Ordivis

MODUL · REPORTING

Modul Reporting & Dashboards

Rollenbasierte Dashboards, Berichte, Zeitpläne und Audit-Log

Produktversion 2026.08.19 · Handbuch-Revision 1.0
Stand 19.08.2026 · Plattform .NET 10 / Windows Server

ID-27 Reporting

Modul Reporting & Dashboards

Die eigentliche Arbeit passiert in den einzelnen Modulen: Tickets werden bearbeitet, CIs gepflegt, Verträge verwaltet. Wer das Ganze steuern will, braucht aber den Überblick darüber – wie viele Tickets offen sind, ob die vereinbarten Zeiten eingehalten werden, welche Verträge bald auslaufen. Diese Zahlen aus jedem Modul einzeln zusammenzusuchen, ist mühsam und immer nur eine Momentaufnahme.

Reporting bündelt genau diese Auswertungen an einer Stelle. Ein *Dashboard* ist eine Übersichtsseite, die die wichtigsten Kennzahlen laufend und auf einen Blick zeigt, zugeschnitten auf die jeweilige Rolle. Ein *Bericht* ist eine ausführlichere Auswertung, die Sie filtern und als Datei (Excel, CSV oder PDF) exportieren können, etwa um sie in einer Besprechung zu zeigen. Berichte lassen sich auch zeitgesteuert erzeugen und automatisch per E-Mail verschicken.

INHALT

1 Rollenbasierte Dashboards

Jeder Bereich beginnt mit seinem Dashboard – es steht überall an erster Stelle im Menü. Der Aufbau ist in allen Bereichen derselbe: oben eine Leiste mit den wichtigsten Kennzahlen, darunter Diagramme (Verläufe und Verteilungen), darunter die **Arbeitslisten** (überfällige und neue Tickets, Prioritätsverteilung). Ein Klick auf eine Kennzahl öffnet die passende **gefilterte** Liste – „SLA verletzt" etwa genau die betroffenen Tickets, „Offen" alle offenen. Die Listen sind als kompakte Tabellen mit Spaltenüberschrift dargestellt; ein Klick auf eine Zeile öffnet den Datensatz.

Dashboard	Inhalt
Start	Eigene offene/neue Tickets, überfällige und zugewiesene Vorgänge, Aufgaben und ausstehende Changes; darunter je eine Zeile pro Bereich

Dashboard	Inhalt
Service Desk	Kennzahlen (SLA-Erfüllung, mittlere Lösungszeit, Zufriedenheit, Durchsatz, Backlog nach Alter, Agentenlast, CSAT) **und** die Arbeitslisten: überfällige/neue Tickets, Prioritätsverteilung
CMDB	CI-Bestand, Lebenszyklus-Verteilung, zuletzt geänderte CIs, Zugänge in Staging
IPAM	Netze, vergebene Adressen, Auslastung je Netz, Adresskonflikte
Informationssicherheit	Zielobjekte, offene Maßnahmen, Schutzbedarf- und Risikoverteilung, Fortschritt des Grundschutz-Checks

Der Auswertungszeitraum lässt sich auf 7, 30 oder 90 Tage stellen.

1.1 Wie die SLA-Erfüllung gerechnet wird

Beide SLA-Kennzahlen zählen ausschließlich Vorgänge, für die es überhaupt eine Frist gibt, und sie zählen dasselbe: **Wie viele davon wurden innerhalb ihrer Frist fertig?**

- **Lösung:** Anteil der gelösten oder geschlossenen Vorgänge, deren **Lösungsfrist** nicht überschritten wurde.
- **Reaktion:** Anteil der Vorgänge mit **Reaktionsfrist** und erfolgter erster Antwort, bei denen diese Frist gehalten wurde.

Maßgeblich ist allein die Frist. Insbesondere gilt:

- Ob ein Vorgang **eskaliert** wurde, spielt für die Kennzahl keine Rolle. Eine von Hand ausgelöste Eskalation oder ein erklärter **Major Incident** sind Handlungen der Bearbeitung, keine Fristverletzung – ein so behandelter, aber pünktlich gelöster Vorgang zählt als eingehalten.
- Umgekehrt zählt eine überschrittene Frist auch dann als Verfehlung, wenn wegen der eingestellten **Wartezeiten der Eskalationsstufen** noch niemand benachrichtigt wurde.
- Verstreicht eine Frist während eines laufenden **Wartungsfensters**, gilt sie nicht als verletzt – ein geplanter Ausfall ist kein Versäumnis.

