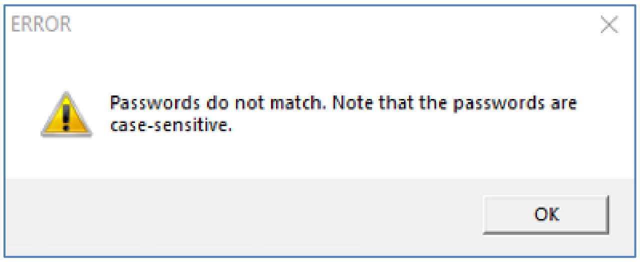
Important

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

4. Define a new User ID and password. This becomes 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:



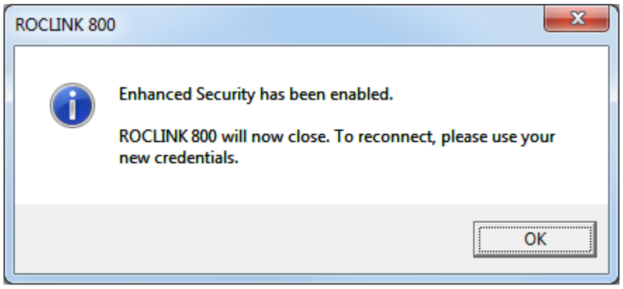
ERROR

Passwords do not match. Note that the passwords are case-sensitive.

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



ROCLINK 800

Enhanced Security has been enabled.

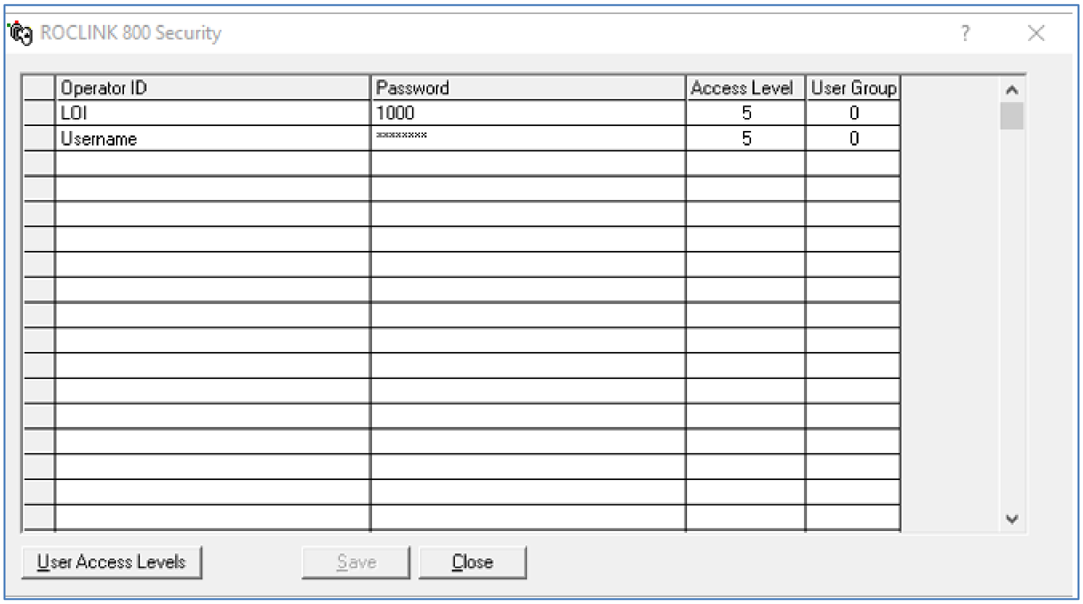
ROCLINK 800 will now close. To reconnect, please use your new credentials.

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



Operator ID	Password	Access Level	User Group
LOI	1000	5	0
Username	********	5	0

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.

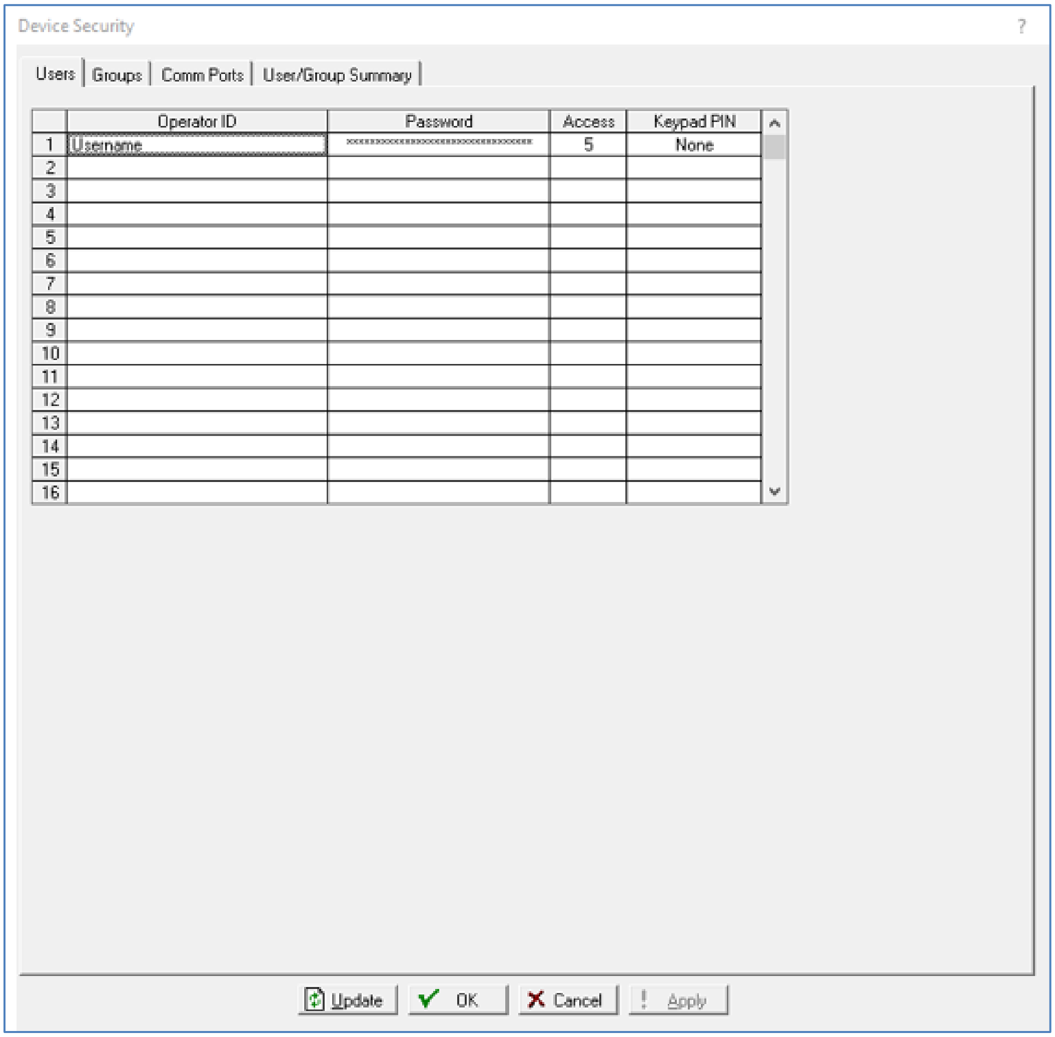
2.3 After Opting In: Device Security (IDs/Passwords)

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 (for ROC800)



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

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.

