BitLocker Compliance Dashboard

Last Modified on 09.09.24

The **BitLocker Compliance** dashboard scans Active Directory, Configuration Manager, Entra ID, and MBAM for BitLocker compliance information. Scans can be filtered based on Domain, OU, and Collection. This dashboard pulls information from Active Directory, the ConfigMgr SQL database, Entra ID, and/or MBAM, depending on your BitLocker configuration.

NOTE: To view Entra ID data on this dashboard, you must be running at least Recast Software Version 5.6.2409.701.

Common Use Cases

- Identifying computers without stored recovery keys
- Identifying computers with no encryption or incorrect encryption
- Monitoring recovery key location changes during a migration

Run a BitLocker Scan

To scan devices for BitLocker compliance:

1. In your Configuration Manager console, expand the **Recast Software** node in the navigation panel and select **Right Click Tools** > **BitLocker Compliance**.

2. Choose filtering options:

- You can **Search By AD OU** or **Search by Collection**.
- You can choose to **Include keys stored in Entra ID**.

  NOTE: To enable this option, Right Click Tools must be connected to Recast Management Server and have a configured service connection between RMS and Entra ID.
- If your BitLocker keys are stored in the Configuration Manager BitLocker, choose to **Search By Collection**.

3. Click **Scan**.

Create a Snapshot or Trend

A dashboard snapshot lets you capture the state of your system at a single point in time. This functionality is available on the BitLocker Web Dashboard. You can view BitLocker compliance over a set period of time by creating a BitLocker Web Dashboard Trend.

BitLocker Compliance Charts

BitLocker Recovery Key Storage: Displays computers according to where keys are stored. Also displays computers without stored keys.

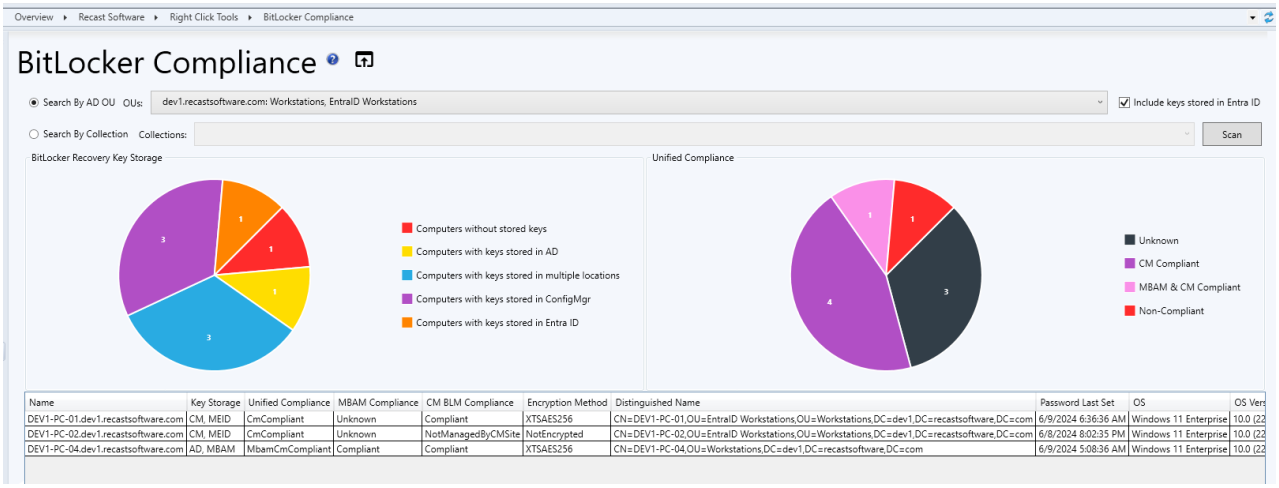
Key Storage Location Abbreviations

- Active Directory - AD
- Configuration Manager - CM
- Entra ID - MEID
- Microsoft BitLocker Administration and Monitoring - MBAM

Unified Compliance: Displays unified MBAM and ConfigMgr BitLocker compliance, which will be unique to each organization. Computers marked as **Non-Compliant** are not compliant in both MBAM and Configuration Manager BitLocker.

Click on a segment of the chart or legend to view details in the table.

Results can be downloaded by clicking **Export to CSV** at the bottom right of the page.



Actionable Results

As with all Right Click Tools Security and Compliance dashboards, the displayed results are actionable with Right Click Tools for single or multi-selected devices.

Tools commonly run against this dashboard:

- Remote Windows Security
- AD BitLocker Recovery Keys
- MBAM BitLocker Recovery Keys
- BitLocker Status

Recast Permissions

No additional permissions required.

Microsoft Permissions

- Read rights to Active Directory OUs and their computer objects contained within for the specific domain

- Read rights to AD computer object leaf/nested objects which contain BitLocker recovery keys
- Read rights to the MBAM Recover and Hardware database
- Read rights to the MBAM Compliance Status database