> **Hinweis zu älteren Auswertungen:** Bis Juli 2026 wurde die Lösungs-Kennzahl ersatzweise an der Eskalationsstufe gemessen und war dadurch in beide Richtungen ungenau. Mit der Umstellung wurden die vorhandenen Vorgänge und die gespeicherte Verlaufshistorie **einmalig nachgerechnet**. Zahlen aus Berichten, die vor der Umstellung erstellt wurden, können deshalb von den heutigen abweichen. Für Zeiträume vor der Umstellung ließen sich damalige Wartungsfenster nicht rekonstruieren; die Nachrechnung ist dort im Zweifel strenger und beschönigt nichts.

1.2 Was die Kachel „SLA verletzt" zählt

Die Kachel ist keine Quote, sondern eine Arbeitsmenge: **offene Vorgänge, deren Lösungsfrist der Prüflauf als gerissen festgehalten hat.** Ein Klick darauf öffnet genau diese Liste, und dieselben Vorgänge sind auch in der Ticketliste rot markiert – Kachel, Liste und Markierung meinen dasselbe.

Maßgeblich ist die Feststellung des Prüflaufs, nicht die bloße Uhrzeit. Daraus folgt:

- In den **Warte-Zuständen** („Warte auf Melder", „Warte auf Dienstleister", „Blockiert") ruht die SLA-Uhr. Dort wird keine Verletzung festgestellt, und beim Verlassen des Warte-Zustands wandert die Frist um die Wartedauer nach hinten. Eine **von Hand gesetzte Fälligkeit** wandert nicht mit – sie ist eine Zusage des Bearbeiters und soll halten, was an ihr steht.
- Eine **vor** dem Warten festgestellte Verletzung bleibt bestehen. Der Vorgang zählt weiter mit, solange er offen ist: Die Frist wurde gerissen, das Warten macht das nicht ungeschehen.
- Ein **gelöster oder geschlossener** Vorgang zählt nicht mehr mit, auch wenn seine Frist längst in der Vergangenheit liegt. War er bei der Bearbeitung verletzt, erscheint das in der SLA-Erfüllung (1.1) – die Kachel fordert zum Handeln auf und meint deshalb nur, was noch offen ist.
- Ein laufendes **Wartungsfenster** verhindert die Feststellung; ein geplanter Ausfall ist kein Versäumnis.

Der Prüflauf arbeitet im Minutentakt. Eine gerade eben abgelaufene Frist erscheint deshalb mit bis zu einer Minute Verzögerung.

Die Verlaufsdiagramme stützen sich auf tägliche Kennzahl-Schnappschüsse. Nach einer Neuinstallation entsteht diese Historie erst mit der Zeit; solange zu wenige Tage vorliegen, weist das Diagramm darauf hin, statt eine Linie aus einem einzigen Punkt zu zeichnen.

Die Auswertungskarten setzen das Recht `reporting.read` voraus. Fehlt es, blendet das Dashboard sie aus und zeigt nur die Kennzahlen, die der Benutzer ohnehin sehen darf.

Das **persönliche Dashboard** nach dem Login (Menüpunkt „Start") zeigt zusätzlich Ihre eigenen Tickets, Aufgaben, Wiedervorlagen und Genehmigungen.

2 Berichte (Report-Verwaltung)

> 💻 **Client:** *Compliance & Reporting* ▸ *Report-Verwaltung* · 🌐 **Portal:** *Compliance & Reporting* ▸ *Berichte* und *Bericht-Baukasten* · 🔑 `reporting.read` zum Lesen, `reporting.manage` zum Anlegen und Ändern

🔒 **Pflichtreihenfolge** — Spalten, Filter und Sortierung wirken auf die gewählte **Datenquelle**. Wird sie nachträglich gewechselt, ist die Zusammenstellung hinfällig.

1. Öffnen Sie die Report-Verwaltung (im Portal den *Bericht-Baukasten*).
2. Legen Sie eine **Report-Definition** an und wählen Sie die Datenquelle – optional mit eigenem SQL (ID-27a).
3. Wählen Sie **Spalten, Filter und Sortierung**.
4. Prüfen Sie das Ergebnis in der **Vorschau**, bevor Sie speichern.
5. **Exportieren** Sie als **Xlsx**, **CSV** oder **PDF**.

✅ **Ergebnis:** Der Bericht steht in der Liste und lässt sich jederzeit erneut ausführen – und zeitgesteuert versenden (Abschnitt 3).

Sie fangen nicht bei null an. Ordivis Platform bringt eine Bibliothek gebrauchsfertiger Berichte über alle Module mit – Vorgänge und Fristen, Gerätebestand, Lizenzen und Verträge, Informationssicherheit,

Datenschutz, Organisation. Sie stehen nach der Einrichtung ohne Zutun in der Liste und lassen sich wie eigene Berichte anpassen oder als Vorlage kopieren.