3. Complete the Keypad PIN field with an eight-digit numeric PIN for any operator IDs that need to access the ROC Keypad Display.

⚠ **Important**

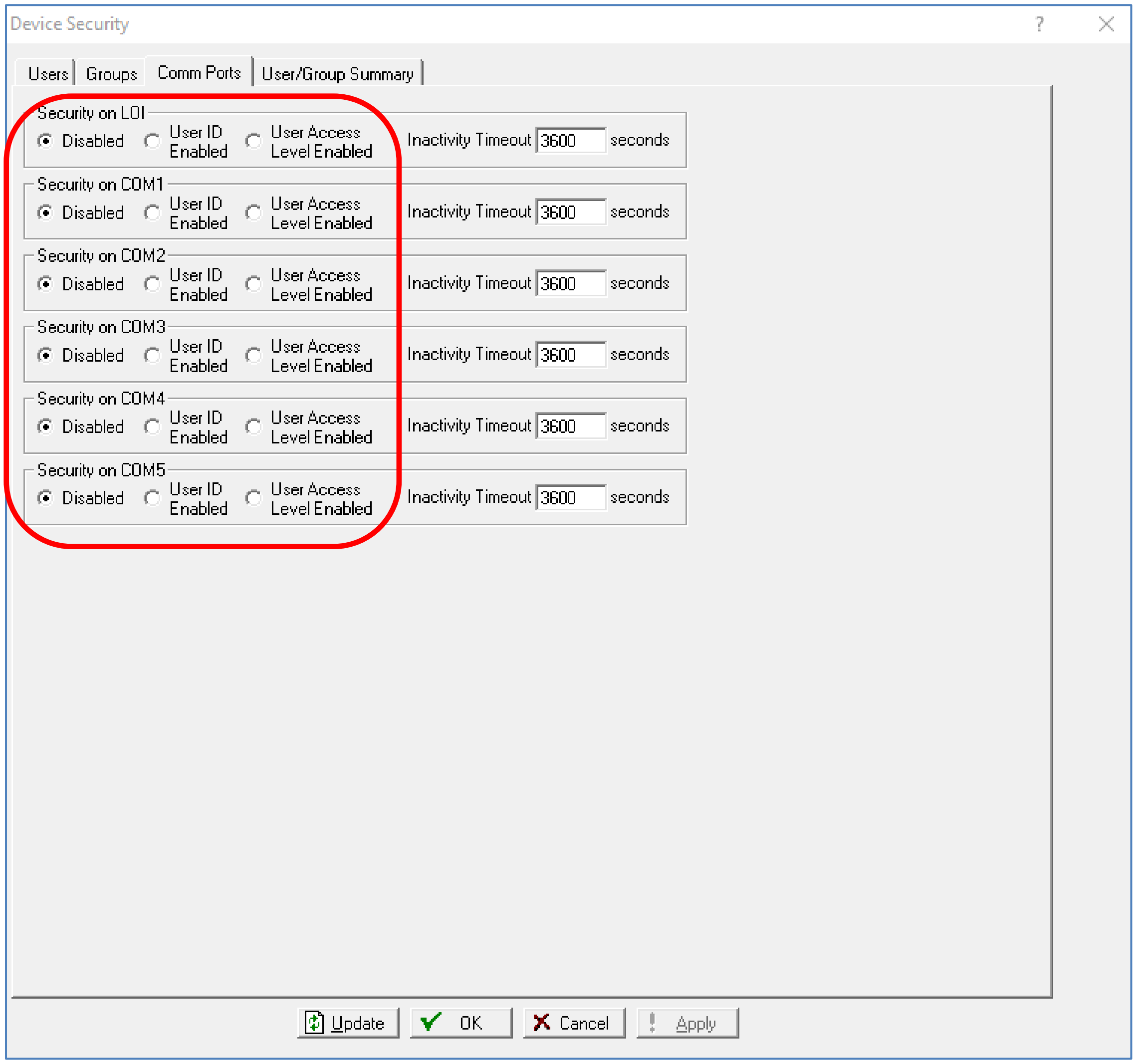
For maximum security, when defining PINs on the ROC Device Security screen, do not implement simplistic PIN combinations (such as 11111111, 00000000, or 12345678) especially for operator IDs with level 5/administrative access. Consult your organization’s IT department to create unique PINs most appropriate for your users.

4. Click **Apply** to save your changes.

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 (for ROC800)



Security on LOI: ● Disabled ○ User ID Enabled ○ User Access Level Enabled — Inactivity Timeout 3600 seconds

Security on COM1: ● Disabled ○ User ID Enabled ○ User Access Level Enabled — Inactivity Timeout 3600 seconds

Security on COM2: ● Disabled ○ User ID Enabled ○ User Access Level Enabled — Inactivity Timeout 3600 seconds

Security on COM3: ● Disabled ○ User ID Enabled ○ User Access Level Enabled — Inactivity Timeout 3600 seconds

Security on COM4: ● Disabled ○ User ID Enabled ○ User Access Level Enabled — Inactivity Timeout 3600 seconds

Security on COM5: ● Disabled ○ User ID Enabled ○ User Access Level Enabled — Inactivity Timeout 3600 seconds

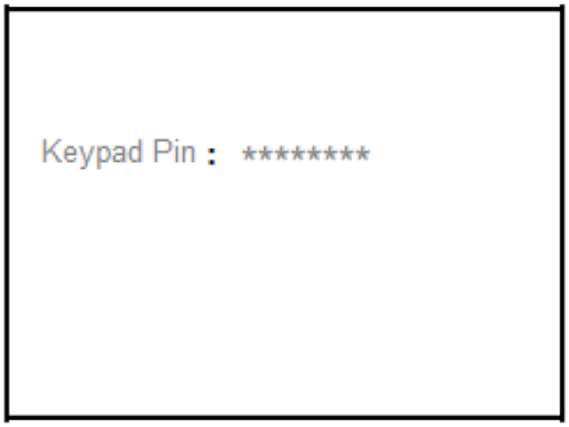
2.5 ROC Keypad Display Security

Important

For maximum security, when defining PINs on the ROC Device Security screen, do not implement simplistic PIN combinations (such as 11111111, 00000000, or 12345678) especially for operator IDs with level 5/administrative access. Consult your organization's IT department to create unique PINs most appropriate for your users.

