Protecting Encrypted Source Data

https://campus.barracuda.com/doc/78156845/

Barracuda Backup, including the Barracuda Backup Agent for Windows and Linux, can protect files, servers, and virtual machines (VMs) that are using various encryption methods including file-, disk-, and volume-based encryption.

File-Based Encryption

Barracuda Backup supports backup of encrypted files. The encrypted files are backed up and stored in the encrypted state on your Barracuda Backup device. Upon recovery, the files are restored back to the restore target in the same encrypted state.

Disk and Volume Encryption

Barracuda Backup supports the backup of files stored on encrypted hard disks or volumes. Because Barracuda Backup backs up data at the file level, the files located on an encrypted disk or volume are backed up and stored on your Barracuda Backup device in an unencrypted state. Because the files are backed up in an unencrypted state, they are restored back to the target unencrypted.

Virtual Machines

VMware vSphere and Microsoft Hyper-V VMs that contain encrypted files, volumes, or disks are backed up in their encrypted state. Upon recovery, the data is restored in its encrypted state.

Microsoft BitLocker Drive Encryption

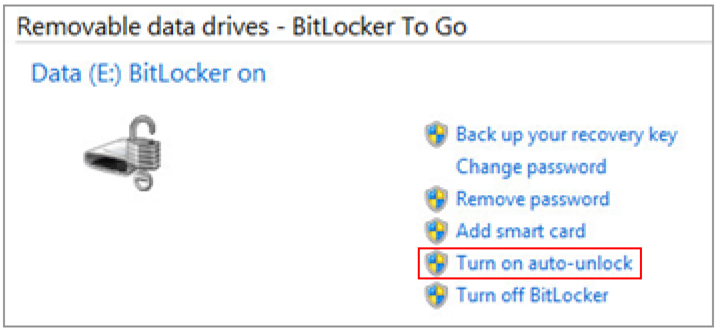
BitLocker Drive Encryption is a Windows data protection operating system feature starting with Windows Vista. Subsequent operating system releases continue to improve security, providing BitLocker protection to more drives and devices. BitLocker and operating system integration addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers.

Backup

The Barracuda Backup Agent for Microsoft Windows supports BitLocker Drive Encryption for both operating system drives and data drives. By default, after booting a system, the operating system drive is "unlocked" and the Barracuda Backup Agent is able to read and access the files. For data drives, the **Auto-Unlock** setting must be turned on so that the Barracuda Backup Agent is able to read and access the files. For data drives, the **Auto-Unlock** setting must be turned on so that the Barracuda Backup Agent can access the encrypted drive. Once all drives are "unlocked" the files are backed up in an unencrypted state even though the drives are still being encrypted.

To enable the **Auto-Unlock** setting on Windows Server 2012 R2:

1. Open the **BitLocker Drive Encryption Manager** from the **Control Panel**.
2. Select the data drive, and click **Turn on auto-unlock**:



3. The encrypted drive is now accessible without password or recovery key prompts.

Recovery

Since the files on the encrypted drives are backed up in an unencrypted state, they are also restored unencrypted. Bare Metal Restoration is possible for systems using BitLocker Drive Encryption. After performing Bare Metal Recovery, the BitLocker service continues running, but BitLocker Drive Encryption is disabled for each drive and must be re-enabled from the BitLocker Drive Encryption Manager in the Control Panel.

Figures