Web Dashboards

Last Modified on 03.13.24

You can access Right Click Tools web dashboards via your Recast Management Server. Our web dashboards offer additional functionality, such as snapshot and trend creation, when compared with the Right Click Tools dashboards available in your Configuration Manager console. These also allow administrators to give users access to dashboards without granting them access to ConfigMgr.

AD Cleanup Web Dashboard

The **AD Cleanup Web Dashboard** allows you to compare information related to devices in Active Directory and Configuration Manager.

Run an AD Cleanup Scan

To scan devices for AD Cleanup:

1. In your Recast Management Server, navigate to **Dashboards** > **AD Cleanup**.

2. On the **Active Directory Cleanup** page, click **Select Service Connections** to choose service connections to include in the scan.

3. In the side panel that opens, select objects in Active Directory and Configuration Manager to compare.

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

Edit Configuration Filters

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

Create a Snapshot

You can take a snapshot of the AD Cleanup 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**.

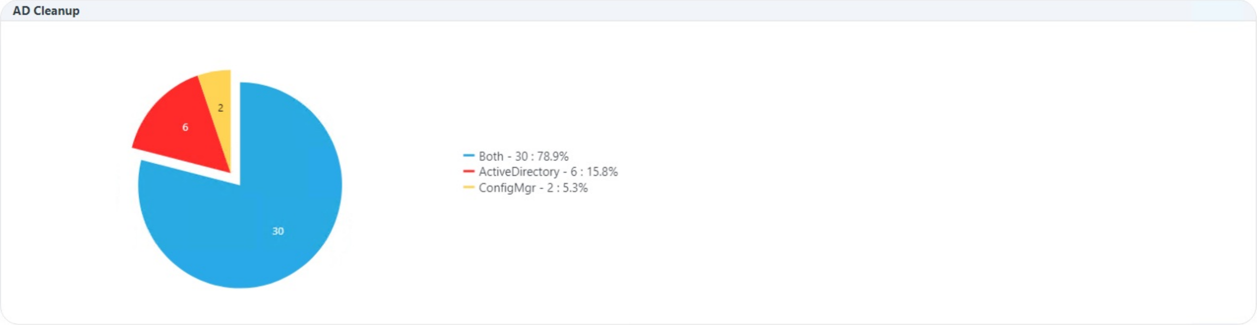
Create a Trend

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

AD Cleanup Charts

The AD Cleanup chart displays devices that appear in Active Directory, Configuration Manager, or both.

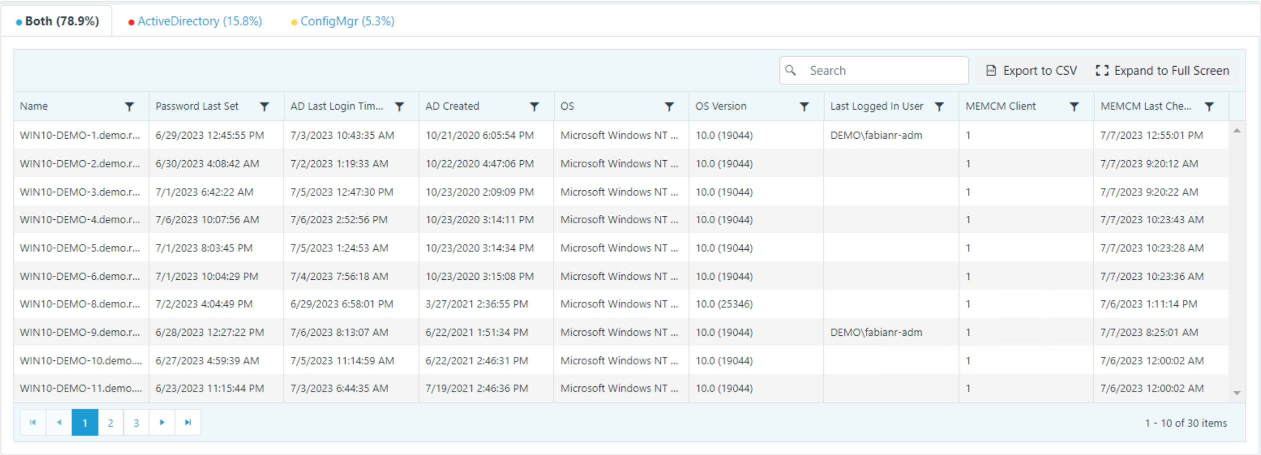
Devices not found in Configuration Manager will not have data in windows pertaining to ConfigMgr. Devices not found in Active Directory will be missing data that pulls from AD.



