



Más seguridad con PUK2.0

La digitalización de los sistemas energéticos es un paso clave hacia un suministro de energía renovable cada vez más descentralizado. Para realizar labores de configuración, monitorización de las plantas o servicio técnico, es imprescindible que los operadores puedan acceder en cualquier momento a sus sistemas y componentes por medio de terminales digitales.

Con el nuevo procedimiento de seguridad PUK2.0 reforzamos la seguridad y mejoramos la gestión de los sistemas para los usuarios.

- Solo pueden acceder a los sistemas los usuarios autorizados por el propietario.
- La integración de tecnologías y procedimientos modernos garantiza una protección segura frente al acceso no autorizado.
- Se optimiza la gestión de los sistemas.

A partir de enero de 2022, PUK2.0 irá sustituyendo gradualmente el procedimiento PUK existente de SMA.

Así funciona el procedimiento PUK2.0

PUK significa Clave de Desbloqueo Personal y se utiliza para restablecer las contraseñas de un terminal digital en caso de que las contraseñas del usuario (PIN en el caso de los teléfonos móviles) ya no estén disponibles o se hayan olvidado.

PUK2.0 ofrece al servicio técnico de SMA la posibilidad de acceder a los productos de SMA de un usuario para resolver cuestiones de servicio, siempre que el usuario haya otorgado la correspondiente autorización.

La clave PUK2.0 sustituye al código de acceso que se podía solicitar a SMA en estas situaciones.

Ventajas del PUK2.0

Más seguro.

- / Se basa en el protocolo de comunicación segura más actual
- / El operador tiene todo el control sobre el acceso al producto que recibe el servicio técnico de SMA
- / Aumenta la seguridad tanto en las plantas nuevas como en las existentes

Más sencillo.

- / Permite restablecer la contraseña de forma rápida y fácil
- / Sin necesidad de solicitar o contactar a SMA

Gratuito.

- / Se eliminan las cuotas anteriormente aplicadas para disponer de una clave PUK.

El procedimiento PUK2.0 ofrece dos niveles de seguridad para satisfacer las necesidades individuales a este respecto. En el primer nivel (seguridad básica), para restablecer la contraseña se utilizan características disponibles en el equipo, como la clave precompartida para WLAN (WLAN-PSK), que funcionan como código secreto específico del equipo. Este nivel de seguridad está automáticamente activo en todos los equipos.

En el segundo nivel de seguridad (seguridad alta), se pueden asignar claves de producto específicas de cada equipo como código secreto del equipo para cada cuenta de usuario. Esta clave de producto sirve después para desbloquear el equipo si ha olvidado la contraseña. El código secreto específico del equipo no basta para restablecer contraseñas con este nivel de seguridad.

Indicación: Si su equipo está instalado en una zona de acceso público, se recomienda utilizar el nivel de "seguridad alta" y cambiar además la contraseña inicial de la WLAN ("WLAN-PSK") que figura en la placa de características.

Seguridad básica

- / Para restablecer contraseñas se utilizan **los códigos secretos existentes** y específicos de los equipos (p. ej., WLAN-PSK, RID, etc.).
- / Estos códigos secretos se encuentran en la placa de características del equipo.
- / La seguridad básica se encuentra activada de forma automática.

