BioStar X 보안 강화

관리자 가이드

버전 1.0.0

한국어
KO 102.00.BSX

suprema
SECURITY & BIOMETRICS

목차

보안 출입 제어의 핵심 원칙 4

최소 권한 원칙 (Principle of Least Privilege, PoLP) 4

직무 분리 4

심층 방어 (Defense in Depth) 4

제로 트러스트 아키텍처 개념 5

서버 보안 강화 6

운영체제 구성 6

사용자 및 접근 제어 11

네트워크 및 방화벽 12

서비스 및 애플리케이션 계층 15

데이터베이스 및 데이터 보호 16

모니터링 및 감사 19

패치 및 유지 관리 21

물리적 보안 22

BioStar X 강화 24

시스템 보안 24

개인 데이터 보안 34

슈프리마 장치 강화 36

장치 펌웨어 최신 상태 유지 36

장치 이벤트 로그 보존 및 보호 37

장치 관리자 구성 38

장치 네트워크 및 로컬 서비스 보안 강화 39

장치 운영 강화 체크리스트 39

참조 41

BioStar X 기본 네트워크 포트 12

BioStar X의 기본 보안 기능 42

컴플라이언스 요구사항 (간략 보기) 43

외부 참조 43

부록 **44**

면책 조항 44

저작권 공지 45

보안 출입 제어의 핵심 원칙

출입 제어 시스템의 보안 강화는 단순히 기술적인 설정에 관한 것이 아닙니다. 이는 사용자, 프로세스, 기술 전반에 걸쳐 검증된 원칙을 일관되게 적용하는 것입니다. BioStar X는 설계상 이러한 원칙을 지원하지만, 관리자가 올바르게 구성하고 시행해야 합니다.

최소 권한 원칙 (Principle of Least Privilege, PoLP)

사용자와 서비스에는 작업 수행에 **필요한 권한만** 부여해야 합니다. 그 이상도 이하도 안 됩니다.

- 관리자 계정은 일상적인 운영이 아닌 구성 및 시스템 변경 용도로만 사용해야 합니다.
- 운영자는 출입문, 사용자, 이벤트를 관리할 수 있지만 보안 정책은 변경할 수 없어야 합니다.
- 감사자는 데이터를 변경할 권한 없이 읽기 전용으로만 모든 정보를 볼 수 있어야 합니다.

> **알아두기**
> 권한을 제한하면 계정이 침해되더라도 피해를 최소화할 수 있습니다. 공격자가 운영자 계정을 탈취하더라도 암호화 키를 변경하거나 로그를 비활성화할 수 없습니다.

직무 분리

중요한 책임은 **여러 역할에 분산**되어야 합니다. 어느 한 사람도 시스템에 대한 무제한적인 통제권을 가져서는 안 됩니다.

예를 들어:

- 관리자는 시스템 구성을 관리하고, 다른 운영자는 일상적인 접근 요청을 처리합니다.
- 감사자는 독립적으로 변경 사항을 확인하고 로그를 모니터링합니다.

> **알아두기**
> 내부자 악용을 방지하고 **견제와 균형**을 보장해야 합니다. 한 계정이 침해되더라도 공격자는 전체 시스템을 통제할 수 없도록 해야 합니다.

심층 방어 (Defense in Depth)

어떠한 단일 보안 조치도 완벽하지 않습니다. 대신, 하나가 실패하더라도 다른 보안 계층이 시스템을 보호할 수 있도록 여러 보안 제어 계층을 적용해야 합니다.

- **네트워크 계층**: 방화벽, VLAN 세분화
- **시스템 계층**: 안전한 운영체제 기본 설정, 패치, 바이러스 백신
- **애플리케이션 계층**: 강력한 비밀번호, 멀티팩터 인증(MFA), 암호화
- **모니터링 계층**: 로그, SIEM, 경보

> **알아두기**
> 공격자는 종종 취약한 연결 고리를 찾습니다. 심층 방어는 단일 실패 지점이 없도록 보장합니다.

제로 트러스트 아키텍처 개념

어떠한 장치, 사용자, 네트워크도 기본적으로 신뢰해서는 안 됩니다. **'절대 신뢰하지 말고, 항상 검증해야 합니다'.**

- 모든 로그인은 인증을 요구해야 합니다. 가능하다면 멀티팩터 인증(MFA)을 사용해야 합니다.
- 장치와 서버 간 통신은 항상 암호화되어야 합니다.
- 내부 트래픽도 외부 트래픽처럼 세분화하고 모니터링해야 합니다.

> **알아두기**
> 현대의 위협은 종종 네트워크 내부(손상된 노트북, 피싱, 악의적인 내부자)에서 발생합니다. 제로 트러스트는 '신뢰할 수 있는 경계'에 대한 의존을 줄이고 지속적인 검증을 강화합니다.

이 네 가지 원칙은 **본 보안 강화 가이드(Hardening Guide)의 기반**입니다. 이 문서에서 안내하는 모든 구성(포트 설정부터 디렉터리 통합까지) 권고 사항은 **최소 권한 원칙(PoLP), 직무 분리, 심층 방어, 제로 트러스트**의 실질적인 적용 사례입니다.

서버 보안 강화

BioStar X를 호스팅하는 Windows 환경을 보안하기 위한 권장 사례를 안내합니다. 시스템, 네트워크 및 애플리케이션 레벨의 제어 기능을 다루며, 이러한 제어 기능은 취약점을 최소화하고 공격 표면(Attack Surface)을 줄이며 조직의 보안 정책을 준수하도록 설계되었습니다.

- BioStar X를 실행하는 모든 Windows 서버(베어 메탈 또는 가상 머신)에 적용됩니다.
- 시스템 구성, 네트워크 보호, 접근 제어, 모니터링 및 패치에 대한 내용을 포함합니다.
- 시스템 관리자, 보안 엔지니어, 배포 팀을 대상으로 합니다.

운영체제 구성

BioStar X 보안 강화(Hardening) 절차의 첫 단계는 운영체제 수준의 보안 기준선을 확보하는 것입니다. 패치되지 않은 운영체제, 불필요한 서비스, 취약한 인증 설정은 BioStar X를 포함한 모든 서버 워크로드의 주요 공격 경로가 됩니다. 이 문서의 안내에 따라 Windows Server 환경을 강화하세요.

Windows Server LTS 릴리스 사용

지원되지 않거나 오래된 Windows 버전에서 BioStar X를 실행하면 패치가 적용되지 않은 취약점에 시스템이 노출됩니다. Microsoft는 보안 업데이트, 안정성 수정 및 10년 이상(5년 기본 지원 + 5년 연장 지원) 지원을 보장하는 Windows Server 장기 지원(LTS) 버전을 제공합니다. LTS 릴리스를 선택하면 BioStar X 서버가 가능한 가장 긴 보안 지원 기간을 확보하고, 기능 업데이트로 인한 시스템 중단을 최소화할 수 있습니다.다.

관리자를 위한 요약

- 반드시 **Windows Server LTS 에디션**(2019 또는 2022)에 BioStar X를 배포하세요.
- 설치 후 운영체제 버전을 **확인**하세요.
- 지원 종료일 이전에 **업그레이드를 계획**하세요.
- **자동 업데이트를 활성화**하거나 WSUS/SCCM에 연결하세요.
- 지원되지 않는 소프트웨어를 실행하지 않도록 **제품 수명 주기를 문서화**하세요.

지원 버전 확인

Microsoft에서 활성 지원하는 LTS Windows Server 에디션(2026년 5월 기준):

- Windows Server 2019 (LTS) — 기본 지원: 2024년 1월까지 / 연장 보안 지원: 2029년 1월까지
- Windows Server 2022 (LTS) — 기본 지원: 2026년 10월까지 / 연장 보안 지원: 2031년 10월까지
- Windows Server 2025 (LTS) — 기본 지원: 2029년 11월까지 / 연장 보안 지원: 2034년 11월까지

주의

Semi-Annual Channel(SAC) 릴리스는 수명이 짧고 BioStar X와 같은 프로덕션 워크로드에는 적합하지 않으므로 피하세요.

현재 OS 버전 확인

- `Win + R` 키를 누른 후 `winver`를 입력하세요. `Enter` 키를 누르면 에디션 및 버전이 표시됩니다.
- PowerShell에서 다음 명령어를 실행하여 운영체제 이름과 버전을 확인할 수도 있습니다.

  PowerShell

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

업그레이드 계획

- Windows Server 2016 버전 이하를 실행 중이라면 마이그레이션을 계획해야 합니다.
- 2019 또는 2022 LTS 버전으로 업그레이드하면 보안 업데이트 및 최신 TLS 프로토콜(TLS 1.2/1.3)과의 호환성이 보장됩니다.

> **모범 사례**
>
> 지원되는 운영체제로 새 가상머신(VM)이나 서버를 구축하세요. BioStar X를 새로 설치한 후 구성 및 데이터베이스를 마이그레이션하세요. 이를 통해 다운타임과 위험을 최소화할 수 있습니다.

Windows Update 구성 확인

보안 패치를 위한 **자동 업데이트**를 활성화하세요. 또는 Windows Server Update Services(WSUS) 또는 System Center Configuration Manager(SCCM)를 사용하는 경우 호스트가 올바르게 등록되어 있는지 확인하세요.

최신 Windows 업데이트 및 보안 패치 적용

프로덕션 배포 전에 최신 Windows 업데이트와 보안 패치를 적용하여 알려진 취약점으로부터 시스템을 보호하세요.

패치되지 않은 Windows 서버는 랜섬웨어, 원격 코드 실행, 권한 상승 익스플로잇(Exploit)의 **주요 공격 경로**입니다. 최신 보안 업데이트를 적용하면 BioStar X 호스트가 모든 **알려진 취약점**으로부터 보호된 상태로 라이프사이클을 시작할 수 있습니다.

현재 패치 수준 확인

- 최신 패치 상태를 확인하려면 **설정** → **Windows 업데이트**를 열고 **업데이트 확인**을 클릭하세요.
- PowerShell에서 최근 설치된 패치 10개를 확인하려면 다음 명령어를 실행하세요.

  PowerShell

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

> **주의**
>
> 최신 패치가 30일 이상 지났다면 즉시 업데이트를 진행하세요.

업데이트 프로세스

1. Windows 업데이트를 수동으로 실행하세요.

2. 모든 보안 및 중요 업데이트를 설치하세요.

> 서버가 아직 프로덕션 상태가 아니더라도 미루지 말고 최신 패치를 적용하는 것을 권장합니다.

3. 필요하다면 서버를 재부팅하세요.
4. '최신 상태입니다'가 표시될 때까지 업데이트 및 설치 작업을 반복하세요.

지속적인 패치 전략

- **월별 패치**: Microsoft는 매월 두 번째 화요일에 새 패치를 배포합니다.
- 스테이징 환경이 있다면 테스트 후 배포에서 1–2주 이내에 패치를 적용합니다.
- 즉시 패치를 적용할 수 없다면, 패치가 적용될 때까지 방화벽 제한, 인터넷 접속 차단, 강화된 모니터링 등의 **보완 제어**(Compensating controls)를 적용하여 위험을 완화하세요.

불필요한 Windows 기능 제거 또는 비활성화

활성화된 모든 Windows 기능은 서버의 **공격 표면(Attack Surface)을 증가**시킵니다. 전용 BioStar X 호스트에서는 Print Spooler, Fax, IIS 등의 서비스가 거의 필요 없으며, 이는 심각한 취약점(예: PrintNightmare)의 이력을 가지고 있습니다.

