BioStar X Hardening Guide

ADMINISTRATOR GUIDE

Version 1.0.0

English
EN 102.00.BSX

suprema
SECURITY & BIOMETRICS

CONTENTS

Core Principles of Secure Access Control 4

Principle of Least Privilege (PoLP) 4

Separation of Duties 4

Defense in Depth 4

Zero Trust Architecture Concepts 5

Server Hardening Guide 6

Operating System Configuration 6

User and Access Control 11

Network and Firewall 12

Service and Application Layer 15

Database and Data Protection 16

Monitoring and Auditing 19

Patch and Maintenance 21

Physical Security 22

BioStar X Hardening 24

System Security 24

Personal Data Security 34

Suprema Device Hardening 37

Keep device firmware up to date 37

Device event log retention and protection 38

Configure device administrator 39

Device network and local service hardening 40

Device-side operational hardening checklist 40

References 42

Default BioStar X network ports 13

Default security features in BioStar X 43

Compliance mapping (quick view) 44

External References 44

Appendices 45

Disclaimers 45

Copyright Notice 46

Core Principles of Secure Access Control

Security hardening for an access control system is not just about technical settings. It's about applying proven principles consistently across people, processes, and technology. BioStar X supports these principles by design, but administrators must configure and enforce them correctly.

Principle of Least Privilege (PoLP)

Users and services should be granted **only the permissions necessary** to perform their tasks. No more, no less.

- Admin accounts should be reserved for configuration and system changes, not daily operations.
- Operators should manage doors, users, and events but not security policies.
- Auditors should have full read-only visibility without the ability to change data.

> **Info**
> Limiting privileges reduces the impact of account compromise. An operator account hijacked by an attacker cannot alter encryption keys or disable logs.

Separation of Duties

Critical responsibilities should be **split across multiple roles**. No single person should have unchecked control over the system.

For example:

- One administrator manages system configuration, while another operator handles daily access requests.
- Auditors verify changes and monitor logs independently.

> **Info**
> Prevents insider abuse and ensures **checks and balances**. Even if one account is compromised, the attacker cannot control the entire system.

Defense in Depth

No single security measure is perfect. Instead, layers of security controls should be applied so that if one fails, others remain to protect the system.

- **Network layer**: Firewalls, VLAN segmentation
- **System layer**: Secure OS baseline, patches, antivirus
- **Application layer**: Strong passwords, MFA, encryption
- **Monitoring layer**: Logs, SIEM, alerting

> **Info**
> Attackers often look for weak links. Defense in depth ensures there's no single point of failure.

Zero Trust Architecture Concepts

Assume no device, user, or network can be trusted by default. This principle is known as "**never trust, always verify**."

- Every login should require authentication (MFA where possible).
- Device-to-server communication should always be encrypted.
- Internal traffic should be segmented and monitored as if it were external.

> **Info**
> Modern threats often originate inside the network (compromised laptops, phishing, malicious insiders). Zero Trust reduces reliance on "trusted perimeters" and enforces continuous verification.

These four principles form the **foundation of the hardening guide**. Every configuration recommendation in later chapters — from port settings to directory integration — is a practical application of **Principle of Least Privilege (PoLP)**, **Separation of Duties**, **Defense in Depth**, and **Zero Trust**.

Server Hardening Guide

This guide provides recommended practices to secure Windows environments hosting BioStar X. It covers system-level, network-level, and application-level controls designed to minimize vulnerabilities, reduce attack surfaces, and ensure compliance with organizational security policies.

- Applies to all Windows Servers (bare metal or VM) running BioStar X.
- Covers system configuration, network protection, access controls, monitoring, and patching.
- Intended for system administrators, security engineers, and deployment teams.

Operating System Configuration

Securing the operating system is the first step in the BioStar X hardening process. Unpatched operating systems, unnecessary services, and weak authentication settings are common attack vectors for any server workload, including BioStar X. Follow the guidance in this document to harden your Windows Server environment.

Use Windows Server LTS releases

Running BioStar X on an unsupported or outdated Windows version exposes the system to unpatched vulnerabilities. Microsoft provides Long-Term Servicing (LTS) releases of Windows Server that guarantee security updates, stability fixes, and support for 10+ years (5 years mainstream + 5 years extended). Choosing an LTS release ensures that your BioStar X server has the longest possible security support window with fewer disruptive feature updates.

> **Summary for Administrators**
> - Always deploy BioStar X on **Windows Server LTS editions** (2019 or 2022).
> - **Verify** the OS version after installation.
> - **Plan upgrades** before end-of-support dates.
> - **Keep automatic updates enabled** or connect to WSUS/SCCM.
> - **Document lifecycle** to avoid running on unsupported software.

Identify supported versions

The following LTS Windows Server editions are actively supported by Microsoft (as of May 2026):

- Windows Server 2019 (LTS) — Mainstream support: until January 2024 / Extended security support: until January 2029
- Windows Server 2022 (LTS) — Mainstream support: until October 2026 / Extended security support: until October 2031
- Windows Server 2025 (LTS) — Mainstream support: until November 2029 / Extended security support: until November 2034

> **Caution**
> Avoid Semi-Annual Channel (SAC) releases — they are short-lived and not intended for production workloads like BioStar X.

Check current OS version

- Press `Win + R`, type `winver`, and press Enter. This will display the edition and version.
- You can also run the following command in PowerShell to check the OS name and version:

  PowerShell

  ```
  systeminfo | findstr /B /C:"OS Name" /C:"OS Version"
  ```

Plan for upgrade if needed

- If the server is running Windows Server 2016 or older, you should plan a migration.
- Upgrading to 2019 or 2022 LTS ensures security updates and compatibility with modern TLS protocols (TLS 1.2/1.3).

> **Best Practice**
>
> Build a new VM or server with the supported OS. And install BioStar X fresh, then migrate configuration and database. This minimizes downtime and risk.

Ensure Windows update is configured

Enable **automatic updates** for security patches. Or if using Windows Server Update Services (WSUS) or System Center Configuration Manager (SCCM), ensure the host is properly enrolled.

Apply the latest Windows Updates and security patches

Before production deployment, apply the latest Windows updates and security patches to protect the system from known vulnerabilities.

Unpatched Windows servers are the **#1 attack vector** for ransomware, remote code execution, and privilege escalation exploits. Applying the latest security updates ensures the BioStar X host starts its lifecycle protected from all **known vulnerabilities**.

Check current patch level

- Open **Settings** → **Windows Update**, then click **Check for updates** to check the patch status.
- To check the 10 most recently installed patches using PowerShell, run the following command:

  PowerShell

  ```
  Get-HotFix | Sort-Object -Descending InstalledOn | Select-Object -First 10
  ```

> **Caution**
> If the most recent patch is older than 30 days, update immediately.

Update process

1. Run Windows Update manually.
2. Install all security and critical updates.

   > We recommend applying the latest patches without delay, even if the server is not yet in production mode.

3. Reboot when required.
4. Verify update status — run again until "You're up to date" is displayed.

Ongoing patch strategy

- **Monthly "Patch Tuesday"**: Microsoft releases new patches the 2nd Tuesday of every month.
- Apply patches **within 1–2 weeks** of release in production, after testing in staging if available.
- If you can't patch immediately, enable **compensating controls**: firewall restrictions, disable internet access, enhanced monitoring until patched.

Remove or disable unnecessary Windows features

Every enabled Windows feature increases the server's **attack surface**. Services like Print Spooler, Fax, or IIS are rarely needed on dedicated BioStar X hosts and have a history of critical vulnerabilities (e.g., PrintNightmare).

