/ PUK2.0 FACT SHEET

Increased security with PUK2.0

The digitalization of energy systems is a crucial element in the energy supply, which is increasingly decentralized and renewable. For settings, system monitoring and servicing, system operators need to be able to securely access their systems and components at all times with the aid of digital devices.

With the new PUK2.0 security feature, we are improving both the security and operation of the systems for users.

- Only users authorized by the owner have access to the systems.
- The use of the latest technologies and methods ensures reliable protection against unauthorized access.
- System operation is optimized.

From January 2022, PUK2.0 will gradually replace SMA's old PUK system.

How PUK2.0 works

PUK stands for Personal Unlocking Key and is used to reset passwords of a digital device if the user loses or forgets the relevant password (or PIN in the case of a cell phone).

PUK2.0 allows SMA Service to access SMA products in case of servicing when given the appropriate authorization by the user.

PUK2.0 replaces the access code that used to be provided for these situations at SMA.

Benefits of PUK2.0

Safer.

- Based on a state-of-the-art secure communication protocol.
- Operator has full control over access for servicing.
- Increases the security of new and existing systems.

Easier.

- Quickly and easily reset password.
- No need to contact SMA.

No extra charge.

- Fees are no longer charged for providing a PUK.

PUK2.0 has two security levels to accommodate specific security needs. At the first level, Basic Security, existing features such as Wi-Fi PSKs are used as device-specific secrets for resetting on the device. This level is enabled automatically on every device.

At the second level, High Security, device-specific product keys can be assigned as device secrets for each user account. This product key can then be used to unlock the device if you have forgotten your password. The device-specific secret will no longer be sufficient here to initiate a password reset.

Note: If your device is installed in a publicly accessible area, the High Security level should be used and the initial Wi-Fi password (Wi-Fi PSK) printed on the type label should be changed as well.

Basic Security

- **Existing device-specific secrets** are used to reset passwords (e.g., Wi-Fi PSK, RID, etc.).
- These secrets are part of the type label on a device.
- Basic Security is enabled automatically.

High Security

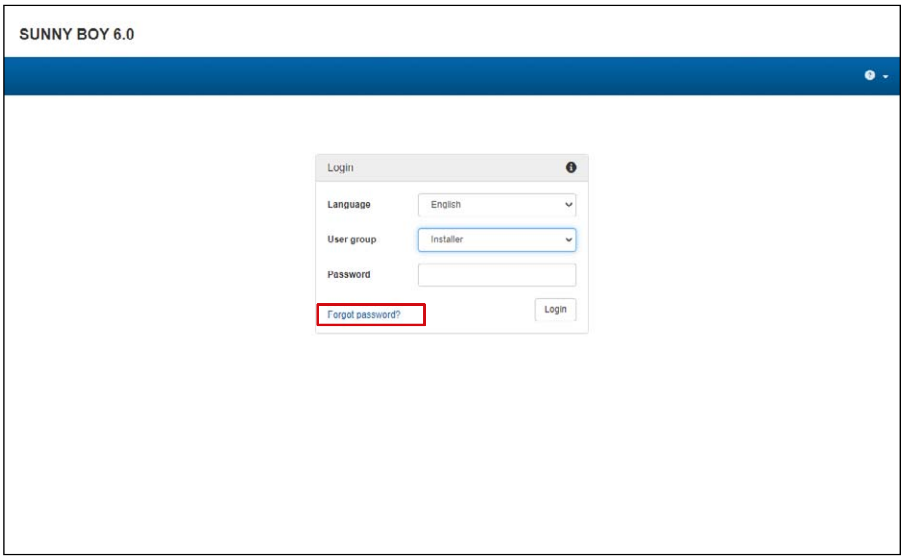
- A device-specific and role-specific **product key** can be assigned.
- This product key is known only to the user and not to any third parties.

You’ve forgotten your password. Well then?

You can use the “Forgot password” function to reset your role-specific password on the device. Depending on whether you are using Basic Security or High Security, you will need a device-specific secret (e.g., Wi-Fi PSK) or the product key that you assigned.

1. Call up the login screen on the device’s web UI.
2. Select user group.
3. Click “**Forgot password?**” on the login screen.
4. Enter the device secret (product key or device-specific secret).
5. Click on **“Login”**
6. Enter a new password for the device.

Note: Refer to the “Forgot password” page for the device to see which device-specific secret you can use to reset.



