Console Dashboards

Last Modified on 03.13.24

Six Right Click Tools dashboards are available via your Configuration Manager console. For snapshot and trend functionality, plus the ability to share dashboard information without giving users access to ConfigMgr, try our Web Dashboards.

AD Cleanup

The **Active Directory Cleanup Dashboard** compares device object data in your Configuration Manager and Active Directory to show where devices are located. The dashboard pulls information from your ConfigMgr SQL database as well as Active Directory. As with all Right Click Tools Security and Compliance dashboards, the displayed results are actionable with Right Click Tools (and support multi-select).

For a video walkthrough, see AD Cleanup Dashboard on on our YouTube channel.

Common Use Cases

- Checking that computers are in the correct collections

Run an AD Cleanup Scan

An AD Cleanup scan compares data in OUs with the collections in which they should appear.

To run an AD Cleanup scan:

1. In your Configuration Manager console, navigate to **Assets and Compliance** > **Recast Software** > **Active Directory Cleanup Tool**.

2. Click in the **OUs** field and enter one or more **Domains**, use the Search tool, or select OUs using the picker.

3. Click in the **Collections** field and enter a **Site Code** and **SMS Provider**, use the Search tool, or select collections using the picker.

4. 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 AD Cleanup Web Dashboard. You can view AD Cleanup data over a set period of time by creating an AD Cleanup Web Dashboard Trend.

AD Cleanup Charts

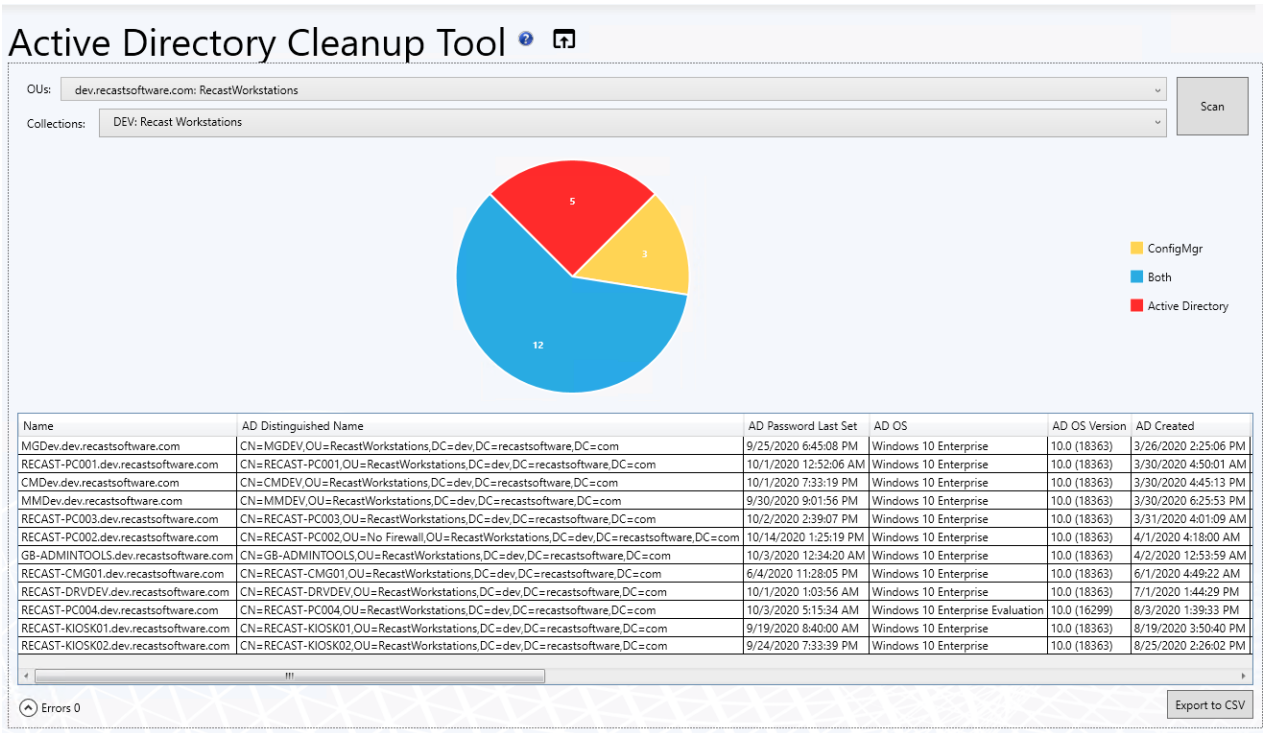
Click on a segment of the chart to view its associated details.

