

BitLocker Management for Windows 10 and 11

Description

This article provides a comprehensive overview of the Compliance Pack dedicated to managing and reporting on the BitLocker encryption status for Windows 10 and 11 devices using FileWave. BitLocker is an essential security feature that encrypts the entire disk to protect data from unauthorized access. Organizations need to ensure BitLocker is activated and properly configured to meet security standards and regulatory mandates. This Compliance Pack facilitates monitoring, reporting, and management of BitLocker on Windows 10 and 11 devices, aiding organizations in maintaining a secure operational landscape.

Ingredients

- FileWave Central
- Windows OS systems running a version of Windows that is licensed for BitLocker
- BitLocker Fileset
 - Activation: Associate the Fileset with Windows clients to enable BitLocker.
 - Deactivation: Remove the association to disable BitLocker.
 - Customization: The script within the Fileset includes specific options that can be customized by administrators based on organizational needs.
- Custom Fields
 - BitLocker Key: Displays the recovery keys for encrypted drives. For example, "C:, 219296-176121-018458-479017-019437-305833-463155-542608". After importing the Custom Field, choose to assign it to specific devices or all devices.
 - BitLocker Status: Presents the current encryption state, such as "Conversion Status: Used Space Only Encrypted".



Directions

Download

1. Download the BitLocker Compliance Pack.
 - Unzip the zip file and you will find a Fileset as well as a Custom Fields file.

BitLocker Custom Fields

The Custom Fields will report information to you and will not encrypt the devices or take any action other than reporting in their current form. The below steps will get you started.

1. In FileWave Central go to Assistants -> Custom Fields -> Edit Custom Field Definitions.
2. Click "Import" and pick the .customfields file from the zip you downloaded.
3. For both BitLocker Key and also BitLocker Status you'll want to select each and check "Assigned to all devices" if you would like to capture the status for all. Otherwise you could pick specific devices in the Clients view and right click there and pick to Edit Custom Field Associations to set specific devices to report.
4. You can now add these 2 new fields to the Clients view or any Query (Report) and see the status. You'll want to do a Model Update and then wait for a device to report in to see the reporting data.

Bitlocker Enforcement Fileset

This Fileset will take action on devices if it is assigned to them. You should test and be sure you understand what it is doing before applying it. If you Associate it with a device you will see that device will encrypt, and the Custom Fields you added will report on that. There is always a delay between action and reporting because an inventory must occur to see it in FileWave so don't worry if it is not immediate, and you can use a Verify to ask the device to inventory sooner when testing.

1. Drag and drop the Bitlocker Enforcement.fileset in to your Filesets area in FileWave Central.
2. Move it to wherever you would like it in the Filesets area.
3. Create an Association or a Deployment to assign it to a device.
4. Watch that device encrypt by looking at properties for the drive on that computer in Explorer or with manage-bde.exe on that computer. The Custom Fields will not update in real time so that is the best way to watch when testing.
5. Notice what happens if you break the Association. The device will decrypt.

You may wonder how this all works. If you pick Scripts from the toolbar when highlighting the Fileset you will see there is a script to encrypt and one to decrypt. If you run in to issues encrypting you will see log information in C:\ProgramData\FileWave\log\fwcld\ in the directory for the Fileset. Every Fileset has an ID number and a directory will be there for that Fileset. Consider if you are running

Windows Home Edition or some other version that doesn't include BitLocker. We can only enable BitLocker when the OS is capable. There are other settings and requirements and you'll see in the encryption script that you could edit it if you would like to set options slightly differently.

Next Steps

We will look to include instructions on setup of a Dashboard in Grafana and to simplify the setup instructions even more.

Related Content

- [Compliance Packs \(Windows\)](#)
- [Compliance Packs \(macOS\)](#)

🔄Revision #6
★Created 2 November 2023 14:26:00 by Josh Levitsky
✎Updated 31 January 2024 18:31:13 by Josh Levitsky