PULSE

Pulse Dokumentation

Pulse · Mobile App · Appliance

Stand 2026-10-26

docs.pulsehq.de

Inhalt

1 Neuigkeiten

2 Einleitung

2.1 Was ist Pulse?

2.2 Erste Schritte

3 Monitoring

3.1 Dashboard

3.2 Monitore

3.3 CSV-Import

3.4 Gerätesuche

3.5 Assets

3.6 Vorfälle

3.7 Ziele

3.8 Berichte

3.9 Schwachstellen

3.10 KI-Canvas

3.11 Abfrage

4 Monitortypen

4.1 OPC UA

4.2 OPC-UA-Sicherheit

4.3 Siemens S7

4.4 Symbolisches S7 (S7-1200/1500)

4.5 Prometheus

4.6 Heartbeat

4.7 Anomalieerkennung

4.8 Nachrichtenvorlagen

5 Alarmierung

5.1 Eskalationsrichtlinien

5.2 Bereitschaftspläne

5.3 Schweregrade

5.4 Benachrichtigungen

6 Verwaltung

6.1 Mitglieder & Rollen

6.2 Teams

6.3 Tags

6.4 Tag-Kategorien

6.5 Organisationseinstellungen

6.6 Lizenzen

6.7 Einstellungen

7 Referenz

7.1 Markdown

7.2 Fehlerbehebung

7.3 SBOM

8 Mobile-App

8.1 Übersicht

8.2 Einrichtung & Verbindung

8.3 Benachrichtigungen & Einstellungen

9 Appliance

9.1 Übersicht

9.2 Bereitstellungsoptionen

9.3 Installation

9.4 Netzwerk

9.5 TLS-Zertifikate

9.6 SFTP-Zugang

9.7 SSH-Zugang

9.8 TUI-Referenz

9.9 Systemupdates

9.10 Betrieb

10 Collector

10.1 Collector-Status

10.2 Collector-Kopplung

1 Neuigkeiten

Wichtige, für Benutzer sichtbare Änderungen an Pulse — neue Funktionen, Verbesserungen und Fehlerbehebungen, die Ihnen auffallen werden. Die neuesten Änderungen stehen oben. Folgen Sie den Links für die vollständigen Details in der Funktionsdokumentation.

---

26. Oktober 2026

Verbessert

- **S7+-Symbolsuche zeigt Datenbausteinnummern** — Suchergebnisse für S7CommPlus-Quellen zeigen die Bausteinnummer (zum Beispiel „DB4") jetzt neben dem Bausteinnamen, wie es TIA Portal tut – Sie können einen Baustein damit auch über seine Nummer suchen. Siehe S7CommPlus.

Behoben

- **S7+-Datenpunkte hinzufügen warnt, wenn Auswahlen nicht mehr im SPS-Programm vorhanden sind** — Wenn Sie auf Hinzufügen klicken und das SPS-Programm einen oder mehrere der ausgewählten Bausteine nicht mehr enthält (zum Beispiel nach einem Programm-Download), nennt der Dialog jetzt die fehlenden Auswahlen, entfernt sie aus Ihrer Auswahl und fügt nichts hinzu – anstatt stillschweigend nur die auffindbaren Bausteine hinzuzufügen. Siehe S7CommPlus.
- **S7+-Warnung über veralteten Collector wird nach erfolgreichem Wiederholungsversuch ausgeblendet** — Nachdem der Hinweis „Collector zu alt" im S7CommPlus-Symbolbrowser erscheint, verschwindet er jetzt sofort, wenn ein erneuter Versuch einen aktualisierten Collector erreicht. Siehe S7CommPlus.
- **CVE-Scan erkennt mehr Linux-Distributionen und Paket-Ökosysteme** — Der Scanner für Software-Stücklisten ordnet Komponenten von Wolfi, openSUSE, SUSE, TuxCare, Chainguard, Alpaquita, Azure Linux, openEuler und weiteren Distributionen jetzt der richtigen Advisories-Datenbank zu; zuvor konnten nicht erkannte Distributionen stillschweigend falsch zugeordnet werden, was zu fälschlicherweise sauberen Schwachstellenscans führte. Neue Paket-Ökosysteme (Hex, Pub, CRAN, Swift, Julia, opam, Bitnami) werden ebenfalls jetzt erkannt. Siehe Schwachstellen.
- **OPC UA Alarms & Conditions: gleichzeitige Alarmmeldungen verursachen keinen Deadlock mehr** — Eine Race Condition, bei der zwei gleichzeitige Alarmmeldungen an denselben Alarms-&-Conditions-Monitor deadlocken und eine davon stillschweigend verworfen werden konnte, ist jetzt behoben. Siehe OPC UA.

- **Verbindungsleck behoben, das den Datenbankverbindungspool erschöpfen konnte** — Ein fehlgeschlagenes Catalog-Attach während eines Datenexports oder einer Lake-Komprimierung konnte eine verwaiste DuckDB-Verbindung hinterlassen, die Postgres-Verbindungen belegte; genug solcher Fehler konnten den Verbindungspool erschöpfen und einen Neustart des Appliance erfordern. Dies ist jetzt behoben.

---

25. Oktober 2026

Verbessert

- **S7+-Symbolauswahl mit Suche, Gruppen und Zählern** — Der Datenpunkt-Dialog für eine S7CommPlus-Quelle gruppiert Symbole jetzt in Kategorien (Datenbausteine, Eingänge, Ausgänge, Merker, Zeiten, Zähler), zeigt, wie viele Datenpunkte jeder Baustein oder jede Struktur anlegen würde, und ermöglicht die Suche nach Symbolen der SPS per Stichwort; durch Auswahl eines Bausteins oder einer Struktur wird alles Lesbare darunter auf einmal hinzugefügt, mit einer Fortschrittsanzeige bei großen Batches. Siehe S7CommPlus.

---

24. Oktober 2026

Verbessert

- **Asset-Verlauf zeigt jede Änderung als kompakte, aufklappbare Zeile** — Der Verlaufsbereich auf der Detailseite eines Assets zeigt nun jedes Ereignis als kompakte Zeile mit einer einzeiligen Beschreibung der Änderung; durch Klicken auf eine Zeile wird sie aufgeklappt und zeigt alle Details. Standardmäßig werden die fünf neuesten Einträge angezeigt; „Mehr anzeigen" zeigt die weiteren geladenen Einträge, bevor ältere Seiten nachgeladen werden. Siehe Asset-Register.
- **Datenpunktadressen können jetzt kopiert werden** — Auf der Detailseite einer Datenquelle wird die Adresse jedes Datenpunkts unter seinem Namen angezeigt; ein Klick auf die Adresse öffnet ein Popover mit dem vollständigen Text und einer Schaltfläche zum Kopieren in die Zwischenablage – zum Einfügen in ein SPS-Projekt oder einen OPC-UA-Client.
- **Prüfungsliste zeigt jede Prüfung als kompakte, aufklappbare Zeile** — Die Prüfungsseite zeigt nun jede Prüfung als einzelne Zeile mit Datum, Prüfer und Vorschau der Notiz; durch Klicken auf eine Zeile werden der vollständige Erfassungszeitraum, die vollständige Notiz, alle eingefrorenen Dateien und deren SHA-256-Prüfsummen mit Kopierschaltflächen angezeigt. Siehe Asset-Register.

- **Geräteerkennung verfolgt den aktiven Scan über die URL** — Die Scanseite speichert nun den laufenden Scan in der URL, sodass Sie die Seite neu laden oder einen Link teilen und genau zu den Ergebnissen dieses Scans zurückkehren können; wenn beim Öffnen der Seite bereits ein Scan läuft, wird er automatisch angehängt. Siehe Geräteerkennung.
- **Geräteerkennung zeigt einen entfernten Collector deutlich an** — Wenn ein als Scan-Ausgangspunkt gewählter Collector aus dem System entfernt wurde, zeigt das Scan-Formular nun „Collector entfernt" an, anstatt den Start stillschweigend zu blockieren. Siehe Geräteerkennung.
- **Collector-Einstellungen zeigen, wann jeder Collector zuletzt verbunden war** — Die Collector-Tabelle in den Organisationseinstellungen enthält jetzt eine Spalte „Zuletzt verbunden" mit dem Zeitpunkt der letzten Verbindung als relativer Zeitangabe; beim Darüberfahren mit der Maus wird das genaue Datum und die Uhrzeit angezeigt.

---

23. Oktober 2026

Neu

- **Geräteerkennung zeigt, welche Module bereits Datenquellen sind** — Das Geräte-Detailblatt markiert jetzt jedes Modul, das bereits als Datenquelle übernommen wurde, sodass Sie auf einen Blick sehen können, was bereits verbunden ist und was noch konfiguriert werden muss. Siehe Geräteerkennung.

Verbessert

- **S7-Datenquellen stehen unter einem einzigen Seitenleisteneintrag** — Die Seitenleiste zeigte „S7 (klassisch)" und „S7 (symbolisch)" bisher als zwei separate Einträge; sie sind jetzt zu einem einzigen „S7"-Eintrag zusammengefasst, der beide Lesemodi abdeckt, wobei der Modus jeder Quelle als Badge angezeigt wird. Siehe S7.
- **Geräteerkennung zeigt S7CommPlus-Fähigkeit je Gerät** — Das Geräte-Detailblatt zeigt jetzt, ob ein gefundenes Siemens-Gerät über Tag-Namen gelesen werden kann (S7CommPlus), und warnt, wenn der gewählte Collector zu alt ist, um diese Fähigkeit zu prüfen. Siehe Geräteerkennung.
- **Datenquellenzeilen zeigen mehr Qualitätszustände** — Datenpunkt- und Quellenzustandszeilen unterscheiden jetzt „Veraltet" (ein guter Messwert, der nicht rechtzeitig erneuert wurde), „Erreichbar" und „Nicht erreichbar", mit einem Hinweis, der erklärt, was jeder Zustand bedeutet.
- **Symbolisches S7-Zertifikatsfeld zeigt Vergleichsergebnis** — Der Bereich für vertrauenswürdige Zertifikate bei einer S7CommPlus-Quelle zeigt jetzt, ob die SPS dasselbe oder ein anderes Zertifikat präsentiert, mit Statusbadges und einem Schalter

zum Anzeigen beider Fingerabdrücke nebeneinander. Siehe S7CommPlus.

Behoben

- **Vorfälle bei symbolischen S7-Quellen geben konkrete Hinweise bei Zertifikatsablehnungen** — Wenn eine symbolische S7-Quelle keine Verbindung herstellen kann, weil das Zertifikat der SPS noch nicht bestätigt wurde oder weil die SPS jetzt ein anderes Zertifikat präsentiert, nennt die Vorfallsursache jetzt das genaue Problem und verweist auf den erforderlichen Schritt. Siehe S7CommPlus.

---

22. Oktober 2026

Neu

- **Symbolische S7-Datenquelle (S7-1200/1500)** — Ein neuer Datenquellentyp „S7 (symbolisch)" ermöglicht es, eine S7-1200 oder S7-1500 SPS per Tag-Name über das TIA-Protokoll zu verbinden und auszulesen; Datenpunkte können durch Durchsuchen des Symbol-Baums der SPS oder durch manuelle Eingabe eines Symbols hinzugefügt werden, und das Zertifikat der SPS wird vor dem ersten Lesen abgerufen und bestätigt. Siehe S7 (symbolisch).

Verbessert

- **Asset-Register: Filterleiste, Mehrfachauswahl und Sammelaktionen** — Die Stationsliste hat jetzt die standardisierte Filterleiste zum Suchen und Filtern sowie einen Auswahlmodus, mit dem Sie mehrere Assets auswählen und in einem Schritt über eine Aktionsleiste löschen können. Siehe Asset-Register.
- **Exportmenü im Asset-Register an einem Ort zusammengefasst** — Alle Exportoptionen sind jetzt über eine einzelne Export-Schaltfläche im Assets-Header verfügbar, statt auf mehrere Seiten verteilt zu sein. Siehe Asset-Register.
- **Registereinstellungen als Registerkarten gegliedert** — Die Einstellungsseite des Registers gliedert ihre Bereiche jetzt in beschriftete Registerkarten, damit Sie die gewünschte Konfiguration schneller finden. Siehe Asset-Register.
- **Assets-Seitenleiste zeigt Unterseiten direkt an** — Der Bereich „Assets" in der Seitenleiste zeigt jetzt Register, Geräte suchen, Prüfungen und Einstellungen als direkte Navigationselemente, und der Bereich öffnet sich automatisch, wenn Sie sich auf einer seiner Unterseiten befinden.
- **Abfrage auf einen Datenpunkt oder Monitor einschränken** — Wenn Sie auf eine Zeile in den Abfrageergebnissen zeigen, erscheint jetzt die Aktion „Auf diesen Datenpunkt einschränken" bzw. „Auf diesen Monitor einschränken", mit der Sie Diagramm und Übersicht auf eine einzelne Reihe fokussieren können. Siehe Abfrage.

Behoben

- **Suchfeld im Asset-Register bleibt auf Tablet-Breite sichtbar** — Das Suchfeld wurde bei mittleren Bildschirmgrößen abgeschnitten; es hat nun genug Platz. Siehe Asset-Register.
- **„In Abfrage öffnen" von einer Datenquelle zeigt den aktuellen Messwert** — Wenn Sie in der Datenquellenliste auf „In Abfrage öffnen" klicken, wird jetzt der zuletzt aufgezeichnete Wert angezeigt statt des Durchschnitts. Siehe Abfrage.

---

20. Oktober 2026

Neu

- **Abfrageergebnisse können jetzt als Link geteilt werden** — Die Abfrageseite speichert jeden Lauf und gibt ihm eine URL; wer den Link öffnet, sieht das gespeicherte Ergebnis, ohne die Abfrage neu auszuführen. Siehe Abfrage.

Verbessert

- **Geräteerkennung jetzt unter Assets** — Die Seite „Geräte suchen" befindet sich jetzt unter Assets, wo auch die Scanergebnisse gespeichert werden; Administratoren haben in der Asset-Liste jetzt eine direkte Schaltfläche „Geräte suchen", und alte Links leiten automatisch weiter. Siehe Geräteerkennung.
- **OPC UA- und S7-Erstellungsformulare mit Stationsdaten vorbelegen** — Wenn Sie bei einer gefundenen Station auf „Hinzufügen" klicken, öffnet sich das Formular für neue Datenquellen mit Adresse und Name der Station bereits ausgefüllt; bei S7-Quellen werden auch Rack und Slot vorbelegt. Siehe Geräteerkennung.

---

19. Oktober 2026

Neu

- **Zonen im Asset-Register (IEC 62443)** — Die Register-Einstellungen enthalten jetzt einen Bereich „Zonen", in dem Sie IEC 62443-Security-Zonen mit Name, Ziel-Security-Level (SL-T), Safety-Zone-Kennzeichen und Verantwortlichem anlegen können. Stationen können einzeln über die Detailseite oder gemeinsam über die Stationsliste einer Zone zugewiesen werden. Die Liste erhält einen Zonenfilter und eine Zonenspalte. Siehe Asset-Register.
- **Register prüfen und abzeichnen** — Administratoren können das Register jetzt prüfen und auf der neuen Seite „Assets › Prüfungen" abzeichnen: Die Prüfungsseite zeigt alle Änderungen seit der letzten Abzeichnung, alle offenen CVE-Befunde mit ihren Entscheidungen und ein Freitextfeld für eine Notiz. Beim Abzeichnen werden eine Momentaufnahme, das Änderungsprotokoll und der Schwachstellenstatus

eingefroren. Die Assets-Seite zeigt an, wann die nächste Prüfung fällig ist oder seit wann sie überfällig ist. Ein Prüfintervall (3, 6 oder 12 Monate) lässt sich in den Register-Einstellungen konfigurieren. Siehe Asset-Register.

- **Audit-Paket herunterladen** — Jede abgezeichnete Prüfung in der Prüfungsliste enthält eine Schaltfläche „Audit-Paket herunterladen", die die eingefrorene Momentaufnahme, das Änderungsprotokoll, den Schwachstellenstatus, die aktuelle Zonenliste und alle Prüfungen bis zu dieser als ZIP-Datei bündelt. Siehe Asset-Register.
- **Änderungsprotokoll und Schwachstellenstatus exportieren** — Das Menü „Exportieren" der Assets-Seite enthält „Änderungsprotokoll (CSV)…" (alle Änderungen in einem von Ihnen festgelegten Zeitraum) und „Schwachstellenstatus (CSV)" (alle offenen CVE-Befunde). Siehe Asset-Register.
- **Support-Ende von Modulen** — Das Register hält jetzt das Datum fest, an dem der Herstellersupport für ein Modul endet. Stationen mit mindestens einem Modul, dessen Support-Datum bereits überschritten ist, erhalten ein Badge, und die Stationsliste erhält einen Filter „Support beendet". Siehe Asset-Register.
- **Datenquelle oder Datenpunkt direkt auf der Abfrageseite öffnen** — Jede Zeile in der Datenquellenliste hat jetzt eine Aktion „In Abfrage öffnen", die direkt zur Abfrageseite mit vorausgewählter Quelle oder vorausgewähltem Datenpunkt navigiert, sodass kein erneutes Eintippen nötig ist. Siehe Abfrage.

Verbessert

- **Vergleich zeigt frühere Werte und prozentualen Unterschied in der Übersicht** — Wenn Sie ein Zeitfenster mit einem früheren Zeitraum vergleichen, zeigt die Übersichtstabelle unter den Diagrammen jetzt eine Spalte „Vorheriger Wert" und eine Spalte „Δ" mit dem prozentualen Unterschied neben jedem Aggregatwert — grün für einen Anstieg, orange für einen Rückgang. Siehe Abfrage.

Behoben

- **Wartungsfenster mit Endzeit 24:00 können wieder gespeichert werden** — Ein Wartungsfenster, dessen Endzeit auf 24:00 (Tagesende) gestellt war, konnte nicht gespeichert werden; dies ist jetzt behoben. Siehe Asset-Register.
- **CSV-Export des Registers enthält die Kopfzeile in Zeile 1** — Die exportierte CSV-Datei öffnet sich jetzt korrekt in Tabellenkalkulationsprogrammen, mit der Kopfzeile in Zeile 1 wie erwartet. Siehe Asset-Register.
- **Aktivitätsverlauf bei Vorfällen aktualisiert sich sofort nach Bestätigung oder Abschluss** — Das Bestätigen oder Abschließen eines Vorfalls aktualisiert den Aktivitätsverlauf sofort, sodass der neue Eintrag sichtbar ist, ohne die Seite neu laden zu müssen. Siehe Vorfälle.

18. Oktober 2026

Neu

- **Abfrage mit einem früheren Zeitraum vergleichen** — Auf der Abfrageseite können Sie jetzt jedes Zeitfenster mit dem gleichlangen Zeitraum unmittelbar davor vergleichen: Öffnen Sie den Zeitraum-Bereich, wählen Sie einen Vergleichsabstand (vorherige 10 Minuten, 1 Stunde, 7 Tage und mehr) und starten Sie die Abfrage; Diagramme zeigen beide Zeiträume entweder überlagert auf einer gemeinsamen Achse oder nebeneinander, jeweils auf eigener Achse. Nur Abstände, die mindestens so lang wie das aktuelle Zeitfenster sind, werden angeboten, sodass sich die Zeiträume nie überschneiden. Siehe Abfrage.

Verbessert

- **Datenpunktnamen im Abfrage-Picker angezeigt** — Der Datenpunkt-Picker auf der Abfrageseite zeigt jetzt den lesbaren Namen jedes Datenpunkts (das von Ihnen vergebene Label oder den eigenen Browse-Namen des Protokolls) über der Adresse an; das Suchfeld trifft auf Namen, Browse-Namen und Adresse. Siehe Abfrage.
- **Bedingungssensordiagramme zeigen jetzt eine Legende** — Wenn ein Sensordiagramm in der Bedingungsmonitor-Vorschau eine gleitende Aggregation über den Messwert oder den gelernten Normalbereich zeichnet, benennt eine kleine Legende unterhalb des Diagramms jede Linie, damit der Unterschied beschriftet und nicht erraten werden muss. Siehe Monitore.
- **⌘↵ führt eine Abfrage von überall auf der Seite aus** — Cmd+Eingabe (oder Strg+Eingabe unter Windows/Linux) führt die Abfrage jetzt von jedem fokussierten Element auf der Abfrageseite aus — auch wenn ein Datenpunkt- oder Aggregations-Picker geöffnet ist — sodass das Tastaturkürzel überall auf der Seite funktioniert. Siehe Abfrage.

17. Oktober 2026

Verbessert

- **Diagrammkarten im KI-Canvas sagen in Worten, was sie messen** — Überschrift, Legende und Übersicht einer Diagrammkarte lauten jetzt „Maximum“, „Mittelwert“ oder „95. Perzentil“ statt der Abfrageschreibweise wie `max(value)`. Die Abfrageseite behält die Schreibweise. Siehe KI-Canvas.
- **KI-Canvas durchgehend in Ihrer Sprache** — Der Seitentitel, die Werkzeugzeilen im Gespräch (jetzt nach dem benannt, was sie getan haben, etwa „Datenabfrage“, mit dem eigenen Namen des Werkzeugs beim Darüberfahren) und der Monitortyp auf einer Monitorkarte folgen der Sprache der App. Außerdem ist der Assistent

angewiesen, einen Status in der Sprache zu erklären, in der Sie schreiben, statt die englischen Werte des Werkzeugs wie „healthy“ oder „unmonitored“ zu zitieren. Siehe KI-Canvas.

- **KI-Assistenten lesen Ihre Datenpunktbeschreibungen** — Die Beschreibung, die Sie einem Datenpunkt unter **Datenpunkt benennen** geben, erreicht jetzt den KI-Canvas und MCP-Clients, wie bisher schon sein Name. Eine Einheit, eine Skalierung oder die Bedeutung der Codes eines Zustandsworts (etwa „0 Stillstand, 1 Fahren“) wird so gelesen, wie Sie sie geschrieben haben, statt erraten. Siehe Verbundene MCP-Clients.

Behoben

- **Offene Vorfälle fehlen nicht mehr in der Vorfallliste** — Bei einem Schnellzeitraum wie **Letzte 8 Stunden** fehlte ein Vorfall, der vor dem Zeitraum begonnen hatte und noch offen war, in der Liste, während die Seitenleiste ihn mitzählte. Offene Vorfälle werden bei einem Schnellzeitraum jetzt immer angezeigt, sodass Liste und Seitenleiste übereinstimmen. Ein benutzerdefinierter Zeitraum zeigt weiterhin nur Vorfälle, die in ihm begonnen haben. Siehe Vorfälle.
- **Datenabfragen nach Datenquellennamen finden jede genannte Quelle** — Eine Abfrage, die ihre Datenquellen beim Namen nannte, fand nur die, die in der Liste Ihrer Organisation zuerst kamen, sodass der KI-Assistent, ein MCP-Client oder ein API-Aufruf für eine Maschine keine Daten bekam oder die einer anderen. Jetzt wird jede genannte Quelle gefunden. Siehe KI-Canvas.
- **KI-Canvas bleibt bei langen Antworten nicht mehr hängen** — Brauchte der Assistent länger als 30 Sekunden für eine Antwort, meist für seine abschließende, ging sie verloren, und der Lauf zeigte dauerhaft „Der Assistent arbeitet…“. Lange Antworten kommen jetzt an. Ein Schritt, der innerhalb von 10 Minuten trotzdem keine Antwort bekommt, beendet den Lauf als „Ausführung fehlgeschlagen“ mit dem Grund, und ein Abfrageergebnis, das zu groß ist, um es ganz zu lesen, erreicht den Assistenten als ein Wert je Reihe, über den ganzen Zeitraum aggregiert, während das Board die Werte selbst zeichnet, bis zu den jüngsten 5.000 je Karte. Siehe KI-Canvas.

---

16. Oktober 2026

Neu

- **Stationsverlauf wird seitenweise geladen** — Der Verlauf auf der Stationsdetailseite lädt jetzt jeweils 20 Einträge; die Schaltfläche „Mehr anzeigen" lädt die nächste Seite nach, sodass Stationen mit langem Verlauf deutlich schneller geöffnet werden. Siehe Asset-Register.

- **Canvas-Diagrammkarten zeigen jetzt eine Reihenlegende** — Das Diagramm-Tab einer Canvas-Karte listet jede Datenreihe mit einem Farbfeld auf; bei mehr als sechs Reihen erscheint ein „+N weitere"-Hinweis. Siehe KI-Canvas.
- **Bestätigungsdialog beim Verlassen nicht gespeicherter Wartungsfenster** — Wenn Sie die Register-Einstellungsseite verlassen, obwohl Änderungen an den Wartungsfenstern noch nicht gespeichert wurden, erscheint jetzt eine Bestätigung, bevor Ihre Änderungen verworfen werden. Siehe Asset-Register.
- **Register-Vorfalldetails für Mitglieder sichtbar** — Mitglieder (Nicht-Admins) können auf den Detailseiten von Register-Vorfällen jetzt den Stationsnamen, die Adresse und die aufgetretene Änderung sehen, ohne Adminzugriff oder einen Link ins Register zu benötigen. Siehe Vorfälle.

Verbessert

- **Bedingungsvorschau zeichnet den gelernten Normalbereich** — Das Diagramm eines Datenpunkts, der von einer Anomalieprüfung „Außerhalb des normalen Bereichs" überwacht wird, zeigt jetzt den Bereich, mit dem die Prüfung vergleicht, als zwei gestrichelte Linien, die jeder nächtlichen Messung folgen; die Grenzen am Fadenkreuz erscheinen neben dem Messwert. Eine an einen Maschinenzustand gebundene Prüfung zeichnet den für diesen Zustand gemessenen Bereich. Siehe Monitore.
- **Stationsdetailseite aktualisiert sich automatisch** — Die Stationsdetailseite lädt jetzt alle 30 Sekunden neu, sodass CPU-Betriebsart, Scanergebnisse und Änderungen anderer Admins aktuell bleiben; geöffnete Formulare werden dabei beibehalten. Siehe Asset-Register.
- **Mehrere gespeicherte Felder erscheinen als ein Verlaufseintrag** — Wenn mehrere Felder auf einmal gespeichert werden, zeigt der Stationsverlauf jetzt einen zusammengefassten Eintrag — z. B. „Maria Weber hat 4 Felder geändert." — statt einer Zeile je Feld. Siehe Asset-Register.
- **„Außer Betrieb" als einheitliche Lebenszyklusbezeichnung** — Der Lebenszyklusstatus wird jetzt überall im Asset-Register einheitlich als „Außer Betrieb" angezeigt — auf dem Badge der Detailseite, in der Stationsliste, im Lebenszyklusfilter, im Stilllegungsdialog und in den Hinweistexten. Siehe Asset-Register.
- **Canvas-Diagrammkarten zeigen Aggregation und Gruppierung** — Die Überschrift einer Canvas-Diagrammkarte zeigt jetzt die Aggregation in Monospace (z. B. „avg(value)") und eine „gruppiert nach X"-Zeile erscheint, wenn die Abfrage gruppiert ist. Siehe KI-Canvas.
- **Canvas-KI-Untersuchung verwendet die leistungsstärkste Modellstufe** — Der Canvas-Untersuchungsagent läuft jetzt auf der leistungsstärksten Modellstufe und erstellt dadurch gründlichere und detailliertere Analysen. Siehe KI-Canvas.

- **Register-Vorfallzeilen zeigen Art und Stationszusammenfassung** — Zeilen von Register- und Systemvorfällen in der Vorfallsliste zeigen jetzt ein kurzes Typkennzeichen (z. B. „Firmware geändert", „Modul entfernt") und eine einzeilige Stationszusammenfassung statt „Keine Details." Siehe Vorfälle.
- **Vorfalldetails zeigen das betroffene Modul** — Die Vorfalldetailseite zeigt jetzt, an welchem Modul eine Firmware-Änderung stattgefunden hat — einschließlich Rack, Steckplatz, Bestellnummer und Seriennummer — neben den Firmware-Versionen vorher und nachher. Siehe Vorfälle.
- **Wartungsfenster-Validierung direkt am Feld** — Konfigurationsfehler (z. B. Endzeit vor Startzeit, kein Wochentag aktiviert) erscheinen jetzt direkt am Feld statt als Toast nach dem Speichern; die Schaltfläche „Fenster hinzufügen" wird mit einem erklärenden Hinweis deaktiviert, sobald das Serverlimit erreicht ist. Siehe Asset-Register.

Behoben

- **Bestätigungsmeldung bei Wiederinbetriebnahme ist korrekt, wenn die Station noch offline ist** — Wenn eine wieder in Betrieb genommene Station von einem Scan oder einer Datenquelle noch als offline gemeldet wird, zeigt die Erfolgsmeldung jetzt genau dies an, anstatt zu behaupten, die Station sei wieder erreichbar. Siehe Asset-Register.
- **Hover-Zeitstempel verwenden die gespeicherte Zeitzone des Benutzers** — Relative-Zeit-Tooltips in der gesamten Anwendung (zuerst gesehen, zuletzt gesehen, Ereigniszeiten u. a.) zeigen jetzt die Zeit in der konfigurierten Zeitzone des Benutzers statt im Browser-Standard an.

---

15. Oktober 2026

Neu

- **Vorschaugraphen der Bedingung auf der Abfrageseite öffnen** — Jedes Sensordiagramm im Vorschaubereich des Bedingungseditors hat jetzt ein Menü „Graph-Aktionen" (⋯-Schaltfläche klicken oder Zeile mit der rechten Maustaste anklicken) mit Optionen, um diese Datenreihe — oder alle Vorschaureihen auf einmal — auf der Abfrageseite zu öffnen, voreingestellt auf dasselbe Zeitfenster und dasselbe Raster. Siehe Abfrage.
- **Anomalieerkennung für Prometheus-Metriken** — Prometheus-Metriken können jetzt als Eingang eines Anomalieprüfungs-Knotens im Bedingungsgraphen verwendet werden, genau wie OPC-UA- und S7-Datenpunkte. Siehe Anomalieerkennung.

Verbessert

- **Bedingungsvorschau zeigt Daten für Anomalieprüfungs-Knoten** — Der Vorschaubereich des Bedingungseditors zeigt jetzt Sensordiagramme und wertet Anomalieprüfungs-Knoten aus; zuvor blieben diese Knoten leer, während der Rest des Graphen ausgeführt wurde.
- **Vorschaudiagramm-Beschriftungen enthalten die Aggregationsfunktion** — Reihenbeschriftungen in der Bedingungsvorschau zeigen jetzt die verwendete Aggregationsfunktion — zum Beispiel `latest(Kesseltemperatur)` — sodass die Beschriftung zum angezeigten Wert passt.

Behoben

- **Ergebnisse von PQL-`latest`-Abfragen sind jetzt stabil** — Diagramme, die die `latest`-Aggregation verwenden, zeigen bei jedem Seitenaufruf dieselben Werte, auch wenn mehrere Datenpunkte denselben Zeitstempel teilen. Siehe Abfrage.

---

14. Oktober 2026

Neu

- **Anomalieprüfungs-Knoten im Bedingungsgraphen-Editor** — Sie können jetzt einen „Anomalieprüfung"-Knoten direkt auf die Zeichenfläche des Bedingungsgraphen ziehen, einen Datenpunkt auswählen, Prüfungstyp und Empfindlichkeit festlegen und die Prüfung optional so einschränken, dass sie nur läuft, während ein anderes Signal einen bestimmten Wert hält. Siehe Anomalieerkennung.

Verbessert

- **Prüfungen, die vor der ersten Messung angelegt werden, aktivieren sich automatisch** — Das Anlegen einer Drift-Prüfung für einen Datenpunkt, der noch nie gemessen wurde, führte bisher dazu, dass die Prüfung niemals aktiviert wurde; sie zeigt jetzt den Status „Aktiv nach der Messung" und beginnt nach dem nächsten nächtlichen Basislinienlauf automatisch zu überwachen, ohne dass weiteres Eingreifen nötig ist. Siehe Anomalieerkennung.
- **Deutliche Warnung, wenn keine Eskalationsrichtlinie konfiguriert ist** — Wenn für einen Monitor noch keine Eskalationsrichtlinie eingerichtet ist, wird jetzt eine Meldung angezeigt, die erklärt, dass niemand alarmiert werden kann, anstatt die Konfiguration stillschweigend zu akzeptieren. Siehe Monitore.

---

12. Oktober 2026

Neu

- **Stationen stilllegen und wieder in Betrieb nehmen** — Admins können eine Station jetzt mit einer Pflichtbegründung stilllegen; sie wird als „Außer Betrieb" markiert, verbleibt im Register und wird weiterhin durch Scans aktualisiert. Ein einzelner Klick nimmt sie wieder in Betrieb, und der Verlauf protokolliert, wer wann und warum gehandelt hat. Siehe Asset-Register.
- **Offline-Stationen im Asset-Register gekennzeichnet** — Eine Station, die der letzte Scan zwar abgedeckt, aber nicht gefunden hat, oder bei der jede Live-Datenquelle die Verbindung verloren hat, wird jetzt in der Liste und auf der Detailseite mit einem „Offline"-Badge angezeigt — mit dem Datum der letzten Sichtung und Hinweisen, wie sie wieder erreichbar gemacht werden kann. Siehe Asset-Register.
- **Asset-Register-Einstellungen** — Eine neue Einstellungsseite (nur für Admins) ermöglicht die Auswahl einer Eskalationsrichtlinie, über die Register-Vorfälle weitergeleitet werden, sowie die Konfiguration von Wartungsfenstern, damit Firmware-Änderungen, entfernte Module und neue Stationen während geplanter Stillstandszeiten keine Vorfälle auslösen. Siehe Asset-Register.

Verbessert

- **Asset-Register nach Lebenszyklus filtern** — Die Stationsliste hat jetzt eine Lebenszyklus-Umschaltung — Alle, In Betrieb, Offline oder Außer Betrieb — sodass Sie sich auf die Stationen konzentrieren können, die Aufmerksamkeit benötigen. Siehe Asset-Register.
- **Stationsverlauf protokolliert weitere Ereignistypen** — Der Stationsverlauf zeichnet jetzt Firmware-Änderungen, Adressänderungen, Bearbeitungen von Angaben, Hinzufügen und Entfernen von Modulen, CPU-Betriebsartänderungen und Statusänderungen auf — zusätzlich zu den bereits erfassten Identitätsersetzungen und Zusammenführungen. Siehe Asset-Register.
- **Entfernte Module in der Modultabelle der Station gekennzeichnet** — Module, deren Entfernung durch Scans bestätigt wurde, werden in der Modultabelle jetzt mit einem „Entfernt"-Badge angezeigt und grau dargestellt; sie werden nicht mehr für die CVE-Überwachung angeboten. Siehe Asset-Register.
- **CPU-Betriebsart auf der Stationsdetailseite angezeigt** — Die aktuelle Betriebsart einer Siemens-CPU (RUN oder STOP) wird jetzt als Badge neben dem Modul in der Stationstabelle angezeigt, wie sie beim letzten Scan oder durch eine Live-Datenquelle gelesen wurde. Siehe Asset-Register.
- **Stationsdetailseite zeigt letzte Abdeckung und letzte Live-Sichtung** — Die Stationsdetailseite zeigt jetzt, wann die Station zuletzt von einem Scan abgedeckt und wann sie zuletzt von einer Live-Datenquelle gelesen wurde, damit Sie erkennen können, wie aktuell der angezeigte Zustand ist. Siehe Asset-Register.

- **Register-Vorfalldetails verlinken zur Station** — Detailseiten von Asset-Register-Vorfällen enthalten jetzt einen direkten Link zur betreffenden Station sowie die Angaben zu den aufgetretenen Änderungen — Firmware-Version vorher und nachher oder welches Modul an welcher Position entfernt wurde. Siehe Vorfälle.
- **S7-Erkennung zeigt Rack- und Steckplatzergebnisse** — Das Erkennungsdetail-Sheet für S7-Geräte listet jetzt auf, welche Racks und Steckplätze der Scan abgefragt hat, ob die Abfrage beantwortet wurde, abgelehnt wurde oder nicht versucht wurde — mit Kontexthinweisen, warum eine Ablehnung nicht immer einen leeren Steckplatz bedeutet. Siehe Geräteerkennung.

---

10. Oktober 2026

Neu

- **CVE-Überwachung auf Stationsdetailseiten** — Die Stationsdetailseite im Asset-Register hat jetzt einen Abschnitt „Schwachstellen": Sie können direkt von der Station aus einen CVE-Monitor für jedes Modul starten, alle zutreffenden CVEs einsehen, Entscheidungen prüfen und neue Bewertungen erfassen — Entscheidungen erscheinen auch auf den CVE-Seiten. Siehe Asset-Register und Schwachstellen.
- **Datenquellen-Panel auf Stationsdetailseiten** — Die Stationsdetailseite listet jetzt alle Datenquellen auf, die von dieser Station lesen, sodass Sie auf einen Blick sehen, was von jedem Gerät erfasst wird. Siehe Asset-Register.
- **Neuer CVE-Bewertungsstatus „Mitigiert"** — CVE-Funde können jetzt als „Mitigiert" bewertet werden, wenn eine kompensierende Maßnahme das Risiko reduziert, ohne die Firmware zu ersetzen. Siehe Schwachstellen.

Verbessert

- **CVE-Monitore können mit einem Asset-Register-Modul verknüpft werden** — Beim Erstellen oder Bearbeiten eines CVE-Monitors können Sie jetzt ein bestimmtes Modul aus dem Asset-Register auswählen; Pulse hält Bestellnummer und Firmware dann automatisch bei jedem Scan synchron. Siehe Schwachstellen.
- **Stationsliste zeigt Datenquellenabdeckung und neuen Filter** — Die Stationsanzahl zeigt jetzt, wie viele Stationen eine verbundene Datenquelle haben, und die Filterleiste bietet eine neue Option, um nur Stationen mit oder ohne Datenquelle anzuzeigen. Siehe Asset-Register.
- **Datenquellendetails zeigen verknüpfte Station** — Die Detailseite einer Datenquelle zeigt jetzt, von welcher Asset-Register-Station die Quelle liest. Siehe Asset-Register.

8. Oktober 2026

Neu

- **Stationen im Asset-Register zusammenführen** — Wenn zwei Registereinträge eigentlich ein Schaltschrank sind (z. B. eine CPU und ihr Kommunikationsprozessor, die jeweils unter einer eigenen Adresse antworten), können Sie jetzt beide auswählen und zu einer Station zusammenführen; die verbleibende Station übernimmt alle Adressen, MAC-Adressen und Module der entfernten Station. Siehe Asset-Register.
- **Zusammenführungsvorschläge für wahrscheinliche Schaltschrankpaare** — Das Asset-Register erkennt jetzt CPU- und Kommunikationsprozessor-Paare im selben Subnetz, deren Adressen am nächsten beieinander liegen, und stellt sie als Zusammenführungskandidaten dar, sodass Sie jeden Vorschlag prüfen, bestätigen oder verwerfen können, ohne manuell suchen zu müssen. Siehe Asset-Register.
- **Zusammenführung einer Station aufheben** — Wenn eine Zusammenführung irrtümlich erfolgte, können Sie sie jetzt rückgängig machen: Das Register stellt die übernommene Station unter ihrer ursprünglichen ID wieder her und gibt ihr die Adressen, MAC-Adressen und Module zurück, die von ihr stammten. Siehe Asset-Register.

Verbessert

- **Stationsdetailseite zeigt alle Adressen und MAC-Adressen** — Eine Station, die unter mehr als einer Adresse antwortet (z. B. nach einer Zusammenführung), listet jetzt alle bekannten Adressen und MAC-Adressen auf, nicht nur die primäre. Siehe Asset-Register.
- **OPC-UA-Serverdetails auf der Stationsdetailseite** — Stationen, die über OPC UA erkannt wurden, zeigen jetzt einen eigenen Abschnitt mit der ApplicationUri und dem Anwendungsnamen des Servers, wie sie bei der Erkennung beobachtet wurden. Wenn eine Station anhand ihrer ApplicationUri identifiziert wird, wird dies auf der Seite angezeigt, und spätere Scans erkennen die Station auch dann wieder, wenn sich ihre Adresse ändert. Siehe Asset-Register.
- **Stationsverlauf protokolliert Zusammenführungen, Aufhebungen und Identitätsersetzungen** — Die Stationsdetailseite verfügt jetzt über einen Verlaufsabschnitt, der alle identitätsrelevanten Ereignisse zeigt: wenn ein Scan ein anderes Gerät unter derselben Adresse gefunden hat, wenn die Station mit einer anderen zusammengeführt wurde oder wenn eine Zusammenführung rückgängig gemacht wurde — einschließlich wer gehandelt hat und wann. Siehe Asset-Register.

6. Oktober 2026

Neu

- **Eigene Benachrichtigungstöne in der mobilen App** — In der mobilen App erklingen Alarmierungen (neue Vorfälle, Eskalationen) jetzt mit einem markanten Alarmton, während Statusmeldungen (bestätigt, behoben) einen sanfteren Zweiklang verwenden — so erkennen Sie allein am Ton, ob Sie sofort handeln müssen.

Verbessert

- **Alarmierungen erreichen Sie auch im Fokus-Modus auf dem iPhone** — Vorfalls-Alarmierungen werden jetzt als zeitkritische Mitteilungen (Time Sensitive) zugestellt und erreichen Sie auch dann, wenn auf Ihrem iPhone ein Fokus-Modus oder „Nicht stören" aktiv ist.

---

4. Oktober 2026

Neu

- **OPC-UA-Knoten auf dem Mobilgerät Ebene für Ebene durchsuchen** — Im Dialog „Datenpunkt hinzufügen" wird auf Smartphones jetzt eine Ebene-für-Ebene-Ansicht verwendet: Tippen Sie auf einen Ordner, um ihn zu öffnen und jeder Zeile die volle Bildschirmbreite zu geben; ein Navigationspfad zeigt den Weg zurück. Die Auswahl bleibt beim Navigieren erhalten, sodass in einem Ordner ausgewählte Knoten nach dem Wechsel in einen anderen weiterhin markiert sind. Siehe OPC UA.

Verbessert

- **Genaue Werte für OPC-UA-Schweregradbandgrenzen eingeben** — Der Schweregradbandeditor zeigt jetzt neben den Ziehgriffen auch numerische Eingabefelder, sodass Sie einen genauen Grenzwert eintippen können, statt ihn per Drag zu positionieren. Siehe OPC UA.
- **Datenpunkt-Aktionen (Hinzufügen, Importieren, Exportieren) befinden sich jetzt über der Datenpunkttabelle** — Die Schaltflächen zum Hinzufügen, Importieren und Exportieren von Datenpunkten wurden aus dem Seitenkopf direkt über die Datenpunkttabelle verschoben, sodass der Seitenkopf bei langen Quellnamen übersichtlich bleibt und die Aktionen neben dem stehen, worauf sie wirken. Siehe OPC UA.
- **Vorfälle nach dem Typ „OPC-UA-Alarme & Bedingungen" filtern** — Die Vorfallsliste enthält jetzt den Filtertyp „OPC-UA-Alarme & Bedingungen", sodass Sie ausschließlich alarmbasierte Vorfälle anzeigen können. Siehe Vorfälle.

- **Monitore nach dem Typ „OPC-UA-Alarme & Bedingungen" filtern** — Die Monitorliste zeigt einen Filterchip „OPC-UA-Alarme & Bedingungen", wenn solche Monitore vorhanden sind, damit Sie die Liste direkt auf Alarmmonitore einschränken können. Siehe Monitore.

Behoben

- **Dialoge mit breitem oder hohem Inhalt laufen auf Smartphones nicht mehr über** — Ein Dialog, dessen Inhalt langen nicht umbrechenden Text enthielt (z. B. OPC-UA-Knotennamen und -IDs), konnte den gesamten Dialog auf kleinen Smartphones über den rechten Bildschirmrand hinausschieben; der Dialog hält seinen Inhalt jetzt in den Grenzen und scrollt bei Bedarf. Auch sehr hohe Dialoge auf sehr kleinen Bildschirmen bleiben jetzt im Sichtbereich, statt an beiden Enden abgeschnitten zu werden.
- **Die Schrittanzeige des CSV-Import-Assistenten läuft auf Smartphones nicht mehr über den Drawer hinaus** — Die Schrittzeile füllt jetzt die Drawerbreite aus und umbricht Schritttitel, statt die äußeren Schritte auf beiden Seiten abzuschneiden. Siehe CSV-Import.