Results can be filtered by Domain, OU and Collection.

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

Actionable Results

You can run Right Click Tools actions for single or multi-selected devices.



Recast Permissions

Active Directory	Add Account to Group, Remove Account from Group
Installed Software	Active Directory Cleanup Tool

Microsoft Permissions

The Active Directory Cleanup tool requires read rights to Active Directory OUs and their computer objects contained within for the specific domain. It also needs read rights to Configuration Manager Device Collections, the ability to query collection membership, and read rights to the Configuration Manager devices themselves.

If you have entered the ConfigMgr database information in Recast Management Server or the Configure Recast Console Extension application, you will need to have at least "Read Only" Access to the ConfigMgr SQL Database.

BitLocker

The **BitLocker Compliance** dashboard scans Active Directory, MBAM, and ConfigMgr for BitLocker compliance information. Scans can be filtered based on Domain, OU, and Collection. This dashboard pulls information from

ConfigMgr SQL database, MBAM, and/or Active Directory, depending on your BitLocker configuration.

As with all Right Click Tools Security and Compliance dashboards, the displayed results are actionable with Right Click Tools (and support multi-select).

For a video walkthrough, see BitLocker Compliance Dashboard on YouTube.

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, navigate to **Assets and Compliance** > **Recast Software** > **BitLocker Compliance**.

2. Choose filtering options:

- If your BitLocker keys are stored in Active Directory or a standalone MBAM instance, choose to **Search By AD OU**.
- 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.