> *e.g., Internet Explorer, SMBv1, legacy components*

1. Open Start → **Server Manager** → **Manage** → **Remove Roles and Features**.
2. Review installed roles (e.g., File Services, IIS, Print Services).
3. Remove roles not required by BioStar X.
4. Only keep **.NET Framework Features** and **Desktop Experience** if needed by your admin workflow.
5. Open `services.msc` and set unneeded services (e.g., Fax, Remote Registry, Bluetooth, SMBv1) to **Disabled**.

> **Best Practice**
>
> Keep the host **dedicated** to BioStar X only. No additional workloads.

Ensure Windows Defender is enabled and up-to-date.

Windows Defender (built-in antivirus) protects against malware and ransomware. Disabling it leaves the host exposed.

1. Open **Settings** → **Privacy & security** → **Windows Security** → **Virus & threat protection**.
2. Confirm **Manage settings** → **Real-time protection** is enabled.
3. Confirm **Cloud-delivered protection** and **Automatic sample submission** are enabled.
4. Keep Security intelligence (sometimes referred to as definitions) updated. Usually automatic via Windows Update.

> **Caution**
> If using a 3rd party antivirus, ensure only **one antivirus solution** is running to prevent conflicts.

Enable BitLocker to protect against physical theft

If an attacker gains physical access to the server (e.g., stolen disk, VM snapshot, backup media), unencrypted drives allow direct access to sensitive data such as credentials, logs, and biometric information. BitLocker provides full-disk encryption to protect data at rest.

Recommendation

- Enable BitLocker on:
  - OS drive (C:)
  - All data drives storing: BioStar X database, logs, and backups
- Use TPM + PIN where possible for stronger protection

Step-by-step

1. Open **Control Panel** → **System and Security** → **BitLocker Drive Encryption**.
2. Click **Turn on BitLocker** for each drive.
3. Choose authentication method: **TPM** (default) or **TPM + PIN** (recommended).
4. Save recovery key: **Active Directory / Azure AD** (preferred), or **secure vault** (do NOT store locally).
5. Choose encryption mode: **XTS-AES 256-bit** (recommended).
6. Start encryption.

Monitor BitLocker status

Run the following command to check BitLocker status.

PowerShell

```
Get-BitLockerVolume
```

> **Info**
> BitLocker protects **data at rest only**. It does NOT replace database encryption or TLS encryption.

Enforce secure authentication policies

Weak local accounts or cached credentials make the server vulnerable to brute-force or privilege escalation.

1. Open **Local Security Policy** (`secpol.msc`).
2. Configure the following **Account Policies** → **Password Policy**:
   - **Minimum password length**: 12+ characters
   - **Password must meet complexity requirements**: Enabled
   - **Maximum password age**: 90 days
3. Configure the following **Account Policies** → **Account Lockout Policy**:
   - **Account lockout threshold**: 5 attempts
4. Disable or rename default **Administrator** account.
5. Require multi-factor authentication (MFA) for RDP or remote admin access.

Enforce Group Policy settings for security baselines

Microsoft's **Security Compliance Toolkit (SCT)** provides downloadable **Group Policy Objects (GPOs)** that align with security baselines. These baselines reduce misconfiguration risks and ensure BioStar X runs on a hardened Windows OS.

1. Download the latest Microsoft Security Compliance Toolkit.
2. Select the baseline for your OS version: **Windows Server 2019** or **2022 Security Baseline**.
3. Import baseline GPOs into **Group Policy Management Console (GPMC)**

   Open `gpmc.msc` → Right-click **Group Policy Objects** → Click **Import Settings**.
4. Link the baseline GPO to the **BioStar X server OU** in Active Directory (or apply locally if standalone).
5. Review critical settings:

   account lockout, audit logging, network security (SMB signing, LDAP signing, disabling NTLM fallback), LSA Protection.
6. **Test in staging first**, confirming BioStar X compatibility and then deploy to production.

Disable Remote Desktop if not required

RDP is a common attack vector (brute force, credential stuffing).

If not required

Select **Don't allow remote connections to this computer** in **System Properties** → **Remote**

Harden if needed

If Remote Desktop is required, apply the following security hardening measures to mitigate risks.

- Restrict to VPN or LAN only.

- Require Network Level Authentication (NLA).
- Change default RDP port (3389 → custom).
- Monitor with event logs & alerts.

User and Access Control

After hardening the operating system, the next step is to control **who** can access the system and **what** they can do. Misconfigured account permissions, weak passwords, and neglected built-in accounts are the most common paths for attackers to escalate privileges on a BioStar X server. Follow the guidance in this document to strengthen user and access controls.

Enforce least privilege

- Create separate user groups in Active Directory or Local Users and Groups.
- Assign file system and application permissions based on these groups.
- Configure BioStar X roles within the application to mirror the OS-level least-privilege model.

Restrict local administrative privileges

- Use `lusrmgr.msc` to remove unnecessary accounts from the Administrators group.
- Assign least privilege — use standard user accounts for normal operation, admin only when required.
- If domain-joined, apply Group Policy Restricted Groups to enforce consistent permissions.

Enforce strong authentication

- Configure Group Policy to require complex passwords (minimum 12–15 characters, mix of upper/lowercase, numbers, symbols).
- Set password expiration (e.g., every 90 days) and limit reuse.
- Configure Account Lockout Policy to lock accounts after several failed attempts.
- For remote access or privileged accounts, enforce Multi-Factor Authentication (MFA).

Step-by-step

1. Open **Local Group Policy Editor** (`gpedit.msc`).
2. Navigate to **Computer Configuration** → **Windows Settings** → **Security Settings** → **Account Policies** → **Password Policy**.
3. Configure password length, complexity, and history.
4. Set lockout duration and threshold under **Account Lockout Policy**.

Manage built-in accounts

Open **Local Users and Groups** (`lusrmgr.msc`).

- Right-click the Administrator account and then rename it (use a non-obvious name).
- Disable Guest account unless explicitly required.
- Regularly audit accounts with `net user` in PowerShell.

Session management

- Configure automatic lockout after 15 minutes of inactivity.
- Prevent simultaneous logins with the same account, if possible.
- Limit idle remote sessions.

> **Info**
> **Local Group Policy Editor** (`gpedit.msc`) → **Computer Configuration** → **Windows Settings** → **Security Settings** → **Local Policies** → **Security Options** → **Interactive logon: Machine inactivity limit** (e.g., 900 seconds = 15 minutes)

Auditing and monitoring

- Enable auditing for login attempts, privilege use, and account management.
- Forward logs to a **SIEM** or central log collector.
- Review security logs regularly for anomalies.

> **Info**
> **Local Group Policy Editor** (`gpedit.msc`) → **Computer Configuration** → **Windows Settings** → **Security Settings** → **Advanced Audit Policy Configuration**
>
> Enable categories: **Logon/Logoff**, **Account Management**, **Privilege Use**.

Network and Firewall

Securing the network perimeter and host-based firewall settings is critical for protecting BioStar X against unauthorized access and lateral movement in the network. Since BioStar X can expose services over HTTPS, REST, gRPC, WebSockets, and Thrift, it's important to strictly control inbound and outbound connections.

Enable and configure Windows Defender Firewall

A properly configured firewall ensures that only explicitly authorized traffic reaches BioStar X, significantly reducing attack surface.

Default BioStar X network ports

Service	Purpose	Default Port(s)
BioStar X Core Web Service	HTTPS / Web Interface	5002
	Thrift RPC	9310
BioStar X Core Service	WebSocket	9002
	FastCGI	9000
	API	9010
	RPC	51218
Unified Gateway Service	HTTPS	443
Coordinator Service	Client Communication	21810
Main Server	TCP Server	51212
	SSL Server	51213
	gRPC	51219
Cache Service	Client	10800
	Communication	47500
	Discovery	47100

Info

When Multi Communications Server is deployed, it uses the same Main Server communication ports (`51212`, `51219`). Administrators should ensure these ports are reachable between the Multi Communications Server and the Main Server according to the deployment topology.

