Più sicurezza con PUK2.0

La digitalizzazione dei sistemi energetici è un fattore essenziale per un approvvigionamento di energia che è sempre più decentralizzato e rinnovabile. Per configurare e monitorare l'impianto e consentire l'accesso del servizio assistenza, i proprietari degli impianti devono essere in grado di accedere in sicurezza ai loro sistemi e componenti in qualsiasi momento, utilizzando dispositivi digitali.

Con la nuova procedura PUK2.0 miglioriamo ulteriormente la sicurezza e la gestione dei sistemi per gli utilizzatori.

- Solo gli utenti autorizzati dal proprietario hanno accesso ai sistemi.
- L'impiego delle più recenti tecnologie e procedure garantisce una protezione affidabile da accessi non autorizzati.
- La gestione dei sistemi viene ottimizzata.

Da gennaio 2022 PUK2.0 sostituisce gradualmente l'attuale procedura SMA PUK.

Come funziona PUK2.0

PUK significa Personal Unlocking Key ed è utilizzato per resettare le password di un dispositivo digitale nel caso in cui le password (PIN nel caso dei cellulari) siano state dimenticate o smarrite dall'utente.

PUK2.0 consente al servizio di assistenza tecnica SMA di accedere ai prodotti SMA per effettuare interventi, una volta ricevuta l'autorizzazione dall'utente.

PUK2.0 sostituisce il codice di accesso che prima doveva essere richiesto espressamente a SMA.

Vantaggi del PUK2.0

Più sicurezza.

- Basato su un protocollo di comunicazione sicuro e all'avanguardia.
- Il proprietario ha pieno controllo sull'accesso del servizio di assistenza.
- Aumenta la sicurezza sia degli impianti nuovi che di quelli esistenti.

Più semplicità.

- Ripristino della password semplice e rapido
- Non è necessario contattare SMA.

Gratuito.

- Ottieni il PUK senza costi aggiuntivi.

Per soddisfare le singole esigenze individuali, PUK2.0 offre due livelli di sicurezza. Con il primo livello, quello della "Sicurezza Base", per il ripristino vengono utilizzate come dato segreto unico del dispositivo informazioni memorizzate sul dispositivo stesso, come ad esempio la Wi-Fi PSKs. Questo livello è attivo automaticamente su tutti i dispositivi.

Con il secondo livello, quello della "Sicurezza Elevata", si può assegnare una chiave prodotto specifica a ogni account utente come dato segreto unico del dispositivo. Questa chiave prodotto serve per sbloccare il dispositivo nel caso in cui si dimentichi la password. Il dato segreto unico del dispositivo non è più sufficiente per avviare il ripristino della password.

Nota: se il dispositivo è montato in una zona accessibile al pubblico, è consigliabile usare il livello Sicurezza Elevata e modificare la password Wi-Fi iniziale stampata sulla targhetta identificativa ("Wi-Fi PSK").

Sicurezza Base

- Per ripristinare le password vengono usati **dati segreti unici del dispositivo** (ad es. Wi-Fi PSK, RID, etc.).
- Questi dati segreti sono riportati sulla targhetta identificativa del dispositivo.
- La Sicurezza Base è attiva automaticamente.

Sicurezza Elevata

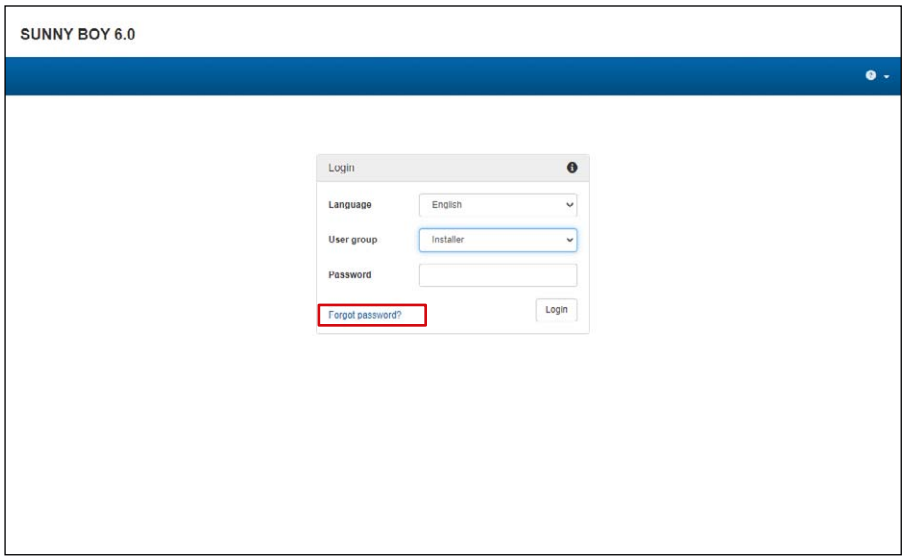
- È possibile assegnare una **chiave prodotto specifica**, unica per il dispositivo e il ruolo.
- La chiave prodotto è nota esclusivamente all'utente e a nessun altro.