> *예: Internet Explorer, SMBv1, 레거시 구성 요소*

1. 시작 → **서버 관리자** → **관리** → **역할 및 기능 제거**를 실행하세요.
2. 설치된 역할(예: 파일 서비스, IIS, 인쇄 서비스)을 검토하세요.
3. BioStar X에 필요하지 않은 역할을 제거하세요.
4. 관리 워크플로에 필요한 경우에만 **.NET Framework 기능** 및 **데스크톱 환경**(Desktop Experience)을 유지하세요.
5. `services.msc`를 열고 불필요한 서비스(Fax, Remote Registry, Bluetooth, SMBv1)를 **사용 안 함**으로 설정하세요.

> **모범 사례**
>
> 호스트를 BioStar X **전용**으로 사용하세요. 다른 워크로드를 실행하지 마세요.

Windows Defender 활성화 및 최신 상태 유지

Windows Defender(기본 제공 바이러스 백신)는 악성 코드 및 랜섬웨어로부터 보호합니다. 비활성화하면 호스트가 취약해집니다.

1. **설정** → **개인 정보 및 보안** → **Windows 보안** → **바이러스 및 위협 방지**를 실행하세요.
2. **설정 관리** → **실시간 보호**가 활성화되어 있는지 확인하세요.
3. **클라우드 전송 보호** 및 **자동 샘플 전송**이 활성화되어 있는지 확인하세요.
4. 보안 인텔리전스(정의라고도 함)를 최신 상태로 유지하세요. 일반적으로 Windows Update를 통해 자동 수행됩니다.

> **주의**
> 타사 바이러스 백신을 사용한다면 충돌을 방지하기 위해 **하나의 바이러스 백신 솔루션**만 실행되고 있는지 확인하세요.

물리적 도난 방지를 위한 BitLocker 활성화

공격자가 서버에 물리적으로 접근하면(예: 디스크 도난, VM 스냅샷, 백업 미디어) 암호화되지 않은 드라이브에서 크리덴셜, 로그, 생체 정보 등 민감한 데이터에 직접 접근할 수 있습니다. BitLocker는 미사용 데이터 보호를 위한 전체 디스크 암호화를 제공합니다.

권고 사항

- 다음 드라이브에 BitLocker를 활성화하세요.
  - OS 드라이브(C:)
  - BioStar X 데이터베이스, 로그, 백업을 저장하는 모든 데이터 드라이브
- 더 강력한 보호를 위해 가능한 경우 TPM + PIN을 사용하세요.

단계별 안내

1. **제어판** → **시스템 및 보안** → **BitLocker 드라이브 암호화**로 이동하세요.
2. 각 드라이브에서 **BitLocker 켜기**를 클릭하세요.
3. 인증 방법으로 **TPM**(기본값) 또는 **TPM + PIN**(권장됨)을 선택하세요.
4. 복구 키를 **Active Directory/Azure AD**(선호) 또는 **보안 볼트**로 저장하세요. 로컬에 저장하지 마세요.
5. 암호화 방법을 **XTS-AES 256비트**(권장)로 선택하세요.
6. 암호화를 시작합니다.

BitLocker 상태 모니터링

다음 명령어를 실행하여 BitLocker 상태를 확인하세요.

PowerShell

```
Get-BitLockerVolume
```

> **알아두기**
> BitLocker는 **미사용 데이터만** 보호합니다. 데이터베이스 암호화 또는 TLS 암호화를 대체하지 않습니다.

안전한 인증 정책 시행

취약한 로컬 계정이나 캐시된 크리덴셜은 서버가 무차별 대입 공격이나 권한 상승에 취약해질 수 있습니다.

1. **로컬 보안 정책**(`secpol.msc`)을 실행하세요.
2. **계정 정책** → **암호 정책**에서 아래와 같이 구성하세요.

- **최소 암호 길이**: 12자 이상
- **암호는 복잡성을 만족해야 함**: 활성화
- **최대 암호 사용 기간**: 90일

3. **계정 정책** → **계정 잠금 정책**에서 아래와 같이 구성하세요.
   - **계정 잠금 임계값**: 5회 시도
4. 기본 **Administrator** 계정을 비활성화하거나 이름을 변경하세요.
5. RDP 또는 원격 관리 액세스에 멀티팩터 인증(MFA)을 요구하세요.

보안 기준선을 위한 그룹 정책 설정 적용

Microsoft의 **Microsoft 보안 준수 도구 키트**(Security Compliance Toolkit, SCT)는 보안 기준선에 맞추어진 **그룹 정책 개체**(Group Policy Objects, GPO)를 다운로드할 수 있도록 제공합니다. 이 기준선은 구성 오류 위험을 줄이고 BioStar X가 강화된 Windows 운영체제에서 실행되도록 보장합니다.

1. Microsoft Security Compliance Toolkit을 다운로드하세요.
2. 운영체제 버전(Windows Server 2019 또는 2022 Security Baseline)에 맞는 기준선을 선택하세요.
3. **그룹 정책 관리 콘솔**에 기준선 그룹 정책 개체(GPO)를 가져오기하세요.

   `gpmc.msc` 실행 → **그룹 정책 개체**(Group Policy Objects)에서 마우스 오른쪽 버튼 클릭 → **설정 가져오기** 클릭
4. 액티브 디렉토리의 **BioStar X 서버 OU**에 기준선 그룹 정책 개체(GPO)를 연결하세요.
5. 중요 설정을 검토하세요.

   계정 잠금, 감사 로깅, 네트워크 보안(SMB 서명, LDAP 서명), LSA 보호
6. **스테이징에서 먼저 테스트** 후 BioStar X 호환성을 확인하고 프로덕션 환경에 배포하세요.

필요하지 않은 원격 데스크톱 비활성화

원격 데스크톱(RDP)은 무차별 대입 공격, 크리덴셜 도용의 일반적인 공격 벡터(Attack Vector)입니다.

필요하지 않은 경우

시스템 속성 → **원격** → **이 컴퓨터에 대한 원격 연결 허용 안 함**을 선택하세요.

필요한 경우 보안 강화

원격 데스크톱을 사용해야 하는 경우 다음 보안 강화 조치를 적용하여 위험을 완화하세요.

- VPN 또는 LAN 환경에서만 접속하도록 제한하세요.
- 네트워크 수준 인증(Network Level Authentication, NLA)을 필수로 설정하세요.
- 기본 RDP 포트를 변경하세요. (`3389` → 사용자 지정)
- 이벤트 로그 및 알림을 통해 모니터링하세요.

사용자 및 접근 제어

운영체제를 강화한 후 다음 단계는 **누가** 시스템에 접근할 수 있는지, **무엇을** 할 수 있는지를 제어하는 것입니다. 잘못 구성된 계정 권한, 취약한 암호, 방치된 기본 계정은 공격자가 BioStar X 서버에서 권한을 상승시키는 가장 흔한 경로입니다. 이 문서의 안내에 따라 사용자 및 접근 제어를 강화하세요.

최소 권한 시행

- Active Directory 또는 로컬 사용자 및 그룹에서 별도의 사용자 그룹을 생성하세요.
- 그룹 기반으로 파일 시스템 및 애플리케이션 권한을 할당하세요.
- 운영체제 수준 최소 권한 모델을 반영하도록 BioStar X 내 역할을 구성하세요.

로컬 관리 권한 제한

- `lusrmgr.msc`를 사용하여 Administrators 그룹에서 불필요한 계정을 제거하세요.
- 일반 작업에는 표준 사용자 계정을 사용하고, 필요할 때만 관리자 계정을 사용하세요.
- 도메인에 가입된 경우 그룹 정책 제한 그룹을 적용하여 일관된 권한을 적용하세요.

강력한 인증 적용

- 그룹 정책에서 복잡한 암호를 사용하도록 설정하세요. (최소 12–15자, 대/소문자, 숫자, 기호 혼합)
- 암호 만료일(예: 90일마다)을 설정하고 재사용을 제한하세요.
- 여러 번 실패한 시도 후 계정을 잠그는 계정 잠금 정책을 구성하세요.
- 원격 접근 또는 특권 계정에 멀티팩터 인증(MFA)을 적용하세요.

단계별 안내

1. **로컬 그룹 정책 편집기**(`gpedit.msc`)를 실행하세요.
2. **컴퓨터 구성** → **Windows 설정** → **보안 설정** → **계정 정책**으로 이동하세요.
3. 비밀번호 길이, 복잡성, 최근 암호 기억 등을 설정하세요.
4. **계정 잠금 정책**에서 ***계정 잠금 임계값***과 **계정 잠금 기간**을 구성하세요.

기본 제공(Built-in) 계정 관리

로컬 사용자 및 그룹(`lusrmgr.msc`)을 실행하세요.

- Administrator 계정에서 마우스 오른쪽 버튼을 클릭하고 알아보기 어려운 이름으로 변경하세요.
- Guest 계정은 특별히 필요하지 않다면 비활성화하세요.
- PowerShell에서 `net user` 명령어를 사용해 정기적으로 계정을 감사하세요.

세션 관리

- 15분 동안 활동이 없으면 계정이 자동 잠기도록 설정하세요.
- 가능하면 동일 계정으로 여러 사용자가 동시에 로그인하는 것을 방지하세요.
- 사용하지 않는 원격 세션을 제한합니다.

> **알아두기**
> **로컬 그룹 정책 편집기**(`gpedit.msc`) → **컴퓨터 구성** → **Windows 설정** → **보안 설정** → **로컬 정책** → **보안 옵션** → **대화형 로그온: 컴퓨터 비활성 제한** (예: 900초 = 15분)

감사 및 모니터링

- 로그인 시도, 권한 사용, 계정 관리에 대한 감사 기능을 활성화하세요.
- 로그를 **SIEM** 또는 중앙 로그 수집기로 전송하세요.
- 보안 로그를 정기적으로 검토하여 이상 징후를 확인하세요.

> **알아두기**
> **로컬 그룹 정책 편집기**(`gpedit.msc`) → **컴퓨터 구성** → **Windows 설정** → **보안 설정** → **고급 감사 정책 구성**
>
> 활성화 범주: **로그온/로그오프**, **계정 관리**, **권한 사용**

네트워크 및 방화벽

BioStar X를 인증되지 않은 접근이나 네트워크 내 측면 이동(Lateral Movement)으로부터 보호하려면 네트워크 보안 경계 및 호스트 기반 방화벽 설정을 안전하게 유지하는 것이 매우 중요합니다. BioStar X는 HTTPS, REST, gRPC, WebSockets 및 Thrift를 통해 서비스를 제공할 수 있으므로, 인바운드 및 아웃바운드 연결을 엄격하게 제어해야 합니다.

Windows Defender 방화벽 활성화 및 구성

방화벽을 올바르게 구성하면 명시적으로 승인된 트래픽만 BioStar X에 도달하도록 하여 공격 표면(Attack Surface)을 크게 줄일 수 있습니다.

BioStar X 기본 네트워크 포트

서비스	용도	기본 포트
BioStar X Core Web Service	HTTPS / 웹 인터페이스	5002
	Thrift RPC	9310
BioStar X Core Service	WebSocket	9002

서비스	용도	기본 포트
	FastCGI	9000
	API	9010
	RPC	51218
Unified Gateway Service	HTTPS	443
Coordinator Service	클라이언트 통신	21810
Main Server	TCP 서버	51212
	SSL 서버	51213
	gRPC	51219
Cache Service	클라이언트	10800
	통신	47500
	검색	47100

> **알아두기**
> 멀티 커뮤니케이션 서버를 배포할 때, 메인 서버와 동일한 통신 포트(`51212`, `51219`)를 사용합니다. 관리자는 배포 토폴로지에 따라 멀티 커뮤니케이션 서버와 메인 서버 간에 이 포트에 대해 접근할 수 있는지 확인해야 합니다.

