atvise®

atvise® Security Check

for a secure and reliable atvise® visualization



How well is your atvise® visualization protected against potential security risks? This checklist helps you systematically review key security measures, identify potential vulnerabilities, and determine where action may be needed.

atvise® Security Check

Checklist for a secure and reliable visualization

Review the following security measures for your atvise® installation. This helps you keep track of your security status and identify areas where further action may be required.

Access & Permissions

- ☐ Set strong passwords for all users and enable the password policy.
- ☐ Use access control consistently and restrict permissions to the areas required for each user.
- ☐ Enable two-factor authentication for critical accounts.

Encryption & Certificates

- ☐ Use HTTPS and disable unencrypted HTTP connections. Use “form” or “script” as the login method.
- ☐ Use CA-signed certificates, disable Auto-Trust, enable Auto-Validate, limit certificate validity to a maximum of one year, and monitor expiry dates regularly.
- ☐ Disable unencrypted OPC UA connections and secure endpoints and data sources with valid certificates.
- ☐ Use secure protocol variants with TLS in atvise® connect X wherever remote device supports them.

Network & Files

- ☐ Open only the required network ports and block external access to the engineering environment.
- ☐ Protect directories using operating system permissions and avoid network shares.
- ☐ Encrypt nodes.db and archives, and securely protect the certificate store and private keys.

Operation & Data Backup

- ☐ Use HTTPS for the license server, restrict access to its installation directory, and configure the backup path and schedule.
- ☐ Configure antivirus exclusions for atserver.exe and the installation and project directories in accordance with the atvise® recommendations.
- ☐ Create consistent backups, store them externally, and regularly test the recovery process.

Libraries & Data Protection

- ☐ Only integrate external libraries after carefully checking their origin, security, and whether they are up to date.
- ☐ When using user accounts or external authentication, ensure that personal data is protected by appropriate access permissions.

Note: By default, atvise® does not store any personal data. If user accounts are created or external authentication is enabled, ensure that access control also provides adequate protection for this data.

Security Check Results as of .....

- ☐ All listed measures have been implemented.
- ☐ Some measures still need to be reviewed or implemented.

Notes / Outstanding Actions:

.....

.....

.....

.....

.....

.....

.....

.....

.....

Disclaimer:

- This checklist does not replace a complete security assessment of your system.
- All measures in detail: atvise® Security White Paper
- Suspect a security vulnerability? Mail to: visutec@bachmann.info
- As of 10/2026

atvise®

www.atvise.com

atvise® Security Checklist
© 10/2026 by Bachmann Visutec GmbH