Step-by-step

1. Open **Windows Defender Firewall with Advanced Security** (`wf.msc`).
2. Go to **Inbound Rules** and remove or disable rules that are not required.
3. Create explicit allow rules for:
   - **Unified Gateway HTTPS** (`443`): external/public if required.
   - **Core Web Service HTTPS** (`5002`): but ideally proxied through 443.

- Internal-only ports (gRPC `51219`, Cache `10800` / `47500` / `47100`, Coordinator `21810`, Thrift `9310`): allow only from localhost or trusted subnets.

4. Set all other inbound traffic to **Block**.
5. Go to **Outbound Rules** and restrict to known trusted endpoints.

> **Caution**
> Avoid broad "Allow All" rules. Changing default ports provides minor obscurity benefits but does not replace firewall enforcement.

Limit remote access

- Restrict Remote Desktop (RDP) to authorized administrators only.
- If RDP is required: use NLA, place server behind a VPN or jump host.
- If not needed: disable it (**System Properties → Remote settings**).

Secure network segmentation

- Place BioStar X servers in a dedicated VLAN or DMZ separated from user networks.
- Only allow communication between BioStar X and required systems (e.g., database server, API consumers, readers).
- Restrict management access (RDP, SSH) to admin subnets only.

> **Best Practice**
>
> Combine segmentation with host firewalls for **defense in depth**.

Harden network protocols

Disable SMBv1

PowerShell command to disable SMBv1:

PowerShell

```
Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
```

Enforce TLS 1.2+

- Registry path: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols`

  Disable SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1.

- Verify with IIS Crypto or `nmap --script ssl-enum-ciphers`.

> **Caution**
> Test in staging before disabling protocols to avoid compatibility issues.

Network intrusion detection & monitoring

- Deploy IDS/IPS (Snort, Suricata, or commercial).
- Enable Windows Defender Firewall logging for dropped packets and allowed connections.
- Forward logs to SIEM for centralized monitoring.

> **Info**
> Firewall log path: `%systemroot%\system32\LogFiles\Firewall\pfirewall.log`

Service and Application Layer

The Service and Application Layer focuses on securing the software components and runtime environment of BioStar X.

Apply principle of least privilege to services

- Run BioStar X services under dedicated service accounts instead of Local System or Administrator.
- Grant only the minimal rights required (logon as a service, read/write specific directories).
- Use separate accounts for each BioStar X service component where possible.

Step-by-step

1. Create a dedicated local user account for BioStar X services.
2. Open **Services.msc** → Right-click the BioStar X service → **Properties** → **Log On** tab.
3. Assign the dedicated account.
4. Apply file system ACLs so the account can only access necessary directories.
5. Deny interactive logon rights for these accounts.

> **Caution**
> Using shared accounts between multiple services makes it harder to audit breaches.

Secure application configuration files

- Restrict access to configuration files that contain secrets (e.g., database connection strings, API keys).
- Use Windows Data Protection API (DPAPI) or Key Vault solutions if supported.

- Store secrets separately from binaries; avoid hard-coding.

Protect encryption key files (`util/` directory)

- Restrict NTFS permissions so only the BioStar X service account has read access.
- Deny access to standard users and interactive logins.
- Back up the `util/` directory securely before upgrades (offline storage recommended).

> **Caution**
> Loss or compromise of these files may result in data loss or unauthorized decryption.

> **Best Practice**
>
> Rotate stored secrets (DB passwords, API keys) periodically.

Maintain application runtime components

- Keep BioStar X and its dependent runtime components (e.g., Visual C++ Redistributables) up to date.
- Subscribe to vendor advisories for patches.
- Document update procedures to avoid downtime.

Application whitelisting

- Use Windows Defender Application Control (WDAC) or AppLocker to allow only trusted binaries.
- Block execution from temporary directories (e.g., `%TEMP%`, `%APPDATA%`).

Step-by-step

1. Open `Local Security Policy → Application Control Policies → AppLocker`.
2. Define rules for executable, script, and DLL paths.
3. Allow signed BioStar X binaries.
4. Deny execution from user-writable directories.
5. **Deploy in Audit Mode first** to test, then enforce.

Database and Data Protection

BioStar X requires a database to store sensitive information such as user credentials, access logs, and configuration data. Depending on the deployment, either **MariaDB** (11.4) or **Microsoft SQL Server** may be used.

Enforce authentication and access control

- Require authentication for all database connections.
- Use dedicated database accounts for BioStar X, not shared or default accounts.
- Assign the least privilege role needed (read/write for application data, no schema modification).
- Regularly audit database accounts for unused or over-privileged users.
- Remove unused or outdated database user entries, especially after IP or infrastructure changes.

> **Caution**
> Never allow BioStar X to connect using `sa` or equivalent superuser accounts.

Encrypt data in transit

MariaDB

my.cnf

```
[mysqld]
require_secure_transport=ON
ssl_cert=/etc/mysql/server-cert.pem
ssl_key=/etc/mysql/server-key.pem
ssl_ca=/etc/mysql/ca-cert.pem
```

Verify:

SQL

```
SHOW VARIABLES LIKE '%ssl%';
```

SQL Server

1. Open **SQL Server Configuration Manager**.
2. Go to **SQL Server Network Configuration → Protocols for MSSQLSERVER**.
3. Enable **Force Encryption**.
4. Install a trusted certificate on the server.

Encrypt data at rest

MariaDB

- Enable `file_key_management` plugin for encryption at rest.
- Define encryption keys in a secure keyfile.

- Apply encryption per table if full TDE is not available.

> **Caution**
> Slight performance overhead (usually 3–5%). If you move/restore the DB on another server, you'll need the certificate and keys. BioStar X's Restore function does not support encrypted backups — this will need to be done manually.

SQL Server TDE

SQL

```
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'StrongP@ssw0rd!';
CREATE CERTIFICATE MyServerCert WITH SUBJECT = 'BioStarX';
CREATE DATABASE ENCRYPTION KEY WITH ALGORITHM = AES_256 ENCRYPTION BY SERVER CERTIFICATE MyServerCert;
ALTER DATABASE biostarx_ac SET ENCRYPTION ON;
```

Enable database auditing

MariaDB

SQL

```
INSTALL SONAME 'server_audit';
SET GLOBAL server_audit_logging=ON;
SET GLOBAL server_audit_events='CONNECT,QUERY_DML,QUERY_DDL';
```

SQL Server

SQL

```
CREATE SERVER AUDIT BioStarX_Audit TO FILE (FILEPATH = 'C:\AuditLogs\');
CREATE SERVER AUDIT SPECIFICATION BioStarX_Spec FOR SERVER AUDIT BioStarX_Audit ADD (FAILED_LOGIN_GROUP);
ALTER SERVER AUDIT BioStarX_Audit WITH (STATE = ON);
```

Backup and secure storage

- Perform regular encrypted backups of the BioStar X database.
- Store backups on a separate secure server, not the same host.
- Test backup restores periodically.
- Store backups on BitLocker-encrypted volumes.

MariaDB

Bash

```
mariadb-dump --all-databases --ssl --result-file=/secure/backups/biostarx.sql
gpg -c /secure/backups/biostarx.sql
```

> **Caution**
> BioStar X Backup function (manual or scheduled) is unencrypted. BioStar X Restore function does not support encrypted backup.

SQL Server

SQL

```
BACKUP DATABASE biostarx_db TO DISK = 'D:\backups\biostarx_db.bak'
WITH ENCRYPTION (ALGORITHM = AES_256, SERVER CERTIFICATE = MyServerCert);
```

Restrict remote access

MariaDB

my.cnf

```
bind-address=127.0.0.1
```

SQL Server

Configure firewall rules to allow connections only from the BioStar X application server.