If your organization uses the ROC Keypad Display, deploying enhanced security simplifies logging into the display. After activating the display, operators only need to enter their eight-digit PIN assigned to them on the Users tab of the ROC800 Device Security screen (see *Figure 2-8*):

Figure 2-10. Enhanced Security Keypad Display Login Screen



Keypad Pin : ********

Note

For further information on installing both the physical Keypad Display and its associated user program, refer to the *ROC Keypad Display Program User Manual* (D301273X012).

Chapter 3. Configuring Security for the FloBoss™ 107

⚠ **CAUTION**

The implementation of enhanced security on the FloBoss 107 is **not** backwards compatible. This is due to the **removal** of the point types shown in *Table 3.1*. **Before** applying this enhancement, **verify** that you are **not** using these point types when communicating to SCADA and/or HMI display drivers.

Table 3-1. Deleted FB107 Point Types

Point Type	Description of Data in Point Type
6	Legacy PID
7	Legacy AGA flow
10	Legacy AGA flow calculations
41	Run parameters
42	Extra runs

To configure the enhancements:

1. Install version **2.71** of ROCLINK 800.
2. Install the new firmware version **2.00**.

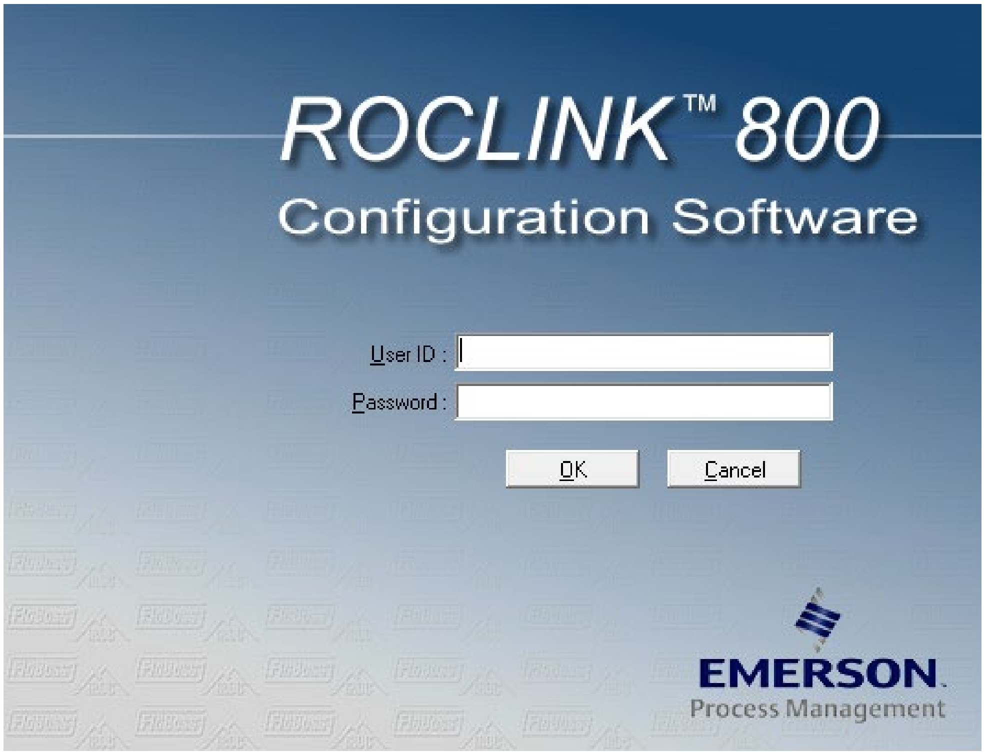
   Note
   Ensure that you are **not** using the point types shown in *Table 3-1* when communicating to SCADA and/or displays.

3. Install the FB107 Security user program (part number W68138X0012) and verify that it is running.

   Note
   Refer to *Section 9.4* in the *ROCLINK 800 Configuration Software User Manual (for FloBoss 107)* (D301249X012) for information on installing user programs.

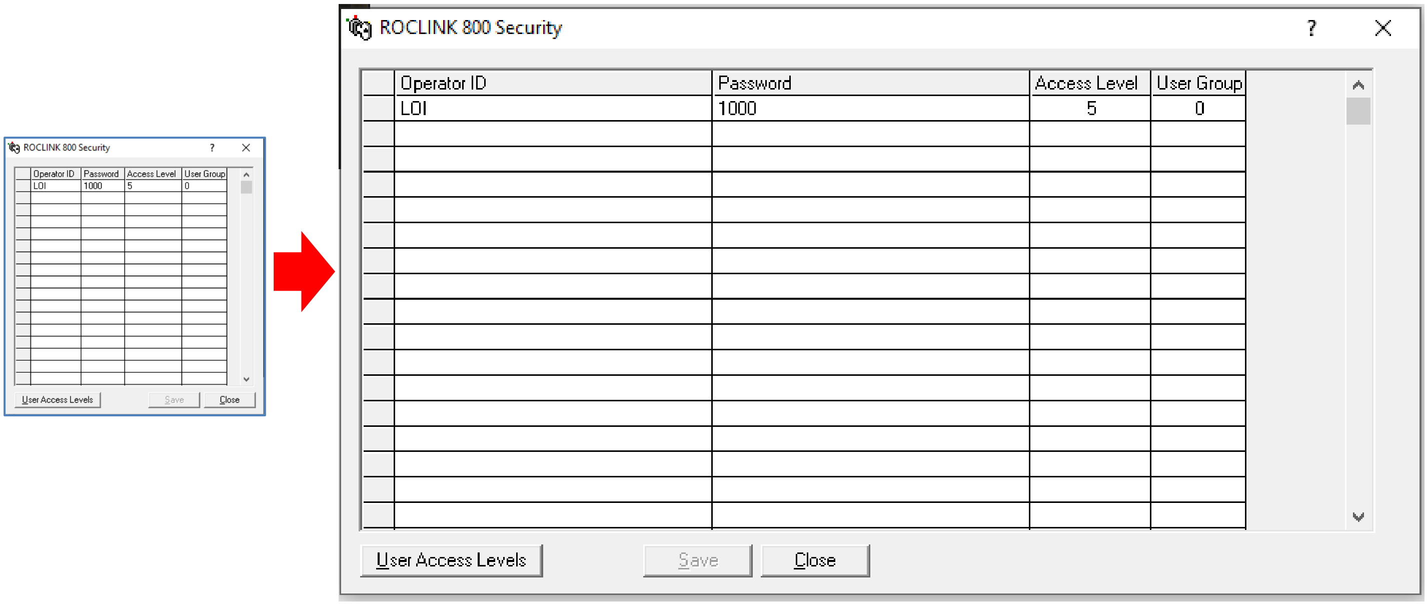
4. Opt into the enhanced security features.
5. After the system performs a warm restart, the revised ROCLINK 800 log-in screen displays (note the longer User ID and Password fields).