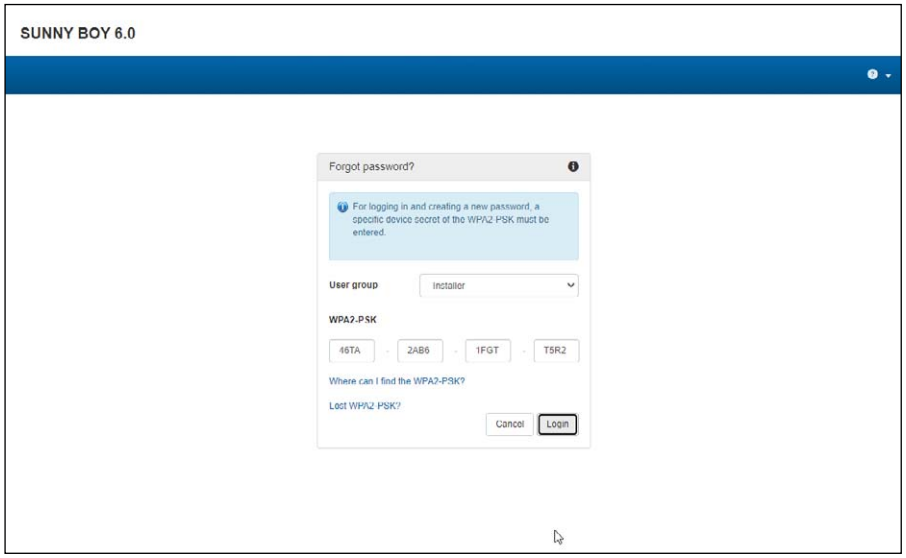
Password dimenticata. E ora?

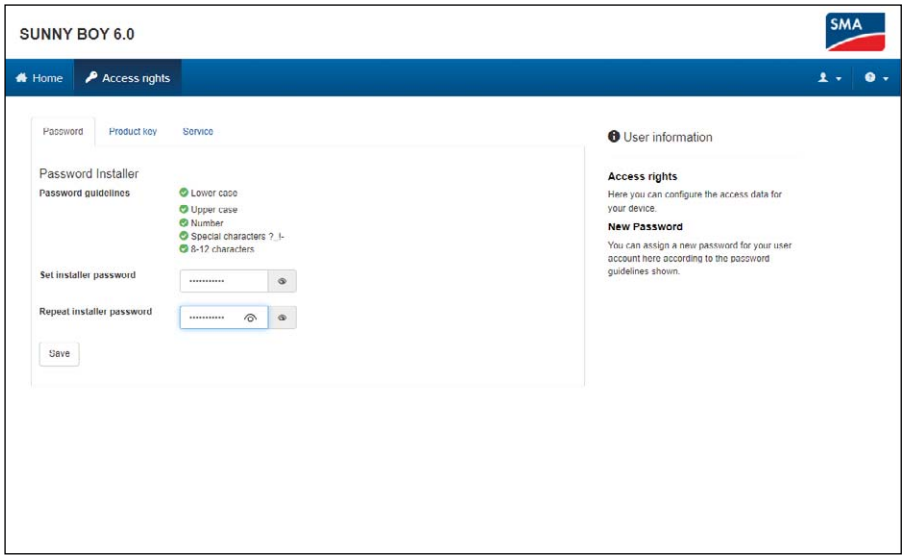
Con la funzione "Forgot password" puoi ripristinare sul dispositivo la password specifica per un certo ruolo. In funzione del livello di sicurezza utilizzato, Base o Elevato, ti serve un dato segreto unico del dispositivo (ad es. Wi-Fi PSK)) o una chiave prodotto da te assegnata.

1. Apri la pagina di login nella Web-UI del dispositivo.
2. Seleziona il gruppo utenti.
3. Nella pagina di login seleziona "Forgot password?".
4. Inserisci il dato segreto del dispositivo (chiave prodotto o dato segreto unico del dispositivo).
5. Fai clic su **"Login"**
6. Assegna una nuova password al dispositivo.

