Recast

SUDS Dashboard

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, expand the **Recast Software** node in the navigation panel and select **Right Click Tools** > **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.
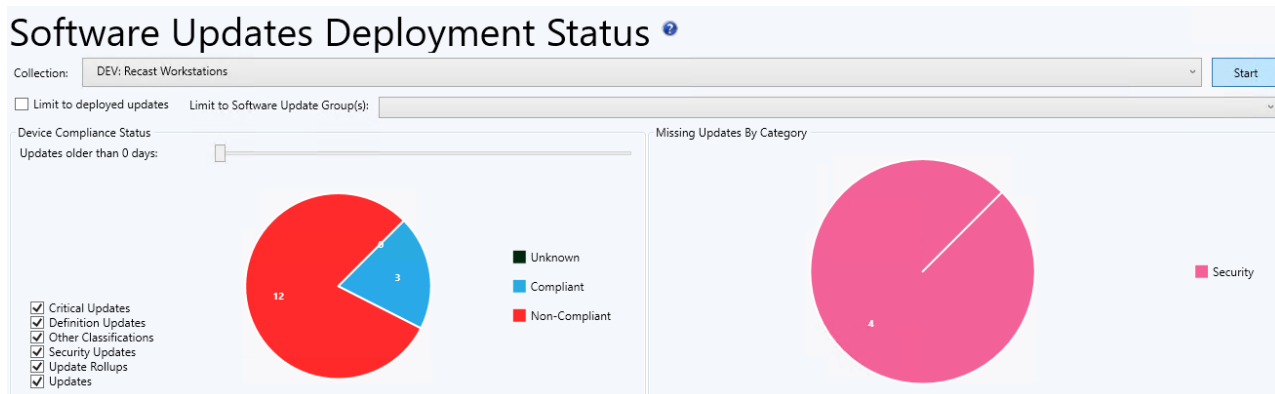
Download results by clicking **Export to CSV** at the bottom right of the page.

Actionable Results

Recast

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

Plugin	Permissions
ConfigMgrServer	GetCollectionById
	GetCollectionsforDevice
	GetInstalledSoftwareUpdates
	GetAllSoftwareUpdates
	GetNonCompliantUpdateStatuses
	GetAllDeviceCollectionMembers
	GetCompliantUpdateStatuses
	GetAllDeviceCollectionsCore
	GetAllDevicesCore
	GetDeviceCollectionInformationforDevice
	GetRecentDevicesScanned
	GetDeviceCollectionMembersByCollections
	GetAllDeviceCollectionsByCollections
	GetSiteDeviceCollectionsWithFoldersByCollections
	GetSoftwareUpdatesInGroup
	GetRequiredSoftwareUpdates
	GetAllDeviceCollections
	GetSoftwareUpdatesByResourceIds
	GetSoftwareUpdatesByCollections
	GetSoftwareUpdateGroups
	GetDistributedSoftwareUpdates
	GetCollectionFolderInformation
	GetDeviceCollectionMembers
	GetAllCollections
	GetDeviceCollectionFolders
	GetAllDevices
	GetDeviceCollectionsinFolder
	GetComputerSystemInformation
	GetSiteDeviceCollectionsWithFolders
	GetDevicesInCollectionScope
	GetDevicesInSiteScope
	GetUnknownDevices
	GetAllDevicesInOu
	GetSystemOperatingSystemInformation

Recast

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.