---

28. September 2026

Behoben

- **Das Suchfeld für Datenpunkte auf der Detailseite einer Datenquelle verliert beim Tippen nicht mehr den Fokus** — Die Eingabe eines Suchbegriffs führt nicht mehr dazu, dass die Seite zwischen den Tastenanschlägen kurz in einen Ladezustand wechselt, sodass das Eingabefeld den Fokus behält und die Ergebnisse sich nahtlos aktualisieren.

---

26. September 2026

Verbessert

- **Datenpunkte auf der Detailseite einer Datenquelle suchen** — Die Datenpunkttabelle verfügt jetzt über ein Suchfeld, das nach Name, Adresse oder Beschreibung filtert und den Suchbegriff an den Server sendet, sodass alle Datenpunkte einer umfangreichen Quelle — auch jene jenseits der ersten Seite — erreichbar sind, unabhängig davon, wie viele Reihen die Quelle enthält.

---

25. September 2026

Neu

- **Mehrere Abfragen parallel auf der Abfrageseite ausführen** — Die Abfrageseite unterstützt jetzt bis zu sechs gleichzeitige Abfragen (gekennzeichnet mit A–F), jede mit eigenem SELECT, WHERE, GROUP BY und optionalem Namen, sodass Sie Signale oder Aggregationen nebeneinander vergleichen können, ohne mehrere Tabs öffnen zu müssen. Siehe Abfragen.
- **Drift-Prüfung — langsame Veränderungen gegen eine festgehaltene Referenz erkennen** — Eine neue Prüfung „Entfernt sich von seiner Referenz" vergleicht das aktuelle Signalniveau mit einem bei der Einrichtung festgehaltenen Ausgangswert und erkennt damit schleichende Veränderungen, die die anderen adaptiven Prüfungen allmählich akzeptieren lernen. Siehe Anomalieerkennung.
- **Zustandsbasierte Anomalieerkennung für zyklische Signale** — Ein neues Feld „Nur während" im Dialog zur Anomalieerkennung ermöglicht die Auswahl eines Zustands-Datenpunkts und eines Werts, sodass Pulse das Signal nur während dieser Betriebsphase überwacht und misst — damit werden Drift- und Bereichsprüfungen für Signale wie Antriebsströme aussagekräftig, die mehrere Betriebszustände überlagern. Siehe Anomalieerkennung.

Behoben

- **Vorfallsmarkierungen liegen auf allen Diagrammen der Abfrageseite jetzt an gleicher Position** — Bei mehreren offenen Abfragediagrammen erschien derselbe Vorfall an unterschiedlichen horizontalen Positionen, weil jedes Diagramm den Marker an sein eigenes Datengitter snappte; Marker werden jetzt auf die gemeinsame Zeitachse ausgerichtet.
- **Diagrammreihen erscheinen jetzt auch für Datengruppen, die erst im Verlauf des Abfragefensters Daten liefern** — Gruppen, deren erster Datenpunkt nach dem Beginn der Abfrage liegt, fehlten in Legende und Diagramm vollständig; sie werden jetzt korrekt angezeigt.
- **Die Übersichtstabelle beschriftet ungegruppierte Abfrageergebnisse jetzt mit ihrem Betreff** — Wenn eine Abfrage kein GROUP BY hatte, zeigte die einzelne Ergebniszeile nur den Aggregationswert ohne Beschriftung; die Zeile zeigt jetzt den Namen des Datenpunkts oder der Quelle.
- **Gemeinsam genutzte Abfrage-Links werden jetzt auch für Organisationen ohne Monitore automatisch ausgeführt** — Eine gespeicherte oder geteilte Abfrage-URL wurde nicht automatisch ausgeführt, wenn die Organisation keine Monitore hatte; sie wird jetzt ausgeführt, sobald die Organisation bekannt ist.

---

24. September 2026

Neu

- **OPC-UA-Monitor für Alarme & Bedingungen** — Jede OPC-UA-Datenquelle verfügt jetzt über einen dedizierten Alarme-&-Bedingungen-Monitor, der den Alarmkanal des Servers abonniert und für jede aktive Bedingung einen Vorfall anlegt; Alarm-Vorfälle werden nun auf diesem Monitor statt auf dem Quellenzustands-Monitor erfasst. Das Abonnement kann auf der Einstellungsseite der Datenquelle ein- oder ausgeschaltet werden. Siehe OPC UA.
- **Schweregradbereiche für das OPC-UA-Alarmrouting** — OPC-UA-Datenquellen können Alarm-Schweregrade (1–1000) über konfigurierbare Schweregradbereiche auf Eskalationsrichtlinien abbilden. Teilen Sie einen Bereich, um eine Grenze einzufügen, führen Sie benachbarte Bereiche zusammen, um die Konfiguration zu vereinfachen, und weisen Sie jedem Bereich eine eigene Richtlinie zu oder übernehmen Sie die Standardrichtlinie des Monitors. Wenn Bereiche konfiguriert sind, zeigt die Spalte „Eskalationsrichtlinie" in der Datenquellenliste an, wie viele Bereiche den Standard überschreiben. Siehe OPC UA.

Verbessert

- **Scaneinstellungen und Protokoll der Gerätesuche befinden sich jetzt in Einschubfenstern** — Die Scan-Konfiguration (Netzwerkbereich, Protokolle und Sondenoptionen) und das Scan-Protokoll wurden in je ein dediziertes Einschubfenster verschoben, sodass die Ergebnisseite auf die gefundenen Geräte fokussiert bleibt. Eine Schaltfläche „Erneut suchen" wiederholt den letzten Scan, ohne die Einstellungen erneut öffnen zu müssen. Vor dem ersten Scan zeigt ein Begrüßungsbildschirm den vorausgefüllten Netzwerkbereich und verweist auf den Einstellungsbereich. Das Scan-Protokoll zeigt jetzt die vergangene Zeit, filterbare Warn- und Fehlerzählungen sowie eine Schaltfläche zum Kopieren des Protokolls. Siehe Gerätesuche.
- **Datenpunktspalten zeigen jetzt Hinweise und erlauben die Ansicht genauer Werte** — Die Spalten „Letzter Wert" und „Letzte Messung" sind jetzt interaktiv: Wählen Sie einen Wert aus, um den vollständigen Messwert oder den genauen Zeitpunkt zu sehen. Die Tags-Spalte zeigt die Anzahl der von der Datenquelle geerbten Tags an; wählen Sie die Zahl aus, um die Tags anzuzeigen.

Behoben

- **Quellenzustands-Datenpunkte sind vor dem Löschen geschützt** — Beim Versuch, den integrierten Quellenzustands-Datenpunkt zu löschen, erscheint jetzt eine Meldung, die erklärt, dass die Datenquelle ihn selbst meldet und er nicht entfernt werden kann.

---

23. September 2026

Neu

- **CVE-Monitore können Geräte jetzt auch über Hersteller und Produktname zuordnen, nicht nur über die Bestellnummer** — Die Bestellnummer (MLFB) ist bei einem CVE-Monitor jetzt optional; Sie können stattdessen oder zusätzlich Hersteller und Produktname angeben. Das Gateway gleicht über alle verfügbaren Schlüssel des Monitors ab, und jeder Fund zeigt jetzt an, ob er über Bestellnummer, Familiencode oder Produktname gefunden wurde — sodass namenbasierte Treffer leicht für eine manuelle Prüfung identifizierbar sind. Siehe Schwachstellen.

Verbessert

- **Der CVE-Schwachstellenkatalog deckt jetzt deutlich mehr Produkte ab** — Advisories, die betroffene Produkte über Komponenten-Plattform-Beziehungen definieren — ein Muster, das unter anderem von Phoenix Contact, WAGO, Endress+Hauser, Festo, Pepperl+Fuchs, Helmholz und Pilz verwendet wird — fehlten bisher im Katalog; diese Produkte werden jetzt indiziert und abgeglichen. Siehe Schwachstellen.
- **Auf der Appliance nummeriert der Installer jeden Schritt gegen die Gesamtanzahl** — Die Installer-Konsole zeigt jetzt „Schritt 2 von 5" während der Einrichtung an, sodass Sie jederzeit wissen, wie weit Sie fortgeschritten sind und wie viele Schritte noch folgen.
- **Auf der Appliance zeigt der Systemstatus jetzt die laufende Softwareversion der Appliance** — Die Version, mit der die Appliance installiert oder zuletzt aktualisiert wurde, wird jetzt auf dem Systemstatusbildschirm neben den Build- und Commit-Informationen angezeigt.
- **Auf der Appliance zeigt der Update-Fortschrittsbildschirm jetzt die vergangene Zeit und einen scrollenden Verlauf** — Während eines Updates zeigt die Konsole an, wie lange das Update bereits läuft, und hält einen begrenzten Verlauf zuletzt angezeigter Statusmeldungen vor, sodass Sie auf einen Blick erkennen können, ob das Update Fortschritte macht.

Behoben

- **Auf der Appliance wird eine Netzwerkänderung jetzt vor der Übernahme bestätigt** — Der Netzwerkkonfigurationsbildschirm zeigt jetzt eine Zusammenfassung der geplanten Änderung und fordert eine Bestätigung an, bevor die neuen Einstellungen geschrieben werden, um versehentliche Neukonfigurationen zu verhindern.
- **Auf der Appliance teilt der Installer nach Abschluss der Einrichtung mit, wie Pulse erreichbar ist** — Der letzte Installationsschritt zeigt jetzt die URL und alle Hinweise an, die der Bediener benötigt, um die Web-Oberfläche der neu installierten Appliance zu öffnen.

- **Auf der Appliance akzeptiert die Pairing-Code-Eingabe jetzt visuell ähnliche Zeichen** — Zeichen, die in manchen Schriften ähnlich aussehen (z. B. O und 0), werden bei der Eingabe eines Pairing-Codes jetzt gleichwertig akzeptiert, sodass ein falsch gelesenes Zeichen keinen fehlgeschlagenen Kopplungsversuch verursacht.
- **Auf der Appliance werden Fehler beim Installer und Statuswerte jetzt auf Deutsch angezeigt** — Validierungsfehler während der Installation und nicht klassifizierbare Statuswerte wurden bisher auf Englisch angezeigt; sie werden jetzt auf Deutsch ausgegeben.
- **Auf der Appliance bleibt die tty1-Konsole nach schnellen Neustarts nicht mehr hängen** — Eine Folge von schnellen Beendigungen der lokalen Oberfläche (Absturz, frühzeitiges Beenden oder wiederholte Tastendrücke) konnte die Auto-Login-Konsole dauerhaft deaktivieren und erforderte SSH-Zugang zur Wiederherstellung; die Konsole startet jetzt unabhängig von der Ausstiegsgeschwindigkeit zuverlässig neu.
- **Die Gerätesuche beurteilt die Erreichbarkeit jetzt über alle Netzwerkschnittstellen** — Wenn ein Gerät über mehrere Schnittstellen erreichbar ist, prüft die Gerätesuche jetzt jeden Pfad, anstatt beim ersten zu stoppen, sodass Geräte, die nur über eine sekundäre Schnittstelle erreichbar sind, nicht mehr stillschweigend übergangen werden. Siehe Gerätesuche.
- **Die Gerätesuche setzt beim Neustart den Log-Cursor zurück** — Das Starten eines neuen Scans löscht jetzt den Log-Cursor des vorherigen Durchlaufs, sodass die Ergebnisse den aktuellen Scan widerspiegeln und keine veralteten Einträge aus dem letzten Scan übernommen werden. Siehe Gerätesuche.

---

22. September 2026

Verbessert

- **Der Kopplung-Dialog und die Push-Benachrichtigungseinstellungen verlinken jetzt direkt auf die Pulse-Dispatch-App** — Beim Koppeln eines Mobilgeräts oder beim Aktivieren von Push-Benachrichtigungen für einen Schweregrad zeigt die Web-App jetzt einen direkten Link zum Download von Pulse Dispatch im App Store an, sodass Empfänger die App ohne Suche finden können.

Behoben

- **Die mobile Deeplink-Weiterleitungsseite verweist jetzt auf den korrekten App-Store-Eintrag** — Wenn ein geteilter Vorfalls-Link auf einem Smartphone ohne installiertes Pulse Dispatch geöffnet wurde, verlinkten die Weiterleitungsseite auf einen veralteten Eintrag; sie verweist jetzt auf die veröffentlichte Pulse-Dispatch-App.

- **S7-Datenquellen schlagen jetzt korrekt fehl, wenn die Statusabfrage einen Verbindungsfehler zurückgibt** — Ein Transportfehler bei der S7-Statusabfrage wird jetzt als Fehler im Abtastvorgang behandelt, sodass die Datenquelle den Zustand „nicht erreichbar" widerspiegelt, anstatt die Abtastung stillschweigend fortzusetzen.
- **Auf der Appliance werden bei einem fehlgeschlagenen Update mit fehlgeschlagenem Rollback jetzt alle Wiederherstellungsinformationen protokolliert** — Wenn sowohl ein Update als auch sein Rollback fehlschlagen, enthält das Protokoll jetzt den Wiederherstellungshinweis mit dem Pfad des Backups vor dem Update, sodass Administratoren die nötigen Informationen für eine manuelle Wiederherstellung haben.
- **Das Bestätigen oder Auflösen eines Vorfalls über einen Aktionslink wird jetzt genau einmal ausgeführt** — Ein Gateway-Aktionstoken (aus einer E-Mail, SMS oder Push-Benachrichtigung) wird jetzt atomar vor der Ausführung des Befehls beansprucht, sodass eine doppelte Zustellung während eines Zero-Downtime-Updates die Bestätigung oder Auflösung nicht wiederholt.
- **OPC-UA-Alarmereignisse lösen während eines Update-Überlappungsfensters keine doppelten Vorfälle mehr aus** — Wenn zwei Prozesse kurzzeitig Abonnements für denselben OPC-UA-Endpunkt halten, wird jede Alarmbenachrichtigung jetzt genau einmal protokolliert und verarbeitet, was fehlerhafte doppelte Vorfälle oder Auflösungen verhindert.

---

21. September 2026

Sicherheit

- **Collectors authentifizieren sich jetzt mit kryptografischen Schlüsselpaaren statt mit Bearer-Tokens** — Jeder Collector generiert ein eigenes Ed25519-Schlüsselpaar und beweist dessen Besitz bei jeder Verbindung mit einer neuen Nonce-Signatur; ein kompromittiertes Token kann nicht mehr wiedergegeben werden. Bei einer Neukopplung wird automatisch ein neues Schlüsselpaar generiert. Siehe Collector-Kopplung.

Verbessert

- **Auf der Appliance werden zwei neue Collector-Statuszustände mit einem Schnellzugang zur Neukopplung angezeigt** — Die Collector-Konsole zeigt jetzt eine spezifische Meldung, wenn die Appliance einen Identitätsnachweis ablehnt oder wenn der Schlüssel eines Collectors bereits einem anderen Collector zugeordnet ist, und bietet in beiden Fällen die Einzug-Neukopplung an. Siehe Collector-Status.

20. September 2026

Verbessert

- **Die Datenquelle-Detailseite zeigt, warum eine Datenquelle fehlschlägt und seit wann** — Wenn eine Datenquelle keine Verbindung herstellen kann, zeigt die Detailseite jetzt einen klassifizierten Fehlergrund (z. B. „Zertifikat abgelehnt", „DNS-Auflösung fehlgeschlagen" oder „SPS-Verbindungsanfrage abgelehnt"), den Zeitpunkt des ersten Fehlers und die rohe Gerätemeldung — erweiterbar und kopierbar, ohne die Seite zu verlassen. Gilt für OPC-UA-, S7- und Prometheus-Datenquellen.
- **Die Gerätesuche erfasst mehr Identitätsinformationen für PROFINET- und OPC-UA-Geräte** — PROFINET-Funde enthalten jetzt LLDP-Systemname und LLDP-Systembeschreibung, wenn das Gerät LLDP ausstrahlt, und OPC-UA-Serverfunde enthalten jetzt Hersteller, Produktname und Softwareversion aus dem BuildInfo-Knoten des Servers. Siehe Gerätesuche.

Behoben

- **Die Gerätesuche verwirft binäre LLDP-Kennungen nicht mehr** — Chassis- und Port-IDs mit binärer Kodierung werden jetzt als Hexadezimalwert in den Scan-Ergebnissen angezeigt, anstatt stillschweigend verworfen zu werden. Siehe Gerätesuche.

---

18. September 2026

Neu

- **Auf der Appliance können jetzt mehrere Ethernet-Schnittstellen konfiguriert werden** — Der Netzwerkbildschirm ermöglicht es, jeden Port einzeln mit DHCP oder einer statischen Adresse einzurichten, statische Routen für die OT-seitige Verbindung hinzuzufügen und die Web-Oberfläche sowie SSH auf bestimmte Schnittstellen zu beschränken, sodass anlagenseitige Ports ausschließlich für die Gerätesuche genutzt werden. Eine Schnittstelle lässt sich durch Aus- und Einstecken des Kabels identifizieren, und die Appliance folgt der Konfiguration automatisch, wenn sich der Interface-Name einer Netzwerkkarte ändert. Siehe Netzwerkkonfiguration.

Verbessert

- **Suchergebnisse der Gerätesuche werden jetzt in einer filterbaren Tabelle mit Detailfenster angezeigt** — Die Ergebnisseite zeigt eine kompakte Tabelle, die nach Name, Adresse, Artikelnummer oder Seriennummer gefiltert werden kann; ein Klick auf eine Zeile öffnet ein Detailfenster mit allen Informationen, die der Scan zu diesem

Gerät gesammelt hat. Hosts, die auf den Netzwerk-Sweep geantwortet haben, aber kein Industrieprotokoll unterstützen, werden standardmäßig in einer Zusammenfassung ausgeblendet. Siehe Gerätesuche.

- **Auf der Appliance zeigt die Konsolenkopfzeile die aktuelle Uhrzeit und die Systemrolle** — Die Hauptmenü-Kopfzeile zeigt jetzt die Systemuhr und ob das System eine Appliance oder ein Collector ist, sodass Sie vor Konfigurationsänderungen bestätigen können, dass Sie die richtige Maschine vor sich haben.

---

17. September 2026

Neu

- **Auf der Appliance akzeptiert die Collector-Konsole jetzt eine Cloud-Link-URL als Adresse** — Beim Koppeln eines Collectors mit einer Pulse-Cloud-Instanz können Sie die Cloud-Link-URL jetzt direkt in der Collector-Konsole eingeben, anstatt eine lokale Appliance-Adresse.

Verbessert

- **Collector-Pairing-Codes sind jetzt 12 Zeichen lang** — Pairing-Codes verwenden jetzt das Format `XXXX-XXXX-XXXX` (bisher `XXXX-XXXX`) und bieten damit einen größeren Coderaum, der Brute-Force-Versuche auch dann unpraktisch macht, wenn Codes über den öffentlichen Cloud-Link eingelöst werden können.
- **Auf der Appliance zeigen Installer und Boot-Menü jetzt Pulse-Branding** — Der Startbildschirm des ISO-Installers und das Appliance-Boot-Menü zeigen jetzt das Pulse-Logo und die Markenfarben anstelle der NixOS-Standards.
- **Die Gerätesuche zeigt die Seriennummer einer S7-Baugruppe** — Ein Siemens-S7-Fund führt die Seriennummer jetzt neben Bestellnummer und Firmware-Version auf, sodass sich eine Ergebniskarte mit dem Typenschild der Baugruppe im Schaltschrank abgleichen lässt. Siehe Gerätesuche.

Behoben

- **Die Gerätesuche führt dieselbe Steuerung nicht mehr doppelt auf** — Eine CPU, die an mehreren Steckplätzen antwortet — eine S7-1500 antwortet auf Steckplatz 1 und auf Steckplatz 0 —, wurde je Steckplatz einmal gemeldet, sodass eine Steuerung als zwei Funde mit zwei Schaltflächen **Als Datenquelle übernehmen** erschien. Baugruppen mit derselben Seriennummer werden jetzt zu dem einen Fund an der Position zusammengefasst, über die eine Datenquelle sie anspricht. Siehe Gerätesuche.

16. September 2026

Verbessert

- **Gerätesuche gruppiert alle Module auf einer Ergebniskarte pro Gerät** — Die Gerätesuche zeigt jetzt eine einzelne Karte pro Gerät und listet jeden gefundenen Modul darauf auf — einschließlich Kommunikationsprozessoren, weiterer Module mit Seriennummern und Ortsangaben aus der Engineering-Konfiguration des Geräts — sodass alle Informationen zu einem Gerät gesammelt erscheinen. Siehe Gerätesuche.
- **PROFINET-Gerätenamen zeigen die ursprüngliche Engineering-Bezeichnung** — Wenn der Name eines PROFINET-Geräts vom Engineering-Tool automatisch aus einer Anlagenbezeichnung konvertiert wurde, entfernt die Gerätesuche jetzt den angehängten Prüfsummenanteil und zeigt den dekodierten ursprünglichen Namen neben der konvertierten Form an, sodass Scan-Ergebnisse leichter dem Anlagenlayout zugeordnet werden können. Siehe Gerätesuche.
- **Collector-Kopplung verwendet einen Einmalcode statt eines Tokens** — Das Hinzufügen oder erneute Koppeln eines Collectors zeigt jetzt einen kurzen, ablaufenden Pairing-Code zusammen mit dem Appliance-Fingerabdruck, den Sie beim Einrichten auf dem Collector eingeben; die Aktion „Token neu erzeugen" heißt jetzt „Neuen Pairing-Code erzeugen".

Behoben

- **CSV-Monitor-Importe mit Schwellwertspalten schlagen nicht mehr mitten im Import fehl** — Der Importeur wertet jetzt zeilenweise aus, ob Schwellwertspalten vorhanden sind, statt anzunehmen, dass alle Zeilen demselben Schema folgen; das behebt unerwartete Zeilenfehler in gemischten Importdateien. Siehe Importieren aus CSV.

---

15. September 2026

Neu

- **S7-Geräteerkennung zeigt Firmware-Version an** — Die Ergebnisseite der Gerätesuche zeigt jetzt die Firmware-Version jeder gefundenen S7-Steuerung neben Bestellcode, Rack und Steckplatz an. Siehe Gerätesuche.

Behoben

- **Bestellcodes für erkannte S7-Geräte werden jetzt korrekt angezeigt** — S7-Bestellcodes in den Suchergebnissen wurden zuvor aus dem falschen Systemregister ausgelesen und konnten abschließende Nullzeichen enthalten; beide Probleme sind behoben, sodass der Bestellcode korrekt angezeigt wird.

14. September 2026

Neu

- **Remote-Collectors** — Eine neue Collectors-Seite unter Einstellungen ermöglicht es, Remote-Collector-Agenten zu registrieren, die in abgeschotteten OT-Netzwerkzonen laufen und sich über Port 443 zur Appliance herauswählen; für jeden Collector werden Verbindungsstatus, Hostname und die zugewiesenen Datenquellen angezeigt. S7- und OPC-UA-Datenquellen können über einen bestimmten Collector abgefragt werden, Erkundungsscans lassen sich von einem Collector aus starten, und wenn ein verbundener Collector offline geht, wird ein Systemvorfall ausgelöst.
- **Monitore oder Datenpunkte als CSV exportieren** — Die Monitor-Liste hat jetzt im Erstellen-Menü die Option „CSV exportieren", und jede S7- oder OPC-UA-Datenquellen-Seite bietet eine entsprechende Exportschaltfläche; beide erzeugen Dateien im gleichen Spaltenformat wie der Importassistent, sodass Sie sie herunterladen, in der Masse bearbeiten und wieder importieren können. Siehe Importieren aus CSV.
- **Bestehende Monitore per CSV-Import aktualisieren** — Der CSV-Importassistent hat jetzt den Schalter „Bestehende Monitore aktualisieren"; wenn er eingeschaltet ist, aktualisiert eine Zeile, deren Name einem vorhandenen Monitor oder einer vorhandenen Bedingung entspricht, diesen statt die Zeile fehlschlagen zu lassen; die Ergebnisseite zeigt eine Aktualisiert-Anzahl neben Erstellt und Fehlgeschlagen. Siehe Importieren aus CSV.

Verbessert

- **Tags-Spalte im CVE-Monitor-Import** — Der CVE-Monitor-Import akzeptiert jetzt eine Tags-Spalte (Werte mit `|` getrennt), mit der Sie Tags als Teil eines Massenimports zuweisen oder aktualisieren können. Siehe Importieren aus CSV.

Behoben

- **CSV-Exporte öffnen sich korrekt in Excel** — Monitor- und Datenpunkt-Exporte enthalten jetzt eine UTF-8-Byte-Order-Mark, sodass sie in Excel und anderen Tabellenkalkulationsprogrammen ohne korrekte Zeichenkodierung geöffnet werden.
- **CSV-Import behält eingetippte Werte beim Aktualisieren** — Wenn „Bestehende Monitore aktualisieren" aktiviert ist, werden fest eingetippte Werte in Importfeldern jetzt korrekt beim Aktualisieren übernommen statt verworfen.

12. September 2026

Neu

- **Steuerungen im Netzwerk suchen** — Eine neue Seite „Geräte suchen" durchsucht einen Netzbereich nach Siemens-S7-, OPC-UA- und PROFINET-Steuerungen und zeigt die Ergebnisse während des Scans in Echtzeit an – mit Fortschrittsbalken, Live-Protokoll und einer Ergebniskarte für jedes gefundene Gerät. Von dort aus können Sie jedes Gerät mit bereits vorausgefüllten Verbindungsdaten als Datenquelle übernehmen. Siehe Gerätesuche.

Verbessert

- **Abfrage- und Bedingungsdiagramme zeigen bei mehrtägigen Zeiträumen Datumsangaben auf der x-Achse** — Wenn eine Abfrage oder eine Bedingungsvorschau mehr als einen Tag umfasst, zeigt die x-Achse jetzt Datumsangaben (z. B. „12. Sep.") statt Uhrzeiten an, sodass auf einen Blick erkennbar ist, auf welchen Tag ein Datenpunkt fällt.

Sicherheit

- **Auf der Appliance verwendet die Jaeger-Tracing-Oberfläche jetzt ein eindeutiges appliance-spezifisches Passwort** — Jede Appliance generiert beim ersten Start ein eigenes zufälliges Passwort für die Jaeger-Oberfläche; die bisher auf allen Appliances identischen Standard-Anmeldedaten funktionieren nicht mehr. Appliances, die noch das alte Standard-Passwort haben, werden beim nächsten Start automatisch migriert. Das generierte Passwort kann in der Expert Shell unter `/var/pulse/secrets/jaeger-password` ausgelesen werden.
- **Auf der Appliance sind Systemmetriken nicht mehr aus dem Netzwerk erreichbar** — Der Prometheus-Node-Exporter (CPU, Arbeitsspeicher, Festplatte und weitere Hostmetriken) ist jetzt nur noch an Loopback gebunden, und Port 9100 ist in der Firewall nicht mehr geöffnet.

---

10. September 2026

Neu

- **On-Call-Änderungen zu einem späteren Zeitpunkt in Kraft setzen** — Wenn Sie einen On-Call-Plan bearbeiten, können Sie jetzt wählen, ob die Änderung sofort oder zu einem bestimmten Datum und einer bestimmten Uhrzeit wirksam wird; die aktuell gültige Rotation bleibt bis zu diesem Zeitpunkt unverändert, und eine ausstehende Änderung wird im Formular angezeigt, sodass eine weitere Bearbeitung sie aktualisiert, anstatt sich dahinter einzureihen. Siehe On-Call-Pläne.
- **Automatisches Onboarding für Ihre Unternehmensdomain** — Beim Erstellen einer neuen Organisation können Sie ein Kontrollkästchen aktivieren, damit jede Kollegin und jeder Kollege, die bzw. der sich mit einer E-Mail-Adresse derselben

Unternehmensdomain registriert, automatisch beitritt – ohne Einladungslink; dieselbe Einstellung steht Admins nach der Erstellung unter Organisationseinstellungen → Allgemein zur Verfügung. Siehe Organisationseinstellungen.

Verbessert

- **Einer vollen Organisation beizutreten erfordert keinen freien lizenzierten Platz mehr** — Wenn Sie eine Einladung zu einer Organisation annehmen, die ihr Platzlimit erreicht hat, treten Sie jetzt als nicht lizenziertes Mitglied bei, anstatt eine Fehlermeldung zu erhalten; ein Admin kann Ihnen später eine Lizenz zuweisen.

---

9. September 2026

Behoben

- **Bedingungsvorschau wertet gegen die zum jeweiligen Zeitpunkt gültige Baseline aus** — Wenn Sie eine Bedingung über einen historischen Zeitraum in der Vorschau prüfen, verwendet die Auswertung jetzt die Baseline-Version, die zu jedem Zeitpunkt tatsächlich in Kraft war; eine Bedingung mit mehreren Baseline-Revisionen liefert damit keine Backtest-Ergebnisse mehr, die von der Entscheidung des Live-Monitors abweichen würden. Siehe Monitore.
- **Beim Massenlöschen von Monitoren werden Blockierer in der Reihenfolge Ihrer Auswahl aufgelistet** — Wenn eine Massenlöschung von Monitoren abgelehnt wird, weil einige Monitore zugeordnete Bedingungen haben, nennt der Dialog diese Monitore jetzt in der Reihenfolge, in der sie in der Liste erscheinen, entsprechend der Reihenfolge, in der Sie sie ausgewählt haben.

---

8. September 2026

Neu

- **Monitore nach Datenquelle filtern** — Die Monitor-Liste verfügt jetzt über einen Datenquellen-Filter, mit dem Sie alle Monitore anzeigen können, die ein bestimmtes Gerät lesen – bei einem Wartungsfenster lassen sich so alle auf einmal auswählen und stummschalten oder Massenaktionen durchführen. Siehe Monitore.
- **Vorfallsberichte auf bestimmte Datenquellen einschränken** — Berichtskonfigurationen unterstützen jetzt einen Datenquellen-Filter; erzeugte Berichte enthalten dann nur Vorfälle von Monitoren, die diese Geräte lesen. Siehe Berichte.

- **Mehrere Bedingungen auf einmal löschen** — Die Bedingungsliste hat jetzt den Auswahlmodus der Monitor-Liste: **Auswählen** macht jede Zeile zum Kontrollkästchen, „Alle auswählen" und Umschalt+Klick greifen ganze Läufe, und die Leiste am unteren Rand löscht sie nach einer eingetippten Bestätigung. Enthält die Auswahl eine Bedingung, auf die ein Monitor alarmiert oder über die ein Ziel etwas zusagt, wird sie als Ganzes abgelehnt; der Dialog nennt dann, was sie hält, und bietet an, den Rest zu löschen. Siehe Monitore.
- **Beim Massenlöschen von Monitoren wird genannt, wie viele Bedingungen mitgegangen sind** — Der letzte Monitor, der auf eine Bedingung alarmiert, hat diese Bedingung schon immer mitgenommen; jetzt nennt die Bestätigungsmeldung beide Zahlen, sodass Sie nach einem Upgrade nicht nach Graphen suchen, die längst weg sind. Siehe Monitore.

Verbessert

- **Auf der Appliance sagt eine abgelehnte Update-Datei jetzt, woran es liegt und was zu tun ist** — Schlug die Prüfung eines Update-Bundles fehl, zeigte der Bildschirm bisher nur die Meldung des Prüfprogramms („verification failed: checked against wrong key"). Jetzt steht dort in einem Satz, was gefunden wurde – etwa dass das Bundle für eine andere Appliance signiert wurde, unvollständig kopiert oder nach dem Signieren verändert wurde – und darunter der nächste Schritt. Die technische Meldung bleibt für den Support in einer dritten, gedämpften Zeile stehen, und lange Meldungen werden jetzt auf schmalen Konsolen umgebrochen statt abgeschnitten.

Behoben

- **Stumm geschaltete Heartbeat-Monitore zeigen jetzt ihren tatsächlichen Gesundheitszustand** — Ein stummgeschalteter Heartbeat-Monitor wurde bisher nicht mehr überprüft und blieb eingefroren im zuletzt bekannten Zustand, auch wenn keine Heartbeats mehr ankamen; er wird jetzt kontinuierlich ausgewertet und wechselt in den Status „nicht in Ordnung", sobald der Heartbeat überfällig ist – der Statusindikator bleibt korrekt, ohne dass der Monitor einen Vorfall auslöst.
- **Bedingungsmonitore verwendeten das falsche Abtastintervall für Aktualitätsprüfungen** — Die Aktualität eines Monitors wurde anhand eines Felds im Datenpunkt-Datensatz berechnet statt aus der Datenquelle, was dazu führen konnte, dass pünktliche Messwerte als veraltet eingestuft wurden. Jetzt wird das korrekte Intervall der Datenquelle verwendet.
- **Die Monitor-Liste von KI-Canvas und MCP ignorierte Typfilter lautlos** — Eine falsche Reihenfolge der Argumente führte dazu, dass Typfilter verworfen und andere Argumente verschoben wurden, sodass fehlerhafte Monitor-Listen zurückgegeben wurden; das Werkzeug wendet jetzt alle Filter korrekt an.

Entfernt

- **Bearbeitungsseite für ältere Heartbeat-Monitore** — Die URL `/monitors/heartbeat/:id` leitet jetzt zur Monitor-Liste weiter; Heartbeat-Monitor-Einstellungen werden über die zugehörige Datenquelle verwaltet.

---

6. September 2026

Behoben

- **Tag-Filter-Zeilen bleiben beim Auswählen an ihrem Platz** — In der Tag-Filterauswahl der Monitor-Liste wurden Zeilen bisher neu sortiert, wenn Sie Kontrollkästchen anklickten; sie behalten jetzt ihre Position, solange die Auswahl geöffnet ist, und werden nur beim erneuten Öffnen neu geordnet. Siehe Monitore.
- **Vorfallshistorie für aktualisierte Monitore wird automatisch wiederhergestellt** — Nach der Aktualisierung eines Geräts, auf dem Knoten-, Endpunkt- oder Heartbeat-Monitore in Bedingungsmonitore umgewandelt wurden, migriert Pulse die verbleibende behobene Vorfallshistorie schrittweise im Hintergrund, sodass die vollständige Vorkommnisliste ohne weiteres Zutun nach und nach sichtbar wird.

---

5. September 2026

Neu

- **KI-Canvas und MCP können Bedingungsgraphen und Vorfalls-Zeitleisten untersuchen** — Zwei neue MCP-Werkzeuge ermöglichen tiefere Untersuchungen durch den KI-Assistenten: `get_condition` liest den vollständigen Bedingungsgraphen, auf den ein Monitor alarmiert, und zeigt, was jeder Knoten aktuell auswertet und seit wann dieser Wert gilt — so lässt sich erkennen, welcher Eingang den Alarm ausgelöst hat; `list_incident_events` liefert die vollständige Zeitleiste eines Vorfalls: Entscheidungen des Monitors zu Ausfall und Erholung, jede Benachrichtigungszustellung mit Empfänger, Bestätigungen, Eskalationen und Behebungen. Siehe KI-Canvas und Organisationseinstellungen.

Behoben

- **Auf dem Gerät werden nach einem Update crash-loopende Dienste jetzt als nicht in Ordnung erkannt** — Wenn ein Dienst durch ein Update beschädigt wurde, aber so konfiguriert ist, dass er automatisch neu startet, würde ein einzelner Snapshot der fehlgeschlagenen Einheiten ihn verpassen — der Dienst würde endlos zwischen „wird aktiviert" wechseln, und der Update-Bericht würde „Update erfolgreich" melden, obwohl der Dienst defekt ist. Das Gerät nimmt jetzt über ein kurzes Zeitfenster

wiederholt Stichproben des systemd-Zustands und wertet einen Dienst als fehlerhaft, wenn er dabei in einem Crash-Loop angetroffen wird — sodass der Gesundheitsbericht nach dem Update tatsächlich defekte Dienste widerspiegelt.

---

4. September 2026

Neu

- **MCP-Clients verbinden sich jetzt über OAuth** — Anstatt Zugriffstoken manuell zu erstellen, verbinden sich KI-Assistenten und Werkzeuge mit dem MCP-Endpunkt von Pulse über browserbasiertes OAuth: Fügen Sie die Endpunkt-URL (sichtbar unter Organisationseinstellungen → MCP-Clients) zu Ihrem Client wie Claude Code hinzu und genehmigen Sie den Zugriff im Einwilligungsfenster, das sich im Browser öffnet. Organisationsadministratoren können alle autorisierten Clients, die autorisiert haben und wann sie zuletzt verwendet wurden einsehen und den Zugriff jederzeit widerrufen.
- **KI-Canvas und MCP können Datenquellen auflisten** — Der KI-Assistent kann jetzt die Datenquellen Ihrer Organisation und deren Datenpunkte auflisten. So lässt sich abfragen, welche Quellen konfiguriert sind und welche Datenpunkte von keinem Monitor überwacht werden. Siehe KI-Canvas.

Behoben

- **Das Update eines Geräts mit umfangreicher Vorfallshistorie wird jetzt abgeschlossen** — Auf Geräten mit monatelanger Vorfallshistorie konnte das Update, das Knoten-, Endpunkt- und Heartbeat-Monitore in Bedingungsmonitore umwandelt, über eine Stunde laufen und zurückgerollt werden, bevor es fertig war — das Gerät blieb auf der alten Version. Das Update schreibt jetzt nur noch die Vorfälle um, die ihren neuen Schlüssel tatsächlich brauchen — offene sowie behobene innerhalb des Wiedereröffnungsfensters ihres Monitors — statt der gesamten Historie, und das Gerät räumt der Datenbankaktualisierung bis zu einer Stunde ein, bevor es eingreift. Planen Sie für dieses Update ein Wartungsfenster von bis zu einer Stunde ein, wenn Ihr Gerät eine lange Vorfallshistorie hat.
- **MCP-Datengraphen erfinden keine Messwerte mehr zwischen Samples** — In MCP-Antworten wurden ASCII-Sparkline-Diagramme zuvor auf die volle Plotbreite gestreckt, indem zwischen tatsächlichen Samples interpoliert wurde; jetzt werden sie mit der echten Auflösung der Zeitreihe dargestellt, sodass spärliche Datensätze schmaler angezeigt werden statt mit erfundenen Werten aufgefüllt zu werden.

---

2. September 2026

Neu

- **Datenpunkte benennen und beschreiben** — Sie können jedem Datenpunkt jetzt einen lesbaren Namen und eine Beschreibung geben; der Name erscheint überall in der App, wo der Datenpunkt angezeigt wird, und erleichtert die schnelle Identifikation von Messwerten.

Verbessert

- **Monitoranzahl in Datenpunkt-Zeilen** — Auf der Detailseite einer Datenquelle zeigt die Monitore-Spalte jetzt eine einzige Schaltfläche „X Monitore" mit einer durchsuchbaren Auswahl statt einzelner Links pro Monitor — die Seite bleibt übersichtlich, auch wenn viele Monitore auf einen Datenpunkt alarmieren.
- **Infohinweise im Bedingungseditor** — Die Felder „Gültig für" und Fensterdauer im Bedingungseditor haben jetzt -Symbole, die Zweck und Format des Felds erläutern — sichtbar, ohne den Editor zu verlassen. Siehe Monitore.
- **Hinweise zu UND/ODER-Gattern** — UND- (Alle) und ODER- (Ein beliebiger) Gatterknoten im Bedingungseditor zeigen jetzt ein , das ihre Logik beschreibt und den Unterschied zwischen beiden Typen auf den ersten Blick klar macht. Siehe Monitore.
- **Hinweis auf lückige Daten in der Bedingungsvorschau** — Die Bedingungsvorschau weist jetzt darauf hin, wenn ein Signal nur für einen Teil des gewählten Zeitraums Messwerte enthält, sodass ein eingeschränktes Backtest-Ergebnis klar gekennzeichnet ist und nicht mit einem vollständigen verwechselt wird. Siehe Monitore.
- **Tag-Badges zeigen bei Hover die vollständige Bezeichnung** — Wenn eine Tag-Bezeichnung in einer Listenzeile abgeschnitten ist, zeigt ein Tooltip beim Darüberfahren jetzt die vollständige Bezeichnung.

Behoben

- **Beschriftungen der Benutzeroberfläche folgen der gewählten Sprache** — Die Schaltfläche „Schließen" in Dialogen und Seitenpanels sowie die Schaltfläche zum Ein- und Ausblenden der Seitenleiste werden jetzt in der aktiven Sprache angezeigt statt immer auf Englisch.
- **Filterkacheln zeigen keine Zählwerte bei paginierten Listen** — Auf der Datenquellen-Seite zeigen Filterkacheln keine irreführenden Zählwerte mehr, wenn das vollständige Ergebnis größer als eine Seite ist; die Kachel zeigt in diesen Fällen nur die Bezeichnung.

---

1. September 2026

Neu

- **Monitore-Panel auf Datenquellenseiten** — Die Detailseite einer Datenquelle zeigt jetzt einen Abschnitt „Monitore", der alle Monitore auflistet, die auf die Datenpunkte dieser Quelle alarmieren, mit einem direkten Link zum Öffnen des jeweiligen Monitors.
- **Näherungsweise Historie für neue Ziele** — Wenn Sie ein neues Ziel erstellen, berechnet Pulse jetzt eine näherungsweise Compliance-Historie für das Zeitfenster vor der Erstellung und kennzeichnet diese entsprechend, sodass Sie sofort eine aussagekräftige Übersicht sehen statt für den größten Teil des ersten Fensters „Nicht genug Daten". Siehe Ziele.
- **Schalter „Erstellte Monitore aktivieren" im CSV-Import** — Der CSV-Import-Assistent verfügt jetzt über einen Schalter, mit dem Sie wählen können, ob importierte Monitore nach dem Import sofort aktiviert werden oder zur Prüfung pausiert in der Monitor-Liste verbleiben. Siehe Monitor-CSV-Import.

Verbessert

- **Vorfall an einen Bereitschaftsplan eskalieren** — Der Dialog „Eskalieren..." bietet jetzt neben Benutzern und Teams auch Bereitschaftspläne an — dieselben Empfänger wie ein Schritt einer Eskalationsrichtlinie. Der Plan alarmiert diejenigen, die in diesem Moment Bereitschaft haben, und der Eintrag im Aktivitätsprotokoll nennt den gewählten Plan. Siehe Vorfälle.
- **Dauer-Spalte akzeptiert lesbare Zeitangaben** — Im Monitor-CSV-Import akzeptiert das Dauer-Feld jetzt Angaben wie „5m" oder „30s" anstatt einer Anzahl von Sekunden. Siehe Monitor-CSV-Import.

Behoben

- **OPC-UA-Browse nach Fehler erneut versuchen** — Wenn der Dialog „Datenpunkt hinzufügen" beim Laden von Knoten vom OPC-UA-Gerät scheitert, erscheint jetzt eine Schaltfläche „Erneut versuchen", sodass Sie es ohne Schließen des Dialogs nochmals versuchen können.
- **OPC-UA-Browse-Dialog zeigt alle deklarierten Knoten** — Der OPC-UA-Node-Browser hat zuvor einige auf der Quelle deklarierte Knoten ausgelassen; alle deklarierten Knoten werden jetzt korrekt im Browse-Dialog angezeigt.
- **Monitor-CSV-Import prüft Schwellwert-Bedingungen vor dem Schreiben** — Der Importer prüft jetzt generierte Schwellwert-Bedingungen, bevor er sie schreibt, und verhindert so, dass Monitore mit ungültigen Parametern (z. B. negativer Dauer) unbemerkt angelegt werden. Siehe Monitor-CSV-Import.

