S12.167 Firmware

Release notes

Version: S12.167

Build date: 2025/3/21, 2025/3/25, 2025/3/26, 2025/4/2, 2025/4/18, 2025/4/29, 2025/5/2 and 2025/6/13, depending on the model.

Release date: 2025/5/9

■ **[Supported model] :**

- **Build date:2025/3/21**
  RGS-PR9000
- **Build date:2025/3/25**
  IGS-9168GP, IGS-9812GP, IGS-P9164GC-HV, IGS-P9164GC-LV, IGS-P9812GP-HV, IGS-P9812GP-LV, RES-P9242GCL-HV, RES-P9242GCL-L, RGPS-9244GP-LP-HV, RGS-9168GCP, RGS-P9160GCM1-LV, RGS-P9160GCM1-HV, TGPS-9084GT-M12X-BP2-WV, TGPS-W9082GF-MM-M12X-QS-MV, RGS-R9244GP+, RGS-R9244GP+-E, GS-P9164GF-MM-SC-LV, RGS-9244GP, TGPS-9084GT-24V-Series, TGPS-9168GT-M12-BP2-24V, TGPS-W9124GT-M12X-BP2-WV, TGS-W9160-M12X-BP2-WV, TPS-W9124GT-M12X-BP2-24V
- **Build date:2025/3/26**
  IGPS-9084GP-LA-24V, IGPS-P9084GP-LA, IGS-9084GP-LA, RES-9242GC, RGPS-92222GCP-NP-P, RGPS-92222GCP-NP-LP, RGS-92222GCP-NP, RGS-92222GCP-NP-E
- **Build date:2025/4/2**
  RGS-P9000-HV, RGS-P9000-LV
- **Build date:2025/4/18**
  RGPS-R9244GP+-LP, RGPS-R9244GP+-LP, RES-P9242GCL series, RGPS-92222GCP-NP, RGPS-92222GCP-NP-P-E
- **Build date:2025/4/29**
  RGS-9168GCP-E
- **Build date:2025/5/2**
  IGPS-9084GP-LA
- **Build date:2025/5/14**
  IGS-R9812GP
- **Build date:2025/5/27**
  TES-W9124GT-M12X-BP2-24V
- **Build date:2025/6/12**
  TGPS-9164GT-24V-Series
- **Build date:2025/6/13**

IGS-P9164GF-SS-SC-LV

- **Build date:2025/11/27**

  RGS-9244GP-E

- **[Note]:**
  - The initial official release of the S12 firmware complies with the IEC 62443-4-2 security standard.
- **[Security updated] :**
  - **Password Policy Configuration**

    Enables administrators to define configurable password strength rules, helping organizations strike a balance between security and usability. This improves protection against cyber threats while maintaining user convenience.
  - **Group Privilege Level**

    Introduces configurable group-based (role-based) user accounts, allowing for enhanced access control, simplified user management, improved operational efficiency, and better compliance.
  - **Account Lockout**

    Protects against brute-force attacks by locking user accounts after a predefined number of failed login attempts, preventing unauthorized access.
  - **Audit Log**

    Maintains a comprehensive record of system activities, user actions, and security-related events, supporting accountability and traceability.
  - **Auto Logout Configuration**

    Enhances security by automatically logging out inactive users after a specified period of inactivity, minimizing the risk of unauthorized access.
  - **Concurrent Session Control**

    Limits each user to a single active session. Any new login will automatically terminate the previous session, ensuring session integrity and preventing account sharing.
  - **System Banner Configuration**

    Allows customization of the login banner message to clearly inform users that unauthorized access is prohibited and may lead to legal consequences. The system also restricts access to a maximum of five concurrent logins.
- **[New Feature] :**

  N/A
- **[Enhancement] :**

N/A

- **[Bug fixed] :**

  N/A