

28th January 2026

Release Update

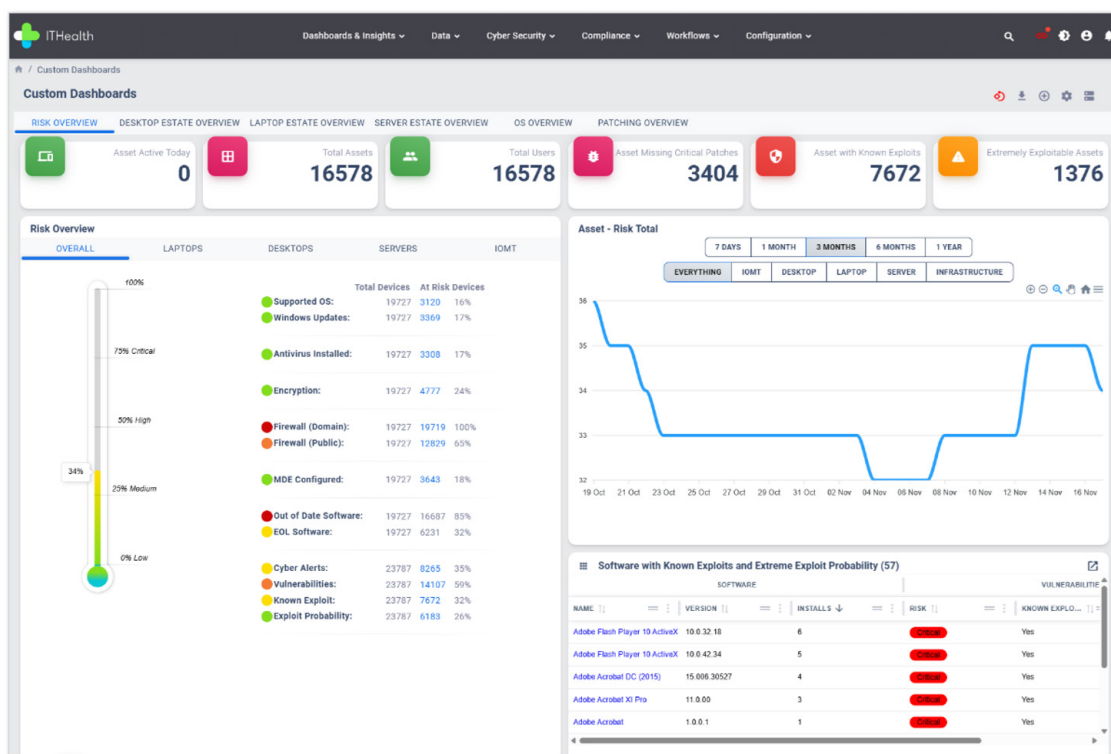
ITHealth Dashboard - Version 2.19.0.0

New and Improved

Custom Dashboards (ISR-30)

Where to find it: *Dashboards & Insights > Custom Dashboards*

Users can now build [fully customisable dashboards](#) by selecting from a library of configurable widgets, enabling tailored views for specific operational, security, or compliance use cases.

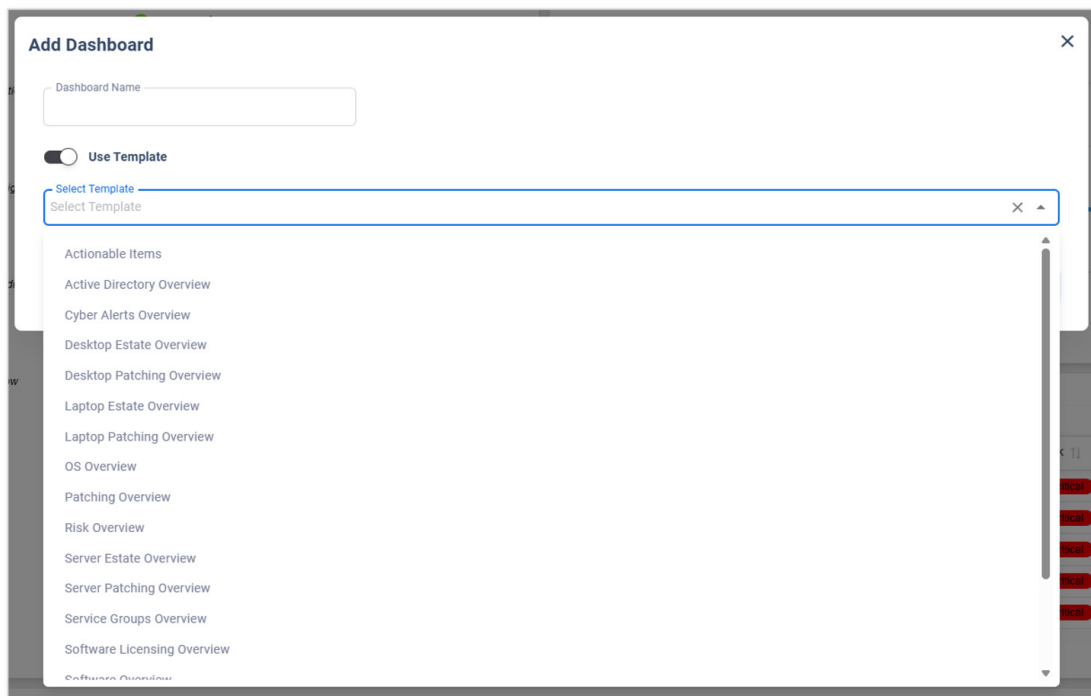
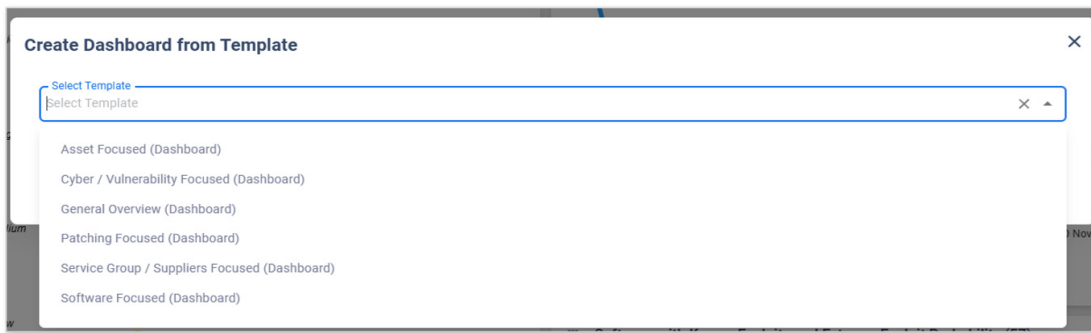