---

31. August 2026

Neu

- **Betriebszeiten-Gate in Eskalationsrichtlinien** — Eskalationsrichtlinien unterstützen jetzt einen Schritt vom Typ „Betriebszeiten", der die Eskalation an dieser Stelle anhält, bis die konfigurierten Zeiten gelten; außerhalb dieser Zeiten wartet die Richtlinie, und wenn das Fenster wieder öffnet, läuft sie automatisch weiter. Die Pause wird in der Vorfalls-Zeitleiste protokolliert. Siehe Eskalationsrichtlinien.
- **Betriebszeiten umkehren** — Sowohl die persönlichen Benachrichtigungseinstellungen als auch Betriebszeiten-Gate-Schritte verfügen jetzt über einen Schalter „Betriebszeiten umkehren": Wenn er aktiviert ist, gilt das Fenster *außerhalb* der konfigurierten Zeiten statt während ihnen — nützlich für Bereitschaftszeiten, die Nächte und Wochenenden abdecken. Siehe Eskalationsrichtlinien.
- **Nach Eskalationsrichtlinie filtern** — Die Listen für Monitore, Vorfälle, Ziele und Bedingungen haben jetzt einen Filter nach Eskalationsrichtlinie. Siehe Monitore und Vorfälle.
- **Kontextmenü per Rechtsklick auf Vorfallszeilen** — Auf dem Desktop öffnet ein Rechtsklick auf eine Vorfallszeile ein Kontextmenü mit denselben Aktionen wie die Schaltfläche „⋯" der Zeile: Bestätigen, Beheben, Eskalieren und Öffnen.

Verbessert

- **Push-Benachrichtigung bei Bestätigung an andere Responder** — Wenn jemand einen Vorfall bestätigt, erhalten die anderen noch alarmierten Benutzer eine Push-Benachrichtigung, sodass das gesamte Reaktionsteam weiß, dass der Vorfall übernommen wurde. Siehe Vorfälle.
- **Berichtseinträge verlinken auf ihre Live-Seiten** — Monitornamen und andere Entitäten im Berichts-Viewer sind jetzt anklickbare Links, die die entsprechende Live-Seite in der App öffnen. Siehe Berichte.
- **Datenquellenzeilen sind jetzt vollständig anklickbar** — Ein Klick auf eine beliebige Stelle in einer Datenquellenzeile navigiert zur Detailseite, einheitlich mit Monitor- und Vorfallszeilen.
- **Die App bleibt navigierbar, wenn eine Seite abstürzt** — Wenn eine Seite einen unerwarteten Fehler auslöst, bleiben Seitenleiste und Navigation zugänglich und eine klare Fehlermeldung erscheint anstelle der abgestürzten Seite — statt eines leeren Bildschirms, der einen vollständigen Neustart erfordert.

Behoben

- **Baseline-Monitore ermitteln Ziele jetzt korrekt** — Ein Fehler, der dazu führte, dass nächtliche Baselines auf veraltete Monitor-Untertypen statt auf übernommene Datenpunkte verwiesen, wurde behoben; Baseline-Monitore, die zuvor fälschlicherweise „Unzureichende Daten" anzeigten, sollten jetzt korrekt berechnen. Siehe Monitore.

- **Berichts-Snapshots mit fehlenden Feldern öffnen jetzt korrekt** — Berichte, die vor der Einführung der Ziele-Funktion erstellt wurden, werden jetzt wie erwartet gerendert statt fehlzuschlagen, und ein Berichtsabschnitt, der nicht geladen werden kann, zeigt jetzt einen isolierten Fehler statt den gesamten Bericht zu beeinträchtigen. Siehe Berichte.

---

30. August 2026

Neu

- **Karenzzeit für Heartbeats** — Heartbeat-Datenquellen haben jetzt ein konfigurierbares Feld „Karenzzeit", das festlegt, wie viel später ein Ping eintreffen darf, bevor Pulse einen Vorfall auslöst; die Detailseite der Datenquelle zeigt das erwartete Intervall und die Karenzzeit gemeinsam als Auslösedeadline an. Siehe Heartbeat.
- **Ziel durch Klick auf die Zeile öffnen** — Ein Klick auf eine Zielkarte in der Zielliste öffnet jetzt die Detailseite dieses Ziels – einheitlich mit dem Verhalten von Monitor- und Vorfallskarten. Siehe Ziele.
- **„Bedingung öffnen" im Zeilenmenü** — Das Aktionsmenü jeder Zeile in der Zielliste enthält jetzt einen Eintrag „Bedingung öffnen", der direkt zur Bedingung im Editor führt. Siehe Ziele.
- **Prometheus-Reihen als Bedingungssensorknoten** — Prometheus-Reihen können jetzt direkt als Sensorknoten im Bedingungseditor verwendet werden, sodass Sie auf Prometheus-Metriken mit denselben graphbasierten Bedingungen wie bei jeder anderen Datenquelle alarmieren können. Siehe Monitore und Prometheus.
- **Push-Benachrichtigungen zeigen ein Symbol für das Ereignis** — Jede Vorfallsbenachrichtigung beginnt jetzt mit einem Symbol, sodass ein Blick auf den Sperrbildschirm genügt: neuer Vorfall, jemand hat bestätigt, behoben und eine Kollegin oder ein Kollege hat den Vorfall persönlich an Sie eskaliert. Siehe Mobile Benachrichtigungen.

Verbessert

- **Bedingungseditor hat jetzt einen Tab „Zusammenfassung"** — Die textuelle Darstellung einer Bedingung ist jetzt hinter einem eigenen Tab „Zusammenfassung" im Vorschau-Panel zu finden (neben „Vorschau" und „Live"), sodass die lesbare Form des Graphen nicht mehr mit dem Backtest oder den Live-Werten um Platz konkurriert. Siehe Monitore.
- **Speicherfehler im Bedingungseditor benennen das Problem** — Wenn der Server das Speichern einer Bedingung ablehnt, werden die konkreten Probleme jetzt im Chip in der Werkzeugleiste gezählt, an den betroffenen Knoten hervorgehoben und neben

der Speichern-Schaltfläche beschrieben, sodass Sie genau wissen, was zu beheben ist, statt nur „Die Bedingung kann noch nicht gespeichert werden." zu sehen. Siehe Monitore.

- **Lösch-Dialog für Ziele erklärt, was mit der Bedingung passiert** — Die Bestätigung beim Löschen eines Ziels sagt jetzt, ob die Bedingung, um die es ging, mitgelöscht wird (wenn dieses Ziel der einzige Verwender war) oder erhalten bleibt (wenn ein Monitor oder ein anderes Ziel sie noch verwendet). Siehe Ziele.
- **Burndown-Diagramme in Berichten starten eingeklappt** — Das Fehlerbudget-Burndown-Diagramm jedes Ziels im Berichts-Viewer startet jetzt eingeklappt mit einer Schaltfläche „Budgetverlauf anzeigen", damit der Zuverlässigkeitsabschnitt übersichtlich bleibt, bis Sie ihn aufklappen. Siehe Berichte.

---

29. August 2026

Neu

- **Vorfälle manuell an beliebige Benutzer oder Teams eskalieren** — Eine Aktion „Eskalieren..." auf offenen Vorfällen ermöglicht es, bestimmte Personen direkt zu alarmieren und dabei zu wählen, über welche Kanäle (E-Mail, SMS, Anruf oder Push) sie benachrichtigt werden. Die Eskalation ergänzt die automatische Eskalationsrichtlinie und steht sowohl bei unbestätigten als auch bei bestätigten Vorfällen zur Verfügung; nach der Lösung wird die Aktion nicht mehr angeboten. Jede manuelle Eskalation erscheint als eigener Eintrag in der Vorfalls-Zeitleiste. Siehe Vorfälle.

Verbessert

- **Berichte blenden die Vorfallsliste standardmäßig aus** — Der Abschnitt mit den Vorfallsdetails im Berichts-Viewer ist jetzt standardmäßig eingeklappt und zeigt nur die Anzahl der Vorfälle auf der Schaltfläche an, sodass die Berichtszusammenfassung sofort lesbar ist, ohne durch potenziell tausende Zeilen scrollen zu müssen. Bei Bedarf lässt sich die Liste aufklappen. Siehe Berichte.

---

28. August 2026

Neu

- **Eigene Anlage- und Bearbeitungsseite für Bedingungsmonitore** — Das Anlegen eines Bedingungsmonitors erfolgt jetzt über eine eigene Seite unter **Monitore → Neuer Monitor → Bedingungsmonitor**, auf der Eskalationsrichtlinie, Tags und Bedingung von Anfang an erfasst werden. Die Bedingung wird inline über ein

Satzformular beschrieben (für den häufigen Schwellwertfall) oder Sie hängen eine bereits bestehende Bedingung an. Bisher wurde der Monitor über den Bedingungseditor angelegt. Auch das Bearbeiten der Details eines bestehenden Monitors (Richtlinie und Tags) hat jetzt eine eigene Seite. Siehe Monitore.

- **Neue Seite zum Anlegen von Zielen** — Das Anlegen eines Service-Level-Ziels erfolgt jetzt über eine eigene Seite unter **Ziele → Neues Ziel**, auf der Name, Zielwert, Fenster und Abdeckungsuntergrenze zusammen mit einer inline-Beschreibung des Indikators erfasst werden. Bisher war dies im Bedingungseditor möglich. Siehe Ziele.
- **Die Bedingungsliste kann einen Monitor für eine Bedingung anlegen** — Die Zeilenaktion „Monitor erstellen" in der Bedingungsliste führt von einer vorhandenen Bedingung direkt auf die Monitor-Anlageseite, mit dieser Bedingung bereits angehängt. Ein zweiter Monitor auf einer geteilten Bedingung beginnt damit nicht mehr in der Monitor-Liste. Siehe Monitore.

Verbessert

- **Beschreibungen von Trigger-Vorfällen werden jetzt als Markdown gerendert** — Wenn die Regel **Vorfallbeschreibung** eines Trigger-Monitors Text aus der Webhook-Nutzlast extrahiert, wird dieser Text auf der Vorfalldetailseite nun als Markdown gerendert. Der Alarmtext eines Paging-Systems enthält oft Links zu Runbooks, Listen betroffener Anlagen und anderen formatierten Kontext; Markdown lässt diese Formatierung durch. Wenn Beschreibung und Ursache dieselbe Information wiedergeben würden, wird der Ursache-Untertitel ausgeblendet. Siehe Vorfälle.

---

27. August 2026

Neu

- **Bedingungseditor auf Mobilgeräten** — Wenn Sie einem Link zum Bedingungseditor auf einem Smartphone folgen, sehen Sie jetzt eine schreibgeschützte Ansicht der Bedingung: den Graphen, der mit der Live-Auswertung der Appliance für jeden Knoten angezeigt wird, und einen Details-Tab mit Beschreibung, offenen Problemen, Zielen und der Anzahl der Monitore, die die Bedingung verwenden. Siehe Monitore.
- **Live-Werte im Bedingungseditor** — Das Vorschau-Panel des Bedingungseditors hat jetzt einen Tab „Live", der die Echtzeit-Auswertung der Appliance für jeden Knoten der gespeicherten Bedingung zeigt – so sehen Sie genau, welche Werte einen Alarm auslösen, ohne einen Backtest starten zu müssen. Der Tab ist verfügbar, sobald die Bedingung gespeichert wurde und keine ungespeicherten Änderungen vorliegen. Siehe Monitore.

- **Quellzeitstempel für Trigger-Monitore** — Trigger-Monitore können jetzt mit einer Regel „Quellzeitstempel" konfiguriert werden, die ausliest, wann der Sender den Alarm laut eigener Angabe ausgelöst hat; der extrahierte Zeitpunkt erscheint im Zustellungsprotokoll und wird im Aktivitäts-Feed des Vorfalls festgehalten, wenn er sich ändert – so lässt sich erkennen, wann ein Alarm beim Sender und wann er bei Pulse eingegangen ist. Siehe Monitore.

Verbessert

- **Bedingungsliste zeigt aktuellen Status und Nutzungsdetails** — Jede Zeile auf der Bedingungsseite zeigt jetzt einen Statusindikator (Verletzt, Gilt, Unbekannt usw.), wie viele Monitore und Ziele die Bedingung verwenden und wie viele Datenpunkte sie liest; neue Filter ermöglichen es, nach Status oder nur nach ungenutzten Bedingungen zu filtern. Siehe Monitore.
- **Berichts-Detailseite lädt ältere Snapshots auf Anfrage** — Die Liste der bisher generierten Berichte auf der Detailseite eines Berichtsplans zeigt jetzt eine Schaltfläche „Mehr laden", um ältere Einträge seitenweise abzurufen, statt die gesamte Historie auf einmal zu laden. Siehe Berichte.

Behoben

- **Bedingungseditor kann einen unlesbaren gespeicherten Graphen reparieren** — Wenn der gespeicherte Graph einer Bedingung von einem neueren Appliance-Build geschrieben wurde und diese Version ihn nicht dekodieren kann, zeigt der Editor jetzt einen deutlichen Hinweis und ermöglicht es, einen neuen Graphen zu zeichnen und zu speichern, um ihn zu ersetzen, anstatt in einer Sackgasse zu enden. Siehe Monitore.
- **Organisationsauswahl auf Mobilgeräten schließt sich nach der Auswahl** — Das Auswahlblatt für die Organisation auf Mobilgeräten schließt sich jetzt automatisch, wenn Sie eine Organisation auswählen, und hat eine eigene Schließen-Schaltfläche, damit Sie nie in einem offenen Blatt ohne offensichtlichen Ausweg verbleiben.

---

26. August 2026

Neu

- **Auswahlmodus in der Monitor-Liste** — Organisationsadministratoren können auf dem Desktop in der Werkzeugleiste auf **Auswählen** klicken, um den Auswahlmodus zu aktivieren. In diesem Modus wird jede Zeile zu einem auswählbaren Element statt zu einem Link, und eine schwebende Aktionsleiste am unteren Rand bietet **Stummschalten**, **Stummschaltung aufheben** und **Löschen** für die gesamte Auswahl. Drücken Sie Escape, um den Modus zu verlassen — der erste Druck hebt die Auswahl auf, der zweite verlässt den Modus. Siehe Monitore.

- **Trigger-Monitore können jetzt das sendende System identifizieren** — Fügen Sie einem Trigger-Monitor eine Regel „Sendendes System" hinzu, damit zwei Dienste, die sich eine Webhook-URL teilen, getrennte Vorfälle behalten – auch wenn sie dieselbe Alarm-ID senden; das sendende System wird auf jedem erzeugten Vorfall genannt. Siehe Monitore.
- **Trigger-Monitore können Vorfälle jetzt automatisch über ein Reset-Signal schließen** — Fügen Sie eine Regel „Reset-Signal" hinzu, und Pulse schließt sofort alle offenen Vorfälle eines Senders, sobald ein passendes Reset-Signal eingeht. Siehe Monitore.
- **Bedingungsmonitore haben jetzt einen eigenen Eintrag im Seitenbereich** — Bedingungsmonitore erscheinen direkt im Seitenbereich, sodass Sie die vollständige Liste mit einem Klick öffnen können, ohne über einen anderen Abschnitt zu navigieren. Siehe Monitore.
- **Die Bedingungsbibliothek und die Zielliste sind jetzt durchsuchbar** — Geben Sie einen Begriff ein, um eine Bedingung oder ein Ziel nach Name zu finden, statt die gesamte Liste zu scrollen. Siehe Monitore.
- **Tags werden jetzt auf den Listen für Datenquellen und CVEs angezeigt und können dort gefiltert werden** — Jede Listenzeile trägt die jeweiligen Tags, und der Tag-Filter ist in der Werkzeugleiste jeder Liste zu finden, sodass Sie ohne das vollständige Filtermenü nach Tag eingrenzen können — so wie es die Monitor- und Vorfallliste bereits erlauben. Siehe Schwachstellen.

Verbessert

- **Vorfallkarten in der Liste zeigen jetzt die Tags des auslösenden Monitors** — Jede Vorfallkarte in der Liste zeigt neben dem Status-Badge und dem Monitor-Typ auch die Tags des Monitors, der den Vorfall ausgelöst hat. So lassen sich Muster erkennen und filtern, ohne jeden Vorfall öffnen zu müssen. Siehe Vorfälle.
- **Typ-Chips ersetzen die CVE-Schnellfilterschaltfläche** — Eine Chip-Zeile unterhalb der Suchleiste zeigt nun jeden in Ihrer Liste vorhandenen Monitor-Typ mit seiner Anzahl. Klicken Sie auf einen Chip, um nach diesem Typ zu filtern; klicken Sie erneut, um den Filter aufzuheben. Siehe Monitore.
- **Tags-Filter in die Monitor-Werkzeugleiste befördert** — Die Schaltfläche für den Tags-Filter befindet sich nun neben dem Suchfeld und den Typ-Chips statt im Filtermenü, entsprechend seiner Bedeutung als wichtigster Weg zur Einschränkung einer großen Monitor-Liste. Siehe Monitore.
- **„Filter zurücksetzen" löscht den Suchbegriff nicht mehr** — Die Schaltfläche **Filter zurücksetzen** in den Werkzeugleisten der Monitor- und Vorfallliste setzt jetzt nur noch die menügesteuerten Filter zurück (Status, Typ, Tags, Veraltete Daten, Nur stummgeschaltet) und lässt den eingegebenen Suchbegriff unberührt. Siehe Monitore.

- **Die Filter-Schaltfläche jeder Liste zeigt jetzt an, wie viele Filter aktiv sind** — Ein kleines Zähler-Abzeichen erscheint auf der Filter-Schaltfläche, wenn Filter angewendet sind, sodass eine eingeschränkte Liste immer sichtbar ist, ohne das Menü öffnen zu müssen.
- **Gefilterte leere Zustände erklären jetzt, welche Filter aktiv sind** — Wenn eine Filterkombination eine Liste ohne Einträge hinterlässt, nennt der leere Zustand die aktiven Filter und bietet eine Ein-Klick-Schaltfläche zum Löschen an.
- **Suchbegriffe werden jetzt auf weiteren Listen in der URL gespeichert** — Die Eingabe in das Suchfeld einer Liste aktualisiert die URL, sodass eine gefilterte Ansicht als Lesezeichen gespeichert oder geteilt werden kann.
- **Detailseiten passen sich auf schmalen Bildschirmen besser an** — Auf Mobilgeräten wird der Seitentitel nicht mehr von Aktionsschaltflächen zusammengedrückt; er stapelt sich nun sauber unterhalb der Zurück-Schaltfläche, und eingeklappte Aktionen teilen sich die Zurück-Zeile, sodass keine eigene Zeile benötigt wird.
- **Destruktive Aktionen befinden sich jetzt in einem `···`-Überlaufmenü** — Löschen und andere selten benötigte Aktionen auf Detailseiten erscheinen unter einer `···`-Schaltfläche statt in der Hauptschaltflächenleiste, sodass sie einen Klick entfernt sind, aber nicht direkt neben der eigentlichen Arbeit. Siehe Monitore und Vorfälle.
- **Prometheus-Datenpunkte tragen jetzt ihren vollständigen Reihennamen** — Wenn eine Prometheus-Abfrage mehrere Reihen zurückgibt, wird jeder Datenpunkt durch seinen vollständigen Label-Satz statt durch den reinen Metriknamen identifiziert, sodass mehrzeilige Panels ihre Linien unterscheiden können. Siehe Monitore.

Behoben

- **Die Massenaktionsleiste der Monitore überlagert die Listenzeilen nicht mehr** — Die Aktionsleiste, die beim Auswählen von Monitoren erscheint, schwebt jetzt oberhalb der Zeilen darunter, ohne diese zu verdecken.
- **Dialoge schneiden jetzt keine langen Titel oder Fußzeilenschaltflächen mehr ab** — Lange Dialogtitel werden frei vom Schließen-Button gehalten; Aktionsschaltflächen in der Fußzeile bleiben innerhalb des Dialogs; und der „Editor verlassen?"-Bestätigungsdialog passt sich jetzt an seinen Inhalt an.

---

25. August 2026

Verbessert

- **Berichte enthalten jetzt für jedes Ziel ein Fehlerbudget-Burndown-Diagramm** — Jeder Zielabschnitt in einem geplanten Bericht zeigt jetzt ein Diagramm, das darstellt, wie das Fehlerbudget Tag für Tag verbraucht wurde. So können Sie auf einen Blick

erkennen, ob der Budgetverlust in einem kurzen Zeitraum konzentriert oder gleichmäßig über den Berichtszeitraum verteilt war. Siehe Berichte und Ziele.

Behoben

- **Auf dem Gerät werden Software-Updates mit langsamen Datenbankmigrationen jetzt erfolgreich abgeschlossen** — Bisher konnte ein Update mit einer lang laufenden Migration — etwa dem Neuaufbau eines Index für eine umfangreiche Vorfallshistorie — in einer Neustart-Schleife scheitern: Das System hat die App durch eine Zeitüberschreitung beendet, bevor die Migration abgeschlossen war, sie zurückgerollt und den Vorgang anschließend wiederholt, bis das Update abgebrochen wurde. Das Startfenster ist jetzt lang genug, damit Migrationen abgeschlossen werden können.

---

24. August 2026

Behoben

- **Bedingungsvorschau zeigt jetzt Daten für 24-h- und 7-Tage-Bereiche** — Das Vorschaudiagramm im Bedingungseditor zeigte keine Daten, wenn der Zeitbereich „24 h" oder „7 Tage" ausgewählt war. Das Vorschauraster wird jetzt an denselben Bucket-Grenzen ausgerichtet, die der Server verwendet, sodass alle zurückgegebenen Messwerte mit einem Rasterpunkt übereinstimmen und das Diagramm korrekt befüllt wird. Siehe Monitore.
- **Bedingungs- und SLO-Monitore zeigen jetzt ihren Aktivitätsfeed** — Ihre Detailseiten haben jede Statusänderung aufgezeichnet, aber keine davon angezeigt; der Verlauf eines Monitors war damit nur über seine Vorfälle erreichbar. Beide zeigen jetzt denselben Aktivitätsfeed wie die übrigen Typen und dazu ihren aktuellen Status sowie den Zeitpunkt ihrer letzten Prüfung. Verloren gegangen ist nichts: Die Einträge, die Sie nun sehen, wurden die ganze Zeit geschrieben. Siehe Monitore.

---

23. August 2026

Behoben

- **Das Navigieren von Listenansichten zu Detailseiten kehrt nicht mehr zur Liste zurück** — Eine Race Condition sorgte dafür, dass die CVE- und Vorfalls-Listenköpfe die Browser-URL kurz nach dem Navigieren zu einer Detailseite überschrieben und Sie auf der Liste ließen; beide Köpfe stoppen jetzt die URL-Synchronisierung, sobald Sie die Liste verlassen haben.

22. August 2026

Geändert

- **Heartbeats sind jetzt Datenquellen, ihre Monitore ganz normale Monitore** — Ein Heartbeat ist eine Push-Datenquelle: Pulse erfasst von ihr genau ein Signal, „ein Ping ist eingetroffen“, und ein Bedingungsmonitor alarmiert, wenn dieses Signal länger als das eingestellte Intervall verstummt. Ihre vorhandenen Heartbeats wurden für Sie umgewandelt und behalten Namen, Tags, Eskalationsrichtlinie, Vorfallshistorie und Link. **Die Ping-URL hat sich nicht geändert** — an dem, was Sie ausgerollt haben, muss nichts angepasst werden. Angelegt wird ein Heartbeat weiterhin mit denselben zwei Feldern, jetzt unter „Datenquellen“; Ping-URL und Schaltfläche zum Wechseln der URL finden Sie dort auf seiner Seite. Siehe Heartbeat-Monitore.
- **Ein Heartbeat lässt sich jetzt mit allem anderen verknüpfen** — Weil der Ping ein gewöhnliches Signal ist, wird aus „das nächtliche Backup hat sich nicht gemeldet **und** es ist ein Werktag“ eine einzige Bedingung statt etwas, das sich gar nicht ausdrücken ließ. Öffnen Sie den Monitor, der mit dem Heartbeat entstanden ist, und bearbeiten Sie seine Bedingung wie jede andere. Siehe Monitore.
- **Heartbeats kosten weiterhin nichts** — Die Datenquelle eines Heartbeats und ihr einer Datenpunkt bleiben aus den bereitgestellten Zählern Ihrer Lizenz ausgenommen, genau wie Heartbeat-Monitore es immer waren. Ihre Zahlen ändern sich nicht.
- **Der Seitenbereich besteht jetzt aus Datenquellen, Monitoren und Zielen** — Drei Abschnitte für die drei Dinge, die Pulse tut: Datenquellen erfassen, Monitore alarmieren, Ziele sagen zu. Unter **Datenquellen** stehen die Einträge je Protokoll — OPC UA, S7 und Prometheus —, sodass der Eintrag, über den Sie jeden Morgen Ihre SPSen gefunden haben, weiterhin einen Klick entfernt ist, nur einen Abschnitt weiter, und nun die Verbindung samt allem zeigt, was darüber gelesen wird, statt einer Liste von Schwellwerten. **Monitore** öffnet eine einzige flache Liste; Abkürzungen bleiben nur für CVE, Trigger und SLO. Alte Links auf die OPC-UA- und S7-Monitorlisten führen zu den passenden Datenquellen. Siehe Monitore.
- **Tags filtern die Monitor-Liste über eine eigene Schaltfläche** — Da die Einträge je Typ im Seitenbereich entfallen, sind Tags der wichtigste Weg, die Liste einzuschränken. Die Tag-Auswahl liegt deshalb in der Werkzeugleiste neben dem Suchfeld statt im Filtermenü. Ein Bedingungsmonitor übernimmt die Tags der Daten, die er liest — eine SPS einmal zu taggen genügt weiterhin. Siehe Monitore.
- **Bedingungen sind an das untere Ende des Seitenbereichs umgezogen** — Die Bedingungsbibliothek steht jetzt neben Tags und Schweregraden. Eine Bedingung öffnen Sie weiterhin über den Monitor, der auf sie alarmiert; die Bibliothek ist für den Fall gedacht, dass mehrere Monitore oder ein Ziel sich eine Bedingung teilen. Siehe Monitore.

- **OPC-UA- und S7-Verbindungen werden jetzt als Datenquellen angelegt** — Eine SPS oder ein OPC-UA-Server wird unter „Datenquellen“ angelegt — mit Adresse, Zugangsdaten, Zertifikat und Sicherheitseinstellungen an einer Stelle, genau wie ein Prometheus-Endpunkt bisher schon. Es gibt keinen separaten „Endpunkt-Monitor“ mehr, den Sie vorher anlegen müssten. Vorhandene Verbindungen wurden für Sie übernommen und sind dort bereits aufgeführt. Siehe OPC UA und S7.
- **Eine neue Datenquelle alarmiert Sie bei Unerreichbarkeit — sofern Sie nichts anderes sagen** — Beim Anlegen einer Quelle entsteht zugleich ein Bedingungsmonitor namens „<Quelle> nicht erreichbar“. Er ist ein ganz normaler Monitor: Sie können ihn umbenennen, stummschalten, seine Eskalationsrichtlinie ändern, seine Bedingung bearbeiten oder ihn löschen. Wenn Sie keinen möchten, entfernen Sie beim Anlegen einfach das Häkchen. Siehe OPC UA und S7.
- **Das Durchsuchen der Knoten eines Servers und das Anheften seines Zertifikats sind mit der Verbindung umgezogen** — Beides liegt jetzt an der Datenquelle statt an einem Monitor — dort, wo die genutzte Verbindung seit Einführung der Datenquellen ohnehin liegt.
- **Aus einem Gerät ermittelte CVE-Monitore verweisen jetzt auf dessen Datenquelle** — Es ist dieselbe Verknüpfung; sie zeigt nur auf die Quelle statt auf den Monitor, der früher für sie stand.
- **OPC-UA- und S7-Endpunkt-Monitore sind jetzt Bedingungsmonitore** — Alle vorhandenen Endpunkt-Monitore wurden an Ort und Stelle umgewandelt. Sie behalten ihren Namen, ihre Tags, ihre Eskalationsrichtlinie, ihre Vorfallshistorie und ihren Link und sagen jetzt, was sie immer gemeint haben: „Alarm, wenn diese Datenquelle nicht erreichbar ist“. Sie öffnen sich in einem einfachen Formular, nicht in einem Diagramm. Sie müssen für das Update nichts tun. Siehe Monitore.
- **Sie können einen Messwert jetzt mit der Erreichbarkeit seiner Quelle verknüpfen** — Eine Bedingung kann die Erreichbarkeit einer Datenquelle zusammen mit deren Messwerten lesen. „Alarm, wenn der Kessel über 80 °C liegt **und** die SPS antwortet“ ist damit eine einzige Bedingung. Ein gezogenes Kabel löst dann den einen Vorfall aus, der sagt, dass das Kabel gezogen ist — statt eines Vorfalls pro Messwert, der darüber gelesen wird. Siehe Monitore.
- **Umgewandelte Endpunkt-Monitore werden alle fünf Sekunden geprüft** — Ein Endpunkt-Monitor hatte ein eigenes Prüfintervall; eine Bedingung hat das nicht, denn Bedingungen werden im Fünf-Sekunden-Takt von Pulse ausgewertet. Die Erkennung ist dadurch schneller, und eine Verbindung, die immer wieder abreißt, öffnet und schließt Vorfälle häufiger als zuvor. Wenn Ihnen das zu unruhig ist, öffnen Sie die Bedingung und fügen Sie einen Schritt „durchgehend für“ hinzu, damit erst dann alarmiert wird, wenn die Quelle länger nicht erreichbar war. Siehe Monitore.

- **Ein umgewandelter Monitor bleibt still, wenn Pulse selbst keine Antwort hat** — Ein Endpunkt-Monitor hat auch dann einen Vorfall ausgelöst, wenn der OPC-UA- oder S7-Dienst von Pulse selbst ausgefallen war — das las sich, als sei das Gerät ausgefallen, obwohl es das nicht war. Ein umgewandelter Monitor meldet, was er weiß: Er alarmiert, wenn das Gerät ablehnt oder nicht antwortet, und bleibt unverändert, wenn Pulse überhaupt kein aktuelles Ergebnis hat.
- **Eine eigene Vorfallsnachricht an einem Endpunkt-Monitor ist jetzt die Alarmbeschreibung der Bedingung** — War Ihre Nachricht reiner Text, wurde sie wortgleich übernommen. Enthielt sie einen Platzhalter — eine Adresse in doppelten geschweiften Klammern —, wurde sie nicht übernommen: Eine Alarmbeschreibung wird genau so angezeigt, wie sie geschrieben ist — der Platzhalter wäre also unausgefüllt bei Ihnen angekommen. Bereits vor dem Update ausgelöste Vorfälle sind nicht betroffen. Siehe Monitore.

Behoben

- **Übergabe-E-Mails im Bereitschaftsdienst zeigen jetzt die richtige Nachricht** — Im Klartext-Format wurden Übergabe-E-Mails aufgrund eines Template-Fehlers sowohl mit dem Text für den Beginn als auch für das Ende einer Schicht versendet; Empfängerinnen und Empfänger erhalten jetzt nur noch die Nachricht, die ihrer tatsächlichen Übergaberichtung entspricht.
- **Bereit-E-Mails für Berichte enthalten keine falschen Zugangsinformationen mehr** — Im Klartext-Format enthielten Bereit-E-Mails für Berichte unabhängig vom Passwortschutz stets beide Zugangsvarianten; jede E-Mail enthält nun nur noch den zutreffenden Abschnitt.
- **Das Löschen von Monitoren oder Zielen blockiert Sensoren nicht mehr dauerhaft** — Wenn ein durch eine Bedingung gesicherter Monitor oder ein Ziel gelöscht wurde, blieb der Bedingungsdatensatz manchmal erhalten; diese verwaiste Bedingung verhinderte anschließend das Löschen aller Sensoren, die sie gelesen hatte. Bedingungen, deren letzter Verbraucher gelöscht wird, werden jetzt in derselben Operation bereinigt.
- **Das Öffnen oder Aktualisieren der mobilen App zeigt keinen Serverfehler mehr** — Ein Konflikt bei der Registrierung von Geräte-Tokens konnte bei jedem App-Start zu einem Eindeutigkeitsfehler führen, der als dauerhafter „Serverfehler"-Hinweis angezeigt wurde; die Registrierung löscht nun alle veralteten Ansprüche auf das Token, bevor es gespeichert wird.

Entfernt

- **Endpunkt-, Knoten- und Tag-Monitore können nicht mehr angelegt werden** — Alle drei wurden in den letzten beiden Releases in Bedingungsmonitore umgewandelt; die Formulare und API-Endpunkte, die sie angelegt haben, wurden zusammen mit den

dahinterliegenden Tabellen entfernt. Bedingungen leisten alles, was diese Monitore konnten, und lassen sich frei kombinieren — ein Messwert und die Erreichbarkeit seiner Quelle in einer Regel ist genau der Fall, der zuvor nicht ausdrückbar war. Siehe Monitore.

- **Das Löschen eines Monitors wirkt nicht mehr kaskadierend, und Richtlinien und Tags werden nicht mehr „auf untergeordnete Monitore“ übertragen** — Ein Monitor hat keine untergeordneten Monitore mehr. Der Bestätigungsschritt, der ihr Mitlöschen angeboten hat, und die Abfragen, die das Übertragen einer Eskalationsrichtlinie oder eines Tag-Satzes angeboten haben, entfallen damit. Tags an einer Datenquelle gelten weiterhin für alles, was darüber gelesen wird.
- **Der CSV-Import von Monitoren umfasst jetzt nur noch CVE-Monitore** — Die OPC-UA- und S7-Zeilen haben Monitortypen angelegt, die es nicht mehr gibt. Legen Sie diese stattdessen als Datenquellen und Bedingungen an.

---

21. August 2026

Neu

- **Monitore in großen Mengen stummschalten und löschen** — In der Monitorliste können jetzt mehrere Monitore gleichzeitig ausgewählt und mit einer einzigen Aktion stummgeschaltet, entstummt oder gelöscht werden; eine Auswahlleiste erscheint, sobald Monitore ausgewählt sind, mit Schnellauswahl für die gesamte Liste. Siehe Monitore.
- **Vorfälle werden innerhalb des Wiederöffnungsfensters der Eskalationsrichtlinie automatisch erneut geöffnet** — Eskalationsrichtlinien verfügen jetzt über eine Einstellung für das Wiederöffnungsfenster; wenn der Auslöser eines geschlossenen Vorfalls erneut ausgelöst wird, bevor das Fenster abläuft, öffnet Pulse den vorhandenen Vorfall wieder, anstatt einen neuen zu erstellen, und hält die Auflösungsbenachrichtigung zurück, bis das Fenster abläuft. Siehe Eskalationsrichtlinien und Vorfälle.

Verbessert

- **Das Löschen eines Endpunktmonitors entfernt jetzt alle seine Untermonitore in einem Schritt** — Bisher wurde das Löschen eines OPC-UA- oder S7-Endpunktmonitors blockiert, solange Knoten- oder Tag-Monitore daran angehängt waren; der Löschdialog zeigt jetzt die Gesamtzahl der zu entfernenden Monitore an und löscht alles zusammen, nachdem Sie den Namen des Monitors zur Bestätigung eingegeben haben. Siehe Monitore.

Geändert

- **OPC-UA-Node-Monitore und S7-Tag-Monitore sind jetzt Bedingungsmonitore** — Alle vorhandenen Node- und Tag-Monitore wurden an Ort und Stelle umgewandelt. Sie behalten ihren Namen, ihren Schwellenwert, ihre Tags, ihre Eskalationsrichtlinie, ihre Vorfallshistorie und ihren Link und öffnen sich im selben einfachen Formular wie zuvor — „Alarm, wenn der Durchschnitt dieses Werts über die letzten fünf Minuten über 80 liegt" — jetzt zusätzlich mit der Möglichkeit, einen zweiten Messwert hinzuzufügen oder die Erreichbarkeit der Datenquelle einzubeziehen. Sie müssen für das Update nichts tun. Ein neuer Monitor dieser Art wird jetzt im Bedingungseditor statt im alten Node-/Tag-Formular angelegt. Siehe Monitore.
- **Umgewandelte Monitore werden alle fünf Sekunden geprüft** — Ein Node- oder Tag-Monitor hatte ein eigenes Prüfintervall; eine Bedingung hat das nicht, denn Bedingungen werden im Fünf-Sekunden-Takt von Pulse ausgewertet. Ein Monitor, der bisher alle fünf Minuten geprüft wurde, wird jetzt alle fünf Sekunden geprüft. Die Erkennung ist dadurch schneller, und ein Wert, der seinen Schwellenwert mehrfach überschreitet, öffnet und schließt Vorfälle häufiger als zuvor. Wenn Ihnen das für einen bestimmten Monitor zu unruhig ist, öffnen Sie dessen Bedingung und fügen Sie einen Schritt „durchgehend für" hinzu, damit erst dann alarmiert wird, wenn der Messwert anhält. Siehe Monitore.
- **Berichte mit Monitortyp-Filter umfassen jetzt alle Ihre Bedingungsmonitore** — Ein geplanter Bericht, der auf „OPC-UA-Node" oder „S7-Tag" eingeschränkt war, filterte auf einen Monitortyp, den es nicht mehr gibt; sein Filter wurde daher auf „Bedingung" umgeschrieben. Andernfalls wäre der Bericht weiterhin planmäßig verschickt worden, aber leer angekommen. Umgewandelte Monitore und selbst erstellte Bedingungen sind jetzt derselbe Typ, der Filter unterscheidet sie also nicht mehr, und ein so eingeschränkter Bericht enthält nun Bedingungsmonitore, die er vorher nicht umfasste. Um ihn wieder enger zu fassen, öffnen Sie den Bericht und ergänzen Sie einen Tag-Filter — Ihre umgewandelten Monitore haben ihre Tags behalten. Siehe Berichte.

Behoben

- **Die Aggregationen „Summe" und „Anzahl" zählen jetzt Ihre Messwerte statt Zeitraster** — Eine Bedingung mit der Aggregation Summe oder Anzahl hat das interne Auswertungsraster von Pulse gefaltet statt der Messwerte selbst: Ein Messwert wurde für jeden Rasterpunkt erneut gezählt, an dem er noch der aktuellste war. Praktische Folge: Ein Sensor, der nicht mehr meldete, ergab weiterhin die volle Anzahl — eine Bedingung „Anzahl liegt unter N", der übliche Weg, um auf einen verstummten Sensor zu alarmieren, blieb also genau dann still, wenn sie hätte auslösen müssen. Summe und Anzahl zählen jeden Messwert jetzt einmal. Erwarten Sie bei diesen beiden Aggregationen **niedrigere** Werte als bisher; wenn Sie einen Schwellwert gegen den alten Wert eingestellt haben, prüfen Sie ihn. Minimum, Maximum und Durchschnitt sind nicht betroffen. Zwei Schritte sind davon bewusst ausgenommen: „Ersatzwert"

trägt weiterhin jeden Wert bei, den er für fehlende Daten einsetzt, und „Hat Daten" liefert weiterhin eine Antwort pro Rasterpunkt — Bedingungen zum Auffüllen von Lücken und zur Verfügbarkeit zählen also weiterhin Rasterpunkte, denn genau dafür sind sie da. Siehe Monitore.

- **Das Löschen von Eskalationsrichtlinien prüft jetzt korrekt, ob die Richtlinie noch verwendet wird** — Ein Fehler wurde behoben, der das Löschen von Eskalationsrichtlinien erlaubte, die noch von Monitoren oder Vorfällen referenziert wurden, während das Löschen ungenutzter Richtlinien blockiert war. Siehe Eskalationsrichtlinien.

---

19. August 2026

Verbessert

- **Bedingungsknoten zeigen, welchen Wert ein Vorfall nennen wird** — Automatisch generierte Bedingungen (z. B. Banddetektoren, die durch die Anomalieerkennung auf Sensormonitoren erstellt wurden) beschriften jetzt jeden relevanten Knoten — Messwert, Obergrenze oder Untergrenze — auf der Knotenkarte und in der Bedingungsvorschau auf der Monitorseite, sodass Sie auf einen Blick erkennen, auf welche Zahl sich ein Vorfall bezieht, ohne den Editor öffnen zu müssen. Wenn Sie einen gekennzeichneten Knoten im Inspektor auswählen, erscheint dieselbe Bezeichnung unter „Wird in Vorfällen genannt als". Siehe Monitore.
- **Bedingungseditor prüft verschachtelte Zeitfensterketten** — Wenn Aggregationsknoten in Reihe verbunden sind (z. B. ein Durchschnitt, der in einen weiteren Durchschnitt eingespeist wird), prüft der Editor jetzt, ob der gemeinsame Rückblick die Datenaufbewahrungsdauer von Pulse überschreitet, und hebt den ersten Knoten hervor, an dem die Summe die Grenze überschreitet, damit Sie genau wissen, welchen Knoten Sie kürzen müssen. Siehe Monitore.

Behoben

- **Anomalieerkennung: Baseline-Läufe werden jetzt immer abgeschlossen** — Ein Fehler, bei dem das letzte Datenstück jedes Baseline-Laufs den Abschlussschritt nicht auslöste, wurde behoben; Baselines werden jetzt zuverlässig abgeschlossen und liefern ihr vollständiges Ergebnis. Siehe Anomalieerkennung.

---

18. August 2026

Neu

- **Service-Level-Objectives** — Der neue Abschnitt „Ziele" ermöglicht es, eine Zusage über eine Bedingung zu machen – zum Beispiel „Diese muss mindestens 99,5 % der Zeit über die letzten 30 Tage erfüllt sein" –, das Fehlerbudget zu verfolgen und auf einen Blick zu sehen, ob das Ziel eingehalten wird. Legen Sie Budget-Alarme an, um alarmiert zu werden, wenn das Budget zu schnell verbraucht wird. Siehe Ziele.
- **Mehrere benannte Alarme im Bedingungseditor** — Ein einzelner Bedingungsgraph kann jetzt mehrere Alarm-Knoten mit je eigenem Vorfall-Namen und einer Beschreibung enthalten, sodass eine Bedingung unterschiedlich benannte Vorfälle für verschiedene Fehlermodi auslösen kann.

Verbessert

- **Seitenleiste zeigt nur Ihre eigenen Teams** — Der Abschnitt „Teams" in der Seitenleiste listet jetzt nur noch die Teams auf, denen Sie angehören, und blendet sich vollständig aus, wenn Sie kein Mitglied eines Teams sind.

Behoben

- **Die App meldet Sie nicht mehr bei unbezogenen 401-Antworten ab** — Das Sitzungsende wird jetzt präzise erkannt: Die App beendet Ihre Sitzung nur noch, wenn die Authentifizierungsprüfung bestätigt, dass das Token ungültig ist – nicht bei einer ressourcenbezogenen 401-Antwort.

---

15. August 2026

Verbessert

- **Panels des Bedingungseditors können eingeklappt werden** — Die Palette und der Inspektor im Bedingungseditor haben jetzt Einklappschaltflächen, die jedes Panel auf einen schmalen Streifen reduzieren, damit der Graph mehr Platz erhält. Siehe Bedingungen.
- **Bedingungseditor merkt sich Ihr Layout** — Der Einklappzustand beider Seitenpanels, der Graphs-Schalter in der Vorschau und die Höhe des Vorschau-Panels werden jetzt im Browser gespeichert, sodass der Editor genau so geöffnet wird, wie Sie ihn verlassen haben. Siehe Bedingungen.
- **Sensorgraphen zeigen, was Ihre Bedingung tatsächlich vergleicht** — Wenn ein Sensor einen Aggregationsknoten speist, zeigt sein Diagramm in der Bedingungsvorschau jetzt neben den Rohdaten auch die Ausgabe des Aggregationsknotens — den Wert, den Ihr Vergleichsknoten prüft — berechnet mit derselben Bündelung wie die Bedingungsauswertung. Siehe Bedingungen.

- **Sensorgraphen behalten ihre Position beim Laden neuer Daten** — Das Vorschau-Panel bricht beim Wechsel des Zeitbereichs nicht mehr zusammen; jeder Graph zeigt einen Platzhalter, während die Daten geladen werden.
- **Das Überfahren eines Sensorgraphen hebt ihn auf der Zeichenfläche hervor** — Wenn Sie den Zeiger über einen Sensorgraphen in der Bedingungsvorschau bewegen, werden die entsprechenden Knoten auf der Zeichenfläche hervorgehoben.
- **Fadenkreuz auf der Abfrageseite erstreckt sich über alle Aggregationsdiagramme** — Der vertikale Referenzstrich auf der Abfrageseite bleibt jetzt sichtbar, wenn der Zeiger zwischen Aggregationsdiagrammen wechselt, auch über Überschriften und Abstände hinweg, sodass sich Werte verschiedener Aggregationen zu einem Zeitpunkt leicht vergleichen lassen. Siehe Abfrage.