Monitoring and Auditing

Monitoring and auditing ensure visibility into the security posture of BioStar X. Effective auditing requires enabling logs at the **operating system**, **application**, and **database** levels, centralizing them, and reviewing them regularly.

Define logging policy

Establish a logging policy that specifies what events must be logged, retention periods, and who is responsible for review.

You must log at minimum the following event types:

- Authentication attempts (success/failure)
- Privilege changes
- Configuration changes
- Database access
- Firewall activity

> **Info**
> **Retention**: typically 90–180 days locally, longer in centralized systems.

Enable Windows event logging and monitoring

- Open Event Viewer and ensure logging is enabled for: Security, Application, System.
- Configure log size. It is recommended to set the security log to at least 1Gb.
- Set up auditing for the following policies in **Local Security Policy** (`secpol.msc`) → **Local Policies** → **Audit Policy**.

> *Logon events, privilege use, policy change, account logon, object access.*

Centralized log forwarding and SIEM integration

- Forward logs to a central SIEM or log management system.
- Supported options: Splunk, Elastic Stack, Microsoft Sentinel, or Windows Event Forwarding (WEF).

> **Best Practice**
>
> Encrypt logs in transit (TLS) to prevent interception or tampering.

Enable application-level auditing

- From BioStar X → **Settings** → **Server**, find **System Log Level Settings**.
- Log file location: `[BioStar X Install Path]\logs\acs.log`
- Set permissions so only the BioStar X service account and administrators can access.
- Forward logs to SIEM or central logging solution.

Enable database auditing

- **MariaDB**: Use the Audit Plugin (`server_audit`).
- **SQL Server**: Use SQL Server Audit (logs to file or event log).
- Forward to central log system.

> **Info**
> For more information on enabling database auditing, see Database and Data Protection.

Monitor firewall and network activity

- In **Windows Defender Firewall with Advanced Security** (`wf.msc`) → **Properties** → **Logging**, enable logging of dropped

packets.

- Store logs at `%systemroot%\system32\LogFiles\Firewall\pfirewall.log`.
- Forward logs to SIEM.
- Deploy IDS/IPS (Snort, Suricata, Zeek) to detect anomalies.

> **Caution**
> Firewall logs grow quickly — implement log rotation and secure storage.

Review and alerting

Establish automated alerts for critical events:

- Multiple failed logins
- Privilege escalation
- Unexpected service startup/shutdown
- Database schema modifications

Conduct manual log reviews periodically.

Patch and Maintenance

After hardening a server, you must maintain that posture. New vulnerabilities are continuously discovered, and unpatched systems become increasingly exposed to risk over time. This document explains how to maintain the security baseline of the BioStar X server through regular patching, vulnerability scanning, and asset management.

Backup and restore security configuration

PowerShell

```
# Export Group Policy settings
secedit /export /cfg C:\backup\secpol.cfg

# Backup Windows Firewall rules
netsh advfirewall export "C:\backup\firewall.wfw"
```

Establish patch management policy

- Define a formal patching policy covering operating system, database engines, BioStar X software, and third-party dependencies.
- Specify timelines (e.g., OS patches within 2 weeks, application patches within 1 month).
- Include rollback and recovery procedures if a patch causes instability.

> **Caution**
> Before patching BioStar X bundled third-party dependencies, confirm with Suprema Global Technical Support Team that the update is supported. Try it first in a staging or VM environment.

Maintain BioStar X software updates

- Keep BioStar X updated to the latest supported version provided.
- Subscribe to release notes and advisories at https://www.supremainc.com/en/support/main.asp.
- Test new releases in a staging environment before production rollout.

Keep database engines up to date

- Apply updates to MariaDB 11.4 or Microsoft SQL Server according to Suprema's security advisories.
- Avoid running unsupported versions.

Manage dependencies and runtime components

- Patch supporting frameworks like Visual C++ Redistributables and Java runtimes.
- Maintain reverse proxy/WAF software (if used).
- Update quarterly or whenever advisories are published.

Perform regular vulnerability scanning

- Run vulnerability scans on BioStar X hosts quarterly (or monthly in high-security environments).
- Tools: Nessus, OpenVAS, Qualys, or Microsoft Defender for Endpoint.
- Schedule scans after patch cycles and track remediation in ticketing systems.

Maintain asset and patch inventory

- Keep an inventory of all BioStar X servers: OS versions, database versions, and patch levels.
- Use automated tools (e.g., SCCM, Intune, Ansible) where possible.
- Review inventory quarterly.

Physical Security

Physical security controls prevent unauthorized individuals from gaining direct access to the servers or storage hosting BioStar X.

Secure server location

- Host BioStar X servers in a physically secured data center or locked server room.
- Access should be limited to authorized IT staff only.
- Use surveillance (CCTV) and access logs for server rooms.
- Place servers in locked racks or cages; maintain visitor logs.

Protect portable and backup media

- Store backup drives or tapes in secure, access-controlled areas.
- Use encryption for all removable storage containing BioStar X data.
- Encrypt backups with AES-256 before transport.

> **Best Practice**
>
> Use **cloud-based encrypted backups** to reduce reliance on physical media.

Secure BIOS/UEFI settings

- Set BIOS/UEFI passwords to prevent unauthorized configuration changes.
- Disable booting from external devices (USB, DVD).
- Enable Secure Boot if supported.

> **Caution**
> Keep BIOS/UEFI passwords documented in a secure vault. Losing them can block legitimate maintenance.

Protect against device theft

- Enable full-disk encryption using BitLocker on all system and data drives.
- For more information on configuring BitLocker, see Operating System Configuration.
- Use TPM + PIN for enhanced protection where applicable.
- Use cable locks or secured racks for non-data-center deployments.

Environmental controls

- Ensure server rooms have stable temperature, humidity, and power supply (UPS).
- Protect against fire (extinguishers or suppression systems such as FM200 or inert gas).
- Monitor temperature/humidity with sensors.

BioStar X Hardening

Securing BioStar X requires protecting two interconnected layers: the system itself and the personal data it stores.

- **System Security** reinforces the application through default admin account changes, role-based access control, strong authentication, and encrypted device communication.
- **Personal Data Security** protects sensitive user credentials and biometric data through database encryption and minimal storage practices.

Implementing both layers ensures regulatory compliance (GDPR, ISO 27001, etc.) and minimizes breach risk.

System Security

After hardening the server security on BioStar X server, the next step is securing the BioStar X application itself. Default admin accounts, weak passwords, and unencrypted device communication become paths to directly compromise the system while bypassing infrastructure-level security. This document explains how to establish a security baseline at the application layer through BioStar X authentication, role management, device encryption, and backup strategies.

Change default admin login ID and password

Change the default **Administrator** login ID (`admin`) and assign a strong, unique password immediately after installation.

Default credentials are one of the most common entry points for attackers. Since every BioStar X installation ships with a predefined Administrator account (UID: 1), leaving it unchanged makes the system predictable and highly vulnerable to brute-force or dictionary attacks.

1. Log in with the default admin account (Login ID: `admin`).
2. Navigate to **User**.
3. Double-click the **Administrator** account.

   > *User Name: Administrator, UID: 1*

4. In the edit user page, find the **Permission** section:
   - **Login ID**: Change from `admin` to a unique, non-obvious user ID. Avoid names like `root` , `system` , or your company name.
   - **Password**: Change to a secure password. By default, BioStar X enforces **Medium strength** passwords. Passwords must be 8–32 characters and include both letters (uppercase/lowercase) and numbers.
5. Click **Save** at the top right of the screen.
6. Log out, then log back in with the **new credentials** to confirm the change.

