Table of Contents

Duplication Check of Fingerprint / Face / Visual Face for User Registration Process

If multiple users were enrolled same fingerprints or face, then there can be some security problem. To prevent user enrollment with duplicated fingerprints or faces, duplication check-in BioStar 2 is supported from BioStar 2 v2.7.8. You need to match BioStar 2 server version and device firmware versions to enable the '**Duplicate Check**' feature.

Supporting Devices:

- FaceStation 2 v1.3.0 and later
- FaceLite v1.1.0 and later
- BioStation 2 v1.8.0 and later
- BioStation L2 v1.5.0 and later
- BioStation A2 v1.7.0 and later
- BioLite N2 v1.2.0 and later
- FaceStation F2 v1.0.0 and later
- BioStation 3 v1.0.0 and later
- X-Station 2 v1.0.0 and later
- BioStation 2a v1.0.0 and later

1. Basic information of 'Duplicate Check' feature

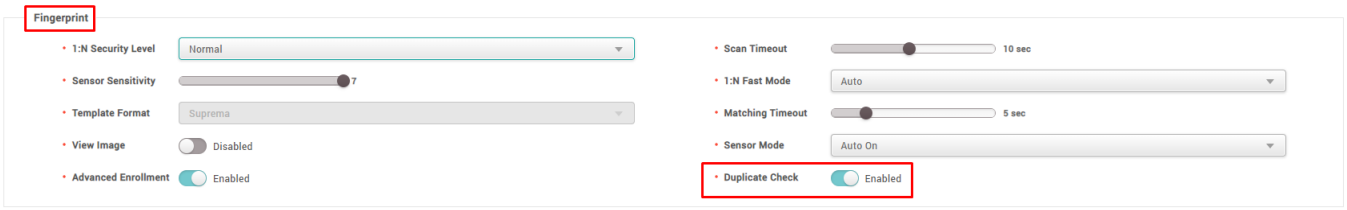
- You must use BioStar 2 v2.7.8 and supporting firmware to support this feature.
- It is supported when you use 1:N matching. (It is not supported when you use 1:1 matching)
- If one user registers the same fingerprints/faces, there will be no duplication check for those data.
- Duplication checking time and speed will differ by the location of fingerprint/face data stored.
- Even though there are many duplicated fingerprint / face / visual face users from current database, BioStar 2 and device will show 1 user information.
- You can enable this feature in the 'Slave' device, however, the function will not work.
- If someone tries to enroll a user with duplicate biometric information, the registration will fail. You can check the log through Monitoring and Settings—Audit Trail.

- The duplication-checking feature is supported when enrolling a user fingerprint or face from the device menu, not BioStar 2.

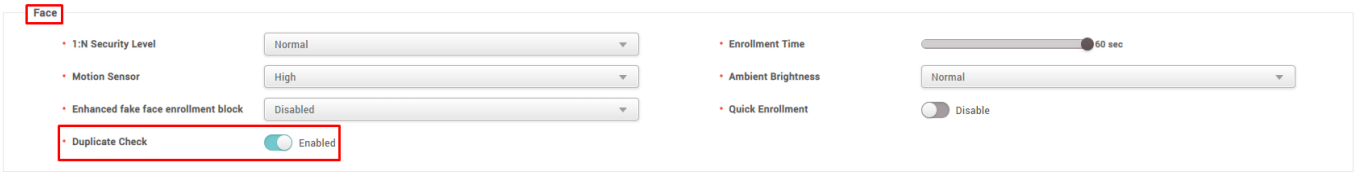
2. Configure from BioStar 2 server / client

- You can configure for fingerprint/face duplicate check, enable or disable.
- It does not have a limitation on whether your device has an LCD or not. (Only needs your firmware to support this feature.)
- BioStar 2 - Device - (Selected Device) - Fingerprint or Face/Visual Face - Duplicate Check - Enable / Disable
- The default setting in BioStar 2 server is 'disabled.'

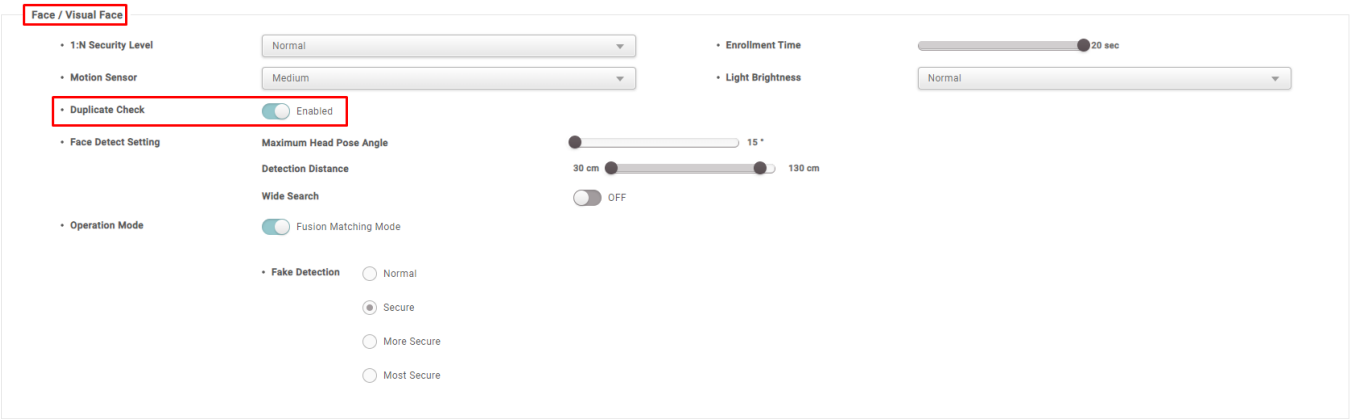
<Fingerprint Duplicate Check from BioStation 2>



<Face Duplicate Check from FaceStation 2>



<Visual Face Duplicate Check from FaceStation F2>



3. Configure from Suprema device

- You can configure for fingerprint/face duplicate check, enable or disable.
- It is only supported in LCD on devices.
- Device menu (ESC key) - Authentication - Fingerprint / Face - Operation - Duplicate Check
- The default setting in the device is 'enabled.' (You should manually set 'enabled' after you upgraded the firmware after you upgrading from 'not supported' version to 'supported' version.)