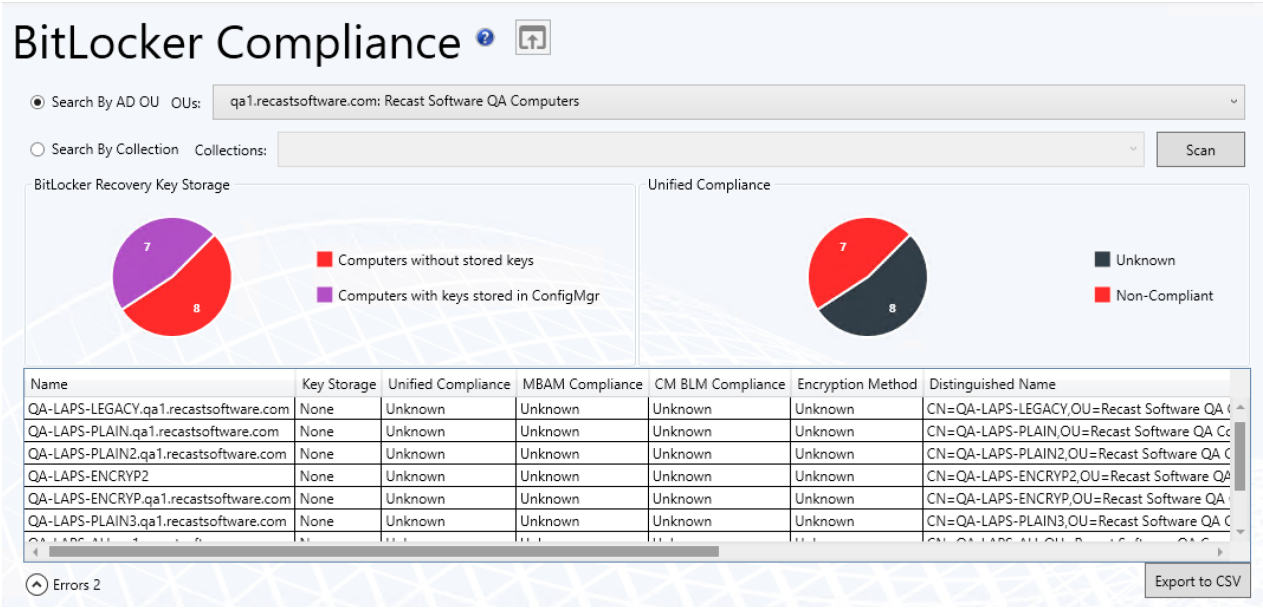
BitLocker Compliance Charts

BitLocker Recovery Key Storage: Displays computers according to where keys are stored (AD, ConfigMgr, MBAM). Also displays computers without stored keys.

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

You can run Right Click Tools actions 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

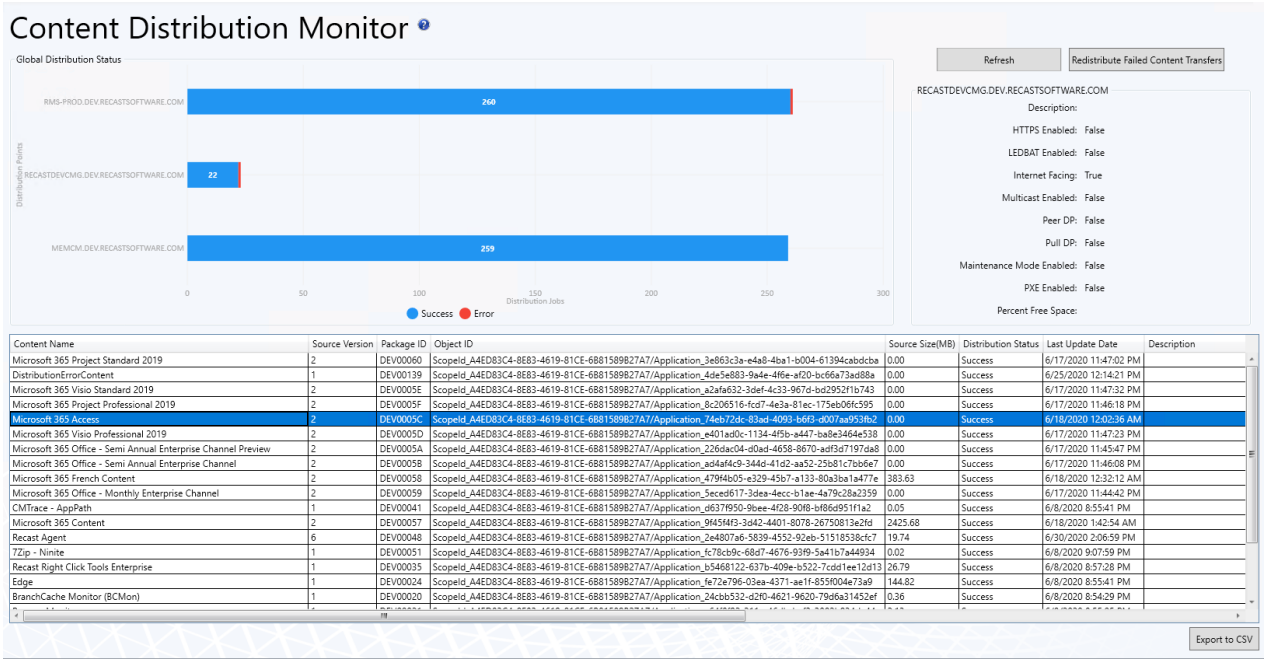
- Read rights to Active Directory OUs and their computer objects contained within for the specific domain
- Read rights to AD computer object leaf/nested objects which contain BitLocker recovery keys
- Read permissions to the MBAM Recover and Hardware database
- Read rights to the MBAM Compliance Status database

Content Distribution

The **Content Distribution Monitor** dashboard provides valuable information about your Distribution Point and assists in the management of content in your environment. This dashboard pulls information from your ConfigMgr database.