When creating a custom dashboard, users can:

- ▶ **Build from scratch:** Select individual widgets to design a fully custom layout.

OR

- ▶ **Start from a template:** Begin with a pre-defined layout, providing a quick starting point for common dashboard options.



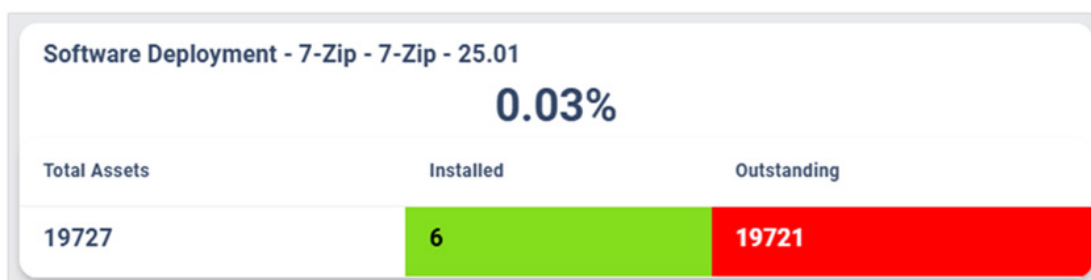
Available widgets include:

- ▶ **Tables:** Software Tracking, Data Tables, Counters, and Free Text
- ▶ **Charts:** KPI Trending, Software Trending, and Data Charts
- ▶ **Pre-Built Widgets:** Risk Thermometers, Patching Charts, and Windows Support indicators

Each widget supports filtering by device type, service group, department, and asset group.

New software widgets

[Software Tracking](#) and [Software Trending](#) widgets add new functionality to the ITHealth Dashboard by allowing software installations and removals to be tracked in real-time.





Dashboards are user-specific but can be shared via the [Manage Dashboard Tabs](#) administration.

Alerts and Notifications (ISR-25)

Where to find it: *Profile > Notifications*

Users can now configure [personalised alerts and notifications](#), giving greater control over which events trigger notifications across the platform.

Notifications
Choose how you receive notifications.

Settings

- In-App Notifications (Enabled by Default)
- Email Notifications
- Browser Notifications

Email Cadence: Immediate

SAVE SETTINGS

Notification Subscriptions
Choose which notifications you receive.

- Cyber Alerts Preset
- + New Updated
- Tracked Change

Tracking: 2 ⚙️

- Assets Preset
- Tracked Change

Tracking: 2 ⚙️

Notifications can be configured as [In-App \(enabled by default\)](#), [Email](#), or [Browser](#).

Users can also set the [email cadence](#) to control how frequently notifications are sent.

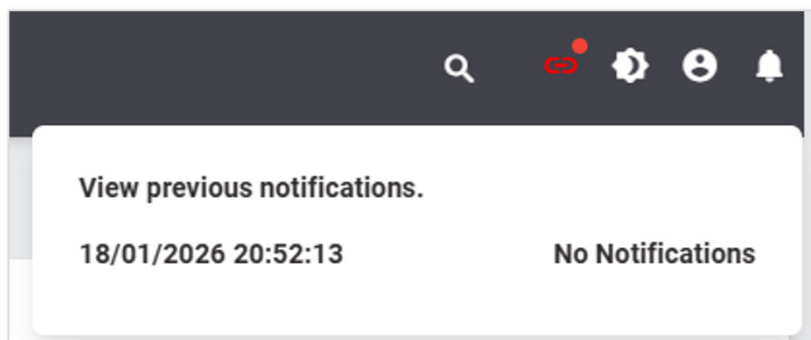
Notifications can be enabled or disabled for different system areas. Within each area, users can refine notifications by specific event types, such as:

- ▶ New, updated, or deleted records
- ▶ Tracked changes

For areas with [Tracked Changes](#) notifications, users can track specific items, such as assets not seen or cyber alert detection changes. These notifications can be enabled when you see the [notification bell icon](#).