Seguridad alta

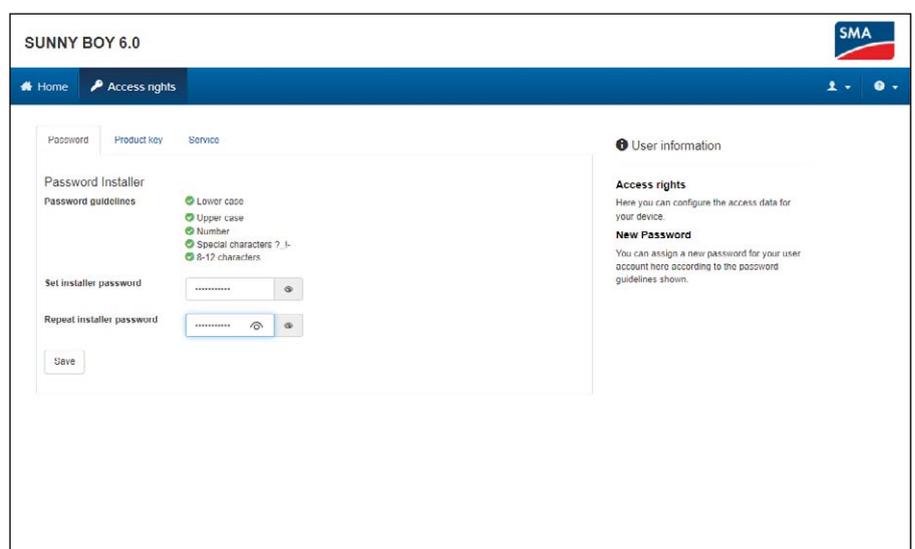
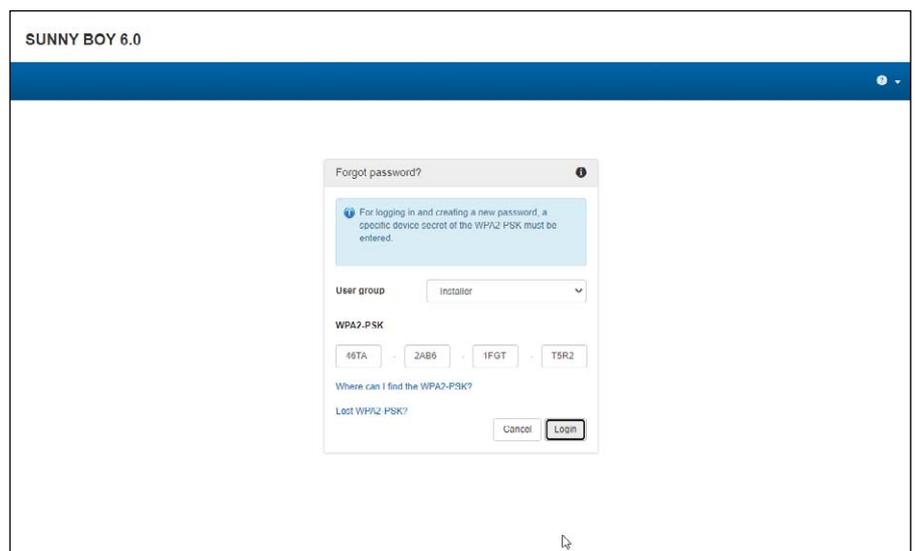
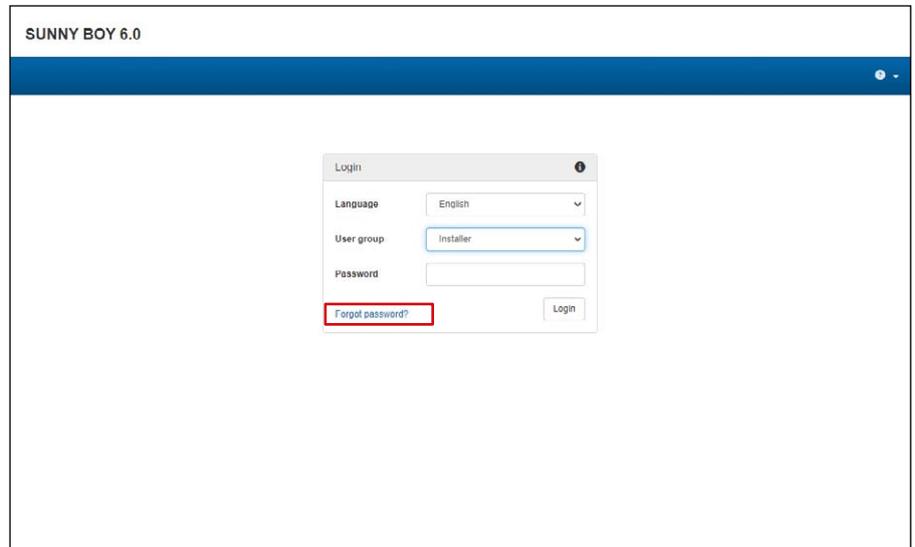
- / Se puede asignar una **clave de producto** específica para un equipo y específica para un rol.
- / La clave de producto solo está a disposición del usuario y no la conoce ningún tercero.

