Table of Contents

BioStar 1, Encryption

How to secure the device and user information

There are three different methods to secure the device and user information in BioStar.
1. Lock All Devices
2. Personal Information Encryption
3. Fingerprint Encryption

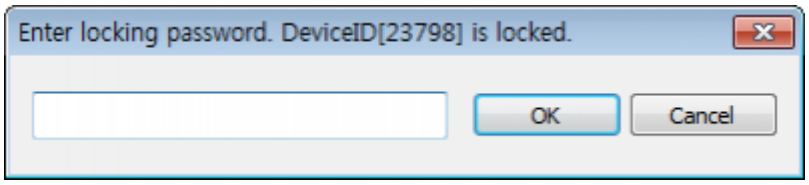
Lock All Devices

Lock All Devices feature allows the devices to be protected from unauthorized access when BioStar Client is not running. There is a possibility that unauthorized users to manipulate the device settings when maximum number of connections is set to more than one on the devices. Lock All Devices feature will minimize the risk of unauthorized access.

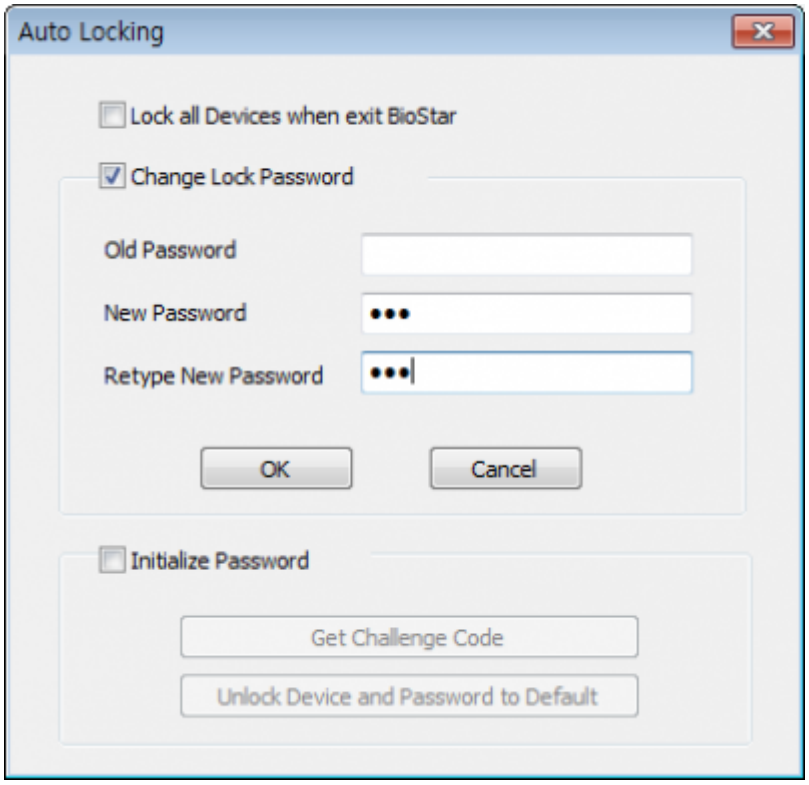
> Lock All Devices feature is not supported when the devices are connected directly to the server.

To lock connected devices:
1. Go to **Option** > **Device** > **Lock All Devices**.

To unlock connected devices:
1. Go to **Option** > **Device** > **Unlock All Devices**.
2. Enter the password then click **OK**. (If you have not created a password, simply click **OK**.)



No default password assigned when using for the first time. Follow the steps below to create a password:
1. Go to **Option** > **Device** > **Automatic Locking**.



2. Enter the new password then click **OK**.

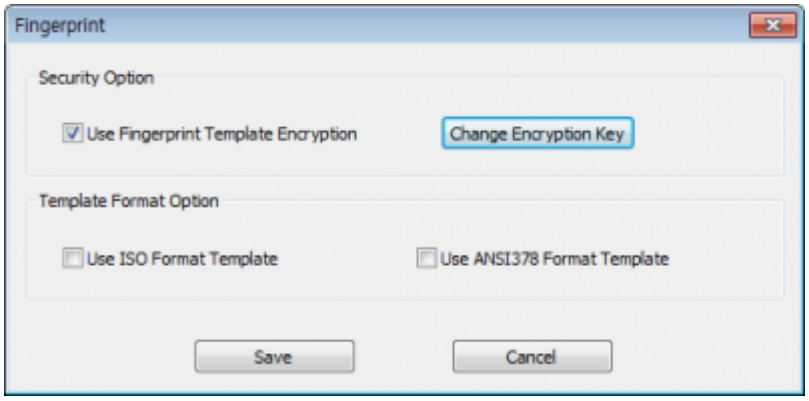
3. Please refer to **How to unlock a device using Challenge code**, if you have forgotten your password.

- It is not possible to assign new password to BioStation, BioStation T2, FaceStation and D-Station devices. Please use the master password to lock/unlock the devices.

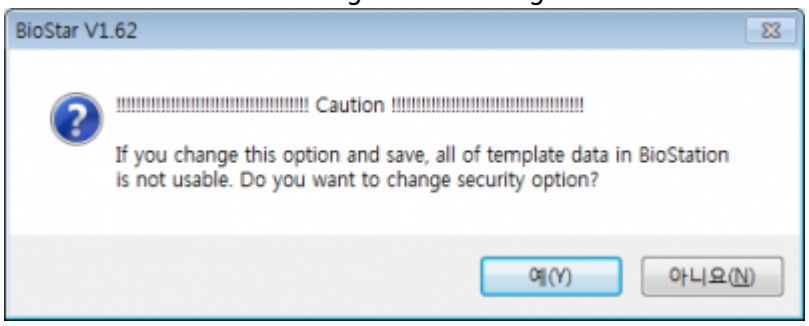
Fingerprint Encryption

Using AES Algorithm, all Suprema devices store encrypted fingerprint templates within the device. When the templates are transferred to BioStar Server, original templates are transferred without encryption. Therefore, BioStar supports **Fingerprint Encryption** feature which allows BioStar Client to encrypt fingerprint templates using encryption key for higher security and privacy.