단계별 안내

1. **고급 보안이 포함된 Windows Defender 방화벽**(`wf.msc`)을 실행하세요.
2. **인바운드 규칙**에서 필요하지 않은 규칙을 제거하거나 비활성화하세요.
3. 다음과 같이 명시적 허용 규칙을 생성하세요.
   - **Unified Gateway HTTPS**(`443`): 필요한 경우 외부/공용 포트로 설정
   - **Core Web Service HTTPS**(`5002`): 가급적 `443`을 통해 프록시 설정
   - 내부 전용 포트(gRPC `51219`, Cache `10800` / `47500` / `47100`, Coordinator `21810`, Thrift `9310`): 로컬 호스트(localhost) 또는 신뢰할 수 있는 서브넷에서만 접속 허용
4. 다른 모든 인바운드 트래픽은 **차단**으로 설정하세요.
5. **아웃바운드 규칙**에서 알려진 신뢰할 수 있는 엔드포인트로 제한하세요.

> **주의**
> 모두 허용과 같은 포괄적인 규칙은 사용하지 마세요. 기본 포트 변경은 약간의 모호성 개선 효과를 제공하지만 방화벽 적용을 대체할 수는 없습니다.

원격 접근(Remote access) 제한

- 원격 데스크톱(Remote Desktop Protocol, RDP) 접근 권한을 인증된 관리자에게만 제한하세요.
- RDP가 필요하다면 NLA 사용하거나, 서버를 VPN 뒤에 배치하거나, 점프 호스트를 사용하세요.
- RDP가 필요하지 않다면 비활성화하세요. (**시스템 속성 → 원격 설정**).

안전한 네트워크 세분화

- BioStar X 서버는 사용자 네트워크와 분리된 전용 VLAN 또는 DMZ에 배치하세요.
- BioStar X와 필수 시스템(예: 데이터베이스 서버, API 소비자, 리더) 간에만 통신을 허용하세요.
- 관리 접근(RDP, SSH)을 관리자 서브넷으로만 제한하세요.

> **모범 사례**
> **심층 방어**(Defense in Depth)를 위해 네트워크를 세분화하고 호스트 방화벽을 결합하세요.

네트워크 프로토콜 강화

SMBv1 비활성화

PowerShell 명령어를 사용하여 SMBv1을 비활성화하세요.

PowerShell

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

TLS 1.2+ 적용

- 레지스트리 경로: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols`

  SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 비활성화
- IIS Crypto 또는 `nmap --script ssl-enum-ciphers`로 검증하세요.

> **주의**
> 호환성 문제를 방지하려면 프로토콜 비활성화하기 전에 스테이징 환경에서 테스트하세요.

네트워크 침입 감지 및 모니터링

- IDS/IPS(Snort, Suricata 또는 상용 제품)를 배포하세요.
- Windows Defender 방화벽에서 차단된 패킷 및 허용된 연결에 대한 로깅을 활성화하세요.
- 중앙 집중식 모니터링을 위해 SIEM으로 로그를 전달하세요.

> **알아두기**
> 방화벽 로그 저장 위치: `%systemroot%\system32\LogFiles\Firewall\pfirewall.log`

서비스 및 애플리케이션 계층

서비스 및 애플리케이션 계층은 BioStar X의 소프트웨어 구성 요소와 런타임 환경을 보호하는 데 중점을 둡니다.

서비스에 최소 권한 원칙 적용

- 로컬 시스템 계정 또는 Administrator 계정 대신 전용 서비스 계정으로 BioStar X 서비스를 실행하세요.
- 필요한 최소 권한(서비스로 로그온, 특정 디렉터리 읽기/쓰기)만 부여하세요.
- 가능하다면 각 BioStar X 서비스 구성 요소에 별도 계정을 사용하세요.

단계별 안내

1. BioStar X 서비스를 위한 전용 로컬 사용자 계정을 생성하세요.
2. 서비스(`services.msc`)를 열고 BioStar X 서비스를 마우스 오른쪽 버튼으로 클릭한 후 **속성** → **로그온** 탭을 선택하세요.
3. 전용 계정을 할당하세요.
4. 파일 시스템 액세스 제어 목록(ACL)을 적용해 해당 계정이 필요한 디렉터리에만 접근할 수 있도록 설정하세요.
5. 해당 계정에 대한 대화형 로그온 권한을 거부하세요.

> **주의**
> 여러 서비스 간에 계정을 공유하면 침해 감사가 어려워집니다.

보안 애플리케이션 구성 파일

- 시크릿 정보(예: 데이터베이스 연결 문자열, API 키)가 포함된 구성 파일에 대한 접근을 제한하세요.
- 지원되는 경우 Windows 데이터 보호 API(DPAPI) 또는 Key Vault 솔루션을 사용하세요.
- 시크릿 정보는 바이너리 파일과 별도로 저장하고 하드 코딩을 피하세요.

암호화 키 파일 보호 (`util/` 디렉터리)

- BioStar X 서비스 계정만 읽기 권한을 갖도록 NTFS 권한을 제한하세요.

- 일반 사용자 및 대화형 로그인에 대한 접근을 차단하세요.
- 업그레이드 전에 `util/` 디렉터리를 오프라인 저장소에 안전하게 백업하세요.

> **주의**
> 암호화 키 파일을 분실하거나 손상되면 데이터 손실 또는 무단 복호화가 발생할 수 있습니다.

> **모범 사례**
>
> 저장된 시크릿 정보(예: 데이터베이스 암호, API 키)를 주기적으로 교체하세요.

애플리케이션 런타임 구성 요소 유지

- BioStar X와 종속 런타임 구성 요소(예: Visual C++ 재배포 가능 패키지)를 최신 상태로 유지하세요.
- 패치 관련 벤더 공지 사항을 구독하세요.
- 다운타임을 방지하기 위해 업데이트 절차를 문서화하세요.

애플리케이션 허용 목록

- Windows Defender 애플리케이션 제어(Windows Defender Application Control, WDAC) 또는 AppLocker를 사용하여 신뢰할 수 있는 바이너리만 허용하세요.
- 임시 디렉터리(예: `%TEMP%`, `%APPDATA%`)에서의 실행을 차단하세요.

단계별 안내

1. **로컬 보안 정책**을 실행하고 **응용 프로그램 제어 정책** → **AppLocker**로 이동하세요.
2. 실행 파일, 스크립트 및 DLL 경로에 대한 규칙을 정의하세요.
3. 서명된 BioStar X 바이너리를 허용하세요.
4. 사용자가 쓰기 권한이 있는 디렉터리에서의 실행을 거부하세요.
5. **먼저 감사 모드로 배포**하여 테스트하고 적용하세요.

데이터베이스 및 데이터 보호

BioStar X는 사용자 크리덴셜, 액세스 로그, 구성 데이터와 같은 중요한 정보를 저장할 데이터베이스가 필요합니다. 배포 환경에 따라 **MariaDB**(11.4) 또는 **Microsoft SQL Server**를 사용합니다.

인증 및 접근 제어

- 모든 데이터베이스 연결에 인증을 요구하도록 설정하세요.
- BioStar X 전용 데이터베이스 계정을 사용하고, 공유 계정 또는 기본 계정을 사용하지 마세요.

- 필요한 최소 권한 역할(애플리케이션 데이터에 대한 읽기/쓰기, 스키마 수정 불가)만 할당하세요.
- 사용하지 않거나 과도한 권한을 가진 사용자가 있는지 정기적으로 데이터베이스 계정을 감사하세요.
- 특히 IP 또는 인프라 변경 후에는 사용하지 않거나 오래된 데이터베이스 사용자 항목을 삭제하세요.

> **주의**
> `sa` 또는 동급의 슈퍼 유저 계정을 사용해 BioStar X에 연결하지 마세요.

전송 중 데이터 암호화

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
```

설정 확인

SQL

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

SQL Server

1. **SQL Server 구성 관리자**를 실행하세요.
2. **SQL Server 네트워크 구성 → MSSQLSERVER에 대한 프로토콜**로 이동하세요.
3. **암호화 강제**를 활성화하세요.
4. 서버에 신뢰할 수 있는 인증서를 설치하세요.

미사용 데이터 암호화

MariaDB

- 저장 데이터 암호화를 위해 `file_key_management` 플러그인을 활성화하세요.
- 안전한 키 파일에 암호화 키를 정의하세요.
- 전체 TDE를 사용할 수 없다면 테이블별로 암호화를 적용하세요.

> **주의**
> 약간의 성능 저하(일반적으로 3~5%)가 발생할 수 있습니다. 데이터베이스를 다른 서버로 이동 또는 복원하는 경우 인증서와 키가 필요합니다. BioStar X의 복원 기능은 암호화된 백업을 지원하지 않으므로 수동으로 처리해야 합니다.

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;
```

데이터베이스 감사 활성화

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);
```

백업 및 보안 저장소

- BioStar X 데이터베이스를 정기적으로 암호화하여 백업합니다.
- 백업은 동일한 호스트가 아닌 별도의 보안 서버에 저장합니다.
- 백업 및 복원을 주기적으로 테스트합니다.
- BitLocker로 암호화된 볼륨에 백업을 저장합니다.

MariaDB

Bash

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

> **주의**
> BioStar X 백업 기능(수동 또는 예약)은 암호화되지 않습니다. BioStar X 복원 기능은 암호화된 백업을 지원하지 않습니다.

SQL Server

SQL

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

원격 접근 제한

MariaDB

my.cnf