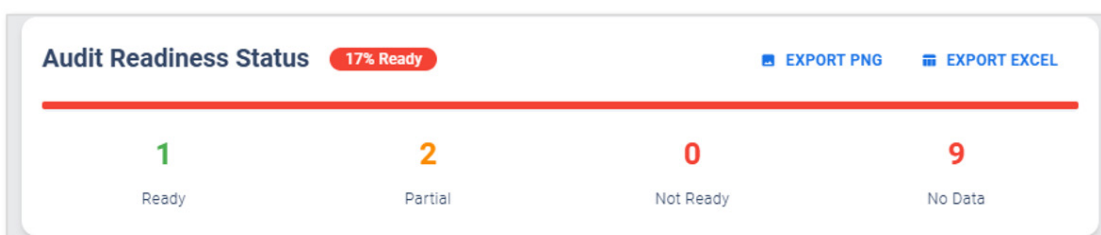


Current and previous notifications can be viewed via the notification bell.



CAF-DSPT Module Enhancements

- ▶ (IFR-324, IFR-286) – You can now [bulk export all CAF documents, including the document map](#) from the Document Library. (CAF-DSPT Submission > Document Library)
- ▶ (IFR-252) – The [CAF Audit View can now be exported](#) as a PNG (Dashboard View) or as an Excel spreadsheet, including a breakdown of responses and supporting evidence in separate tabs. (CAF-DSPT Submission > Audit View)



- ▶ (IFR-284) – Documents in the Document Library can now have [an expiry date](#), helping identify documents that require regular renewal. (CAF-DSPT Submission > Document Library)
- ▶ (IFR-287) – The Document Library now [prevents duplicate document uploads](#) and highlights existing duplicates. (CAF-DSPT Submission > Document Library)
- ▶ (IFR-314) – A new [Review option](#) has been added to Outcomes for items marked as “Uploaded for Baseline” (CAF-DSPT Submission > Outcomes)
- ▶ (IFR-285) – [All Assigned Indicators are now displayed by default](#) (CAF-DSPT Submission > Assigned Indicators)
- ▶ (IFR-332) – [Documents can now be deleted directly from the Document Library](#), with Outcomes updated automatically (CAF-DSPT Submission > Document Library)

- ▶ (IFR-336) – The CAF-DSPT Matrix can now be filtered to show [Auditable items only](#) (*CAF-DSPT Submission > Matrix Overview*)
- ▶ (IFR-285) – The [Assigned Owner](#) is now displayed more clearly within an Outcome (*CAF-DSPT Submission > Outcomes*)

Asset Module Enhancements

- ▶ (IFR-172) – ‘[Bulk add](#)’ and [edit functionality](#) for asset environment and priority is now available. (*Data > Any Asset Table*)
- ▶ (IFR-185) – [Manually created assets can now be edited](#) (*Data > Any Asset Table*)
- ▶ (IFR-198) – [Manual assets can now be bulk imported](#) via the Manual Asset Creation dialog (template provided) (*Data > Any Asset Table*)
- ▶ (IFR-280) – Asset Disposal imports now support adding a [URL link to a Destruction Certificate](#) (*Data > Asset Disposal*)
- ▶ (IFR-262) – [MAC address](#) has been added to the asset details (*Data > Any Asset Table*)
- ▶ (IFR-66) – [Comments](#) can now be added to an Asset (*Asset Details*)
- ▶ (IFR-309) – A manual [Primary User](#) field has been added for assets and software (*Asset Details*)

Service Groups Enhancements

- ▶ (IFR-295) – Service Group linked assets now show if they are [legacy](#) (*Service Group Details*)
- ▶ (IFR-301) – A checkbox has been added for “[Essential Function](#)” (*Service Group*)

The following additional fields have been added:

- ▶ Review Date per Section
- ▶ Recovery Point (BCMP and Disaster Recovery)
- ▶ SaaS Usage (System Identification)
- ▶ Geographical Location (System Identification)
- ▶ Paper or Electronic Format (Data Controls / System Usage)
- ▶ Data Retention Period (Data Controls / System Usage)
- ▶ Staff Data (Data Controls / System Usage)
- ▶ Common Law Duty of Confidentiality (Data Controls / System Usage)

Supplier Module Enhancements

The following additional fields have been added:

- ▶ Certification checks for:
 - IEC 81001-5-1
 - DCB0129 (required clinical risk standard)
 - DCB0160 (risk officer for implementation record)
- ▶ Alternative Addresses (For international organisations)

New Integrations

- ▶ [ManageEngine Endpoint Central](#) – Support for additional asset information and blind spot visibility
- ▶ [ControlUp](#) – Support for additional asset information and blind spot visibility
- ▶ [Trend Deep Security \(On-Prem\)](#) – Support for additional asset information and blind spot visibility