Nota: nella pagina "Forgot password" del dispositivo puoi vedere quale dato segreto unico del dispositivo utilizzare per il ripristino.





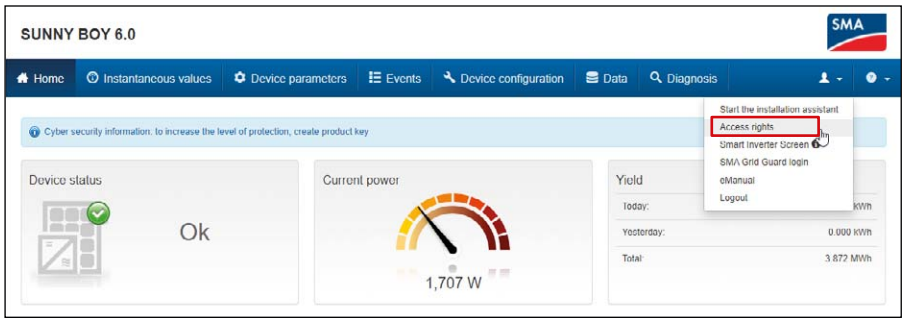


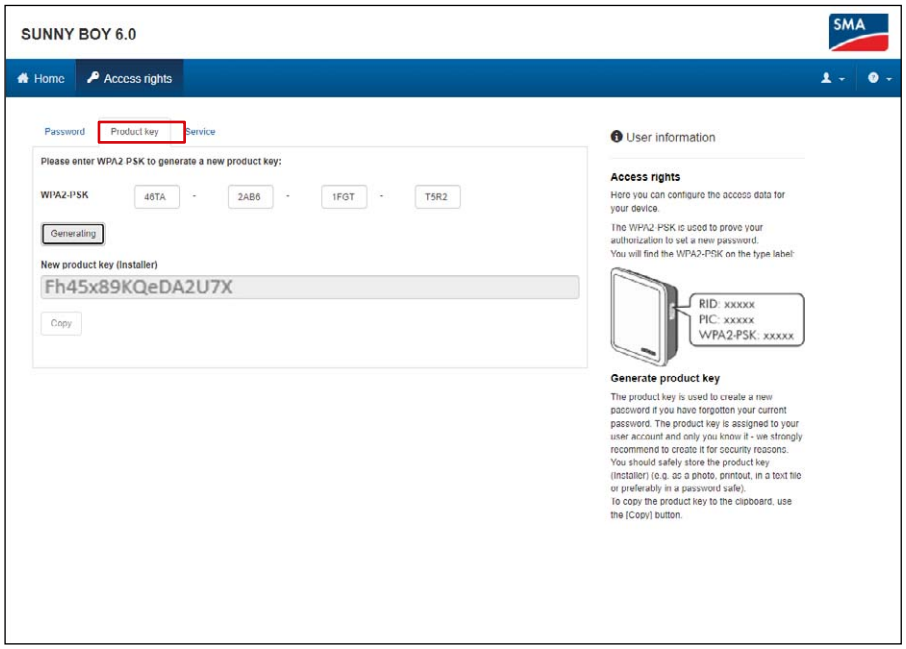
Assegnazione di chiavi prodotto

Con la chiave prodotto unica puoi sbloccare il vostro dispositivo, se hai dimenticato la password. In questo modo aumenterai ulteriormente la sicurezza rispetto al livello di "Sicurezza Base".

1. Effettua l'accesso al dispositivo tramite Web-UI.
2. Nella pagina "User settings > Access rights" seleziona la scheda "Product key".
3. Trovi il dato segreto unico del dispositivo (nell'esempio viene usata la Wi-Fi PSK) sulla targhetta identificativa, inseriscilo e seleziona "Generating".
4. Verrà generata e visualizzata la chiave prodotto. Annota la chiave prodotto generata o copiala negli appunti e salvala in modo che sia sicura e facilmente recuperabile (ad es. in una cassaforte di password).

Avviso: nel caso in cui il tuo dispositivo sia montato in una zona accessibile al pubblico, è necessario è necessario assegnargli una chiave prodotto unica!