```
bind-address=127.0.0.1
```

SQL Server

BioStar X 애플리케이션 서버에서만 연결을 허용하도록 방화벽 규칙을 구성하세요.

모니터링 및 감사

모니터링 및 감사를 통해 BioStar X의 보안 상태를 파악할 수 있습니다. 효과적인 감사를 위해서는 **운영 체제**, **애플리케이션**, **데이터베이스** 수준에서 로그를 활성화하고, 이를 중앙 집중화하여 정기적으로 검토해야 합니다.

로깅 정책 정의

로그에 기록해야 하는 이벤트, 보존 기간, 검토 담당자를 명시하는 로깅 정책을 수립해야 합니다.

최소한 다음 이벤트 유형을 로깅해야 합니다.

- 인증 시도(성공/실패)
- 권한 변경
- 구성 변경
- 데이터베이스 접근
- 방화벽 활동

> **알아두기**
> **보존 기간**: 일반적으로 로컬에서 90~180일, 중앙화된 시스템에서는 더 오랜 기간 설정하는 것을 권장합니다.

Windows 이벤트 로깅 및 모니터링 활성화

- 이벤트 뷰어에서 보안, 애플리케이션, 시스템 로깅이 활성화되어 있는지 확인하세요.
- 로그 크기를 구성하세요. 보안 로그는 최소 1GB 이상으로 설정하는 것을 권장합니다.
- **로컬 보안 정책**(`secpol.msc`) → **로컬 정책** → **감사 정책**에서 다음 정책에 대한 감사를 설정하세요.

  > *로그온 이벤트, 권한 사용, 정책 변경, 계정 로그온, 개체 접근*

중앙화된 로그 전달 및 SIEM 연동

- 중앙 SIEM 또는 로그 관리 시스템으로 로그를 전달하세요.
- 지원 옵션: Splunk, Elastic Stack, Microsoft Sentinel, Windows Event Forwarding(WEF)

> **모범 사례**
>
> 전송 중인 로그를 TLS로 암호화하여 가로채기 또는 변조를 방지하세요.

애플리케이션 수준 감사 활성화

- BioStar X → **설정** → **서버**에서 **시스템 로그 단계 설정** 섹션으로 이동하세요.
- 로그 파일 위치는 `[BioStar X 설치 경로]\logs\acs.log` 경로입니다.
- BioStar X 서비스 계정과 관리자만 접근할 수 있도록 권한을 설정하세요.
- SIEM 또는 중앙 로깅 솔루션으로 로그를 전달하세요.

데이터베이스 감사 활성화

- **MariaDB**: 감사 플러그인(`server_audit`)을 사용합니다.
- **SQL Server**: SQL Server Audit 기능을 사용하여 로그를 파일 또는 이벤트 로그에 기록합니다.
- 중앙 로그 시스템으로 전달합니다.

> **알아두기**
> 데이터베이스 감사 활성화에 대한 자세한 내용은 데이터베이스 및 데이터 보호를 참조하세요.

방화벽 및 네트워크 활동 모니터링

- **고급 보안이 포함된 Windows Defender 방화벽**(`wf.msc`) → **속성** → **로깅**에서 패킷 손실 로깅을 활성화하세요.
- `%systemroot%\system32\LogFiles\Firewall\pfirewall.log` 경로에 로그를 저장하세요.
- SIEM으로 로그를 전달하세요.
- 이상 징후를 탐지하기 위해 IDS/IPS(Snort, Suricata, Zeek)를 배포합니다.

> **주의**
> 방화벽 로그는 빠르게 증가하므로 로그 순환 및 안전한 저장소를 구현해야 합니다.

검토 및 알림

중요 이벤트에 대한 자동 알림을 설정하세요.

- 반복된 로그인 실패
- 권한 상승
- 예기치 않은 서비스 시작 및 종료
- 데이터베이스 스키마 수정

정기적으로 로그를 수동 검토하세요.

패치 및 유지 관리

서버를 강화한 후에는 그 상태를 유지해야 합니다. 새로운 취약점은 지속적으로 발견되며, 패치되지 않은 시스템은 시간이 지날수록 위험에 노출됩니다. 이 문서에서는 정기적인 패치 적용, 취약점 검사, 자산 관리를 통해 BioStar X 서버의 보안 기준선을 지속적으로 유지하는 방법을 안내합니다.

보안 구성 백업 및 복원

PowerShell

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

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

패치 관리 정책 수립

- 운영 체제, 데이터베이스 엔진, BioStar X 소프트웨어 및 타사 종속성을 포괄하는 공식적인 패치 정책을 정의하세요.
- 운영체제 패치는 2주 이내, 애플리케이션 패치는 1개월 이내와 같이 일정을 수립하세요.
- 패치로 인해 시스템이 불안정해질 경우 롤백 및 복구 절차를 포함한 정책을 수립하세요.

> **주의**
> BioStar X에 포함된 타사 종속성에 패치를 적용하기 전에 슈프리마 기술 지원팀(CS@suprema.co.kr)에 업데이트 지원 여부를 확인하세요. 스테이징 환경이나 가상 머신(VM)에서 먼저 테스트하기를 권장합니다.

BioStar X 소프트웨어 업데이트 유지 관리

- BioStar X를 제공된 최신 지원 버전으로 최신 상태를 유지하세요.
- 슈프리마 지원 페이지에서 릴리스 노트 및 보안 공지를 구독하세요.
- 프로덕션 환경에 배포하기 전에 스테이징 환경에서 새 릴리스를 테스트하세요.

데이터베이스 엔진 최신 상태 유지

- 슈프리마의 보안 권고에 따라 MariaDB 11.4 또는 Microsoft SQL Server 업데이트를 적용하세요.
- 지원하지 않는 버전을 사용하지 마세요.

종속성 및 런타임 구성 요소 관리

- Visual C++ Redistributables, Java 런타임과 같은 지원 프레임워크에 패치를 적용하세요.
- 리버스 프록시/WAF 소프트웨어를 사용한다면 유지 관리하세요.
- 분기별 또는 보안 권고가 발표될 때마다 업데이트하세요.

정기적인 취약점 검사 수행

- BioStar X 호스트에 대해 분기별(높은 보안 환경에서는 매월) 취약점 검사를 실행하세요.
- Nessus, OpenVAS, Qualys, Microsoft Defender for Endpoint와 같은 도구를 사용하세요.
- 패치 주기 후 검사를 예약하고 티켓팅 시스템을 통해 해결 상황을 추적하세요.

자산 및 패치 목록 유지 관리

- 모든 BioStar X 서버의 운영 체제 버전, 데이터베이스 버전 및 패치 수준을 포함한 자산 목록을 유지 관리하세요.
- 가능하면 자동화 도구(예: SCCM, Intune, Ansible)를 활용하세요.
- 분기별로 재고를 검토하세요.

물리적 보안

물리적 보안 제어를 통해 권한이 없는 사용자가 BioStar X가 저장된 서버 또는 스토리지에 직접 접근하는 것을 방지하세요.

안전한 서버 위치

- BioStar X 서버는 물리적으로 보안이 강화된 데이터 센터 또는 잠금 장치가 있는 서버실에 설치하세요.
- 접근 권한은 승인된 IT 직원으로만 제한해야 합니다.
- 서버실에 CCTV를 설치하고 출입 기록을 관리하세요.
- 서버를 잠금 장치가 있는 랙이나 케이지에 보관하고 방문객의 출입을 기록하세요.

이동식 및 백업 미디어 보호

- 백업 드라이브 또는 백업 테이프는 접근이 통제된 안전한 장소에 보관하세요.
- BioStar X 데이터가 저장된 모든 이동식 저장 매체는 암호화해야 합니다.
- 백업 파일을 전송하기 전에 AES-256으로 암호화해야 합니다.

> **모범 사례**
>
> 물리적 저장 매체에 대한 의존도를 줄이기 위해 **클라우드 기반 암호화 백업** 사용을 권장합니다.

안전한 BIOS/UEFI 설정

- BIOS/UEFI 암호를 설정하여 권한이 없는 사용자의 설정 변경을 방지하세요.
- 외부 기기(USB, DVD)를 통한 부팅을 비활성화하세요.
- 지원되는 경우 보안 부팅을 활성화하세요.

> **주의**
> BIOS/UEFI 암호는 Secure vault에 문서화하세요. 암호를 분실하면 정상적인 유지 보수가 불가능해질 수 있습니다.

장치 도난 방지

- 모든 시스템 및 데이터 드라이브에 BitLocker를 사용하여 전체 디스크 암호화를 활성화하세요.
- BitLocker를 구성에 대한 자세한 내용은 운영체제 구성을 참조하세요.
- 가능하다면 TPM + PIN을 사용하여 보안을 강화하세요.
- 데이터 센터 이외의 환경에서는 케이블 잠금 장치 또는 보안 랙을 사용하세요.

환경 제어

- 서버실의 온도, 습도 및 전원 공급 장치(UPS)가 안정적인지 확인하세요.
- 소화기 또는 FM200이나 불활성 가스와 같은 화재 방지 시스템을 설치하세요.
- 센서를 사용하여 온도/습도를 모니터링하세요.

BioStar X 강화

BioStar X를 안전하게 운영하려면 두 가지 보안 계층을 함께 강화해야 합니다.

- **시스템 보안**은 기본 관리자 계정 변경, 역할 기반 접근 제어, 강력한 인증, 장치 암호화 통신을 통해 애플리케이션 자체를 보호합니다.
- **개인 데이터 보안**은 사용자 정보와 바이오메트릭 데이터를 데이터베이스 암호화와 최소 저장 원칙으로 보호합니다.

이 두 영역을 모두 구성해야 규정 준수(GDPR, ISO 27001 등)를 충족하고, 데이터 침해 위험을 최소화할 수 있습니다.

시스템 보안

BioStar X 서버 보안을 강화한 후 다음 단계는 BioStar X 애플리케이션 자체의 보안 설정입니다. 기본 관리자 계정, 취약한 암호, 암호화되지 않은 장치 통신은 인프라 수준의 보안을 우회하여 시스템을 직접 침해하는 경로가 됩니다. 이 문서에서는 BioStar X의 인증, 역할 관리, 장치 암호화, 백업 전략을 통해 애플리케이션 계층의 보안 기준선을 확립하는 방법을 안내합니다.

기본 관리자 아이디 및 암호 변경

설치 직후 기본 **Administrator** 계정의 로그인 아이디(`admin`)를 변경하고 강력하고 고유한 암호로 업데이트하세요.

기본 크리덴셜은 공격자가 침입하는 가장 일반적인 경로 중 하나입니다. 모든 BioStar X 설치는 사전 정의된 Administrator 계정(UID: 1)이 포함되어 있으므로, 이를 변경하지 않으면 시스템이 예측 가능해지고 무차별 대입 공격이나 사전 공격에 매우 취약해집니다.

1. 기본 관리자(`admin`) 계정으로 로그인하세요.
2. **사용자**로 이동하세요.
3. 사용자 목록에서 **Administrator** 계정을 더블 클릭하세요.

   > *사용자 이름: Administrator, UID: 1*

4. 사용자 편집 페이지의 **권한** 섹션에서 아래 항목을 변경하세요.