To view the dashboard in your Configuration Manager console, navigate to **Assets and Compliance** > **Recast Software** > **Content Distribution Monitor**.

For a video walkthrough, see Content Distribution Monitor on the Recast Software YouTube channel.



Content Distribution Monitor Charts

Global Distribution Status: Displays individual distribution points in your environment, as well as their distribution status. Successful, Error, and In Progress distributions are shown.

The section to the right of the chart displays information for the distribution point selected on the left. You can also **Refresh** the information to show any changes, and **Redistribute Failed Content Transfers** for the distribution point.

Click on a segment of the chart to view details in the bottom section.

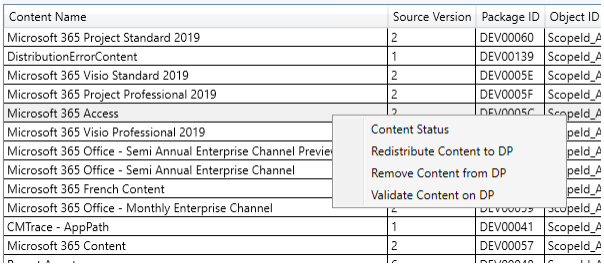
Results can be downloaded by clicking **Export to CSV** at the bottom right of the page.

Actionable Results

You can run Right Click Tools actions for a single or multi-selected devices.

Actions commonly run against this dashboard:

- Content Status
- Redistribute Content to DP



Recast Permissions

Administration	GetAllSettings
ConfigMgrServer	GetFailedContentOnDistributionPoint
ConfigMgrServer	GetAllContentStatus
ConfigMgrServer	GetAllDistributedContent
ConfigMgrServer	GetFailedContentOnDistributionPoint
ConfigMgrServer	GetDistributionPointContent
ConfigMgrServer	ContentDetails
ConfigMgrServer	AddContentToDistributionPoint
ConfigMgrServer	RedistributeContenttoDistributionPoint
ConfigMgrServer	RemoveContentfromDistributionPoint
ConfigMgrServer	GetContentStatus
ConfigMgrServer	UpdateContent
ConfigMgrServer	ValidateContentonDistributionPoint
ConfigMgrServer	GetDistributionPointConfigurationStatus

Hardware & Firmware

The **Hardware and Firmware Audit** dashboard displays computers in selected ConfigMgr collections according to chassis type, manufacturer, model, SecureBoot, UEFI, and BIOS version. This dashboard pulls information from your ConfigMgr database.

