

LEGRAND – ACCESS & CONTROL
SECURITY INFORMATION

Dominion® KX III

Dawn Syskowski – Updated 10/13/2026



TABLE OF CONTENTS

Security System Overview 03

Operating System – Security Stack 04

Operating System – Security 05



Security System Overview

DKX3 Firmware v3.10

- At Legrand, there is a heightened awareness of the impact that poor product security could have on the end customer.
- As part of our Dominion KX III 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.
- DKX3 firmware requires strong passwords for administrator by default. Strong password rules can be customized and enabled for all users too.
- Legrand uses the OpenSSL FIPS 140-3 module on the KX3 device. This can be optionally enabled to force only FIPS 140-3 validated algorithms to be used
- KX3 firmware requires an immediate change from the default user password to a new password
- Legrand has a Security Working Group which is dedicated on staying ahead of the requirements for security.

Operating System – Security Stack

DKX3 Firmware v3.10

- The Operating System source code is solely based on:
  - Source Code written and owned by Raritan (proprietary source code) and
  - Open Source library and program source code (a complete list of all used Open Source libraries can be provided on demand)
- The SSH stack is based on:
  - Package: Dropbear
  - Version: 2025.88
  - URL : http://matt.ucc.asn.au/dropbear/dropbear.html
  - License: MIT
- The SSL stack is based on:
  - Package: openssl
  - Version: 3.5.5
  - FIPS 140-3 Version: 3.1.2
  - URL : http://www.openssl.org/
  - License: OpenSSL
  - Note: own license (http://www.openssl.org/source/license.html

Operating System – Security

DKX3 Firmware v3.10

- Details about the encryption technology, cryptographic libraries, algorithms, and mode choices:
  - OpenSSL
    - TLS 1.0, 1.1, 1,2, 1.3 are enabled by default.
    - The ciphers and modes used can be customized for user security requirements.
    - Default Supported TLS ciphers and mode combinations in order of priority (priority is server enforced):
      - TLSv1.0 / TLSv1.1:
        - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
        - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
        - TLS_RSA_WITH_AES_256_CBC_SHA
        - TLS_RSA_WITH_AES_128_CBC_SHA
      - TLSv1.2:
        - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
        - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
        - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
        - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
        - TLS_RSA_WITH_AES_256_GCM_SHA384
        - TLS_RSA_WITH_AES_256_CCM
        - TLS_RSA_WITH_AES_128_GCM_SHA256
        - TLS_RSA_WITH_AES_128_CCM

Operating System – Security

DKX3 Firmware v3.10

        - TLS_RSA_WITH_AES_256_CBC_SHA256
        - TLS_RSA_WITH_AES_128_CBC_SHA256
        - TLS_RSA_WITH_AES_256_CBC_SHA
        - TLS_RSA_WITH_AES_128_CBC_SHA
        - TLS_RSA_WITH_AES_256_CCM_8
        - TLS_RSA_WITH_AES_128_CCM_8
    - TLSv1.3:
        - TLS_AKE_WITH_AES_256_GCM_SHA384
        - TLS_AKE_WITH_CHACHA20_POLY1305_SHA256
        - TLS_AKE_WITH_AES_128_GCM_SHA256
- Unused protocols like SSL2, SSL3, DTLS, SRP and unused algorithms are not compiled in to reduce attack risk
- Upstream code is 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.

Operating System – Security

DKX3 Firmware v3.10

- Dropbear SSH server:
  - Key exchange:
    - sntrup761x25519-sha512
    - sntrup761x25519-sha512@openssh.com
    - mlkem768x25519-sha256
    - curve25519-sha256
    - curve25519-sha256@libssh.org
    - ecdh-sha2-nistp521
    - ecdh-sha2-nistp384
    - ecdh-sha2-nistp256
    - diffie-hellman-group14-sha256
    - kexguess2@matt.ucc.asn.au
    - kex-strict-s-v00@openssh.com
  - Host key algorithms:
    - ssh-ed25519
    - ecdsa-sha2-nistp256
    - rsa-sha2-256
  - Ciphers:
    - aes128-ctr
    - aes256-ctr
  - MACs:
    - hmac-sha2-256
    - hmac-sha2-512

Operating System – Security

DKX3 Firmware v3.10

- TLS:
  - customer can create/upload custom certificates
  - client code does certificate and hostname verification (i.e. rejects invalid certificates)
- SNMPv3:
  - AES and DES
- User credentials (passwords) are hashed using PBKDF2 function (SHA512, 10000 rounds, 16 bytes salt)
- By default, a secure connection is required (HTTPS instead of HTTP)
- HTTPS:
  - Defaults with Content-Security-Policy headers for XSS protection.
  - Can be configured with HSTS headers to force HTTPS communications.
  - Certificate authentication can be configured with CRL or OCSP certificate validation.
  - Host Allowlist can be configured to prevent HOST redirect attacks.
  - Password fields in UI set with autocomplete off.
  - Smartcards can be used to log in to the device
- SSH:
  - Legacy DSA algorithms disabled by default.
  - Certificate authentication can be used rather than passwords.
- 802.1x:
  - 802.1x can be configured for physical ethernet router security and validation.
- IP Access control can be enabled to allow/disallow device access from IP ranges
- Strong passwords enabled by default, password strength requirements can be configured
- Disable user accounts because of failed login attempts