   - **로그인 ID**: `admin`을 고유하고 쉽게 알아볼 수 없는 사용자 아이디로 변경하세요. `root`, `system`, 또는 회사 이름을 사용하지 마세요.
   - **암호**: 안전한 암호로 변경하세요. BioStar X는 기본적으로 **중간 강도**의 암호를 사용합니다. 암호는 8~32자 길이이며, 대문자/소문자와 숫자를 모두 포함해야 합니다.
5. 화면 오른쪽 상단의 **저장** 버튼을 클릭하세요.
6. 로그아웃한 후 **새로운 아이디와 비밀번호**로 다시 로그인하세요.

> **모범 사례**
> - 개인 이름이나 단순한 패턴(`admin1`, `company2025`)은 **사용하지 마세요**.
> - 새 아이디와 비밀번호는 안전한 암호 관리자 또는 기업용 비밀번호 저장소에 저장하세요.
> - 비상 사용을 위한 **보조 관리자 계정**을 생성하세요.
> - 관리자 로그인 시도에 대한 **감사 로그**를 정기적으로 검토하세요.

접근 권한 분리

BioStar X 내에서 **전체 관리자**, **오퍼레이터**, **감사자** 계정에 명확히 정의된 권한을 부여하고, 역할 분리를 엄격하게 적용해야 합니다.

모든 작업을 하나의 최고 관리자 계정으로 처리하는 것은 불필요한 위험을 초래합니다. 역할을 분리하면 다음과 같은 효과를 얻을 수 있습니다.

- 실수로 인한 설정 오류 발생 가능성 감소
- 한 명의 사용자가 무제한 권한을 갖지 않도록 내부자 위협 방지
- 역할별 명확한 책임 소재를 통해 감사 가능성 및 규정 준수 향상

이러한 방식은 ISO 27001, NIST 및 기타 프레임워크의 핵심 원칙인 **최소 권한** 및 **직무 분리**와 일맥상통합니다.

설치 후 권장 조치

1. **기본 관리자(`admin`) 이름 변경 및 보안 설정**

   기본 관리자(`admin`) 계정은 **비상시 전용 계정**으로 관리합니다. 자세한 내용은 기본 관리자 아이디 및 암호 변경을 참고하세요.

2. **명명된 역할 계정 생성**

   - **전체 관리자(Admin) 역할**: 시스템 구성 및 역할 관리 전용으로, 신뢰할 수 있는 1~2명의 사람으로 제한합니다.
   - **오퍼레이터(Operator) 역할**: 사용자 추가 및 제거, 출입문/장치 제어 등 일상적인 운영을 담당합니다. 시스템 보안 설정 또는 감사 로그 접근은 없습니다.
   - **감사자(Auditor) 역할**: 로그, 보고서, 구성에 대한 읽기 전용 액세스 권한만 부여합니다. 시스템의 주요 설정을 변경할 수 없습니다.

3. **멀티팩터 인증(MFA) 인증 활성화**

   모든 역할 계정에 MFA를 적용하세요. 자세한 내용은 멀티팩터 인증 (MFA)을 참고하세요.

4. **커스텀 권한 계정 사용**(필요한 경우)

   - **설정** → **계정**으로 이동한 후 **커스텀 권한 추가** 버튼을 클릭하세요.
   - 사용자 그룹, 장치 그룹, 출입문 그룹, 엘리베이터 그룹, 출입 그룹에 걸쳐 세부적인 액세스 권한을 구성하세요.
   - **메뉴 별 권한**에서 각 메뉴 항목에 대해 **수정/보기** 또는 **보기** 권한을 선택하세요.

커스텀 감사자(Auditor) 역할 생성 예시

1. **설정** → **계정**으로 이동하세요.
2. **커스텀 권한 추가** 버튼을 클릭하세요.
3. 커스텀 권한의 **이름**을 `Auditor`로 입력하고, 설명을 추가하세요.
4. **메뉴 별 권한**에서 아래와 같이 권한을 설정하세요.
   - **사용자**: **보기**
   - **모니터링**: **보기**
   - **데이터**: **보기**
   - **대시보드**: **보기**

- **설정**: 선택하지 않음

5. 지정된 감사자 계정에 역할을 할당하려면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

> **모범 사례**
> - **개인별로 고유한 계정**을 할당하여 로그인 정보를 공유하지 마세요.
> - 분기별로 계정 역할을 검토하고 사용하지 않는 계정을 삭제합니다.
> - 이름이 변경된 기본 제공 관리자 계정은 비상시에만 사용합니다.

강력한 암호 정책 적용

모든 사용자 계정에 강력한 암호 정책을 적용하도록 BioStar X를 구성하세요.

암호 정책 옵션

- **비밀번호 레벨**
  - **낮음**: 최대 32자까지 입력할 수 있습니다.
  - **보통**: 비밀번호를 설정할 때 8~32 영어 문자(대문자 또는 소문자)와 숫자를 조합해야 합니다.
  - **강함**: 비밀번호를 설정할 때 10~32 영어 문자(대문자와 소문자, 최소 한 글자 이상의 대문자 포함)와 숫자, 특수 기호를 조합해야 합니다.
- **비밀번호 변경 주기**: 1일부터 180일까지 설정할 수 있습니다.
- **비밀번호 최대 실패 허용 횟수**: 설정한 횟수를 초과하여 비밀번호를 잘못 입력하면 제한 시간 동안 로그인할 수 없습니다. 기본값은 10분 내 100회이며, **15분 내 5~10회로 줄이는 것**을 권장합니다.
- **비밀번호 일일 변경 허용 횟수**: 사용자가 하루에 비밀번호를 변경할 수 있는 횟수를 제한할 수 있습니다.

비밀번호 정책 강화

1. **설정** → **시스템** → **시스템 보안**으로 이동하세요.
2. **로그인 비밀 번호**에서 아래와 같이 설정하세요.
   - **비밀번호 레벨**: **강함**
   - **비밀번호 변경 주기**: 활성화 후, **90일**로 설정하세요.
   - **비밀번호 최대 실패 허용 횟수**: 활성화 후 **15분 내 5회**로 설정하세요.
   - **비밀번호 일일 변경 허용 횟수**: 활성화 후 최대 **5회**로 설정하세요.
3. 화면 오른쪽 하단의 **확인**을 클릭하세요.

모든 사용자에게 새로운 비밀번호 정책을 공지하세요.

세션 보안

메뉴 경로: **설정** → **시스템** → **시스템 보안** → **세션 보안**

각 계정이 한 번에 하나의 활성 세션에만 사용될 수 있도록 **동시 접속 허용**을 비활성화하세요.

- **활성**: 동일한 크리덴셜로 여러 사용자가 동시에 로그인할 수 있습니다.
- **비활성**: 계정당 하나의 로그인만 허용합니다. 새 로그인이 발생하면 이전 세션은 자동 로그아웃됩니다.

> **주의**
>
> - 계정 공유가 감지되지 않으면 누가 어떤 작업을 수행했는지 알 수 없습니다.
> - 탈취된 크리덴셜을 획득한 공격자는 정당한 사용자가 활동 중인 동안에도 눈에 띄지 않게 로그인할 수 있습니다.
> - 감사 로그는 특정 사용자의 작업을 추적할 수 없으므로 그 가치가 떨어지게 됩니다.

멀티팩터 인증 (MFA)

BioStar X의 모든 고위 권한 계정(관리자, 운영자)에 대해 지문 인증을 추가하여 멀티팩터 인증을 활성화할 수 있습니다.

> **BioStar X에서 작동 방식**
>
> - 슈프리마 BioMini 또는 BioMini Plus 2와 같은 지문 스캐너를 사용하여 MFA를 구현합니다.
> - 사용자가 로그인 아이디와 비밀번호를 입력하면 시스템에서 지문 스캔을 요청합니다.

> **주의**
>
> - 관리자 계정에 MFA가 활성화되어 있고, 지문 인식에 실패하면 계정이 잠길 수 있습니다.
> - 클라우드 인터페이스를 통한 로그인 시 MFA는 지원되지 않습니다.
> - Active Directory 또는 지원되지 않는 서비스를 통해 인증된 계정에는 MFA를 활성화할 수 없습니다.

단계별 안내

1. BioStar X 서버 또는 클라이언트 PC에 지문 스캐너를 연결하고 설치하세요.
2. BioStar X에서 **사용자**로 이동하세요.
3. 사용자 프로필을 열고 지문을 등록하세요.
4. **권한** 섹션에서 **다중 인증 로그인** 항목을 **사용**으로 설정하세요.
5. 변경 사항을 적용하려면 화면 오른쪽 상단의 **저장** 버튼을 클릭하세요.

로그아웃 후 유효한 크리덴셜을 입력하고, 지문을 스캔하여 로그인하세요.

> **모범 사례 및 안전 조치**
>
> - 스캐너 오류를 대비하여 다른 손가락으로 대체 지문을 등록하세요.
> - 바이오메트릭 장치 오류 발생 시 복구할 수 있도록 기본 제공되는 관리자 계정('비상용' 계정)을 백업 계정으로 설정해 두세요.
> - 멀티팩터 인증(MFA)이 활성화된 계정을 문서화하고 복구 메커니즘을 유지 관리하세요.

장치와의 보안 통신

디지털 인증서(TLS/SSL 방식)를 사용하여 BioStar X와 연결된 장치 간 트래픽을 암호화하려면 **장치와 보안 통신**을 활성화하세요.

옵션 A: 서버 생성 인증서(기본값)

BioStar X에서 인증서를 생성하여 장치에 자동으로 프로비저닝합니다.

> **주의**
> 이 기능을 비활성화했다가 다시 활성화하면 새 인증서가 생성되어 장치를 수동으로 재설정해야 합니다.

옵션 B: 외부 인증서(엔터프라이즈 사용 권장)

- 조직의 인증서 체인과 개인 키를 업로드할 수 있습니다.
- 엔터프라이즈 PKI와의 연동이 용이합니다.

단계별 안내

1. 관리자 계정으로 BioStar X에 로그인하세요.
2. **설정** → **시스템** → **시스템 보안** → **고급 보안 설정**으로 이동하세요.
3. **장치와 보안 통신**를 **사용**으로 설정하세요.
4. 외부 CA 인증서를 사용한다면 **외부 인증서 사용**를 **사용**으로 설정하세요.
    - 루트 CA, 공개 인증서 및 개인 키를 업로드하세요.
5. 적용하고 장치가 보안 채널을 통해 연결되는지 확인하세요.

> **모범 사례**
> - 항상 **강력한 암호 키**(RSA 2048 이상 또는 이에 상응하는 ECC)를 사용하세요.
> - 장치 연결 방식(호스트 이름 또는 IP 주소)과 일치하는 적절한 **CN/SAN 값**을 가진 인증서를 사용하세요.
> - 만료 전에 인증서를 교체하고 갱신 일정을 관리하세요.

> **로그 업로드 참고**
>
> **로그 업로드**가 **수동**으로 설정되어 있다면, **이벤트 가시성 지연** 또는 **감사 추적 누락**의 위험이 있습니다. 가능하다면 **로그 업로드**를 **자동**으로 유지하세요.

장치 해시키 수동 관리

BioStar X와 장치 간에 사용되는 암호화 키를 수동으로 제어하려면 **장치 해시키 수동 관리**를 활성화해야 합니다. 이 기능은 탬퍼 방어 기능을 활성화합니다. 물리적 변조가 감지되면 기기에서 중요한 데이터가 자동으로 삭제됩니다.

알아두기

