

Attachment D

Ethos Connected and supporting devices comply with the AES 256 standard. AES is a symmetric key cipher. This means the same secret key is used for both encryption and decryption, and both the sender and receiver of the data need a copy of the key. By contrast, asymmetric key systems use a different key for each of the two processes. Asymmetric keys are best for external file transfers, whereas symmetric keys are better suited to internal encryption. The advantage of symmetric systems like AES is their speed. Because a symmetric key algorithm requires less computational power than an asymmetric one, it's faster and more efficient to run. AES 256 is virtually impenetrable using brute-force methods.