

目次

サーバーおよびデバイスの暗号化キーの手動管理	1
概念	1
構成	2
機能を終了する	4

, BioStar 2, TLS, セキュリティー通信, “暗号化キー”

サーバーおよびデバイスの暗号化キーの手動管理

概念

これはBioStar

2.6に追加された新たなセキュリティー機能で、自分の暗号化キーを選択してデータベースとデバイスを暗号化することができます。

この機能は、必ず暗号化機能について完璧に理解してから使用してください。
この機能を既存サイトに適用する場合、データが失われ、全てのPIN
およびパスワードを再度設定しなければなりません。
サーバーおよびデバイスはMigration
進行中には使用できず、この機能を使う際にはセキュリティータンパーが常にON
の状態で作動します。

この機能を使うにはデバイスと**セキュリティー通信(Secure communication with device)**機能をONにしなければなりません。

使用前には注意事項を必ず熟知してください。

デバイス

- この機能をONにすると、デバイスの全てのユーザーが削除され、デバイスに再送信されます。
- 新しいデバイスが暗号化されたサーバーに追加されると、全てのデータは削除され、サーバーと再度同期化されます。
- この機能をONにすると、自動的にセキュリティータンパーがONになり、任意に解除できません。
つまり、デバイスをブラケットから分離する場合、デバイスの全てのデータは削除されます。

ユーザー

- 暗号化後には既存の設定したユーザーPIN
あるいはパスワードを使用できないため、再度構成しなければなりません。
- ユーザーにPINまたはパスワードがある場合はこの機能を適用できません。
暗号化を行う前に全て削除しなければなりません。
- スマートカードが発行された場合、暗号化後に'カード+指紋'認証は作動しますが、'カード+PIN'
'認証は作動しません。スマートカードは新しいPINで再発行しなければなりません。

PINおよびパスワードは、暗号化が不可能なため暗号化後は使用できず、再設定が必要です。

データベース

- データベースは暗号化機能を適用した後、Migration段階を経て暗号化されます。この状態でBioStar
2クライアントは使用できません。

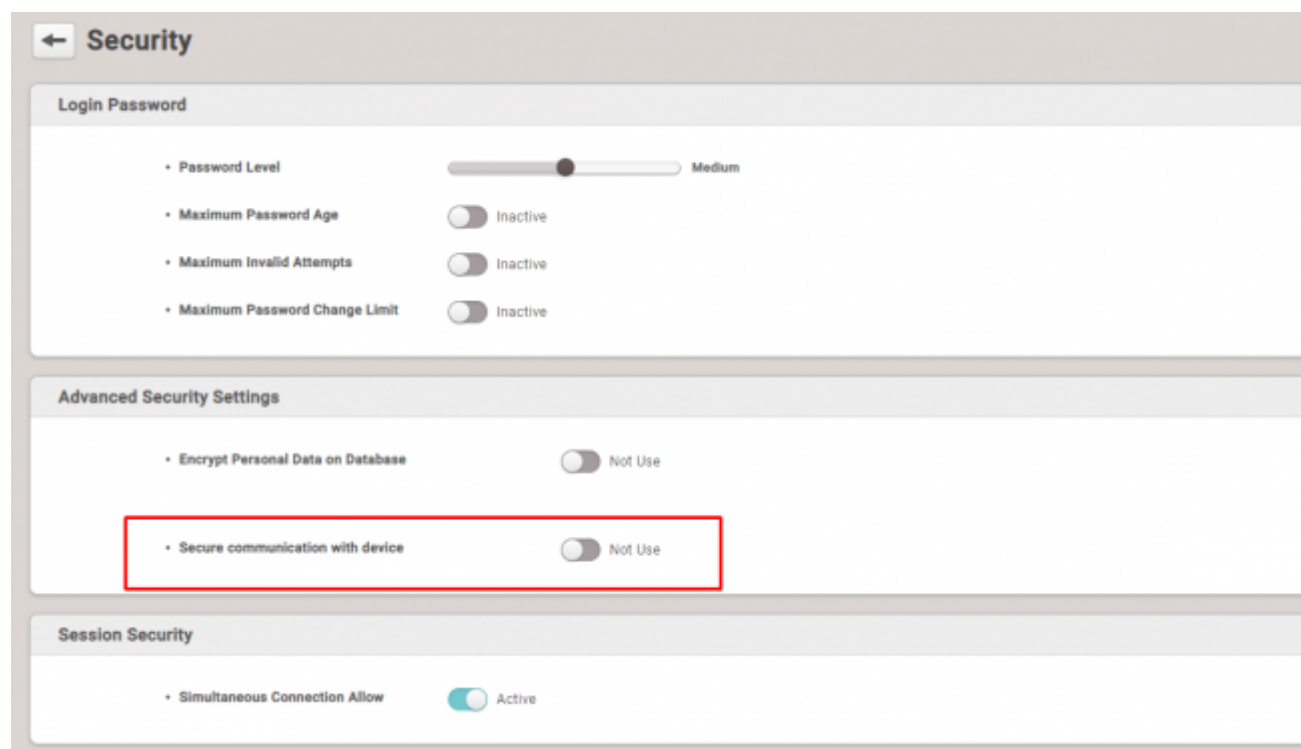
Migrationはデータベースで個人データ(パスワード、PIN、顔および指紋テンプレート)を暗号化します。