---

14. August 2026

Neu

- **Bedingungsliste** — Eine neue Seite „Bedingungen" zeigt alle gespeicherten Bedingungen an einem Ort, gibt an, wie viele Monitore jede Bedingung verwenden, und ermöglicht das Erstellen neuer sowie das Löschen ungenutzter Bedingungen.
- **Bedingungsmonitore lösen Vorfälle aus und lösen sie auf** — Pulse wertet Bedingungsmonitore jetzt regelmäßig aus; wenn eine Bedingung zu alarmieren beginnt, wird über die Eskalationsrichtlinie ein Vorfall geöffnet, und wenn sie sich wieder beruhigt, wird der Vorfall automatisch geschlossen.

Verbessert

- **Bedingungsmonitore in der Seitenleiste** — Die Monitor-Navigation enthält jetzt einen Eintrag „Bedingungsmonitore", über den Sie direkt zu Monitoren springen können, die auf Ihren Bedingungen basieren – neben OPC-UA-, S7- und anderen Monitortypen. Siehe Monitore.

Behoben

- **Löschen eines von einer Bedingung genutzten Monitors zeigt jetzt eine klare Fehlermeldung** — Der Versuch, einen Monitor zu löschen, von dem eine Bedingung abhängt, erklärt jetzt die Sperrung und fordert Sie auf, den Monitor zuerst aus der Bedingung zu entfernen, anstatt ohne Erklärung fehlzuschlagen.

---

13. August 2026

Neu

- **„Neuester"-Aggregation in PQL** — Der Abfrage-Builder bietet jetzt eine Aggregation „Neuester", die den aktuellsten Sensorwert in jedem Zeitfenster zurückgibt und so den zuletzt erfassten Messwert pro Intervall anzeigt, anstatt eine statistische Zusammenfassung zu liefern. Siehe Abfrage.

---

12. August 2026

Neu

- **Heartbeat-Monitore** — Ein neuer Monitortyp zur Überwachung regelmäßiger Jobs: Konfigurieren Sie ein erwartetes Ping-Intervall, richten Sie Ihren Cron-Job oder geplanten Task auf die erzeugte URL aus, und Pulse öffnet einen Vorfall, wenn der Ping planmäßig ausbleibt. Die Detailseite zeigt den letzten Ping-Zeitpunkt, eine kopierbare Ping-URL und eine Ein-Klick-URL-Rotation zum Invalidieren alter Anmeldedaten. Siehe Heartbeat.
- **Bedingungseditor** — Ein neues visuelles Canvas zum Erstellen von Monitor-Alarmbedingungen: Platzieren und verbinden Sie typisierte Knoten — Sensoren, Monitorstatus, Arithmetik, Vergleiche und Logikgatter — und prüfen Sie in einer Vorschau, wie die Bedingung auf historische Daten reagiert hätte; ein Spiegelstreifen zeigt den vollständigen Ausdruck als lesbaren Text.

---

11. August 2026

Neu

- **Weitere Vorkommen auf der Vorfall-Detailseite** — Die Vorfall-Detailseite zeigt jetzt bis zu zehn frühere Vorfälle, die durch dieselbe Monitorbedingung ausgelöst wurden, jeweils mit Zeitpunkt und Dauer, sodass Sie auf einen Blick erkennen können, ob das Problem wiederholt auftritt. Siehe Vorfälle.

Verbessert

- **Warnung vor dem Lösen eines Vorfalls bei fehlerhaftem Monitor** — Wenn Sie einen Vorfall lösen, während der zugehörige Monitor noch fehlerhaft ist, zeigt Pulse jetzt eine Warnung an, dass innerhalb von Sekunden ein neuer Vorfall entstehen wird; klicken Sie auf „Trotzdem lösen", um fortzufahren. Siehe Vorfälle.
- **Monitor- und CVE-Listenfilter auf Mobilgeräten verwenden eine Vollbild-Schublade** — Die Listenseiten für Monitore und Schwachstellen verwenden jetzt dieselbe Filter-Schublade auf Mobilgeräten wie die Vorfallsliste: Tippen Sie auf „Filter", um alle Filtergruppen zu öffnen, treffen Sie Ihre Auswahl und tippen Sie auf „Anwenden". Siehe Monitore und Schwachstellen.

- **Abfragediagramm-Tooltips zeigen vollständiges Datum und Uhrzeit** — Datenpunkt-Tooltips im Abfragediagramm zeigen jetzt zusätzlich zur Uhrzeit auch Tag, Monat und Jahr an, sodass bei Abfragen über mehrere Tage klar erkennbar ist, auf welchen Tag ein Datenpunkt fällt. Siehe Abfrage.
- **Wiederkehrende Monitore in Berichten auf zehn begrenzt** — Der Abschnitt „Häufigste wiederkehrende Monitore" in einem Berichts-Snapshot zeigt jetzt maximal zehn Monitore und gibt an, wie viele ausgelassen wurden, damit das Panel eine einheitliche Größe behält. Siehe Berichte.

Behoben

- **Geleerte Vorfallsstatus-Filter werden nicht mehr auf den Standard zurückgesetzt** — Wenn alle Statusfilter in der Vorfallsliste entfernt werden und Sie dann die Seite verlassen, wird die Auswahl nicht mehr auf „Unbestätigt + Bestätigt" zurückgesetzt; der explizit geleerte Filter wird jetzt korrekt in der URL gespeichert. Siehe Vorfälle.

---

17. August 2026

Neu

- **Anomalien auf Sensor-Monitoren erkennen** — OPC-UA- und S7-Sensor-Monitore haben jetzt eine Aktion „Anomalien erkennen", die Bedingungs-Monitore anlegt, die überwachen, ob der Sensor keine Werte mehr meldet, außerhalb seines gelernten Normalbereichs liest, einfriert oder ungewöhnlich stark schwankt; jede Prüfung startet im Schattenbetrieb (zeichnet auf, was sie getan hätte, ohne zu alarmieren), damit Sie eine Woche Ergebnisse prüfen können, bevor Sie sie aktivieren. Siehe Anomalieerkennung.

Verbessert

- **KI-Canvas-Board und Chat sind jetzt unabhängige Bereiche** — Das Board enthält nur noch die Erkenntnisse des Assistenten als persistente Karten, die Sie frei verschieben, in der Größe ändern und anordnen können; der danebenliegende Chat-Bereich zeigt das vollständige Gespräch einschließlich Werkzeugaufrufe; und ein leeres Board zeigt jetzt einen Hinweis, was dort erscheint, sobald der Assistent etwas findet. Siehe KI-Canvas.
- **Monitore und Vorfälle nach Bedingungsmonitor-Typ filtern** — Der Typfilter in der Monitorliste und der Vorfallsliste enthält jetzt „Bedingungsmonitore" (und „Trigger" in der Vorfallsliste), damit Sie direkt auf diese Monitore filtern können. Siehe Monitore und Vorfälle.

- **Vorfalls-Eskalation pausiert, wenn das Monitor-Ergebnis unbekannt ist** — Wenn ein Monitor nicht ausgewertet werden kann — zum Beispiel weil sein Sensor keine Daten mehr meldet — hält die Eskalation jetzt an statt weiterhin Bereitschaftsdienst-Mitarbeiter zu benachrichtigen; sie wird automatisch fortgesetzt, sobald der Monitor wieder ein eindeutiges Ergebnis liefert. Siehe Vorfälle.

Behoben

- **Abfrage-Diagramme flimmern nicht mehr beim Bewegen des Fadenkreuzes** — Das Bewegen des Fadenkreuzes löst keine vollständige Neudarstellung aller Diagrammreihen mehr aus und beseitigt damit ein sichtbares Ruckeln bei Diagrammen mit vielen Datenpunkten. Siehe Abfrage.

---

10. August 2026

Sicherheit

- **Berichts-Snapshots sind jetzt Ende-zu-Ende verschlüsselt** — Wenn Pulse einen Berichtslink per E-Mail sendet, wird der Berichtsinhalt jetzt in einem verschlüsselten Envelope versiegelt, bevor er das Gateway erreicht; nur der beabsichtigte Empfänger kann ihn mit dem Passwort aus seiner E-Mail entsperren, und es werden weder Passwort-Hashes gespeichert noch übertragen. Siehe Berichte.

---

9. August 2026

Neu

- **Zähler für offene Vorfälle in der Seitenleiste** — Die Navigationseinträge „Vorfälle" und „Meine Vorfälle" in der Seitenleiste zeigen jetzt ein Live-Abzeichen mit der Anzahl der derzeit offenen Vorfälle an, sodass Sie auf einen Blick sehen, wie viele Vorfälle Ihre Aufmerksamkeit erfordern, ohne die Vorfallsliste öffnen zu müssen. Siehe Vorfälle.

Verbessert

- **PQL-Abfragen nach Tag filtern** — Der Datenpunkt-Selektor im Query Builder ermöglicht es jetzt, Tags neben einzelnen Monitor-Endpunkten auszuwählen; die Abfrage gibt aggregierte Daten für alle Sensoren zurück, die diese Tags tragen, sodass Sie ein Diagramm einfach auf eine Maschinengruppe oder einen Standort einschränken können, ohne Endpunkte einzeln auswählen zu müssen. Siehe Abfrage.

8. August 2026

Verbessert

- **PQL-Abfragen decken historische und Live-Sensordaten nahtlos ab** — Sensordaten werden jetzt alle ~20 Sekunden in einen lokalen Analytics-Lakehouse exportiert, und PQL-Abfragen lesen daraus in einer einzigen Abfrage, die archivierten Verlauf und den Live-Datenschwanz gemeinsam abdeckt und so Lücken zwischen historischen und aktuellen Ergebnissen vermeidet. Siehe Abfrage.
- **Sicherungen der Appliance umfassen jetzt Analytics-Lake-Daten** — Der Sicherungsbefehl der Appliance erfasst jetzt das Analytics-Lake-Verzeichnis zusammen mit dem Datenbank-Dump und stellt es bei der Wiederherstellung wieder her, sodass historische Sensor-Zeitreihendaten über Sicherungszyklen hinweg erhalten bleiben.

Behoben

- **Vorfalls-Markierungen auf der Abfrageseite erscheinen mit dem ersten Ergebnis** — Vorfalls-Overlay-Markierungen werden jetzt vor der Abfrageausführung geladen, sodass sie in derselben Antwort wie die Ergebnisse erscheinen statt erst nach einem zweiten Rendervorgang. Das erneute Ausführen einer unveränderten Abfrage löst jetzt immer eine neue Anfrage aus. Siehe Abfrage.

---

5. August 2026

Verbessert

- **Vorgeschlagene Abfragen öffnen auf Mobilgeräten als Bottom-Drawer** — Auf kleinen Bildschirmen wird das Panel für vorgeschlagene Abfragen auf der Abfrage-Seite jetzt als Bottom-Drawer angezeigt, der Name und Beschreibung jeder Abfrage inline zeigt, sodass Sie per Touch leichter stöbern und Abfragen ausführen können. Siehe Abfragen.
- **CVE-Schweregrad-Diagrammbezeichnungen auf Mobilgeräten lesbar** — Das Schweregrad-Balkendiagramm im CVE-Dashboard dreht seine Achsenbeschriftungen auf kleinen Bildschirmen, sodass sie sich nicht mehr überlappen. Siehe Schwachstellen.
- **Auf der Appliance wird der Fortschritt bei Installation und Updates nun auf Deutsch angezeigt** — Fortschrittsmeldungen während der Installation und Software-Updates erscheinen jetzt auf dem Bildschirm des Betreibers auf Deutsch; das Audit-Log und das Installations-Log bleiben für den Support-Bereich auf Englisch.

- **Auf der Appliance meldet die erneute Anwendung der laufenden Version „Bereits aktuell"** — Wenn ein Update-Bundle das auf der Appliance bereits laufende Systemabbild enthält, wird jetzt korrekt gemeldet, dass keine Änderung vorgenommen wurde, anstatt eine irreführende Erfolgsmeldung anzuzeigen.

Behoben

- **Vorfallslistenzeilen navigieren zuverlässig** — Die Vorfallslistenzeilen wurden mit einer korrekten Klickzielstruktur neu aufgebaut, sodass ein Klick auf die gesamte Zeile zur Vorfall-Detailseite navigiert; das Aktionen-Dropdown und das Status-Badge lösen keine Zeilennavigation mehr aus. Siehe Vorfälle.
- **Eskalationsschritt-Karten zeigen die Schrittnummer** — Jede Schritt-Karte im Eskalationsrichtlinien-Editor zeigt jetzt ihre Nummer an („Schritt 1", „Schritt 2" usw.) statt der allgemeinen Bezeichnung „Schritt". Siehe Eskalationsrichtlinien.
- **Eingabefelder mit Schaltflächen-Addons ragen auf Desktop-Breiten nicht mehr heraus** — Ein Layout-Fehler, bei dem ein Addon-Button auf Desktop-Bildschirmen einen unsichtbaren, aber klickbaren Bereich außerhalb des Feldrahmens erzeugte, wurde behoben.
- **E-Mail-Aktionslinks erreichen Pulse direkt** — Aktionslinks in E-Mails zu Vorfallswarnungen, Digest-E-Mails, Rufbereitschafts-Übergaben und Berichten tragen jetzt `clicktracking="off"`, damit E-Mail-Anbieter diese nicht über eine Tracking-Umleitung umschreiben — Ein-Klick-Aktionen wie „Bestätigen" funktionieren weiterhin unabhängig davon, welcher E-Mail-Dienst die Nachricht zustellt.

---

4. August 2026

Neu

- **Vorfallaktionen auf Mobilgeräten** — Auf kleinen Bildschirmen zeigt die Vorfall-Detailseite jetzt eine große Schaltfläche „Bestätigen" oder „Lösen", die am unteren Bildschirmrand fixiert ist; ein Bestätigungs-Drawer verhindert versehentliche Aktionen, sodass die primäre Aktion erreichbar ist, ohne das Dropdown „Aktionen" öffnen zu müssen. Siehe Vorfälle.

Verbessert

- **Kompakte Vorfallslisten-Toolbar auf Mobilgeräten** — Auf kleinen Bildschirmen ist das Suchfeld jetzt hinter einem Toggle-Symbol verborgen, das beim Antippen den Fokus auf das Eingabefeld setzt; die Schaltfläche „Vorfall erstellen" wechselt zu einem schwebenden Button in der unteren Ecke, und der Filterbutton zeigt nur noch das Symbol — so bleibt die Toolbar übersichtlich. Siehe Vorfälle.

- **Vorschlagslisten im Abfrage-Builder funktionieren korrekt auf kleinen Bildschirmen** — Die Auswahlmenüs im Abfrage-Builder werden nicht mehr am oberen Bildschirmrand abgeschnitten, wenn wenig Platz vorhanden ist, und jede Option hat auf Mobilgeräten ein größeres Berührungsziel. Siehe Abfrage.

Behoben

- **Geplante Berichte enthalten nur Vorfälle aus dem gewählten Zeitraum** — Ein Fehler, durch den Vorfälle außerhalb des Berichtszeitraums in geplanten Vorfallsberichten erschienen, wurde behoben. Siehe Berichte.

---

2. August 2026

Verbessert

- **Vorfallsstatus als beschriftetes Badge angezeigt** — Der farbige Punkt auf den Vorfallskarten in der Liste wurde durch ein Text-Badge ersetzt, das den Status benennt (z. B. „Unbestätigt"), sodass der Status auf einen Blick lesbar ist, ohne auf Farbe angewiesen zu sein. Siehe Vorfälle.
- **App-Header bleibt auf Mobilgeräten beim Scrollen sichtbar** — Die obere Navigationsleiste ist auf Mobilgeräten jetzt fest (sticky), sodass der Menü-Button und die Steuerelemente beim Scrollen immer zugänglich bleiben.
- **Berichtsaktionen in einem Dropdown zusammengefasst** — Die Aktionen „Jetzt erstellen" und „Löschen" auf der Detailseite eines Berichts sind jetzt unter einer einzigen Schaltfläche „Aktionen" zusammengefasst, was den Header übersichtlicher hält. Siehe Berichte.

Behoben

- **Vorfallsursache wird nicht mehr wiederholt, wenn sie dem Titel entspricht** — Wenn die Ursache eines Monitors exakt mit dem Vorfallstitel übereinstimmt, wird sie auf der Vorfallskarte in der Liste oder der Detailseite nicht mehr ein zweites Mal angezeigt. Siehe Vorfälle.
- **Drawer springen auf iOS nicht mehr zur Seite** — In der mobilen App führte das Öffnen eines Drawers (z. B. des Kommentar-Panels) nicht mehr dazu, dass die Seite dahinter nach oben springt; Schaltflächen innerhalb von Drawers reagieren nun wieder korrekt, und ein Tippen auf das Overlay neben dem Drawer schließt diesen zuverlässig.

---

1. August 2026

Neu

- **Tag-Änderungen auf untergeordnete Monitore übertragen** — Wenn Sie die Tags eines OPC-UA-Endpunkt- oder S7-Endpunkt-Monitors speichern, erscheint jetzt ein Dialog, der anbietet, dieselben Hinzufügungen und Entfernungen auf alle untergeordneten Monitore zu übertragen, damit die Tags des übergeordneten und der untergeordneten Monitore ohne einzelnes Bearbeiten synchron gehalten werden können. Siehe Monitore.

Verbessert

- **Trigger-Monitor zeigt einen einheitlichen Aktivitäts-Feed mit Zustellungsdetails** — Die Detailseite des Trigger-Monitors fasst jetzt Webhook-Zustellungen und Statusänderungsereignisse in einem einzigen chronologischen Feed zusammen; Zustellungen in schneller Folge werden zu einem gruppierten Eintrag zusammengefasst, den Sie aufklappen können, und durch Klicken auf „Details" einer Zustellung öffnet sich ein Panel mit dem vollständigen Inhalt (mit JSON-Formatierungsschalter und Kopierschaltfläche), Inhaltstyp, verlinktem Vorfall sowie Navigation zwischen den Einträgen. Siehe Monitore.
- **Berichte können jetzt an Teams gesendet werden** — Der Empfängerabschnitt im Berichtsformular heißt jetzt „Pulse-Benutzer und Teams" und ermöglicht es, ganze Teams als Empfänger hinzuzufügen; die Teammitglieder werden bei jeder Berichtserstellung ermittelt. Siehe Berichte.
- **Löschen eines Berichts erfordert jetzt eine Bestätigung** — Das Löschen eines Berichts zeigt jetzt einen Bestätigungsdialog, der erklärt, dass keine weiteren Berichte mehr erstellt werden und dass bereits versendete Berichte über ihre bestehenden Links weiterhin verfügbar bleiben, um versehentliches Löschen zu verhindern. Siehe Berichte.
- **Große Vorfallstabellen in Berichten scrollen flüssig** — Die Vorfallstabelle in einer Berichtsmomentaufnahme wird jetzt virtualisiert, sodass Berichte mit Hunderten oder Tausenden von Vorfällen ohne Leistungseinbußen dargestellt werden und flüssig gescrollt werden kann. Siehe Berichte.

---

3. August 2026

Verbessert

- **Vorfallsfilter auf Mobilgeräten nutzen eine Vollbild-Schublade** — Auf Mobilgeräten öffnet ein Tippen auf die Filterschaltfläche eine Schublade mit allen Filtergruppen (Status, Typ, Monitor-Typ, Tags, Bestätigt von, Gelöst von) als zusammenklappbare Abschnitte; Auswahlen werden zwischengespeichert und erst nach dem Tippen auf „Anwenden" übernommen, und aktive Filter erscheinen als entfernbare Chips unterhalb der Symbolleiste. Siehe Vorfälle.

- **Bereitschaftskalender hat auf Mobilgeräten einen eigenen Ansichts-Umschalter** — Ein beschriftetes Dropdown ermöglicht die Auswahl von Tag-, Wochen-, Monats- oder Jahresansicht auf kleinen Bildschirmen; der Kalender speichert die Ansichtseinstellung für Mobilgeräte und Desktop separat. Siehe Bereitschaftspläne.
- **Schaltflächen, Eingabefelder und Menüs haben auf Mobilgeräten größere Tippflächen** — Alle interaktiven Elemente erfüllen jetzt die Mindestanforderung von 44 px für Tippflächen auf Touch-Bildschirmen, und Texteingabefelder verwenden mindestens 16 px Schriftgröße, damit iOS Safari beim Fokussieren eines Feldes nicht heran zoomt.

Behoben

- **Zurück-Navigation funktioniert, wenn Seiten über externe Links geöffnet werden** — Die Zurück-Schaltfläche auf Monitor-, Monitor-Bearbeiten- und Vorfall-Detailseiten navigiert jetzt zur jeweiligen Listenansicht, wenn Sie über einen direkten Link (z. B. aus einer Benachrichtigung oder einem Lesezeichen) auf die Seite gelangt sind, anstatt die App zu verlassen.

---

6. August 2026

Verbessert

- **Auf der Appliance werden beim erneuten Anwenden des aktuellen Bundles kein Backup und kein Import mehr durchgeführt** — Wenn das Update-Bundle dieselbe Systemversion enthält, die bereits läuft, erkennt die Appliance dies jetzt unmittelbar nach der Bundle-Prüfung und schließt den Vorgang in Sekunden ab – das Datenbank-Backup und der mehrere Gigabyte große Systemabbild-Import, die zuvor trotzdem ausgeführt wurden, entfallen.

Behoben

- **Auf der Appliance zeigt der Systemstatus jetzt die tatsächliche Betriebszeit** — Der Bildschirm „Systemstatus" zeigt jetzt die tatsächliche Betriebszeit an (z. B. „2h 4m" oder „1d 2h 4m") statt immer „unbekannt". Das `uptime`-Programm der Appliance unterstützt das bisher verwendete Argument nicht; der Bildschirm liest nun direkt aus `/proc/uptime`.
- **Auf der Appliance sind die Rückfallwerte des Systemstatus jetzt lokalisiert** — Der Rückfalltext, der angezeigt wird, wenn Betriebszeit oder Festplattennutzung nicht ausgelesen werden können, erscheint jetzt in der Sprache des Benutzers (z. B. „unbekannt" auf Deutsch) statt immer auf Englisch.

- **Auf der Appliance sind Update-Fehlermeldungen jetzt vollständig in der Sprache des Benutzers** — Der Bildschirm für fehlgeschlagene Updates zeigt Fehlermeldungen jetzt durchgängig in der Sprache des Benutzers an. Zuvor hatte ein Teil der Meldungen eine übersetzte äußere Bezeichnung mit einem nicht übersetzten inneren Detail (z. B. „Überprüfung fehlgeschlagen: checksum mismatch: …").
- **Auf der Appliance wiederholen Signaturprüfungsfehler „signify:" nicht mehr** — Wenn die Bundle-Signaturprüfung fehlschlägt, erscheint die Bezeichnung „signify:" in der Fehlermeldung jetzt genau einmal statt doppelt (zuvor las man „signify: signify: …").
- **Auf der Appliance weist der Bildschirm für vorgemerkte Updates nicht mehr zweimal zum Neustart auf** — Nach dem Vormerken eines Updates, das einen Neustart erfordert, erscheint die Neustart-Anweisung jetzt genau einmal (in der Fußzeile des Abschlussbildschirms) statt zusätzlich im Fortschrittsverlauf.

---

31. Juli 2026

Neu

- **Eskalationsrichtlinie auf untergeordnete Monitore übertragen** — Nach dem Speichern eines Endpunkt-Monitors mit einer geänderten Eskalationsrichtlinie erscheint jetzt ein Dialog, der anbietet, dieselbe Richtlinie auf alle untergeordneten Monitore anzuwenden, damit übergeordnete und untergeordnete Monitore ohne einzelnes Bearbeiten synchron bleiben. Siehe Monitore.

Verbessert

- **Tag-Liste gruppiert Tags nach Kategorie** — Die Tags-Seite zeigt Tags jetzt in zusammenklappbaren Kategorieabschnitten mit Filterchips oben an, sodass Sie sich auf eine Kategorie konzentrieren können; bei einer Suche wird weiterhin eine flache Liste über alle Kategorien angezeigt. Siehe Tags.
- **Trigger-Monitor zeigt den Zeitpunkt der letzten Webhook-Zustellung** — Die Empfangs-URL-Karte auf der Detailseite eines Trigger-Monitors zeigt jetzt an, wie lange der zuletzt empfangene Webhook her ist, sodass Sie die Aktivität der Integration prüfen können, ohne das vollständige Zustellungsprotokoll zu öffnen. Siehe Monitore.
- **Monitor-Ereignisverlauf zeigt 20 Ereignisse pro Seite** — Der Ereignisverlauf auf der Monitor-Detailseite lädt jetzt 20 Ereignisse auf einmal statt 5, sodass Sie ohne häufiges Blättern ein vollständigeres Bild der aktuellen Aktivitäten erhalten. Siehe Monitore.

Behoben

- **Push-Benachrichtigungs-Tippen und Tray-Aktionen funktionieren in der mobilen App jetzt zuverlässig** — Mehrere Fehlerbehebungen bei der Verarbeitung von Benachrichtigungen stellen sicher, dass das Antippen einer Push-Benachrichtigung den richtigen Vorfall öffnet, Tray-Aktionen (Bestätigen/Lösen) zuverlässig beim Gateway ankommen, fehlgeschlagene Aktionen eine Fehlermeldung anzeigen statt lautlos zu verschwinden, und Offline-Aktionen automatisch wiederholt werden, sobald die Verbindung wiederhergestellt ist.

---

30. Juli 2026

Neu

- **Geplante Vorfallsberichte** — Administratoren können jetzt wiederkehrende Berichtsserien (täglich, wöchentlich oder monatlich) erstellen, enthaltene Vorfälle nach Status, Monitor-Typ oder Tag filtern, externe E-Mail-Empfänger sowie Pulse-Benutzer hinzufügen und die Gültigkeitsdauer freigegebener Links festlegen. Berichte werden automatisch nach Plan per E-Mail versendet; Empfänger öffnen sie über einen passwortgeschützten öffentlichen Link. Siehe Berichte.
- **Vorfälle direkt aus dem iOS-Benachrichtigungstray bestätigen oder lösen** — In der mobilen App zeigen Push-Benachrichtigungen für offene Vorfälle jetzt die Schaltflächen „Bestätigen" und „Beheben"; durch Antippen wird der Befehl an Pulse weitergeleitet, auch wenn die App offline ist.

Verbessert

- **Push-Benachrichtigungen können zu mehr Seiten navigieren** — In der mobilen App öffnet das Antippen einer Zusammenfassung oder Übergabe-Benachrichtigung jetzt das richtige Ziel (z. B. die Vorfallsliste oder den Bereitschaftskalender) statt nur zur Vorfall-Detailseite zu führen.

Behoben

- **Pull-to-Refresh leitet nicht mehr zum Dashboard weiter** — In der mobilen App wurde der Benutzer beim Aktualisieren einer Seite per Pull-to-Refresh nicht mehr zum Dashboard weitergeleitet; die App bleibt jetzt auf der aktuellen Seite, indem das Auth-Token ohne Neustart eingeschleust wird.

---

29. Juli 2026

Neu

- **Vorfallsberichte — geplante Zusammenfassungen für Ihr Team** — Die neue Seite Berichte (`/app/reports`) ermöglicht es Administratoren, geplante Vorfallsberichte zu erstellen, die täglich, wöchentlich oder monatlich erzeugt werden. Jeder erstellte Bericht wird zum Zeitpunkt der Erstellung eingefroren und enthält Kennzahlen, Reaktionszeiten (MTTA/MTTR), Volumentrends, Onset-Heatmap, Monitor- und Tag-Aufschlüsselungen, Bereitschaftslast und eine filterbare Vorfallstabelle. Pulse-Benutzer erhalten eine In-App-Benachrichtigung und eine E-Mail mit Link zur angemeldeten In-App-Ansicht; externe Empfänger erhalten einen persönlichen geteilten Link mit Einmalpasswort. Siehe Berichte.
- **Tag-Kategorien — zusammengehörige Tags in Dimensionen gruppieren** — Organisationsadministratoren können jetzt Tag-Kategorien erstellen (z. B. Kunde, Projekt, Standort), die verwandte Tags bündeln; jede Kategorie kann als Einzelauswahl (ein Monitor darf höchstens ein Tag aus dieser Kategorie tragen) oder als Mehrfachauswahl konfiguriert werden. Tags können beim Erstellen oder Bearbeiten einer Kategorie zugewiesen werden; der Tag-Selektor an einem Monitor zeigt die Optionen jetzt nach Kategorie gruppiert und mit Kookkurrenz-Zählern an, damit verwandte Tags schnell zu finden sind. Siehe Tags und Tag-Kategorien.
- **Passwort vergessen / Passwort zurücksetzen** — Die Anmeldeseite hat jetzt einen Link „Passwort vergessen?", über den Benutzer eine E-Mail zum Zurücksetzen des Passworts anfordern können; der Link in der E-Mail öffnet ein Formular, in dem ein neues Passwort gewählt werden kann. Der Link läuft nach einer Stunde ab.
- **Vorfälle nach bearbeitender Person filtern** — Das Filtermenü der Vorfallsliste enthält jetzt die Filter „Bestätigt von" und „Gelöst von", mit denen Sie die Liste auf Vorfälle einschränken können, die ein bestimmtes Teammitglied bearbeitet hat. Ein neuer Eintrag „Meine Vorfälle" in der Seitenleiste verlinkt direkt auf die von Ihnen bestätigten Vorfälle. Siehe Vorfälle.

Verbessert

- **Vorfallsliste zeigt, wer gehandelt hat** — Bestätigte und gelöste Vorfälle zeigen jetzt ein kleines Initialen-Abzeichen in der Zeile; beim Darüberfahren erscheinen Name und Zeitpunkt der Aktion, und ein Klick auf das Abzeichen schränkt die Liste auf die Vorfälle dieser Person ein. Die Vorfall-Detailseite zeigt für die bestätigende oder lösende Person entsprechend einen Initialen-Avatar mit Link zur gefilterten Liste. Siehe Vorfälle.
- **Tag-Filter gruppiert Optionen nach Kategorie** — Beim Filtern von Monitoren, Vorfällen oder CVE-Funden nach Tag werden die Optionen im Tag-Untermenü jetzt nach Kategorieüberschriften gruppiert und zeigen einen Kookkurrenz-Zähler für Tags, die zur aktuellen Auswahl passen, damit die relevantesten Einträge oben erscheinen.

- **Tag-Badges zeigen ihre Kategorie im Tooltip** — Beim Zeigen auf ein Tag-Badge an einem Monitor oder Vorfall erscheint jetzt die zugehörige Kategorie (z. B. „Kategorie: Kunde") zusammen mit einer eventuellen Beschreibung. Siehe Tags.
- **KI-Canvas kann Tags auflisten** — Der KI-Assistent kann jetzt eine Liste von Tags als Canvas-Karte zurückgeben; jede Zeile verlinkt auf die nach diesem Tag gefilterte Monitorliste. Siehe KI-Canvas.
- **CVE-Anbieterstatus unterscheidet Abfragen von Downloads** — Die CVE-Statusseite zeigt jetzt neben „Letzter Versuch" auch einen Zeitstempel „Zuletzt abgefragt", damit Administratoren erkennen können, ob der Feed eines Anbieters regelmäßig geprüft wird (auch wenn sich keine Advisories geändert haben) oder ob er tatsächlich nicht erreichbar ist. Siehe Schwachstellen.

---

28. Juli 2026

Verbessert

- **Bestätigungs-E-Mail mit überarbeitetem Design** — Die Kontobestätigungs-E-Mail verwendet jetzt dasselbe visuelle Design wie andere Pulse-System-E-Mails, mit einem übersichtlicheren Layout und konsistenter Darstellung.

---

27. Juli 2026

Verbessert

- **Aktualisiertes Pulse-Erscheinungsbild in Web- und mobiler App** — Die Web-App zeigt die Pulse-Wortmarke nun in der Seitenleiste und auf den Anmeldeseiten sowie ein aktualisiertes Favicon; die mobile App heißt jetzt „Pulse Dispatch" und zeigt aktualisierte Icons, darunter helle, dunkle und getönte Varianten unter iOS.
- **KI-Canvas-Schrittkarten zeigen keine Verbindungslinien mehr** — Die geschwungenen Pfeile, die Schrittkarten zuvor in der Ausführungsreihenfolge verbunden haben, wurden entfernt; der Canvas wird dadurch übersichtlicher, während die nummerierten Schritt-Abzeichen weiterhin angezeigt werden. Siehe KI-Canvas.

Behoben

- **S7-Monitor-Verbindungen sind zuverlässiger** — Verbindungsaufbauten zu S7-Geräten werden jetzt pro Endpunkt dedupliziert verarbeitet, wodurch redundante gleichzeitige Verbindungsversuche vermieden und mögliche Blockierungen verhindert werden, wenn mehrere Monitore auf dieselbe SPS zeigen. Siehe S7.

21. Juli 2026

Neu

- **Vorfälle und CVE-Funde nach Monitor-Tag filtern** — Die Filter in den Listen für Vorfälle und Schwachstellen enthalten jetzt eine Tag-Option, mit der Sie Ergebnisse auf die Monitore mit einem bestimmten Label einschränken können, ohne die zugehörigen Monitore einzeln kennen zu müssen. Siehe Vorfälle und Schwachstellen.

25. Juli 2026

Neu

- **Trigger-Monitore — Vorfälle aus eingehenden Webhooks auslösen** — Ein neuer Trigger-Monitor-Typ generiert eine eindeutige Empfangs-URL, an die externe Systeme (Grafana, Alertmanager, eigene Skripte) per POST senden können; Pulse wertet die Nutzlast mithilfe konfigurierbarer Regeln (Regex, JSONPath oder Textvergleich) aus, um eine Alarm-ID, einen Vorfallstitel und eine Beschreibung zu extrahieren, und kann den Vorfall automatisch bestätigen oder auflösen, sobald eine passende Nutzlast eingeht. Optionale Request-Header-Abgleicher ermöglichen es, eine eigene Shared-Secret-Authentifizierung vor die Empfangs-URL zu setzen. Die Monitor-Detailseite zeigt die Empfangs-URL mit Kopieren- und Erneuern-Aktionen sowie ein Protokoll der letzten Zustellungen, das anzeigt, wie jeder eingehende Webhook verarbeitet wurde. Siehe Monitore.

19. Juli 2026

Verbessert

- **Schwachstellenseite mit einheitlicher Tab-Leiste** — Die CVE-Seite ist jetzt in vier übergeordnete Tabs unterteilt – Übersicht, CVEs, Funde und Aktivität – und ersetzt damit das bisherige Layout, bei dem Dashboard und ein Umschalter zwischen gruppierter und flacher Ansicht innerhalb eines einzelnen Funde-Tabs verschachtelt waren. Siehe Schwachstellen.

18. Juli 2026

Neu

- **Canvas-Ergebniskarten verlinken direkt zu Monitor-, Vorfall- und CVE-Detailseiten** — Monitore, Vorfälle und CVE-Funde, die der KI-Assistent zurückgibt, sind jetzt anklickbare Zeilen, die die jeweilige Detailseite öffnen, sodass der Canvas dort endet, wo Ihre nächste Aktion beginnt. Siehe KI-Canvas.
- **Canvas-Ausführungsstatus als farbiges Abzeichen in Liste und Wechsler angezeigt** — Ein roter Punkt kennzeichnet einen fehlgeschlagenen Canvas, ein pulsierender bernsteinfarbener Punkt einen noch laufenden – anstelle der unauffälligen grauen Textbeschriftung. Siehe KI-Canvas.

Verbessert

- **KI-Assistent zeigt Zeiten in der Zeitzone der Organisation an** — Wenn der Assistent Zeiten in Fließtext, Tabellen oder Berichten nennt, werden diese jetzt in die lokale Zeitzone Ihrer Organisation umgerechnet (einschließlich des jeweils gültigen Sommerzeit-Offsets), sodass deutsche Betreiber die mitteleuropäische Zeit statt UTC sehen. Siehe KI-Canvas.
- **Canvas-Titel werden in der Sprache der Unterhaltung generiert** — Der automatisch generierte Canvas-Titel entspricht jetzt der Sprache, in der Sie geschrieben haben; ein auf Deutsch begonnener Canvas erhält einen deutschen Titel statt eines englischen. Siehe KI-Canvas.
- **Canvas-Werkzeugkarten zeigen benutzerfreundliche Namen und Icons** — Die KI-Ergebniskarten zeigen jetzt „Monitore", „Vorfälle", „Datenabfrage" oder „CVE-Suche" mit passendem Icon statt des internen Toolnamens. Siehe KI-Canvas.
- **Lange Ergebnislisten in Canvas-Karten werden mit „Weitere anzeigen" begrenzt** — Listen von Monitoren, Vorfällen oder CVE-Funden zeigen zunächst fünf Zeilen; eine Schaltfläche blendet den Rest ein, ohne die Karte unlesbar groß werden zu lassen. Siehe KI-Canvas.
- **Beim Öffnen des Canvas eines anderen Benutzers erscheint jetzt ein Hinweis auf den Nur-Lese-Zugriff** — Wenn Sie einen Canvas öffnen, der einem Kollegen gehört, erklärt der Chat-Bereich, dass nur Lesezugriff besteht, nennt den Eigentümer und bietet einen Link zum Erstellen eines eigenen Canvas an. Siehe KI-Canvas.
- **Eingetippte Nachricht bleibt erhalten, wenn der Assistent noch arbeitet** — Wenn Sie eine Folgefrage senden möchten, während ein Canvas-Durchlauf noch läuft, verbleibt Ihre Nachricht im Eingabefeld und eine Benachrichtigung erklärt, warum sie nicht gesendet wurde – nichts geht lautlos verloren. Siehe KI-Canvas.
- **Erweiterte CVE-Advisory-Abdeckung** — Der CSAF-Aggregator umfasst jetzt CERT@VDE und 39 weitere Hersteller-Feeds, wodurch mehr industrielle CVEs auf der Schwachstellenseite erscheinen. Siehe Schwachstellen.

15. Juli 2026

Neu

- **Schwachstellenliste gruppiert Funde jetzt nach CVE** — Der Tab „Funde" wechselt standardmäßig zur Ansicht „CVEs", die alle Funde jeder Schwachstelle auf Ihren Geräten in einer einzelnen aufklappbaren Zeile zusammenfasst und Schweregrad, Anzahl betroffener Geräte sowie eine Statusübersicht anzeigt; durch Klicken auf eine Zeile werden die einzelnen Funde direkt eingeblendet. Ein Umschalter wechselt zur flachen Ansicht „Funde". Siehe Schwachstellen.
- **Alle Funde einer CVE auf einmal bewerten** — Organisationsadministratoren können jetzt mit der Aktion „Alle bewerten" im Menü der CVE-Zeile eine Bewertungsentscheidung auf alle Funde einer bestimmten CVE über alle Geräte hinweg in einem Schritt anwenden; der Dialog zeigt die Anzahl der zu aktualisierenden Funde an und warnt, wenn aktive Filter dafür sorgen, dass diese Anzahl nur einen Teil aller organisationsweiten Funde umfasst. Siehe Schwachstellen.

---

14. Juli 2026

Verbessert

- **CVE-Fund-Detailseite zeigt jetzt alle betroffenen Geräte** — Die Schwachstellen-Detailseite enthält jetzt ein Panel „Betroffene Geräte", das alle Monitore Ihrer Organisation mit einem Fund für dieselbe CVE auflistet – jeweils mit Bewertungsstatus –, sodass Sie den vollständigen Ausstrahlungsbereich auf einer einzigen Seite überblicken können. Siehe Schwachstellen.

---

13. Juli 2026

Neu

- **Zwischen Canvases wechseln, ohne den Editor zu verlassen** — Ein neues Wechsler-Panel im KI-Canvas-Editor (Ebenen-Symbol in der Kopfzeile) listet alle Ihre Canvases auf, damit Sie direkt zwischen ihnen wechseln können, ohne zur Canvas-Listenansicht zurückzukehren. Siehe KI-Canvas.
- **KI-Canvas-Chat und Canvas-Bereich sind auf Mobilgeräten zugänglich** — Auf kleinen Bildschirmen ermöglicht eine Canvas-/Chat-Tab-Leiste das Umschalten zwischen dem räumlichen Canvas und dem Gesprächsbereich. Siehe KI-Canvas.

Verbessert

- **KI-Canvas-Liste zeigt Ladeplatzhalter und behandelt Fehler korrekt** — Die Canvas-Liste zeigt jetzt Platzhalterzeilen während des Ladens statt kurz den leeren Zustand anzuzeigen; bei Ladefehlern erscheint eine Schaltfläche zum Wiederholen, und bei einer langen Liste wird ein Filtereingabefeld eingeblendet. Siehe KI-Canvas.
- **Canvases erhalten sofort einen Namen aus der ersten Eingabe** — Wenn Sie Ihre erste Nachricht senden, wird der Canvas-Titel direkt aus der Eingabe abgeleitet, sodass der Canvas erkennbar ist, während der Durchlauf läuft oder wenn er fehlschlägt; ein erfolgreicher Durchlauf ersetzt den Namen durch einen vom Modell generierten Titel. Siehe KI-Canvas.
- **CVE-Advisory-Daten werden zuverlässiger abgerufen** — Der CSAF-Abrufdienst verfolgt jetzt jedes Advisory-Dokument einzeln und wiederholt fehlgeschlagene Downloads bei jedem Durchlauf, sodass Lücken durch vergangene Netzwerkfehler nachträglich gefüllt werden statt stillschweigend verloren zu gehen.

---

12. Juli 2026

Verbessert

- **OPC-UA-Monitor-Verbindungseinstellungen in ein dediziertes Seitenpanel verschoben** — Endpunkt-URL, Authentifizierungstyp, Sicherheitskonfiguration und Zertifikatsanheftung werden jetzt gemeinsam in einem Panel „Verbindung konfigurieren" bearbeitet, das über eine kompakte Zusammenfassungskarte im Bearbeitungsformular geöffnet wird. Dadurch werden teilweise gespeicherte Verbindungseinstellungen beim Wechsel zwischen Konfigurationen verhindert. Siehe OPC UA.
- **Das Lösen eines OPC-UA-Serverzertifikats erfordert jetzt eine Bestätigung** — Das Entfernen eines angehefteten Zertifikats im Bearbeitungsformular oder auf der Monitor-Detailseite zeigt jetzt einen Bestätigungsdialog mit einem Hinweis auf die Sicherheitsauswirkungen, um versehentliches Entfernen zu verhindern. Siehe OPC UA.
- **OPC-UA-Verbindungsfehler zeigen jetzt spezifische, handlungsorientierte Vorfallbeschreibungen** — Wenn ein OPC-UA-Monitor keine Verbindung herstellen kann, erstellt Pulse jetzt einen Vorfall mit einer spezifischen Ursache – Server nicht erreichbar, Sicherheits-Handshake fehlgeschlagen, Zertifikat abgelehnt, Authentifizierung fehlgeschlagen oder Zeitüberschreitung – statt einer allgemeinen Fehlermeldung. Siehe OPC UA.
- **Das OPC-UA-Zertifikatsrotations-Panel kennzeichnet den ausstehenden Fingerabdruck** — In den Organisationseinstellungen wird der Fingerabdruck des ausstehenden Ersatzzertifikats jetzt entsprechend gekennzeichnet, um ihn vom aktiven zu unterscheiden, und das Verwerfen eines ausstehenden Ersatzes erfordert einen Bestätigungsschritt. Siehe OPC UA.

11. Juli 2026

Neu

- **OPC-UA-Serverzertifikat per Datei-Upload oder PEM-Einfügen anheften** — Der Bereich zum Anheften von Zertifikaten bei OPC-UA-Endpunkt-Monitoren ermöglicht es jetzt, eine Zertifikatsdatei (PEM oder DER) hochzuladen oder ein PEM direkt einzufügen, sodass Sie das Zertifikat auch dann vorab konfigurieren können, wenn der OPC-UA-Server zum Einrichtungszeitpunkt nicht erreichbar ist. Siehe OPC UA.