Click on a segment of the chart or legend to view details in the table below.

AD Cleanup 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**.



Name	Password Last Set	AD Last Login Tim...	AD Created	OS	OS Version	Last Logged In User	MEMCM Client	MEMCM Last Che...
WIN10-DEMO-1.demo.r...	6/29/2023 12:45:55 PM	7/3/2023 10:43:35 AM	10/21/2020 6:05:54 PM	Microsoft Windows NT ...	10.0 (19044)	DEMO\fabianr-adm	1	7/7/2023 12:55:01 PM
WIN10-DEMO-2.demo.r...	6/30/2023 4:08:42 AM	7/2/2023 1:19:33 AM	10/22/2020 4:47:06 PM	Microsoft Windows NT ...	10.0 (19044)		1	7/7/2023 9:20:12 AM
WIN10-DEMO-3.demo.r...	7/1/2023 6:42:22 AM	7/5/2023 12:47:30 PM	10/23/2020 2:09:09 PM	Microsoft Windows NT ...	10.0 (19044)		1	7/7/2023 9:20:22 AM
WIN10-DEMO-4.demo.r...	7/6/2023 10:07:56 AM	7/6/2023 2:52:56 PM	10/23/2020 3:14:11 PM	Microsoft Windows NT ...	10.0 (19044)		1	7/7/2023 10:23:43 AM
WIN10-DEMO-5.demo.r...	7/1/2023 8:03:45 PM	7/5/2023 1:24:53 AM	10/23/2020 3:14:34 PM	Microsoft Windows NT ...	10.0 (19044)		1	7/7/2023 10:23:28 AM
WIN10-DEMO-6.demo.r...	7/1/2023 10:04:29 PM	7/4/2023 7:56:18 AM	10/23/2020 3:15:08 PM	Microsoft Windows NT ...	10.0 (19044)		1	7/7/2023 10:23:36 AM
WIN10-DEMO-8.demo.r...	7/2/2023 4:04:49 PM	6/29/2023 6:58:01 PM	3/27/2021 2:36:55 PM	Microsoft Windows NT ...	10.0 (25346)		1	7/6/2023 1:11:14 PM
WIN10-DEMO-9.demo.r...	6/28/2023 12:27:22 PM	7/6/2023 8:13:07 AM	6/22/2021 1:51:34 PM	Microsoft Windows NT ...	10.0 (19044)	DEMO\fabianr-adm	1	7/7/2023 8:25:01 AM
WIN10-DEMO-10.demo....	6/27/2023 4:59:39 AM	7/5/2023 11:14:59 AM	6/22/2021 2:46:31 PM	Microsoft Windows NT ...	10.0 (19044)		1	7/6/2023 12:00:02 AM
WIN10-DEMO-11.demo....	6/23/2023 11:15:44 PM	7/3/2023 6:44:35 AM	7/19/2021 2:46:36 PM	Microsoft Windows NT ...	10.0 (19044)		1	7/6/2023 12:00:02 AM

Microsoft Permissions for the Proxy Service Account

- Requires read rights to Active Directory OUs and their computer objects contained within for the specific domain.
- Requires 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 by entering the database information in the Configure Recast Console Extension application or the Recast Management Server, you must have at least Read Only Access to the ConfigMgr SQL Database.

BitLocker Web Dashboard

The **BitLocker Web Dashboard** scans Active Directory, Configuration Manager, and MBAM for BitLocker compliance information.

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 Recast Management Server, navigate to **Dashboards** > **BitLocker**.