Figure 3-1. ROCLINK 800 Log-in Screen



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

Figure 3-2. Enhanced ROCLINK 800 Security Screen



Operator ID	Password	Access Level	User Group
LOI	1000	5	0

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. As shown in *Figure 3-2,* the ROCLINK 800 Security Table maintains both old and new IDs and passwords.

3.1 Upgrading Firmware

⚠ **CAUTION**

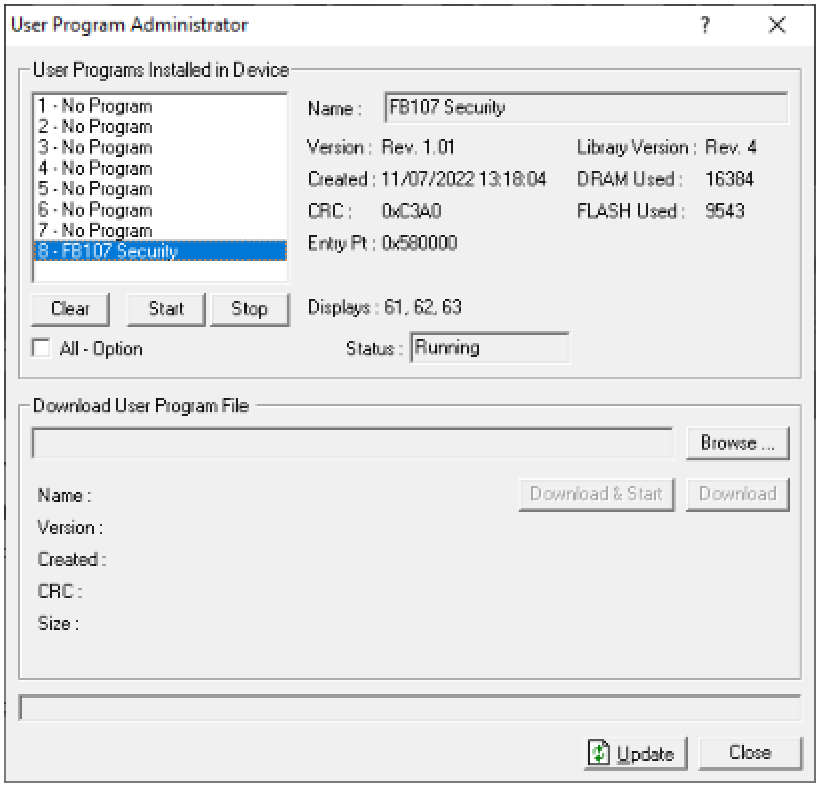
The implementation of enhanced security on the FloBoss 107 is **not** backwards compatible. This is due to the **removal** of the point types shown in *Table 3.1*. Before applying this enhancement, **verify** that you are **not either** using these point types when communicating to SCADA and/or HMI display drivers **or** using these point types in any FSTs.

Upgrade the firmware in the FloBoss 107 to v2.0 **before** you install the Security user program. This program installs **only** in the previously unavailable slot 8 and contains software checks to prevent you from opting-in if the Security program has not yet been installed. Additionally, once you install the program it cannot be stopped or removed. This ensures that the security features remain in place when subsequent upgrades or restarts occur.

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

1. Install the Security user program in slot 8 of the FloBoss 107. (For instructions on installing a user program, refer to *Section 9.4* in the *ROCLINK 800 Configuration Software User Manual (for FloBoss 107)*, part D301249X012.) Once the program is installed and running, the User Program Administrator screen should look like *Figure 3-3*:

Figure 3-3. User Program Administrator Screen (with Security User Program in Slot 8)



User Program Administrator

User Programs Installed in Device

- 1 - No Program
- 2 - No Program
- 3 - No Program
- 4 - No Program
- 5 - No Program
- 6 - No Program
- 7 - No Program
- 8 - FB107 Security

Name : FB107 Security

Version : Rev. 1.01
Library Version : Rev. 4
Created : 11/07/2022 13:18:04
DRAM Used : 16384
CRC : 0xC3A0
FLASH Used : 9543
Entry Pt : 0x580000

Displays : 61, 62, 63

□ All - Option

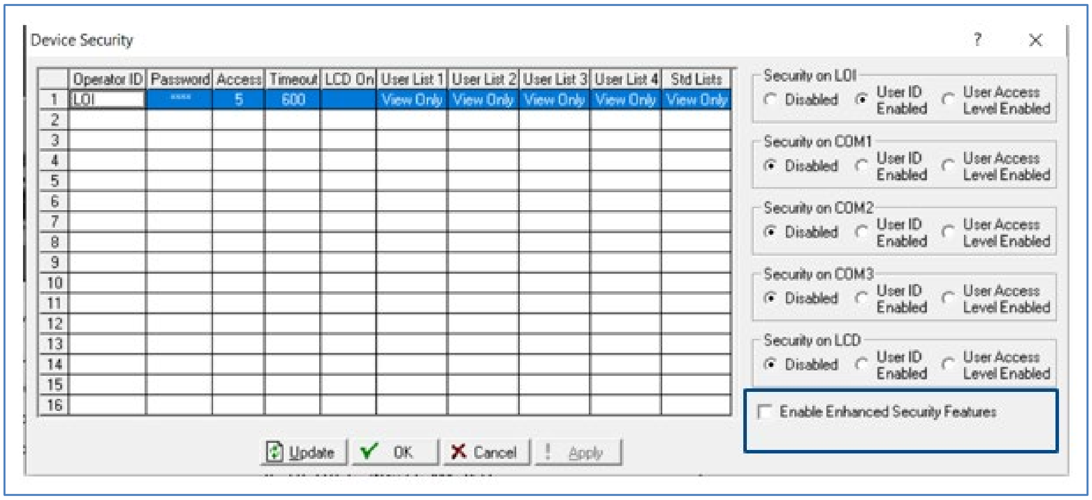
Status : Running

Download User Program File

Name :
Version :
Created :
CRC :
Size :