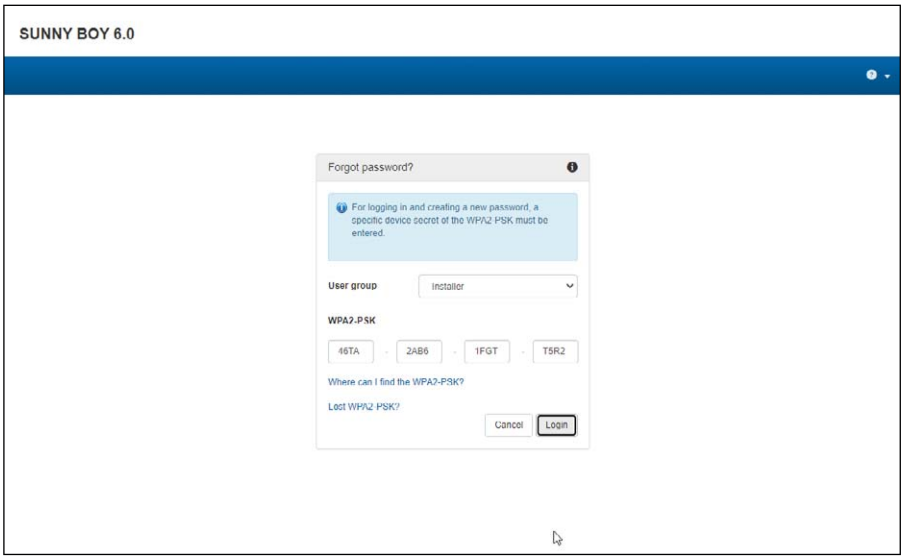
SUNNY BOY 6.0

Login

Language: English

User group: Installer

Password:



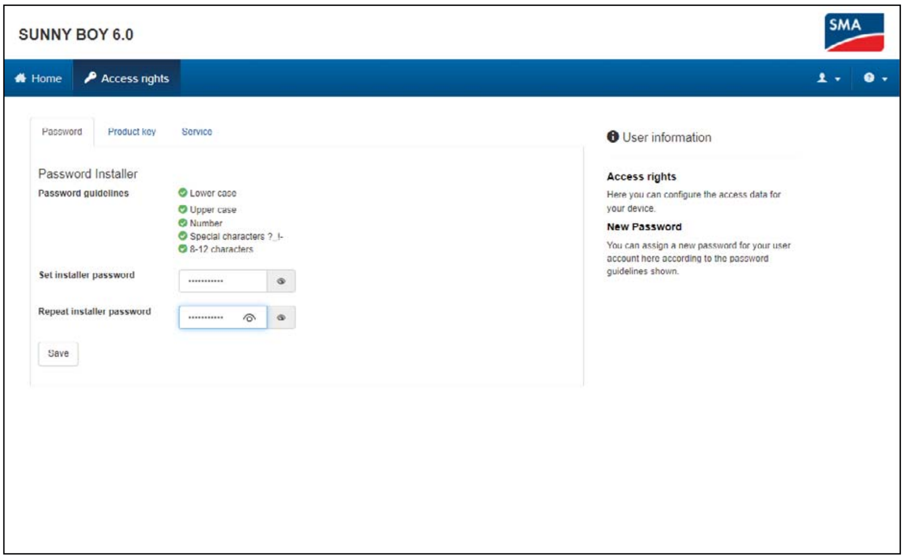
SUNNY BOY 6.0

Forgot password?

For logging in and creating a new password, a specific device secret of the WPA2 PSK must be entered.

User group: Installer

WPA2-PSK: 46TA - 2AB6 - 1FGT - T5R2



SUNNY BOY 6.0

Password Installer

Password guidelines
- ✓ Lower case
- ✓ Upper case
- ✓ Number
- ✓ Special characters ? _ !-
- ✓ 8-12 characters

Set installer password: ••••••••••••

Repeat installer password: ••••••••••••

User information

Access rights

Here you can configure the access data for your device.

New Password

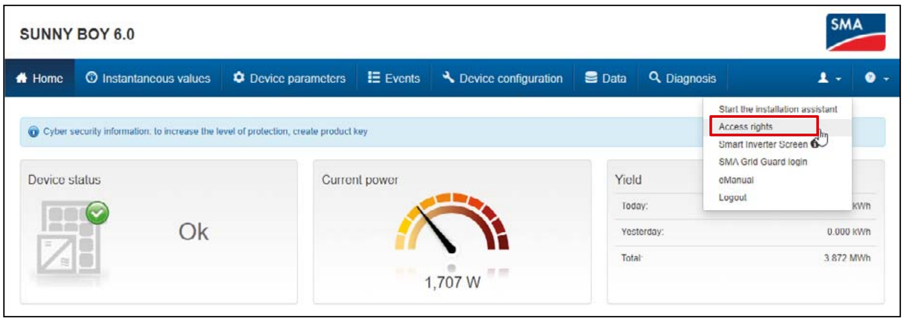
You can assign a new password for your user account here according to the password guidelines shown.

