

Tabla de Contenidos

Cómo administrar manualmente la clave de cifrado del Servidor y del Dispositivo	1
Concepto	1
Configuración	2
Desactivación de la función	4

[System Configuration](#), [BioStar 2](#), [TLS](#), [secure communication](#), [“Encryption, Key”](#)

Cómo administrar manualmente la clave de cifrado del Servidor y del Dispositivo

Concepto

Esta es una nueva característica de seguridad que se introduce con BioStar 2.6. que le permite elegir su propia clave de cifrado para cifrar su base de datos y sus dispositivos.

No proceda con el uso de esta característica de cifrado antes de comprender completamente sus efectos.

Si va a aplicar esta función a un sitio existente, provocará la pérdida de datos y le pedirá que vuelva a configurar todos los PINs y contraseñas.

El servidor y los dispositivos no se pueden usar durante el proceso de migración y el Seguro contra alteraciones (Tamper) se habilitará cuando se utilice esta característica.

Debe activar la función **Comunicación segura con el dispositivo(Secure communication with device)** para utilizar esta función.

Tenga en cuenta las precauciones antes de usar esta función:

Dispositivo

- Cuando esta función está activada, TODOS los usuarios del dispositivo se eliminan y se transfieren de nuevo al dispositivo.
- Cuando se agrega un nuevo dispositivo al servidor que se ha cifrado, TODOS los datos se eliminarán y sincronizarán de nuevo con el servidor.
- El Seguro contra alteraciones (Tamper) estará activado de forma predeterminada cuando se utilice esta función. No puede desactivar esta función. Esto significa que al eliminar el dispositivo del panel, se eliminarán TODOS los datos del dispositivo.

Usuario

- Los usuarios con PIN o contraseña tienen que volver a configurar la contraseña, porque queda inutilizada después del cifrado.
- No se puede aplicar esta función si algún usuario tiene un PIN o una contraseña. Para proceder, primero se debe eliminar todos los PINs y contraseñas.
- Si las tarjetas inteligentes se emitieron antes del cifrado, funcionará la autenticación de tarjeta + huella dactilar, pero no así tarjeta + PIN. Se deberá emitir nuevamente la tarjeta inteligente y tendrá que ser emitida con un nuevo PIN.

La razón por la que las contraseñas de PIN e ID no se pueden usar después del cifrado es porque esos elementos tienen cifrado irreversible.

Base de datos

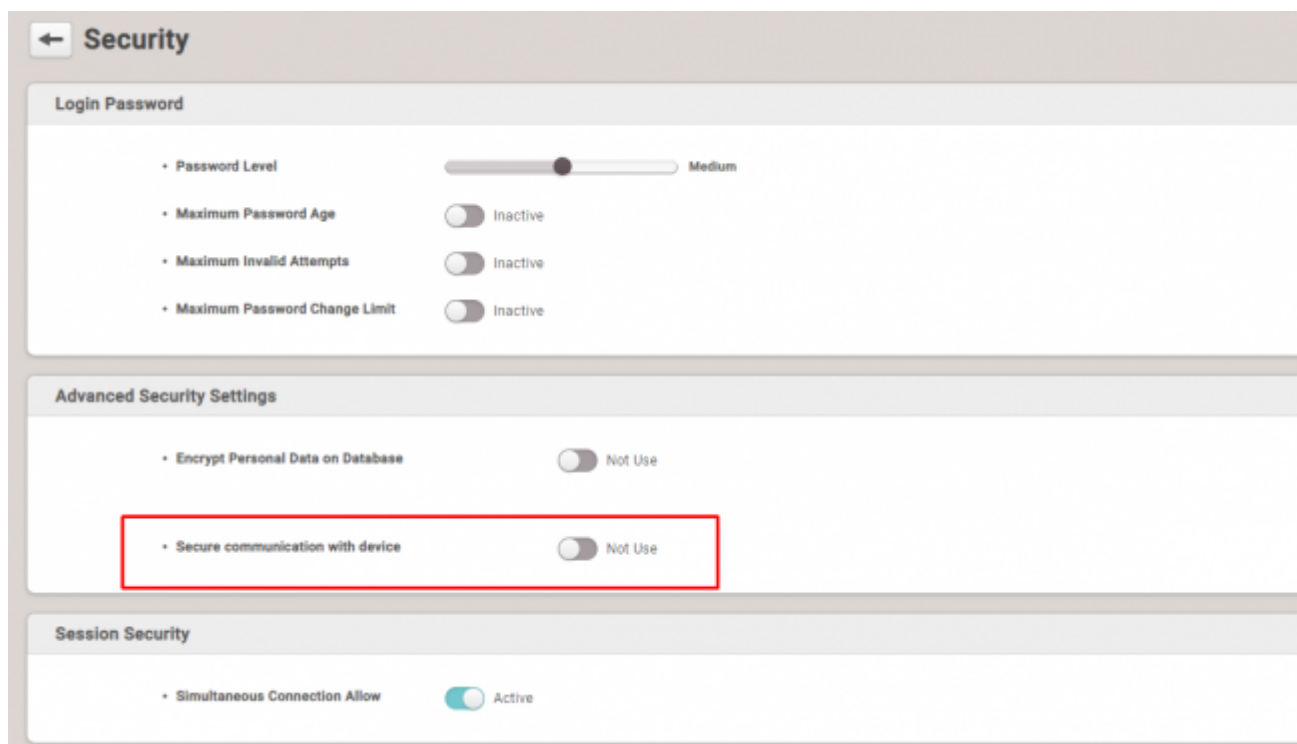
- Una vez que se aplica esta característica, la base de datos pasa por una fase de migración para cifrar la base de datos. No es posible usar BioStar Client en este estado.
- La migración cifra los datos personales (contraseña, PIN, plantilla de rostro y huella) en la base de datos.