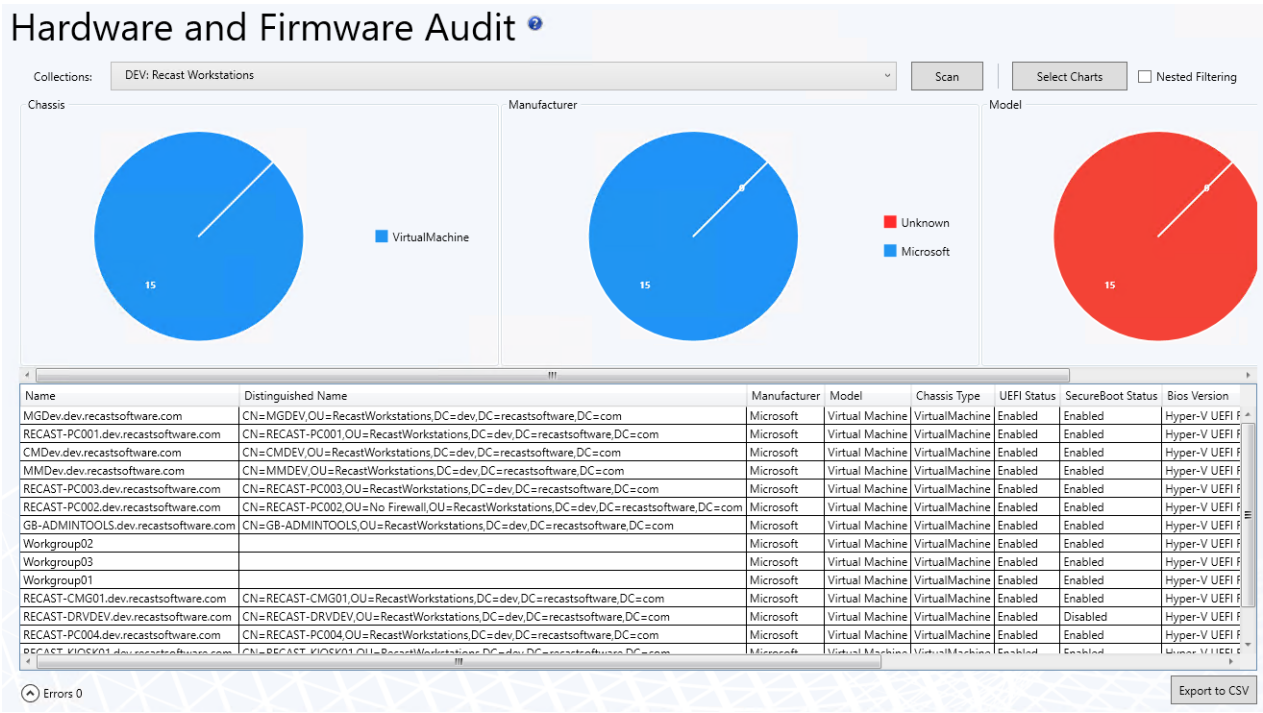
> **win32_computersystemproduct** and **win32_baseboard** must be added to your hardware inventory classes for full functionality with Lenovo and HP models.

To scan devices:

1. In your Configuration Manager console, navigate to **Assets and Compliance** > **Recast Software** > **Hardware and Firmware Audit**.

2. Filter by **Collections**.

3. Click **Scan**.



Hardware and Firmware Audit Charts

By default, the dashboard displays devices by **Chassis**, **Manufacturer**, and **Model**.

You can also click **Select Charts** to add SecureBoot, UEFI, and BIOS version charts. Scroll to the right to view additional charts. Click and drag charts to reorder them.

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

Enable **Nested Filtering** to drill down on chart data.

Download results by clicking **Export to CSV** at the bottom right of the page.

Actionable Results

From the dashboard, you can run any Right Click Tools device action on single or multi-selected devices.

Recast Permissions

ConfigMgrServer	GetActiveDirectoryForests
ConfigMgrServer	GetAllCollections
ConfigMgrServer	GetAllDeploymentTypes
ConfigMgrServer	GetAllDeviceCollections
ConfigMgrServer	GetAllDevices
ConfigMgrServer	GetAllDevicesinOu
ConfigMgrServer	GetBaseboardInformation
ConfigMgrServer	GetChassisInformation

ConfigMgrServer	GetComputerSystemInformation
ConfigMgrServer	GetComputerSystemProductInformation
ConfigMgrServer	GetDeviceCollectionFolders
ConfigMgrServer	GetDeviceCollectionInformationforDevice
ConfigMgrServer	GetDeviceCollectionMembers
ConfigMgrServer	GetDeviceCollectionsinFolder
ConfigMgrServer	GetDevicesInCollectionScope
ConfigMgrServer	GetDevicesInSiteScope
ConfigMgrServer	GetSiteDeviceCollectionsWithFolders
ConfigMgrServer	GetSystemBiosInformation
ConfigMgrServer	GetSystemConsoleUsageData
ConfigMgrServer	GetSystemOperatingSystemInformation
ConfigMgrServer	GetUnknownDevices

Microsoft Permissions

The Hardware and Firmware Audit Dashboard requires read rights to device collections for the Collection drop-down. It will need permissions to query devices within those collections as well as those devices' hardware inventory data.