Assigning product keys

With a device-specific product key, you can unlock your device if you forget your password. This adds an extra layer of security on top of the Basic Security level.

1. Log in to the device through the web UI.
2. Under “User settings“ > “Access rights,“ select the “Product key“ tab.
3. Find the device-specific secret (in this example, the Wi-Fi PSK) on the device’s type label, enter it and click “Generating.”
4. The product key will be generated and displayed. Note the product key generated or copy it to your clipboard and save it somewhere where it is secure and easily retrievable (e.g., in a password safe).

Notice: If your device is installed in a publicly accessible area, you should make absolutely sure that you assign a device-specific product key.



SUNNY BOY 6.0

Cyber security information: to increase the level of protection, create product key

Device status: Ok

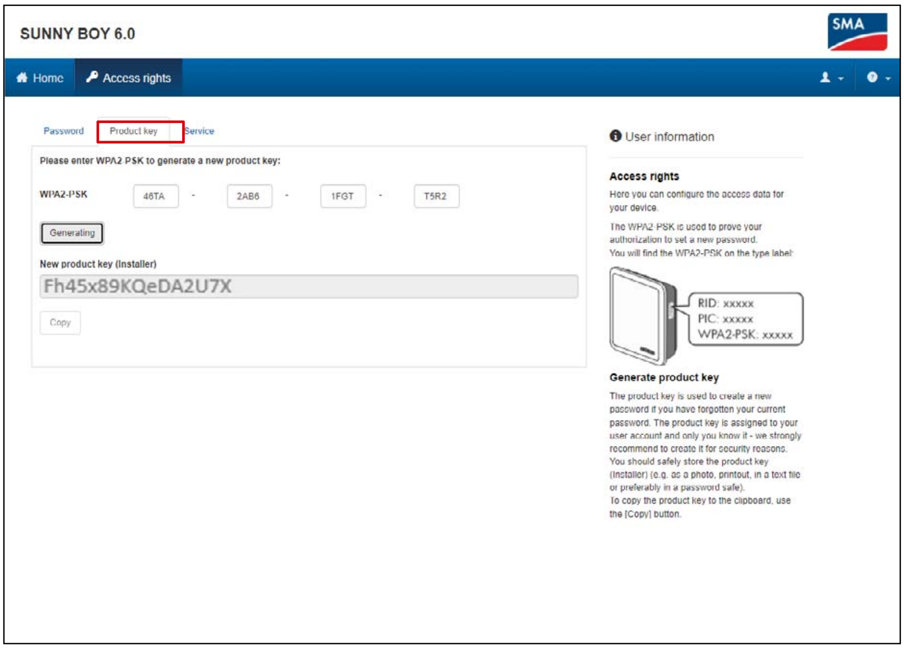
Current power: 1,707 W

Yield

Today: kWh

Yesterday: 0.000 kWh

Total: 3.872 MWh



SUNNY BOY 6.0

Please enter WPA2 PSK to generate a new product key:

WPA2-PSK 46TA - 2AB6 - 1FGT - T5R2

New product key (Installer)

Fh45x89KQeDA2U7X

User information

Access rights

Here you can configure the access data for your device.

The WPA2-PSK is used to prove your authorization to set a new password.
You will find the WPA2-PSK on the type label:

