Data Encryption on Barracuda Backup Appliances

https://campus.barracuda.com/doc/93198754/

Encryption of data at rest on Barracuda Backup appliances is a new feature **only available on appliances that have shipped after September 25, 2020**. If you received a Barracuda Backup appliance after April 2020 and would like to confirm if it is encrypted, contact Barracuda Networks Technical Support.

As data breaches become a daily occurrence, it is important for organizations to adopt effective data security strategies to protect themselves. In some cases, organizations do not have a choice as more countries are putting data protection laws in place, such as the European Union’s General Data Protection Regulation (GDPR). Encrypting data is often the most common strategy for securing data and meeting compliance requirements. However, if done incorrectly, can have a negative impact on both performance and productivity. With Barracuda Backup, you have an encryption strategy that is both secure and efficient.

Benefits of data encryption in Barracuda Backup include:

- Support all Barracuda Backup appliances with XTS-AES 256-bit encryption of data stored at rest.
- Allow secure encryption key management with the use of Trusted Platform Module (TPM).
- Enable compliance with the most common industry regulations with software-based encryption.
- Retain the high standard of backup and recovery performance expected in Barracuda Backup.

Using volume-level encryption, Barracuda Backup securely stores data at rest and minimizes the intrusiveness and performance degradation typically associated with encryption. The addition of a Trusted Platform Module (TPM) provides an additional layer of security, allows encryption key management, and follows industry best practices. A TPM is a specialized chip on a device that stores RSA encryption keys specific to the host system for hardware authentication. Each TPM chip contains an RSA key pair called an Endorsement Key (EK). The pair is maintained inside the chip and cannot be accessed by software. Each TPM generates a unique set of encryption keys for each Barracuda Backup appliance. Without the TPM, the Barracuda Backup appliance will fail to boot.

Encryption of data at rest is supported on all Barracuda Backup appliance models (190 – 1191), is enabled by default, and comes at no additional cost. If you are using an older hardware version of Barracuda Backup that does not include support for data encryption at rest, contact your Barracuda Networks representative to learn more about upgrade or replacement options.