Software Updates Web Dashboard

Last Modified on 12.16.24

The **Software Updates Web Dashboard** displays update compliance in your environment. This dashboard requires a service connection to Configuration Manager.

Run a Software Updates Scan

To scan devices for update compliance:

1. In your Recast Management Server, navigate to **Dashboards** > **Software Updates**.

2. On the **Software Updates** page, click **Select Service Connections** to choose service connections to include in the scan.

3. In the side panel that opens, select the Configuration Manager collections to include.

4. Click **Save & Run Scan**.

Apply Filters

Once the scan runs, you can select and apply filters.

To apply filters:

1. Select from the following filters:

- **Limit to deployed updates**, with an option to only display **Updates older than x days**.
- **Limit to software update groups** by selecting a group from the drop-down list.
- Remove software update categories (Security Updates, Updates, Definition Updates, Update Rollups, Critical Updates, and Other Classifications) by unchecking them.

2. Click **Apply Filters**.

Edit Configuration Filters

After a scan runs, you can click **Edit** to change the service connections included in the scan.

Create a Snapshot

Take a snapshot of the dashboard to capture the state of your system at a single point in time.

To create a snapshot:

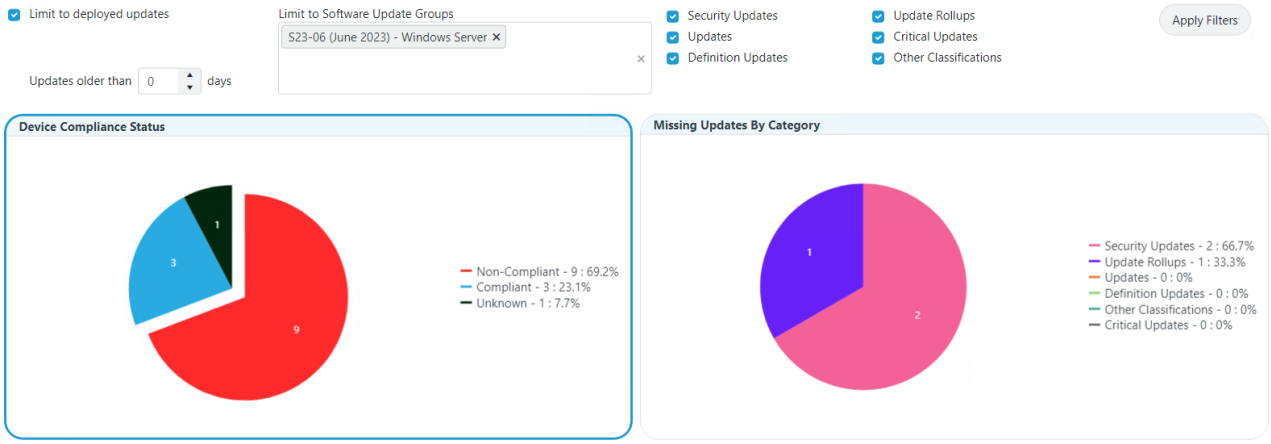
After a scan runs, click **Create Snapshot**.

Create a Trend

Schedule regular snapshots to view update compliance over a set period of time. See Software Updates Web Dashboard Trend.

Software Updates Charts

The Software Updates Dashboard displays two charts: **Device Compliance Status** and **Missing Updates by Category**. Click on a segment of the chart or legend to view details in the table below.



Device Compliance Status

Displays devices according to whether they have reported their compliance to Configuration Manager.

A **Compliant** device is reporting installed updates and no missing updates.

A **Non-Compliant** device is reporting 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 updates missing according to included categories (Security Updates, Updates, Definition Updates, Update Rollups, Critical Updates, Other Classifications).

Software Updates Tabs

Tabbed views offer additional information about the devices in each category. There are also options to **Export to CSV** and to **Expand to Full Screen**.