

A-Serie und X-Serie 64MB

Version V6_00_07

28.04.2026

ab Softwareversion V4

Die Version V6_00_07 enthält zusätzlich alle Änderungen der nicht veröffentlichten Version V6_00_06.

⚠ Wichtiger Hinweis zur SSH-Authentifizierung

Mit dem aktuellen Update wurde die Anmeldung per Benutzername und Passwort für den SSH-Zugang aus Sicherheitsgründen deaktiviert.

Der Zugriff ist danach **nur noch per Public-Key-Authentifizierung** möglich.

Bitte beachten Sie:

Wenn Sie aktuell noch Username/Passwort verwenden und keinen Public Key eingerichtet haben, ist nach dem Update **kein SSH-Zugriff mehr möglich**.

Einrichtung der Public-Key-Authentifizierung z.B mit PuTTY

- SSH-Schlüssel mit PuTTY erstellen
- PuTTYgen öffnen
- RSA (SSH-2) auswählen
- 2048 oder 4096 Bit einstellen
- „Generate“ klicken und Maus bewegen
 - Schlüssel speichern
- Optional: Passphrase setzen
- Private Key speichern
- Public Key speichern
 - Public Key auf dem Gateway hinterlegen

1. Anmelden

Logge dich über das Webinterface am Gateway mit einem Admin-Account ein.

2. Navigation öffnen

Gehe im Menü zu:

General → IP Network

3. SSH Accounts aufrufen

Scrolle zum Abschnitt **SSH Accounts**.

4. Neuen Eintrag erstellen

Klicke auf **Edit → Add**.

5. Daten eingeben

Trage eine **Description** ein (z. B. Benutzername oder Zweck).

Füge den **SSH Public Key** in das entsprechende Feld ein.

6. Speichern

Bestätige die Eingabe

- PuTTY konfigurieren
- Connection → SSH → Auth
- Private Key auswählen
- Verbindung testen

SSH-Verbindung starten

→ Anmeldung erfolgt ohne Passwort

- Typische Fehler
- Kein Zugriff → Key nicht korrekt hinterlegt
- Permission denied → falscher Key/User
- Verbindung schlägt fehl → Netzwerk prüfen

Bei Fragen oder Unterstützungsbedarf helfen wir Ihnen gerne weiter.

Allgemein

- Firmwareupdate auch bei falscher Zeiteinstellung möglich
- Umbenennung von "Factory-Reset" in "Userdata-Reset"
- SSH Zugang ausschließlich per Public-Key-Authentifizierung
- Verhinderung von HTML Injection über Datenpunkt-Werte
- DPmngr: Threshold Value Funktion korrigiert
- DPmngr: Korrekte Berechnung von Formeln bei ganzzahligen Werten
- sudo: Einschränkung der Parameter für tcpdump
- sudo: Ausführung von tcpdump mit manipulierten Parametern verhindert
- Web-Backend: Verhinderung von Command Injection
- System: Nicht mehr verwendete Datenpunkte aus Default-Konfiguration entfernt

Treiberspezifisch

BACnet

- Verbesserung im Modus "UseEventsForDataRetrieval"
- Zugriff auf Properties von Server-Objekten
- Empfang und Quittierung von NC-Meldungen
- Initialwert von Scheduler wird korrekt übergeben
- UseEventsForDataRetrieval bei initialem Polling korrigiert

CSV

- Domain explizit konfigurierbar
- FD-Leak bei (S)FTP Upload behoben

dpsh

- Korrekte Defaultwerte für MaxInput und MaxOutput

ESPA

- Auswertung von Textnachrichten verbessert

Modbus

- Korrektes Handling des Failure Datenpunktes bei Neustart
- Fehlerdatenpunkt [M failure] entfernt
- Erweiterung um SetInvalid Flag
- Verbesserte Fehlerbehandlung bei Socket Reinitialisierung

M-BUS

- Verbesserte Unterstützung von Tibbo Pegelwandlern
- Korrekte Übertragung von Beschreibung, sbit und failure bei automatischer BACnet Datenpunkterstellung

MQTT

- TLS 1.3 funktioniert wieder
- Passwörter dürfen das Zeichen '#' enthalten

LCN

- Optimierung der Diagnoseausgaben
- Erweiterung Relais-/Keyblock-Datenpunkte

LUA

- Unnötige Konfigurationsoption für Skriptpfade entfernt

OPCUA

- Initialisieren von entfernten Server Objekten aktivierbar

SNMP

- Unterstützung von Protokollversion v1 und v2c

DC3500

- Erweiterung Event-Handling

Saia

- Frame-Handling im DATA-Mode korrigiert

EIB/KNX

- Unterstützung für Datenpunkttyp SINT64 (DPT29)

detectomat

- Kommando Datenpunkte schalten bei Neustart nicht mehr

VDS

- Fehlender Default-Wert für AutoAck hinzugefügt

Buildumgebung

- Update der Yocto Buildumgebung von Version 5.0.12 auf 5.0.16

Yocto 5.0.13

Security Fixes

- busybox: CVE-2025-46394
- curl: CVE-2025-9086
- expat: CVE-2024-8176
- openssl: CVE-2025-9230, CVE-2025-9231, CVE-2025-9232
- sudo: CVE-2025-32463

Yocto 5.0.14

Security Fixes

- lz4: CVE-2025-62813
- openssh: CVE-2025-61984, CVE-2025-61985
- curl: CVE-2025-10966 (ignored)
- gnupg: CVE-2025-30258 (ignored)

Yocto 5.0.15

Security Fixes

- libssh2: CVE-2023-48795
- libxml2: CVE-2025-7425
- musl: CVE-2025-26519
- rsync: CVE-2025-10158

Yocto 5.0.16

Security Fixes

- curl: mehrere CVEs behoben
- dropbear: CVE-2019-6111
- expat: CVE-2026-24515, CVE-2026-25210

Security Advisory vde-2026-036

- CVE-2026-35076: Arbitrary file delete (bac-scanresult)
- CVE-2026-35077: Arbitrary file delete (ugw-delete-file)
- CVE-2026-35078: Arbitrary file delete (ugw-logstop)
- CVE-2026-35079: Arbitrary file delete (ugw-restore)
- CVE-2026-35080: Arbitrary file delete (ugw-restoreinfo)
- CVE-2026-35081: Arbitrary process termination (ugw-logstop)
- CVE-2026-35082: Local file inclusion / delete (ugw-logread)
- CVE-2026-35083: Stack buffer overflow (bac-scantrend, bac-deviceobject)
- CVE-2026-35084: Stack buffer overflow (dali-devconfig)
- CVE-2026-35085: Stack buffer overflow (gdv-serverconfig)