¿Qué debe hacer si ha olvidado su contraseña?

Con la función para contraseñas olvidadas puede restablecer la contraseña en el equipo de forma específica para un rol específico o grupo de usuarios. Dependiendo del nivel de seguridad utilizado (seguridad básica o alta), necesitará un código secreto específico del equipo (p. ej., WLAN-PSK) o la clave de producto que ha asignado.

1. Abra la página de acceso (Login) en la interfaz de usuario web del equipo.
2. Seleccione el grupo de usuarios.
3. En la página de acceso, seleccione **“Forgot password?”**.
4. Introduzca el código secreto del equipo (clave de producto o secreto específico del equipo).
5. Haga clic en **„Login“**
6. Asigne una nueva contraseña al equipo.

Indicación: En la página “Forgot password” del equipo se indica qué código secreto específico del equipo puede utilizar para restablecer la contraseña.

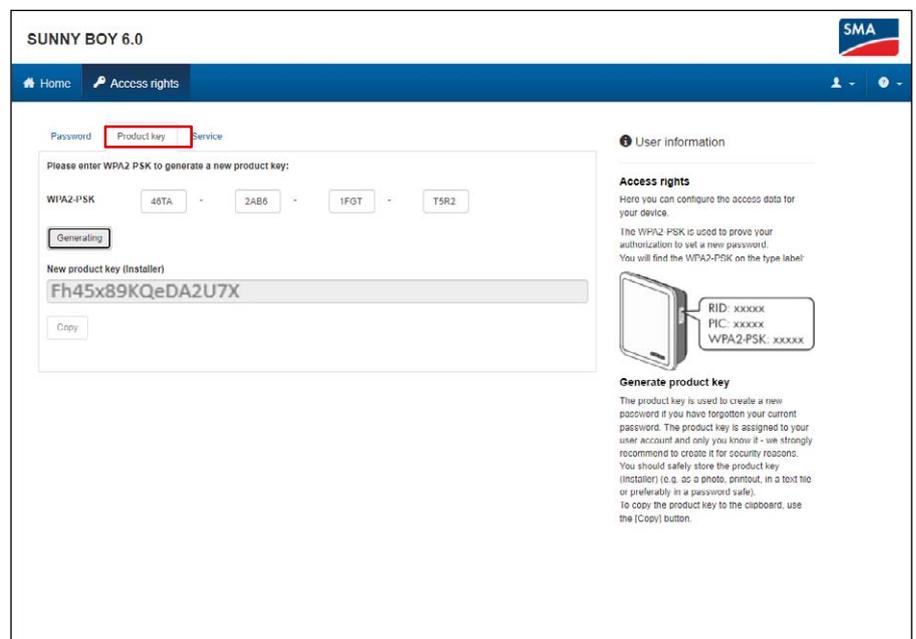


Asignación de claves de producto

Con la clave individual de producto puede desbloquear su equipo si ha olvidado la contraseña. Así refuerza el nivel de seguridad con respecto a la seguridad básica estándar.

1. Inicie la sesión en la interfaz de usuario web del equipo.
2. En la página "Access rights" de los ajustes de usuario, seleccione la pestaña "Product key".
3. Lea el código secreto específico del equipo (en el ejemplo se requiere la clave WLAN-PSK) en la placa de características del equipo, introdúzcalo y seleccione "Generating".
4. Se creará la clave de producto y se mostrará. Anótese la clave de producto creada o cópiela en el portapapeles y guárdela en un lugar seguro que pueda volver a localizar fácilmente (p. ej., un llavero virtual).