Clave de cifrado

- La clave de seguridad configurada manualmente se almacena en una ubicación secreta y no en la base de datos.
- En los dispositivos P2 y N2, la clave de seguridad se almacena en el elemento seguro, que es un hardware independiente de la memoria flash.
- Debe mantener un registro de la clave de seguridad manual que configuró.

Configuración

1. Inicie sesión en Biostar 2 con la cuenta de administrador para el **usuario con ID 1(User ID 1)**. Otros usuarios administradores no pueden acceder a la **Configuración de seguridad Avanzada(Advanced Security Settings)**.
2. Vaya a **Ajustes(Setting) > SERVIDOR(SERVER) > Configuración de seguridad avanzada(Advanced Security Settings)**.
3. Active **Comunicación segura con el dispositivo(Secure communication with device)**.



4. Haga clic en **Continuar(Continue)** cuando aparezca una ventana emergente de advertencia.
5. Active **Administración manual de claves de cifrado de servidor y dispositivo(Server & device encryption key manual management)**.

No proceda con el uso de esta característica de cifrado antes de comprender completamente

las precauciones arriba mencionadas.

6. Haga clic en **Continuar(Continue)** cuando aparezca una ventana emergente de advertencia.

Si todavía tiene algún usuario con Contraseña o PIN que no sea el usuario de administrador predeterminado (ID 1), debe eliminar todas las contraseñas y PINs antes de continuar. De lo contrario, no podrá activar esta función.

7. Haga clic en **Cambiar(Change)** en el elemento **Clave de cifrado(Encryption Key)**.



8. Introduzca el nuevo valor de cifrado.

La longitud de la clave de cifrado debe ser de 32 letras.

9. Introduzca la contraseña predeterminada de administrador. Esta será la contraseña para el administrador predeterminado ID 1.