Best Practice

- Do **not** use personal names or simple patterns (`admin1` , `company2025`).
- Store the new credentials in a secure password manager or enterprise vault.
- Create a **secondary administrator account** for emergency use.
- Regularly review **audit logs** for Administrator login attempts.

Access separation

Enforce strict separation of roles inside BioStar X by assigning **Administrator**, **Operator**, and **Auditor** accounts with clearly defined privileges.

A single super-user account for all tasks introduces unnecessary risk. By separating roles, you:

- Reduce the chance of accidental misconfiguration.
- Limit insider threats (no single user has unchecked power).
- Improve auditability and compliance (clear accountability per role).

This practice aligns with **least privilege** and **separation of duties** — two core principles in ISO 27001, NIST, and other frameworks.

Recommended approach after installation

1. **Rename & Secure the Default Admin**:

   Treat it as a **break-glass only emergency account**. For more information, see Change default admin login ID and password.

2. **Create Named Role Accounts**:

   - **Admin Role**: For system configuration and role management. Limit to **1–2 trusted people**.
   - **Operator Role**: For daily operations. No access to system security settings or audit logs.
   - **Auditor Role**: Read-only access to logs, reports, and configurations. No ability to change settings.

3. **Enable Multi-Factor Authentication (MFA)**:

   Enforce MFA for all role accounts. For more information, see Multi-factor authentication.

4. **Use Custom Account Levels (if required)**:

   - Navigate to **Settings** → **Account**, and then click **Add Custom Level**.
   - Configure granular access across User Groups, Device Groups, Doors Groups, etc.
   - Select the **Edit/Read** or **Read** permission for each menu item in **Admin Menu Settings**.

Step by step example: Creating a custom auditor role

1. Go to **Settings** → **Account**.
2. Click **Add Custom Level**.

3. Enter **Name** as `Auditor`, add description.
4. Under **Admin Menu Settings**, set:
   - **User**: **Read**
   - **Monitoring**: **Read**
   - **Data**: **Read**
   - **Dashboard**: **Read**
   - **Settings**: Do not select.
5. Click **Apply**, then assign this role to designated auditor accounts.

> **Best Practice**
> - Assign **unique accounts per individual** — avoid shared logins.
> - Review account roles quarterly and remove unused accounts.
> - Keep the renamed built-in Administrator account for emergencies only.

Enforcing strong password policy

Configure BioStar X to enforce strong password policies for all user accounts.

Password policy options in BioStar X

- **Password Level**
  - **Low**: You can enter up to 32 characters.
  - **Medium**: When setting a password, a combination of 8 to 32 alphabetic characters (uppercase or lowercase) and numbers is required.
  - **Strong**: When setting a password, a combination of 10 to 32 alphabetic characters (uppercase and lowercase, including at least one uppercase letter), numbers, and special characters is required.
- **Maximum Password Age**: Can be set from 1 to 180 days.
- **Maximum Invalid Attempts**: If you enter the password incorrectly more than the set number of times, you will not be able to log in for the time limit. The default is 100 attempts within 10 minutes, and it is recommended to **reduce it to 5–10 attempts within 15 minutes**.
- **Maximum Password Change Limit**: To limit the number of password changes a user can make in a day.

Step by step: Strengthening password policy

1. Go to **Settings** → **System** → **Security**.
2. Under **Login Password**, configure:
   - **Password Level**: **Strong**
   - **Maximum Password Age**: Enable, set to **90 days**
   - **Maximum Invalid Attempts**: Enable, set to **5 attempts** per **15 minutes**

- **Maximum Password Change Limit**: Enable, set to **5 times** maximum

3. Click **Apply** at the bottom right of the screen.

Communicate new policies to all users.

Session security

Path: Settings → System → Security → Session Security

Disable **Simultaneous Connection Allow** to ensure that each account can only be used for one active session at a time.

- **Active**: Multiple concurrent logins with the same credentials are allowed.
- **Inactive**: Only one login per account is permitted. A new login automatically logs out the previous session.

> **Caution**
>
> - Account sharing goes undetected — impossible to know who performed which action.
> - Attackers who gain stolen credentials can log in unnoticed while the legitimate user is still active.
> - Audit logs lose their value because they cannot attribute actions to specific individuals.

Multi-factor authentication

Enable multi-factor authentication for all high-privilege accounts (Admin, Operator) in BioStar X by requiring an additional biometric fingerprint factor.

> **How it works in BioStar X**
>
> - MFA is implemented using a fingerprint scanner (Suprema BioMini or BioMini Plus 2).
> - After users enter their Login ID and Password, the system prompts for a fingerprint scan.

> **Caution**
>
> - If the Admin account has MFA enabled and the fingerprint component fails, you may get locked out.
> - MFA is not supported when logging in via Cloud interfaces.
> - MFA can't be enabled for accounts authenticated via Active Directory or non-supported services.

Step-by-step

1. Connect and install the fingerprint scanner on the BioStar X server or client machine.
2. In the BioStar X, go to **User**.
3. Open the user's profile and ensure fingerprint is enrolled.
4. Set **Multi-Factor Auth for Login** to **Use** in the **Permission** section.
5. Click **Save** at the top right of the screen to apply the changes.

Test by logging in: enter valid credentials, then scan your fingerprint to gain access.

Best Practices & Safety Measures:
- Enroll backup fingerprints (alternate finger) to mitigate scanner failures.
- The original built-in Administrator ("break-glass" account) should have fallback recovery in case biometric hardware fails.
- Document MFA-enabled accounts and maintain a recovery mechanism.

Secure communication with device

Enable **Secure communication with device** to encrypt traffic between BioStar X and connected devices using digital certificates (TLS/SSL-style).

Option A: Server-generated certificates (default)

BioStar X generates a certificate and automatically provisions it to devices.

Caution
If disabled and re-enabled, a new certificate is generated, which may require manual device resets.

Option B: External certificates (recommended for enterprise use)

- Upload your organization's certificate chain and private key.
- Provides easier integration with enterprise PKI.

Step-by-step

1. Log in to BioStar X with an Administrator account.
2. Go to **Settings** → **System** → **Security** → **Advanced Security Settings**.
3. Set **Secure communication with device** to **Use**.
4. If using external CA certificates, set **Use external certificates** to **Use**.
    - Upload the Root CA, Public certificate, and Private key.
5. Apply and verify that devices reconnect successfully over secure channels.

Best Practice
- Always use **strong keys** (RSA 2048+ or ECC equivalent).
- Use certificates with proper **CN/SAN values** that match how devices connect (hostname or IP).
- Rotate certificates before expiry; keep a renewal calendar.

Note on log upload

If **Log Upload** is **Manual**, you risk **delayed event visibility** or **gaps in audit trails**. Keep **Log Upload** to **Automatic** whenever possible.

Device hashkey management

Enable **Device Hashkey Management** to manually control the encryption key used between BioStar X and devices. This activates tamper-resistance. Devices can automatically wipe critical data if physical tampering is detected.

Info

While Secure communication with device protects data in transit, **Device Hashkey Management** goes further:

- It ensures the **data encryption key is controlled by the administrator**, not generated automatically.
- It activates **tamper defense**. If a device detects unauthorized opening or manipulation, it deletes stored users, logs, and its encryption key.

Caution

- Manual key management **cannot be applied if non-administrator users have login PW or PIN**.
- Remove such logins before enabling.