Verbessert

- **OPC-UA-Monitor warnt, wenn Anmeldedaten ohne angeheftetes Zertifikat offengelegt werden** — Wenn Sie Benutzername-/Passwort-Authentifizierung auf einem signierten oder verschlüsselten Kanal ohne angeheftetes Zertifikat verwenden, zeigt das Bearbeitungsformular des Monitors jetzt eine Warnung an, dass ein Man-in-the-Middle-Angriff die Anmeldedaten abfangen könnte. Siehe OPC UA.
- **OPC-UA-Monitor warnt, bevor ein veraltetes angeheftetes Zertifikat entfernt wird** — Wenn Sie die Endpunkt-URL eines Monitors ändern, der bereits ein angeheftetes Zertifikat hat, zeigt das Formular jetzt einen Hinweis an, dass das Zertifikat beim Speichern entfernt wird, damit die Änderung nie unbemerkt erfolgt. Siehe OPC UA.
- **Segmentierte Steuerelemente haben ein neues Track-und-Pill-Erscheinungsbild** — Verbundene Umschaltgruppen (z. B. bei der Auswahl von OPC-UA-Sicherheitsmodus und -richtlinie) werden jetzt als einzeln abgerundete Pills innerhalb einer gedämpften Leiste dargestellt, was die ausgewählte Option visuell besser hervorhebt.

Behoben

- **Fehlermeldungen bei OPC-UA-Zertifikatsoperationen erscheinen nicht mehr doppelt** — Wenn ein Anheften oder Upload mit einem Fehler fehlschlägt, den die App bereits zentral behandelt, wird die Fehlermeldung jetzt nur noch einmal angezeigt, nicht mehr zweimal. Siehe OPC UA.

10. Juli 2026

Neu

- **Verwaltung des OPC-UA-Anwendungsinstanzzertifikats** — Unter „Organisationseinstellungen → OPC-UA-Zertifikat" gibt es einen neuen Tab, der das Zertifikat anzeigt, das Pulse bei sicheren OPC-UA-Verbindungen vorlegt, einschließlich SHA-1-Thumbprint zum Abgleich, PEM-Download sowie Aktionen zum Rotieren des

Zertifikats (ein Ersatz wird vorab erstellt, während das aktuelle weiterhin verwendet wird), zum Abschließen einer Rotation durch Umschalten oder zum Widerrufen des aktiven Zertifikats im Notfall; auf den OPC-UA-Monitor-Detailseiten wird bei sicheren Kanälen zusätzlich ein Link zu diesem Tab angezeigt. Siehe OPC UA.

- **Warnmeldungen bei Ablauf des OPC-UA-Anwendungsinstanzzertifikats** — Pulse eröffnet nun 60 Tage vor Ablauf des gemeinsamen OPC-UA-Anwendungsinstanzzertifikats einen Vorfall und benachrichtigt die Administratoren der Organisation per E-Mail; ein ausstehendes Ersatzzertifikat wird automatisch erstellt, damit der Thumbprint vorab hinterlegt werden kann, und nach dem tatsächlichen Ablauf stuft Pulse es automatisch als Absicherung hoch. Siehe OPC UA.

Verbessert

- **Auf der Appliance sind Updates widerstandsfähiger** — Die Gesundheitsprüfung nach einem Update wartet nun bis zu fünf Minuten (bisher 60 Sekunden), was unnötige Rollbacks bei zeitaufwändigen Datenbankmigrationen vermeidet; Updates, bei denen nur periphere Dienste fehlschlagen, Pulse selbst aber gesund antwortet, lösen keinen Rollback mehr aus; und wenn für einen Generationswechsel ein Neustart erforderlich ist, weist die TUI Sie nun klar zum Neustart auf statt scheinbar fehlzuschlagen.
- **CVE-Berichts-E-Mails haben jetzt ein HTML-Layout** — Die wöchentliche Schwachstellen-Berichts-E-Mail enthält nun zusätzlich zur Klartextversion eine gestaltete HTML-Version mit farbcodierten Zählern für offene, in Bearbeitung befindliche, behobene und als Risiko akzeptierte Funde.

---

9. Juli 2026

Neu

- **OPC UA-Endpunkterkennung** — Beim Erstellen oder Bearbeiten eines OPC-UA-Monitors können Sie jetzt auf „Endpunkte erkennen" klicken, um den Server abzufragen und eine Liste der tatsächlich unterstützten Sicherheitskonfigurationen zu erhalten; Pulse wählt standardmäßig die stärkste Option und zeigt das Serverzertifikat mit Antragsteller, Aussteller, Gültigkeitszeitraum und Thumbprint an (mit einer Ablaufwarnung, wenn das Ablaufdatum nah ist oder bereits überschritten wurde). Siehe OPC UA.
- **Serverzertifikat-Anheftung für OPC-UA-Monitore** — Pulse kann das erkannte Serverzertifikat jetzt an einen OPC-UA-Monitor anheften: bei signierten oder verschlüsselten Verbindungen wird es gespeichert und bei jeder Prüfung verifiziert.

Organisationsadministratoren können das angeheftete Zertifikat einsehen, eine erneute Erkennung zur Überprüfung auf Zertifikatswechsel starten, das Zertifikat aktualisieren oder es auf der Monitor-Detailseite vollständig entfernen. Siehe OPC UA.

---

8. Juli 2026

Neu

- **KI fragen direkt aus dem Abfrage-Builder** — Die Sparkle-Schaltfläche im Abfrage-Builder öffnet jetzt den KI-Canvas mit einem vorausgefüllten Prompt, der den Assistenten bittet, eine Abfrage über Ihre Monitoring-Daten zu erstellen, sodass Sie mit einem Klick vom Erkunden der Daten zu einer KI-gestützten Abfrage gelangen. Siehe Abfrage.

Verbessert

- **KI-Canvas-Karten fließen in einer einzelnen horizontalen Reihe** — Canvas-Karten werden jetzt in einem Filmstreifen von links nach rechts angeordnet statt in gestapelten Spalten, sodass der Gesprächsverlauf von einem Schritt zum nächsten leichter zu verfolgen ist. Siehe KI-Canvas.
- **Auf der Appliance lädt die TUI nach einem Update oder Rollback automatisch neu** — Nach einem erfolgreichen Systemupdate oder Generationswechsel startet die Oberfläche automatisch mit der neuen Version neu, anstatt auf der alten Version zu verbleiben.

---

7. Juli 2026

Verbessert

- **KI-Canvas zeigt Schrittfolge mit Nummernabzeichen und Verbindungslinien** — Canvas-Karten zeigen nun eine Sequenznummer in der Ecke und sind durch geschwungene Pfeile in der Ausführungsreihenfolge verbunden; wenn Sie mit der Maus über eine Karte fahren, werden die zugehörigen Verbindungslinien hervorgehoben, damit Sie den Ablauf auf einem überfüllten Canvas nachverfolgen können. Siehe KI-Canvas.
- **Fehlermeldungen bei KI-Canvas-Durchläufen sind jetzt ausklappbar** — Wenn ein Durchlauf fehlschlägt, erscheint ein kompaktes Fehlerbanner am oberen Rand des Canvas; klicken Sie darauf, um die vollständigen Fehlerdetails einzublenden, sodass der Fehler den Canvas nicht mehr verdeckt. Siehe KI-Canvas.

Behoben

- **KI-Canvas-Karten überlappen sich beim Streamen von Inhalten nicht mehr** — Das Canvas-Layout verwendet jetzt die tatsächlich gerenderte Höhe jeder Karte für die Masonry-Anordnung, sodass Karten unterhalb einer wachsenden oder sich ändernden Karte korrekt nach unten verschoben werden statt überlappt zu werden. Siehe KI-Canvas.
- **Auf der Appliance zeigt die TUI-Kopfzeile nach einem Update die korrekte Version** — Die Versionsnummer in der Kopfzeile wird sofort aktualisiert, wenn Sie vom Update- oder Rollback-Bildschirm zurückkehren, ohne dass ein Neustart der TUI erforderlich ist.

---

6. Juli 2026

Neu

- **KI fragen direkt aus einem CVE-Fund** — Die Detailseite jedes CVE-Fundes verfügt nun über eine Schaltfläche „KI fragen", die den KI-Canvas mit einem vorausgefüllten Prompt öffnet, der die Schwachstelle erklärt und das praktische Risiko für das betroffene Gerät in Ihrer Umgebung analysiert. Siehe Schwachstellen.

Verbessert

- **KI-Canvas kann CVE-Funde abfragen und anzeigen** — Der KI-Canvas-Assistent kann jetzt die CVE-Funde Ihrer Organisation durchsuchen und als strukturierte Karten darstellen, sodass Sie schwachstellenbezogene Fragen neben Monitor- und Vorfallabfragen stellen können. Siehe KI-Canvas.

---

4. Juli 2026

Neu

- **Schwachstellenseite** — Ein neuer Bereich „Schwachstellen" in der Navigation listet alle CVE-Funde geräteübergreifend auf, mit einem Dashboard zu Funden nach Schweregrad und Bewertungsstatus, einem Erkennungs-vs.-behobener-Trend-Diagramm, den am stärksten betroffenen Geräten sowie einer durchsuchbaren, filterbaren Fundliste mit einer Detailseite je Fund. Siehe Schwachstellen.
- **CVE-Funde bewerten** — Organisationsadministratoren können auf der Detailseite eines Fundes nun eine Bewertungsentscheidung erfassen (Offen, In Bearbeitung, Behoben, Wird nicht behoben, Nicht betroffen oder Risiko akzeptiert), eine schriftliche Begründung hinterlegen und ein Ablaufdatum für die Risikoakzeptanz festlegen. Siehe Schwachstellen.

- **„KI fragen" auf Listenseiten** — Die Listenseiten für Monitore, Vorfälle und Schwachstellen zeigen nun jeweils eine Schaltfläche „KI fragen", die den KI-Canvas mit einer vorbereiteten Statusberichts-Eingabe für den jeweiligen Bereich öffnet, die Sie vor dem Absenden prüfen und anpassen können.

Verbessert

- **Canvas-Eingabe wächst mit und akzeptiert vorausgefüllte Eingaben** — Das Eingabefeld auf der Canvas-Seite dehnt sich beim Tippen automatisch aus; außerdem können andere Seiten per Deep-Link zum Canvas navigieren und dabei eine vorbereitete Eingabe mitgeben, die Sie vor dem Absenden prüfen oder bearbeiten können.
- **Canvas-Liste behandelt gelöschte Eigentümer korrekt** — Wenn der Ersteller eines Canvas die Organisation verlassen hat, wird in der Liste nun „Gelöschter Eigentümer" angezeigt, anstatt dass der Name leer bleibt oder fehlerhaft dargestellt wird.

Behoben

- **CVE-Vorfallsbezeichnungen zeigen nicht mehr „undefined"** — Fehlende Übersetzungsschlüssel wurden wiederhergestellt, sodass ältere CVE-bezogene Vorfälle nun die korrekten Bewertungsstatusbezeichnungen anzeigen statt roher Schlüsselzeichenketten.

---

3. Juli 2026

Behoben

- **OPC UA-Zertifikatsauthentifizierung funktioniert jetzt mit mehr Servern** — Das von Pulse generierte Application-Instance-Zertifikat enthält nun die von der OPC-UA-Spezifikation geforderten Erweiterungen (ApplicationUri, Schlüsselverwendungen) und überträgt sowohl das Zertifikat als auch den zugehörigen privaten Schlüssel korrekt, wodurch Verbindungsfehler mit mbedTLS-basierten Servern wie open62541 behoben werden. Siehe OPC UA.

---

30. Juni 2026

Neu

- **KI-Canvas** — Eine neue KI-Canvas-Seite ermöglicht es Ihnen, Fragen zu Ihren Vorfällen, Monitoren oder dem Systemzustand zu stellen; der Assistent legt seine Erkenntnisse als Schrittkarten auf einem räumlichen, verschiebbaren Canvas dar. Sie können mehrere Canvases erstellen, umbenennen (der Assistent vergibt nach dem

ersten Durchlauf automatisch einen Titel), frühere Sitzungen in der Canvas-Liste aufrufen und nicht mehr benötigte Canvases löschen. Der KI-Canvas steht Organisationen zur Verfügung, deren Lizenz diese Funktion enthält.

Verbessert

- **Breite Tabellen in Canvas-Karten scrollen statt zu überlaufen** — Tabellen, die der Assistent zurückgibt, werden nun horizontal scrollbar, wenn sie breiter als eine Canvas-Karte sind, sodass die Kartenbreite vorhersehbar bleibt.

---

24. Juni 2026

Behoben

- **Auf der Appliance fragen Backup-Wiederherstellung und Enrollment-Reset nicht mehr nach einem Passwort** — Beide Vorgänge werden jetzt ohne Unterbrechung abgeschlossen; ein fehlender absoluter Pfad für `systemctl` hatte dazu geführt, dass sie auf eine Sudo-Passwortabfrage warteten.

---

23. Juni 2026

Neu

- **Monitore nach Stummschaltung filtern** — Die Monitorliste bietet jetzt einen Filter, um stummgeschaltete Monitore ein- oder auszublenden, damit Sie sich auf die Monitore konzentrieren können, die aktiv alarmieren. Siehe Monitore.

Verbessert

- **Badge für veraltete Daten** — Monitore zeigen jetzt ein Badge an, wenn ihr letzter Messwert veraltet ist. So erkennen Sie auf einen Blick, wenn eine Quelle keine aktuellen Werte mehr liefert. Siehe Monitore.

Behoben

- **Zuverlässige Vorfallaktionen** — Das Bestätigen oder Beheben eines Vorfalls aus einer Benachrichtigung heraus wird bei schnellem Antippen nicht mehr doppelt ausgeführt.

---

21. Juni 2026

Neu

- **Schwachstellen-Überwachung (CVE)** — Pulse kann jetzt Ihre verbundenen Geräte mit einem Katalog bekannter Schwachstellen abgleichen und einen Vorfall öffnen, wenn eine relevante CVE gefunden wird. Enthält eine eigene CVE-Detailansicht, einen manuellen erneuten Scan und CSV-Import für CVE-Monitore. Siehe Monitore.
- **Zusätzliche Zertifikatsnamen auf der Appliance verwalten** — Sie können dem TLS-Zertifikat der Appliance jetzt zusätzliche DNS-Namen und IP-Adressen direkt über das Menü am Gerät hinzufügen, ohne die Appliance neu zu erstellen. Siehe TLS-Zertifikate.

Teil 2 · Einleitung

2.1 Was ist Pulse?

Pulse ist eine Monitoring-Lösung für operationale Technologie (OT)-Infrastruktur. Es bietet Echtzeit-Einblicke in industrielle Steuerungssysteme, einschließlich OPC-UA-Server und Siemens-S7-SPS.

Kernfunktionen

- **Datenquellen** -- Anbindung an OPC-UA-Server, S7-SPS und Prometheus-Endpunkte und kontinuierliches Lesen ihrer Werte
- **Bedingungsüberwachung** -- Alarmierung auf einen Messwert, auf eine ausbleibende Verbindung oder auf beides in einer Regel
- **Vorfallmanagement** -- Automatische Vorfallerstellung bei Problemerkennung, mit Bestätigungs- und Lösungsworkflows
- **Eskalationsrichtlinien** -- Mehrstufige Benachrichtigungsregeln mit konfigurierbaren Schweregraden, Verzögerungen und Empfänger-Teams
- **Teamverwaltung** -- Benutzer in Teams organisieren mit rollenbasierter Zugriffskontrolle (Admin / Mitglied)

Unterstützte Protokolle

OPC UA

Open Platform Communications Unified Architecture ist ein Maschine-zu-Maschine-Kommunikationsprotokoll für die industrielle Automatisierung. Pulse unterstützt:

- Erreichbarkeit des Servers als Signal, das eine Bedingung lesen kann
- Einzelne Knotenwerte
- Sicherheitsmodi: Keine, Signieren, Signieren & Verschlüsseln
- Authentifizierung: Anonym, Benutzername/Passwort, Zertifikat

Siemens S7

Das S7-Kommunikationsprotokoll wird von Siemens-SIMATIC-SPS verwendet. Pulse unterstützt:

- Erreichbarkeit der SPS (IP, Rack, Slot) als Signal, das eine Bedingung lesen kann
- Tag-Werte im S7-Adressformat (z.B. `DB1.DBW0`)

- S7-1200 und S7-1500 Serien

Architekturübersicht

Pulse besteht aus mehreren Komponenten:

- **Webanwendung** -- React-basiertes Dashboard für Monitoring und Konfiguration
- **Backend-Server** -- Haskell-basierter API-Server für Geschäftslogik
- **Protokolldienste** -- Dedizierte Go-Dienste für OPC-UA- und S7-Kommunikation
- **Datenbank** -- PostgreSQL für persistente Speicherung von Monitoren, Vorfällen und Konfiguration

2.2 Erste Schritte

> Richten Sie die Pulse-Appliance vom ISO-Abbild ein? Beginnen Sie stattdessen mit der Appliance-Installationsanleitung — diese Seite beschreibt die anschließende Einrichtung auf Anwendungsebene.

Diese Anleitung führt Sie durch die Ersteinrichtung von Pulse nach der Installation.

Erste Anmeldung

Öffnen Sie nach der Bereitstellung von Pulse die Weboberfläche in Ihrem Browser. Sie sehen die Anmeldeseite.

Wenn Sie noch kein Konto haben, klicken Sie auf **Registrieren**, um eines zu erstellen.

Konto erstellen

1. Navigieren Sie zur Registrierungsseite
2. Geben Sie Ihre E-Mail-Adresse ein und wählen Sie ein Passwort
3. Ihr Passwort muss die folgenden Anforderungen erfüllen:
   - Zwischen 8 und 64 Zeichen
   - Mindestens ein Großbuchstabe
   - Mindestens ein Kleinbuchstabe
   - Mindestens eine Zahl
   - Mindestens ein Sonderzeichen

Passwort vergessen?

Wenn Sie Ihr Passwort vergessen haben, klicken Sie auf der Anmeldeseite auf **Passwort vergessen?** und geben Sie Ihre E-Mail-Adresse ein. Falls ein Konto für diese Adresse existiert, sendet Pulse Ihnen einen Link zum Zurücksetzen des Passworts. Der Link läuft nach einer Stunde ab.

Organisation einrichten

Nach der Registrierung werden Sie aufgefordert, Ihre Organisation zu erstellen. Eine Organisation ist der übergeordnete Container für Ihre gesamte Monitoring-Konfiguration.

1. Geben Sie Ihren Organisationsnamen ein
2. Wählen Sie Ihre Zeitzone

Nächste Schritte

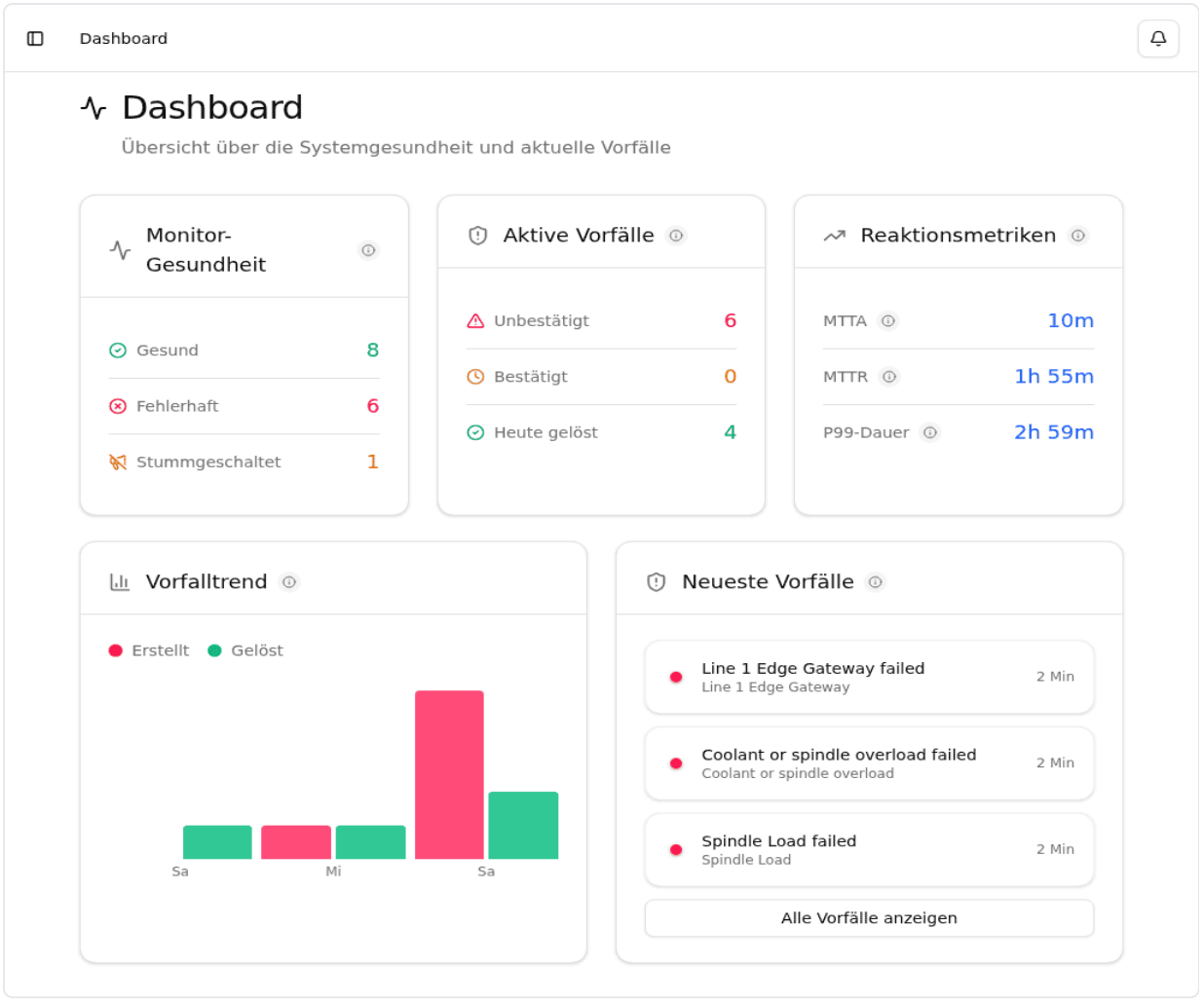
Sobald Ihre Organisation eingerichtet ist, können Sie:

- Ihren ersten Monitor konfigurieren
- Teams einrichten
- Eskalationsrichtlinien erstellen
- Ihre Einstellungen anpassen

Teil 3 · Monitoring

3.1 Dashboard

Das Dashboard bietet einen Echtzeit-Überblick über Ihre gesamte Monitoring-Infrastruktur auf einen Blick.



Monitor-Zustand

Der obere Bereich zeigt den aktuellen Zustand aller konfigurierten Monitore:

- **Gesund** -- Monitore, die innerhalb der erwarteten Parameter arbeiten
- **Fehlerhaft** -- Monitore, die Probleme erkannt haben
- **Stummgeschaltet** -- Monitore, die vorübergehend stummgeschaltet sind

Aktive Vorfälle

Der Vorfallbereich zeigt den aktuellen Status offener Vorfälle:

- **Unbestätigt** -- Neue Vorfälle, die Aufmerksamkeit erfordern
- **Bestätigt** -- Vorfälle, die gesehen aber noch nicht gelöst wurden
- **Heute gelöst** -- Vorfälle, die am aktuellen Tag gelöst wurden

Reaktionsmetriken

Das Dashboard verfolgt wichtige Vorfallreaktionsmetriken der letzten 7 Tage:

- **MTTA** -- Mittlere Zeit bis zur Bestätigung: Durchschnittliche Zeit von der Vorfallerstellung bis zur ersten Bestätigung
- **MTTR** -- Mittlere Zeit bis zur Lösung: Durchschnittliche Zeit von der Vorfallerstellung bis zur Lösung
- **P99 Dauer** -- 99. Perzentil der Vorfalldauer

Vorfalltrend

Ein Diagramm zeigt den Trend der erstellten im Vergleich zu gelösten Vorfällen der letzten 7 Tage. Dies hilft zu erkennen, ob Ihr Team mit eingehenden Vorfällen Schritt hält.

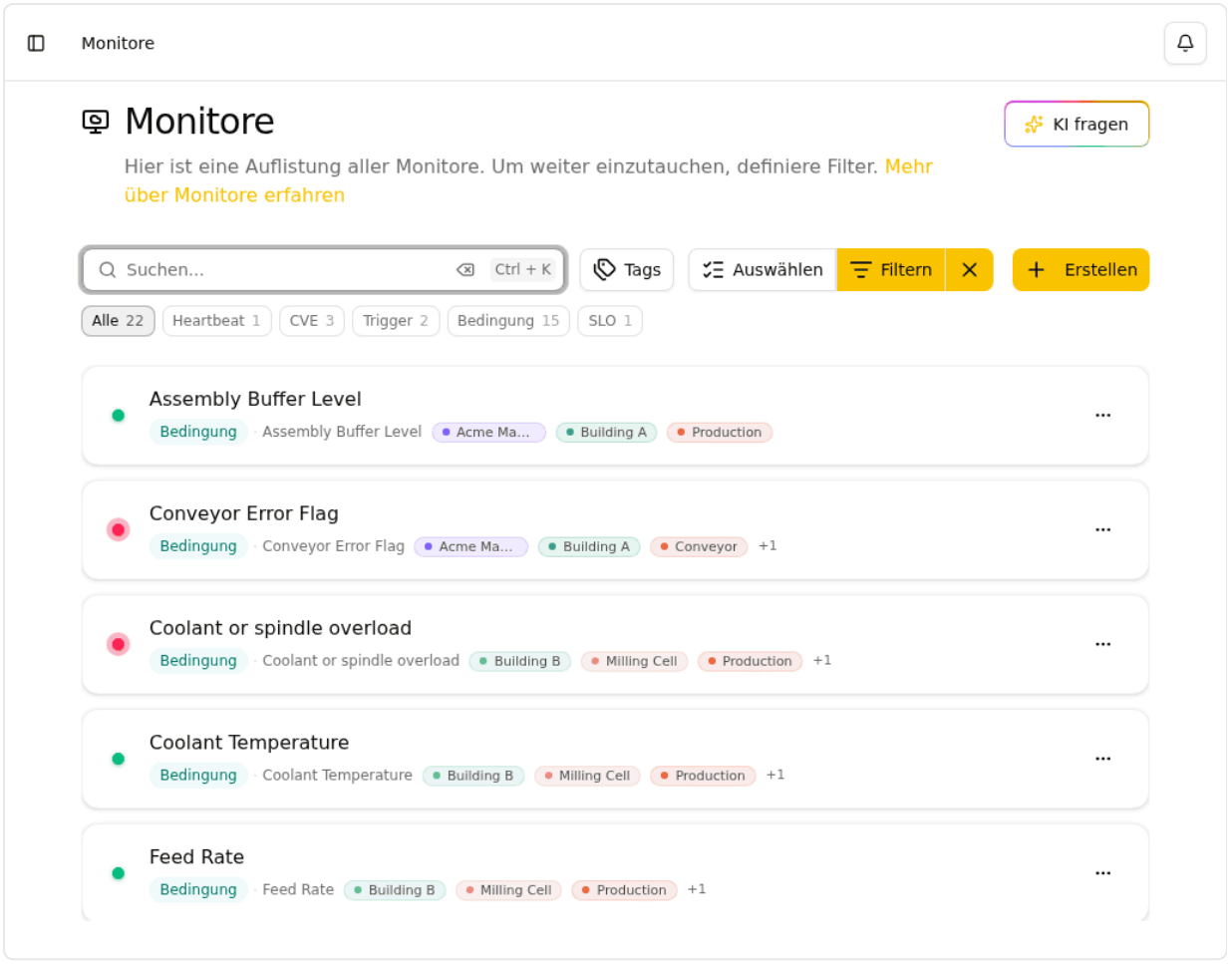
Letzte Vorfälle

Der untere Bereich zeigt die drei aktuellsten Vorfälle mit ihrem aktuellen Status und bietet schnellen Zugriff auf die dringendsten Probleme.

Teil 3 · Monitoring

3.2 Monitore

Monitore sind die Kernbausteine von Pulse. Jeder Monitor überwacht einen bestimmten Aspekt Ihrer OT-Infrastruktur und erstellt Vorfälle, wenn Probleme erkannt werden.



Monitor-Typen

Pulse unterstützt verschiedene Arten von Monitoren:

Bedingungsmonitor

Wertet eine **Bedingung** aus -- einen visuellen Ausdruck aus Messwerten von Datenpunkten, Monitorzuständen und Logikknoten -- und löst einen Vorfall aus, wenn der Ausdruck wahr ist. Mit diesem Monitortyp alarmieren Sie auf alles, was Pulse von einem OPC-UA-Server, einer S7-SPS oder einem Prometheus-Endpunkt liest.

Einen Bedingungsmonitor anlegen:

Öffnen Sie **Monitore → Neuer Monitor → Bedingungsmonitor**. Die Anlageseite erfasst die monitoreigenen Felder zusammen mit der Bedingung:

- **Name** -- Anzeigename des Monitors
- **Eskalationsrichtlinie** -- Welche Richtlinie beim Auslösen der Bedingung greift
- **Tags** -- Optionale Tags zur Kategorisierung
- **Bedingung** -- Wird inline über ein Satzformular beschrieben (für den häufigen Schwellwertfall), oder Sie hängen über **Vorhandene Bedingung verwenden** eine bereits bestehende Bedingung an

Das Satzformular deckt den Alltagsfall ab -- einen Messwert, der eine Grenze überschreitet. Alles, was ein Satz nicht ausdrücken kann, verlinkt in den vollständigen Bedingungseditor, wo Sie anschließend auch Änderungen vornehmen.

Falls die Bedingung bereits vorhanden ist (etwa weil ein zweiter Monitor mit einer anderen Eskalationsrichtlinie auf dieselbe Bedingung alarmieren soll), wählen Sie diese über **Vorhandene Bedingung verwenden** aus. Die Bedingung ist auf diesem Weg schreibgeschützt -- Änderungen daran erfolgen im Editor.

Einen vorhandenen Bedingungsmonitor bearbeiten:

Öffnen Sie die Detailseite des Monitors und klicken Sie auf **Bearbeiten**. Das Bearbeitungsformular zeigt die aktuelle Eskalationsrichtlinie und die Tags des Monitors; die Bedingung selbst wird schreibgeschützt angezeigt und öffnet sich über einen Link im Editor.

Eine einzelne Bedingung kann mehreren Monitoren zugrunde liegen, jeder mit einer eigenen Eskalationsrichtlinie. Die Bedingung wird alle fünf Sekunden ausgewertet. Der Monitorzustand wird auf **Fehlerhaft** gesetzt, wenn die Bedingung auslöst, auf **Gesund**, wenn sie sich wieder legt, und auf **Unbekannt**, wenn Daten fehlen oder ein Zeitfenster leer ist. Ein unbekanntes Ergebnis lässt einen offenen Vorfall offen -- Pulse behandelt „keine Daten" nicht als Entwarnung.

Beim Anlegen einer OPC-UA- oder S7-Datenquelle entsteht ein solcher Monitor automatisch mit dem Namen *<Datenquelle> nicht erreichbar*, sofern Sie den Haken beim Anlegen nicht entfernen. Er ist von Anfang an ein ganz gewöhnlicher Bedingungsmonitor.

Fehlerursache einer Datenquelle ermitteln

Wechselt eine Datenquelle in den Zustand **Fehlerhaft**, zeigt Pulse genau an, warum — nicht nur, dass sie nicht mehr funktioniert. Die Ursache erscheint an zwei Stellen:

- **Datenquellenliste** — der Tooltip des Badges **Fehlerhaft** enthält eine einzeilige Erklärung.

- **Detailseite der Datenquelle** — ein Banner unterhalb des Headers zeigt die Ursache als Überschrift, den Zeitpunkt, ab dem die Datenquelle fehlerhaft ist, sowie die Rohmeldung des Geräts oder der Verbindungsschicht. Die Rohmeldung ist in der Vorschau abgeschnitten; sie lässt sich aufklappen oder in die Zwischenablage kopieren.

Vorfälle, die ein Monitor „Datenquelle nicht erreichbar" auslöst, enthalten die spezifische Ursache auch in ihrer Beschreibung, sodass Bereitschaftstechniker dieselbe Information sehen, ohne die Datenquellenseite öffnen zu müssen.

Mögliche Ursachen und ihre Bedeutung:

Ursache	Bedeutung
Nicht erreichbar	Der Verbindungsversuch ist auf Netzwerkebene fehlgeschlagen. Prüfen Sie Adresse und Port sowie den Betriebszustand des Geräts.
Zeitüberschreitung	Die Verbindung wurde hergestellt, das Gerät hat aber aufgehört zu antworten. Das Gerät ist möglicherweise ausgelastet oder das Netz instabil.
Schutzschalter offen	Wiederholte Fehler haben Pulse veranlasst, die Erfassung vorübergehend auszusetzen. Sie wird automatisch wieder aufgenommen — es ist keine Aktion erforderlich.
Zertifikat abgelehnt	Bei OPC UA: Der Server hat das Anwendungsinstanzzertifikat von Pulse abgelehnt — stufen Sie es auf dem Server als vertrauenswürdig ein, siehe OPC-UA-Sicherheit. Bei symbolischem S7: Es ist noch kein SPS-Zertifikat bestätigt, oder die SPS legt ein anderes vor.
Sicherheits-Handshake fehlgeschlagen	Bei OPC UA: Sicherheitsmodus oder -richtlinie stimmen nicht mit dem Angebot des Servers überein. Bei symbolischem S7: Der TLS-Handshake kam nicht zustande, meist eine SPS, deren Firmware älter ist als das Protokoll.
Sicherheitsmodus nicht unterstützt	Der OPC-UA-Server unterstützt den konfigurierten Sicherheitsmodus nicht. Prüfen Sie die Endpunktliste des Servers und passen Sie die Sicherheitseinstellungen an.
Authentifizierung fehlgeschlagen	Die Zugangsdaten wurden abgelehnt oder sind erforderlich, aber nicht konfiguriert. Prüfen Sie Benutzername, Passwort oder Bearer-Token. Bei einer symbolischen S7-SPS verlangt ihre Schutzstufe, dass sich der Client legitimiert.

Ursache	Bedeutung
Adressierung abgelehnt	Die S7-SPS hat die Verbindung abgelehnt — Baugruppenträger und Steckplatz stimmen mit keiner ihrer CPUs überein. Prüfen Sie die konfigurierten Werte.
PDU-Aushandlung fehlgeschlagen	Die S7-SPS konnte sich auf keine PDU-Größe einigen. Das ist selten und kann auf ein Firmware- oder Konfigurationsproblem der SPS hinweisen.
Lesevorgang abgelehnt	Die S7-SPS hat die Rückgabe der angeforderten Datenbausteine verweigert. Prüfen Sie, ob die Datenbaustein-Adressen existieren und ob externe Lesezugriffe erlaubt sind. Bei einer symbolischen Quelle verweigert die Schutzstufe der SPS den Lesezugriff.
Collector kann Protokoll nicht lesen	Der dieser Quelle zugewiesene Collector kann dieses Protokoll nicht lesen — sein Build ist älter als die Funktion. Aktualisieren Sie den Collector oder weisen Sie die Quelle einem passenden zu.
Firmware nicht unterstützt	Die Firmware der SPS liegt außerhalb des Bereichs, den das symbolische S7-Protokoll unterstützt; sie kann nicht per Tag-Name gelesen werden. Lesen Sie sie als klassische S7-Datenquelle über absolute Adressen.
DNS-Auflösung fehlgeschlagen	Der Hostname in der Prometheus-Scrape-URL konnte nicht aufgelöst werden. Prüfen Sie, ob der Hostname korrekt ist und ob der DNS-Server der Appliance ihn auflösen kann.
Unerwarteter HTTP-Status	Der Prometheus-Endpunkt hat mit einem anderen HTTP-Status als 200 geantwortet. Der Status-Code steht in der Rohmeldung. Ein 401 oder 403 deutet in der Regel auf fehlende oder falsche Zugangsdaten hin.

Fehlt die Ursache oder lautet sie **Nicht einordbar**, läuft an der Datenquelle ein älterer Collector, oder der Fehler ist vor der Einführung der Ursachenverfolgung aufgetreten — prüfen Sie in diesem Fall die Rohmeldung.

CVE-Monitor

Verfolgt veröffentlichte Common Vulnerabilities and Exposures (CVEs), die ein bestimmtes Gerät betreffen. Pulse prüft den Sicherheitsmeldungskatalog regelmäßig und stellt jede zutreffende CVE als **Fund** im Bereich Schwachstellen dar, wo Sie ihn bewerten können.

- **Hersteller** -- Gerätehersteller (z.B. Siemens)
- **Bestellnummer** -- Gerätebestellnummer / MLFB, der genaueste Abgleich mit Sicherheitsmeldungen (z.B. `6ES7518-4AX01-0AB0`). Optional, wenn ein Produktname angegeben ist.
- **Produktname** -- Der Produkt- oder Modultypname in der Schreibweise der Hersteller-Sicherheitsmeldungen (z.B. `SIMATIC S7-1500 CPU 1518-4 PN/DP`). Findet Meldungen, die ein Produkt statt einer Bestellnummer nennen. Optional, wenn eine Bestellnummer angegeben ist.
- **Firmware-Version** -- Optional. Schränkt Treffer auf Meldungen ein, die diese spezifische Firmware-Version betreffen.

Mindestens eine der Angaben **Bestellnummer** oder **Produktname** ist erforderlich.

Wenn Ihre Organisation das Asset-Register nutzt, können Sie stattdessen ein **Asset aus dem Register** und dann das **Modul** wählen. Bestellnummer und Firmware stammen dann vom Modul und folgen ihm bei jedem Scan. Siehe Gerät aus dem Asset-Register übernehmen.

Ein CVE-Monitor wird als **fehlerhaft** angezeigt, solange er einen Fund mit dem Status **Offen** oder **In Bearbeitung** enthält. Auf der Detailseite des Monitors führt jeder passende Fund über **Fund anzeigen** direkt zu seinem Eintrag auf der Schwachstellen-Seite.

> **INFO**
>
> CVE-Überwachung erfordert eine Lizenz, die CVE-Überwachung enthält. Wenn Ihre Lizenz diese Funktion nicht enthält, zeigt die CVE-Monitor-Erstellungsseite eine Informationsmeldung an. Wenden Sie sich an Ihren Administrator, um sie zu aktivieren.

OPC-UA-Alarms-&-Conditions-Monitor

Nicht von Ihnen angelegt: Pulse erstellt automatisch einen, benannt *<Quelle> Alarms & Conditions*, sobald Sie Alarms & Conditions für eine OPC-UA-Quelle zum ersten Mal einschalten, und jeder Alarm dieser Quelle löst gegen ihn einen Vorfall aus. Er ist **Fehlerhaft**, solange ein Alarm der Quelle aktiv ist. Das vollständige Bild — einschließlich der schweregradbasierten Eskalations-Weiterleitung und dessen, was mit ihm passiert, wenn der Schalter der Quelle ausgeschaltet wird — finden Sie unter OPC-UA-Konfiguration → OPC-UA-Alarme & Bedingungen.

Trigger-Monitor

Empfängt eingehende Webhooks von externen Systemen und erstellt Vorfälle in Pulse. Wenn Sie einen Trigger-Monitor erstellen, generiert Pulse eine eindeutige **Empfangs-URL**. Externe Systeme senden beliebige Text- oder JSON-Nutzdaten per POST an diese

URL; Pulse wertet sie mit den von Ihnen konfigurierten Regeln aus und erstellt, aktualisiert, bestätigt oder löst Vorfälle entsprechend auf.

Grundkonfiguration:

- **Name** -- Anzeigename des Monitors
- **Eskalationsrichtlinie** -- Welche Eskalationsrichtlinie beim Erstellen eines Vorfalls verwendet wird

Auswertungsregeln für Nutzdaten:

Jede Regel extrahiert einen Wert oder prüft eine Bedingung im eingehenden Anforderungstext. Verfügbare Modi sind **Regex** (mit optionaler Capture-Gruppe), **JSONPath** und (nur für Bedingungen) **Enthält Text**.

- **Alarm-ID** -- Identifiziert einen Vorfall über mehrere POSTs hinaus eindeutig und ermöglicht Deduplizierung, Bestätigung und Auflösung. Wenn keine Alarm-ID-Regel festgelegt ist, erstellt jeder POST einen neuen Vorfall.
- **Sendendes System** -- Benennt das System, von dem eine Meldung stammt, damit zwei Sender, die sich eine Empfangs-URL teilen, getrennte Vorfälle behalten -- auch bei gleicher Alarm-ID. Lassen Sie die Regel leer, wenn nur ein System an diesen Monitor sendet.
- **Quellzeitstempel** -- Extrahiert den Zeitpunkt, zu dem der Alarm laut sendendem System ausgelöst wurde (Alertmanagers `startsAt`, das `created`-Feld eines Ticket-Webhooks und Ähnliches). Akzeptierte Formate sind RFC 3339 mit ausdrücklichem UTC-Offset, Epoch-Sekunden und Epoch-Millisekunden; alles andere, auch ein Wert ohne Zeitzone, gilt als nicht auswertbar. Wird im Vorfallverlauf und im Zustellungsprotokoll angezeigt -- siehe Wenn die Uhr des Absenders von der Uhr von Pulse abweicht unten. Optional und unabhängig von Alarm-ID oder sendendem System.
- **Vorfalltitel** -- Extrahierter Text als Vorfalltitel. Fällt auf den Monitor-Namen zurück, wenn nicht konfiguriert oder kein Treffer vorliegt.
- **Vorfallbeschreibung** -- Optionaler extrahierter Text, der als Vorfallbeschreibung gespeichert wird.
- **Bestätigt, wenn** -- Eine Bedingung, die bei Erfüllung einen offenen Vorfall mit derselben Alarm-ID bestätigt. Erfordert eine konfigurierte Alarm-ID.
- **Aufgelöst, wenn** -- Eine Bedingung, die bei Erfüllung einen offenen Vorfall mit derselben Alarm-ID auflöst. Erfordert eine konfigurierte Alarm-ID. Auflösung wird vor Bestätigung geprüft.
- **Reset-Signal** -- Eine Bedingung, die bei Erfüllung alle offenen Vorfälle schließt, die dieser Monitor noch für das sendende System hält. Erfordert eine Regel für das sendende System. Das Reset-Signal wird vor Auflösung und Bestätigung geprüft; eine

Meldung, die darauf zutrifft, wird nie zusätzlich als Alarm gelesen.

Mehrere Systeme hinter einer URL

Eine Empfangs-URL wird häufig an mehr als ein System weitergegeben -- zwei Werke, zwei Cluster, mehrere Alarmgruppen. Solche Systeme verwenden meist dieselben allgemeinen Alarm-IDs (`NodeDown` , `DiskFull` , ein Alarmname ohne Standortkennzeichnung). Ohne eine Regel für das **sendende System** kann Pulse zwei solche Meldungen nicht unterscheiden: Sie teilen sich einen Vorfall, die Auflösung des einen Systems schließt ihn für beide, und die Bereitschaft sieht einen Vorfall, wo tatsächlich zwei Probleme vorliegen.

Konfigurieren Sie **Sendendes System** so, dass etwas pro Sender Unterschiedliches extrahiert wird -- eine Standortkennung, ein Clustername, der Schlüssel der Alarmgruppe -- und jeder Sender erhält eigene Vorfälle. Der Wert wird am Vorfall und im Zustellungsprotokoll angezeigt, sodass eine kopierte Konfiguration, die an zwei Standorten denselben Wert stehen lässt, sichtbar wird statt unbemerkt zu bleiben.

Richten Sie die Regel ein, solange der Monitor ruhig ist. Bereits offene Vorfälle wurden erfasst, bevor Pulse die Sender unterscheiden konnte, und gehören daher zu keinem Sender -- sobald die Regel steht, schließt weder eine Auflösung noch ein Reset eines sendenden Systems sie. Der Editor weist Sie darauf hin, wenn der Monitor solche Vorfälle hält; lösen Sie diese von Hand auf.

