LAPS Dashboard

Last Modified on 11.02.23

The **Local Administrator Password Solution (LAPS) Dashboard** displays LAPS compliance. The dashboard can help you to quickly determine if passwords are stored using the Microsoft LAPS tool, which is designed to help organizations store Local Administrator passwords securely without impeding the required access. This dashboard pulls information from your ConfigMgr database and Active Directory.

Run a LAPS Scan

To scan devices for LAPS compliance:

1. In your Configuration Manager console, navigate to **Assets and Compliance** > **Recast Software** > **LAPS Dashboard**.

2. Filter by **Domain** or **OU**.

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 LAPS Web Dashboard. You can view LAPS compliance over a set period of time by creating a LAPS Web Dashboard Trend.

LAPS Charts

LAPS Password in AD: Displays devices according to whether they have passwords stored in Active Directory.

LAPS Client Install State: Overall compliance of the LAPS client installed in the selected OU.

Click a segment of the chart or legend to view the associated list of devices.

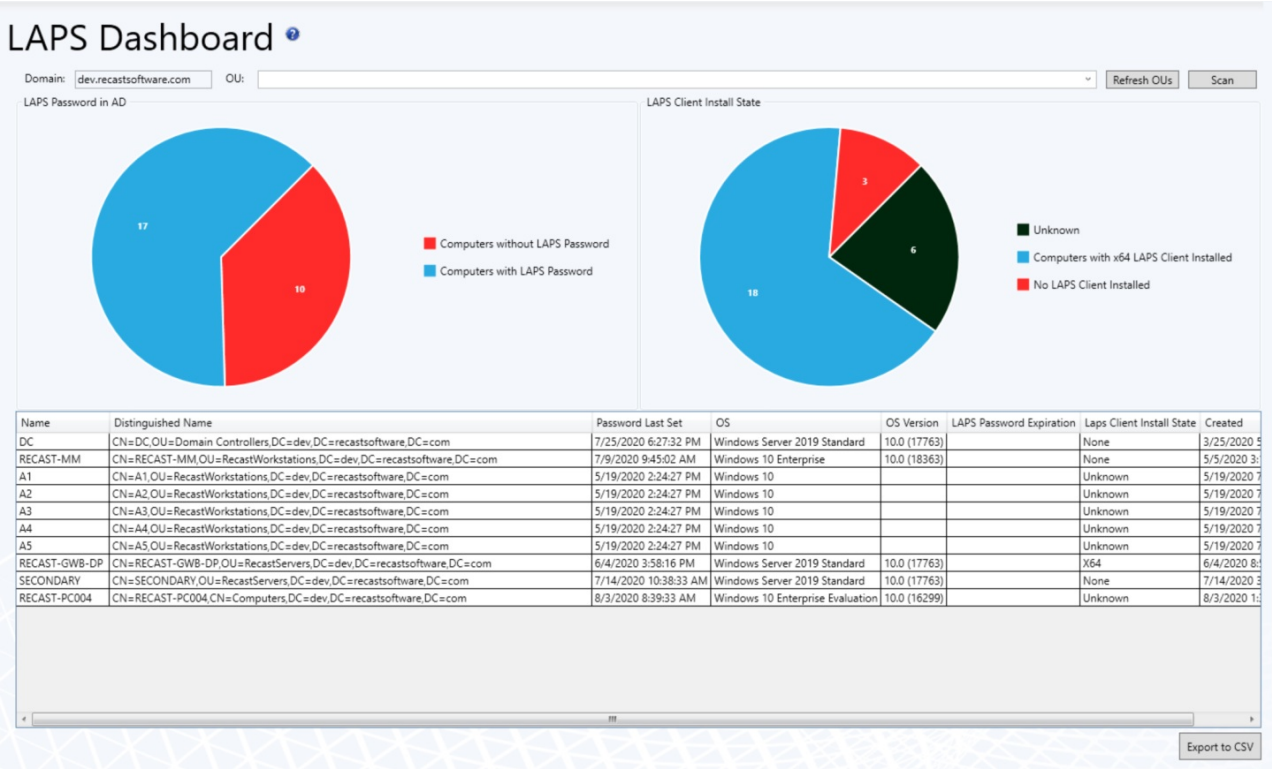
Results can be downloaded by clicking **Export to CSV** at the bottom right of the page.

Actionable Results

As with all of the RCT Security and Compliance Dashboards, LAPS results are actionable with Right Click Tools (and support multi-select).

Tools commonly run from this dashboard:

- AD LAPS Password
- Set LAPS Password Expiration



Recast Permissions

No additional permissions required.

Microsoft Permissions

- Requires read rights to Active Directory OUs and their computer objects contained within for the specific domain.
- Left-hand chart: Requires permission to read the LAPS password attribute.
- Right-hand chart: Requires permissions to device hardware inventory.