Step-by-step

1. Log in to BioStar X with an Administrator account.
2. Go to **Settings** → **System** → **Security** → **Advanced Security Settings**.
3. Set **Device Hashkey Management** to **Use**.
4. Read and acknowledge the warning pop-up.
5. Remove any non-admin PW/PIN logins from devices before applying.
6. Rotate the encryption key and administrator password when prompted.
7. Confirm devices can still sync users, logs, and events.
8. Document the key change (date, responsible admin, next scheduled rotation).

Best Practice

- Rotate the device hashkey on a regular cycle (e.g., annually or semi-annually).
- Document all rotations and store in a secure vault.
- Test tamper events in a lab/staging device.
- Pair with Secure communication with device for full defense-in-depth.

System backup

Use the built-in **System Backup** feature to regularly back up BioStar X's database, system settings, and key values.

> **Caution**
>
> - If BioStar X and MSSQL are installed on different servers, **System Backup/Restore is not available**.
> - BioStar X Backup function (manual or scheduled) is **unencrypted**.
> - BioStar X Restore function does not support encrypted backup.

Manual backup settings

Path: **Settings** → **System** → **System Backup**

- **Backup File Path**: Define the directory. The path must exist and have appropriate write permissions.
- **Number of Backup Files to Keep**: Range 1–100. Recommendation: at least **7–10 rotating backups** for daily schedules.
- **Backup Now**: Trigger an immediate backup on demand. Useful before upgrades or major changes.

Automatic system backup

- **Frequency**: **Daily** / **Weekly** / **Monthly**
- **Time**: Specify the time. Follows BioStar X server time zone.

> **Best Practice**
>
> For production, **daily backups at off-peak hours.**
>
> > *e.g., 02:00 local time*

Configuring automatic backups

1. Go to **Settings** → **System** → **System Backup**.
2. Under **Automatic System Backup**, set:
   - **Frequency**: **Daily**
   - **Time**: 02:00 (or another off-peak time)
   - **Number of Backup Files to Keep**: 30
3. Click **Apply** to save the settings.
4. Verify backups are created by checking the target directory.
5. Periodically test **restore procedures** in a staging environment.

Caution

Ensure server is protected by UPS. Do not interrupt operations while "In Progress" status is displayed. Interruptions may cause database corruption.

Directory Integration

Directory Integration allows BioStar X to connect with enterprise identity systems such as **Entra ID (Azure AD)** or **Microsoft Active Directory (AD)**.

- **Stronger security**: Enterprise policies for password rules, MFA, and conditional access are automatically applied to BioStar X.
- **Centralized control**: User lifecycle is handled in Entra ID/AD, reducing risk of stale accounts.
- **Audit and compliance**: All user actions are tied back to corporate accounts.

Info

Directory Integration requires the **Advance license** to be active.

Best Practice

- Use **dedicated Entra ID/AD service accounts** with limited privileges.
- Restrict synchronization to **only relevant groups**.
- Always use **LDAPS** for Active Directory connections.
- Periodically review synchronized accounts for stale entries.

Microsoft Entra ID — Step-by-step

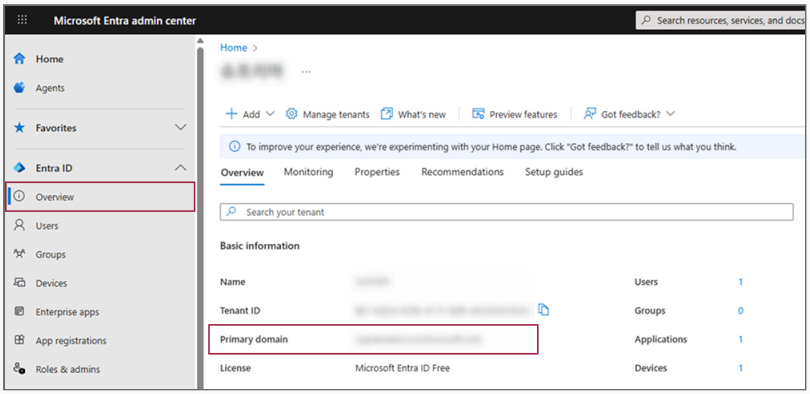
1. Log in to BioStar X with an Administrator account.
2. Go to **Settings** → **Directory Integration**.
3. Under **Directory Service**, select **Microsoft Entra ID**.
4. Configure **Directory Server**:
   - **Client ID**: Enter the **Client ID** of the application registered in **Entra ID**.
   - **Client Secret**: Enter the **Client secret** added in **Certificates & secrets** of the application registered in **Entra ID**.
   - **Primary Domain**: Enter the primary domain name that you input when creating your organization in **Entra ID**.
5. Click **Connect** to retrieves user group information to BioStar X.
6. Enable **BioStar X Login with Entra ID**.
7. Copy **Redirection URI** and paste it into the SSO redirection settings in the **Entra ID** portal.
8. Select the desired sync mode under **Sync Mode**.

9. Click **Apply** to save the settings.

Confirm sync by checking user list.

Info

- For more information about registering an application in **Entra ID**, refer to the following link.
- For more information about configuring **Certificates & secrets** in **Entra ID**, refer to the following link.
- **Tenant ID** can be found in the **Overview** of the registered application in **Entra ID**.
- You can check the information for **Primary Domain** in the **Overview** of **Entra ID**.



Microsoft Active Directory — Step-by-step

1. Log in to BioStar X with an Administrator account.
2. Go to **Settings** → **Directory Integration**.
3. Under **Directory Service**, select **Microsoft Active Directory**.
4. Configure **Directory Server**:
   - **Server Address**: IP or hostname of AD server.
   - **User Name** and **Password**: AD service account credentials.
   - **Base Domain Name**: Distinguished name of your AD domain.
5. To use an encrypted connection (LDAPS), enable **Secure Transfer**:
   - Install AD Certificate Services on the AD server.
   - Export the root certificate, convert to *.jks*, place in the BioStar X installation path.
   - Enter **Keystore Password** in BioStar X.
6. Click **Connect** to retrieves user group information to BioStar X.
7. Deselect groups not needed in **User Group Filter**.
8. Enable **BioStar X Login with Active Directory**.
9. Select the desired sync mode under **Sync Mode**.
10. Click **Apply** to save the settings.

Confirm sync by checking user list.

System log settings

Path: Settings → Server → Server

Configure BioStar X logging to retain sufficient data for audits and troubleshooting.

System log storage duration

- **Log Upload**: Select the method for uploading event logs.
  - **Automatic** (default): Logs are automatically deleted after the retention period.
  - **Manual**: Logs must be purged manually.
- **System log storage duration**: 1–120 days (default: 60 days).

> **Best Practice**
>
> For compliance-sensitive environments, set retention to 90–120 days and forward logs to a SIEM.

System log level settings

Per subsystem: Debug, Network, SQL, System, Web, WebSocket

Level	Description
Trace	Captures everything (very verbose)
Debug	Detailed developer-level logs
Info	Operational events, successful connections (default for most)
Warning	Potential issues
Error	Failures only

> **Caution**
> Running with **Trace** or **Debug** in production can generate excessive logs, impacting performance and filling disks rapidly. Reserve for short-term troubleshooting only.

BioStar X default log levels

- Debug, SQL, WebSocket: **Not Use**
- Network, System, Web: **Info**

Server port configuration

Configure BioStar X ports explicitly and prefer secure channels wherever possible. Use the default HTTPS port (`443`) for system access, and restrict device communication ports to trusted networks only.

Change the HTTPS port

1. Open **BioStar X Service Manager**: `http://127.0.0.1:28088/`
2. In the side menu, select **SERVICE SETTINGS**.
3. Under **Unified Gateway Service**, locate the **HTTPS Port** field (default: 443).
4. Change the port to your desired value.

