Security Hardening Reference

Apply best practices to secure deployments.

Reference **Solution** **Deployment** Runtime | Server | Client Types | Container | Redundancy | Security

---

Security Hardening (Reference): Securing FrameworX deployments for production environments.

Security Checklist
Authentication Configuration
Network Security
Access Control
Data Protection
Audit and Compliance
Hardening Guidelines
Incident Response

Security Checklist

System Level

- Operating system hardened and patched
- Unnecessary services disabled
- Firewall configured with minimal ports
- Antivirus exclusions for FrameworX folders
- User accounts with minimal privileges
- Audit logging enabled

Application Level

- Default passwords changed
- SSL/TLS enabled for all connections
- Authentication required for all access
- Role-based access control configured
- Secure communication with devices
- Encrypted database connections

Authentication Configuration

Windows Authentication

For domain environments:

xml

```xml
<authentication mode="Windows">
  <domain>COMPANY</domain>
  <allowedGroups>
    <group>SCADA_Operators</group>
    <group>SCADA_Engineers</group>
  </allowedGroups>
</authentication>
```

Forms Authentication

For non-domain:

xml

```xml
<authentication mode="Forms">
  <passwordPolicy>
    <minLength>12</minLength>
    <requireUppercase>true</requireUppercase>
    <requireNumbers>true</requireNumbers>
    <requireSpecialChars>true</requireSpecialChars>
    <expirationDays>90</expirationDays>
  </passwordPolicy>
</authentication>
```

Multi-Factor Authentication

Configure MFA provider:

xml

```xml
<mfa enabled="true">
  <provider>AzureAD</provider>
  <timeout>300</timeout>
</mfa>
```

Network Security

SSL/TLS Configuration

Generate Certificate:

powershell

```powershell
New-SelfSignedCertificate `
  -DnsName "scada.company.com" `
  -CertStoreLocation "cert:\LocalMachine\My"
```

Bind to Service:

cmd

```
netsh http add sslcert ipport=0.0.0.0:10108
  certhash=<thumbprint>
  appid={12345678-1234-1234-1234-123456789012}
```

Firewall Rules

Minimal Access:

powershell

```powershell
# Remove default allow-all
Remove-NetFirewallRule -DisplayName "FrameworX*"

# Add specific rules
New-NetFirewallRule -DisplayName "FrameworX Clients" `
  -Direction Inbound -Protocol TCP -LocalPort 10108 `
  -RemoteAddress 192.168.1.0/24 -Action Allow
```

Access Control

Role-Based Security

Define Roles:

xml

```xml
<roles>
  <role name="Operator">
    <permissions>
      <allow>Display.View</allow>
      <allow>Alarms.Acknowledge</allow>
      <deny>Configuration.*</deny>
    </permissions>
  </role>
  <role name="Engineer">
    <permissions>
      <allow>*</allow>
      <deny>Security.Modify</deny>
    </permissions>
  </role>
</roles>
```

Tag Security

Protect critical tags:

xml

```xml
<tagSecurity>
  <tag name="Emergency_Stop">
    <writeAccess>Engineers,Supervisors</writeAccess>
    <audit>true</audit>
  </tag>
</tagSecurity>
```

Data Protection

Database Encryption

SQL Server TDE:

sql

```sql
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'StrongPassword123!';
CREATE CERTIFICATE FrameworXCert WITH SUBJECT = 'FrameworX TDE';
CREATE DATABASE ENCRYPTION KEY WITH ALGORITHM = AES_256
  ENCRYPTION BY SERVER CERTIFICATE FrameworXCert;
ALTER DATABASE FrameworX SET ENCRYPTION ON;
```

Communication Encryption

Device Connections:

xml

```xml
<deviceSecurity>
  <protocol name="OPC_UA">
    <security>SignAndEncrypt</security>
    <certificate>device-cert.pfx</certificate>
  </protocol>
</deviceSecurity>
```

Audit and Compliance

Audit Configuration

xml

```xml
<audit enabled="true">
  <events>
    <login>true</login>
    <logout>true</logout>
    <configChange>true</configChange>
    <tagWrite>true</tagWrite>
    <alarmAck>true</alarmAck>
  </events>
  <storage>
    <path>C:\Logs\Audit\</path>
    <retention>365</retention>
  </storage>
</audit>
```

Compliance Reports

Generate for:

- NERC CIP
- ISO 27001
- FDA 21 CFR Part 11

Hardening Guidelines

Windows Server

powershell

```
# Disable unnecessary services
Stop-Service -Name "Spooler"
Set-Service -Name "Spooler" -StartupType Disabled

# Configure security policies
secedit /configure /db security.sdb /cfg security.inf

# Enable Windows Defender
Set-MpPreference -DisableRealtimeMonitoring $false
```

Linux Server

bash

```
# Disable root login
sed -i 's/PermitRootLogin yes/PermitRootLogin no/' /etc/ssh/sshd_config

# Configure firewall
ufw default deny incoming
ufw allow from 192.168.1.0/24 to any port 10108
ufw enable

# Set file permissions
chmod 750 /opt/FrameworX chown -R FrameworX:FrameworX /opt/FrameworX
```

Incident Response

Security Monitoring

Monitor for:

- Failed login attempts > 5
- Configuration changes
- Unusual tag write patterns
- Network scanning attempts

Response Plan

1. **Detection**: Alert on security event
2. **Containment**: Isolate affected system
3. **Investigation**: Review audit logs
4. **Recovery**: Restore from backup
5. **Documentation**: Update security procedures

In this section...
