LEGRAND – DPC
SECURITY INFORMATION

CommandCenter® Secure Gateway v13

Dawn Syskowski – Updated 07/15/2025

TABLE OF CONTENTS

Security System Overview 03

Server – Security Stack 04

Web Server – Security 05

Server - Security 06

Security System Overview

CC-SG Firmware v13.0.0

- At Legrand, there is a heightened awareness of the impact that poor product security could have on the end customer.
- As part of our CommandCenter® Secure Gateway (CC-SG) firmware development cycle and ongoing threat assessment, Legrand runs a security scanner on firmware releases.
  - Legrand owns a Nessus vulnerability scanner license, renewed annually.
  - Before a new firmware is released, it is tested with this scanner tool.
  - Nessus security plugins are automatically updated as soon as Tenable releases them.
  - As soon as a new Nessus scanner version is available from the vendor Tenable, Legrand will update the scanner tool to it‘s latest version.
- During a firmware release system test cycle, security-related firmware features are tested.
- CC-SG firmware requires strong passwords for administrator by default. Strong password rules can be customized and enabled for all users too.
- Legrand has a Security Working Group which is dedicated on staying ahead of the requirements for security.

Server – Security Stack

CC-SG Firmware v13.0.0

- The Operating System is based on:
  - Rocky Linux with some minor modifications by Raritan for specific platform support and configuration.
    - Version: 9.5
    - URL: https://www.rockylinux.org/
    - Open Source library and program source code
      - Complete list of all used Open Source licenses can be found in CC-SG Admin Client Help Menu
- The SSH stack for Diagnostic Console at port 23 is:
    - Package: Openssh
    - Version: 8.7p1
    - URL: https://www.openssh.com/
    - License: BSD
- The SSH stack for CLI at port 22 is based on:
    - Package: Apache SSHD
    - Version: 0.14.0
    - URL: https://mina.apache.org/sshd-project/
    - License: Apache Licenses

Web Server – Security

CC-SG Firmware v13.0.0

- The SSL stack is provided by Java:
  - Package: OpenJDK
  - Version: 1.8.0_432
  - URL: https://adoptium.net/temurin/releases/
  - License: GPL
- Details about the encryption technology, cryptographic libraries, algorithms, and mode choices:
  - SSL
    - TLS 1.0, 1.1, 1,2, 1.3 are enabled by default.
    - AES128 is enabled by default, can select only AES256.
    - The ciphers and modes used can be customized for user security requirements.
    - Default Supported TLS ciphers and mode combinations in order of priority (from high to low, highest priority is server enforced):
      - TLSv1.3:
        - TLS_AKE_WITH_AES_128_GCM_SHA256
        - TLS_AKE_WITH_AES_256_GCM_SHA384
      - TLSv1.2:
        - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
        - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
        - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
        - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
        - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
      - TLSv1.0 / TLSv1.1:
        - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
        - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

Server – Security

CC-SG Firmware v13.0.0

- Details about the encryption technology, cryptographic libraries, algorithms, and mode choices:
  - Unused protocols like SSL3 and unused algorithms are not enabled to reduce attack risk
  - Upstream packages are monitored by engineering for updates and decided on case-by-case when to integrate it in the firmware. I.e. depending on if the product is affected and the severity of an issue it is determined if an intermediate update is provided or if the changes are available with the next regular release.
  - Diagnostic Console SSH server:
    - Key Exchange
      - curve25519-sha256@libssh.org
      - curve25519-sha256
      - ecdh-sha2-nistp521
      - ecdh-sha2-nistp384
      - ecdh-sha2-nistp256
      - diffie-hellman-group-exchange-sha256
      - diffie-hellman-group16-sha512
      - diffie-hellman-group18-sha512
      - diffie-hellman-group14-sha256
      - kex-strict-s-v00@openssh.com
    - Host Key Algorithms:
      - rsa-sha2-512
      - rsa-sha2-256
      - ssh-rsa
      - ecdsa-sha2-nistp256
      - ssh-ed25519

Server – Security

CC-SG Firmware v13.0.0

- Ciphers:
  - aes256-ctr
  - aes256-gcm@openssh.com
- MACs:
  - umac-64-etm@openssh.com
  - umac-128-etm@openssh.com
  - hmac-sha2-256-etm@openssh.com
  - hmac-sha2-512-etm@openssh.com
  - hmac-sha1-etm@openssh.com
  - umac-64@openssh.com
  - umac-128@openssh.com
  - hmac-sha2-256
  - hmac-sha2-51
  - hmac-sha1

- CLI SSH server:
  - Key exchange:
    - diffie-hellman-group14-sha1
    - diffie-hellman-group-exchange-sha256
    - ecdh-sha2-nistp256
    - ecdh-sha2-nistp384
    - ecdh-sha2-nistp521
  - Host key algorithms:
    - ssh-rsa

Server – Security

CC-SG Firmware v13.0.0

        - Ciphers:
            - aes128-ctr
            - aes192-ctr
            - aes256-ctr
        - MACs:
            - hmac-sha2-256
            - hmac-sha2-512
            - hmac-sha1
- TLS:
        - Customer can create/upload custom certificates or regenerate self-signed certificate from CC-SG.
        - Client code does certificate and hostname verification (i.e. rejects invalid certificates)
- SNMPv3:
        - AES and DES
- User credentials (passwords) are hashed using MD5.
- Default password policy requires default administrator account to set a new strong password prior to operation in a production environment.
- HTTPS:
        - Defaults with Content-Security-Policy headers for XSS protection.
        - Uses HSTS headers to force HTTPS communications.
        - Password fields in UI set with autocomplete off.
        - Certificate authentication can be used rather than passwords
- CLI SSH:
        - Certificate authentication can be used rather than passwords.
- IP Access control can be enabled to allow/disallow CC-SG access from IP ranges.
- User account lockout can be enabled after failed login attempts.
- Concurrent logins per user can be disabled for administrators or all users