장치와의 보안 통신이 전송 중인 데이터를 보호하지만, **장치 해시키 수동 관리**는 아래와 같은 추가 기능을 제공합니다.

- **데이터 암호화 키가 자동으로 생성되는 것이 아니라 관리자가 관리**합니다.
- **탬퍼 방어** 기능을 활성화합니다. 장치가 무단 접근 또는 조작을 감지하면 저장된 사용자 정보, 로그 및 암호화 키를 삭제합니다.

주의

- **관리자 계정이 아닌 사용자가 로그인 비밀번호 또는 PIN을 가지고 있다면 수동 키 관리를 적용할 수 없습니다.**
- 활성화하기 전에 해당 로그인 정보를 제거하세요.

단계별 안내

1. 관리자 계정으로 BioStar X에 로그인하세요.
2. **설정** → **시스템** → **시스템 보안** → **고급 보안 설정**으로 이동하세요.
3. **장치 해시키 수동 관리**를 **사용**으로 설정하세요.
4. 경고 팝업을 읽고 확인하세요.
5. 적용하기 전에 장치에서 관리자 이외의 사용자 비밀번호/PIN 로그인을 모두 제거하세요.
6. 메시지가 표시되면 암호화 키와 관리자 비밀번호를 변경하세요.
7. 장치가 여전히 사용자, 로그 및 이벤트를 동기화할 수 있는지 확인하세요.
8. 키 변경 사항을 문서화(날짜, 담당 관리자, 다음 변경 예정일)하세요.

모범 사례

- 장치 해시키를 매년 또는 6개월마다 정기적으로 변경하세요.
- 모든 변경 사항을 기록하고 안전한 저장소에 보관하세요.
- 실험실/임시 장치에서 탬퍼 이벤트를 테스트하세요.
- 심층 방어(defense-in-depth)를 위해 장치와의 보안 통신과 함께 사용하세요.

시스템 백업

시스템 백업 기능을 사용하여 BioStar X의 데이터베이스, 시스템 설정, 키 값을 정기적으로 백업하세요.

주의

- BioStar X와 MSSQL이 서로 다른 서버에 설치된 경우, **시스템 백업/복원** 기능을 사용할 수 없습니다.
- BioStar X 백업 기능(수동 또는 예약)은 **암호화되지 않습니다**.
- BioStar X 복원 기능은 암호화된 백업을 지원하지 않습니다.

수동 백업 설정

메뉴 경로: 설정 → 시스템 → 시스템 백업

- **백업 파일 저장 경로**: 디렉터리를 지정하세요. 경로는 존재해야 하며 적절한 쓰기 권한이 있어야 합니다.
- **최대 백업파일 수**: 1~100개까지 설정할 수 있으며, 일일 예약의 경우 최소 **7~10개의 순환 백업**을 유지하도록 권장합니다.
- **백업하기**: 필요에 따라 즉시 백업을 실행합니다. 업그레이드 또는 주요 변경 전에 유용합니다.

시스템 자동 백업

- **빈도**: **일간** / **주간** / **월간**
- **시간**: 시간을 지정하세요. BioStar X의 서버 시간대에 맞춰 예약이 실행됩니다.

> **모범 사례**
>
> 운영 환경의 경우 **사용자가 적은 시간대에 매일 백업**을 권장합니다.
>
> > *예: 현지 시간 오전 2시*

자동 백업 구성

1. **설정** → **시스템** → **시스템 백업**으로 이동하세요.
2. **시스템 자동 백업**을 설정하세요.
   - **빈도**: **일간**
   - **시간**: 02:00 (또는 다른 사용자가 적은 시간대)
   - **최대 백업파일 수**: 30
3. 설정을 저장하려면 **확인**을 클릭하세요.
4. 대상 디렉터리에서 백업 파일을 생성했는지 확인하세요.
5. 스테이징 환경에서 **복원 과정**을 주기적으로 테스트하세요.

> **주의**
> 서버가 UPS로 보호되는지 확인하세요. '진행 중' 상태가 표시되는 동안에는 작업을 중단하지 마세요. 백업 또는 복원을 중단하면 데이터베이스가 손상될 수 있습니다.

디렉터리 연동

디렉터리 연동을 통해 BioStar X는 **Entra ID(Azure AD)** 또는 **Microsoft Active Directory(AD)**와 같은 엔터프라이즈 ID 시스템과 연결할 수 있습니다.

- **강화된 보안**: 암호 규칙, 멀티팩터 인증(MFA) 및 조건부 액세스에 대한 엔터프라이즈 정책을 BioStar X에 자동 적용할 수 있습니다.
- **중앙 집중식 제어**: 사용자 수명 주기가 Entra ID/AD에서 관리되므로 계정 만료 위험이 줄어듭니다.

- **감사 및 규정 준수**: 모든 사용자 작업이 회사 계정과 연결됩니다.

> **알아두기**
> 디렉터리 연동에는 **어드밴스**(Advanced) 라이선스가 필요합니다.

> **모범 사례**
> - 권한이 제한된 **전용 Entra ID/AD 서비스 계정**을 사용하세요.
> - 동기화를 **관련 그룹**으로만 제한하세요.
> - Active Directory 연결에는 항상 **LDAPS**를 사용하세요.
> - 동기화된 계정을 주기적으로 검토하여 오래된 항목이 있는지 확인하세요.

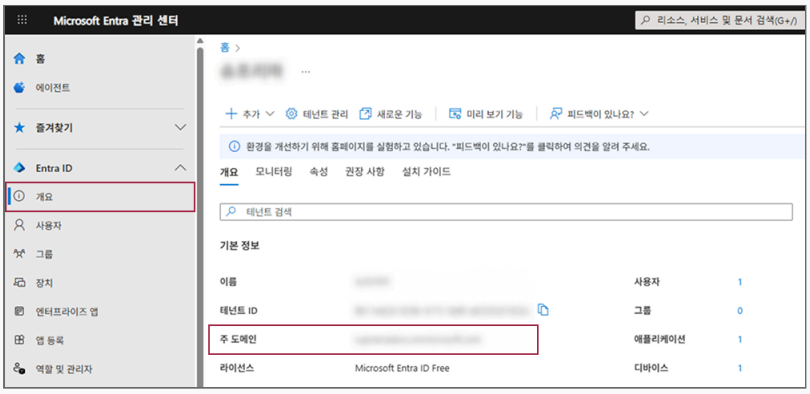
Microsoft Entra ID 단계별 안내

1. 관리자 계정으로 BioStar X에 로그인하세요.
2. **설정** → **디렉토리 연동**으로 이동하세요.
3. **디렉토리 서비스**에서 **Microsoft Entra ID**를 선택하세요.
4. **디렉토리 서버**를 구성하세요.
   - **클라이언트 ID**: **Entra ID**에서 등록한 애플리케이션의 **클라이언트 아이디**(**Client ID**)를 입력하세요.
   - **클라이언트 시크릿**: **Entra ID**에서 등록한 애플리케이션의 **인증서 및 암호**(**Certificates & secrets**)에 추가한 **클라이언트 암호**(**Client secrets**)를 입력하세요.
   - **주 도메인**: **Entra ID**에서 조직을 만들 때 입력한 기본 도메인 이름을 입력하세요.
5. BioStar X에 사용자 그룹 정보를 가져오려면 **연결** 버튼을 클릭하세요.
6. **Entra ID로 BioStar X 로그인**을 활성화하세요.
7. **리디렉션 URI**를 복사하고, **Entra ID** 포털의 SSO 리디렉션 설정에 붙여넣으세요.
8. **동기화 모드**에서 원하는 동기화 방식을 선택하세요.
9. 설정을 저장하려면 **확인** 버튼을 클릭하세요.

사용자 목록을 확인하여 동기화가 완료되었는지 점검하세요.

알아두기

- **Entra ID**에서 애플리케이션을 등록하는 방법은 다음 링크를 참고하세요.
- **Entra ID**에서 **인증서 및 암호** 설정 방법은 다음 링크를 참고하세요.
- **테넌트 ID**는 **Entra ID**에서 등록한 애플리케이션의 **개요(Overview)**에서 확인할 수 있습니다.
- **주 도메인** 정보는 **Entra ID**의 **개요(Overview)**에서 확인할 수 있습니다.



Microsoft Active Directory 단계별 안내

1. 관리자 계정으로 BioStar X에 로그인하세요.
2. **설정** → **디렉토리 연동**으로 이동하세요.
3. **디렉토리 서비스**에서 **Microsoft Active Directory**를 선택하세요.
4. **디렉토리 서버**를 구성하세요.
   - **서버 주소**: AD 서버의 IP 주소 또는 호스트 이름입니다.
   - **사용자명** / **비밀번호**: AD 서비스 계정 크리덴셜입니다.
   - **기본 Domain 명**: AD 도메인의 고유 이름입니다.
5. 암호화된 연결(LDAPS)을 사용하려면 **암호화 사용**을 활성화하세요.
   - AD 서버에 AD 인증서 서비스를 설치하세요.
   - 루트 인증서를 내보내고 *.jks* 파일로 변환하여 BioStar X 설치 경로에 배치하세요.
   - BioStar X에서 **키 저장소 비밀번호**를 입력하세요.
6. BioStar X에 사용자 그룹 정보를 가져오려면 **연결** 버튼을 클릭하세요.
7. **사용자 그룹 필터**에서 필요 없는 그룹은 선택 해제하세요.
8. **Active Directory로 BioStar X 로그인**을 활성화하세요.
9. **동기화 모드**에서 원하는 동기화 방식을 선택하세요.
10. 설정을 저장하려면 **확인** 버튼을 클릭하세요.

사용자 목록을 확인하여 동기화가 완료되었는지 점검하세요.

시스템 로그 설정

메뉴 경로: 설정 → 서버 → 서버

감사 및 문제 해결에 필요한 충분한 데이터를 보존하도록 BioStar X 로깅을 구성하세요.

시스템 로그 저장 기간

- **로그 업로드**: 이벤트 로그의 업로드 방법을 선택하세요.
  - **자동**(기본값): 보존 기간이 지나면 로그를 자동 삭제합니다.
  - **수동**: 수동으로 로그를 삭제해야 합니다.
- **시스템 로그 저장 기간**: 1~120일(기본값: 60일)

> **모범 사례**
>
> 규정 준수가 중요한 환경에서는 보존 기간을 90~120일로 설정하고 로그를 SIEM으로 전송하세요.

시스템 로그 수준 설정

하위 시스템별: 디버그, 네트워크, SQL, 시스템, 웹, 웹소켓

수준	설명
추적	모든 항목 캡처(매우 상세)
디버그	개발자 수준의 상세 로그
정보	운영 이벤트, 성공 연결(대부분 기본값)
경고	잠재적 문제
에러	실패만

> **주의**
> 운영 환경에서 **추적** 또는 **디버그** 모드로 실행하면 과도한 로그가 생성되어 성능 저하 및 디스크 용량 부족 현상이 발생할 수 있습니다. 단기적인 문제 해결 용도로만 사용하세요.

BioStar X 기본 로그 수준

- 디버그, SQL, WebSocket: **사용 안 함**
- 네트워크, 시스템, 웹: **정보**

서버 포트 구성

BioStar X 포트를 명시적으로 구성하고 가능하다면 보안 채널을 우선 사용하세요. 시스템 액세스에는 기본 HTTPS 포트(`443`)를 사용하고, 장치 통신 포트는 신뢰할 수 있는 네트워크로만 제한해야 합니다.

HTTPS 포트 변경

1. **BioStar X Service Manager**(`http:/127.0.0.1:28088/`)를 실행하세요.
2. 왼쪽 사이드 메뉴에서 **SERVICE SETTINGS**를 클릭하세요.
3. **Unified Gateway Service**에서 **HTTPS Port**(기본값: 443) 필드로 이동하세요.
4. 포트 번호를 원하는 값으로 변경하세요.

   > *예: 8443*

5. **Apply** 버튼을 클릭하고, 필요시 서비스를 재시작하세요.
6. 변경한 포트에 맞게 방화벽 규칙 및 클라이언트 연결을 업데이트하세요.

개인 데이터 보안