暗号化キー

- 手動で構成されたセキュリティーキーは、データベースでなくセキュリティーが適用された経路に保存されます。
- BioEntry P2およびBioLite N2において、セキュリティーキーはフラッシュメモリと分離されたハードウェアであるセキュリティー要素に保存されます。
- 構成された手動セキュリティーキーを記録しておいてください。

構成

1. 管理者アカウントでBioStar 2にログインしてください。
2. 設定(**Setting**) > サーバー(**SERVER**) > 高度セキュリティー設定(**Advanced Security Settings**)に移動してください。
3. **デバイスとセキュリティー通信(Secure communication with device)**をONにしてください。



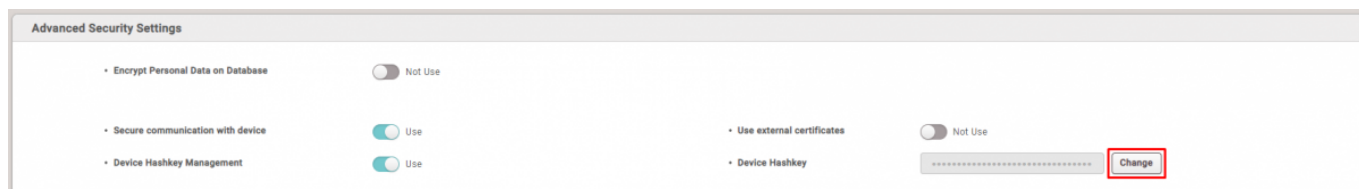
4. 警告ポップアップが表示されたら、続行(**Continue**)をクリックしてください。
5. サーバーおよびデバイス暗号化キー手動管理(**Server & device encryption key manual management**)をONにしてください。

この機能は、上記で言及した注意事項を必ず熟知してから使用してください。

6. 警告ポップアップが表示されたら、続行(**Continue**)をクリックしてください。

この機能は、パスワードやPINを設定したユーザーがいる場合には使用できません。基本admin(ID 1)ユーザーでないパスワードやPINを設定したユーザーがいる場合、全てのパスワードとPINを削除しなければなりません。

