Mais segurança com PUK2.0

A digitalização dos sistemas de energia é um elemento essencial para o fornecimento energético cada vez mais descentralizado e regenerativo. Para configurações, monitoramento ou assistência, os operadores podem acessar aos seus sistemas e componentes a qualquer momento e de forma segura, com a ajuda de terminais digitais.

Com o novo procedimento de segurança PUK2.0 aumentamos ainda mais a segurança e a facilidade de utilização dos sistemas para os utilizadores.

- Apenas os usuários autorizados pelo proprietário têm acesso aos sistemas.
- A utilização de tecnologias e procedimentos atuais garante uma proteção segura contra acessos não autorizados.
- O manuseamento dos sistemas é otimizado.

A partir de janeiro de 2022, o PUK2.0 substitui gradualmente o atual procedimento PUK da SMA.

Como funciona o PUK2.0

PUK significa Personal Unlocking Key e serve para redefinir as palavras-passe de um terminal no caso de o utilizador não dispor ou ter se esquecido de palavras-passe (PIN no caso de smartphones).

O PUK2.0 dá à Assistência SMA a possibilidade de acessar aos produtos SMA do usuário, caso seja necessário e após a devida autorização do administrador da planta.

O PUK2.0 substitui o código de acesso que poderia ser adquirido com a SMA para este caso.

Vantagens do PUK2.0

Mais seguro.

- Com base num protocolo de comunicação seguro de última geração.
- O operador tem controle total sobre o acesso do serviço de assistência.
- Aumenta a segurança tanto para sistemas novos como para os existentes.

Mais simples.

- Redefinir palavra-passe de forma rápida e descomplicada.
- Sem pedidos à SMA.

Gratuito.

- As taxas anteriormente existentes para o fornecimento de um PUK já não são aplicáveis.

Para atender às necessidades individuais de segurança, o PUK2.0 oferece dois níveis de segurança. No primeiro nível, de segurança básica, as características disponíveis no dispositivo, tais como WLAN-PSK, são utilizadas como segredo específico do dispositivo para proceder com as redefinições. Este nível está automaticamente ativado em todos os dispositivos.

No segundo nível, de segurança elevada, podem ser atribuídas chaves de produto específicas de dispositivo como segredo do dispositivo para cada planta do administrador. Esta chave de produto serve para desbloquear o dispositivo, caso se esqueça da sua palavra-passe. O segredo específico do dispositivo deixa de ser suficiente para iniciar uma redefinição de palavras-passe.

Nota: se o seu dispositivo estiver instalado numa área acessível ao público, deve ser utilizado o nível "High security" e a palavra-passe WLAN inicial ("WLAN-PSK") impressa na placa de identificação deve também ser alterada.

Segurança básica

- Para redefinir palavras-passe, são utilizados **segredos já existentes específicos do dispositivo** (por exemplo, WLAN-PSK, RID, etc.).
- Estes segredos fazem parte da placa de identificação de um dispositivo.
- A segurança básica está automaticamente ativada.

Segurança elevada

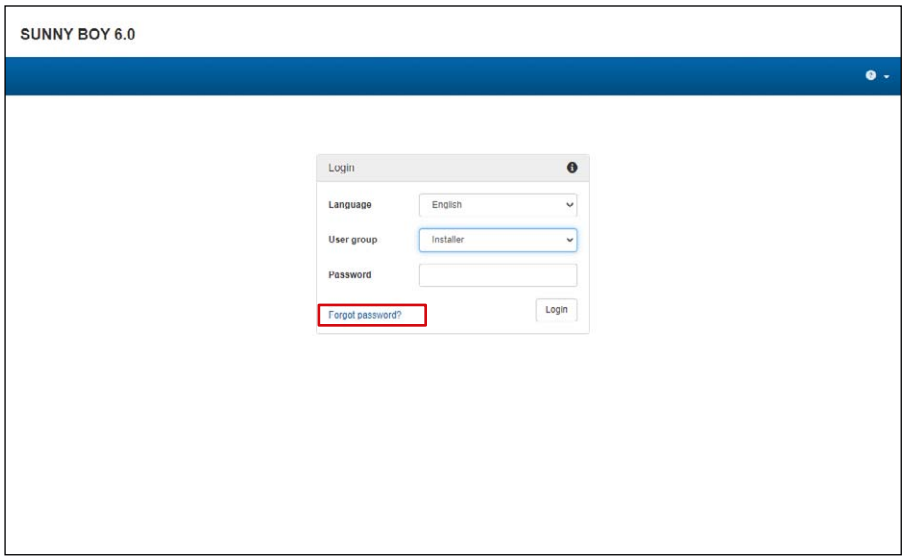
- Pode ser atribuída uma **chave de produto** específica do dispositivo e da função.
- A chave de produto é conhecida exclusivamente pelo administrador e não por terceiros.