LAPS

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.

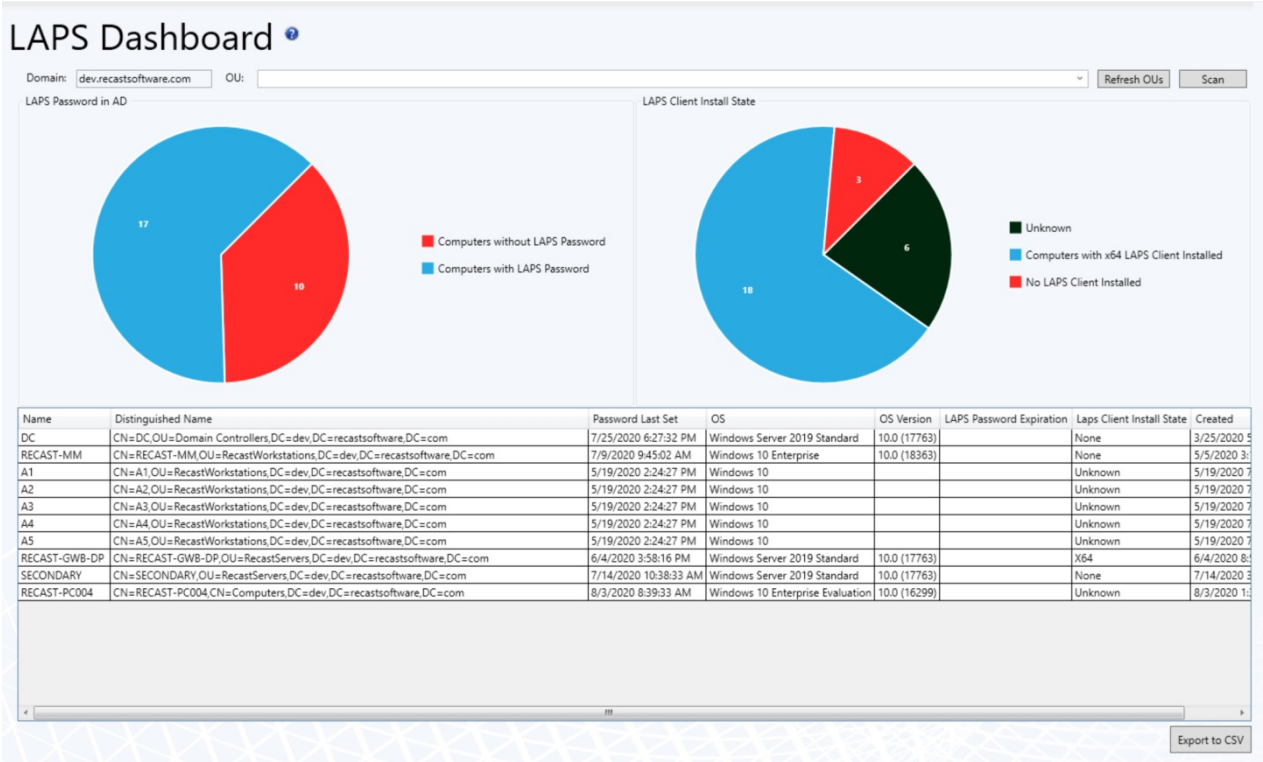
Results can be downloaded by clicking **Export to CSV** at the bottom right of the page.

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.