Pulse übernimmt das sendende System so, wie es in den Nutzdaten steht, und überprüft es nicht: Wer an die Empfangs-URL senden kann, kann sich als beliebiger Sender ausgeben und damit die Vorfälle eines anderen Senders zurücksetzen. Die maßgebliche Grenze ist die URL; das sendende System ist nur eine Zuordnung innerhalb dieser Grenze. **Wenn zwei Systeme einander nicht beeinflussen können sollen, richten Sie getrennte Trigger-Monitore ein** -- die Trennung leisten getrennte URLs, nicht unterschiedliche Werte für das sendende System.

Ein System neu beginnen lassen

Ein System, das neu startet, neu ausgerollt oder umkonfiguriert wird, kann den Überblick darüber verlieren, was es bereits gemeldet hat. Seine Vorfälle bleiben dann dauerhaft offen und der Monitor dauerhaft rot, weil nie etwas eintrifft, das sie auflöst. Mit dem **Reset-Signal** sagt eine Integration: *„Ich habe meinen Zustand verloren -- schließe, was du noch für mich hältst."*

Ein Reset schließt nur die Vorfälle des Systems, das ihn gesendet hat, und nur solche, die bei seinem Eintreffen bereits offen waren. Zwei Dinge lässt er bewusst unberührt:

- **Bestätigte Vorfälle.** An diesen arbeitet bereits jemand; ein Reset nimmt sie nicht weg, sie bleiben in Ihrer Hand.
- **Alles von anderen Sendern desselben Monitors.**

Ein Reset ist keine Entwarnung. Die Vorfälle werden geschlossen, weil ihr Nachweis fehlt, nicht weil Pulse eine Erholung beobachtet hätte -- ein Zustand, der in der Anlage weiterhin besteht, wird durch einen Reset des meldenden Systems trotzdem geschlossen. Deshalb werden diese Schließungen im Vorfallverlauf als eigene Ereignisart erfasst und sehen nicht wie eine gewöhnliche Auflösung aus; das Zustellungsprotokoll zeigt zudem, wie viele Vorfälle jeder Reset geschlossen hat.

Legen Sie zusammen mit Reset ein Wiederöffnungsfenster fest

Ein System, das zurücksetzt, meldet unmittelbar danach fast immer erneut, was weiterhin gestört ist -- genau darum geht es bei einem Neustart. Was dann passiert, hängt vom **Wiederöffnungsfenster** der Eskalationsrichtlinie des Monitors ab, das **null beträgt, solange Sie es nicht festlegen**.

Mit einem Wiederöffnungsfenster öffnet jede erneute Meldung den Vorfall wieder, den sie kurz zuvor geschlossen hat: derselbe Vorfall, dieselbe Bereitschaft, dieselbe Position in der Eskalation, und niemand wird erneut benachrichtigt. Ohne ein solches Fenster sind die Schließungen endgültig, und jede erneute Meldung beginnt einen neuen Vorfall, der von vorn benachrichtigt -- aus einem Reset von vierzig Alarmen werden vierzig neue Alarmierungen.

Der Monitor-Editor warnt Sie, wenn eine Reset-Regel bei einer Richtlinie ohne Wiederöffnungsfenster konfiguriert ist. Siehe Eskalationsrichtlinien.

Wenn die Uhr des Absenders von der Uhr von Pulse abweicht

Pulse berichtet darüber, *wann es von einem Alarm erfahren hat* -- nicht darüber, wann der Absender behauptet, dass er aufgetreten ist. Eskalationszeiten, SLAs, Vorfalldauern und jeder Bericht laufen ausschließlich nach dem Zeitpunkt, zu dem die Zustellung eingetroffen ist -- immer nach der eigenen Uhr von Pulse. Eine **Quellzeitstempel**-Regel ändert daran nichts; sie fügt die Behauptung des Absenders als zusätzlichen Beleg hinzu, niemals als Ersatz.

Ist die Regel konfiguriert, erscheint der Wert im Vorfallverlauf mit der Kennzeichnung **Gemeldet vom Absender**, direkt neben der Differenz zum tatsächlichen Empfangszeitpunkt bei Pulse -- zum Beispiel „Gemeldet vom Absender: 14:03, 4 Minuten bevor Pulse ihn empfangen hat." Meldet eine spätere Zustellung für denselben Alarm einen abweichenden Wert gegenüber dem bereits erfassten, erhält diese Änderung einen eigenen Eintrag im Verlauf -- ein Absender, der sich selbst korrigiert oder dessen Uhr während des Vorfalls driftet, wird so sichtbar statt stillschweigend überschrieben.

Eine große oder negative Differenz -- der Absender behauptet einen Zeitpunkt *nach* dem tatsächlichen Empfang bei Pulse -- bedeutet fast immer, dass die Uhr des sendenden Systems falsch geht, nicht dass Pulse etwas verpasst hat. Pulse zeigt diese Differenz

unverändert an, statt sie zu verbergen oder zu begrenzen, denn genau das Aufdecken einer falsch gehenden Absenderuhr ist der Zweck der Anzeige.

Die Regel wirkt sich stets nur auf den Vorfall aus, den sie auslöst oder wieder öffnet; ein Wert, der fehlt oder nicht ausgewertet werden kann, lässt den Alarm einfach ohne erfassten Quellzeitstempel unberührt -- er blockiert die Zustellung nicht, wie es eine falsch konfigurierte Alarm-ID-Regel könnte.

Request-Header:

Sie können einen oder mehrere HTTP-Header für jeden eingehenden POST verlangen. Alle konfigurierten Header müssen übereinstimmen, damit Pulse die Anforderung akzeptiert — ein fehlender oder nicht übereinstimmender Header führt zu einer 401-Antwort. Damit lässt sich eine eigene Shared-Secret-Authentifizierung vor die Empfangs-URL setzen (z.B. `X-API-Key: ihr-secret` verlangen). Verfügbare Vergleichsmodi: **Gleich**, **Enthält Text** und **Regex**.

Empfangs-URL und Zustellungsprotokoll:

Die Detailseite des Monitors zeigt die Empfangs-URL mit den Schaltflächen **Kopieren** und **URL erneuern**. Ein **Letzte Zustellung**-Zeitstempel zeigt an, wann der letzte Webhook empfangen wurde; wenn noch keine Zustellung eingegangen ist, lautet die Anzeige *Noch keine Zustellung empfangen*. Das Erneuern der URL macht die alte sofort ungültig — aktualisieren Sie alle Systeme, die an sie senden.

Eingehende Webhook-Zustellungen erscheinen im Aktivitätsfeed neben Statusänderungs-Ereignissen. Jeder Zustellungseintrag zeigt das Ergebnis (Vorfall erstellt, aktualisiert, bestätigt, aufgelöst, ignoriert, Vorfall wieder geöffnet oder zurückgesetzt), die extrahierte Alarm-ID, das sendende System (sofern eines gelesen wurde) und eine Schaltfläche **Details**. Ein Reset-Eintrag zeigt statt eines Links auf einen einzelnen Vorfall, wie viele Vorfälle er geschlossen hat. Über **Details** sehen Sie die Nutzdaten wie empfangen, den Content-Type, eine formatierte Ansicht (sofern verfügbar) und einen direkten Link zum zugehörigen Vorfall. Mehrere Zustellungen, die in kurzer Folge eingehen, werden zu einem Eintrag zusammengefasst — klicken Sie auf **Alle N anzeigen**, um die Gruppe aufzuklappen. Ein Hinweis am Ende des Feeds markiert den Punkt, ab dem ältere Zustellungen nicht mehr vorgehalten werden.

> **TIP**
>
> Behandeln Sie die Empfangs-URL als Geheimnis. Jeder, der sie kennt, kann an Ihren Monitor senden. Verwenden Sie Request-Header-Matcher, um eine zusätzliche Authentifizierungsebene hinzuzufügen.

Heartbeat-Monitor

Überwacht einen Job, der nach Zeitplan läuft -- ein nächtliches Backup, einen stündlichen Export, ein Edge-Gerät, das sich regelmäßig meldet. Der Job ruft nach jedem erfolgreichen Durchlauf eine geheime **Ping-URL** auf, und Pulse löst einen Vorfall aus, sobald der Ping ausbleibt. Als einziger Monitortyp wartet Pulse hier, statt eine Verbindung aufzubauen -- die richtige Wahl für alles, was Pulse nicht direkt erreichen kann.

- **Name** -- Anzeigename des Monitors, üblicherweise der Name des Jobs
- **Erwartetes Intervall** -- Wie lange Pulse auf einen Ping wartet, bevor ein Vorfall ausgelöst wird (mindestens 1 Minute)
- **Eskalationsrichtlinie** -- Welche Eskalationsrichtlinie beim Ausbleiben des Pings greift

Die Ping-URL ist ein Geheimnis: Wer sie kennt, kann einen Heartbeat fälschen. Der Ping muss **hinter** dem Job stehen und darf nur bei Erfolg ausgeführt werden. Die vollständige Anleitung -- einschließlich der korrekten Einbindung in Cron -- finden Sie unter Heartbeat-Monitore.

SLO-Monitor

Ein Ziel ist selbst ein Monitor: Es trägt eine Eskalationsrichtlinie, Tags und einen Stummschalter und benachrichtigt jemanden, wenn sein Fehlerbudget zu schnell aufgebraucht wird. Es lebt im Bereich **Ziele**, nicht in dieser Liste — die Budget-Alarm-Staffel liegt neben dem Versprechen, das sie überwacht. Siehe Ziele → Benachrichtigt werden für die vollständige Anleitung.

Bedingungen

Bedingungen sind wiederverwendbare Graphen, die die Logik dafür ausdrücken, wann ein Monitor alarmieren oder ein Versprechen messen soll. Eine Bedingung ist ein gerichteter azyklischer Graph aus typisierten Knoten -- Datenpunkte, Aggregationen, Vergleiche, Logikgatter und ein oder mehrere Ausgangsknoten -- den Pulse anhand von Live-Daten auswertet.

Der Eintrag **Bedingungen** am unteren Ende des Seitenbereichs, neben Tags und Schweregraden, öffnet die Bedingungsliste unter `/conditions`. Er steht dort und nicht unter Monitore, weil eine Bedingung vor allem die Bearbeitungsoberfläche des Monitors ist — Sie erreichen sie über den Monitor, der auf sie alarmiert; die Bibliothek ist für den Fall gedacht, dass mehrere Monitore oder ein Ziel dieselbe Bedingung teilen.

Jede Zeile der Liste zeigt:

- Einen **Statuspunkt**, der das aktuelle Ergebnis der Bedingung widerspiegelt: **Gilt nicht** (rot), **Gilt** (grün), **Unbekannt**, **Veraltet** (wird nicht ausgewertet) oder **Nie ausgewertet**
- Wann die Bedingung zuletzt aktualisiert wurde
- Wie viele **Datenpunkte**, **Monitore** und **Ziele** sie verwenden
- Ein **Aktionen**-Menü (die Schaltfläche `···`) mit Verknüpfungen zum Öffnen der Bedingung, zum Wechsel zu den Monitoren, die auf sie alarmieren, zu den Zielen darüber sowie zum Löschen

Nutzen Sie den Filter **Status**, um die Liste auf Bedingungen mit einem bestimmten Ergebnis einzugrenzen, oder die Umschaltung **Von nichts verwendet**, um Bedingungen zu finden, auf die kein Monitor oder Ziel aktuell verweist. Administratoren können mit **Neue Bedingung** eine neue Bedingung anlegen oder eine vorhandene löschen. Eine Bedingung kann nicht gelöscht werden, solange ein Monitor auf sie alarmiert oder ein Ziel etwas darüber zusagt; entfernen Sie diese zuerst.

Mehrere Bedingungen auf einmal löschen

Administratoren der Organisation können mehrere Bedingungen in einem Zug aufräumen. Die Mehrfachauswahl gibt es nur am Desktop.

Klicken Sie in der Werkzeugleiste auf **Auswählen**, um in den Auswahlmodus zu wechseln. Jede Zeile wirkt dann als Kontrollkästchen, und die ganze Zeile ist das Ziel — ein Klick wählt die Bedingung aus, statt sie zu öffnen. Das Kontrollkästchen **Alle N Bedingungen auswählen** über der Liste wählt alle Zeilen des aktuellen Filters aus oder hebt die Auswahl auf; mit gedrückter **Umschalttaste** nimmt ein Klick alle Zeilen zwischen der zuletzt geklickten und dieser hinzu. Eine Änderung an den Filtern hebt die Auswahl auf. Zum Verlassen klicken Sie erneut auf **Auswählen** oder drücken **Escape** — der erste Druck hebt die Auswahl auf, der zweite verlässt den Modus.

Sobald mindestens eine Bedingung ausgewählt ist, erscheint am unteren Rand der Liste eine schwebende Leiste mit **Löschen** und einem **×**, das die Auswahl aufhebt. Löschen öffnet einen Bestätigungsdialog, in dem Sie die Anzahl der zu löschenden Bedingungen eintippen.

Es gilt dieselbe Regel wie beim einzelnen Löschen, und zwar für die gesamte Auswahl: Eine Bedingung, auf die ein Monitor alarmiert oder über die ein Ziel etwas zusagt, kann nicht gelöscht werden. Ist auch nur eine ausgewählte Bedingung noch in Verwendung, wird gar nichts gelöscht — der Dialog nennt dann, welche Bedingungen gehalten werden und wovon, und bietet an, stattdessen den Rest der Auswahl zu löschen. Die Umschaltung **Von nichts verwendet** zusammen mit **Alle auswählen** ist der schnellste Weg, Entwürfe und Übriggebliebenes zu entfernen, da in dieser Liste nichts blockiert sein kann.

Ein Klick auf den Namen einer Bedingung öffnet deren Graphen im Bedingungseditor. Dort können Sie:

- Den Knotengraphen auf der Arbeitsfläche aufbauen oder ändern
- Vorschau ansehen, wann die Bedingung in einem vergangenen Zeitraum ausgelöst hätte (**Vorschau**-Modus)
- Die aktuelle Live-Auswertung des gespeicherten Graphen durch die Appliance einsehen (**Live**-Modus)
- Die Bedingung speichern und optional einen Monitor anhängen oder aktualisieren

Layout des Bedingungseditors

Der Editor ist in drei Hauptbereiche von links nach rechts gegliedert: die **Palette** (Knotentypen, die Sie auf die Arbeitsfläche ziehen), die Arbeitsfläche selbst und der **Inspektor** (Eigenschaften und Probleme des ausgewählten Knotens).

Sie können beide Seitenbereiche einklappen, um der Arbeitsfläche mehr Platz zu geben. Klicken Sie auf den Umschalter am Rand der Palette oder des Inspektors, um ihn zu einer schmalen Leiste einzuklappen; klicken Sie erneut auf die Leiste, um ihn wiederherzustellen. Der Editor merkt sich, welche Bereiche Sie geöffnet oder geschlossen hatten, sodass Ihr Layout beim nächsten Öffnen wiederhergestellt wird — dies wird pro Browser gespeichert und folgt Ihnen nicht auf ein anderes Gerät.

Der **Vorschaubereich** am unteren Rand zeigt Datenpunktdiagramme für den von Ihnen gewählten Zeitraum. Sie können den oberen Rand ziehen, um seine Höhe anzupassen. Die eingestellte Höhe wird ebenfalls pro Browser gespeichert und an die aktuelle Fenstergröße angepasst, wenn Sie den Editor auf einem anderen Bildschirm öffnen.

Gelernter Normalbereich — Enthält der Graph eine Anomalieprüfung **Außerhalb des normalen Bereichs**, zeichnet ihr Diagramm zusätzlich den gelernten Normalbereich als zwei gestrichelte Linien: die Grenzen, mit denen die Prüfung den Messwert vergleicht, in den Einheiten des Datenpunkts. Der Bereich folgt der nächtlichen Messung — er springt dort, wo eine neue Version übernommen hat, und fehlt überall dort, wo noch nichts gemessen wurde oder die Messung zu alt ist. Eine an einen Maschinenzustand gebundene Prüfung zeichnet den für diesen Zustand gemessenen Bereich. Steht das Fadenkreuz auf einem Zeitabschnitt, erscheinen die Grenzen zu diesem Zeitpunkt neben dem Messwert. Siehe Anomalieerkennung.

Vorschau vs. Live — Ein Umschalter im Zeitbereich wechselt zwischen zwei Wertquellen:

- **Vorschau** — Testet den aktuellen Entwurf rückblickend über den gewählten Zeitraum. Dies ist die Standardeinstellung; sie beantwortet die Frage „Würde meine Änderung auslösen?".

- **Live** — Liest die aktuelle Auswertung des *gespeicherten* Graphen durch die Appliance in Echtzeit. Verwenden Sie diesen Modus, um zu sehen, was die Bedingung gerade tatsächlich tut. Live-Werte sind für eine nicht gespeicherte Bedingung oder bei nicht gespeicherten Änderungen am Entwurf nicht verfügbar; bitte zuerst speichern.

Wenn Live aktiv ist, kennzeichnet ein Badge in der oberen rechten Ecke der Arbeitsfläche die Knotenwerte als live, damit sie nicht mit Vorschauergebnissen verwechselt werden.

Diagramm in der Abfrage öffnen — Jede Sensordiagramm-Zeile im Vorschaubereich hat eine Schaltfläche **Graph-Aktionen** (⋯). Klicken Sie darauf oder rechtsklicken Sie auf die Zeile, um ein Menü mit folgenden Einträgen zu öffnen:

- **In Abfrage öffnen** — Wechselt zur Abfrageseite mit der vorgeladenen Sensorserie, im gleichen Zeitraum und mit der gleichen Granularität wie die Vorschau. So lassen sich Messwerte genauer untersuchen, ohne den Bedingungseditor zu verlassen.
- **Alle Graphen in Abfrage öffnen** — Öffnet alle Sensoren im Vorschaubereich auf einmal in der Abfrageseite. Erscheint nur, wenn mehr als ein Diagramm vorhanden ist.

Bedingungseditor auf einem Telefon — Der Editor ist eine Desktop-Arbeitsoberfläche und auf Telefonen nicht verfügbar. Wird eine Bedingungseditor-URL auf einem schmalen Gerät aufgerufen, wird stattdessen eine **Nur-Lese**-Ansicht angezeigt: ein Tab **Graph** mit der Bedingungsarbeitsfläche (Verschieben und Zoomen, kein Bearbeiten) und ein Tab **Details** mit der aktuellen Live-Auswertung jedes Knotens. Zum Erstellen einer neuen Bedingung ist ein Desktop-Browser erforderlich.

Unlesbarer gespeicherter Graph — Kann der gespeicherte Graph einer Bedingung nicht geöffnet werden (z. B. weil er mit einer neueren Version von Pulse gespeichert wurde), zeigt der Editor einen Hinweis dazu an. Sie können einen neuen Graphen auf der leeren Arbeitsfläche zeichnen und speichern, um den unlesbaren zu ersetzen.

Tastenkürzel — Die Arbeitsfläche reagiert auf Tastenkürzel zum Auswählen, Bearbeiten und Navigieren von Knoten. Drücken Sie `?` oder klicken Sie auf das Tastatur-Symbol in den Steuerelementen der Arbeitsfläche, um die Übersicht der Tastenkürzel zu öffnen.

Bedingungsknoten-Typen

Die Palette des Bedingungseditors gliedert Knoten in fünf Kategorien:

Alarme & Ziele — Ausgangsknoten, die dem Graphen eine Bedeutung geben:

Knoten	Funktion
Alarm	Löst einen Vorfall aus, wenn sein Eingang wahr ist. Eine Bedingung kann mehrere benannte Alarm-Knoten tragen, von denen jeder einen eigenen, separat benannten Vorfall auslöst

Knoten	Funktion
Ziel	Misst, wie viel der Zeit sein Eingang erfüllt ist – als Service Level Objective. Verbinden Sie ihn mit dem gleichen Signal wie den Alarm-Knoten – oder dessen Kehrwert –, damit Versprechen und Alarm dieselbe Definition von „gut" teilen

Quellen — Werte, die in den Graphen eintreten:

Knoten	Ausgabe
Sensor	Der aktuelle Messwert eines Datenpunkts einer Datenquelle -- oder deren Erreichbarkeit
Gelernter Normalwert	Der gemessene Normalwert-Statistikwert für einen Datenpunkt (siehe unten)
Anomalieprüfung	Wahr, wenn die gewählte Anomalieerkennungsprüfung für einen Datenpunkt auslöst (siehe unten)
Monitorzustand	Wahr, wenn ein Monitor gesund oder fehlerhaft ist
Konstante	Eine feste Zahl oder ein boolescher Wert

Transformation — numerische Operationen:

Knoten	Ausgabe
Aggregation	Min, Max, Durchschnitt, Summe oder Anzahl über ein Zeitfenster
Änderung über Zeit	Wie stark sich der Wert eines Datenpunkts innerhalb eines Zeitfensters verändert hat
Anstiegsrate	Wie schnell ein Zähler pro Sekunde steigt; ein Rückgang gilt als Zählerrücksetzung
Mathematik	Arithmetik auf zwei Zahlen
Vergleich	Wahr, wenn ein numerischer Vergleich erfüllt ist

Verkettete Aggregationszeitfenster summieren sich

Das Zeitfenster jedes Aggregationsknotens muss innerhalb der Hot-Tier-Datenaufbewahrungsfrist von Pulse liegen. Wenn Sie Aggregationen verketten (z.B. ein Durchschnitt über einen anderen Durchschnitt), addieren sich die Zeitfenster: Ein äußerer 24-Stunden-Durchschnitt über einen inneren 24-Stunden-Durchschnitt erfordert 48 Stunden Verlaufsdaten. Der Editor markiert den tiefsten Knoten, an dem der kumulative Pfad die Aufbewahrungsgrenze erstmals überschreitet — kürzen Sie eines der Zeitfenster in der Kette, um das Problem zu beheben.

Logik — boolesche Operationen:

Knoten	Ausgabe
Gatter (UND / ODER)	Wahr, wenn alle oder mindestens ein Eingang wahr ist
Nicht	Kehrt einen booleschen Wert um
Nur während	Lässt einen Wert nur durch, solange eine Bedingung wahr ist; sonst keine Daten
Anhaltend	Wahr erst, nachdem der Eingang für eine bestimmte Dauer gehalten hat — **Durchgehend erfüllt** verlangt, dass der Eingang während des gesamten Fensters wahr bleibt; **Irgendwann erfüllt** verlangt, dass er mindestens einmal wahr war

Ausfallsicherheit — Umgang mit fehlenden Daten:

Knoten	Ausgabe
Ersatzwert	Setzt einen Standardwert ein, wenn der Eingang keine Daten hat
Hat Daten	Wahr, wenn der Eingang gerade Daten hat

Rollen von Bedingungsknoten

Bestimmte Bedingungen — insbesondere solche, die Pulse automatisch für Anomalieerkennungs-Monitore generiert — versehen bestimmte Knoten mit einer **Rolle**. Eine Rolle identifiziert, welcher Messwert des Knotens in der Vorfallbeschreibung namentlich genannt wird, wenn die Bedingung ausgelöst wird (z.B. „78,2 liegt über der Obergrenze von 76,0").

Es gibt drei Rollen:

Rolle	Was sie markiert
Messwert	Der verglichene Messwert des Datenpunkts
Obergrenze	Die berechnete Obergrenze
Untergrenze	Die berechnete Untergrenze

Ein markierter Knoten zeigt seine Rolle als Präfix in der Zusammenfassungszeile der Karte — zum Beispiel **Obergrenze · Durchschnitt über 15 min**. Wenn Sie den Knoten auswählen, öffnet der Inspektor eine Notiz **Wird in Vorfällen genannt als**, die bestätigt, welche Rolle er trägt. Die Rolle wird von Pulse beim Generieren der Bedingung gesetzt; der Editor übernimmt sie, erlaubt jedoch keine Änderung.

Gelernter Normalwert (Baseline)

Der Knoten **Gelernter Normalwert** liest die gemessene Baseline für einen bestimmten Datenpunkt — was Pulse als normales Verhalten des Datenpunkts über die letzten 14 Tage gemessen hat. Damit lassen sich Bedingungen formulieren wie „der Messwert liegt mehr als zwei normale Streuungen über dem Normalwert des Datenpunkts", ohne die genauen Zahlen vorab kennen zu müssen.

Jeder Baseline-Knoten gibt jeweils eine Statistik aus:

Statistik	Bedeutung
Normaler Wert	Der typische Wert des Datenpunkts (Median)
Normale Streuung	Wie weit der Datenpunkt typischerweise von seinem Normalwert abweicht
Normales Minimum (1 %)	Die untere Grenze des normalen Bereichs des Datenpunkts
Normales Maximum (99 %)	Die obere Grenze des normalen Bereichs des Datenpunkts
Normale Bewegung	Wie stark sich der Datenpunkt typischerweise innerhalb weniger Minuten verändert
Hohe Bewegung	Die obere Grenze der typischen Bewegung des Datenpunkts
Normale Datenabdeckung	Der Anteil des Zeitfensters, in dem der Datenpunkt normalerweise Daten hat

Statistik	Bedeutung
Niveau des letzten Tages	Der Median des Datenpunkts über die letzten 24 Stunden

Zustandsbasierte Messung — Für ein Signal, das Zustände durchläuft (ein Antriebsstrom, der stillsteht, anfährt und fährt), können Sie die Messung auf einen bestimmten Zustand einschränken. Setzen Sie **Gemessen über** auf *Nur während eines Zustands*, verbinden Sie das Zustandssignal der Steuerung mit dem zweiten Eingang des Knotens und geben Sie den Zustandswert ein, unter dem gemessen werden soll. Pulse misst dann, was der Datenpunkt in genau diesem Zustand als normal gilt — sodass sich beschreiben lässt, was für einen fahrenden Antrieb normal ist, getrennt von dem, was im Stillstand normal ist. Die erste zustandsbasierte Messung erfolgt in der folgenden Nacht.

Festgehaltene Referenz — Die Option **Mit der festgehaltenen Referenz vergleichen** ändert, welche Baseline-Version der Knoten liest: Statt der letzten nächtlichen Messung gibt er die Version zurück, die beim Einrichten der Drift-Prüfung festgehalten wurde. Diese Version ändert sich nie, sodass sie langsame Veränderungen erkennt, die die nächtliche Baseline als normal einordnen würde.

Die Baseline wird vom nächtlichen Messjob berechnet, der unter Anomalieerkennung beschrieben ist. Ein heute angelegter Datenpunkt hat keine Baseline bis zum nächsten Nachtlauf; ein Knoten, der auf ihn zeigt, meldet bis dahin **Unbekannt**.

Anomalieprüfungs-Knoten

Der Knoten **Anomalieprüfung** ist ein in sich geschlossenes Blatt: Er benennt seinen eigenen Datenpunkt, führt eine der fünf Anomalieerkennungsprüfungen aus und gibt `wahr` aus, wenn diese Prüfung auslöst. Es müssen keine Eingaben verdrahtet werden; der einzige Ausgang verbindet sich wie jede andere boolesche Quelle mit einem Gatter-, Anhaltend- oder Alarm-Knoten.

Die Prüfungsart und die Empfindlichkeit werden im Inspektor gewählt:

Einstellung	Optionen
Prüfung	Meldet keine Werte mehr · Außerhalb des normalen Bereichs · Ändert sich nicht mehr · Ungewöhnliche Bewegung · Entfernt sich von seiner Referenz
Empfindlichkeit	Niedrig — nur das Offensichtliche · Mittel — empfohlen · Hoch — früh erkennen

Die fünf Prüfungen sind dieselben, die der Dialog zur Anomalieerkennung erstellt, mit denselben Baselines und demselben Verhalten — auf dieser Seite ist beschrieben, was jede Prüfung beobachtet und wann sie eine Baseline benötigt.

Nur während — Standardmäßig bewertet die Prüfung den gesamten Verlauf des Datenpunkts. Bei einem Signal, das Zustände durchläuft (ein Antrieb, der stillsteht, anfährt und fährt), unterscheidet sich der Normalbereich je nach Zustand. Setzen Sie **Nur während** auf *Nur während ein anderes Signal einen Wert hält*, wählen Sie das Zustandssignal und geben Sie den zu haltenden Wert ein: Die Prüfung berücksichtigt dann nur die Messwerte, die der Datenpunkt während dieses Zustands erzeugt hat, und beurteilt sie anhand dessen, was in dieser Phase normal ist.

Die Zusammenfassungszeile des Knotens im Canvas zeigt die Prüfungsart und die Empfindlichkeit — zum Beispiel **Außerhalb des normalen Bereichs · Mittel**. Wenn **Nur während** aktiv ist, wird der Zustandsausdruck angehängt — **Außerhalb des normalen Bereichs · Mittel · Kranstatus = 2**.

Qualität der Messwerte

Ein Bedingungsmonitor meldet **Unbekannt** statt Gesund, wenn die benötigten Messwerte fehlen oder unzuverlässig sind -- etwa weil die SPS-Verbindung unterbrochen wurde oder ein Wert auf dem Server nicht mehr verfügbar ist. Ein unbekanntes Ergebnis lässt einen offenen Vorfall offen und pausiert die Eskalation; es löst sich auf, sobald wieder ein gültiger Messwert eintrifft.

Wo ein Messwert ausbleibt, sehen Sie an der Datenquelle: Ihre Detailseite zeigt zu jedem Datenpunkt den letzten Wert, den Zeitpunkt der letzten Messung und ob diese Messung Gut, Schlecht oder Keine Daten war. Die Liste der Datenquellen zeigt dasselbe auf einen Blick -- **Liest**, **Liest nicht** oder **Wartet auf erste Abfrage**.

Monitore filtern

Die Monitor-Liste unterstützt verschiedene Filteroptionen:

- **Status** -- Filtern nach Gesund, Fehlerhaft oder Unbekannt
- **Typ** -- Filtern nach Monitor-Typ (Heartbeat, CVE, Trigger, Bedingung, Alarme & Bedingungen)
- **Tags** -- Filtern nach zugewiesenen Tags
- **Eskalationsrichtlinie** -- Filtern nach der dem Monitor zugewiesenen Eskalationsrichtlinie
- **Datenquelle** -- Filtern nach der Datenquelle, die der Monitor liest

- **Veraltete Daten** -- Nur Monitore anzeigen, deren letzter Messwert veraltet ist
- **Nur stummgeschaltet** -- Nur aktuell stummgeschaltete Monitore anzeigen
- **Suche** -- Textsuche über Monitor-Namen

Eine **Typ-Chip-Zeile** unterhalb der Suchleiste zeigt jeden Monitor-Typ mit seiner Anzahl. Klicken Sie auf einen Chip, um nach diesem Typ zu filtern; klicken Sie erneut, um den Filter aufzuheben. Heartbeat sowie Alarme & Bedingungen bilden die Ausnahme: Beide werden nicht auf dieser Seite angelegt, ihre Chips erscheinen deshalb nur dort, wo solche Monitore vorhanden sind. Die Schaltfläche **Tags** öffnet die Tag-Auswahl direkt — Tags sind der wichtigste Weg, die Liste zu unterteilen, deshalb liegen sie in der Werkzeugleiste statt im Filtermenü.

Der Eintrag **Monitore** im Seitenbereich öffnet diese Liste ungefiltert. Darunter stehen Abkürzungen für die zwei Typen, die sich genug unterscheiden, um einen eigenen Eintrag zu rechtfertigen: CVE-Monitore und Trigger-Monitore. Heartbeat- und Bedingungsmonitore haben keine eigene Abkürzung — sie machen den Großteil der Liste aus und werden über Tags oder den Filter **Typ** gefunden. Ziele befinden sich im Bereich **Ziele**; sie sind zwar unter der Haube Monitore, stehen aber neben ihren Budget-Alarm-Staffeln — nicht in dieser Liste.

OPC UA und S7 erscheinen hier nicht mehr. Eine Verbindung ist jetzt eine Datenquelle, daher sind diese Einträge nach **Datenquellen → OPC UA** und **Datenquellen → S7** umgezogen — dorthin führen auch die alten Links auf die Monitor-Liste.

Auf mobilen Geräten werden die Filtersteuerelemente durch eine Schaltfläche **Filter** ersetzt, die ein Einschubfeld von unten öffnet. Das Einschubfeld enthält Abschnitte für Status, Typ und Tags sowie eigenständige Schalter für **Veraltete Daten** und **Nur stummgeschaltet**. Tippen Sie auf **Anwenden**, um die gewählten Filter zu aktivieren, oder auf **Zurücksetzen**, um alle Entwurfsauswahlen zu verwerfen. Aktive Filter werden als Nur-Lese-Chips unterhalb der Suchleiste angezeigt; um eine Auswahl zu ändern, öffnen Sie erneut das Einschubfeld.

Massenaktionen

Organisationsadministratoren können mehrere Monitore gleichzeitig bearbeiten und in einem einzigen Schritt auf alle reagieren. Die Mehrfachauswahl ist nur auf dem Desktop verfügbar.

Klicken Sie in der Werkzeugleiste auf **Auswählen**, um den Auswahlmodus zu aktivieren. Im Auswahlmodus zeigt jede Zeile ein Auswahlkästchen, und die gesamte Zeile ist das Ziel — ein Klick auf eine Zeile wählt den Monitor aus, anstatt ihn zu öffnen. Ein Auswahlkästchen **Alle N Monitore auswählen** über der Liste wählt alle Zeilen aus, die dem aktuellen Filter entsprechen, oder hebt die Auswahl auf. Halten Sie **Umschalt**

gedrückt, während Sie eine Zeile anklicken, um alle Zeilen zwischen der zuletzt angeklickten und der aktuellen Zeile hinzuzufügen, ohne die bisherige Auswahl zu verlieren. Beim Ändern der Filter wird die Auswahl aufgehoben, denn alles Ausgewählte muss eine Zeile sein, die Sie noch vor sich haben.

Um den Auswahlmodus zu verlassen, klicken Sie erneut auf **Auswählen** oder drücken Sie **Esc**. Esc geht dabei Schritt für Schritt zurück: Das erste Drücken hebt die Auswahl auf, ein zweites verlässt den Modus.

Sobald mindestens ein Monitor ausgewählt ist, erscheint am unteren Rand der Liste eine schwebende Aktionsleiste:

- **N ausgewählt** — zeigt die Anzahl der aktuell ausgewählten Monitore
- **Stummschalten** — schaltet alle ausgewählten Monitore stumm. Ein Toast bestätigt, wie viele Monitore den Zustand gewechselt haben, und bietet **Rückgängig** an. Das macht nur die Monitore rückgängig, die die Aktion tatsächlich verändert hat — ein bereits stummgeschalteter Monitor bleibt stummgeschaltet.
- **Stummschaltung aufheben** — hebt die Stummschaltung aller ausgewählten Monitore auf, mit demselben Toast und Rückgängig.
- **Löschen** — öffnet den Bestätigungsdialog für das Massenlöschen.
- **×** (Auswahl aufheben) — hebt die Auswahl auf, ohne den Modus zu verlassen.

Massenlöschen

Das Löschen von Monitoren in einem Schritt öffnet einen Bestätigungsdialog, der die tatsächliche Anzahl der zu entfernenden Monitore berechnet. Bei der Auswahl eines S7-Endpunkt-Monitors oder OPC-UA-Endpunkt-Monitors werden auch alle untergeordneten Monitore (S7-Tag- oder OPC-UA-Knoten-Monitore dieses Endpunkts) mitgelöscht. Der Dialog ruft diese Kindanzahl ab, bevor er zur Bestätigung auffordert. Geben Sie die angezeigte Zahl ein, um die Lösch-Schaltfläche freizuschalten.

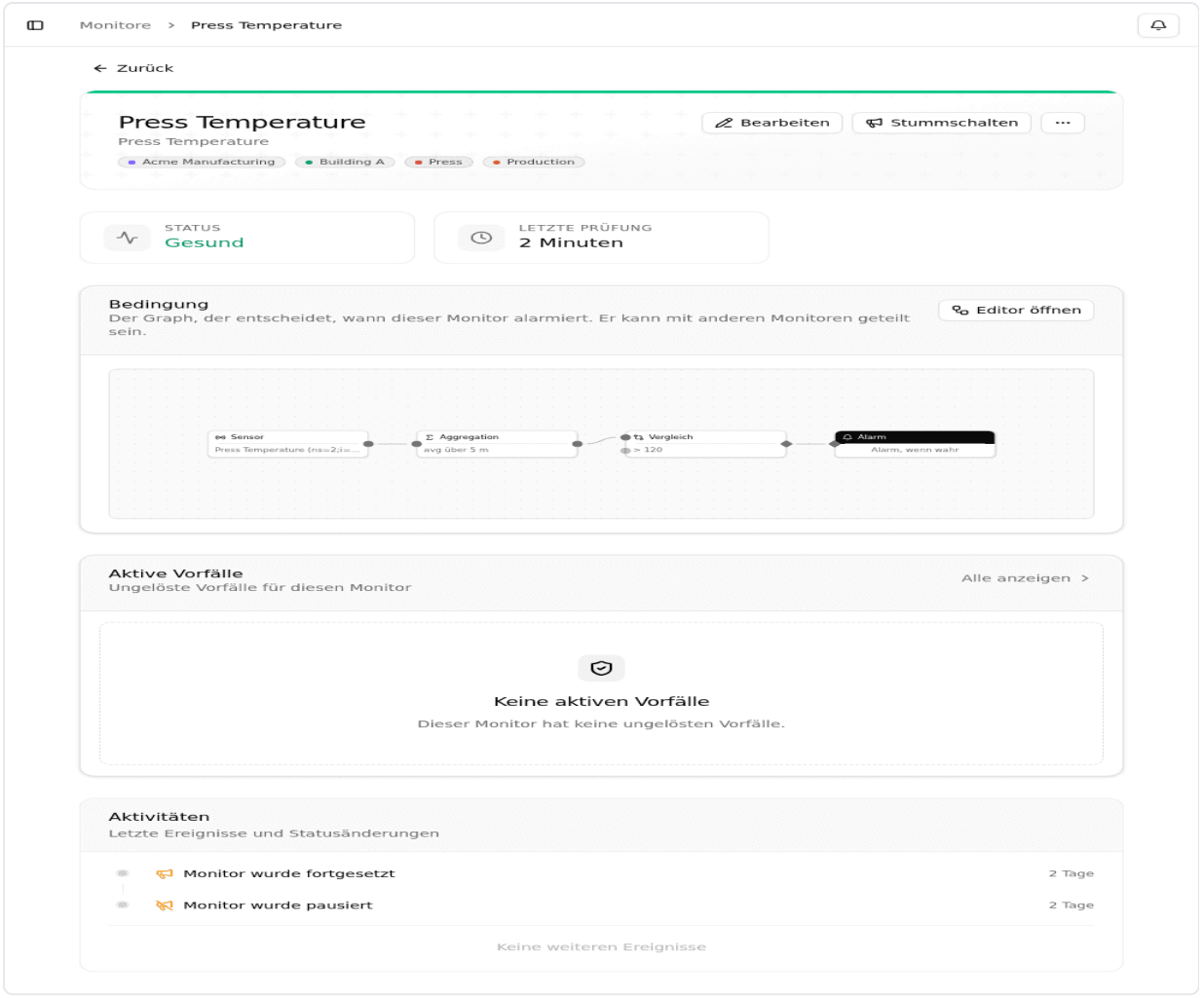
Wenn ausgewählte Monitore von Bedingungen verwendet werden, wird das Löschen blockiert und der Dialog zeigt, welche Bedingungen auf sie verweisen. Sie können diese Monitore zunächst aus den entsprechenden Bedingungen entfernen und es erneut versuchen, oder sofort die verbleibenden, nicht blockierten Monitore löschen.

Ein Monitor und die Bedingung, auf die er alarmiert, gehören zusammen: Wird der letzte Monitor gelöscht, der auf eine Bedingung alarmiert, wird auch diese Bedingung gelöscht — sonst könnte sie niemand mehr erreichen. Die Meldung nennt beide Zahlen — „340 Monitore gelöscht – 340 Bedingungen gingen mit" —, damit Sie nach einem Upgrade nicht nach Graphen suchen, die längst weg sind. Eine Bedingung, die sich mehrere Monitore teilen, oder über die ein Ziel etwas zusagt, bleibt bestehen.

Bedingungen, die nichts mehr verwendet, räumen Sie direkt in der Bedingungsliste auf; siehe Bedingungen.

Monitor-Details

Klicken Sie auf einen Monitor, um seine Detailseite anzuzeigen.



Jede Detailseite zeigt:

- **Status** -- Aktueller Zustand (Gesund oder Fehlerhaft)
- **Konfiguration** -- Worauf der Monitor alarmiert. Bei einem Bedingungsmonitor ist das die Bedingung selbst, als Diagramm dargestellt; zum Bearbeiten öffnen Sie sie. Da mehrere Monitore sich eine Bedingung teilen können, wird sie dort bearbeitet, wo sie liegt, und nicht auf dieser Seite.
- **Tags** -- Dem Monitor zugewiesene Tags zur Kategorisierung
- **Aktionen** -- Monitor bearbeiten, stummschalten oder löschen über den Aktionen-Button
- **Aktivitätsfeed** -- ein chronologischer Verlauf von Statusänderungen und Ereignissen

Den Aktivitätsfeed hat jeder Monitortyp, Bedingungsmonitore eingeschlossen. Teilen sich mehrere Monitore eine Bedingung, hat trotzdem jeder seinen eigenen Feed: Sie halten dieselben Statusänderungen zu denselben Zeitpunkten fest, denn genau das ist jedem von ihnen passiert, und die Stummschaltung eines Monitors erscheint nur in seinem eigenen Feed.

Monitore per CSV importieren

Organisationsadministratoren können CVE-Monitore in großer Anzahl aus einer CSV-Datei importieren. Die vollständige Anleitung und die komplette Spaltenreferenz finden Sie unter Monitore aus CSV importieren.

Tags aus Datenquellen

Ein Monitor trägt eigene Tags, nach denen Sie die Monitorliste filtern können. Tags an einer **Datenquelle** sind davon getrennt: Sie beschreiben die Maschine und nicht den Alarm, und jeder Datenpunkt dieser Quelle erbt sie automatisch. Auch jeder Bedingungsmonitor, der einen dieser Datenpunkte liest, lässt sich nach den geerbten Tags filtern -- eine SPS einmal zu taggen genügt also, um alles wiederzufinden, was sie überwacht.

Monitore stummschalten

Sie können einen Monitor vorübergehend stummschalten, um die Vorfallerstellung während geplanter Wartungen zu unterdrücken. Stummgeschaltete Monitore prüfen weiterhin ihre Ziele, erzeugen jedoch keine neuen Vorfälle.

> **TIP**
>
> Stummschalten ist nützlich während geplanter Wartungsfenster. Denken Sie daran, Monitore nach Abschluss der Wartung wieder zu aktivieren.

Monitore löschen

Um einen Monitor zu löschen, öffnen Sie seine Detailseite, klicken Sie auf **Aktionen** und wählen Sie **Löschen**. Im Bestätigungsdialog müssen Sie den Namen des Monitors eingeben, bevor die Lösch-Schaltfläche aktiv wird — dieser bewusste Schritt verhindert einen versehentlichen Verlust des Messverlaufs.

Das Löschen eines Monitors, der von einer Bedingung verwendet wird, ist blockiert.
Entfernen Sie den Monitor zuerst aus der Bedingung und löschen Sie ihn anschließend.

Teil 3 · Monitoring

3.3 CSV-Import

Derselbe dreistufige Assistent importiert drei verschiedene Dinge, je nachdem, wo Sie ihn öffnen:

- Im Dropdown **Erstellen** der Monitor-Liste legt er **CVE-Monitore** an. Siehe CVE-Monitore importieren weiter unten.
- Über die Aktion **Importieren** einer **S7-Datenquelle** deklariert er **Datenpunkte** auf dieser Quelle. Siehe S7-Datenpunkte importieren weiter unten.
- Über die Aktion **Importieren** einer **OPC-UA-Datenquelle** deklariert er **Datenpunkte** auf dieser Quelle. Siehe OPC-UA-Datenpunkte importieren weiter unten.

Der Assistent führt Sie in beiden Fällen durch dieselben drei Schritte: Hochladen, Spalten zuordnen und Ergebnisse – nur die Spalten und das, was eine Zeile anlegt, unterscheiden sich.

Die Detailseite einer S7- oder OPC-UA-Datenquelle bietet außerdem **Exportieren**, das Gegenstück zur Aktion **Importieren**: eine CSV-Datei mit allen Datenpunkten, die die Quelle deklariert hat, in derselben Spaltenstruktur. Siehe Datenpunkte exportieren weiter unten.