7. 暗号化キー(Encryption Key)項目の変更(Change)をクリックしてください。

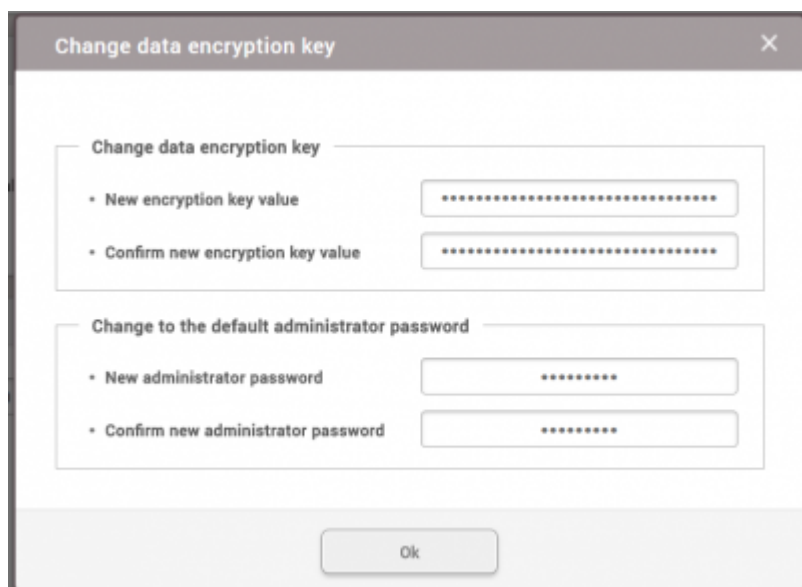


8. 新しい暗号化キーの値を入力してください。

暗号化キーの値の長さは32字です。

9. 基本管理者パスワードを入力してください。これは基本admin(ID 1)のパスワードです。

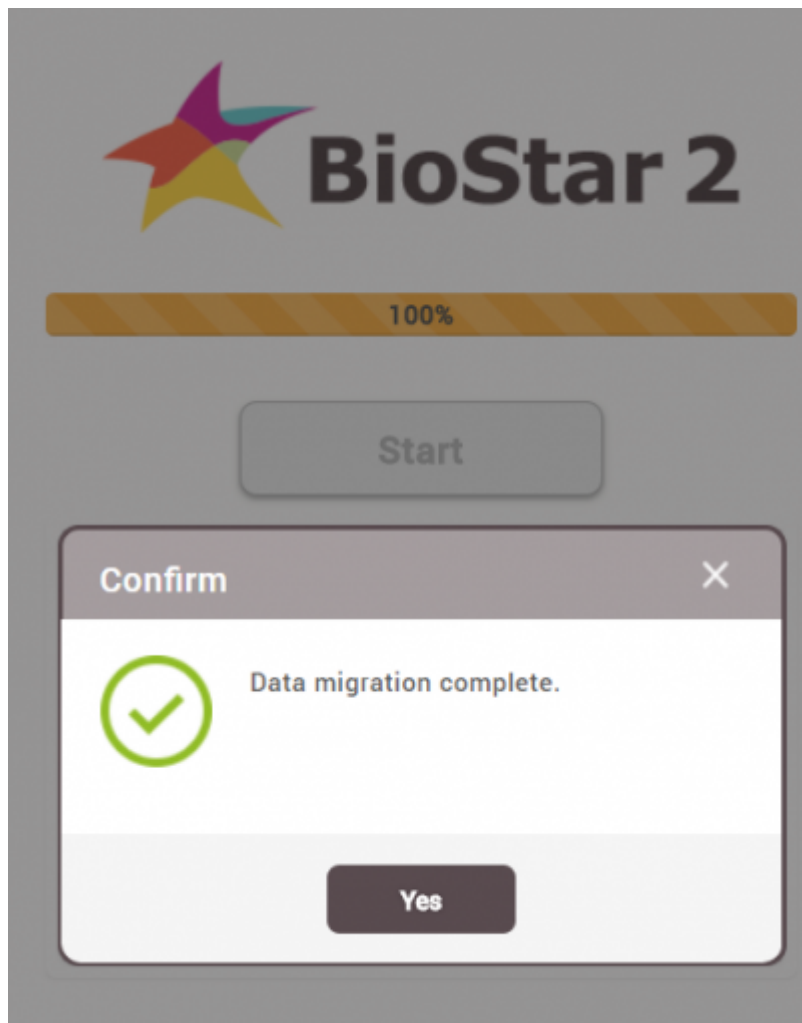
10. 確認(OK)をクリックしてください。



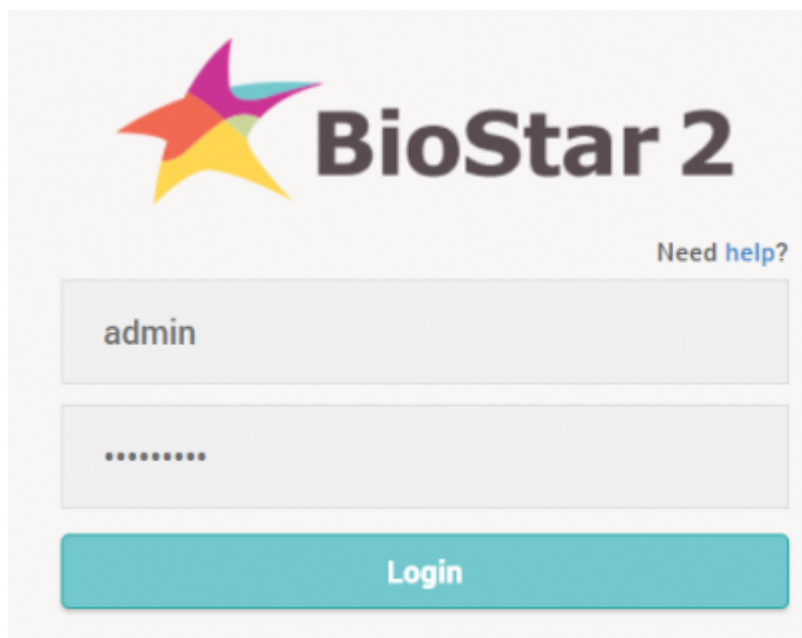
11. 確認(Apply)をクリックしてください。

12. Migrationページが表示されたら、スタート(Start)をクリックしてください。

13. データMigrationが完了するまでお待ちください。



14. 新しい管理者パスワードでBioStar 2にログインしてください。IDは**admin**です。



機能を終了する

機能が終了したら、同一パスワードおよびPIN制限が適用されます。
続行するには全てのユーザーパスワードおよびPINを削除しなければなりません。

1. 管理者アカウントでBioStar 2にログインしてください。
2. 設定(**Setting**) > サーバー(**SERVER**) > 高度セキュリティー設定(**Advanced Security Settings**)に移動してください。
3. サーバーおよびデバイス暗号化キー手動管理(**Server & device encryption key manual management**)をOFFにしてください。