Access the FloBoss 107’s Device Security screen (**ROC** > **Security**):

Figure 3-4. Device Security Screen (FloBoss 107)



Device Security

	Operator ID	Password	Access	Timeout	LCD On	User List 1	User List 2	User List 3	User List 4	Std Lists
1	LOI	****	5	600		View Only	View Only	View Only	View Only	View Only
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										

Security on LOI: ○ Disabled ● User ID Enabled ○ User Access Level Enabled

Security on COM1: ● Disabled ○ User ID Enabled ○ User Access Level Enabled

Security on COM2: ● Disabled ○ User ID Enabled ○ User Access Level Enabled

Security on COM3: ● Disabled ○ User ID Enabled ○ User Access Level Enabled

Security on LCD: ● Disabled ○ User ID Enabled ○ User Access Level Enabled

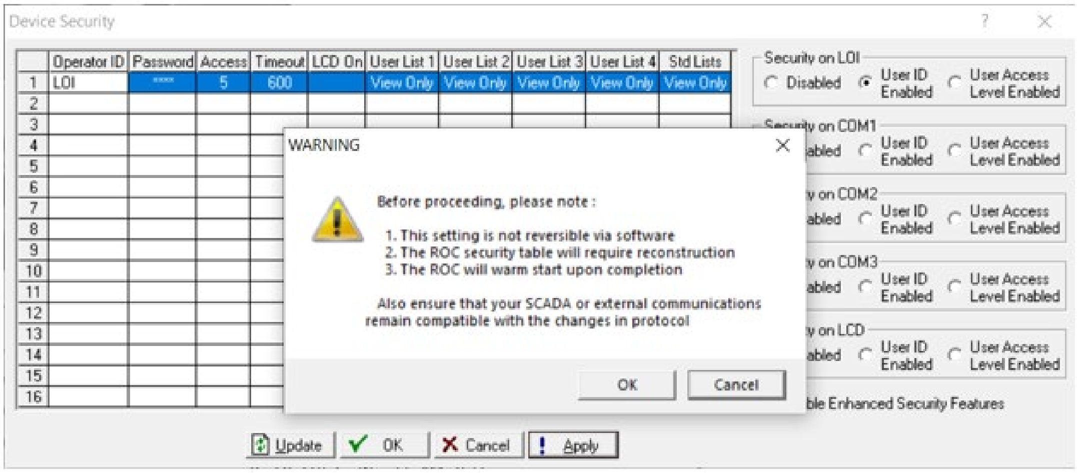
□ Enable Enhanced Security Features

Important

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

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

Figure 3-5. Warning Dialog



Device Security

	Operator ID	Password	Access	Timeout	LCD On	User List 1	User List 2	User List 3	User List 4	Std Lists
1	LOI	****	5	600		View Only	View Only	View Only	View Only	View Only
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										

Security on LOI: ○ Disabled ● User ID Enabled ○ User Access Level Enabled

WARNING

Before proceeding, please note :

1. This setting is not reversible via software
2. The ROC security table will require reconstruction
3. The ROC will warm start upon completion

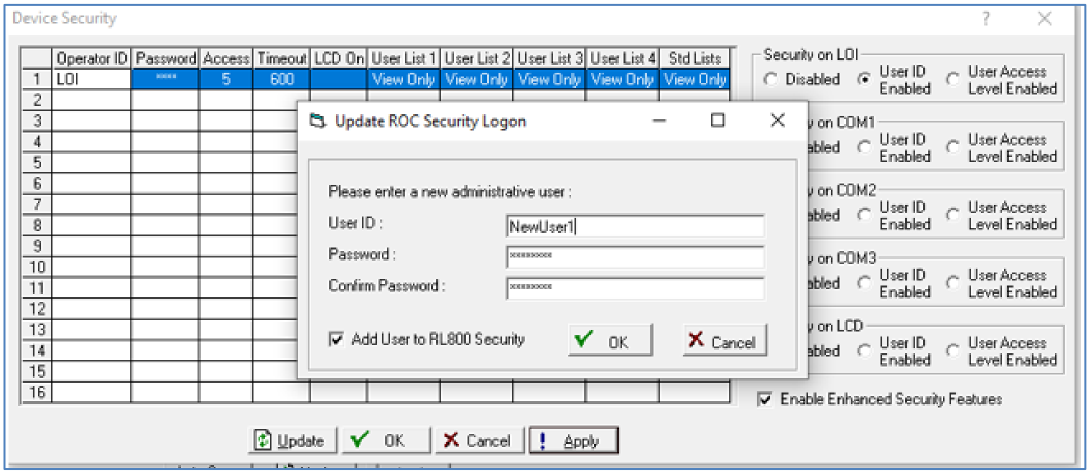
Also ensure that your SCADA or external communications remain compatible with the changes in protocol

Important

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

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

Figure 3-6. Update ROC Security Logon Dialog



Device Security

	Operator ID	Password	Access	Timeout	LCD On	User List 1	User List 2	User List 3	User List 4	Std Lists
1	LOI	****	5	600		View Only	View Only	View Only	View Only	View Only
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										

Security on LOI: ○ Disabled ● User ID Enabled ○ User Access Level Enabled

☑ Enable Enhanced Security Features

Update ROC Security Logon

Please enter a new administrative user :

User ID : NewUser1

Password : *********

Confirm Password : *********

☑ Add User to RL800 Security

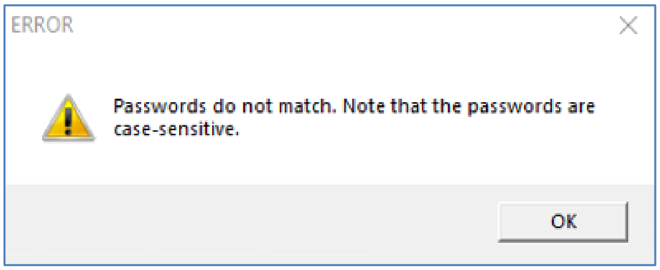
Important

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

5. Define a new User ID and password. This becomes 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:

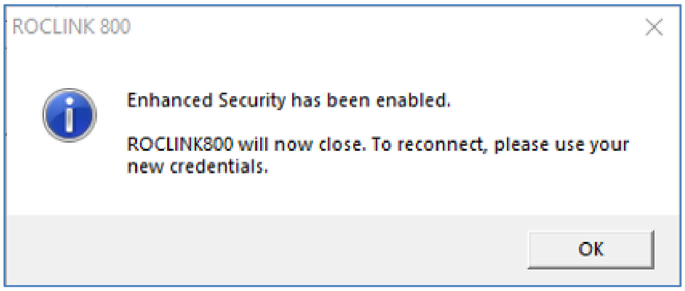


Passwords do not match. Note that the passwords are case-sensitive.

