



*expert*meter™

High Performance Analyzer

PM180

Enhanced Security

Application Note

REVISION HISTORY

A1	June 2021	Initial release
----	-----------	-----------------

Table of Contents

1 GENERAL	4
1.1 User Login.....	4
1.2 Direct Password Authorization	4
1.3 Recording User Activities	4
2 MANAGING USER ACCOUNTS	6
2.1 Creating and Managing User Accounts	6
2.1.1 Creating a New User Account	6
2.1.2 Changing an Account	6
2.1.3 Deleting a User Account.....	7
2.2 Changing a User Password	7

1 General

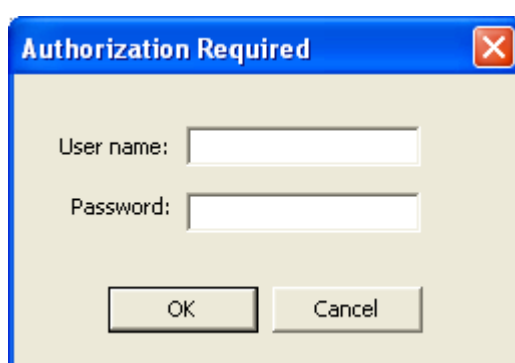
The enhanced security option allows creation and managing of up to 20 individual user accounts for remote device access using a combination of username and password with role-based access control.

In devices with enhanced security, all events associated with protected user activities, such as configuration change, data change, firmware update, time update, and optionally user login and user logout events, that are recorded in the device event log are accompanied by the user account identifier.

The enhanced security option is factory set and is available on devices with firmware V31.XX.44 and higher.

1.1 User Login

Remote access to the device with enhanced security requires user login authentication using a combination of username and password.



A username may be 1 to 15 characters long. The password must contain 8-12 characters with uppercase and lowercase letters, numbers and non-alphanumeric characters (e.g., +~!@#\$\$%&*).

User access permissions are assigned with a device security level from 1 (lowest) to 3 (highest) when a user account is created. See the PM180 Operation Manual for more information on security levels and associated user access rights. Optional recording of user login and logout events can be enabled/disabled in the user account.

A logged-in user is automatically logged out after a period of inactivity that is programmable from 0.5 to 5 minutes for each network port, and is fixed at 15 minutes for serial and USB ports.

Successive failed login attempts after three generate a tampering attempt record in the device event log and the port is blocked for 30 seconds.

1.2 Direct Password Authorization

Direct numeric passwords can still be used to authenticate users when accessing the device through the local display or M2M communication.

PAS login with a direct numeric password can be done using the reserved usernames "User21", "User22" and "User23" for Password1, Password2, and Password3 respectively. These usernames are also used in place of user account IDs to identify the user in the event log records.

NOTE: User login and logout events are not recorded in the case of direct password authorization.

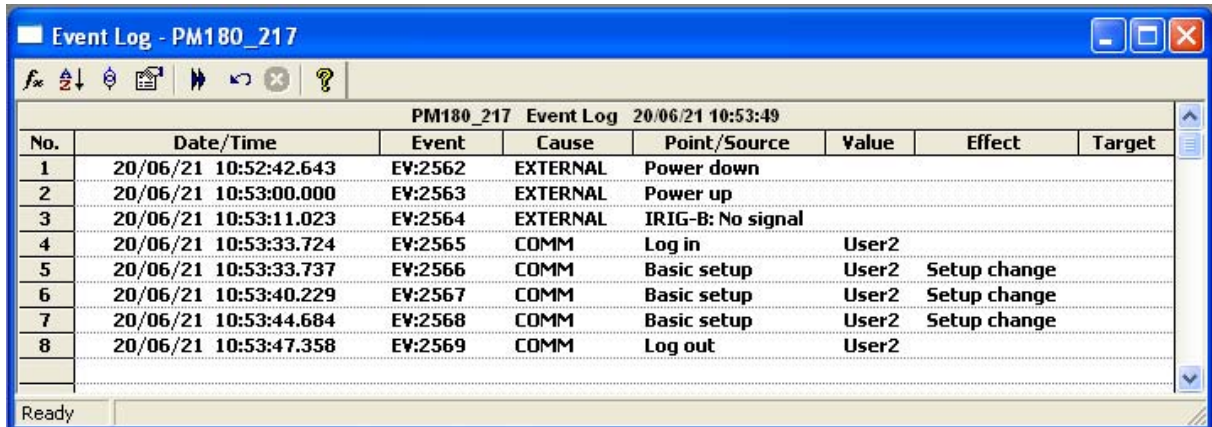
1.3 Recording User Activities

In devices with enhanced security, the device event log is used as the audit trail.