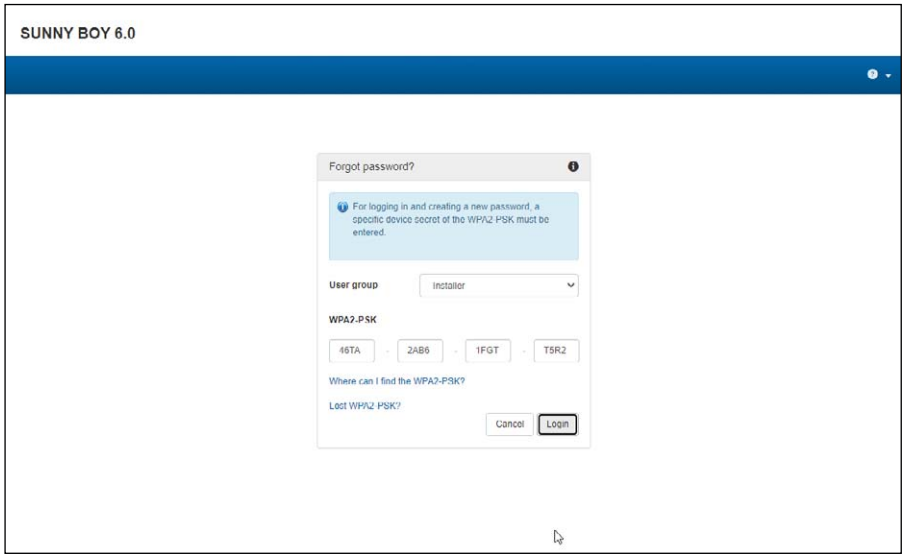
Esqueceu-se da palavra-passe. E agora?

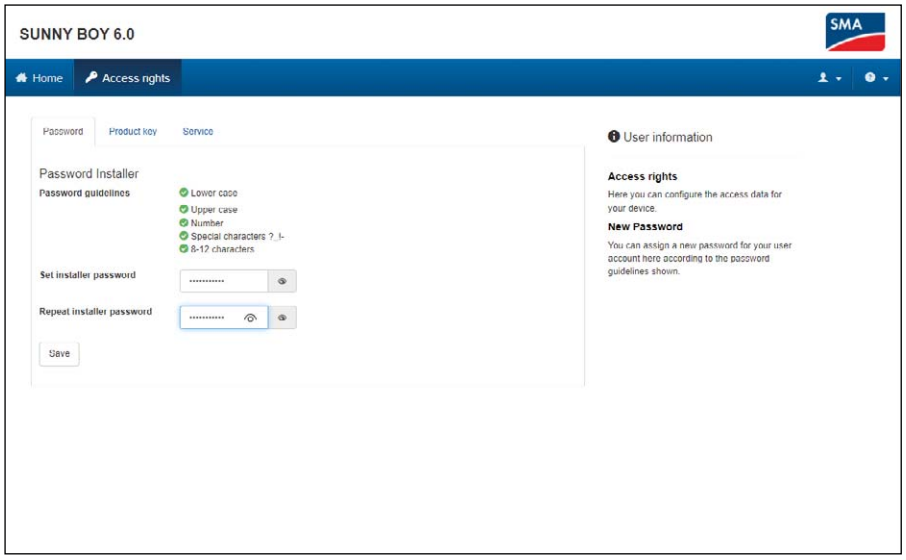
Com a funcionalidade "Forgot password", é possíve redefinir a palavra-passe no dispositivo para funções específicas. Dependendo se utiliza o nível Segurança básica ou Segurança elevada, necessitará de um segredo específico do dispositivo (por exemplo, WLAN-PSK) ou da chave de produto que lhe atribuiu.