> **Hinweis zu Anlagen, die vor 2026.08.02 eingerichtet wurden.** Bis zu dieser Fassung landeten diese Berichte durch einen Fehler in der falschen Datenbank und fehlten deshalb in Ihrer Liste – auch die Checklisten-Vorlagen, der Gefährdungskatalog, der ISO-27001-Katalog, der Datenschutz-Grundkatalog und die Muster-Aufbauorganisation waren davon betroffen. Mit dem Update werden sie beim nächsten Start nachgetragen. Berichte, die Sie **selbst gelöscht** haben, kommen dabei nicht zurück.

3 Geplante Berichte

Berichte lassen sich **zeitgesteuert** ausführen (Cron) und automatisch an **E-Mail-Empfänger** versenden – z. B. ein wöchentlicher SLA-Bericht an die Leitung.

4 Tabellen-Funktionen (überall)

Alle Tabellen in Ordivis Platform sind voll ausgestattet: **filtern, sortieren, Spalten anpassen, Spaltenauswahl** sowie **CSV-/PDF-Export**. Sie arbeiten also überall gleich.

5 Audit-Log

> 💻 **Client:** *Compliance & Reporting* ▸ *Audit-Log* · 🌐 **Portal:** *Compliance & Reporting* ▸ *Audit-Log* · 🔑 `audit.read`, für die Ausgabe zusätzlich `audit.export`

Das **Audit-Log** zeigt revisionssicher sicherheitsrelevante Aktionen mit Filter (Entitätstyp, Zeitraum) und Paginierung.

So finden Sie einen bestimmten Vorgang:

💡 **Empfohlene Reihenfolge** — grenzen Sie zuerst den Zeitraum ein, dann den Entitätstyp. Anders herum blättern Sie durch Tausende Einträge, bevor der Filter greift.

1. Öffnen Sie das Audit-Log.
2. Setzen Sie den **Zeitraum** möglichst eng.
3. Wählen Sie den **Entitätstyp** (z. B. Benutzer, Ticket, CI).
4. Blättern Sie durch das Ergebnis.

✅ **Ergebnis:** Sie sehen, wer wann was geändert hat – nachweisbar und ohne Lücke.

> **Wichtig:** Der Zugriff erfordert `audit.read`, die **Ausgabe als CSV** zusätzlich `audit.export`. Lesen und Herausgeben sind bewusst getrennt: Eine ausgegebene Datei verlässt das System. Einzelheiten zum Export (Filter, Vollständigkeitsangabe, Obergrenze) stehen im Administrationshandbuch.

6 Wallboard (Anzeigegeräte)

Das **Ordivis Wallboard** ist ein eigenes Vollbild-Programm für Bildschirme, die unbeaufsichtigt laufen – im Service-Desk-Büro, am Empfang, im Leitstand. Es zeigt im Wechsel große Kennzahlen und ist bewusst kein zweites Fenster des Arbeitsplatz-Programms: Es braucht keine Anmeldung durch einen Menschen, startet nach einem Stromausfall von allein wieder und lässt sich nicht bedienen wie ein Arbeitsplatz.

6.1 Installieren

Das Wallboard ist eine **abwählbare Komponente des Installers**: „Wallboard (Vollbild-Dashboards für Anzeigegeräte)". Sie ist keinem Installationstyp zugeordnet und muss bewusst angehakt werden – auf einem gewöhnlichen Arbeitsplatz wird sie also nicht mitinstalliert. Nach der Installation liegt eine Verknüpfung **Ordivis Wallboard** im Startmenü.

6.2 Einrichten

Beim ersten Start erscheint die Einrichtung (später jederzeit mit **Esc** erreichbar):