Protected user activities, such as configuration change, data change, firmware update and time update, recorded in the device event log are accompanied by the user account identifier

("User1"- "User23"). User login and user logout events are recorded if enabled in the user account.

The picture below shows how the user activities with enabled user login/logout recording are indicated in the PAS event log report.



Event Log - PM180_217

PM180_217 Event Log 20/06/21 10:53:49

No.	Date/Time	Event	Cause	Point/Source	Value	Effect	Target
1	20/06/21 10:52:42.643	EV:2562	EXTERNAL	Power down			
2	20/06/21 10:53:00.000	EV:2563	EXTERNAL	Power up			
3	20/06/21 10:53:11.023	EV:2564	EXTERNAL	IRIG-B: No signal			
4	20/06/21 10:53:33.724	EV:2565	COMM	Log in	User2		
5	20/06/21 10:53:33.737	EV:2566	COMM	Basic setup	User2	Setup change	
6	20/06/21 10:53:40.229	EV:2567	COMM	Basic setup	User2	Setup change	
7	20/06/21 10:53:44.684	EV:2568	COMM	Basic setup	User2	Setup change	
8	20/06/21 10:53:47.358	EV:2569	COMM	Log out	User2		

Ready

2 Managing User Accounts

2.1 Creating and Managing User Accounts

To add, change or delete a user account, select Administration->User Accounts->Manage Accounts in the Monitor menu, and then log in with high-permission credentials.

NOTES:

1. Only users with high-level permissions are allowed to create and manage user accounts.
2. Devices with enhanced security come with a default high-permission account with a username "User1" and password "Satec2021!" which you can use for authorization to create new accounts.

The picture below shows what the user account listing looks like.



PM180_217 - Manage Accounts

User ID: User1

User name: User1

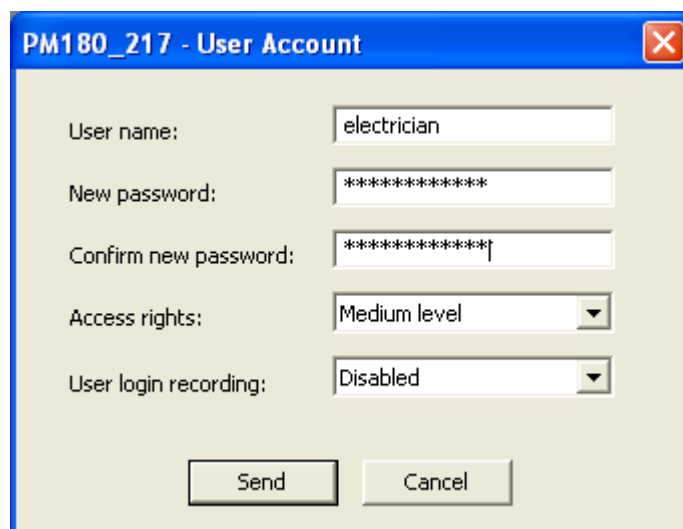
Access rights: High level

User login recording: Disabled

Add Change Delete Cancel

2.1.1 Creating a New User Account

To create a new user account, click Add, enter the username and password and select the appropriate access rights, and then send your settings to the device. Optionally, you can enable recording of user login/logout events in the device event log.



PM180_217 - User Account

User name: electrician

New password: *****

Confirm new password: *****

Access rights: Medium level

User login recording: Disabled

Send Cancel

2.1.2 Changing an Account

To change the user password or access rights, select the desired username in the "User name" box and click Change. Enter a new user password and select the appropriate access rights, and then send your settings to the device.

2.1.3 Deleting a User Account

To delete a user account, select the desired username in the "User name" box and click Delete.

NOTE: You must have at least one high level user on the list. You will not be allowed to delete the only high-permission account on the list.

2.2 Changing a User Password

The account owner is allowed to change his login password. A high-permission user can also change the password for any other user.

To change a user password, select Administration->User Accounts->Change Password in the Monitor menu.



The image shows a software dialog box titled "PM180_217 - Change Password". The dialog has a blue header bar with a close button (X) on the right. The main area is light beige and contains three text input fields. The first field is labeled "User name:" and contains the text "electrician". The second field is labeled "New password:" and contains seven asterisks "*****". The third field is labeled "Confirm new password:" and also contains seven asterisks "*****". At the bottom of the dialog, there are two buttons: "Send" and "Cancel".

Enter the username and new password, and then send your settings to the device.