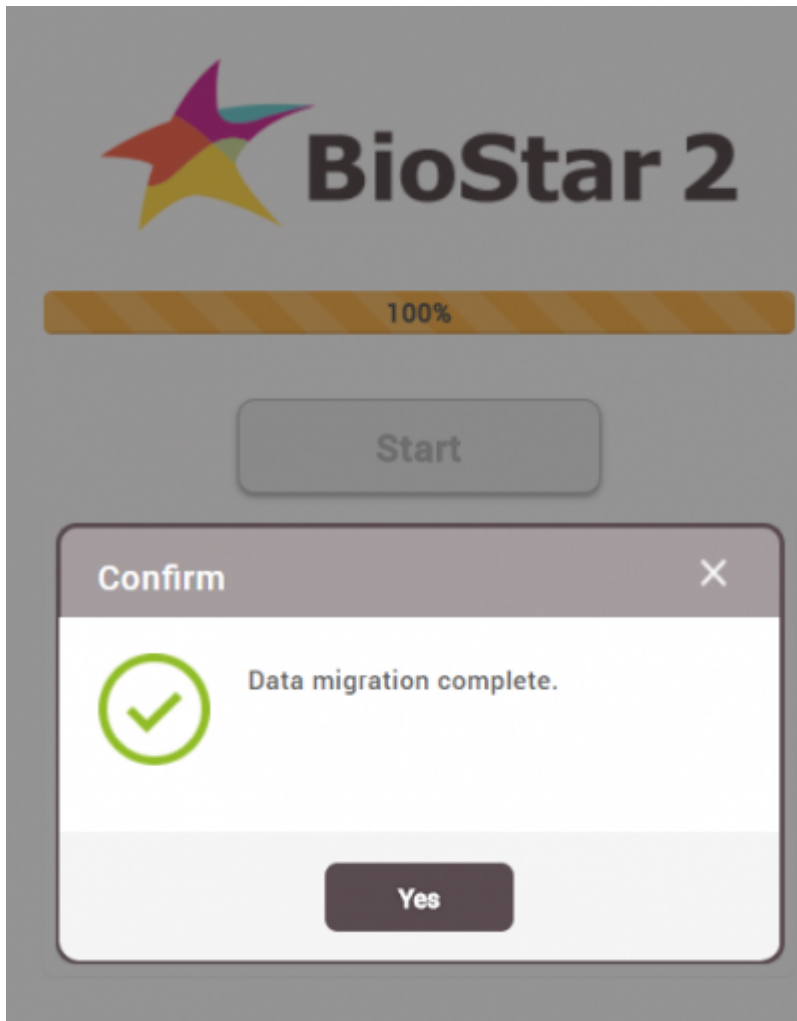
10. Haga clic en **Aceptar(OK)**.



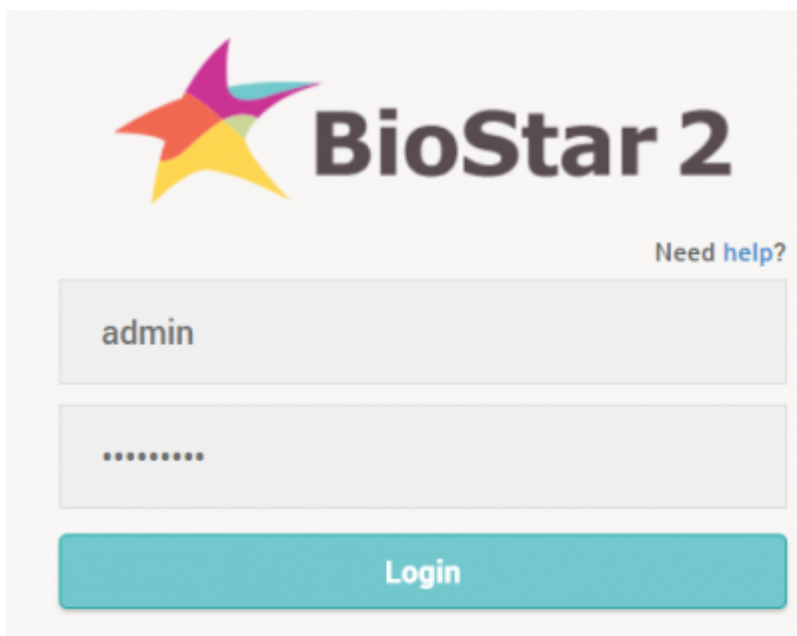
11. Haga clic en **Aplicar(Apply)**.