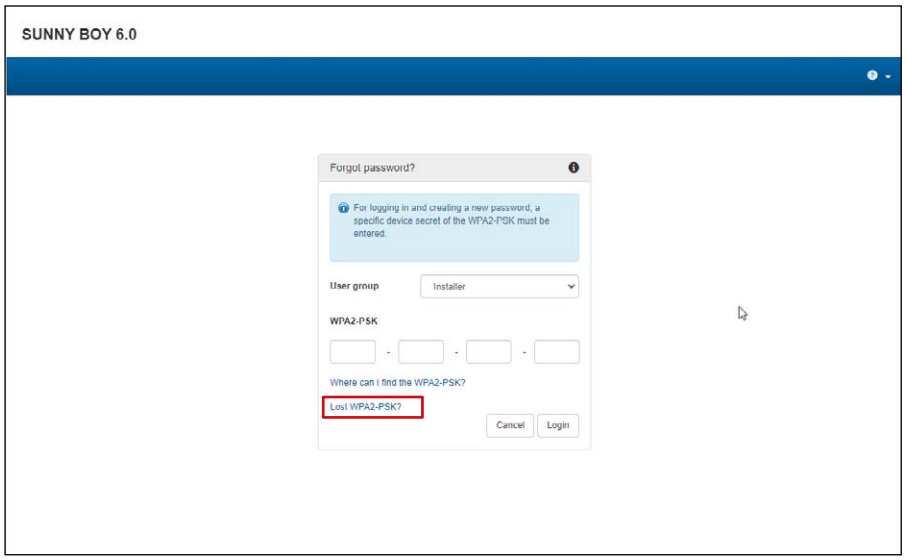


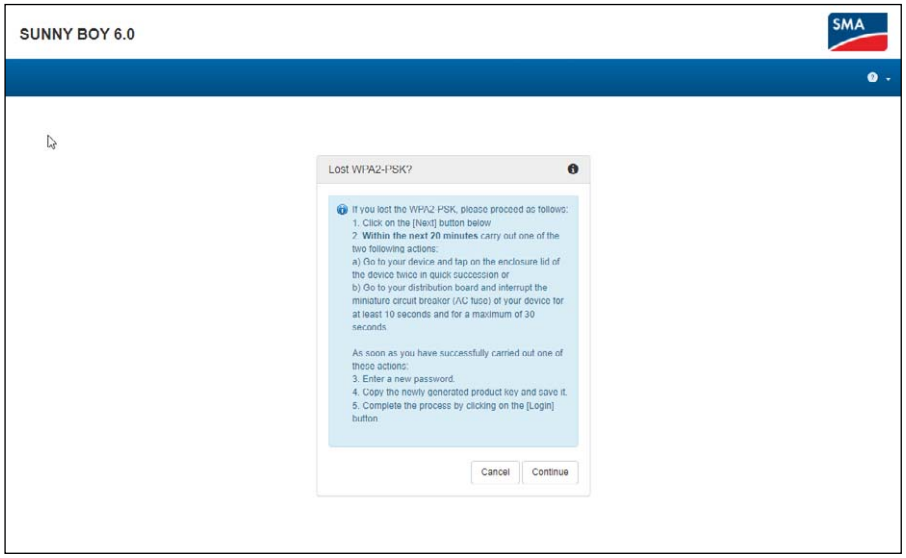


Password e chiave prodotto dimenticate. Cosa fare?

Se non conosci né la password né la chiave prodotto, hai a disposizione un altro metodo per sbloccare il dispositivo. È necessario accedere fisicamente al dispositivo quindi è disponibile solo quando si è presenti sul posto.

1. Apri la pagina di login nella Web-UI del dispositivo.
2. Seleziona il gruppo utenti.
3. Nella pagina di login seleziona "Forgot password?".
4. Nella pagina "Forgot Password" seleziona "Lost WPA2-PSK?".
5. Seleziona "Login".
6. Ora devi fornire una prova di presenza entro 20 minuti.
   In funzione del dispositivo utilizzato, sarà sufficiente toccare velocemente due volte l'involucro del dispositivo (se è presente un sensore tattile). In alternativa puoi scollegare il dispositivo lato CA, dalla rete elettrica, per un tempo compreso fra 10s e 30s (ad es. usando l'interruttore automatico).
7. In seguito, nella Web UI del dispositivo puoi assegnare una nuova password e una chiave prodotto (v. sopra).
8. Annota la nuova chiave prodotto o copiala negli appunti e salvala in modo che sia sicura e facilmente recuperabile (ad es. in una cassaforte di password).