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

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

Figure 3-7. Verification Message



Enhanced Security has been enabled.

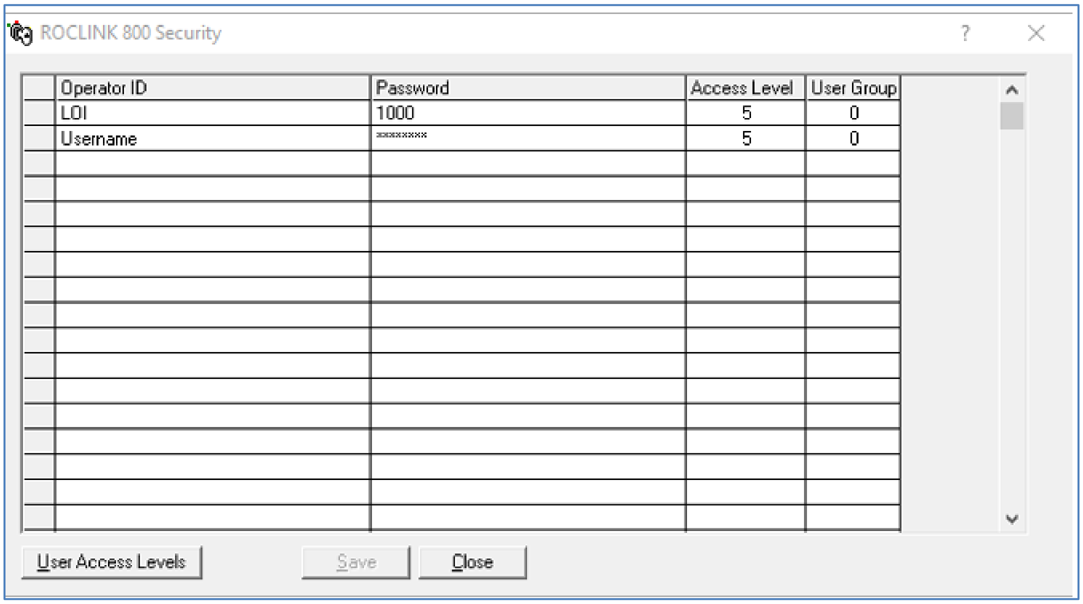
ROCLINK800 will now close. To reconnect, please use your new credentials.

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

3.2 After Opting In: ROCLINK 800 Security

1. Log into ROCLINK using the new **administrator** operator ID and password (defined in step 4 of *Section 3.1*).
2. Access the ROCLINK 800 Security screen (**Utilities** > **ROCLINK 800 Security**).

Figure 3-8. Enhanced ROCLINK 800 Security Screen



Operator ID	Password	Access Level	User Group
LOI	1000	5	0
Username	********	5	0

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.

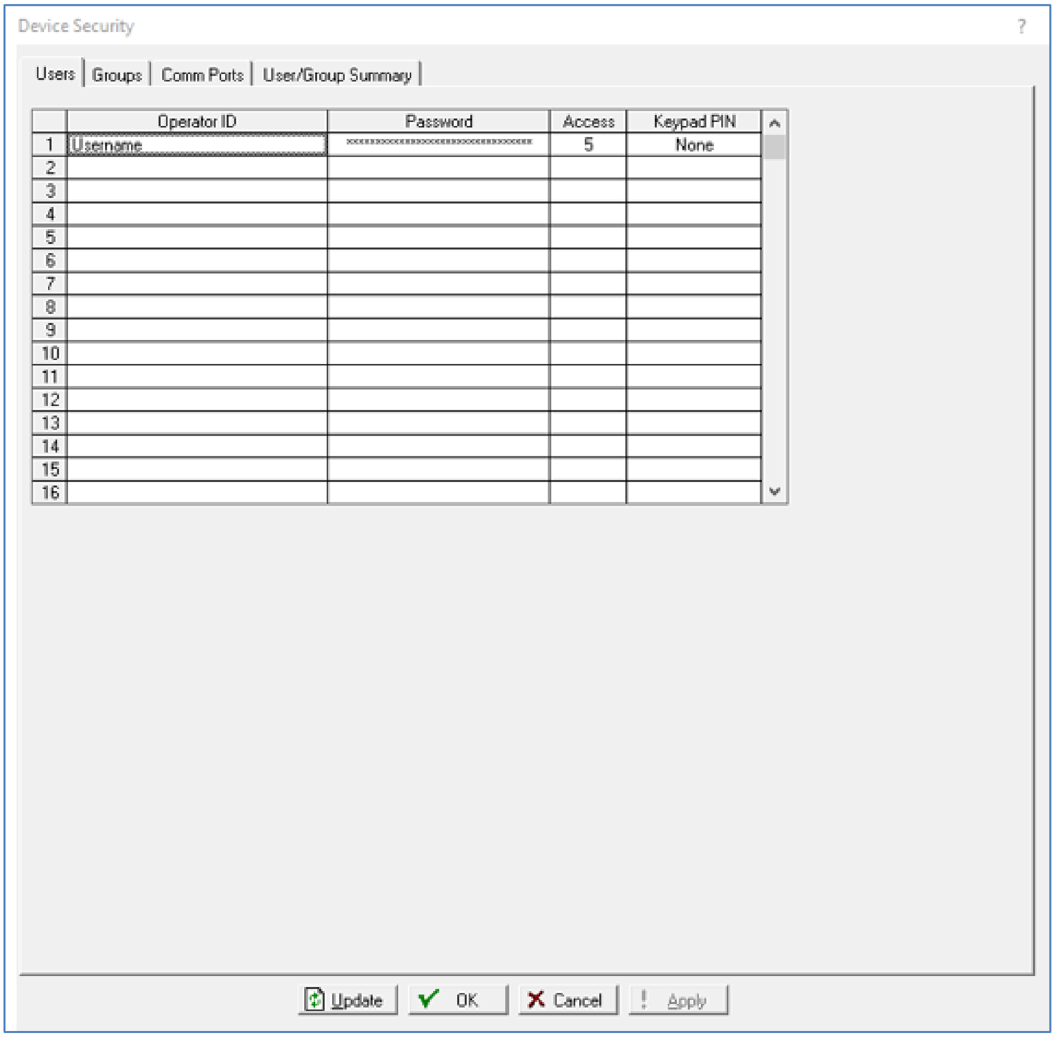
3.3 After Opting In: Device Security (IDs/Passwords)

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 3-9. Enhanced Device Security Screen (for FloBoss 107)



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

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).