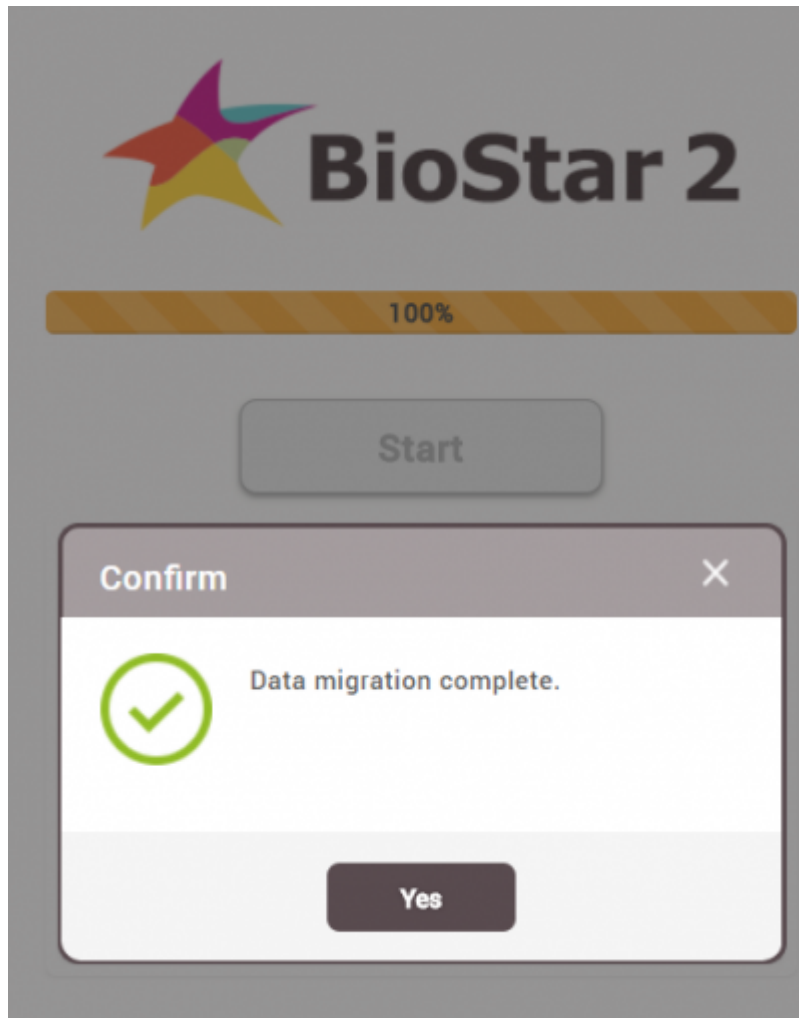
この機能は、パスワードやPINを設定したユーザーがいる場合には使用できません。基本admin(ID

1)ユーザーでないパスワードやPINを設定したユーザーがいる場合、全てのパスワードとPINを削除しなければなりません。

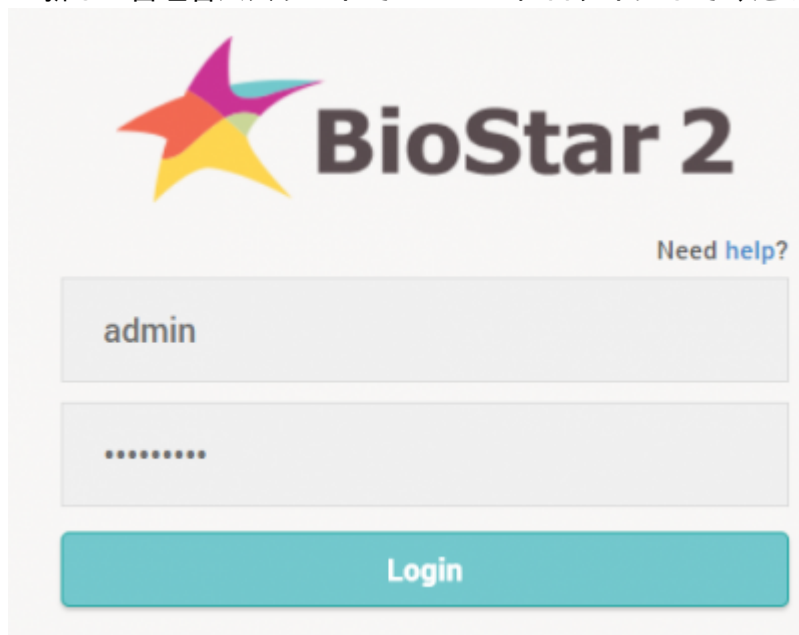
4. 基本管理者パスワードの変更を要求するポップアップが表示されます。



5. パスワードを入力した後、確認(**OK**)をクリックしてください。
6. 確認(**Apply**)をクリックしてください。
7. Migrationページが表示されたら、**スタート(Start)**をクリックしてください。
8. データMigrationが完了するまでお待ちください。



9. 新しい管理者パスワードでBioStar 2にログインしてください。IDは**admin**です。



From:

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

Permanent link:

http://kb.supremainc.com/knowledge/doku.php?id=ja:how_to_manually_manage_server_device_encryption_key

Last update: **2019/08/22 09:20**