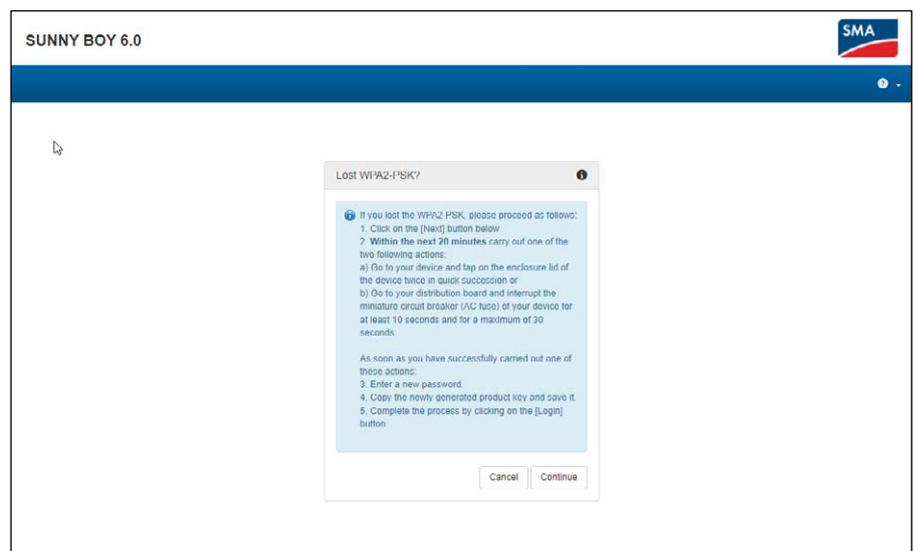
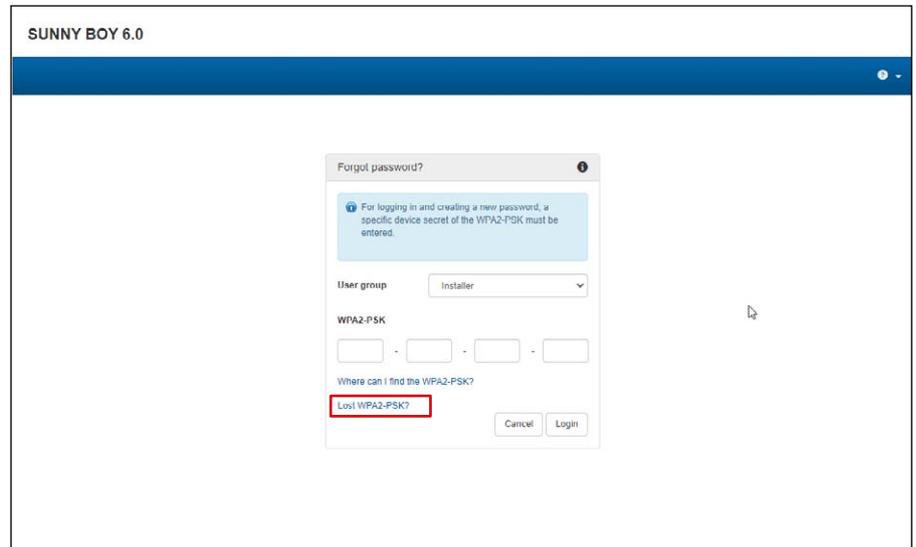
Precaución: Si su equipo está instalado en una zona de acceso público, debe asignar indispensablemente una clave individual de producto.



¿Qué debe hacer si ha olvidado su contraseña y la clave de producto?

Si no dispone de la contraseña ni de la clave de producto, existe otro mecanismo para desbloquear el equipo. Este método requiere el acceso físico al equipo, por lo que solo se puede emplear directamente en el lugar donde está instalado.