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

3. In the side panel that opens, select objects in Active Directory and Configuration Manager.

4. Ensure that at least one MBAM service connection is selected to run MBAM actions.

5. Click **Save & Run Scan**.

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**.

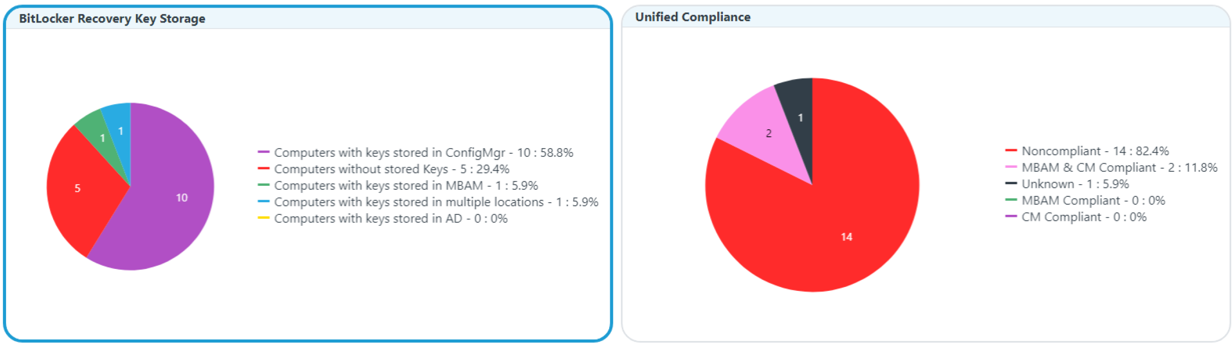
Create a Trend

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

BitLocker Charts

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

Unified Compliance: Displays devices according to compliance in the ConfigMgr database, the MBAM database, or both.

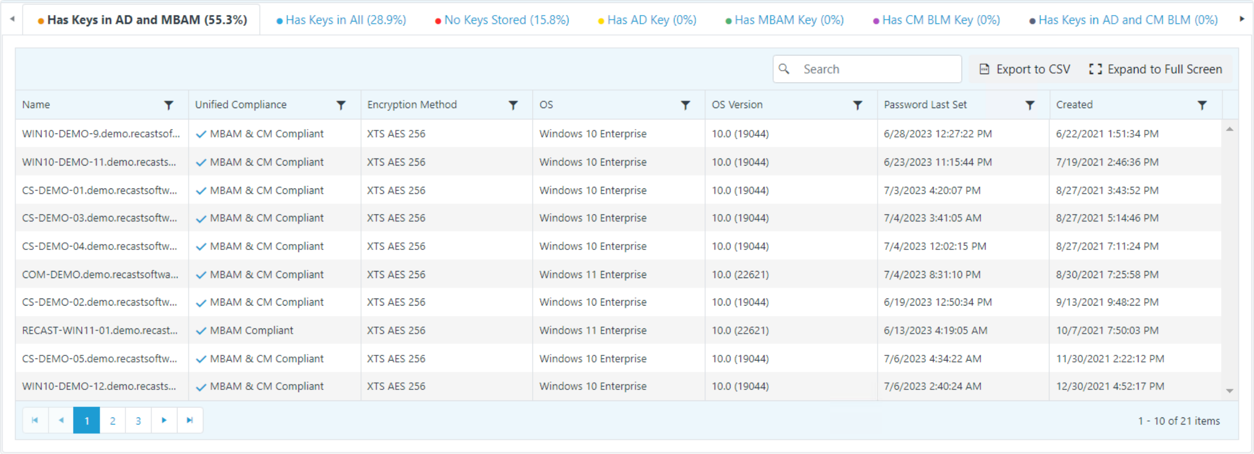


Click on a segment of the chart or legend to view details in the table.

> **NOTE**: Devices may be non-compliant due to a lack of encryption or because they were encrypted using the wrong method.

BitLocker 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**.