Das Dropdown **Erstellen** der Monitor-Liste bietet dieselbe Paarung für CVE-Monitore: **CSV exportieren** lädt alle CVE-Monitore der Organisation herunter, in derselben Spaltenstruktur, die auch **CSV importieren** liest. Siehe CVE-Monitore exportieren weiter unten.

Exportieren und Importieren bilden zusammen einen Kreislauf, keine Einbahnstraße – siehe Eine Tabelle synchron halten weiter unten.

CVE-Monitore importieren

Organisationsadministratoren können mehrere **CVE-Monitore** auf einmal aus einer CSV-Datei anlegen. Öffnen Sie in der Monitor-Liste das Dropdown **Erstellen** und wählen Sie **CSV importieren**, um den Import-Assistenten zu öffnen.

CVE-Monitore sind der einzige Monitor-Typ, den dieser Import anlegt. Verbindungen zu OPC-UA-Servern und S7-SPS werden als Datenquellen angelegt, und alles, was auf einen Wert alarmiert, ist ein Bedingungsmonitor – beides ist keine Zeile in einer Tabelle. Um S7-Tags oder OPC-UA-Knoten in großer Zahl zu deklarieren, siehe S7-Datenpunkte importieren oder OPC-UA-Datenpunkte importieren.

Zwei Werte verhalten sich so, dass es sich lohnt, sie vorab zu kennen:

- `escalationPolicy` verweist per **Name** auf eine bestehende Eskalationsrichtlinie – oder per **id** aus deren eigener URL: `/app/escalation-policies/JgaEBgzn` ist die Richtlinie `JgaEBgzn`. Ein Name muss exakt übereinstimmen – legen Sie die Richtlinie also vor dem Import an. Eine reine Zahl gilt als Name und sonst nichts: Eine Datei, die die Richtlinie als `7` benennt, lässt diese Zeile fehlschlagen, statt eine Zeilennummer aufzulösen.
- `incidentMessageTemplate` ist der literale Vorfallstext, keine Referenz auf eine gespeicherte Vorlage.

Die Spalten sind unter Spalten zuordnen aufgeführt.

S7-Datenpunkte importieren

Organisationsadministratoren können viele **S7-Datenpunkte** auf einmal aus einer CSV-Datei mit Tag-Adressen deklarieren. Öffnen Sie die Detailseite einer **S7-Datenquelle** und wählen Sie **Importieren**, um den Assistenten zu öffnen – er ist bereits an diese Quelle gebunden.

Da die Quelle durch den Startpunkt des Imports feststeht, geht es in der Datei nur um Tags und um nichts anderes – keine Spalte `endpoint`, `rack` oder `slot`, und auch kein `monitorType`. Die Spalten sind unter Spalten zuordnen aufgeführt.

Ein durch diesen Import deklarierter Datenpunkt ist **übernommen** und wird im Takt der Quelle gelesen, wie jeder andere Datenpunkt der Quelle. Eine Zeile, die eine bereits auf der Quelle deklarierte Adresse und einen bereits deklarierten Datentyp nennt, ist ein No-op – sie löst zum bestehenden Datenpunkt auf, statt ein Duplikat anzulegen, sodass ein erneuter Lauf einer unveränderten Datei folgenlos bleibt.

Anders als beim CVE-Import läuft dieser Import **alles oder nichts**: Jede Zeile wird geprüft, bevor irgendetwas geschrieben wird, und wenn eine Zeile fehlschlägt, wird nichts angelegt – der Ergebnisschritt listet jede fehlgeschlagene Zeile auf, damit Sie die Datei korrigieren und es erneut versuchen können. Siehe Ergebnisse.

Auf die importierten Werte alarmieren

Werden vier weitere Spalten zugeordnet – `aggregation`, `operation`, `operand` und `duration` –, wird aus jeder Zeile statt einer reinen Datenpunkt-Deklaration ein Schwellwertalarm darauf: „Alarmieren, wenn der Durchschnitt von `DB1.DBD10` über 5 Minuten über 80 liegt". Sind bei einer Zeile alle vier Spalten zugeordnet, legt der Import an:

- eine **Bedingung** – den Graphen `Sensor → Aggregate → Compare → Alert` – die an den von der Zeile deklarierten Datenpunkt gepinnt ist, und
- einen **Bedingungsmonitor**, der darauf alarmiert, in der Gruppe **Conditions** der Monitor-Liste.

Die Bedingung öffnet sich in derselben geführten Satzform, die auch ein von Hand angelegter Schwellwert verwendet, sodass hundert importierte Alarme danach bearbeitbar bleiben – nichts daran ist ausschließlich über den Canvas erreichbar.

Sobald eine der vier Spalten zugeordnet ist, müssen alle vier zugeordnet sein, zusammen mit `name` (der Name der Bedingung und ihres Monitors) und `escalationPolicy` (wer bei einem daraus entstehenden Vorfall alarmiert wird) – eine Zeile kann keinen Schwellwert aus drei Feldern und einer Vermutung für das vierte bilden. Bleiben alle vier nicht zugeordnet, gilt weiterhin das oben beschriebene einfache Verhalten: Zeilen deklarieren nur Datenpunkte, ohne Bedingungen oder Monitore.

Auch mit zugeordneten Spalten entscheidet jede Zeile selbst, ob sie einen Schwellwert trägt. Eine Zeile, die alle sechs Felder `name`, `escalationPolicy`, `aggregation`, `operation`, `operand` und `duration` ausfüllt, legt einen an. Eine Zeile, die alle sechs leer lässt, deklariert nur ihren Datenpunkt – eine Datei kann also Datenpunkte mit und ohne Schwellwert mischen, so wie der Export einer Quelle sie schreibt. Eine Zeile, die nur einen Teil davon ausfüllt, schlägt fehl, und ihr Fehler nennt die fehlenden Felder. Ein Feld, das über **Fixer Wert…** einen festen Wert erhält, gilt in jeder Zeile als ausgefüllt und hindert eine Zeile, deren übrige Schwellwert-Zellen leer sind, daher nicht daran, nur ihren Datenpunkt zu deklarieren.

Bedingungsnamen sind **pro Organisation eindeutig und Groß-/Kleinschreibung wird ignoriert**. Eine Zeile, deren Name bereits vergeben ist – durch eine bestehende Bedingung oder durch eine andere Zeile derselben Datei –, schlägt bei der Validierung fehl, bevor irgendetwas geschrieben wird, genau wie bei einer ungültigen Adresse – es sei denn, Bestehende Monitore aktualisieren ist aktiviert und die passende Bedingung ist bereits an genau den Datenpunkt dieser Zeile gepinnt; dann wird die Bedingung stattdessen aktualisiert.

Der Schalter **Erstellte Monitore aktivieren** im Zuordnungsschritt entscheidet, ob die von diesem Lauf angelegten Monitore aktiv oder inaktiv starten. Aus (die Voreinstellung) legt sie **inaktiv** an: Sie stehen zur Prüfung in der Monitor-Liste, und die Auswertung überspringt einen inaktiven Monitor vollständig, sodass keiner von ihnen einen Vorfall auslösen kann, bis Sie ihn von Hand aktivieren. Ein schaltet sie sofort scharf. Das ist eine gute Voreinstellung für einen ersten Import von hundert Schwellwerten – prüfen Sie die erzeugten Bedingungen und aktivieren Sie dann die, die passen.

OPC-UA-Datenpunkte importieren

Organisationsadministratoren können viele **OPC-UA-Datenpunkte** auf einmal aus einer CSV-Datei mit Node-IDs deklarieren – der Fall einer Node-Liste eines Maschinenbauers oder eines großen Servers, den Sie lieber nicht durchsuchen möchten. Öffnen Sie die Detailseite einer **OPC-UA-Datenquelle** und wählen Sie **Importieren**, um den Assistenten zu öffnen – er ist bereits an diese Quelle gebunden.

Da die Quelle durch den Startpunkt des Imports feststeht, geht es in der Datei nur um Nodes und um nichts anderes: Eine Zeile besteht aus einer einzigen Spalte, `nodeId`. Anders als bei einem S7-Tag wird der Werttyp eines OPC-UA-Datenpunkts nicht deklariert – er wird aus der ersten Messung gelernt, genau wie beim Deklarieren von Hand – daher gibt es keine `dataType`-Spalte zuzuordnen. Die Spalten sind unter Spalten zuordnen aufgeführt.

Node-IDs werden nur auf gültige **Syntax** geprüft – `ns=2;s=Line1.Temperature` oder `ns=3;i=1001`, dieselbe Textform, die auch die Detailseite der Quelle verwendet. Ob der Node tatsächlich auf dem Server existiert, wird beim Import nicht geprüft: Das würde den Import von einem erreichbaren Server abhängig machen, was dem Sinn einer vorbereiteten Datei vor der Inbetriebnahme widerspricht. Eine Node-ID, die der Server nicht erkennt, kommt als fehlerhafte Messung zurück, sobald die Quelle sie abfragt – sichtbar auf der Detailseite der Quelle wie jede andere fehlerhafte Messung.

Eine Zeile, die den eigenen Gesundheitsprüfungs-Node der Quelle nennt, wird abgelehnt, genau wie beim Deklarieren von Hand – der Punkt existiert bereits als Erreichbarkeits-Sonde der Quelle, ihn erneut zu importieren würde einen zweiten, bedeutungslosen Lebendigkeitspunkt statt einer echten Messung anlegen.

Ein durch diesen Import deklarierter Datenpunkt ist **übernommen** und wird im Takt der Quelle gelesen, wie jeder andere Datenpunkt der Quelle. Eine Zeile, die einen bereits auf der Quelle deklarierten Node nennt, ist ein No-op – sie löst zum bestehenden Datenpunkt auf, statt ein Duplikat anzulegen, sodass ein erneuter Lauf einer unveränderten Datei folgenlos bleibt, und zwei Zeilen, die denselben Node unterschiedlich schreiben (etwa mit oder ohne führende Null im Bezeichner), lösen ebenfalls zu einem einzigen Datenpunkt auf.

Anders als beim CVE-Import läuft dieser Import **alles oder nichts**: Jede Zeile wird geprüft, bevor irgendetwas geschrieben wird, und wenn eine Zeile fehlschlägt, wird nichts angelegt – der Ergebnisschritt listet jede fehlgeschlagene Zeile auf, damit Sie die Datei korrigieren und es erneut versuchen können. Siehe Ergebnisse.

Auf die importierten Werte alarmieren

Werden vier weitere Spalten zugeordnet – `aggregation`, `operation`, `operand` und `duration` –, wird aus jeder Zeile statt einer reinen Datenpunkt-Deklaration ein Schwellwertalarm darauf: „Alarmieren, wenn der Durchschnitt von `ns=3;s=Boiler.Pressure` über 5 Minuten über 80 liegt". Sind bei einer Zeile alle vier Spalten zugeordnet, legt der Import an:

- eine **Bedingung** – den Graphen `Sensor → Aggregate → Compare → Alert` – die an den von der Zeile deklarierten Datenpunkt gepinnt ist, und
- einen **Bedingungsmonitor**, der darauf alarmiert, in der Gruppe **Conditions** der Monitor-Liste.

Die Bedingung öffnet sich in derselben geführten Satzform, die auch ein von Hand angelegter Schwellwert verwendet, sodass hundert importierte Alarme danach bearbeitbar bleiben – nichts daran ist ausschließlich über den Canvas erreichbar. Da der Werttyp eines OPC-UA-Datenpunkts erst aus seiner ersten Messung gelernt wird, importiert und validiert ein Schwellwert auf einen frisch deklarierten Node auch dann sauber, wenn sich der Node als boolescher Wert herausstellt – er löst unter einem numerischen Vergleich wie `avg … > 80` dann schlicht nie sinnvoll aus.

Sobald eine der vier Spalten zugeordnet ist, müssen alle vier zugeordnet sein, zusammen mit `name` (der Name der Bedingung und ihres Monitors) und `escalationPolicy` (wer bei einem daraus entstehenden Vorfall alarmiert wird) – eine Zeile kann keinen Schwellwert aus drei Feldern und einer Vermutung für das vierte bilden. Bleiben alle vier nicht zugeordnet, gilt weiterhin das oben beschriebene einfache Verhalten: Zeilen deklarieren nur Datenpunkte, ohne Bedingungen oder Monitore.

Auch mit zugeordneten Spalten entscheidet jede Zeile selbst, ob sie einen Schwellwert trägt. Eine Zeile, die alle sechs Felder `name`, `escalationPolicy`, `aggregation`, `operation`, `operand` und `duration` ausfüllt, legt einen an. Eine Zeile, die alle sechs leer lässt, deklariert nur ihren Datenpunkt – eine Datei kann also Datenpunkte mit und ohne Schwellwert mischen, so wie der Export einer Quelle sie schreibt. Eine Zeile, die nur einen Teil davon ausfüllt, schlägt fehl, und ihr Fehler nennt die fehlenden Felder. Ein Feld, das über **Fixer Wert…** einen festen Wert erhält, gilt in jeder Zeile als ausgefüllt und hindert eine Zeile, deren übrige Schwellwert-Zellen leer sind, daher nicht daran, nur ihren Datenpunkt zu deklarieren.

Bedingungsnamen sind **pro Organisation eindeutig und Groß-/Kleinschreibung wird ignoriert**. Eine Zeile, deren Name bereits vergeben ist – durch eine bestehende Bedingung oder durch eine andere Zeile derselben Datei –, schlägt bei der Validierung fehl, bevor irgendetwas geschrieben wird, genau wie bei einer ungültigen Node-ID – es

sei denn, Bestehende Monitore aktualisieren ist aktiviert und die passende Bedingung ist bereits an genau den Datenpunkt dieser Zeile gepinnt; dann wird die Bedingung stattdessen aktualisiert.

Der Schalter **Erstellte Monitore aktivieren** im Zuordnungsschritt entscheidet, ob die von diesem Lauf angelegten Monitore aktiv oder inaktiv starten. Aus (die Voreinstellung) legt sie **inaktiv** an: Sie stehen zur Prüfung in der Monitor-Liste, und die Auswertung überspringt einen inaktiven Monitor vollständig, sodass keiner von ihnen einen Vorfall auslösen kann, bis Sie ihn von Hand aktivieren. Ein schaltet sie sofort scharf. Das ist eine gute Voreinstellung für einen ersten Import von hundert Schwellwerten – prüfen Sie die erzeugten Bedingungen und aktivieren Sie dann die, die passen.

Bestehende Zeilen beim erneuten Import aktualisieren

Standardmäßig schlägt eine Zeile, deren Name einem bereits vorhandenen entspricht, fehl – „Monitor name already exists" beim CVE-Import, „Condition name already exists" bei einem S7- oder OPC-UA-Import – ein einfacher Import ändert nie etwas, das bereits vorhanden ist. Um ein Geräteblatt oder eine Tag-Liste laufend zu pflegen und bei Änderungen erneut zu importieren, aktivieren Sie im Zuordnungsschritt den Schalter **Bestehende Monitore aktualisieren** (standardmäßig aus, für jeden Modus).

Beim CVE-Import aktualisiert eine Zeile, deren `name` einem bestehenden **CVE-Monitor** entspricht, dessen `vendor`, `orderCode`, `product`, `firmware` und `escalationPolicy`, statt fehlzuschlagen – Tags und die Quell-Datenquelle bleiben unverändert: Ein `tags`-Wert der Zeile wird bei einer Aktualisierung ignoriert (siehe Tags zuweisen), und die Quell-Datenquelle setzt dieser Import weder beim Anlegen noch bei einer Aktualisierung jemals. Eine Zeile, deren Name einem Monitor eines anderen Typs entspricht (etwa einem Heartbeat-Monitor), bleibt ein Zeilenfehler: Für eine CVE-Zeile gibt es an einem Monitor eines anderen Typs nichts zu aktualisieren, daher wird für diese Zeile nichts geschrieben.

Bei einem S7- oder OPC-UA-Import mit zugeordneten vier Schwellwert-Spalten (siehe Auf die importierten Werte alarmieren oder den entsprechenden OPC-UA-Abschnitt) aktualisiert eine Zeile, deren `name` einer bestehenden **Bedingung** entspricht, die bereits an genau den von der Zeile deklarierten Datenpunkt gepinnt ist – dieselbe Adresse oder Node-ID –, deren `aggregation`, `operation`, `operand` und `duration` sowie die `escalationPolicy` des Monitors, statt fehlzuschlagen. Der Aktiv-Status des Monitors und seine Tags bleiben unverändert, genauso wie der CVE-Import Tags und Quell-Datenquelle eines CVE-Monitors unverändert lässt. Eine Zeile, deren Name einer Bedingung entspricht, die an einen *anderen* Datenpunkt gepinnt ist – der Name wurde etwa für ein anderes Tag wiederverwendet –, bleibt ein Zeilenfehler, und weil ein S7- oder

OPC-UA-Lauf alles oder nichts ist, wird in diesem Fall nichts aus der Datei geschrieben: Es gibt nichts Sicheres zu aktualisieren, wenn Zeile und bestehende Bedingung nicht einig sind, worauf sie überhaupt alarmieren.

Eine Zeile, deren Name noch keinem Eintrag entspricht, legt weiterhin einen an, unabhängig vom Schalter.

Der Ergebnisschritt weist diese aktualisierten Zeilen getrennt von neu angelegten aus – siehe Ergebnisse.

CVE-Monitore exportieren

Öffnen Sie in der Monitor-Liste das Dropdown **Erstellen** und wählen Sie **CSV exportieren**, um alle **CVE-Monitore** der Organisation herunterzuladen – in derselben Spaltenstruktur, die auch CVE-Monitore importieren liest: `monitorType`, `name`, `vendor`, `orderCode`, `product`, `firmware`, `escalationPolicy`, `incidentMessageTemplate` und `tags`. `escalationPolicy` wird als Name geschrieben und `tags` mit `\|` getrennt – dieselben Formen, die Spalten zuordnen auch wieder einliest. `incidentMessageTemplate` ist immer leer – kein CVE-Monitor besitzt dieses Feld, es gibt also nichts hineinzuschreiben.

Der Export berücksichtigt die aktiven Filter der Liste – Status, Eskalationsrichtlinie, Datenquelle, Tags und Suche sowie die Umschalter „Veraltet“ und „Stummgeschaltet“ – mit Ausnahme des Typfilters, da diese Aktion unabhängig von der übrigen Anzeige immer nur CVE-Monitore exportiert.

Importieren Sie die Datei mit eingeschaltetem **Bestehende Monitore aktualisieren** erneut, ist das ein No-op: Jede Zeile trifft anhand ihres Namens auf ihren eigenen Monitor, sodass der Ergebnisschritt jede Zeile als aktualisiert statt als neu angelegt ausweist.

Zum Exportieren ist dieselbe Berechtigung als **Organisationsadministrator** erforderlich wie zum Importieren.

Datenpunkte exportieren

Auf der Detailseite einer **S7**- oder **OPC-UA**-Datenquelle lädt **Exportieren** eine CSV-Datei mit allen Datenpunkten herunter, die die Quelle deklariert hat – in derselben Spaltenstruktur, die ihre eigene Aktion **Importieren** liest: `address` / `dataType` (S7) bzw. `nodeId` (OPC UA), plus `name`, `escalationPolicy`, `aggregation`, `operation`, `operand`, `duration` und `tags` für einen Datenpunkt, an den genau eine Schwellenwert-Bedingung gepinnt ist. Ein Datenpunkt ohne Schwellenwert lässt diese Spalten leer; einer mit mehr als einem Schwellenwert wird einmal pro Schwellenwert exportiert, als separate Zeilen mit

derselben Adresse bzw. Node-ID. `escalationPolicy` wird als Name geschrieben, `duration` in Sekunden, `operation` als `gt` / `gte` / `lt` / `lte` / `eq` / `neq` und `tags` mit `\|` getrennt – dieselben Formen, die **Spalten zuordnen** auch wieder einliest.

Importieren Sie die Datei mit eingeschaltetem **Bestehende Monitore aktualisieren** erneut gegen dieselbe Quelle, ist das ein No-op: Jede Zeile trifft auf ihren eigenen Datenpunkt und ihre eigene Bedingung (soweit vorhanden), sodass der Ergebnisschritt jede Zeile als aktualisiert statt als neu angelegt ausweist.

Zum Exportieren ist dieselbe Berechtigung als **Organisationsadministrator** erforderlich wie zum Importieren.

Eine Tabelle synchron halten

Der Export schreibt genau die Spaltenstruktur, die der Import liest – beide bilden also einen Kreislauf, keine Einbahnstraße: Exportieren Sie die Datenpunkte einer Quelle oder die CVE-Monitore der Monitor-Liste, bearbeiten Sie die Datei in einer Tabellenkalkulation, und importieren Sie sie mit eingeschaltetem **Bestehende Monitore aktualisieren** erneut. Da die exportierten Spaltennamen genau den Feldnamen des Imports entsprechen, erkennt der Zuordnungsschritt beim erneuten Import jede Spalte automatisch wieder – von Hand nachzuordnen ist nichts, auch nicht bei den Schwellwert-Spalten.

So pflegen Sie eine Gerätetabelle oder eine Monitor-Liste dauerhaft außerhalb von Pulse: Ändern Sie einen Operanden, benennen Sie eine Eskalationsrichtlinie um, ergänzen Sie eine Firmware-Version – und importieren Sie die bearbeitete Datei anschließend erneut. Eine Zeile, deren Name (bzw. Adresse oder Node-ID, bei einem Datenpunkt) sich nicht geändert hat, aktualisiert das bereits passende Objekt, statt an der Kollision zu scheitern; eine neu hinzugefügte Zeile legt weiterhin an, wie bei jedem anderen Import.

Tags zuweisen

Eine optionale Spalte `tags` weist einem von diesem Import angelegten Monitor bestehende **Tags** zu: mit `|` getrennte Tag-Namen, jeweils von umgebenden Leerzeichen befreit (zum Beispiel `Line 1|Boiler`). Jeder Name muss exakt (ohne Berücksichtigung von Groß-/Kleinschreibung) auf ein bestehendes Tag passen – der Import legt nie ein Tag an, daher ist ein Name, der auf keines passt, bei einer CVE-Zeile, die einen Monitor anlegt, ein Zeilenfehler oder lässt bei einer S7- oder OPC-UA-Zeile, die einen Bedingungsmonitor anlegt, den ganzen Lauf fehlschlagen, genau wie jede andere Spalte, die diese Importe nicht auflösen können. Eine Zeile, die einen bestehenden

Monitor oder eine bestehende Bedingung aktualisiert, ignoriert ihre `tags`-Spalte, daher ist ein unbekannter Name dort kein Fehler. Was das für das Geschriebene bedeutet, steht unter Schritt 3 — Ergebnisse.

Ein Tag-Name, der selbst ein `|` enthält, kann diese Spalte nicht unverändert durchlaufen: sowohl der Export als auch das Aufteilen an `|` beim Import behandeln jedes `|` als Trennzeichen, ohne ein Escaping für ein `|` innerhalb eines Namens. Vermeiden Sie ein `|` im Namen eines Tags, wenn Sie es exportieren und wieder importieren möchten.

Bei einem S7- oder OPC-UA-Import hat `tags` nur dann einen Monitor, dem es zugewiesen werden kann, wenn die Zeile auch die vier Schwellwert-Spalten zuordnet und einen Bedingungsmonitor anlegt – siehe Auf die importierten Werte alarmieren (S7) oder den entsprechenden OPC-UA-Abschnitt. Bei einer reinen Datenpunkt-Zeile wird die Spalte gelesen, aber ignoriert, da nichts angelegt wird, das ein Tag tragen könnte.

CSV-Format

Die erste Zeile muss eine **Kopfzeile** mit Spaltennamen sein – im nächsten Schritt werden diese Namen den Feldern zugeordnet (die Zuordnung lässt sich von Hand anpassen). Speichern Sie die Datei als **UTF-8**.

Der Import akzeptiert **Komma**, **Semikolon** oder **Tabulator** als Trennzeichen – welches davon in der Kopfzeile am häufigsten vorkommt, gilt für die gesamte Datei, Sie müssen also keines davon auswählen. Ein führendes **UTF-8-Byte-Order-Mark**, das Excel je nach Systemsprache automatisch einfügt, wird beim Einlesen entfernt. Dadurch lässt sich ein mit Semikolon getrennter, mit BOM versehener Export – die Standardausgabe eines deutschsprachigen Excel – genauso importieren wie eine einfache, kommagetrennte Datei. Im Übrigen gelten die üblichen CSV-Regeln (RFC 4180): Werte, die selbst das Trennzeichen, ein Anführungszeichen oder einen Zeilenumbruch enthalten, in doppelte Anführungszeichen setzen und darin enthaltene Anführungszeichen verdoppeln.

Als funktionierende Vorlage nutzen Sie im Upload-Schritt **Beispiel-CSV herunterladen**: Sie enthält die Spalten des gerade geöffneten Assistenten mit einer oder mehreren Beispielzeilen.

Schritt 1 — Hochladen

Ziehen Sie eine CSV-Datei in die Ablagefläche oder klicken Sie, um eine Datei auszuwählen. Eine Vorschautabelle zeigt die ersten Zeilen, damit Sie prüfen können, ob die Datei korrekt gelesen wurde; mit **Ersetzen** tauschen Sie die Datei aus. Klicken Sie auf **Weiter** oder auf **Abbrechen**, um den Assistenten zu schließen.

Schritt 2 — Spalten zuordnen

Ordnen Sie jedem Feld eine Spalte aus Ihrer CSV zu. Der Assistent erkennt passende Spaltennamen automatisch und befüllt die Zuordnung nach Möglichkeit vor. Für jedes Feld können Sie:

- die **CSV-Spalte** wählen, deren Werte verwendet werden,
- mit **Fixer Wert…** einen Wert für alle Zeilen festlegen (praktisch für gemeinsame Einstellungen wie die Eskalationsrichtlinie) oder
- das Feld **Nicht zugeordnet** lassen – nur bei optionalen Feldern erlaubt.

Die Tabelle listet jede Spalte, ob sie erforderlich ist und welche Werte sie akzeptiert.

CVE-Monitor-Spalten

Spalte	Erforderlich	Gültige Werte / Format
`monitorType`	Ja	`cve`
`name`	Ja	Freitext
`vendor`	Ja	Gerätehersteller, z. B. `Siemens`
`orderCode`	Eines von beiden	Bestellnummer / MLFB des Geräts, z. B. `6ES7516-3AN00-0AB0` – eine Zeile braucht dies oder `product`
`product`	Eines von beiden	Produkt- / Modultypname in der Schreibweise der Hersteller-Sicherheitsmeldungen, z. B. `AC500 V3`
`firmware`	Optional	Firmware-Version, z. B. `V2.9.2` (leer → passt auf alle Firmware-Versionen)
`escalationPolicy`	Ja	**Name** (exakt) oder die **id** aus der URL der Richtlinie
`incidentMessageTemplate`	Optional	Freitext (die Nachricht selbst)
`tags`	Optional	Bestehende Tag-Namen, getrennt mit `|`, z. B. `Line 1|Boiler` – siehe Tags zuweisen

TIP

CVE-Monitore gleichen veröffentlichte Sicherheitsmeldungen über `vendor` + `orderCode` und/oder `product` (+ optional `firmware`) mit einem Gerät ab. Siehe CVE-Monitore zur Funktionsweise des Abgleichs.

S7-Datenpunkt-Spalten

Spalte	Erforderlich	Gültige Werte / Format
`address`	Ja	Eine S7-Adresse, z. B. `DB1.DBW0` oder `DB2.DBD4`
`dataType`	Ja	`BOOL`, `BYTE`, `WORD`, `DWORD`, `INT`, `DINT` oder `REAL`
`name`	Nur wenn eine Schwellwert-Spalte zugeordnet ist	Wie die Bedingung und ihr Monitor heißen sollen
`escalationPolicy`	Nur wenn eine Schwellwert-Spalte zugeordnet ist	**Name** (exakt) oder die **id** aus der URL der Richtlinie
`aggregation`	Alle vier, oder keine (siehe unten)	`min`, `max`, `sum`, `avg` (oder `average`), `count`
`operation`	Alle vier, oder keine	`gt` (oder `>`, `above`), `gte` (`>=`), `lt` (`<`, `below`), `lte` (`<=`), `eq` (`=`), `neq` (`!=`)
`operand`	Alle vier, oder keine	Der Schwellwert, z. B. `80` oder `80,5` (ein Komma wird ebenfalls als Dezimaltrennzeichen gelesen)
`duration`	Alle vier, oder keine	Das Aggregationsfenster: Sekunden, oder eine Zahl mit Einheit, z. B. `300`, `5m`, `1h` (auch `2,5m` funktioniert)
`tags`	Optional	Bestehende Tag-Namen, getrennt mit `|` – ignoriert, sofern die Zeile keinen Bedingungsmonitor anlegt (siehe Tags zuweisen)

TIP

Siehe S7-Datenquellen, was jede Adressform und jeder Datentyp bedeutet, und Auf die importierten Werte alarmieren zu den vier Schwellwert-Spalten.

OPC-UA-Datenpunkt-Spalten

Spalte	Erforderlich	Gültige Werte / Format
`nodeId`	Ja	Eine OPC-UA-Node-ID, z. B. `ns=2;s=Line1.Temperature` oder `ns=3;i=1001`
`name`	Nur wenn eine Schwellwert-Spalte zugeordnet ist	Wie die Bedingung und ihr Monitor heißen sollen
`escalationPolicy`	Nur wenn eine Schwellwert-Spalte zugeordnet ist	**Name** (exakt) oder die **id** aus der URL der Richtlinie
`aggregation`	Alle vier, oder keine (siehe unten)	`min`, `max`, `sum`, `avg` (oder `average`), `count`
`operation`	Alle vier, oder keine	`gt` (oder `>`, `above`), `gte` (`>=`), `lt` (`<`, `below`), `lte` (`<=`), `eq` (`=`), `neq` (`!=`)
`operand`	Alle vier, oder keine	Der Schwellwert, z. B. `80` oder `80,5` (ein Komma wird ebenfalls als Dezimaltrennzeichen gelesen)
`duration`	Alle vier, oder keine	Das Aggregationsfenster: Sekunden, oder eine Zahl mit Einheit, z. B. `300`, `5m`, `1h` (auch `2,5m` funktioniert)
`tags`	Optional	Bestehende Tag-Namen, getrennt mit `|` – ignoriert, sofern die Zeile keinen Bedingungsmonitor anlegt (siehe Tags zuweisen)

> **TIP**
>
> Siehe OPC-UA-Konfiguration zur Node-ID-Syntax und dazu, wie der Werttyp eines Datenpunkts gelernt wird, sowie Auf die importierten Werte alarmieren zu den vier Schwellwert-Spalten.

Wenn alle erforderlichen Felder zugeordnet sind, klicken Sie auf **Import starten**. Um den Assistenten zu schließen und Ihre Arbeit zu verwerfen, klicken Sie auf **Abbrechen**; um die Zuordnungen zu behalten und später fortzufahren, schließen Sie den Bereich stattdessen mit der Schaltfläche × in der Kopfzeile – der Assistent setzt dort fort, wo Sie aufgehört haben.

Schritt 3 — Ergebnisse

Eine Zusammenfassung zeigt, wie viele Zeilen erfolgreich importiert wurden und wie viele fehlgeschlagen sind. Ist **Bestehende Monitore aktualisieren** aktiviert, zeigt sie außerdem, wie viele Zeilen statt eines neuen Eintrags einen bestehenden CVE-Monitor oder eine bestehende Bedingung aktualisiert haben.

- **CVE-Monitore** werden zeilenweise übernommen, sodass eine fehlgeschlagene Zeile die übrigen Zeilen nicht davon abhält, angelegt oder aktualisiert zu werden.
- **S7- und OPC-UA-Datenpunkte** (und die Bedingungen, die eine Schwellwert-Zeile anlegt oder aktualisiert) werden gemeinsam übernommen: Ist auch nur eine Zeile fehlgeschlagen, zeigt die Zusammenfassung null Erfolge und null Aktualisierungen, und es wurde nichts geschrieben.

Jede fehlgeschlagene Zeile wird mit der verursachenden Fehlermeldung aufgeführt. Klicken Sie auf **Fehlgeschlagene Zeilen herunterladen**, um nur diese Zeilen als CSV zu exportieren, sie zu korrigieren und die Datei erneut zu importieren.

Verwandte Themen

- Monitore — Monitor-Typen, Konfiguration und Auswertung
- S7-Datenquellen — Datenpunkte von Hand deklarieren, Übernahme und Takt
- OPC-UA-Konfiguration — Datenpunkte von Hand deklarieren, Übernahme und Takt

3.4 Gerätesuche

Die Gerätesuche findet die Geräte in Ihrem Netz, ohne dass Sie deren Adressen vorher kennen müssen. Sie geben Pulse einen Netzbereich vor, Pulse durchsucht ihn nach Siemens-S7-, OPC-UA- und PROFINET-Geräten und zeigt Ihnen, was vorhanden ist — ein Eintrag je Gerät mit allem, was Pulse darüber in Erfahrung gebracht hat. Sie entscheiden anschließend, welche dieser Funde zu Datenquellen werden.

Sie dient zugleich als Bestandsaufnahme. Eine Suche meldet jedes Modul, das geantwortet hat, nicht nur die, aus denen sich Werte lesen lassen, und jeden Host, den sie im Segment gesehen hat — auch die, die kein bekanntes Protokoll sprechen. Was Sie übernehmen können und was in Ihrem Netz steht, sind zwei verschiedene Fragen; die Ergebnisseite beantwortet beide.

Sie öffnen die Gerätesuche über **Assets > Geräte suchen** in der Seitenleiste oder über die Schaltfläche **Geräte suchen** auf der Seite der Datenquellen. Nur Administratoren der Organisation können eine Suche starten.

> **INFO**
>
> Die Gerätesuche meldet ausschließlich, was sie findet. Sie legt niemals selbst eine Datenquelle an — beim Übernehmen gelangen Sie in das gewohnte Anlageformular mit den gefundenen Werten, das Sie selbst bestätigen.

Was die einzelnen Protokolle finden

Protokoll	Wonach gesucht wird
Siemens S7	Jedes Modul, das über ISO-on-TCP antwortet — die CPU und den Kommunikationsprozessor davor. Jedes wird mit Baugruppenträger, Steckplatz, Bestellnummer, Firmware-Version, Seriennummer und Betriebszustand — RUN oder STOP — aufgeführt, soweit es diese meldet.
OPC UA	OPC-UA-Server einschließlich der Endpunkte und Sicherheitseinstellungen sowie — wenn der Server einen ungesicherten Endpunkt anbietet — Herstellername, Produktname und Firmware-Version aus dem Server selbst
PROFINET	PROFINET-Geräte im selben Netzsegment wie der Scanner, gefunden über DCP auf Layer 2, auch solche, die noch keine IP-Adresse haben

Jedes Protokoll wird in Ihrer Lizenz einzeln freigeschaltet. Ist eines nicht freigeschaltet, ist dessen Auswahlfeld deaktiviert und mit **nicht in Ihrem Tarif** gekennzeichnet. Die übrigen funktionieren weiterhin.

Lesezugriff bei S7-1200 und S7-1500

> **Bei S7-1200 und S7-1500 muss PUT/GET freigegeben sein**
>
> Bei diesen Steuerungen ist die PUT/GET-Kommunikation ab Werk abgeschaltet, dasselbe gilt für eine CPU mit vollständigem Schutz. Eine solche Steuerung erscheint zwar im Ergebnis — die Suche erreicht sie —, gibt aber nichts über sich preis: keine Bestellnummer, keine Firmware-Version, keine Seriennummer und keinen Betriebszustand. Ihr Fund ist mit **Lesezugriff deaktiviert** gekennzeichnet, und Pulse kann später auch keine Werte aus ihr lesen.

Damit sie lesbar wird, geben Sie den PUT/GET-Zugriff in den Schutz-Einstellungen der CPU in Ihrem Engineering-Werkzeug frei und starten die Suche erneut. Bei S7-300 und S7-400 ist das in der Regel nicht nötig.

PROFINET erfasst nur ein Segment

> **PROFINET kann keine Routergrenze überschreiten**
>
> PROFINET-Geräte werden über DCP gefunden, und DCP arbeitet auf Layer 2: Die Suche erreicht die Geräte in dem Segment, mit dem der Scanner selbst verbunden ist, und nicht weiter. Ein größer gefasster Netzbereich ändert daran nichts, und ein Router lässt sich nicht überbrücken, unabhängig davon, wie der Bereich geschrieben ist. S7 und OPC UA sind davon nicht betroffen — die werden über IP gescannt und funktionieren wie gewohnt über Routergrenzen hinweg.

Um ein Segment zu erfassen, mit dem die Appliance nicht verbunden ist, scannen Sie es von einem Collector in diesem Segment aus.

Eine Suche starten

1. Öffnen Sie **Assets > Geräte suchen**.
2. Klicken Sie auf **Einstellungen**, um die Sucheinstellungen zu öffnen:
   - **Netzbereich** — Pulse trägt die Netze ein, mit denen das Gerät bereits verbunden ist — in den meisten Anlagen können Sie diese Vorgabe übernehmen. Für andere Netze ersetzen Sie den Eintrag.
   - **Suchen nach** — Wählen Sie die Protokolle aus.

- Sind in Ihrer Organisation Remote-Collectors registriert, **Suchen von** — von dieser Appliance (Standard) oder von einem bestimmten Collector. Verwenden Sie einen Collector, um ein Segment zu erreichen, das die Appliance nicht direkt erreicht. Eine Suche kann nicht gestartet werden, wenn der gewählte Collector nicht aktiv verbunden ist, widerrufen wurde oder aus der Organisation entfernt wurde. Wurde ein zuvor gewählter Collector entfernt, zeigt die Auswahl **Collector entfernt** an seiner Stelle; wählen Sie einen verbundenen Collector oder suchen Sie von dieser Appliance aus.

3. Klicken Sie auf **Suche starten**.

Sobald eine Suche abgeschlossen ist, startet **Erneut suchen** eine neue Suche mit denselben Einstellungen.

Formate für den Netzbereich

Trennen Sie mehrere Einträge durch Leerzeichen oder Kommas. Die Formate lassen sich mischen:

Format	Beispiel
Einzelner Host	`192.168.10.5`
CIDR-Block	`192.168.10.0/24`
Bereich	`192.168.10.10-20`
Ausgeschriebener Bereich	`192.168.10.1-192.168.10.254`

Umfasst ein Bereich sehr viele Hosts, fragt Pulse vor dem Start nach einer Bestätigung. Diese Rückfrage fängt vertippte Präfixe ab — ein `/16` sind erheblich mehr Adressen als ein `/24`.

Alle Baugruppenträger und Steckplätze prüfen

Ein S7-Modul antwortet auf einem bestimmten Baugruppenträger und Steckplatz. Standardmäßig prüft Pulse die vier häufigsten Positionen, was nahezu jede Installation abdeckt.

Ein Aufbau antwortet meist mehrfach. Ist er über einen Kommunikationsprozessor angebunden — etwa einen CP 443-1 in einer S7-400 —, antwortet der CP auf einem eigenen Steckplatz für sich selbst, die CPU dahinter ebenfalls. Beide erscheinen unter demselben Gerät, jeweils mit eigener Bestellnummer und Firmware, denn beide sind Anlagenteile, die Ihnen gehören. **Als Datenquelle übernehmen** bietet nur die CPU an: Ein Kommunikationsprozessor enthält keine Datenbausteine der CPU, eine darauf gerichtete Datenquelle käme also zustande und läse nichts.

Ein einzelnes Modul kann außerdem an mehreren Positionen antworten — eine S7-1500-CPU antwortet auf Steckplatz 1 und auf Steckplatz 0. Sie wird einmal aufgeführt, an der Position, über die eine Datenquelle sie anspricht.

Zeigt ein Gerät einen Kommunikationsprozessor und keine CPU, steckt die CPU meist an einer Position außerhalb der vier standardmäßig geprüften.

Aktivieren Sie **Alle Baugruppenträger und Steckplätze prüfen** (unter Einstellungen), wenn Sie CPUs an ungewöhnlichen Positionen erwarten. Die Suche findet dann mehr, dauert aber deutlich länger, weil jede Position für jede Adresse geprüft wird, die nicht bereits geantwortet hat.

Während der Suche

Die Seite füllt sich laufend, statt erst am Ende ein Ergebnis zu zeigen. Eine **Statusleiste** oberhalb der Ergebnisse zeigt die bisherige Laufzeit sowie die Zahl der Warnungen und Fehler — klicken Sie sie an, um das vollständige Suchprotokoll zu öffnen.

- Die **Ergebnisse**, ein Eintrag je Gerät, die sich im Verlauf der Suche füllen. Verwenden Sie den Filter über der Tabelle, um nach Gerätename, Adresse, Artikelnummer oder Seriennummer einzugrenzen. Klicken Sie auf eine Zeile, um ein Seitenpanel mit allen gefundenen Details zu öffnen — Seriennummer, Gerätename, Funktions- und Ortskennzeichen, Endpunkt-URL und CPU-Zustand.

  Hat ein Gerät auf mehr als ein Protokoll geantwortet oder hat ein Baugruppenträger für mehrere Module geantwortet, können Sie die Zeile über den Aufklappschalter aufklappen, um jeden Fund einzeln zu sehen.

In einem direkt angeschlossenen Netz erscheinen die Geräte, bevor sie geprüft wurden: Die Siemens-S7-Suche fragt zuerst im Segment nach, wer welche Adresse belegt, und diese Antwort ist bereits eine Bestandsaufnahme. Anschließend füllt sich jedes Gerät mit dem, was es tatsächlich spricht. Bei einer Suche über einen Router entfällt dieser Schritt — dort erscheinen die Geräte, sobald sie antworten.

Sie können die Seite verlassen und später zurückkehren — die Suche läuft weiter, und die Seite zeigt sie wieder mit allem, was bisher gefunden wurde. Das gilt auch für einen anderen Browser-Tab oder ein anderes Gerät: Wer die Seite öffnet, während eine Suche läuft, sieht diese Suche und kann sie anhalten. Um vorzeitig abzubrechen, klicken Sie auf **Anhalten**. Bereits gefundene Geräte bleiben erhalten.

Die Adresse der Seite benennt die angezeigte Suche. Ein Lesezeichen oder ein geteilter Link öffnet deshalb genau diese Suche wieder, auch nachdem sie beendet ist. Ohne einen solchen Link zeigt die Seite eine laufende Suche oder ist bereit für eine neue.

Pro Organisation läuft immer nur eine Suche gleichzeitig. Zwei sich überschneidende Suchen würden dieselben Steuerungen gleichzeitig ansprechen. Das kann die begrenzte Zahl an Verbindungen einer S7-300 erschöpfen und ein Programmiergerät aussperren.

Was ein PROFINET-Fund zeigt

Jeder PROFINET-Fund zeigt die MAC-Adresse des Geräts und, sofern vorhanden, dessen IP-Adresse. Pulse fragt anschließend das Gerät selbst nach seinen Identifikationsdaten und ergänzt den Fund um die auf dem Gehäuse aufgedruckte Bestellnummer, die Firmware-Version und die Seriennummer.

Pulse fragt außerdem nach den Kennzeichen, die bei der Inbetriebnahme auf das Gerät geschrieben wurden: seine Funktion und sein Einbauort. Trägt ein Gerät diese Angaben, steht dieser Name über dem Fund — derselbe, der auf Ihrem Schaltschrank und in Ihrer Dokumentation steht — und der PROFINET-Gerätename rückt in die Zeile darunter. Viele Geräte haben keine Kennzeichen, weil die Felder optional sind und oft leer bleiben; über diesen Funden steht dann der PROFINET-Gerätename.

Diese zweite Abfrage ist in beide Richtungen optional. Ein Gerät ohne IP-Adresse lässt sich gar nicht abfragen, ebenso wenig ein Gerät, dessen Adresse außerhalb aller Subnetze der Appliance liegt — über alle Netzwerkschnittstellen hinweg; und nicht jedes Gerät antwortet — manche Firmware unterstützt die Abfrage nicht. Bleibt sie unbeantwortet, ist der Fund dennoch vollständig; er zeigt dann nur, was die Suche allein ermitteln konnte.