   > *e.g., 8443*

5. Click **Apply** and restart the service if required.
6. Update firewall rules and client connections accordingly.

Personal Data Security

BioStar X stores user credentials, biometric templates, and personally identifiable information. Without database encryption, a breach exposes this information in plaintext, leading to identity theft, legal liability, and regulatory violations. This document explains how to enable personal information database encryption and minimize biometric image storage to protect sensitive data.

Encrypt personal data on database

Enable **Encrypt Personal Data on Database** to ensure all sensitive user and credential information is stored in an encrypted state.

Scope of encrypted data

When enabled **Encrypt Personal Data on Database**, the following items are encrypted at rest:

- Profile images
- User ID, Name, Phone number, User IP, Email addresses
- Login ID and Login password
- Face templates, Fingerprint templates
- Card ID, Smart card layout keys
- Custom information for users and visitors
- Image log files

Personal data encryption key

- Becomes configurable once **Encrypt Personal Data on Database** is set to **Use**.

- The key must be **32 characters**, using letters, numbers, and symbols.
- Changing the key triggers re-encryption of all existing data.

> **Best Practice**
>
> Generate the key using a **secure random generator**. Store it in a **password vault**. Rotate periodically (e.g., annually) or immediately if compromise is suspected.

Step-by-step

1. Log in to BioStar X with an Administrator account.
2. Go to **Settings** → **System** → **Security**.
3. Set **Encrypt Personal Data on Database** to **Use**.
4. Optionally, click **Change** under **Personal Data Encryption Key**, enter a new encryption key of **32 characters**.

> **Caution**
>
> Changing the encryption key will **re-encrypt all existing personal data**. Schedule during maintenance windows. Losing the encryption key may make encrypted data unrecoverable.

Store visual face image

Disable **Store Face Image** unless there is a strict operational requirement to retain actual facial images.

- **Templates** vs **Images**: Templates are mathematical representations of biometric data and are harder to reverse-engineer into a recognizable face.
- Many privacy regulations (GDPR, PDPA, etc.) treat biometric images as highly sensitive data.
- Storing images unnecessarily increases legal risk and attack surface.

Step-by-step

1. Go to **Settings** → **Server** → **Server**.
2. Set **Display expert settings** to **Use**.
3. Under **Expert Settings**, configure **Store Face Image**.
    - Default: **Use**
    - Recommended: **Not Use**

Best Practice

- Retain only **templates**, not images, for biometric authentication.
- If images are required for audit purposes: store in a **separate secure repository** with strict access controls and **short retention periods** (30–60 days).
- Periodically review settings after upgrades to ensure the value hasn't reverted to default.

Suprema Device Hardening

This documents provides hardening recommendations for Suprema-manufactured access control devices connected to BioStar X.

While server and BioStar X application hardening protect the central system, access control devices are installed at physical entry points and may be exposed to local network access, physical tampering, unauthorized operation, or outdated firmware. Device-level hardening must be treated as an essential part of the overall security posture.

This document covers the following:

- Applies to Suprema access control devices connected to BioStar X.
- Covers firmware maintenance, device event log handling, administrator configuration, and device-side operational controls.
- Device capabilities may differ depending on the model and firmware version.

Keep device firmware up to date

Keep Suprema device firmware updated to the latest supported version approved for the customer environment.

General best practices

- Maintain an inventory of all connected devices (model name, device ID, firmware version, installation location, role).
- Review Suprema firmware release notes before upgrading.
- Test firmware upgrades on a non-production device before broad deployment.
- Schedule firmware upgrades during a maintenance window.
- Ensure the device has stable power during the upgrade. Do not disconnect power or network.
- After upgrade, confirm device reconnects to BioStar X and all functions operate normally.

Firmware upgrade from software

When possible, perform firmware upgrades through the management software rather than directly from the device.

1. Download the correct firmware file for the target device model in Suprema Download Center.
2. Review the release notes and compatibility notes.
3. Confirm that the device is online and communicating normally.
4. Back up or confirm synchronization of users, credentials, logs, and device configuration.
5. Select the target device and run Firmware Upgrade.
6. Wait until the upgrade completes and the device restarts.
7. Confirm the firmware version after the restart.

Device reconnects to BioStar X; authentication, door control, and event log upload work normally; secure communication

and hashkey settings remain as expected.

> **Caution**
>
> - Do not apply firmware intended for a different device model.
> - Do not interrupt the upgrade process.
> - Some firmware upgrades may restrict downgrade paths — always review release notes before upgrading.

Firmware upgrade directly from device / USB

Some Suprema devices support firmware upgrade by connecting a USB memory device directly to the device.

1. Save the firmware upgrade file to a supported USB memory device.

   > It is recommended to save only one file to the USB memory.

2. Connect the USB memory to the device.
3. When prompted, authenticate using an administrator-level credential.
4. Wait for the firmware file to transfer to the device.
5. When instructed, remove the USB memory.
6. Wait until the firmware upgrade completes and the device restarts automatically.
7. Confirm the firmware version and validate device operation.

> **Caution**
> A device administrator must be configured before device-side firmware upgrade can proceed. Do not disconnect power during firmware upgrade.

Device event log retention and protection

Preserve device event logs and ensure they are uploaded to BioStar X regularly.

Device log policy

- Device logs are retained locally up to the device's supported capacity unless deleted or overwritten.
- Administrators should not rely only on device-local storage for long-term audit retention.
- Automatic log upload to BioStar X should be enabled whenever possible.
- Event logs should be reviewed and backed up according to the organization's audit and compliance policy.
- Ensure device date, time, time zone, and daylight-saving time settings are configured correctly. Enable Time Sync where

supported.

Secure tamper consideration

Some Suprema devices support **Secure Tamper** behaviour. If tamper protection is enabled and a tamper event occurs, the device may delete sensitive data stored on the device — including users, logs, encryption keys, and SSL certificates. Enable automatic log upload to reduce the risk of losing device-local logs.

Operational best practices

- Treat device tamper events as security incidents.
- After a tamper event, inspect the device physically before re-enrolment or redeployment.
- Do not disable tamper-related protections without documented security approval.

Configure device administrator

Configure a device administrator on supported Suprema devices and restrict access to the device administrator menu. Devices should not be deployed in production without administrator protection.

Info

Device administrator privileges are separate from BioStar X user permissions.

Best Practice

- Register at least one device administrator before production deployment.
- Use unique administrator credentials assigned to authorized personnel only.
- Use strong authentication methods (card + PIN, biometric + PIN, or multi-credential administrator authentication).
- Periodically review device administrator assignments.
- Remove administrator access immediately when staff roles change.
- Document emergency recovery procedures in case administrator credentials are lost.

Configure device administrator from software

1. Log in to BioStar X with an Administrator account.
2. Create or select the user who will act as the device administrator.
3. Enrol the required credential (card, PIN, fingerprint, or face).
4. Assign administrator-level privilege or the appropriate device administrator role.
5. Transfer or synchronize the user to the target device.
6. Confirm on the device that the administrator credential can access the admin menu.

Configure device administrator directly from device

1. Access the device menu.
2. Open the user enrolment or administrator configuration menu.
3. Enrol the administrator user and credential.
4. Assign administrator-level privilege.
5. Save the configuration.
6. Test administrator authentication by accessing the admin menu again.

Device network and local service hardening

Configure device network and local service settings according to the principle of least functionality.

Recommended actions

- Use stable and documented device IP addressing (reserve IP in DHCP, or document static IP with subnet mask, gateway, DNS, port, device ID, and location).
- Verify the BioStar X server address and server port used by the device.
- Disable device-side features that are not required.

  > *e.g., RTSP, IP Intercom*

- If RTSP, intercom, or other optional services are required, configure strong credentials and restrict access to trusted systems only.
- Enable Time Sync where supported.
- After Restore Default or Factory Default, recheck network settings, administrator levels, root certificates, secure communication, and BioStar X connection.

