FIELD BULLETIN

Senetas network encryptors' V5.1.0 Firmware upgrade (recommended action)

Product Variants: All CN and CV Series Encryptors

Purpose: This bulletin provides guidance for transitioning to the V5.1.0 firmware release for all fielded encryptors. Senetas recommends that all CN and CV Series encryptors be updated to the 5.1.0 firmware.

Although, the V5.1.0 firmware is not backward compatible with prior versions of firmware, it provides extensive feature enhancements, customer benefits, and updates to meet the latest security standards while addressing a known issue as outlined below.

The release is being provided at no cost to all Senetas customers from the Senetas Support Portal.

Feature Enhancement – Network Independent Encryption:

The V5.1.0 firmware release introduces Network Independent Encryption, providing customers significant benefits of a single encryption security solution suitable for today's increasingly complex and mixed network protocols (Layers).

V5.1.0 enables policy-based concurrent encryption of multi-Layer (network protocol Layers 2, 3, and 4) networks. Customers using a mix of these network protocols and V5.1.0 may avoid the costs, management overheads and inflexibilities of multiple encryption solutions.

Additionally, V5.1.0 enables support for GCM authenticated encryption and Forward Error Correction (FEC) on CN9000 Series 100Gbps encryptors; CN6140 1/10Gbps multi-port encryption and ETSI draft Quantum Key Distribution (EQKD). Please refer to the Release Notes and User Guide for a full list of features now available with V5.1.0.

Security Standard Updates:

V5.1.0 firmware meets the latest NIST guidance set out in the Transitioning the Use of Cryptographic Algorithms and Key Lengths publication (SP800-131A).

However, the NIST updates incorporated in V5.1.0 render it inoperable with all prior firmware versions.

Senetas recommends that all fielded encryptors be upgraded to firmware V5.1.0 to meet this latest NIST guidance; and ensure encryptors' interoperability within the network.

Please see the Release Notes for further details on interoperability and upgrade caveats.

Known Issue:

The encryptors' software library required modification in order to address an undesired function. The change removes an authentication mechanism whereby self-signed encryptor certificates may be accepted during session establishment. The change reduces the scope of accepted certificates, but does not alter the underlying security or cryptographic mechanism.

Firmware updates are available in the Senetas support portal to address this issue.

Please address all questions regarding firmware upgrades for the CN Series encryptors to the Senetas Support Team.

Senetas is a leading developer of encryption security solutions; trusted to protect enterprise, government, defence, cloud and service provider data in over 40 countries. From certified high-assurance hardware, and virtualised encryption, to secure file sharing and collaboration with data sovereignty control, all are based on the same crypto-agile platform and deliver security without compromise.

Senetas encryption solutions are distributed and supported internationally (outside Australia and New Zealand) by Thales.

Asia	**T:** +65 8307 3540	**E:** infoasia@senetas.com
Australia & New Zealand	**T:** +61 (03) 9868 4555	**E:** info@senetas.com
Europe, Middle East & Africa	**T:** +44 (0) 1256 345 599	**E:** info@senetas-europe.com
The Americas	**T:** +1 949 436 0509	**E:** infousa@senetas.com

SENETAS
Security without compromise