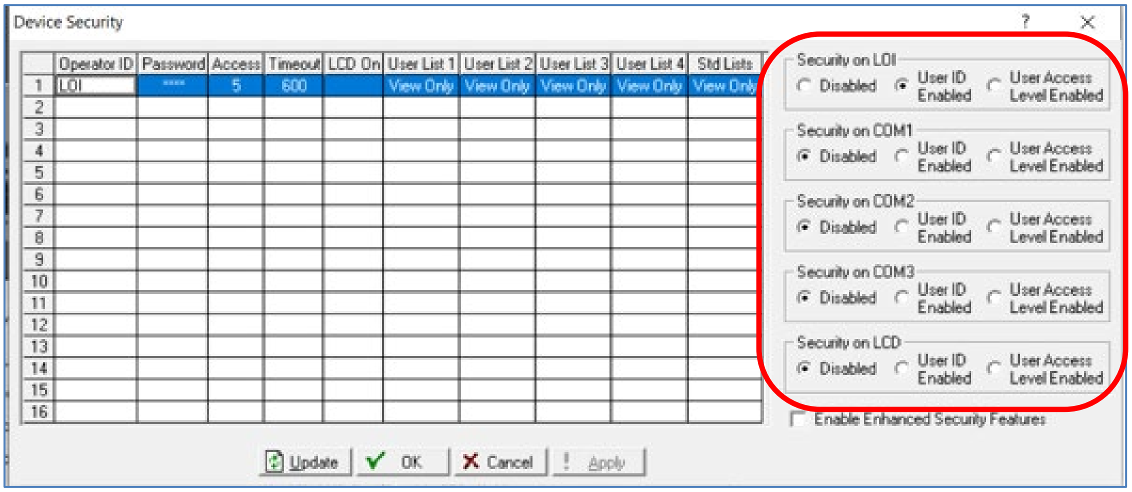
Note

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

3.4 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 3-10. Enhanced Device Security Screen (for FloBoss 107)



Device Security

	Operator ID	Password	Access	Timeout	LCD On	User List 1	User List 2	User List 3	User List 4	Std Lists
1	LOI	****	5	600		View Only	View Only	View Only	View Only	View Only
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										

Security on LOI: ○ Disabled ● User ID Enabled ○ User Access Level Enabled

Security on COM1: ● Disabled ○ User ID Enabled ○ User Access Level Enabled

Security on COM2: ● Disabled ○ User ID Enabled ○ User Access Level Enabled

Security on COM3: ● Disabled ○ User ID Enabled ○ User Access Level Enabled

Security on LCD: ● Disabled ○ User ID Enabled ○ User Access Level Enabled

□ Enable Enhanced Security Features

3.5 Managing Future Upgrades

Important

Before applying any subsequent firmware upgrades (later than v2.00) to a FloBoss 107 with enhanced security, **save the configuration to the device's flash memory**.

Before applying firmware upgrades (later than 2.00), first disable the port security. During a firmware upgrade, the FloBoss 107 clears all configured users and retains only the default (long) user. To retain all defined users, save the configuration to flash memory.

In case you forget to save the configuration **and** port security was **enabled**, you can still log onto the device with the new default user ID and password (Username/Password) you established when you initially applied the security enhancement.

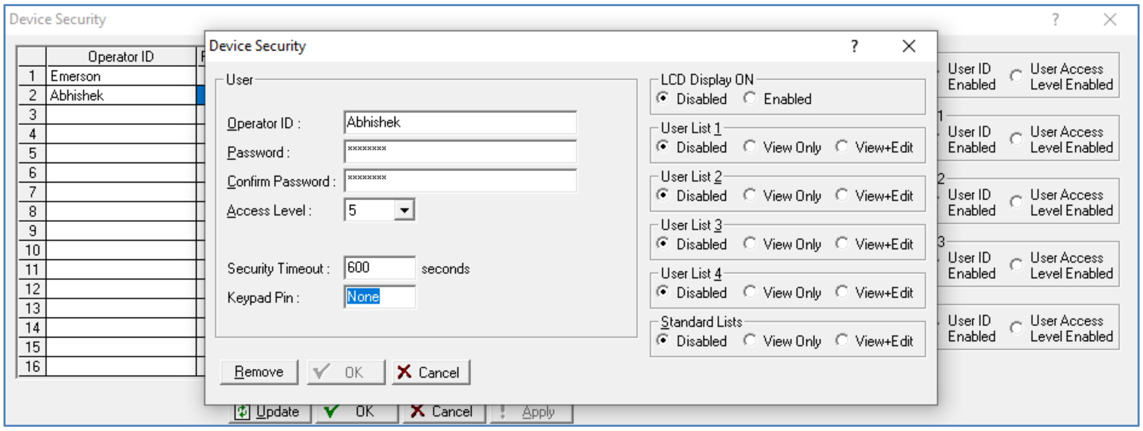
Note

Enhanced security requires that you immediately change the default password on first use.

3.6 LCD Touchpad Security

The previous security system allowed the 4-digit user password to function as the password for the LCD Touchpad. Implementing enhanced security resets all the old password, which means you must configure a Touchpad login PIN separately for each user.

Figure 3-11. Original LCD Keypad PIN



Device Security

	Operator ID
1	Emerson
2	Abhishek
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	