1. Acesse à página de login na interface web do dispositivo.
2. Selecione o grupo de utilizadores.
3. Selecione "**Forgot password?"** na página de login.
4. Introduza o segredo do dispositivo (chave do produto ou segredo específico do dispositivo).
5. Clique em "**Login**".
6. Atribua uma nova palavra-chave para o dispositivo.

Nota: na página "Forgot password" do dispositivo, você pode consultar qual segredo específico do dispositivo que pode ser usado para proceder com a redefinição.





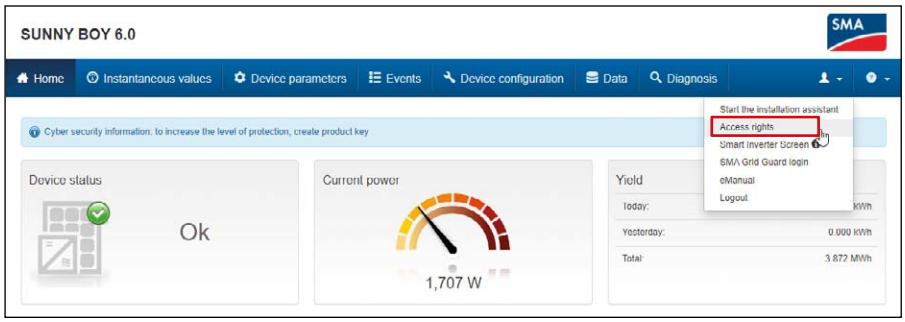


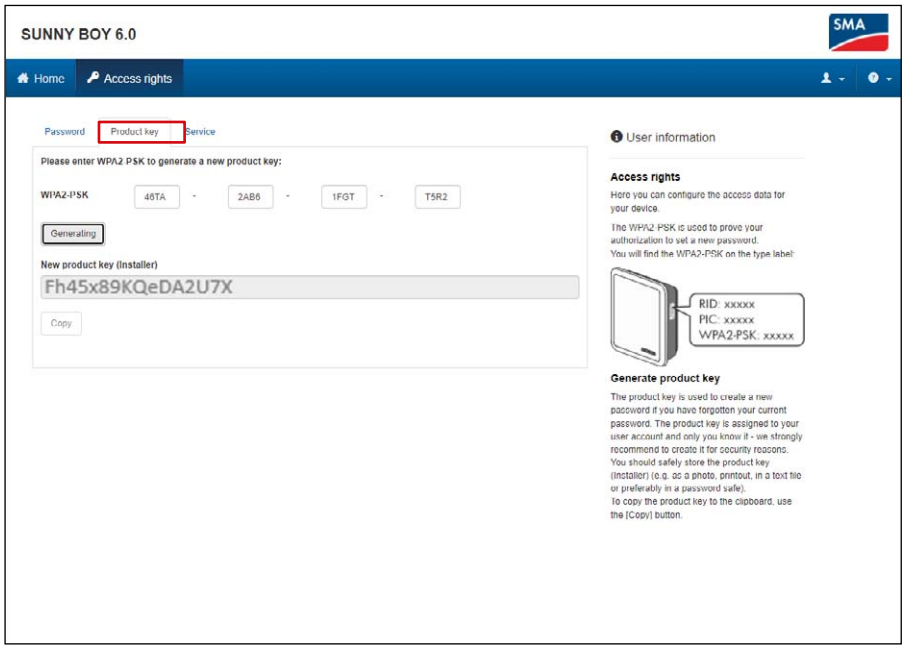
Atribuição de chaves de produto

Pode utilizar a chave de produto individual para desbloquear o seu dispositivo caso tenha esquecido da sua palavra-passe. Isto aumenta ainda mais a segurança em comparação com o nível de segurança básica.

1. Entre na interface web do dispositivo.
2. Na página "Use settings > Access rights", selecione o item "Product key".
3. Leia o segredo específico do dispositivo (no exemplo, é necessário o WLAN-PSK) na placa de identificação do mesmo, introduza-o e selecione "Generating".
4. A chave de produto é gerada e exibida. Anote a chave de produto gerada ou copie-a para a área de transferência e guarde-a em segurança e de forma que possa ser facilmente recuperada (por exemplo, num cofre de palavras-passe).

Precaução: se o seu dispositivo estiver instalado numa área acessível ao público, deve, definitivamente, atribuir uma nova chave de produto individual!