Device-side operational hardening checklist

- ☐ Keep firmware updated to the latest supported version.
- ☐ Maintain an inventory of device model, device ID, firmware version, location, and role.
- ☐ Configure device administrator access before production use.
- ☐ Restrict administrator privileges to authorized personnel only.
- ☐ Enable secure communication with BioStar X where supported.
- ☐ Enable Device Hashkey Management and Secure Tamper where appropriate for the deployment risk level.
- ☐ Set Log Upload to Automatic where possible.
- ☐ Confirm device event logs are uploaded to BioStar X regularly.

- ☐ Physically secure device installation and cabling.
- ☐ Treat tamper events, unexpected restarts, firmware changes, and log gaps as security-relevant events.
- ☐ Review device configuration after firmware upgrades, device replacement, or restore operations.
- ☐ Use stable and documented network addressing for production devices.
- ☐ Disable device-side features that are not required for the deployment.
- ☐ Restrict Restore Default and Factory Default operations to authorized administrators only.

References

This document provides essential technical reference information for deploying and securing BioStar X. Find network port configurations, recommended security settings, and key compliance requirements at a glance. Refer to the external resources section for additional support and detailed guidelines.

Default BioStar X network ports

Service	Purpose	Default Port(s)	Notes / Recommendations
Unified Gateway Service	HTTPS (system access)	443	Default for admin/operator login. Changeable via **Service Manager** → **Service Settings**.
Core Web Service	HTTPS (internal UI)	5002	Prefer proxied to 443; restrict direct access.
	CloudNgrok	52000	Disable if not required.
	Thrift RPC	9310	Restrict to trusted services.
Core Service	WebSocket	9002	Internal only.
	FastCGI	9000	Should be bound locally.
	API	9010	Secure with TLS & authentication.
Coordinator Service	Client Communication	21810	Internal only.
Main Server	TCP Server	51212	**Plaintext** device comms — block if possible.
	SSL Server	51213	**Preferred** device comms (TLS).
	gRPC	51219	Internal service comms only.
Cache Service	Client	10800	Equivalent to Redis — do not expose externally.
	Communication	47500	Internal only.
	Discovery	47100	Internal only.

Default security features in BioStar X

Feature	Location in UI	Default	Recommendation
Change default admin login ID & password	**User** → Edit Default Admin (UID:1)	admin / installer PW	Change immediately after install.
Access separation (roles)	**User** → Select a user → **Permission** → **Account Level**	Predefined: **Administrator**, **User Operator**, **Monitoring Operator**	Create custom roles as needed.
Password strength policy	**Settings** → **System** → **Security** → **Login Password** → **Password Level**	**Medium**	Set to **Strong**, enforce MFA.
Session security (Simultaneous connection)	**Settings** → **System** → **Security** → **Session Security** → **Simultaneous Connection Allow**	**Active**	Set to **Inactive** to prevent shared logins.
Multi-factor authentication	**User** → Select a user → **Permission** → **Multi-Factor Auth for Login**	**Not Use**	Enable for **Administrator**, **User Operator**, **Monitoring Operator** accounts.
Secure communication with device	**Settings** → **System** → **Security** → **Advanced Security Settings** → **Secure communication with device**	**Not Use**	Enable + use SSL port (51213).
Device hashkey management	**Settings** → **System** → **Security** → **Advanced Security Settings** → **Device Hashkey Management**	**Not Use**	Enable for tamper protection in high-security deployments.
System Backup	**Settings** → **System** → **System Backup**	**Manual**	Enable **Automatic System Backup**.
Directory Integration	**Settings** → **System** → **Directory Integration**	Not Configured	Integrate with Entra ID or Active Directory where available.
Log settings (Retention & Levels)	**Settings** → **System** → **Server** → **Server**	**System log storage duration**: 60 days **System log level**: **Info**	Adjust per compliance. Forward to SIEM.
Encrypt personal data on database	**Settings** → **System** → **Security** → **Advanced Security Settings** → **Encrypt Personal Data on Database**	**Not Use**	Enable in production.
Store visual face image	**Settings** → **System** → **Server** → **Expert Settings** → **Store Face Image**	**Use**	Disable unless justified.

Compliance mapping (quick view)

Security Control	Supports Compliance Areas
Database encryption (PII, biometrics)	GDPR, CCPA, ISO 27001
System log retention + forwarding	ISO 27001, PCI-DSS
MFA for admin/operator accounts	NIST 800-63, ISO 27001
Secure comms with devices (TLS)	GDPR, ISO 27001
Backup & restore capability	ISO 27001, SOC 2
Directory integration (Entra ID / Active Directory)	SOX, ISO 27001, SOC 2

External References

- Suprema Knowledge Base – Secure Communication with Device
- Suprema Knowledge Base – Device Hashkey Management
- Suprema Knowledge Base – Import/Export Device Logs via USB
- Suprema Knowledge Base – BioEntry W3 USB Firmware Upgrade Guide
- Suprema Knowledge Base – How to Configure Secure Tamper
- Microsoft – Windows Security Compliance Toolkit

Appendices

Includes legal notices contained in the product.

Disclaimers

- Information in this web site is provided in connection with Suprema products.
- The right to use is acknowledged only for Suprema products included in the terms and conditions of use or sale for such products guaranteed by Suprema. No license, express or implied, by estoppel or otherwise, to any intellectual property is granted by this web site.
- Except as expressly stated in an agreement between you and Suprema, Suprema assumes no liability whatsoever, and Suprema disclaims all warranties, express or implied including, without limitation, relating to fitness for a particular purpose, merchantability, or noninfringement.
- All warranties are VOID if Suprema products have been: 1) improperly installed or where the serial numbers, warranty date or quality assurance decals on the hardware are altered or removed; 2) used in a manner other than as authorized by Suprema; 3) modified, altered or repaired by a party other than Suprema or a party authorized by Suprema; or 4) operated or maintained in unsuitable environmental conditions.
- Suprema products are not intended for use in medical, lifesaving, life-sustaining applications, or other applications in which the failure of the Suprema product could create a situation where personal injury or death may occur. Should you purchase or use Suprema products for any such unintended or unauthorized application, you shall indemnify and hold Suprema and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Suprema was negligent regarding the design or manufacture of the part.
- Suprema reserves the right to make changes to specifications and product descriptions at any time without notice to improve reliability, function, or design.
- Personal information, in the form of authentication messages and other relative information, may be stored within Suprema products during usage. Suprema does not take responsibility for any information, including personal information, stored within Suprema’s products that are not within Suprema’s direct control or as stated by the relevant terms and conditions. When any stored information, including personal information, is used, it is the responsibility of the product users to comply with national legislation (such as GDPR) and to ensure proper handling and processing.
- You must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Suprema reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.
- Except as expressly set forth herein, to the maximum extent permitted by law, the Suprema products are sold "as is".
- Contact your local Suprema sales office or your distributor to obtain the latest specifications and before placing your product order.

Copyright Notice

The copyright for this website is owned by Suprema. Rights to other product names, trademarks, and registered trademarks belong to the respective individuals or organizations that own them.

Suprema Inc.

17F Parkview Tower, 248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13554, Rep. of KOREA

Tel: +82 31 783 4502 | Fax: +82 31 783 4503 | Inquiry: sales_sys@supremainc.com

For more information about Suprema's global branch offices,
visit the webpage below by scanning the QR code.
https://supremainc.com/en/about/global-office.asp

© 2026 Suprema Inc. Suprema and identifying product names and numbers herein are registered trade marks of Suprema, Inc.
All non-Suprema brands and product names are trademarks or registered trademarks of their respective companies.
Product appearance, build status and/or specifications are subject to change without notice.