Device Security

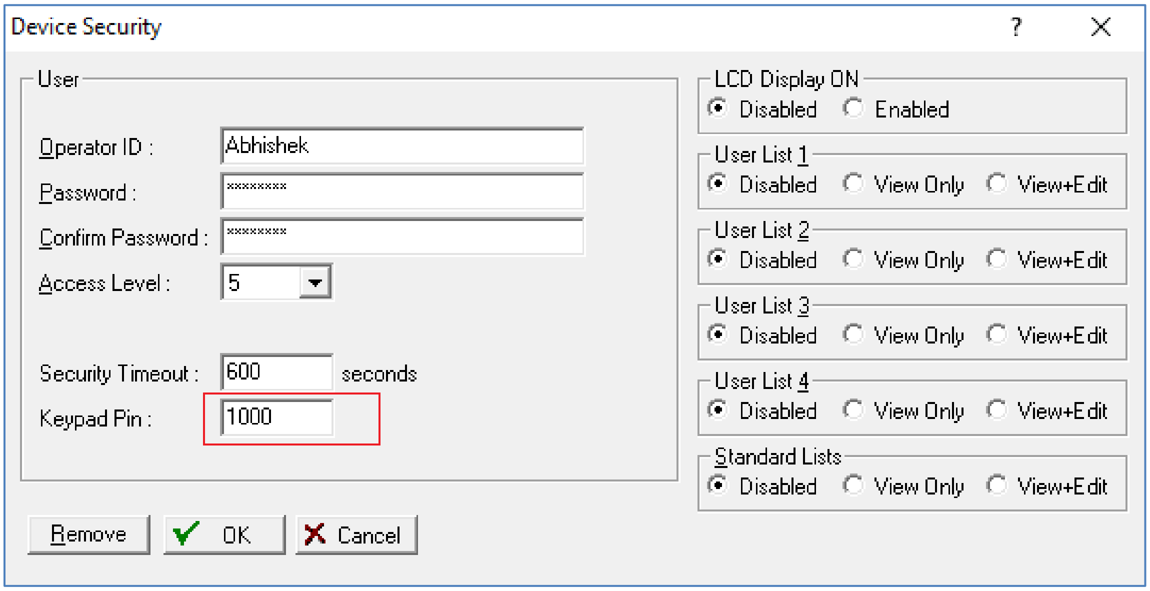
User

Operator ID : Abhishek
Password : ********
Confirm Password : ********
Access Level : 5
Security Timeout : 600 seconds
Keypad Pin : None

LCD Display ON: ● Disabled ○ Enabled
User List 1: ● Disabled ○ View Only ○ View+Edit
User List 2: ● Disabled ○ View Only ○ View+Edit
User List 3: ● Disabled ○ View Only ○ View+Edit
User List 4: ● Disabled ○ View Only ○ View+Edit
Standard Lists: ● Disabled ○ View Only ○ View+Edit

User ID Enabled ○ User Access Level Enabled
1
User ID Enabled ○ User Access Level Enabled
2
User ID Enabled ○ User Access Level Enabled
3
User ID Enabled ○ User Access Level Enabled
User ID Enabled ○ User Access Level Enabled
Remove
OK
Cancel
Update
OK
Cancel
Apply

Figure 3-12. Enhanced LCD Keypad PIN



Device Security

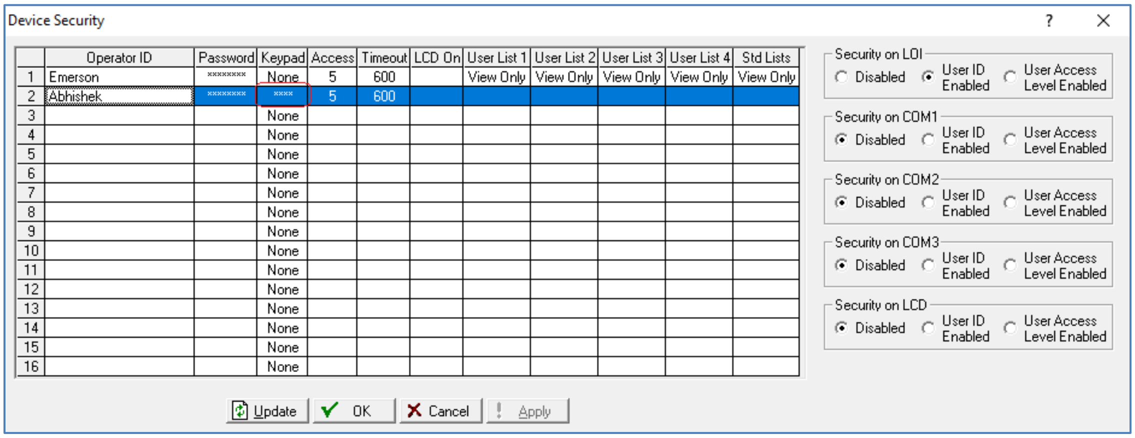
User

Operator ID : Abhishek
Password : ********
Confirm Password : ********
Access Level : 5
Security Timeout : 600 seconds
Keypad Pin : 1000

LCD Display ON: ● Disabled ○ Enabled
User List 1: ● Disabled ○ View Only ○ View+Edit
User List 2: ● Disabled ○ View Only ○ View+Edit
User List 3: ● Disabled ○ View Only ○ View+Edit
User List 4: ● Disabled ○ View Only ○ View+Edit
Standard Lists: ● Disabled ○ View Only ○ View+Edit

Once you set a value in the Keypad Pin field and click **OK**, the revised Device Security screen shows the configured user (here, **Abhishek**) with a keypad PIN. Non-configured IDs display **None,** and cannot use the Touchpad until a keypad PIN is set:

Figure 3-13. Enhanced LCD Keypad PIN



Device Security

	Operator ID	Password	Keypad	Access	Timeout	LCD On	User List 1	User List 2	User List 3	User List 4	Std Lists
1	Emerson	********	None	5	600		View Only	View Only	View Only	View Only	View Only
2	Abhishek	********	****	5	600						
3			None								
4			None								
5			None								
6			None								
7			None								
8			None								
9			None								
10			None								
11			None								
12			None								
13			None								
14			None								
15			None								
16			None								

Security on LOI: ○ Disabled ● User ID Enabled ○ User Access Level Enabled

Security on COM1: ● Disabled ○ User ID Enabled ○ User Access Level Enabled

Security on COM2: ● Disabled ○ User ID Enabled ○ User Access Level Enabled

Security on COM3: ● Disabled ○ User ID Enabled ○ User Access Level Enabled

Security on LCD: ● Disabled ○ User ID Enabled ○ User Access Level Enabled

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

North America and Latin America:
Emerson Automation Solutions
Energy and Transportation Solutions
6005 Rogerdale Road
Houston, TX 77072 U.S.A.
T +1 281 879 2699 | F +1 281 988 4445
Emerson.com/SCADAforEnergy

United Kingdom:
Emerson Automation Solutions
Meridian East
Meridian Business Park 7
Leicester LE19 1UX UK
T +44 0 870 240 1987
F +44 0 870 240 4389

Europe:
Emerson S.R.L
Regulatory Compliance Shared
Services Department
Company No. J12/88/2006
Emerson 4 Street
Parcul Industrial Tetarom 11
Romania
T +40 374 132 000

Middle East/Africa:
Emerson Automation Solutions
Energy and Transportation 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
Energy and Transportation Solutions
1 Pandan Crescent
Singapore 128461
T +65 6777 8211| F +65 6777 0947

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. Bristol Inc. (hereinafter “Energy and Transportation Solutions” or 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.