12. Cuando aparezca la página de migración, haga clic en **Iniciar(Start)**.

13. Espere a que se complete la migración de datos.



14. Inicie sesión en BioStar 2 con su nueva contraseña de administrador. La ID es **admin**.



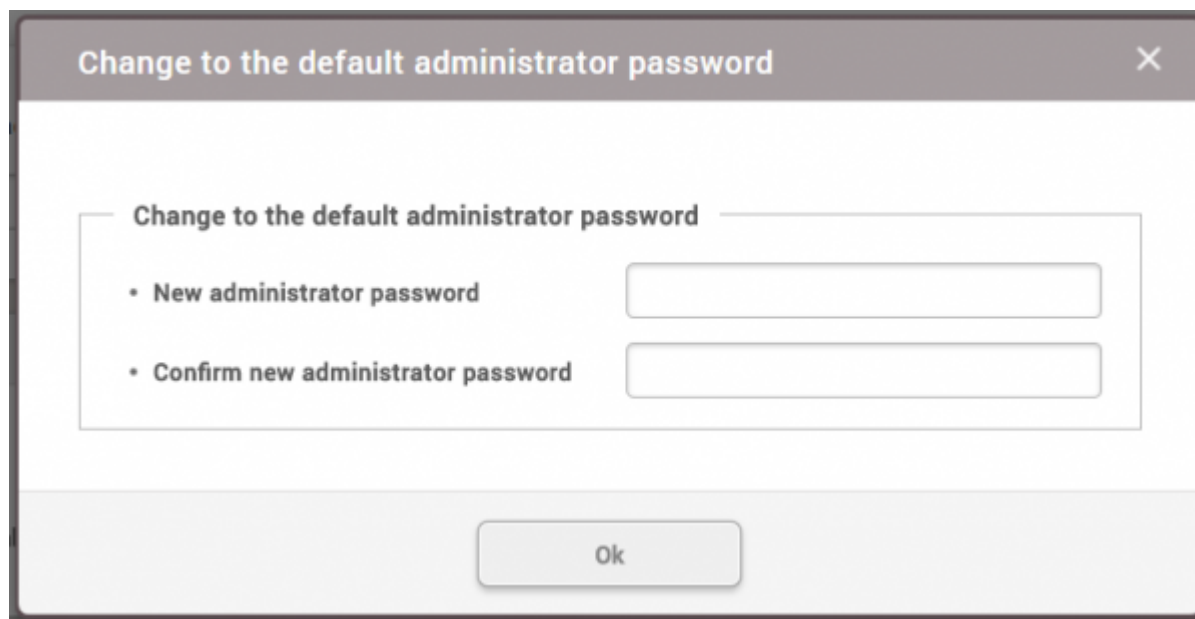
Desactivación de la función

Al desactivar la función se aplican las mismas restricciones de PIN y PW. Se debe eliminar todos los PINs y contraseñas de los usuarios para continuar.

1. Inicie sesión en Biostar 2 con la cuenta de administrador.
2. Vaya a **Ajustes(Setting) > SERVIDOR(SERVER) > Configuración de seguridad Avanzada(Advanced Security Setting)**.
3. Desactive **Administración manual de claves de cifrado de servidor y dispositivo(Server & device encryption key manual management)**.

Si todavía tiene algún usuario con Contraseña o PIN que no sea el usuario de administrador predeterminado (ID 1), debe eliminar todas las contraseñas y PINs antes de continuar. De lo contrario, no podrá desactivar esta función.

4. A popup will appear to ask you to change the default admin password.



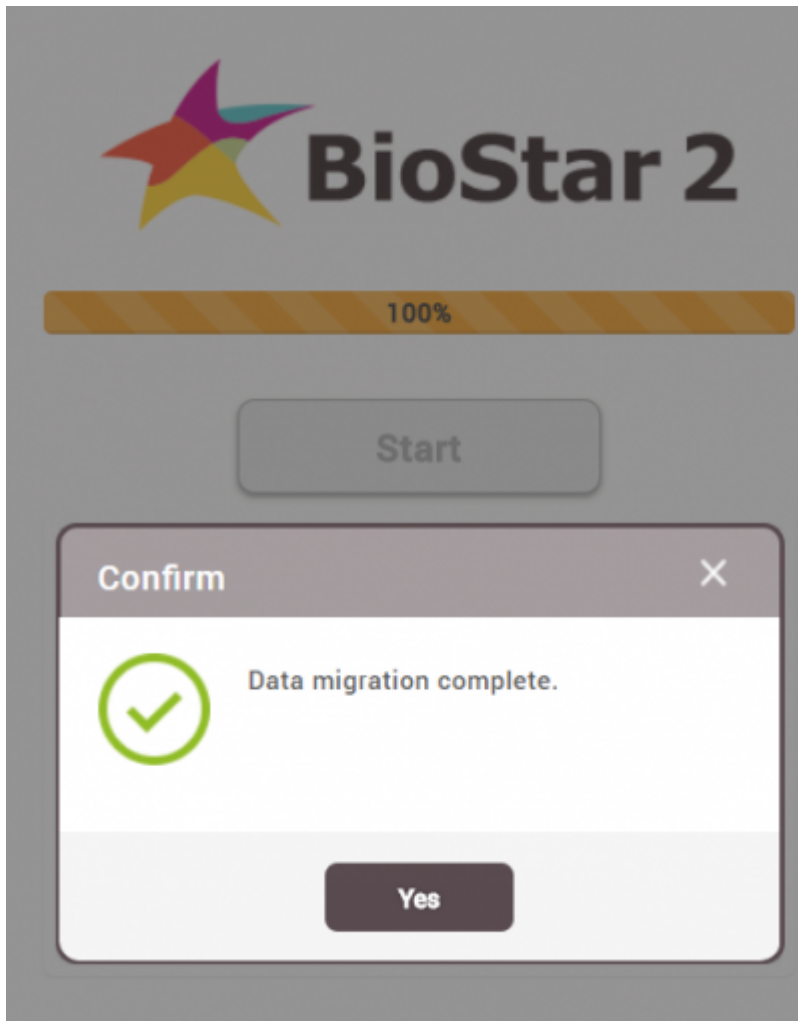
Change to the default administrator password