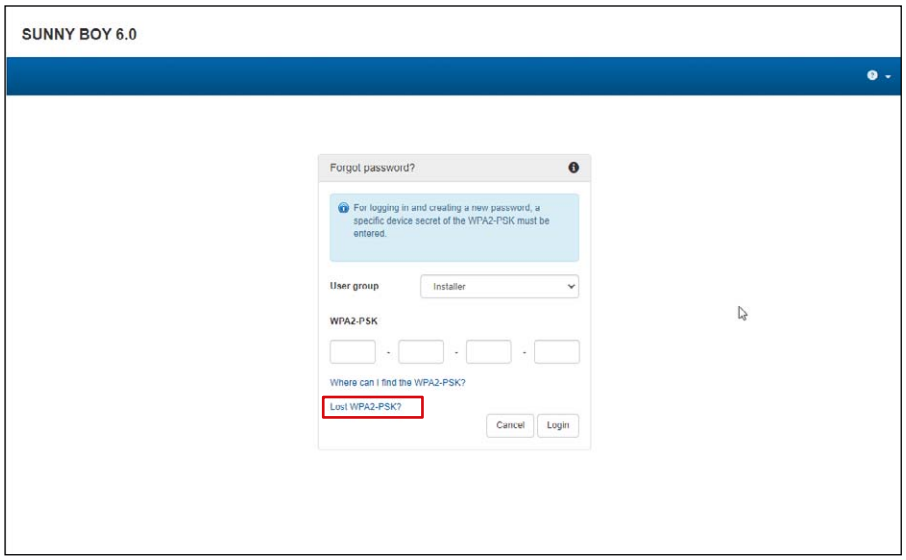


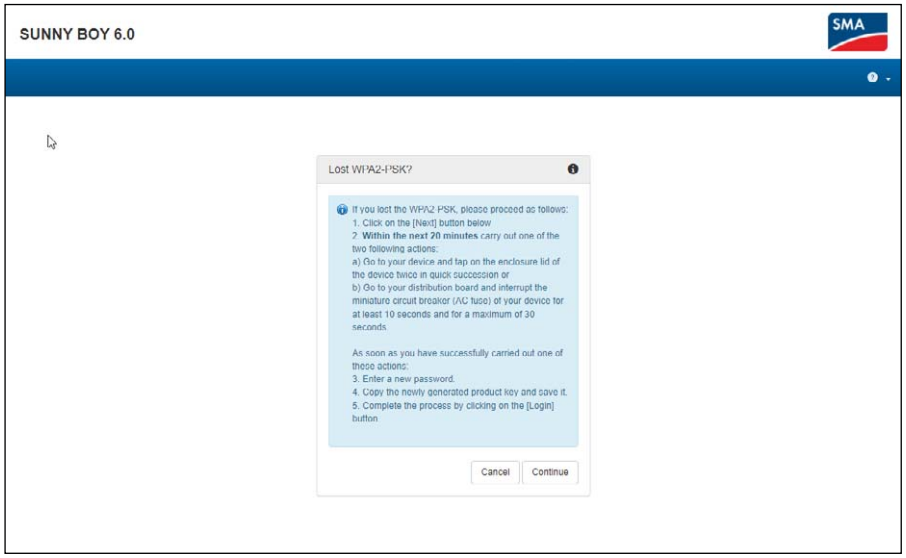


Palavra-passe e chave de produto esquecidas. O que fazer?

Caso não saiba a palavra-passe nem a chave de produto, está disponível outro mecanismo para desbloquear o dispositivo. Isto requer acesso físico ao dispositivo, pois esta funcionalidade só é possível diretamente no local.

1. Ir para a página de login na interface web do dispositivo.
2. Selecionar o grupo de utilizadores (User groups).
3. Selecionar "Forgot password?" na página de login.
4. Na página da palavra-passe esquecida, selecionar "Lost WLAN-PSK / Product key?"
5. Selecionar "Continue".
6. Agora tem de apresentar um comprovativo de presença no prazo de 20 minutos: dependendo do dispositivo utilizado, bata duas vezes seguidas na tampa da caixa (caso exista um sensor de batida). Em alternativa, desligue o dispositivo da rede elétrica pública, do lado CA, durante 10 a 30 segundos (por exemplo, utilizando o disjuntor).
7. Em seguida, pode atribuir uma nova palavra-passe e uma chave de produto na interface web do dispositivo (ver acima).
8. Anote a chave de produto gerada ou copie-a para a área de transferência e guarde-a em segurança e de forma que possa ser facilmente recuperada (por exemplo, num cofre de palavras-passe).