BioStar X는 사용자 크리덴셜, 바이오메트릭 템플릿, 개인 식별 정보를 저장합니다. 데이터베이스가 암호화되지 않으면 침해 시 이러한 정보가 평문으로 노출되어 신원 도용, 법적 책임, 규정 위반으로 이어질 수 있습니다. 이 문서에서는 개인 정보 데이터베이스 암호화를 활성화하고 바이오메트릭 이미지 저장을 최소화하여 민감한 데이터를 보호하는 방법을 안내합니다.

개인 정보 데이터베이스 암호화

모든 민감한 사용자 및 크리덴셜 정보가 암호화된 상태로 저장되도록 **개인 정보 DB 암호화**를 활성화하세요.

암호화 데이터 범위

개인 정보 DB 암호화를 활성화하면 다음 항목을 데이터베이스에 저장할 때 암호화됩니다.

- 프로필 이미지
- 사용자 아이디, 이름, 전화번호, 사용자 IP 주소, 이메일 주소
- 로그인 아이디 및 로그인 비밀번호
- 얼굴 템플릿, 지문 템플릿
- 카드 아이디, 스마트 카드 레이아웃 키
- 사용자 및 방문자 맞춤 정보
- 이미지 로그 파일

개인 정보 DB 암호화 키

- **개인 정보 DB 암호화**를 **사용**으로 설정하면 구성할 수 있습니다.
- 키는 문자, 숫자 및 기호를 조합하여 **32자**로 구성해야 합니다.

- 키를 변경하면 기존 데이터가 모두 다시 암호화합니다.

> **모범 사례**
>
> **안전한 난수 생성기**를 사용하여 키를 생성하고 **암호 보관함**(Password Vault)에 저장하세요. 정기적으로 변경하거나 보안 침해가 의심되는 경우 즉시 암호화 키를 변경하세요.

단계별 안내

1. 관리자 계정으로 BioStar X에 로그인하세요.
2. **설정** → **시스템** → **시스템 보안**으로 이동하세요.
3. **개인 정보 DB 암호화**를 **사용**으로 설정하세요.
4. 선택 사항으로, **개인 정보 DB 암호화 키**에서 **변경** 버튼을 클릭하고 새로운 암호화 키 **32자**를 입력하세요.

> **주의**
> 암호화 키를 변경하면 **기존의 모든 개인 데이터가 다시 암호화됩니다.** 유지 관리 기간에 변경 작업을 예약하세요. 암호화 키를 분실하면 암호화된 데이터를 복구할 수 없습니다.

얼굴 이미지 저장

얼굴 이미지를 보관해야 하는 엄격한 운영상의 요구 사항이 없는 한, **얼굴 이미지 저장하기** 기능을 비활성화하세요.

- **템플릿 vs 이미지**: 템플릿은 바이오메트릭 데이터의 수학적 표현으로, 역추적을 통해 얼굴을 식별하기가 더 어렵습니다.
- GDPR, PDPA 등 많은 개인정보 보호 규정에서 바이오메트릭 이미지를 매우 민감한 데이터로 취급합니다.
- 이미지를 불필요하게 저장하면 법적 위험과 공격 가능성이 높아집니다.

단계별 안내

1. **설정** → **서버** → **서버**로 이동하세요.
2. **전문가 설정 보기**을 **사용**으로 설정하세요.
3. **전문가 설정**에서 **얼굴 이미지 저장하기**을 설정하세요.
   - 기본값: **사용**
   - 권장 설정: **사용 안 함**

> **모범 사례**
> - 바이오메트릭 인증에는 이미지가 아닌 **템플릿**만 보관하세요.
> - 감사 목적으로 이미지가 필요하다면 엄격한 접근 제어와 짧은 보존 기간(30~60일)을 적용하여 **별도의 보안 저장소**에 저장하세요.
> - 업그레이드 후 설정이 기본값으로 되돌아가지 않았는지 주기적으로 검토하세요.

슈프리마 장치 강화

BioStar X에 연결된 슈프리마의 출입 제어 장치에 대한 보안 강화 권고 사항을 안내합니다.

BioStar X 서버 및 애플리케이션의 보안 강화는 중앙 시스템을 보호하지만, 출입 통제 장치는 물리적 출입구에 설치되어 로컬 네트워크 접근, 물리적 훼손, 무단 작동 또는 오래된 펌웨어에 노출될 수 있습니다. 따라서 장치 수준의 보안 강화는 전체 보안 체계의 필수 요소로 취급해야 합니다.

이 문서에서는 다음 항목들을 다룹니다.

- BioStar X에 연결된 슈프리마 출입 통제 장치에 적용됩니다.
- 펌웨어 유지 관리, 장치 이벤트 로그 처리, 관리자 구성 및 장치 측 운영 제어를 다룹니다.
- 장치 기능은 모델 및 펌웨어 버전에 따라 다를 수 있습니다.

장치 펌웨어 최신 상태 유지

슈프리마 장치 펌웨어를 고객 환경에 승인된 최신 지원 버전으로 업데이트하세요.

일반적인 모범 사례

- 연결된 모든 장치의 목록(모델명, 장치 아이디, 펌웨어 버전, 설치 위치, 역할)을 유지 관리하세요.
- 업그레이드하기 전에 슈프리마 펌웨어 릴리스 노트를 검토하세요.
- 광범위하게 배포하기 전에 운영 환경이 아닌 장치에서 펌웨어 업그레이드를 테스트하세요.
- 유지 관리 기간에 펌웨어 업그레이드를 예약하세요.
- 업그레이드 중에는 장치에 안정적인 전원이 공급되는지 확인하고, 전원이나 네트워크 연결을 유지하도록 관리하세요.
- 업그레이드 후 장치가 BioStar X에 다시 연결되는지, 모든 기능이 정상 작동하는지 확인하세요.

소프트웨어에서 펌웨어 업그레이드

가능하다면 장치에서 직접 업그레이드하는 대신 관리 소프트웨어를 통해 펌웨어를 업그레이드하세요.

1. 슈프리마 다운로드 센터에서 대상 장치 모델에 맞는 펌웨어 파일을 다운로드하세요.
2. 릴리스 노트 및 호환성 정보를 검토하세요.
3. 장치가 온라인 상태이고 정상적으로 통신하는지 확인하세요.
4. 사용자, 크리덴셜, 로그 및 장치 구성을 백업하거나 동기화를 확인하세요.
5. 대상 장치를 선택하고 펌웨어 업그레이드를 실행하세요.
6. 업그레이드가 완료되고 장치가 재시작될 때까지 기다리세요.
7. 재시작 후 펌웨어 버전을 확인하세요.

장치가 BioStar X에 다시 연결되었는지, 인증, 출입문 제어 및 이벤트 로그 업로드가 정상 작동하는지, 보안 통신 및 해시 키 설정이 예상대로 유지되는지 확인하세요.

주의

- 다른 장치 모델용으로 제작된 펌웨어를 적용하지 마세요.
- 업그레이드 진행 절차를 중단하지 마세요.
- 일부 펌웨어 업그레이드는 펌웨어 다운그레이드를 제한할 수 있으므로 업그레이드하기 전에 항상 릴리스 노트를 확인하세요.

장치/USB에서 직접 펌웨어 업그레이드

일부 슈프리마 장치는 USB 메모리 장치를 기기에 직접 연결하여 펌웨어를 업그레이드할 수 있습니다.

1. 펌웨어 업그레이드 파일을 지원되는 USB 메모리에 저장하세요.

   USB 메모리에 한 개의 파일만 저장하는 것을 권장합니다.

2. USB 메모리를 장치에 연결하세요.
3. 메시지가 나타나면 관리자 권한으로 인증하세요.
4. 펌웨어 파일이 장치로 전송될 때까지 기다리세요.
5. 안내에 따라 장치로부터 USB 메모리를 제거하세요.
6. 펌웨어 업그레이드가 완료되고 장치가 자동으로 재시작할 때까지 기다리세요.
7. 펌웨어 버전을 확인하고 장치가 정상 작동하는지 확인하세요.

주의

장치에서 펌웨어를 업그레이드하기 전에 장치 관리자가 구성되어 있어야 합니다. 펌웨어 업그레이드 중에는 전원을 차단하지 마세요.

장치 이벤트 로그 보존 및 보호

장치 이벤트 로그를 보존하고 BioStar X에 정기적으로 업로드하도록 설정하세요.

장치 로그 정책

- 장치 로그는 삭제되거나 덮어쓰기되지 않는 한 장치에서 지원하는 용량까지 로컬에 저장됩니다.
- 관리자는 장기 감사 보존을 위해 장치 로컬 저장소에만 의존해서는 안 됩니다.
- 가능한 경우 BioStar X로의 자동 로그 업로드를 활성화하세요.
- 이벤트 로그는 조직의 감사 및 규정 준수 정책에 따라 검토하고 백업해야 합니다.
- 장치의 날짜, 시간, 시간대 및 일광 절약 시간 설정이 올바르게 구성되었는지 확인하세요. 지원되는 경우 시간 동기화를 활성화하세요.

보안 탬퍼 고려 사항

일부 슈프리마 장치는 **보안 탬퍼** 동작을 지원합니다. 탬퍼 이벤트 발생 시 장치는 사용자, 로그, 암호화 키, SSL 인증서를 포함한 민감한 데이터를 삭제할 수 있습니다. 따라서 자동 로그 업로드를 활성화하여 탬퍼 전 로그를 BioStar X에 안전하게 저장하는 것이 중요합니다.

운영 모범 사례

- 장치 탬퍼 이벤트를 보안 사고로 취급하세요.
- 탬퍼 이벤트 발생 후, 재등록 또는 재배포 전에 기기를 물리적으로 검사하세요.
- 문서화된 보안 승인 없이 탬퍼 관련 보호 기능을 비활성화하지 마세요.

장치 관리자 구성

지원하는 슈프리마 장치에 장치 관리자를 구성하고 장치 관리자 메뉴에 대한 접근을 제한하세요. 관리자 보호 없이 장치를 운영 환경에 배포해서는 안 됩니다.

알아두기

장치 관리자 권한은 BioStar X 사용자 권한과 별개입니다.

모범 사례

- 운영 환경에 배포하기 전에 최소 한 명의 장치 관리자를 등록하세요.
- 권한이 있는 직원에게만 할당된 고유 관리자 크리덴셜을 사용하세요.
- 강력한 인증 방법(카드 + PIN, 생체 인식 + PIN 또는 다중 크리덴셜 관리자 인증)을 사용하세요.
- 장치 관리자 할당을 정기적으로 검토하세요.
- 직원 역할이 변경되면 관리자 접근 권한을 즉시 제거하세요.
- 관리자 크리덴셜을 분실한 경우를 대비한 비상 복구 절차를 문서화하세요.

소프트웨어에서 장치 관리자 구성

1. 관리자 계정으로 BioStar X에 로그인하세요.
2. 장치 관리자 역할을 수행할 사용자를 생성하거나 선택하세요.
3. 필요한 크리덴셜(카드, PIN, 지문 또는 얼굴 인식)을 등록하세요.
4. 관리자 권한 또는 적절한 장치 관리자 역할을 할당하세요.
5. 사용자를 대상 장치로 전송하거나 동기화하세요.
6. 대상 장치에서 관리자 크리덴셜로 관리자 메뉴로 이동할 수 있는지 확인하세요.

장치에서 직접 장치 관리자 구성

1. 장치 메뉴로 이동하세요.

2. 사용자 등록 또는 관리자 구성 메뉴를 실행하세요.
3. 관리자로 사용자와 크리덴셜을 등록하세요.
4. 관리자 권한을 할당하세요.
5. 구성을 저장하세요.
6. 관리자 메뉴로 다시 이동하여 관리자 인증을 테스트하세요.

장치 네트워크 및 로컬 서비스 보안 강화

최소 기능 원칙에 따라 장치 네트워크 및 로컬 서비스 설정을 구성하세요.

권장 조치

- 장치 IP 주소를 안정적으로 운영하려면 문서화하세요. DHCP에서 IP 주소를 예약하거나 서브넷 마스크, 게이트웨이, DNS, 포트, 장치 ID 및 위치와 함께 고정 IP 주소를 문서화하세요.
- 장치에서 사용하는 BioStar X 서버 주소와 서버 포트를 확인하세요.
- 필요하지 않은 장치의 기능은 비활성화하세요.

  > *예: RTSP, IP 인터콤*

- RTSP, 인터콤 또는 기타 선택적 서비스가 필요한 경우 강력한 크리덴셜을 구성하고 신뢰할 수 있는 시스템에서만 액세스할 수 있도록 제한하세요.