Autorizzare l'accesso del servizio di assistenza

PUK2.0 regola in modo più semplice e sicuro anche l'accesso da parte del servizio di assistenza tecnica SMA. I proprietari degli impianti possono scegliere se desiderano un accesso temporaneo, permanente oppure nessun accesso da parte del servizio di assistenza tecnica SMA. Questa impostazione regola l'accesso del servizio di assistenza sia da remoto che in loco.

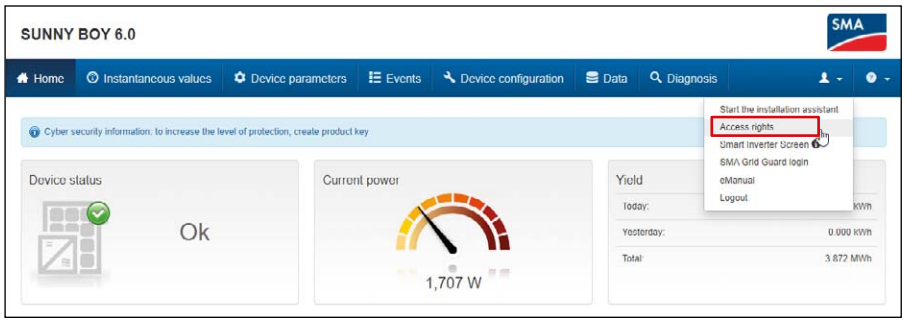
1. Effettua l'accesso al dispositivo tramite Web-UI.
2. Seleziona sul sito "Device configuration > Access rights" e apri la scheda "**Service**".
3. Seleziona nel campo "Permission to access via SMA Service" l'impostazione per l'accesso del servizio di assistenza desiderato:

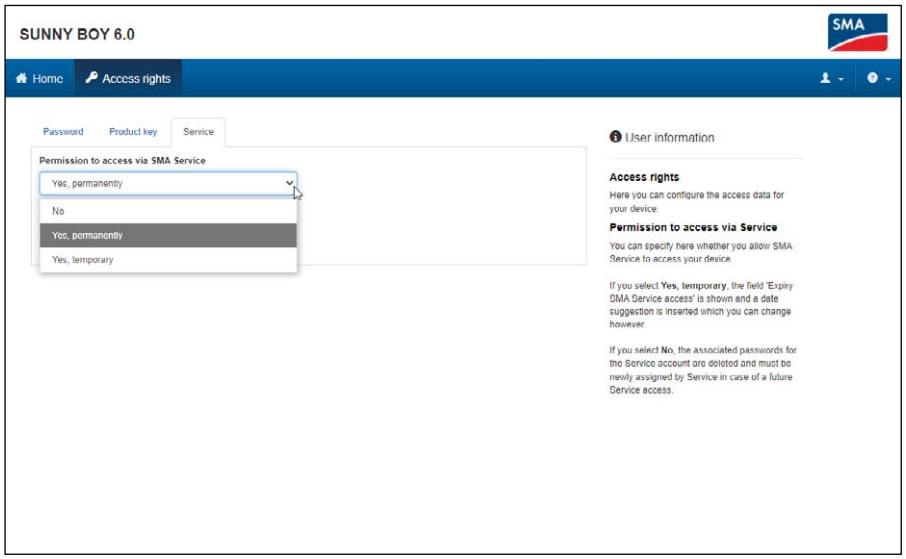
   - "**Yes, permanently**"

   - "**Yes, temporary**"

   - "**No**"

   Con l'autorizzazione temporanea viene inserita automaticamente come scadenza la data di due giorni dopo. Puoi impostare manualmente anche una data diversa.
4. Fai clic su [**Save**].





Dove si trovano altre informazioni su PUK2.0?

Ulteriori informazioni sulla sicurezza con PUK2.0 sono disponibili nei seguenti capitoli del manuale d'uso:

- Panoramica del prodotto: SMA PUK2.0
- Creare o modificare una chiave prodotto
- Attivare o disattivare l'accesso del servizio di assistenza
- Ricerca degli errori: password dimenticata per prodotti con versione firmware ≥ 4.00.00.R
- Chiave prodotto persa

In questo Tech Tip è spiegato come assegnare il PUK2.0 al proprio dispositivo.

Sull'area download del sito web di SMA troverai ulteriori informazioni e documenti sui prodotti SMA.

ENERGY
THAT
CHANGES

SMA-Italia.com

INFOPAPERPRUK2.AIT2208 Con riserva di modifiche. SMA declina ogni responsabilità per eventuali errori di stampa o refusi.