Table of Contents

Duplication Check of Fingerprint / Face for User Registration Process 1
1. Basic information of 'Duplicate Check' feature 1
2. Configure from BioStar 2 server / client 2
3. Configure from Suprema device 2

Duplication Check of Fingerprint / Face for User Registration Process

If multiple users had enrolled the same fingerprints or faces, then there can be some security problems. To prevent users from enrolling duplicated fingerprints or faces, duplication check in BioStar 2 is supported from BioStar 2 v2.7.8. You must match BioStar 2 server version and device firmware versions to enable **'Duplicate Check'** feature.

Supporting Devices:

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

1. Basic information of 'Duplicate Check' feature

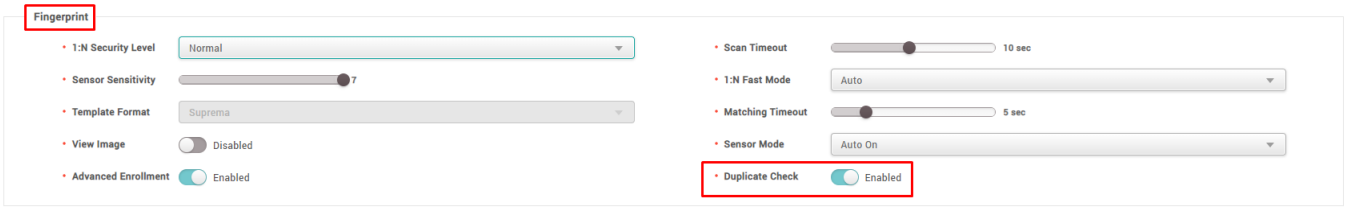
- To support this feature, you need to use both BioStar 2 v2.7.8 or above and supporting firmware.
- Supported for 1:N matching. (Not supported for 1:1 matching)
- If one user has registered the same fingerprints / faces, there will be no duplication checks for those data.
- Duplication checking time and speed will be different by the location of fingerprint / face data stored.
- Even though there are many duplicated fingerprints / faces in current database, BioStar 2 and device will show 1 user information.
- You can enable this feature in 'Slave' device however, the function will not work.
- If someone tries to enroll users with duplicated biometric information, the registration will fail. You can check the log at Monitoring and Settings - Audit Trail.

- Duplication checking feature is supported when you enroll a user fingerprint or face from device menu, not from BioStar 2.

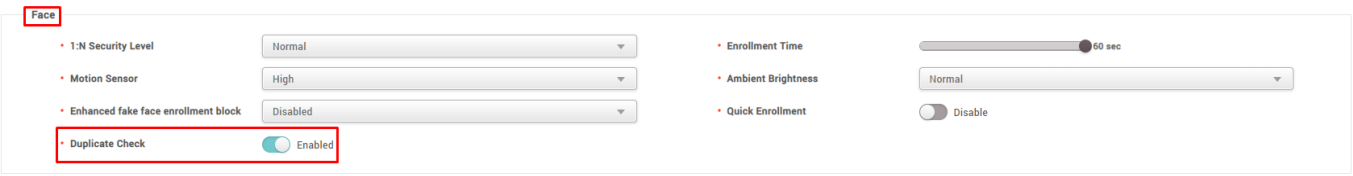
2. Configure from BioStar 2 server / client

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

<Fingerprint Duplicate Check from BioStation 2>



<Face Duplicate Check from FaceStation 2>



3. Configure from Suprema device

- You can configure for fingerprint / face duplicate check, enable or disable.
- It is only supported in LCD on devices. (Supported on : BioStation 2, BioStation L2, BioStation A2, BioLite N2, FaceStation 2, FaceLite, FaceStation F2)
- Device menu (ESC key) - Authentication - Fingerprint / Face - Operation - Duplicate Check
- Default setting in device is 'enabled'. (You should manually set 'enabled' after you upgraded the firmware after you upgrading from 'not supported' version to 'supported' version.)