Name	Unified Compliance	Encryption Method	OS	OS Version	Password Last Set	Created
WIN10-DEMO-9.demo.recastsof...	✓ MBAM & CM Compliant	XTS AES 256	Windows 10 Enterprise	10.0 (19044)	6/28/2023 12:27:22 PM	6/22/2021 1:51:34 PM
WIN10-DEMO-11.demo.recasts...	✓ MBAM & CM Compliant	XTS AES 256	Windows 10 Enterprise	10.0 (19044)	6/23/2023 11:15:44 PM	7/19/2021 2:46:36 PM
CS-DEMO-01.demo.recastsoftw...	✓ MBAM & CM Compliant	XTS AES 256	Windows 10 Enterprise	10.0 (19044)	7/3/2023 4:20:07 PM	8/27/2021 3:43:52 PM
CS-DEMO-03.demo.recastsoftw...	✓ MBAM & CM Compliant	XTS AES 256	Windows 10 Enterprise	10.0 (19044)	7/4/2023 3:41:05 AM	8/27/2021 5:14:46 PM
CS-DEMO-04.demo.recastsoftw...	✓ MBAM & CM Compliant	XTS AES 256	Windows 10 Enterprise	10.0 (19044)	7/4/2023 12:02:15 PM	8/27/2021 7:11:24 PM
COM-DEMO.demo.recastsoftwa...	✓ MBAM & CM Compliant	XTS AES 256	Windows 11 Enterprise	10.0 (22621)	7/4/2023 8:31:10 PM	8/30/2021 7:25:58 PM
CS-DEMO-02.demo.recastsoftw...	✓ MBAM & CM Compliant	XTS AES 256	Windows 10 Enterprise	10.0 (19044)	6/19/2023 12:50:34 PM	9/13/2021 9:48:22 PM
RECAST-WIN11-01.demo.recast...	✓ MBAM Compliant	XTS AES 256	Windows 11 Enterprise	10.0 (22621)	6/13/2023 4:19:05 AM	10/7/2021 7:50:03 PM
CS-DEMO-05.demo.recastsoftw...	✓ MBAM & CM Compliant	XTS AES 256	Windows 10 Enterprise	10.0 (19044)	7/6/2023 4:34:22 AM	11/30/2021 2:22:12 PM
WIN10-DEMO-12.demo.recasts...	✓ MBAM & CM Compliant	XTS AES 256	Windows 10 Enterprise	10.0 (19044)	7/6/2023 2:40:24 AM	12/30/2021 4:52:17 PM

Actionable Results

Right Click Tools actions commonly run against results in this dashboard:

- Remote Windows Security
- AD BitLocker Recovery Keys
- MBAM BitLocker Recovery Keys

Microsoft Permissions for the Proxy Service Account

- Requires read rights to Active Directory OUs and the computer objects contained within them for the specific domain.

- Requires read rights to AD computer object leaf/nested objects which contain BitLocker recovery keys.
- Requires read rights to the MBAM Recovery and Hardware database.
- Requires read rights to the MBAM Compliance Status database.

LAPS Web Dashboard

The **Local Administrator Password Solution (LAPS) Web Dashboard** displays LAPS compliance. The dashboard can help you to quickly determine if passwords are stored using Microsoft's LAPS tool, which is designed to help organizations store Local Administrator passwords securely without impeding the required access.

Run a LAPS Scan

To scan devices for LAPS compliance:

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

2. On the **LAPS Dashboard** page click **Select Service Connections** to choose service connections to include in the scan.

3. In the side panel that opens, select objects in Active Directory.

Your Configuration Manager information is automatically selected. It is used to determine the LAPS client install state.

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

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**.