1. Abra la página de acceso (Login) en la interfaz de usuario web del equipo.
2. Seleccione el grupo de usuarios (User group).
3. En la página de acceso, seleccione "Forgot password?".
4. En la página "Forgot password?", seleccione "Lost WPA2-PSK?".
5. Seleccione "Continue".
6. Ahora tiene que demostrar en los 20 minutos siguientes que está presente: en función del equipo utilizado, deberá dar dos golpecitos seguidos en la tapa de la carcasa (si el equipo dispone de un sensor de golpes) o bien desconectar el equipo de la red pública por el lado de la corriente alterna durante un espacio de tiempo de entre 10 y 30 segundos (p. ej., con el interruptor automático).
7. A continuación, ya puede asignar una nueva contraseña y una clave de producto en la interfaz de usuario web del equipo (véase arriba).
8. Anótese la clave de producto nueva o cópiela en el portapapeles y guárdela en un lugar seguro que pueda volver a localizar fácilmente, p. ej., un llavero virtual.



Autorizar el acceso para el servicio técnico de SMA

Con PUK2.0 también se ha reconfigurado el acceso del servicio técnico de SMA para que sea más sencillo y seguro. Los operadores de las plantas pueden decidir si desean otorgar al servicio técnico de SMA un acceso temporal, un acceso permanente o no desean otorgar ningún acceso. Esta decisión se aplicará tanto al acceso remoto como al acceso local por parte del servicio técnico.

1. Inicie la sesión en la interfaz de usuario web del equipo.
2. En la página "Access rights" de los ajustes de usuario, seleccione la pestaña "Service".
3. Seleccione en el campo "Permission to access via SMA-Service" el permiso de acceso para el servicio técnico.

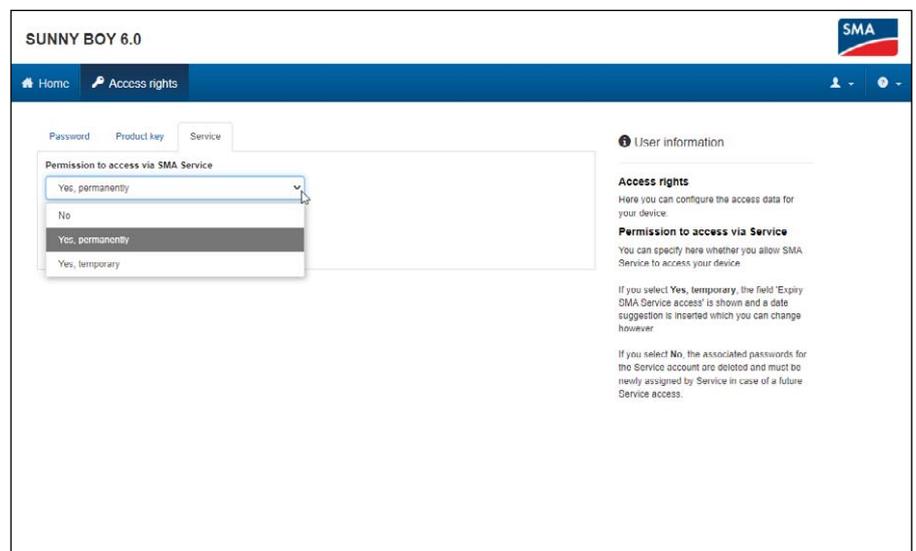
- "Yes, permanently"
("Sí, permanentemente") o

- "Yes, temporary"
("Sí, temporalmente") o

- "No"

Si selecciona la autorización temporal, aparecerá automáticamente una fecha de permiso para los siguientes dos días. Puede ajustar manualmente otra fecha de finalización del permiso.

4. Seleccione "Guardar".



¿Dónde puedo encontrar más información sobre PUK2.0?

Encontrará más información sobre seguridad con el procedimiento PUK2.0 en los siguientes capítulos del manual de funcionamiento de su equipo:

- Vista general del producto: SMA PUK2.0
- Generar o modificar la clave del producto
- Activar o desactivar el acceso de servicio técnico
- Localización de errores: Contraseña olvidada para productos con la versión de firmware $\geq 4.00.00.R$
- Se ha perdido la clave del producto

En este [Consejo técnico](#) se explica cómo asignar la clave PUK2.0 en su equipo.

Encontrará más información y documentos sobre los productos y soluciones de SMA en la página web [Sección de descargas](#).



SMA-Iberica.com