Change to the default administrator password

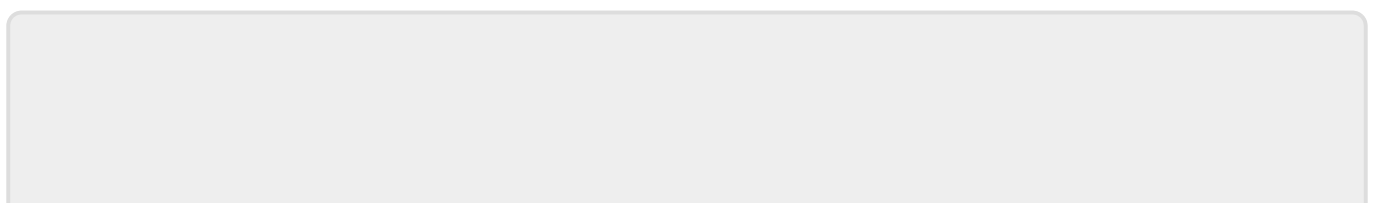
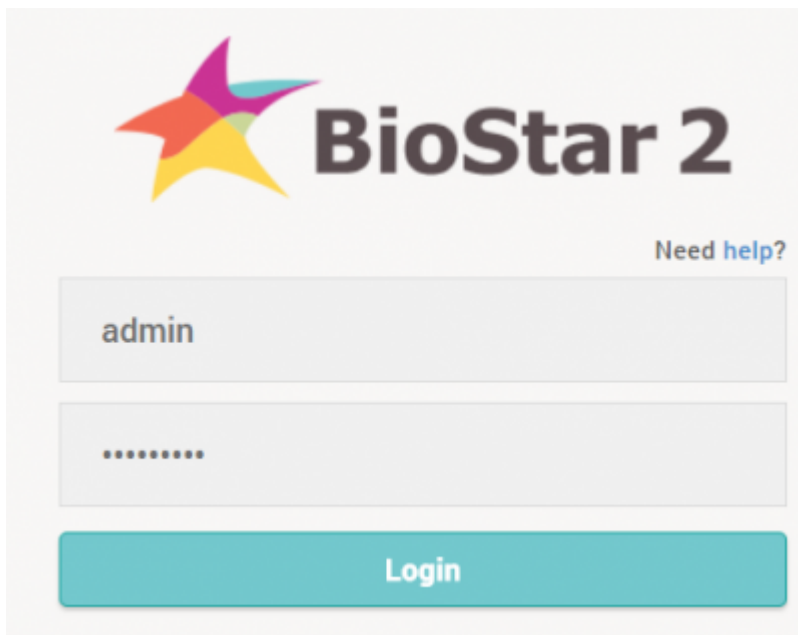
- New administrator password
- Confirm new administrator password

Ok

5. Introduzca su contraseña y haga clic en **Aceptar(OK)**.
6. Haga clic en **Aplicar(Apply)**.
7. Cuando aparezca la página de migración, haga clic en **Iniciar(Start)**.
8. Espere a que se complete la migración de datos.



9. Inicie sesión en BioStar 2 con su nueva contraseña de administrador. La ID es **admin**.



From:

<https://kb.supremainc.com/knowledge/> -

Permanent link:

https://kb.supremainc.com/knowledge/doku.php?id=es:how_to_manually_manage_server_device_encryption_key

Last update: **2020/05/18 18:17**