LEGRAND – DPC
SECURITY INFORMATION

Dominion® Enhanced User Station v5.2

Dawn Syskowski – Updated 07/28/2025

TABLE OF CONTENTS

Security System Overview | DKX3-EUST & DKX4-EUST Firmware v5.2

- At Legrand, there is a heightened awareness of the impact that poor product security could have on the end customer.
- As part of our Enhanced User Station (EUST) firmware development cycle and ongoing threat assessment, Legrand does run two security scanners on firmware releases.
    - Legrand owns a Nessus vulnerability scanner license, renewed annually.
    - Before a new firmware is released, we test it 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 its latest version.
    - In addition, Legrand owns a Veracode static code analyzer license. Before each new firmware release, we test our software with this tool for common mistakes in software development.
- During a firmware release system test cycle, security-related firmware features are tested.
- EUST firmware require strong passwords for administrator by default. Strong password rules can be customized and enabled for all users too.
- Legrand uses the OpenSSL FIPS 140-2 module on the KXUST device. This can be optionally enabled to force only FIPS 140-2 validated algorithms to be used.
- KXUST firmware requires an immediate change from the default user password to a new password.
- In the default configuration, EUST is a pure client device. It does not offer any network services (all network ports are closed by a firewall), unless explicitly enabled by the administrator.
- Legrand has a Security Working Group which is dedicated on staying ahead of the requirements for security.

Security Stack

DKX3-EUST & DKX4-EUST Firmware v5.2

- The Operating System is based on:
  - Rocky Linux with some minor modifications by Raritan for specific platform support and configuration.
    - Version: 9.3 (Blue Onyx)
    - URL: https://www.rockylinux.org/
    - Open Source library and program source code
- Linux Kernal
  - Version 5.14.0-362.18.1.el9_3.x86_64 (with modifications and fixes done by Rocky Linux)
- The SSL stack is:
  - OpenSSL
    - Version: 3.0.7
    - URL: https://www.openssl.org/
    - License: Apache 2.0
  - GnuTLS
    - Version: 3.7.6
    - URL: https://www.gnutls.org/
    - License: GPL / LGPL

Security Stack

DKX3-EUST & DKX4-EUST Firmware v5.2

- The SSH stack for Diagnostic Console at port 22 is (if “Support Login” is enabled):
  - Package: OpenSSH
  - Version: 8.7p1
  - URL: https://www.openssh.com/
  - License: BSD
- The web server at port 8443 is (https; if “Remote API” is enabled), 443 (https; if “Remote Control” is enabled) and port 80 (http; only if “Allow HTTP” is enabled):
  - Package: nginx
  - Version: 1.20.1
  - URL: https://nginx.org/
  - License: BSD

Web Server

DKX3-EUST & DKX4-EUST Firmware v5.2

- By default, the web server is disabled
- The web server can be enabled by the following settings:
  - “Remote Control”
    - Port 443 for remotely controlling KXUST via web browser
    - Uses https
  - “Allow HTTP” (for Remote Control)
    - Port 80 for remotely controlling KXUST via web browser
    - Uses http
  - “Remote Control API”
    - Port 8443 for remotely controlling KXUST via API
    - Uses https
- https web server
  - TLSv1.2 and TLSv1.3 only
  - Security related headers:
    - Strict-Transport-Security "max-age=31536000; includeSubDomains"
    - Content-Security-Policy "default-src 'none'; script-src 'self' 'unsafe-inline'; connect-src 'self'; img-src 'self' data:; style-src 'self' 'unsafe-inline'; font-src 'self'; base-uri 'self'; form-action 'self'"
  - SSL ciphers: ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384

- http web server is discouraged, but can be enabled for compatibility reasons
- Customer can create/upload custom certificates or regenerate self-signed certificate from KXUST

Other Security Considerations | DKX3-EUST & DKX4-EUST Firmware v5.2

- Passwords of local users are hashed with the bcrypt algorithm.
- Credentials for other devices (KX3, KX4, CC-SG, VNC passwords, etc.) are stored encrypted using AES-256-CBC.
- Default password policy requires default administrator account to set a new strong password prior to operation in a production environment.
- Strong passwords are enabled by default, password strength requirements can be configured.
- Client code does certificate and hostname verification (i.e. rejects invalid certificates) if configured. This can be set up separately for each client protocol.
- User account lockout can be enabled after failed login attempts.
- 802.1x can be configured for physical ethernet router security and validation