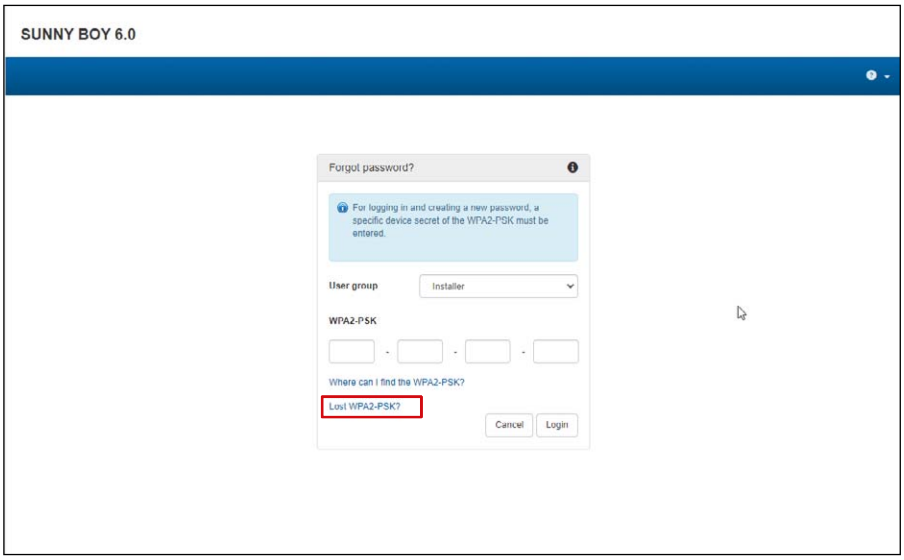
Generate product key

The product key is used to create a new password if you have forgotten your current password. The product key is assigned to your user account and only you know it - we strongly recommend to create it for security reasons. You should safely store the product key (Installer) (e.g. as a photo, printout, in a text file or preferably in a password safe).
To copy the product key to the clipboard, use the [Copy] button.

You’ve forgotten your password and product key. What to do?

If you do not know either your password or product key, there is another way of unlocking your device. This function requires physical access to the device, which means that it is possible only on-site.

1. Call up the login screen on the device’s web UI.
2. Select a user group.
3. Click “Forgot password?” on the login screen.
4. On the “Forgot password?” screen, click “Lost WPA2-PSK?”.
5. Select “Login.”
6. You will then need to provide proof that you are there in person within 20 minutes. Depending on the device used, you may be able to tap twice in quick succession on the enclosure lid (if it is fitted with touch-sensitive technology). Alternatively, you can disconnect the device’s AC utility grid connection for a period of between 10 s and 30 s (e.g., with the aid of the circuit breaker).
7. You can then assign a new password and a product key in the device’s web UI (see above).
8. Note the new product key or copy it to your clipboard and save it somewhere where it is secure and easily retrievable (e.g., in a password safe).



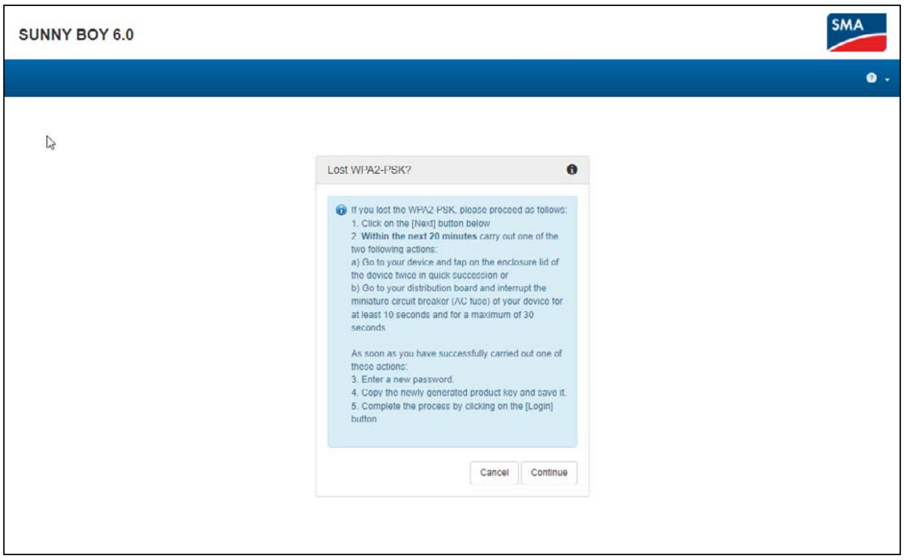
SUNNY BOY 6.0

Forgot password?

For logging in and creating a new password, a specific device secret of the WPA2-PSK must be entered.

User group: Installer

WPA2-PSK: □ - □ - □ - □



SUNNY BOY 6.0

Lost WPA2-PSK?

If you lost the WPA2-PSK, please proceed as follows:
1. Click on the [Next] button below
2. **Within the next 20 minutes** carry out one of the two following actions:
a) Go to your device and tap on the enclosure lid of the device twice in quick succession or
b) Go to your distribution board and interrupt the miniature circuit breaker (AC fuse) of your device for at least 10 seconds and for a maximum of 30 seconds.