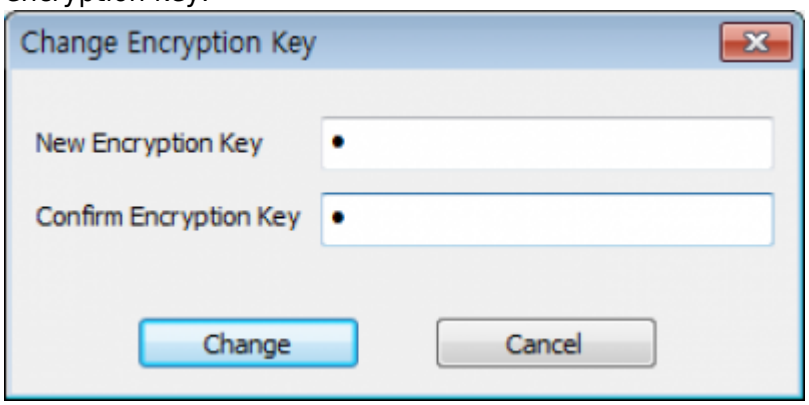
To encrypt fingerprint templates in BioStar:
1. Go to **Option** > **Fingerprint** > **Use Fingerprint Template Encryption**.



2. Click **Yes** to acknowledge the warning statement.



3. Enter the new encryption key and click **Change**. Encryption keys are not necessary and any combination of letters, numbers and special characters up to 32 characters are supported as the encryption key.



4. Click **Change** to close the windows then click **Save** to save changes.

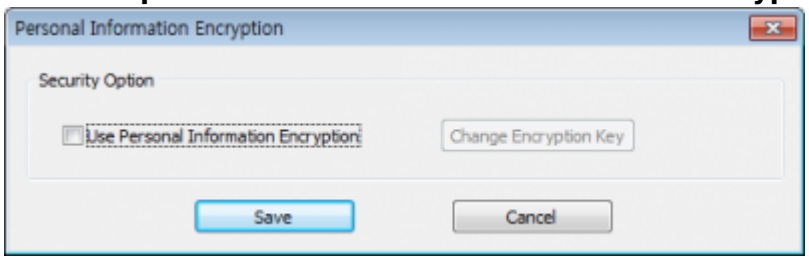
- It is not possible to reproduce a fingerprint image from the templates even the fingerprint encryption is not turned on.

Personal Information Encryption

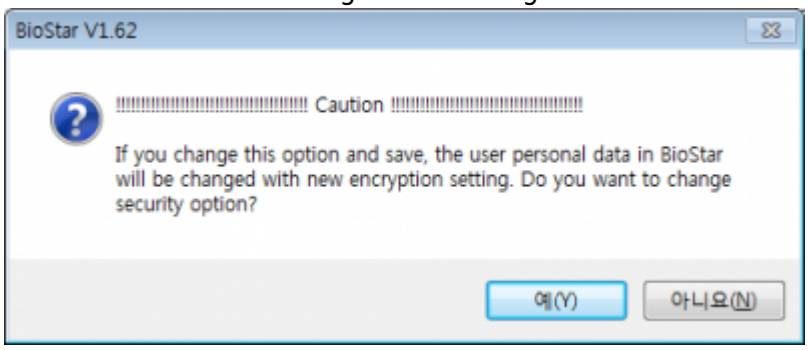
Using AES Algorithm, BioStar also supports **Personal Information Encryption** feature which allows BioStar to encrypt the confidential user information. This helps to protect valuable private user data against crimes.

To encrypt personal information in BioStar:

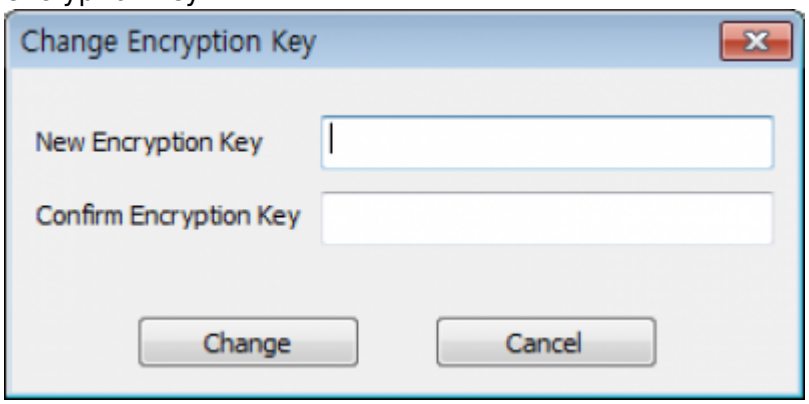
1. Go to **Option** > **User** > **Personal Information Encryption**.



2. Click Yes to acknowledge the warning statement.



3. Enter the new encryption key and click Change. Encryption keys are not necessary and any combination of letters, numbers and special characters up to 32 characters are supported as the encryption key.



4. Click **Change** to close the windows then click **Save** to save changes.