

v1.7

Coro version 1.7 provides many new features, enhancements, and fixes:

New features

This section describes the new features that we're releasing with version 1.7.

Remote disk encryption

Note

This feature is supported on installed drives only. It is not yet available for removable drives.

Coro now enables remote disk encryption for MS Windows endpoint devices. When you encrypt an endpoint remotely, the encryption key is automatically stored in the device details from the Coro Console.

For any device, you can see the list of drives and their statuses under **Actionboard > Devices > View**.

The screenshot displays the Coro console interface. On the left, a list of devices is shown with checkboxes and status icons. The selected device is 'User MARIANA052E' (Microsoft Windows 7 Professional). Below it are 'larysa' (MacBook Pro - Larysa (Offline) Monterey 12.6), 'dmitriydysa' (DMITRIYDYSYA14B9 (Offline) Microsoft Windows 10 Pro), and 'administrator' (Administrator's MacBook Pro Big Sur 11.6). On the right, a log entry shows 'Drive encryption was requested on MARIANA052E of user User' at 'Tue, Oct 25, 2:10 PM by Coro support'. Below the log, a 'Drives' table lists the drives and their encryption status.

Name	Status	Action
A:\ Non-removable	Not Encrypted	ENCRYPT (BITLOCKER)
C:\ Non-removable	Not Encrypted	ENCRYPT (BITLOCKER)

Additionally, tickets are generated for the vulnerability *Unencrypted Endpoint Drive* for supported endpoints when at least one of their drives is unencrypted. In this case, the device details per drive also appear in the ticket itself.

For more information, see [Endpoint encryption](#).

The **domain** and **violater** search operators are now available from a dropdown in the search field from **ticket logs**. This is the first of many additional operators we plan on adding.