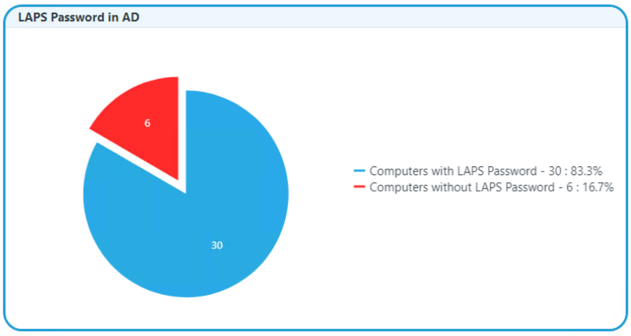
Create a Trend

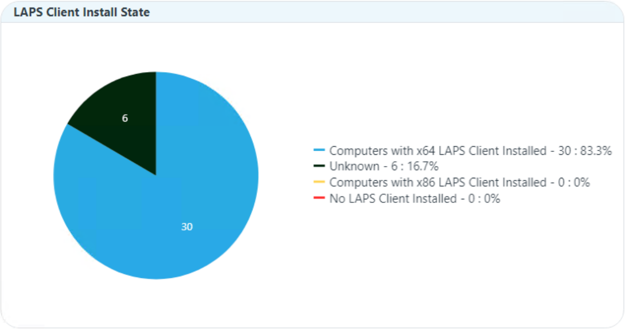
Schedule regular snapshots to view LAPS compliance over a set period of time. See LAPS Web Dashboard Trend.

LAPS Charts

LAPS Password in AD: Displays devices with and without a LAPS Password in Active Directory.

LAPS Client Install State: Displays devices with and without the LAPS Client installed.

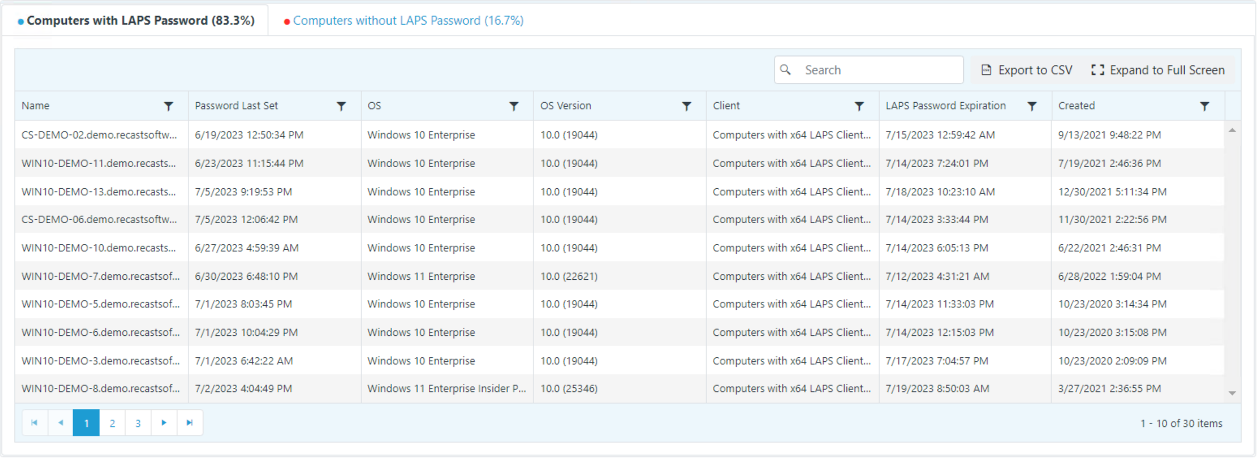




Click on a segment of the chart or legend to view details in the table.

LAPS 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**.


● Computers with LAPS Password (83.3%)
● Computers without LAPS Password (16.7%)
Search
Export to CSV
Expand to Full Screen
1
2
3