SUDS

The **Software Updates Deployment Status (SUDS) Dashboard** displays the update compliance for each update classification in your environment. It allows you to obtain detailed information about each update classification and take action on devices as needed.

The global list of updates is populated from SMS_SoftwareUpdate (WMI). The list of required/missing updates that are not in the Updates classification or the Office 365 Client product category is populated from SMS_UpdateComplianceStatus (WMI) or v_Update_ComplianceStatus (SQL, if configured).

For a video walkthrough, see SUDS Dashboard on the Recast Software YouTube channel.

Run a SUDS Scan

To scan devices for update compliance:

1. In your Configuration Manager console, navigate to **Assets and Compliance** > **Recast Software** > **Software Update Deployment Status**.

2. Select filtering options. Results can be filtered by **Collection**, **Software Update Group(s)**, **Deployed Updates**, **Update Date** and **Update Type**.

3. Click **Start**.

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

SUDS Charts

Device Compliance Status: Displays devices according to whether they have reported their compliance to Configuration Manager.

- A **Compliant** device has reported installed updates and no missing updates.
- A **Non-Compliant** device has reported at least one missing update.
- When compliance is listed as **Unknown**, a device has not reported installed and/or missing updates to Configuration Manager. This can occur if devices have not checked in since updates were deployed, if devices are no longer on the network, or if devices are not able to communicate with ConfigMgr servers for some other reason.

  If **Limit to deployed updates** is enabled, both the installed updates and missing updates will include only those that have been deployed. If no known updates have been deployed, no updates will be in either list, resulting in all devices being displayed as 'Unknown'.

Missing Updates By Category: Displays devices according to software update. Click on a segment of the chart or legend to view details in the bottom section.

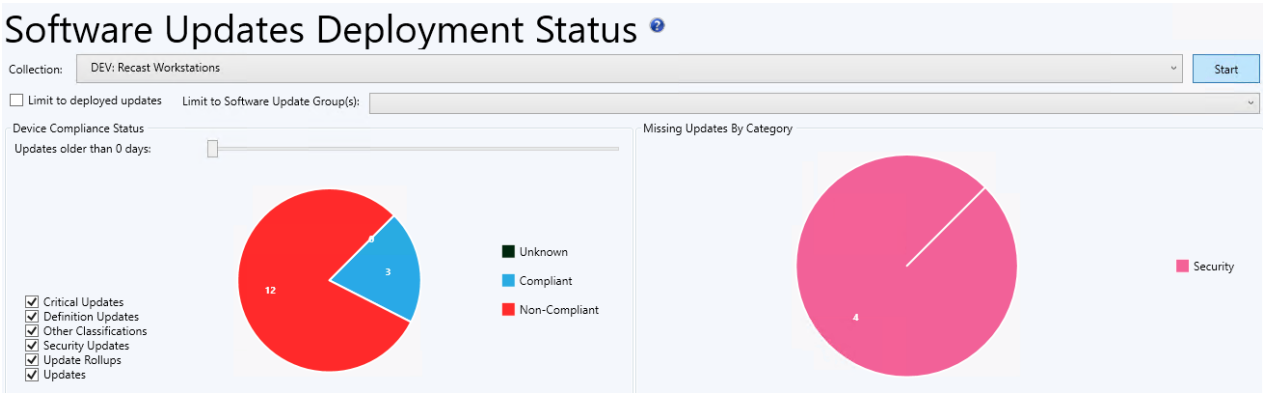
Click the chevron beside any device in the table to see additional information about each update on each device.

Download results by clicking **Export to CSV** at the bottom right of the page.

Actionable Results

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

From this dashboard you can access Remote Software Center to install missing updates on selected devices.



Recast Permissions

No additional permissions are required.

Microsoft Permissions

The Software Update Deployment Status dashboard requires read rights to device collections for the Collection drop-down. It will need permissions to query devices within those collections. In addition, it will need read permissions to Software Updates and Software Update groups within Configuration Manager.