- **Serveradresse** – z. B. `https://server.firma.local:5001`. Mit **Verbindung testen** prüfen. Für interne Netze ohne eigene PKI lässt sich die Zertifikatsprüfung abschalten; verwenden Sie das nur dort.
- **Wallboard-Token** – wird vorher im Arbeitsplatz-Programm ausgestellt (siehe Betriebshandbuch, **7.4.2 Anzeigegeräte**). Er ersetzt Benutzername und Kennwort.
- **Dashboards** – Auswahl und Reihenfolge. Angehakte Dashboards laufen von oben nach unten durch: **Service Desk**, **CMDB**, **IP-Verwaltung**.
- **Takt** – wie viele Sekunden ein Dashboard stehen bleibt und wie oft die Zahlen neu geholt werden.
- **Darstellung** – dunkles Erscheinungsbild sowie, wie der Mandant oben links erscheint (Logo und Name, nur Name, nur Logo). Ist im Mandanten ein Logo hinterlegt, rückt die Ordivis-Marke klein nach unten rechts.
- **Im Vollbild öffnen auf** – der Bildschirm, auf dem das Wallboard aufgeht. An einem Anzeigegerät hängen oft zwei Schirme, einer an der Wand und einer am Arbeitsplatz; ohne diese Angabe öffnet das Wallboard dort, wo Windows das Fenster platziert. Ist der gewählte Bildschirm nicht angeschlossen, bleibt es beim aktuellen — auf einen Bildschirm zu springen, den es nicht gibt, hieße, das Fenster ins Nichts zu schieben.
- **Beim Anmelden dieses Windows-Kontos automatisch starten** – trägt das Wallboard für den angemeldeten Benutzer ein (kein Eingriff in Dienste oder Gruppenrichtlinien).
- **Nach einem unerwarteten Fehler weiterlaufen** – empfohlen für Schirme im Dauerbetrieb (Vorgabe: an). Der Fehler wird protokolliert, das Bild zeichnet sich beim nächsten Takt neu. Zum Einrichten eines neuen Anzeigegeräts kann es hilfreich sein, dies abzuschalten.

6.2.1 Dauerbetrieb: Was einen Schirm über Nacht abschaltet

Ein Wandschirm hat niemanden davor, der auf „Wiederholen" klickt. Drei Dinge greifen deshalb ineinander:

Vorkehrung	Wirkung
Weiterlaufen nach Fehler	Ein Fehler in der Oberfläche beendet den Schirm nicht mehr, sondern landet im Protokoll.
Lebenszeichen	Alle 15 Minuten hält das Protokoll fest, dass der Schirm läuft.
Geordnetes Ende	Wird der Schirm geschlossen, steht das ausdrücklich im Protokoll.

Das Lebenszeichen ist der Schlüssel zur Fehlersuche: Steht die letzte Zeile um 03:12 und fehlt der Vermerk über das geordnete Ende, wurde der Schirm um diese Zeit **abgebrochen** — und die Uhrzeit sagt meist schon, wodurch. Das Protokoll liegt unter `%ProgramData%\InfraDesk\Logs\wallboard-JJJJMMTT.log`.

⚠️ **Der häufigste Grund ist kein Fehler des Programms.** Der automatische Start hängt an der **Anmeldung** dieses Windows-Kontos — das ist nötig, weil der Token an dieses Konto gebunden ist (DPAPI, siehe Betriebshandbuch). Startet Windows nachts wegen Updates neu, steht der Rechner am Anmeldebildschirm, und der Schirm bleibt bis zur nächsten Anmeldung dunkel. Für den Dauerbetrieb empfiehlt sich eine **automatische Anmeldung** des Anzeigekontos.

6.3 Im Betrieb

Taste	Wirkung
Esc	Einstellungen öffnen
Leertaste	Wechsel anhalten / fortsetzen
Pfeiltasten	ein Dashboard vor / zurück
F5	Zahlen sofort neu holen

Wartet mindestens ein **neues Ticket**, blendet die zugehörige Kachel ruhig auf und ab – auffällig genug, um über den Raum bemerkt zu werden, ohne zu blinken.

Was der Schirm zeigt, bestimmt das Konto hinter dem Token. Ein Wallboard im Flur ist für jeden Vorbeigehenden sichtbar. Binden Sie den Token deshalb an ein eigenes Konto mit ausschließlich lesenden Rechten, nicht an ein persönliches.

7 Rollen & Rechte (Auszug)

Recht	Erlaubt
`reporting.read`	Berichte und Dashboards ansehen
`reporting.create`	Eigene Berichte erstellen
`reporting.manage`	Alle Berichte und Zeitpläne verwalten

Recht	Erlaubt
`reporting.dashboard.manage`	Dashboard-Widgets konfigurieren
`audit.read` / `audit.export`	Audit-Log ansehen / exportieren
`system.config.manage`	Wallboard-Token ausstellen und widerrufen

Verwandte Themen

- **ID-27a – Reports & SQL-Abfragen** – eigene Reports bauen und per SQL abfragen
- **ID-52 – Datenbank-Referenz** – Tabellen und Felder für eigene Abfragen
- **ID-44 – Rollen- & Rechte-Matrix** – warum zwei Benutzer verschiedene Zahlen sehen
- **ID-20 – Modul Service Desk / Ticketing** – Herkunft der Service-Desk-Kennzahlen