Name	Password Last Set	OS	OS Version	Client	LAPS Password Expiration	Created
CS-DEMO-02.demo.recastsoftw...	6/19/2023 12:50:34 PM	Windows 10 Enterprise	10.0 (19044)	Computers with x64 LAPS Client...	7/15/2023 12:59:42 AM	9/13/2021 9:48:22 PM
WIN10-DEMO-11.demo.recasts...	6/23/2023 11:15:44 PM	Windows 10 Enterprise	10.0 (19044)	Computers with x64 LAPS Client...	7/14/2023 7:24:01 PM	7/19/2021 2:46:36 PM
WIN10-DEMO-13.demo.recasts...	7/5/2023 9:19:53 PM	Windows 10 Enterprise	10.0 (19044)	Computers with x64 LAPS Client...	7/18/2023 10:23:10 AM	12/30/2021 5:11:34 PM
CS-DEMO-06.demo.recastsoftw...	7/5/2023 12:06:42 PM	Windows 10 Enterprise	10.0 (19044)	Computers with x64 LAPS Client...	7/14/2023 3:33:44 PM	11/30/2021 2:22:56 PM
WIN10-DEMO-10.demo.recasts...	6/27/2023 4:59:39 AM	Windows 10 Enterprise	10.0 (19044)	Computers with x64 LAPS Client...	7/14/2023 6:05:13 PM	6/22/2021 2:46:31 PM
WIN10-DEMO-7.demo.recastsof...	6/30/2023 6:48:10 PM	Windows 11 Enterprise	10.0 (22621)	Computers with x64 LAPS Client...	7/12/2023 4:31:21 AM	6/28/2022 1:59:04 PM
WIN10-DEMO-5.demo.recastsof...	7/1/2023 8:03:45 PM	Windows 10 Enterprise	10.0 (19044)	Computers with x64 LAPS Client...	7/14/2023 11:33:03 PM	10/23/2020 3:14:34 PM
WIN10-DEMO-6.demo.recastsof...	7/1/2023 10:04:29 PM	Windows 10 Enterprise	10.0 (19044)	Computers with x64 LAPS Client...	7/14/2023 12:15:03 PM	10/23/2020 3:15:08 PM
WIN10-DEMO-3.demo.recastsof...	7/1/2023 6:42:22 AM	Windows 10 Enterprise	10.0 (19044)	Computers with x64 LAPS Client...	7/17/2023 7:04:57 PM	10/23/2020 2:09:09 PM
WIN10-DEMO-8.demo.recastsof...	7/2/2023 4:04:49 PM	Windows 11 Enterprise Insider P...	10.0 (25346)	Computers with x64 LAPS Client...	7/19/2023 8:50:03 AM	3/27/2021 2:36:55 PM

1 - 10 of 30 items

Microsoft Permissions for the Proxy Service Account

- Requires read rights to Active Directory OUs and their computer objects contained within for the specific domain.
- **LAPS Password in AD**: Requires permissions to read the LAPS password attribute.
- **LAPS Client Install State**: Requires permissions to device hardware inventory.

Software Updates Web Dashboard

The **Software Updates Web Dashboard** displays update compliance in your environment.

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:

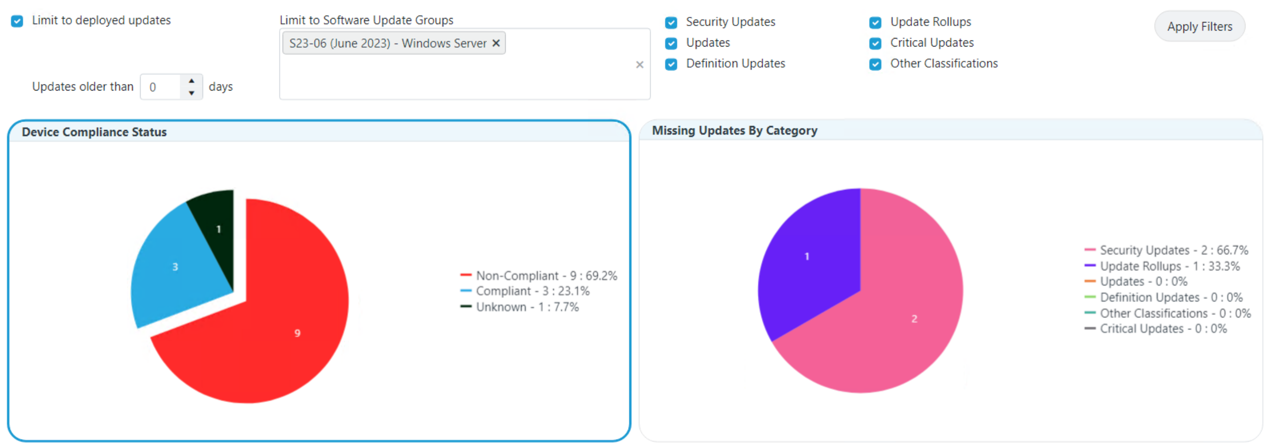
After a scan runs, click **Create Snapshot**.