As soon as you have successfully carried out one of these actions:
3. Enter a new password.
4. Copy the newly generated product key and save it.
5. Complete the process by clicking on the [Login] button

Authorizing access for servicing

PUK2.0 also allows SMA Service to access your device more easily and securely than before. Operators can choose whether they would like to allow SMA Service access temporarily, permanently or not at all. This choice will apply to access for servicing both remotely and on-site.

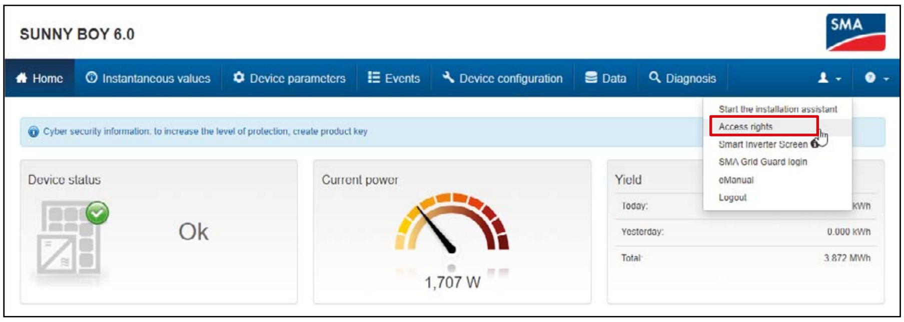
1. Log in to the device through the web UI.
2. Go to "User settings" > "Access rights" and open the **"Service"** tab.
3. Under **"Permission to access via SMA Service"** select the Permissions for Service access setting:

   - **"Yes, permanently"**

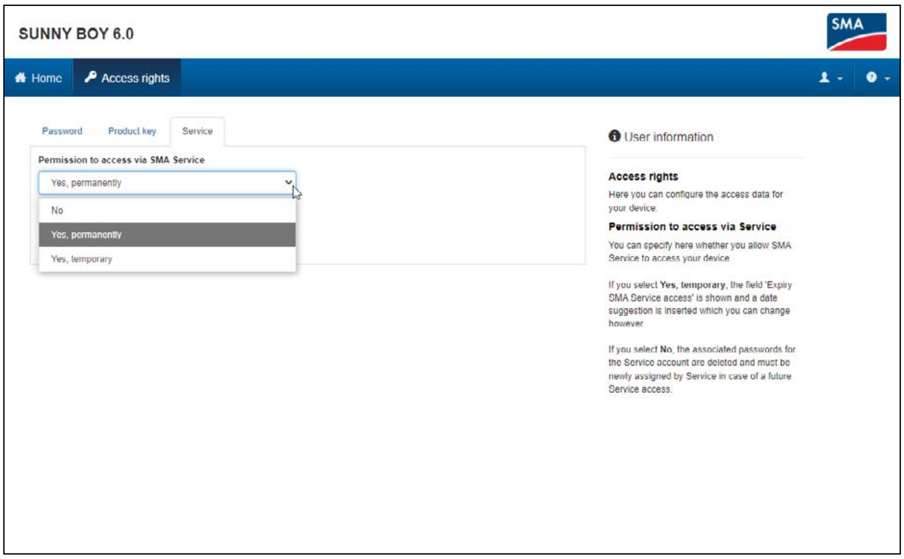
   - **"Yes, temporary"**

   - **"No"**

   With temporary authorization, a date two days in the future will be set by default. You can manually adjust this to a different expiration date if you like.
4. Select **"Save."**



Cyber security information: to increase the level of protection, create product key



Permission to access via SMA Service: Yes, permanently

User information

Access rights

Here you can configure the access data for your device.

Permission to access via Service

You can specify here whether you allow SMA Service to access your device.

If you select **Yes, temporary**, the field 'Expiry SMA Service access' is shown and a date suggestion is inserted which you can change however.

If you select **No**, the associated passwords for the Service account are deleted and must be newly assigned by Service in case of a future Service access.

Where can I find more information about PUK2.0?

You can find more information about security with PUK2.0 in the following sections of your device's operating manual:

- Product Overview: SMA PUK2.0
- Generating or Changing a Product Key
- Activating or Deactivating Service Access
- Troubleshooting: Password Forgotten for Products with Firmware Version ≥ 4.00.00.R
- Product Key Lost

This Tech Tip will show you how to assign PUK2.0 to your device.

More information and documents on SMA products can be found in the download area of the SMA website.

SMA

ENERGY
THAT
CHANGES

SMA-Solar.com

INFOPAPERPUK2-AEN2202 Subject to change. SMA assumes no liability for mistakes or printing errors.