- 지원되는 경우 시간 동기화를 활성화하세요.
- 기본 설정 복원 또는 공장 초기화 후 네트워크 설정, 관리자 권한, 루트 인증서, 보안 통신 및 BioStar X 연결을 다시 확인하세요.

장치 운영 강화 체크리스트

- ☐ 펌웨어를 지원되는 최신 버전으로 업데이트하세요.
- ☐ 장치 모델, 장치 아이디, 펌웨어 버전, 위치 및 역할에 대한 인벤토리를 유지 관리하세요.
- ☐ 실제 사용하기 전에 장치 관리자 액세스 권한을 구성하세요.
- ☐ 관리자 권한은 승인된 직원에게만 부여하세요.
- ☐ 지원되는 경우 BioStar X와의 보안 통신을 활성화하세요.
- ☐ 배포 위험 수준에 따라 장치 해시키 수동 관리 및 보안 탬퍼 기능을 활성화하세요.
- ☐ 가능하다면 로그 업로드를 자동로 설정하세요.
- ☐ 장치 이벤트 로그가 BioStar X에 정기적으로 업로드되는지 확인하세요.
- ☐ 장치 설치 및 케이블 연결을 물리적으로 안전하게 보호하세요.
- ☐ 탬퍼 이벤트, 예기치 않은 재시작, 펌웨어 변경 및 로그 누락을 보안 관련 이벤트로 취급하세요.
- ☐ 펌웨어 업그레이드, 장치 교체 또는 복원 작업 후 장치 구성을 검토하세요.

- ☐ 실제 사용 장치에 안정적이고 문서화된 네트워크 주소를 사용하세요.
- ☐ 배포에 필요하지 않은 장치의 기능은 비활성화하세요.
- ☐ 시스템 기본 설정 복원 및 공장 초기화 작업은 승인된 관리자만 수행할 수 있도록 제한하세요.

참조

이 문서는 BioStar X 시스템 구축 및 보안 강화 시 필요한 기술적 참조 정보를 제공합니다. 네트워크 포트 구성, 권장 보안 설정, 주요 컴플라이언스 요구사항을 한눈에 확인할 수 있으며, 추가 지원이 필요한 경우 외부 참조 자료를 참고하세요.

BioStar X 기본 네트워크 포트

서비스	용도	기본 포트	참고 / 권장 사항
Unified Gateway Service	HTTPS (시스템 접근)	443	관리자/운영자 로그인 기본 포트입니다. **Service Manager** → **Service Settings**에서 변경할 수 있습니다.
Core Web Service	HTTPS (내부 UI)	5002	443 포트로 프록시 연결을 권장하며, 직접 접근을 제한합니다.
	CloudNgrok	52000	필요하지 않은 경우 비활성화하세요.
	Thrift RPC	9310	신뢰할 수 있는 서비스로 제한합니다.
Core Service	WebSocket	9002	내부 전용입니다.
	FastCGI	9000	로컬에서 바인딩해야 합니다.
	API	9010	TLS 및 인증으로 보안을 유지합니다.
Coordinator Service	클라이언트 통신	21810	내부 전용입니다.
Main Server	TCP 서버	51212	**일반 텍스트** 장치 통신 — 가능하면 차단하세요.
	SSL 서버	51213	**권장** 장치 통신(TLS)
	gRPC	51219	내부 서비스 통신 전용입니다.
Cache Service	클라이언트	10800	Redis와 동일 — 외부에 노출하지 마세요.
	통신	47500	내부 전용입니다.
	검색	47100	내부 전용입니다.

BioStar X의 기본 보안 기능

기능	UI 위치	기본값	권장 사항
기본 관리자 로그인 ID & 암호 변경	**사용자** → 사용자 목록에서 기본 관리자 편집(UID:1)	admin / 설치 비밀번호	설치 직후 변경하세요.
권한 및 역할 분리	**사용자** → 사용자 선택 → **권한** → **관리자 등급**	사전 정의: **전체 관리자**, **사용자 관리자**, **모니터링 관리자**	필요에 따라 커스텀 권한을 생성하세요.
암호 강도 정책	**설정** → **시스템** → **시스템 보안** → **로그인 비밀 번호** → **비밀번호 레벨**	**보통**	**강함**으로 설정하고 멀티팩터 인증(MFA)을 적용하세요.
세션 보안(동시 연결)	**설정** → **시스템** → **시스템 보안** → **세션 보안** → **동시 접속 허용**	**활성**	공유 로그인 방지를 위해 **비활성**로 설정하세요.
멀티팩터 인증	**사용자** → 사용자 선택 → **권한** → **다중 인증 로그인**	**사용 안 함**	**전체 관리자**, **사용자 관리자**, **모니터링 관리자** 계정에 대해 활성화할 수 있습니다.
장치와 보안 통신	**설정** → **시스템** → **시스템 보안** → **고급 보안 설정** → **장치와 보안 통신**	**사용 안 함**	기능을 활성화하고, SSL 포트(51213)를 사용하세요.
장치 해시키 관리	**설정** → **시스템** → **시스템 보안** → **고급 보안 설정** → **장치 해시키 수동 관리**	**사용 안 함**	높은 보안 환경 배포에서 탬퍼 보호를 위해 활성화하세요.
시스템 백업	**설정** → **시스템** → **시스템 백업**	**수동**	**시스템 자동 백업** 기능을 활성화하세요.
디렉터리 연동	**설정** → **시스템** → **디렉토리 연동**	구성되지 않음	가능하다면 Entra ID 또는 Active Directory와 연동하세요.
로그 설정(보존 및 수준)	**설정** → **시스템** → **서버** → **서버**	**시스템 로그 저장 기간**: 60일 **시스템 로그 단계**: **정보**	규정 준수 여부에 따라 조정하세요. 로그는 SIEM으로 전달하세요.
개인 정보 데이터베이스 암호화	**설정** → **시스템** → **시스템 보안** → **고급 보안 설정** → **개인 정보 DB 암호화**	**사용 안 함**	프로덕션 환경에 활성화하세요.
얼굴 이미지 저장	**설정** → **시스템** → **서버** → **전문가 설정** → **얼굴 이미지 저장하기**	**사용**	정당한 이유가 없는 한 비활성화하세요.

컴플라이언스 요구사항 (간략 보기)

보안 제어	지원하는 컴플라이언스 영역
데이터베이스 암호화(개인 식별 정보, 바이오메트릭 정보)	GDPR, CCPA, ISO 27001
시스템 로그 보존 및 전달	ISO 27001, PCI-DSS
관리자/운영자 계정 멀티팩터 인증(MFA)	NIST 800-63, ISO 27001
장치와 보안 통신(TLS)	GDPR, ISO 27001
백업 및 복원 기능	ISO 27001, SOC 2
디렉터리 연동(Entra ID/Active Directory)	SOX, ISO 27001, SOC 2

외부 참조

- 슈프리마 지식 베이스 – 장치와 서버 간 보안 통신 구성하기
- 슈프리마 지식 베이스 – 서버 및 장치 암호화 키 수동으로 관리하기
- 슈프리마 지식 베이스 – USB 메모리로 BioStar 2와 장치 간 사용자 및 로그 불러오고 내보내기
- 슈프리마 지식 베이스 – USB를 이용하여 펌웨어 업그레이드하기
- 슈프리마 지식 베이스 – 보안 탬퍼 구성하기
- Microsoft 보안 준수 도구 키트 - 사용 방법

부록

제품에 포함된 법적 고지 사항을 수록합니다.

면책 조항

- 이 웹 사이트는 슈프리마 제품과 관련된 정보를 제공합니다.
- 이 웹 사이트는 슈프리마의 제품 사용 및 판매 계약에 포함된 슈프리마 제품에만 사용될 수 있습니다. 이 웹 사이트는 명시적, 묵시적, 금반언의 원칙 또는 어떠한 방식으로도 지식재산권에 대한 라이선스를 부여하지 않습니다.
- 귀하와 슈프리마 간의 계약에 명시된 경우를 제외하고, 슈프리마는 어떠한 책임도 지지 않으며 슈프리마는 특정 목적에의 적합성, 상품성 또는 비침해와 관련된 모든 명시적, 묵시적 보증을 부인합니다.
- 모든 보증이 무효화되는 경우는 다음과 같습니다: 슈프리마 제품이 1) 잘못 설치된 경우 또는 하드웨어의 일련번호, 보증정보 또는 품질 보증 스티커가 변경 또는 제거된 경우; 2) 슈프리마가 허용한 방법 이외의 방법으로 사용한 경우; 3)슈프리마 또는 슈프리마가 승인한 당사자 이외의 당사자에 의하여 변경, 수정 또는 수리된 경우; 또는 4) 부적절한 환경에서 작동되거나 유지된 경우.
- 슈프리마 제품은 제품의 고장이 부상이나 사망사고로 이어질 수 있는 의료, 인명 구조, 생명 유지와 같은 용도로 사용하도록 만들어진 것은 아닙니다. 만약 귀하께서 이러한 용도로 슈프리마 제품을 구매하거나 사용할 경우, 이로 인한 부상 또는 사망으로 발생하는 모든 청구, 비용, 손실, 지출 및 합리적인 변호사 비용으로부터 슈프리마와 그 구성원, 자회사, 계열사 및 공급사를 면책시켜야 합니다. 제품 디자인이나 제조에 슈프리마의 과실이 있다고 주장되는 경우에도 마찬가지입니다.
- 슈프리마는 신뢰성, 기능 또는 디자인을 개선하기 위하여 언제든지 예고없이 사양과 제품 설명을 변경할 권리를 가지고 있습니다.
- 개인정보는 제품 사용시 인증메시지 및 기타 관련 정보의 형태로 슈프리마 제품에 저장될 수 있습니다. 슈프리마는 슈프리마가 직접 통제할 수 없는 또는 관련 계약에 명시된 슈프리마 제품에 저장되는 개인정보를 비롯한 어떠한 정보에 대해서도 책임지지 않습니다. 개인정보를 포함하여 저장된 정보를 사용하는 경우 제품 사용자는 관련 법률 (예를 들어, GDPR)을 준수하고 적절한 취급과 처리를 해야 할 책임이 있습니다.
- 귀하는 어떠한 기능의 부재 또는 특징, "reserved" 또는 "undefined"로 표시된 설명에 의존해서는 안됩니다. 슈프리마는 이를 추후에 정의할 수 있으며 추후에 가한 변경이 현재와 상충된다고 하더라도 슈프리마는 책임지지 않습니다.
- 이 사이트에 명시적으로 기재되어 있는 경우를 제외하고, 슈프리마는 법률이 허용하는 최대 범위 내에서 "있는 그대로" 판매됩니다.
- 제품을 주문하기 전에 가까운 슈프리마 영업소 또는 대리점에 문의하여 최신 사양을 확인하세요.

저작권 공지

이 웹 사이트의 저작권은 슈프리마에게 있습니다. 다른 제품 이름, 상표, 등록된 상표에 대한 권리는 각각 그것을 소유한 개인이나 단체에게 있습니다.

(주) 슈프리마
13554 경기도 성남시 분당구 정자일로 248 파크뷰타워 17층
영업 문의 1522 4507(1번)　korea@suprema.co.kr | 고객지원 1522 4507(2번)　cs@suprema.co.kr

© 2026 Suprema Inc. 이 문서에 표기된 슈프리마, 제품명, 번호는 슈프리마의 등록 상표입니다. 모든 회사명과 제품명은 해당 회사의 상표이거나 등록 상표입니다. 제품 외관, 제조 상태 및 사양은 사전 통지 없이 변경될 수 있습니다.