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.



☑ Limit to deployed updates

Updates older than 0 days

Limit to Software Update Groups: S23-06 (June 2023) - Windows Server

☑ Security Updates
☑ Updates
☑ Definition Updates
☑ Update Rollups
☑ Critical Updates
☑ Other Classifications

Apply Filters
Device Compliance Status
9
3
1
Non-Compliant - 9 : 69.2%
Compliant - 3 : 23.1%
Unknown - 1 : 7.7%
Missing Updates By Category
2
1
Security Updates - 2 : 66.7%
Update Rollups - 1 : 33.3%
Updates - 0 : 0%
Definition Updates - 0 : 0%
Other Classifications - 0 : 0%
Critical Updates - 0 : 0%

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.

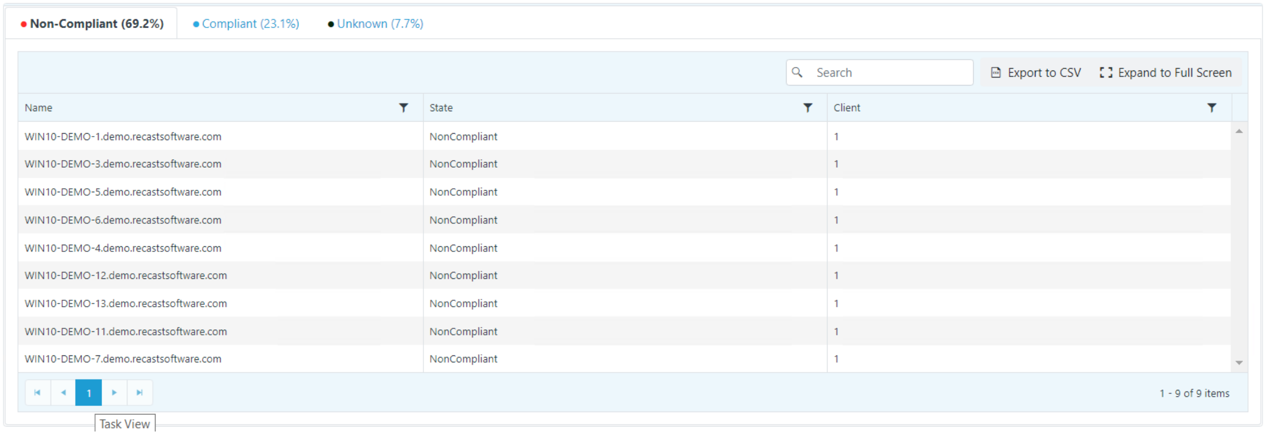
If **Limit to deployed updates** is enabled, both the installed updates and missing updates will include only those that have been deployed. If no known updates have been deployed, no updates will be in either list, resulting in all devices being displayed as 'Unknown'.

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**.



Name	State	Client
WIN10-DEMO-1.demo.recastsoftware.com	NonCompliant	1
WIN10-DEMO-3.demo.recastsoftware.com	NonCompliant	1
WIN10-DEMO-5.demo.recastsoftware.com	NonCompliant	1
WIN10-DEMO-6.demo.recastsoftware.com	NonCompliant	1
WIN10-DEMO-4.demo.recastsoftware.com	NonCompliant	1
WIN10-DEMO-12.demo.recastsoftware.com	NonCompliant	1
WIN10-DEMO-13.demo.recastsoftware.com	NonCompliant	1
WIN10-DEMO-11.demo.recastsoftware.com	NonCompliant	1
WIN10-DEMO-7.demo.recastsoftware.com	NonCompliant	1

1 - 9 of 9 items