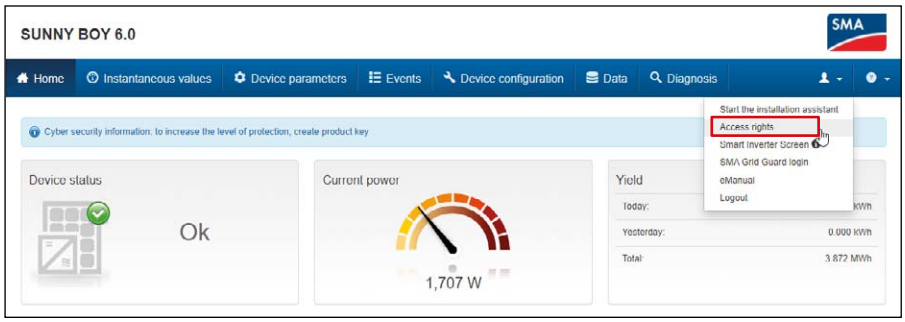


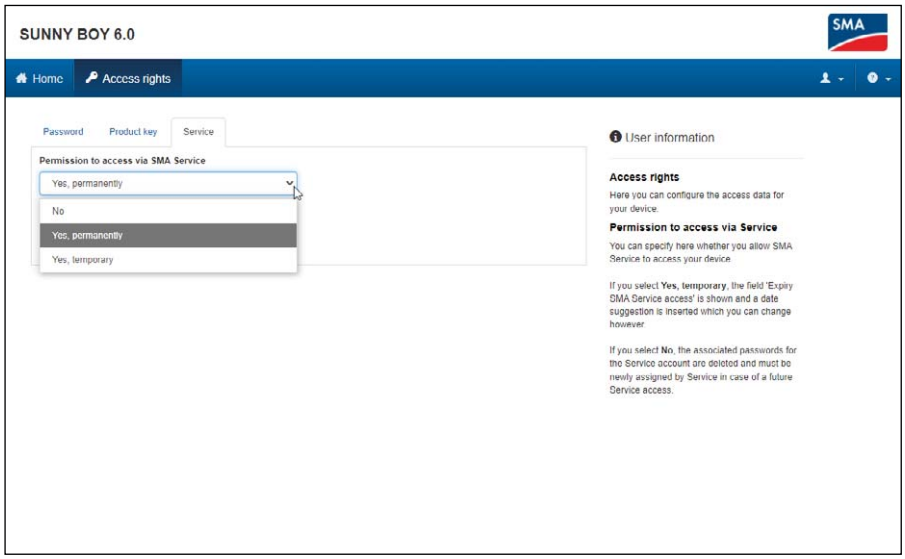
Autorizar acesso à Assistência

Com o PUK2.0, o acesso por parte da Assistência SMA é também mais simples e mais seguro. Os operadores podem escolher se pretendem autorizar o acesso temporário, permanente ou nenhum acesso por parte da Assistência SMA. A determinação regula o acesso da assistência tanto por via remota como no local.

1. Entre na interface web do dispositivo.
2. Nas definições do utilizador ("User settings"), selecione "Access rights" e abra o separador "**Service**".
3. No campo "**Permission to access via SMA Service**", selecione se permite o acesso da Assistência:
   - **"Yes, permanently"** ou
   - **"Yes, temporary"** ou
   - **"No"**

   No caso de autorização temporária ("temporary"), é inserida automaticamente uma data de validade de dois dias. Pode também definir manualmente uma data de validade diferente.
4. Selecione "**Save**".





Onde encontro mais informações sobre PUK2.0?

Pode encontrar mais informações sobre segurança com PUK2.0 nos seguintes capítulos das instruções de serviço do seu dispositivo:

- Apresentação geral do produto: SMA PUK2.0
- Gerar ou alterar chave de produto
- Ativar ou desativar o acesso do serviço de assistência
- Localização de erros: esquecimento da palavra-passe para produtos com versão de firmware ≥ 4.00.00.R
- Chave de produto perdida

Nesta dica técnica aprenderá como atribuir o PUK2.0 no seu dispositivo.

Para obter mais informações e aceder a documentos sobre produtos da SMA, vá à área de downloads do sítio web da SMA.

ENERGY
THAT
CHANGES

SMA-Portugal.com