Die Abfrage braucht einen Moment. Pulse fragt mehrere Geräte gleichzeitig und gibt einem Gerät, das nicht antwortet, einige Sekunden Zeit, bevor es weitergeht. PROFINET-Funde können deshalb noch kurz nach dem Ende der eigentlichen Suche eintreffen. Nach dreißig Sekunden hört Pulse in jedem Fall auf zu fragen; ein Gerät, das dann noch aussteht, wird mit dem gemeldet, was die Suche allein ermitteln konnte.

Parallel zur I&M0-Abfrage hört Pulse auch auf **LLDP-Ankündigungen** im Segment. Ein PROFINET-Gerät, das sich über LLDP bekannt macht — typischerweise ein Switch oder ein Managed-Gerät —, ergänzt den Fund im Detailbereich um seinen **LLDP-Systemnamen** und seine **LLDP-Systembeschreibung**. Da LLDP ein passives, unabhängiges Protokoll ist, werden diese Werte unabhängig vom Ergebnis der I&M0-Abfrage gespeichert: Ein Switch, der die azyklische Abfrage abgelehnt hat, kann seine vollständigen Identifikationsdaten dennoch über LLDP in derselben Suche senden. Die Systembeschreibung ist der Rohtext, den das Gerät selbst sendet — Herstellername, Produktname und Firmware-Version im Format des Herstellers — und keine in Einzelfelder aufgeteilte Darstellung.

Was ein OPC-UA-Fund zeigt

Jeder OPC-UA-Fund enthält die Endpunkt-URL des Servers und die Sicherheitskonfigurationen, die er bei der Suche angeboten hat. Bietet der Server einen Endpunkt ohne Sicherheit (**None/None**) an, liest Pulse außerdem seine **BuildInfo** — den eigenen Bericht des Servers darüber, was er ist — und ergänzt den Fund um Herstellername, Produktname und Firmware-Version. Das sind dieselben Felder, die PROFINET- und S7-Funde über I&M0 befüllen, sodass eine gemischte Anlage protokollübergreifend einheitlich dargestellt wird.

Bietet der Server nur verschlüsselte oder authentifizierte Endpunkte und keinen ungesicherten an, kann BuildInfo ohne Zugangsdaten nicht gelesen werden. Der Fund ist dennoch vollständig; er zeigt dann nur, was die Endpunktsuche ermitteln konnte.

Was ein S7-Fund zeigt

Der Detailbereich eines S7-Geräts enthält den Abschnitt **Geprüfte Baugruppenträger und Steckplätze**, der zeigt, welche Positionen der Scan geprüft hat und was dabei herausgekommen ist:

Ergebnis	Bedeutung
Hat geantwortet	An dieser Position hat ein Modul geantwortet und Bestellnummer, Seriennummer und Firmware gemeldet.
Hat geantwortet, Identifikation verweigert	Ein Modul hat geantwortet, sich aber nicht identifiziert — siehe Lesezugriff bei S7-1200 und S7-1500.
Verbindung abgelehnt	An dieser Position hat der Scan kein Modul erreicht. Auch ein Modul, dessen Verbindungen alle belegt sind, lehnt ab; eine Position, die bei einem früheren Scan geantwortet hat, kann deshalb ablehnen, während eine Engineering-Station verbunden ist.
Nicht geprüft	Der Scan hat aufgehört, nachdem er 8 Module an diesem Gerät gefunden hat. An dieser Position kann trotzdem ein Modul stecken.

Hat der Scan alle Baugruppenträger und Steckplätze geprüft — mehr als 32 Positionen insgesamt —, werden nur die Positionen, die geantwortet haben, einzeln aufgeführt; Positionen, die die Verbindung abgelehnt haben oder nicht geprüft wurden, werden in einer Zusammenfassungszeile am Ende gezählt.

Warum ein Gerätename verstümmelt aussehen kann

Ein PROFINET-Gerätename darf nur Kleinbuchstaben, Ziffern, Bindestriche und Punkte enthalten. Ein Engineering-Werkzeug muss jeden Namen, der dazu nicht passt, deshalb umschreiben: Es wandelt ihn in Kleinbuchstaben, ersetzt die unzulässigen Zeichen und hängt eine kurze Prüfsumme an. Ein Gerät, das im TIA Portal `Tank4_SRV` heißt, meldet sich deshalb als `tank4xbsrv5554`. Ein Name, der nur kleingeschrieben werden musste, bleibt unverändert. Das TIA Portal zeigt beide Namen in den Eigenschaften der PROFINET-Schnittstelle nebeneinander an, als Gerätename und umgewandelten Namen.

Pulse macht diese Umschreibung rückgängig, soweit das möglich ist. Die Prüfsumme zeigt, dass der Name umgewandelt wurde — über einem Gerät, das sich als `xva34xnh10-kt11a343` meldet, steht deshalb `=a34+h10-kt11`, also die Bezeichnung aus Ihrem Projekt. Zweierlei geht dabei nicht: Großbuchstaben gehen bei der Umwandlung verloren und lassen sich nicht zurückholen, eine Rekonstruktion ist also immer klein geschrieben; und ein Name mit einer Ersetzung, die Pulse nicht kennt, bleibt genau so stehen, wie er gemeldet wurde.

Verborgen wird dabei nichts. Der Name, wie das Gerät ihn meldet, steht weiterhin unter der Überschrift in der Fundzeile und passt damit zu dem, was Sie im Engineering-Werkzeug oder auf der Weboberfläche des Geräts sehen. Über einem Gerät mit Kennzeichen aus der Inbetriebnahme steht stattdessen dieses Kennzeichen — das hat ein Mensch getippt, es ist nicht rekonstruiert.

Wie Pulse den Anschluss eines Geräts empfiehlt

Eine Suche kann dieselbe Maschine dreimal finden: eine CPU auf Port 102, deren eigenen OPC-UA-Server auf 4840 und einen PROFINET-Namen auf dem Draht. Jede Gerätezeile trägt deshalb **eine** Empfehlung statt einer Liste — fahren Sie mit der Maus darüber, um den Grund zu sehen.

Empfehlung	Was sie bedeutet
Symbolisch	Die CPU hat eine S7CommPlus-Sitzung beantwortet, Pulse kann sie also über Symbolnamen lesen, ohne dass etwas freigeschaltet werden muss.
OPC UA	Der eigene OPC-UA-Server des Geräts hat geantwortet. Eine dokumentierte Schnittstelle, und auch sie braucht kein PUT/GET.
S7 (klassisch)	Die CPU hat sich über PUT/GET identifiziert, sie lässt sich also über absolute Adressen lesen.

Empfehlung	Was sie bedeutet
Noch kein Weg	Die CPU hat auf Port 102 geantwortet und auf keines von beidem. Der Tooltip sagt, was sich ändern müsste.

Die Reihenfolge ist keine Geschmacksfrage. Symbolisch steht vorn, weil es die Namen liest, die das Programm ohnehin trägt, und an der Steuerung nichts freigeschaltet werden muss; der eigene OPC-UA-Server der CPU folgt aus demselben PUT/GET-freien Grund; der klassische Weg funktioniert und kostet eine Einstellung, die viele Anlagen bewusst ausgeschaltet lassen.

Noch kein Weg ist eine S7-1200 oder S7-1500 mit ausgeschaltetem PUT/GET und einer Firmware oder einem TIA-Projekt, die älter sind als das symbolische Lesen verlangt. Es öffnet sich durch eines von dreien: das Projekt auf TIA Portal V17 oder neuer migrieren (mit Firmware V2.9 auf einer S7-1500 bzw. V4.5 auf einer S7-1200), den eigenen OPC-UA-Server der CPU einschalten oder den PUT/GET-Zugriff freigeben. Wo die Suche die Firmware lesen konnte und sie bereits neu genug ist, sagt der Hinweis das und nennt nur noch die TIA-Migration.

Eine Suche, die flacher als **Identifizieren** läuft, fragt nichts davon ab; Geräte aus einem solchen Lauf tragen deshalb gar keine Empfehlung.

S7CommPlus-Abfrage im Detailbereich

Der Detailbereich eines Geräts zeigt für jeden S7-Fund ein Feld **S7CommPlus** mit einer von drei Antworten:

Antwort	Was sie bedeutet
Ja	Die CPU hat eine S7CommPlus-Sitzung beantwortet — sie lässt sich über Symbolnamen lesen.
Nein	Die CPU wurde gefragt und hat auf die S7CommPlus-Abfrage nicht geantwortet.
Nicht geprüft	Niemand hat dieses Gerät nach S7CommPlus gefragt. Die Suche endete vor der Identifikation, oder der ausführende Collector ist älter als die Abfrage. Das ist nicht dasselbe wie eine Absage des Geräts.

Suchen von einem älteren Collector aus: Wenn der gewählte Collector die S7CommPlus-Abfrage nicht unterstützt, erscheint auf der Suchseite ein Warnbanner. Klassische S7-Geräte werden weiterhin gefunden; nur die Prüfung auf symbolische Lesbarkeit entfällt. Aktualisieren Sie den Collector, um beides zu prüfen.

Ein gefundenes Gerät übernehmen

Funde, aus denen sich Werte lesen lassen, haben die Schaltfläche **Als Datenquelle übernehmen**. Sie öffnet das Anlageformular des empfohlenen Wegs mit den gefundenen Werten — die Adresse bei einer symbolischen S7-CPU, Adresse mit Baugruppenträger und Steckplatz bei einer klassischen oder die Endpunkt-URL bei OPC UA. Prüfen Sie die Werte und speichern Sie.

Funde ohne diese Schaltfläche sind deshalb nicht weniger echt: Es sind Anlagenteile in Ihrem Netz, die diese Suche erkannt hat, und genau darum stehen sie dort. Ihnen fehlt lediglich etwas, das eine Datenquelle lesen könnte.

Geräte, zu denen bereits eine Datenquelle passt, sind als **Bereits übernommen** gekennzeichnet, damit eine erneute Suche dieselbe Steuerung nicht ein zweites Mal anbietet. Der Detailbereich zeigt dasselbe für jedes Modul, das eine Datenquelle lesen kann — eine klassische oder symbolische S7-CPU, einen OPC-UA-Server — und verlinkt auf die Datenquelle, die es bereits liest.

Manche Funde benötigen zuerst eine Anpassung, bevor sie gelesen werden können:

- **Lesezugriff deaktiviert** — die CPU hat geantwortet, sich aber nicht identifiziert. Das Gerät ist echt und kann übernommen werden, an der Steuerung muss aber zuerst der PUT/GET-Zugriff freigegeben werden, bevor Pulse davon lesen kann. Ist sie zugleich als **Symbolisch** gekennzeichnet, ist das nicht nötig: Sie lässt sich so, wie sie ist, über Symbolnamen lesen.
- **Kommunikationsprozessor** — ein CP vor einem Baugruppenträger. Er ist ein echtes Anlagenteil mit eigener Bestellnummer und Firmware und deshalb wissenswert, enthält aber keine Datenbausteine; es gibt also nichts zu übernehmen. Erscheint er ohne CPU daneben, starten Sie die Suche erneut mit **Alle Baugruppenträger und Steckplätze prüfen** oder prüfen Sie, auf welchem Steckplatz die CPU steckt.
- **Nicht identifiziert** — etwas antwortet auf dem S7-Port, hat aber keine der geprüften Positionen aus Baugruppenträger und Steckplatz angenommen. Das kann eine CPU an einer ungewöhnlichen Position sein, ein Bedienpanel oder ein Gateway. Prüfen Sie alle Baugruppenträger und Steckplätze, um mehr zu erfahren.
- **Im Netz gesehen** — ein Host, der auf die Netzabfrage geantwortet hat, aber auf keines der gesuchten Protokolle. Diese Hosts werden am Ende der Ergebnisse in einer zugeklappten Zählung zusammengefasst; aktivieren Sie **Hosts ohne Protokoll anzeigen**, um sie einzublenden. Über sie ist nichts weiter bekannt als ihre Adresse und, soweit Pulse sie ermitteln konnte, ihre Hardware-Adresse.
- **keine IP-Adresse** — ein PROFINET-Gerät, das im Netzsegment geantwortet hat, aber noch keine nutzbare IP-Adresse besitzt. Es muss zuerst eine erhalten, bevor es überwacht werden kann.

Wenn nichts gefunden wird

- Prüfen Sie, ob der Netzbereich derjenige ist, in dem sich die Steuerungen tatsächlich befinden.
- Prüfen Sie, ob Pulse dieses Netz erreichen kann. Ein Bereich hinter einem Router ist für S7 und OPC UA erreichbar.
- Prüfen Sie bei PROFINET, ob das scannende Gerät — die Appliance oder ein Collector — mit dem Segment verbunden ist, in dem die Geräte stehen: PROFINET kann keine Routergrenze überschreiten.
- Erwarten Sie eine S7-CPU an einem ungewöhnlichen Baugruppenträger oder Steckplatz, starten Sie die Suche erneut mit **Alle Baugruppenträger und Steckplätze prüfen**.

Teil 3 · Monitoring

3.5 Assets

Das Asset-Register ist ein dauerhaftes Verzeichnis jedes Assets, das Ihre Netzwerk-Scans gefunden haben, mit den darin enthaltenen Modulen. Im Gegensatz zur Gerätesuche, die nur die Ergebnisse eines einzelnen Scans anzeigt und sich beim nächsten Scan zurücksetzt, behält das Register alle Assets von einem Scan zum nächsten und aktualisiert sie bei jedem weiteren Scan.

Öffnen Sie das Register über den Eintrag **Assets** in der Seitenleiste. Dieser Eintrag und seine Unterpunkte **Register**, **Geräte suchen**, **Prüfungen** und **Einstellungen** werden nur Organisationsadministratoren angezeigt; ein Mitglied, das einem Link auf eine dieser Seiten folgt, erfährt dort, dass sie Administratoren vorbehalten ist. Die Gerätesuche, die das Register füllt, öffnen Sie über **Assets > Geräte suchen**.

Lizenzvoraussetzung

Das Asset-Register ist ein lizenziertes Feature. Wenn es nicht Teil Ihres Tarifs ist, informiert die Seite darüber. Scans funktionieren weiterhin und ihre Ergebnisse erscheinen unabhängig davon auf der Seite Gerätesuche.

Asset-Liste

Jede Zeile in der Liste stellt ein Asset dar — ein Gerät, das die Scans gefunden haben. Die Liste ist nach dem Namen des Assets sortiert, dann nach der Adresse; Assets ohne Namen folgen den benannten, nach Adresse sortiert. Die Spalten sind:

Spalte	Beschreibung
Asset	Der von Ihrem Team vergebene Name oder der vom Scan gelesene Name. Hat es keinen von beiden, trägt es seine Adresse als Namen; die Spalte **Adresse** wiederholt sie dann nicht.
Adresse	Die IP-Adresse, unter der das Asset gefunden wurde.
Modell	Die Bestellnummer des Hauptmoduls des Assets.
Module	Die im Asset identifizierten Module.
Zuletzt gesehen	Wann ein Scan dieses Asset zuletzt gefunden hat.

Spalte	Beschreibung
Status	Gekennzeichnet ist nur, was einen Blick wert ist: **Nicht identifiziert** für ein Asset, das nicht identifiziert ist, **Offline** für ein Asset, das der letzte Scan nicht gefunden hat, **Außer Betrieb** für ein außer Betrieb genommenes Asset und **Support beendet** für ein Asset mit einem Modul, dessen Herstellersupport ausgelaufen ist. Ein Asset in Betrieb, auf das nichts davon zutrifft, trägt kein Badge.
Verantwortlich	Die Person, das Team oder die Rolle, die Ihr Team als verantwortlich eingetragen hat.
Kritikalität	Die von Ihrem Team zugewiesene Kritikalitätsstufe.
Zone	Die Zone, in der das Asset ist.
Datenquelle	Ob eine Datenquelle von dem Asset liest (siehe Datenquellen).

Ein Verantwortlicher, eine Kritikalität oder eine Zone, die niemand eingetragen hat, erscheint als Strich (–).

Auf einem schmaleren Bildschirm werden die weniger wichtigen Spalten zuerst ausgeblendet, beginnend mit **Zone**, **Kritikalität** und **Verantwortlich**; der Name des Assets und sein **Status** werden immer angezeigt.

Liste filtern

Verwenden Sie das Suchfeld, um nach dem Namen des Assets, der Adresse, der Bestellnummer oder der Seriennummer zu filtern.

Die Chips unter dem Suchfeld teilen das Register nach Lebenszyklus auf: **In Betrieb**, **Offline** für die Assets, die der letzte Scan nicht gefunden hat, und **Außer Betrieb**. Jeder Chip zeigt, wie viele Assets er unter Ihren übrigen Filtern anzeigen würde. Klicken Sie auf einen, um nur diese Assets anzuzeigen, auf einen weiteren, um sie hinzuzunehmen, und auf **Alle**, um wieder jedes Asset anzuzeigen.

Alles Weitere finden Sie unter **Filtern**. In jedem Filter können Sie mehr als eine Antwort ankreuzen:

- **Identifizierung** — nur identifizierte oder nur nicht identifizierte Assets.
- **Datenquelle** — nur Assets **Mit Datenquelle** oder **Ohne Datenquelle**.
- **Zone** — nur die Assets einer Zone oder die in **Keine Zone**. Angeboten werden die Zonen, in denen Assets des Registers sind.

- **Collector** — nur die Assets, die ein Collector gefunden hat, oder die, die **Diese Appliance** mit ihren eigenen Scans gefunden hat. Angeboten wird jeder Collector, von dem aus Assets des Registers gesehen wurden.
- **Ohne Verantwortlichen** — die Assets, denen noch niemand zugewiesen wurde, nützlich beim Überprüfen der Abdeckung.
- **Support beendet** — die Assets mit einem Modul, dessen Herstellersupport ausgelaufen ist.

Die Schaltfläche **Filtern** zeigt, wie viele davon gesetzt sind. Mit ✕ daneben setzen Sie sie und die Lebenszyklus-Chips zurück; Ihre Suche bleibt. Auf dem Smartphone öffnet **Filtern** ein Fenster, das auch den Lebenszyklus enthält, und Ihre Auswahl wird unter dem Suchfeld angezeigt.

Die Anzahl über der Liste zeigt, wie viele Assets dem aktuellen Filter entsprechen und von wie vielen davon eine Datenquelle liest. Wenn keine Assets übereinstimmen, gibt die Seite einen entsprechenden Hinweis aus.

CSV exportieren

Öffnen Sie im Seitenkopf **Exportieren** und wählen Sie **Inventar (CSV)**, um das vollständige Register als Tabelle herunterzuladen. Die Datei ist mit dem Exportdatum benannt und enthält alle Assets unabhängig vom aktuellen Filter.

Wie jede CSV-Datei, die Sie aus dem Register erhalten, ist sie reines CSV: Die Spaltennamen stehen in der ersten Zeile, darunter folgen die Zeilen, sodass eine Tabellenkalkulation, eine Datenbank oder ein Importwerkzeug sie so liest, wie sie ist. Jede Zeile beginnt mit **snapshot_taken_at**, dem Zeitpunkt des Exports in UTC, sodass das Datum bei den Zeilen bleibt, wie auch immer Sie sie sortieren oder kopieren. Die Datei enthält eine Zeile je Modul; ein Asset ohne identifiziertes Modul ist eine Zeile mit leeren Modulspalten. Das Register enthält, was die Netzwerkerkennung erreicht hat; fehlt ein Gerät in der Datei, ist das also kein Beleg dafür, dass es nicht im Netzwerk ist.

Neben den Angaben zu jedem Asset und seinen Modulen enthält die Datei:

- **application_uri** und **application_name** — die ApplicationUri und den Anwendungsnamen, den der OPC-UA-Server des Assets bei der Erkennung über sich selbst gemeldet hat, sofern vorhanden.
- **all_addresses**, **all_mac_addresses**, **all_application_uris** — alle Adressen, MAC-Adressen und ApplicationUris, unter denen das Asset antwortet, durch Semikolons getrennt. Ein Asset, das aus anderen Assets zusammengeführt wurde, kann unter mehr als einer Adresse antworten.
- **lifecycle_status**, **decommissioned_at**, **decommission_reason** — `active` für ein Asset in Betrieb, `offline` für eines, das der letzte Scan, der es abgedeckt hat, nicht gefunden hat, `decommissioned` für ein außer Betrieb genommenes Asset, und für ein

außer Betrieb genommenes Asset, wann (in UTC) und warum.

- **component_removed_at** — für ein Modul, dessen Entfernung Scans nachgewiesen haben, wann (in UTC); leer für ein vorhandenes Modul. Ein entferntes Modul behält seine Zeile, zählt aber nicht in **component_count**.
- **zone**, **zone_security_level**, **zone_is_safety** — die Zone, in der das Asset ist, ihr Ziel-Security-Level (SL-T) und `yes` oder `no` dafür, ob sie eine Safety-Zone ist. Für ein Asset ohne Zone sind alle drei leer, und **zone_security_level** ist leer für eine Zone ohne festgelegte SL-T.
- **support_end** — für ein Modul das Datum, an dem sein Herstellersupport endet, als `YYYY-MM-DD`; leer, wenn keines erfasst ist.

Dies sind die letzten Spalten; die Spalten davor behalten ihre Position.

Änderungsprotokoll exportieren

Öffnen Sie **Exportieren** und wählen Sie **Änderungsprotokoll (CSV)…**, um alles herunterzuladen, was das Register in einem Zeitraum erfasst hat, etwa für eine Prüfung. Wählen Sie unter **Von** und **Bis** den ersten und den letzten Tag — beide Tage sind eingeschlossen — und klicken Sie auf **CSV herunterladen**. Voreingestellt sind die letzten 90 Tage; ein Zeitraum darf höchstens 366 Tage umfassen. Für einen längeren sagt der Dialog das neben den Tagen und lädt nichts herunter; exportieren Sie ihn dann Jahr für Jahr. Die Tage gelten als UTC-Tage, wie jede Zeitangabe in der Datei. Der Zeitraum richtet sich danach, wann eine Änderung geschah (**occurred_at**).

Die Datei listet eine Zeile je Änderung, die älteste zuerst: jeden Eintrag, den der Verlauf der Assets zeigt, und jede Entscheidung zu den CVEs eines Moduls (siehe Schwachstellen). Hat sich im Zeitraum nichts geändert, enthält die Datei nur die Spaltennamen. Jede Zeile enthält:

- **occurred_at** und **recorded_at** — wann die Änderung geschah und wann Pulse sie erfasst hat, in UTC.
- **station_id**, **station_name**, **station_address** — das Asset, so benannt, wie die Liste es heute nennt.
- **event_type** — was geschah, etwa `discovered`, `firmware_changed`, `curated_field_changed`, `merged` oder `status_changed`; `cve_decision` für eine CVE-Entscheidung.
- **actor** — wer die Änderung vorgenommen hat: der Name der Person, `scan` für eine Änderung, die ein Scan gefunden hat (mit der Nummer des Scans in **run_id**), `system` für eine, die Pulse selbst vorgenommen hat, etwa eine abgelaufene Risikoakzeptanz. Leer, wenn das Konto der Person inzwischen gelöscht wurde.
- **module_rack**, **module_slot**, **module_order_code**, **module_serial_number** — das Modul, um das es geht, sofern vorhanden.

- **field**, **old_value**, **new_value** — was sich geändert hat, von welchem zu welchem Wert: etwa die Firmware-Version, die Adresse, eines der Felder unter Ihre Angaben oder bei einer CVE-Entscheidung die CVE mit der vorherigen und der neuen Entscheidung.
- **details** — was die Änderung sonst festgehalten hat, etwa den Grund, aus dem ein Asset außer Betrieb genommen oder eine CVE-Entscheidung getroffen wurde, und bis wann ein Risiko akzeptiert ist.
- **period_start**, **period_end**, **period_clock**, **exported_at** — in jeder Zeile gleich: der Zeitraum der Datei in UTC, vom Beginn des ersten Tages bis zum Beginn des Tages nach dem letzten; `occurred_at`, weil sich der Zeitraum danach richtet, wann jede Änderung geschah; und der Zeitpunkt, zu dem Sie die Datei exportiert haben. Asset-Namen und Adressen sind so, wie sie zu diesem Zeitpunkt sind.

Wurden zwei Assets zusammengeführt, steht der Verlauf des absorbierten Assets unter dem Asset, in das es zusammengeführt wurde; nachdem die Zusammenführung aufgehoben wurde, wieder unter dem wiederhergestellten Asset.

Schwachstellenstatus exportieren

Öffnen Sie **Exportieren** und wählen Sie **Schwachstellenstatus (CSV)**, um herunterzuladen, was zu den CVEs der Module im Register gefunden und entschieden wurde, etwa als Nachweis, wie mit jedem Mangel umgegangen wurde. Die Datei zeigt den Stand zum Zeitpunkt des Herunterladens.

Der Abgleich erreicht nur Module, die ein CVE-Monitor überwacht, und nur die Sicherheitsmeldungen, die der Schwachstellen-Feed enthält: Module, die nichts identifiziert hat, und Module, die kein CVE-Monitor überwacht, stehen nicht in der Datei, und eine CVE, die der Feed nicht enthält, wird keinem Modul zugeordnet; die Datei ist daher kein Beleg dafür, dass ein Modul keine weitere Schwachstelle hat. Sie enthält eine Zeile für jede CVE, die je für ein Modul zutraf oder zu der eine Entscheidung erfasst wurde, offen oder geschlossen:

- **station_id**, **station_name**, **station_address** — das Asset, dem das Modul heute gehört, so benannt, wie die Liste es nennt.
- **module_rack**, **module_slot**, **module_order_code**, **module_firmware_version**, **module_serial_number** — das Modul, mit der Firmware, die es heute hat.
- **cve_id**, **severity**, **cvss_score** — die CVE, mit Schweregrad und Bewertung, sofern der Fund sie enthält.
- **state** — `open`, solange die CVE für das Modul zutrifft, `closed`, sobald eine Prüfung sie nicht mehr findet. **closed_reason** nennt den Grund: `fixed`, wenn sie mit einem Firmware-Wechsel verschwunden ist, `no_longer_matched`, wenn sie aus einem anderen Grund nicht mehr zutrifft, etwa nach einer Änderung im Schwachstellen-Feed.

- **first_matched_at** und **closed_at** — wann die CVE erstmals für das Modul zutraf und wann sie nicht mehr gefunden wurde, in UTC.
- **decision**, **decision_reason**, **risk_accepted_until** — die geltende Entscheidung, ihre Begründung und bei einer Risikoakzeptanz, bis wann sie gilt. `affected` bedeutet, dass noch niemand eine Entscheidung erfasst hat; `open` ist eine Entscheidung, die die CVE wieder auf offen gesetzt hat, etwa eine abgelaufene Risikoakzeptanz.
- **decision_source**, **decided_by**, **decided_at** — was die Entscheidung erfasst hat (`user`, `expiry` für eine abgelaufene Risikoakzeptanz, `merge` für eine Entscheidung, die beim Zusammenführen zweier Assets beibehalten wurde), wer sie getroffen hat und wann. **decided_by** ist `system` bei einem Ablauf oder einer Zusammenführung und leer, wenn das Konto der Person inzwischen gelöscht wurde.
- **status_as_of**, **catalog_advisory_count** — in jeder Zeile gleich: der Zeitpunkt, auf den sich der Stand bezieht, in UTC, und gegen wie viele Sicherheitsmeldungen die Module abgeglichen wurden, das **Abgeglichen mit N Sicherheitsmeldungen** der Asset-Seite. **catalog_advisory_count** ist leer, solange der Schwachstellen-Feed noch nicht geantwortet hat und die Zahl daher nicht bekannt ist.

Ohne CVE-Überwachung in Ihrer Lizenz wird nichts abgeglichen: Die Datei enthält nur die Spaltennamen und listet keine CVE, so wie die Asset-Seite keine zeigt.

Register prüfen

Ein Administrator kann das Register prüfen und abzeichnen, etwa einmal im Quartal. So gibt es einen Nachweis, wer es angesehen hat, wann und was es in diesem Moment enthielt. Unter den Filtern zeigt die Assets-Seite, wann und von wem das Register zuletzt geprüft wurde, oder dass es noch nicht geprüft wurde. Öffnen Sie **Assets > Prüfungen** in der Seitenleiste, um jede Prüfung zu sehen, und klicken Sie auf **Register prüfen**, um eine zu beginnen.

Die Prüfseite zeigt, was sich seit der letzten Prüfung geändert hat: Der Zeitraum beginnt mit dem Moment, in dem die letzte Prüfung abgezeichnet wurde, bei der ersten Prüfung 90 Tage zuvor. Der Zeitraum einer Prüfung richtet sich danach, wann Pulse eine Änderung erfasst hat (**recorded_at** im Änderungsprotokoll), nicht danach, wann sie geschah. Eine Änderung, die erst nach einer Prüfung erfasst wurde — etwa von einem Scan, der später fertig wurde —, gehört deshalb zur nächsten Prüfung, auch wenn sie vor dem Abzeichnen geschah. Für jedes Asset, an dem sich etwas geändert hat, listet sie die Einträge seines Verlaufs in diesem Zeitraum und die CVE-Entscheidungen zu seinen Modulen, jeweils mit der Entscheidung, die sie ersetzt hat. Darunter listet sie jede CVE, die an einem Modul noch offen ist, mit der geltenden Entscheidung (siehe Schwachstellen); ohne CVE-Überwachung in Ihrer Lizenz sagt sie das stattdessen. Enthält der Zeitraum mehr als 500 Änderungen, zeigt die Seite die neuesten 500; das eingefrorene Änderungsprotokoll enthält jede einzelne.

Schreiben Sie bei Bedarf eine **Notiz** — was Sie geprüft haben oder was ein Auditor wissen sollte, bis zu 2.000 Zeichen — und klicken Sie auf **Abzeichnen**. Pulse hält fest, wer abgezeichnet hat (den Anzeigenamen des Kontos oder seine E-Mail-Adresse), wann und die Notiz, und friert drei Dateien so ein, wie sie in diesem Moment sind:

- **asset-register.csv** — der CSV-Export des Registers in diesem Moment, dieselbe Datei, die Ihnen die Liste zu diesem Zeitpunkt gegeben hätte. Wer die Prüfung wann abgezeichnet hat, hält die Prüfung selbst fest, ebenso die **reviews.csv** des Audit-Pakets.
- **change-log.csv** — das Änderungsprotokoll des Zeitraums der Prüfung, vom Moment der vorherigen Prüfung bis zu dem dieser, danach, wann jede Änderung erfasst wurde (seine **period_clock** ist `recorded_at`). Der Zeitraum der nächsten Prüfung beginnt, wo dieser endet, sodass sich die Änderungsprotokolle zweier aufeinanderfolgender Prüfungen weder überschneiden noch eine Lücke lassen.
- **vulnerability-status.csv** — der Schwachstellenstatus in diesem Moment.

Alle drei Dateien beschreiben denselben Moment: Eine Änderung, die Pulse erfasst, während Sie abzeichnen, steht in allen dreien oder in keiner. Erfasst das Register gerade Änderungen, wenn Sie auf **Abzeichnen** klicken — etwa weil ein Scan eingearbeitet wird —, und ist es einige Sekunden später noch nicht fertig, wartet Pulse nicht darauf: Die Seite meldet, dass das Register gerade Änderungen aufzeichnet, nichts wird abgezeichnet, und Ihre Notiz bleibt, wie Sie sie geschrieben haben, sodass Sie einen Moment später erneut auf **Abzeichnen** klicken können.

Die Seite **Prüfungen** listet die Prüfungen, die neueste zuerst, je eine Zeile: wann abgezeichnet wurde, von wem, der Anfang der Notiz und wie viele Dateien die Prüfung eingefroren hat. Klappen Sie eine Zeile auf, sehen Sie den Zeitraum, den sie umfasst, die ganze Notiz und ihre drei Dateien. Jede Datei zeigt ihren SHA-256, der beim Abzeichnen berechnet wurde, und **Herunterladen** liefert die Datei genau so, wie sie gespeichert wurde, gleich wie sich das Register seither geändert hat. Um eine Kopie zu prüfen, vergleichen Sie ihren SHA-256 mit dem angezeigten, etwa mit `sha256sum change-log.csv`. Die Schaltfläche neben einem SHA-256 kopiert ihn in die Zwischenablage.

Eine Prüfung kann weder geändert noch gelöscht werden. Zeichnet ein anderer Administrator eine Prüfung ab, während Sie die Seite lesen, zeichnet Pulse Ihre nicht ab: Die Seite zeigt stattdessen, was sich seit dieser Prüfung geändert hat, damit Sie es sich vor dem Abzeichnen noch einmal ansehen können.

Prüfintervall festlegen

Wie oft das Register geprüft wird, legt Ihr Managementsystem für Informationssicherheit fest; TISAX etwa verlangt ein festgelegtes Intervall, kein bestimmtes. Administratoren stellen es auf dem Tab **Prüfintervall** in den Einstellungen des Registers ein (**Assets >**

Einstellungen in der Seitenleiste): **Kein Intervall** (die Voreinstellung), **Alle 3 Monate**, **Alle 6 Monate** oder **Alle 12 Monate**. Klicken Sie auf **Speichern**; es gilt sofort.

Mit einem Intervall nennt die Zeile unter den Filtern der Assets-Seite zusätzlich, wann die nächste Prüfung fällig ist:

- **Prüfung fällig in 42 Tagen.** — die nächste Prüfung ist in so vielen Tagen ab heute fällig. Sie ist das Intervall nach dem Abzeichnen der letzten Prüfung fällig: Eine am 14. Juli abgezeichnete Prüfung ist mit **Alle 3 Monate** am 14. Oktober fällig. Eine Prüfung vom letzten Tag eines Monats wird am letzten Tag eines kürzeren Monats fällig, der 31. August plus 3 Monate ist also der 30. November.
- **Prüfung heute fällig.** — heute ist der Tag, an dem sie fällig ist.
- **Überfällig seit 14.10.2026.** (hervorgehoben) — der Tag, an dem sie fällig war, ist vorbei. Sie bleibt überfällig, bis jemand eine Prüfung abzeichnet; die nächste ist dann das Intervall nach dieser Prüfung fällig.

Wurde das Register noch nie geprüft, ist die erste Prüfung ab dem Moment fällig, in dem das Intervall gespeichert wurde: Die Zeile zeigt sofort **Prüfung heute fällig.**, und ab dem nächsten Tag ist die Prüfung überfällig. Wird dasselbe Intervall erneut gespeichert, verschiebt sich dieser Moment nicht; ein anderes Intervall verschiebt ihn. Mit **Kein Intervall** zeigt die Zeile kein Fälligkeitsdatum.

Die Tage werden in der Zeitzone der Organisation gezählt, für jeden Administrator gleich, wo immer er sich befindet. Eine überfällige Prüfung löst keinen Vorfall aus und verschickt keine Benachrichtigung: Sie wird auf der Assets-Seite angezeigt und sonst nirgends, und die Vorfälle des Registers bleiben bei der Anlage.

Audit-Paket herunterladen

Das Audit-Paket ist das, was Sie einem Auditor übergeben: eine ZIP-Datei mit allem, wonach er zum Register fragt, in der Reihenfolge, in der er üblicherweise fragt. Es gibt zwei:

- **Das abgezeichnete Paket** — klicken Sie auf der Seite **Prüfungen** bei einer Prüfung auf **Audit-Paket herunterladen**. Es enthält die drei Dateien, die diese Prüfung eingefroren hat, genau so, wie sie gespeichert wurden, gleich wie sich das Register seither geändert hat.
- **Das aktuelle Paket** — öffnen Sie auf der Assets-Seite **Exportieren** und wählen Sie **Audit-Paket (ZIP)**. Pulse erstellt es in diesem Moment aus dem Register, wie es ist; niemand hat es abgezeichnet. Sein Änderungsprotokoll umfasst die Zeit seit der letzten Prüfung, oder die letzten 90 Tage, wenn das Register noch nie geprüft wurde — das, was die nächste Prüfung umfassen würde.

Beide Pakete enthalten dieselben sechs Dateien:

- **snapshot.csv** — der CSV-Export des Registers. In einem abgezeichneten Paket ist es die **asset-register.csv** der Prüfung, dieselben Bytes unter dem Namen, den das Paket ihr gibt.
- **change-log.csv** — das Änderungsprotokoll des Zeitraums des Pakets.
- **vulnerability-status.csv** — der Schwachstellenstatus.
- **zones.csv** — Ihre Zonen, eine Zeile je Zone, mit Beschreibung, Ziel-Security-Level (SL-T), Verantwortlichem, Safety-Kennzeichen und der Zahl der Assets darin. Eine Prüfung friert die Zonen nicht ein; diese Datei zeigt sie daher so, wie sie beim Herunterladen sind.
- **reviews.csv** — eine Zeile je Prüfung, die älteste zuerst: wer wann abgezeichnet hat, die Notiz, der umfasste Zeitraum und der SHA-256 jeder eingefrorenen Datei. In einem abgezeichneten Paket listet sie die Prüfungen bis einschließlich dieser. Ohne Prüfung enthält sie nur ihre Kopfzeile.
- **README.txt** — in Ihrer Sprache: ob das Paket abgezeichnet oder aktuell ist, wann und von wem es heruntergeladen wurde, der Zeitraum des Änderungsprotokolls, was jede Datei bedeutet und was das Register abdeckt. Das Register enthält, was die Netzwerkerkennung erreicht hat, und die Schwachstellenzuordnung reicht so weit wie der CVE-Katalog; keine der Dateien belegt also, dass sonst nichts da ist.

Der Dateiname jedes Pakets nennt Ihre Organisation und das Datum, etwa `pulse-audit-pack-acme-plant-2026-10-17.zip`, der eines abgezeichneten Pakets das Datum seiner Prüfung, etwa `pulse-audit-pack-acme-plant-reviewed-2026-10-14.zip`. In einem aktuellen Paket sind die Momentaufnahme und der Schwachstellenstatus dieselben Dateien, die Sie in diesem Moment aus ihren eigenen Exporten erhalten; sein Änderungsprotokoll ist das, das die nächste Prüfung einfrieren würde, danach, wann jede Änderung erfasst wurde. Um die Dateien eines abgezeichneten Pakets zu prüfen, vergleichen Sie den SHA-256 jeder Datei mit ihrer Zeile in `reviews.csv` oder mit der Prüfung auf der Seite **Prüfungen**, etwa mit `sha256sum snapshot.csv`.

Identifizierung

Jedes Asset ist entweder **identifiziert** oder **nicht identifiziert**. Ein nicht identifiziertes Asset ist in der Liste und auf seiner Seite mit einem Badge gekennzeichnet, ein identifiziertes nur auf seiner Seite.

- **Identifiziert** — mindestens ein Modul hat sowohl eine Bestellnummer als auch eine Seriennummer gemeldet, oder der OPC-UA-Server des Assets hat eine eigene ApplicationUri bekannt gegeben. Spätere Scans erkennen das Asset an diesen Werten wieder, auch wenn sich seine Adresse ändert.

- **Nicht identifiziert** — kein Modul hat beide Werte gemeldet, und das Asset hat keine OPC-UA-ApplicationUri. Das Asset bleibt unter der zuletzt gesehenen Adresse gelistet. Das ist normal für Switches, Panels und andere Geräte ohne PROFINET-IO-Rolle.

Ein Hinweis unterhalb der Liste gibt an, wie viele Assets nicht identifiziert sind. Diese Information dient der Orientierung — nicht identifizierte Assets sind echte Geräte im Netzwerk und werden aus diesem Grund aufgeführt.

Asset-Details

Klicken Sie auf eine Zeile, um die Detailseite des Assets zu öffnen. Sie zeigt:

- **Asset** — Adresse, MAC-Adresse, die Appliance, die es gefunden hat, Datum der ersten und letzten Sichtung, wann ein Scan es zuletzt abgedeckt hat (siehe Offline-Assets), wann eine Datenquelle es zuletzt gelesen hat und welche (siehe Was Datenquellen dem Register sagen), sowie Identifizierungsstatus. Wenn das Asset mit anderen zusammengeführt wurde, werden alle Adressen und MAC-Adressen, unter denen es antwortet, aufgelistet.
- **OPC-UA-Server (beobachtet)** — die ApplicationUri und den Anwendungsnamen, den der OPC-UA-Server des Assets bei der Erkennung über sich selbst gemeldet hat. Diese Werte wurden beobachtet, nicht von einer Person eingetragen. Die ApplicationUri identifiziert das Asset; der Anwendungsname dient nur zur Information. Wird nur angezeigt, wenn das Asset einen OPC-UA-Server hat.
- **Vom Gerät gemeldet** — den LLDP-Systemnamen und die LLDP-Systembeschreibung, die das Gerät im Netzwerk bekannt gegeben hat. Diese Angaben dienen nur zur Information und werden nicht zur Identifizierung des Assets verwendet.
- **Module** — eine Tabelle aller im Asset gefundenen Module mit Einbauposition, Typ, Bestellnummer, Firmwareversion, Seriennummer, dem Datum der letzten Sichtung, bei einer CPU ihrer aktuellen Betriebsart (RUN oder STOP) und wann sie zuletzt gelesen wurde, sowie dem Datum, an dem sein Herstellersupport endet. Ein Modul, dessen Entfernung Scans nachgewiesen haben, bleibt in der Tabelle, unter den übrigen, mit **Entfernt** und dem Datum gekennzeichnet, und zählt nicht zu den Modulen des Assets. Mit CVE-Überwachung zeigt eine Spalte **CVE-Überwachung**, ob ein CVE-Monitor das jeweilige Modul überwacht (siehe Ein Modul auf CVEs überwachen). Ist die Tabelle zu schmal für alle Spalten, wird zuerst **Zuletzt gesehen** ausgeblendet, dann die Seriennummer, der Typ und das Supportende; Einbauposition, Bestellnummer, Firmware und CVE-Überwachung werden immer angezeigt.
- **Schwachstellen** — mit CVE-Überwachung die CVEs, die auf die Module des Assets zutreffen, und was zu jeder entschieden wurde (siehe Schwachstellen).

- **Datenquellen** — die Datenquellen, die von diesem Asset lesen (siehe Datenquellen).
- **Ihre Angaben** — die von Ihrem Team gepflegten Felder (siehe unten).
- **Verlauf** — ein Protokoll dessen, was das Register zum Asset festgehalten hat: wann es entdeckt wurde und was es damals identifiziert hat — die ApplicationUri seines OPC-UA-Servers oder Bestellnummer und Seriennummer eines Moduls, mit dem Modul, als das der Scan es gefunden hat; wann sich seine Firmware, seine Adresse oder die Betriebsart einer seiner CPUs geändert hat; wann ein Modul hinzugefügt oder entfernt wurde; wann jemand seine Angaben oder das Supportende eines Moduls bearbeitet hat; wann unter seiner Adresse ein anderes Gerät gefunden wurde; wann zwei Assets zu diesem zusammengeführt wurden oder eine Zusammenführung aufgehoben wurde; und wann sich sein Status geändert hat — ein Scan hat das Asset nicht oder wieder gefunden, alle Datenquellen, die es lesen, haben die Verbindung verloren oder eine von ihnen hat wieder geantwortet, oder ein Administrator hat es außer Betrieb oder wieder in Betrieb genommen. Einträge werden nur hinzugefügt; keiner kann geändert oder entfernt werden. Jeder Eintrag ist eine Zeile, die sagt, was sich geändert hat; klicken Sie darauf, um die Einzelheiten zu sehen. Zuerst werden die fünf neuesten Einträge angezeigt; klicken Sie darunter auf **Mehr anzeigen**, um die übrigen der 20 neuesten zu sehen, und erneut, um die nächsten 20 zu laden.

Ihre Angaben

Die Karte **Ihre Angaben** enthält, was Ihr Team über das Asset weiß und ein Scan nicht herausfinden kann. Scans überschreiben diese Felder nie.

Klicken Sie auf **Bearbeiten**, um das Formular zu öffnen. Die Felder sind:

Feld	Beschreibung
Name	Wie Ihr Werk dieses Asset nennt, zum Beispiel „SPS Linie 3". Wird anstelle des Scan-Namens angezeigt.
Verantwortlich	Wer dafür zuständig ist: eine Person, ein Team oder eine Rolle.
Kritikalität	Niedrig, Mittel, Hoch oder Kritisch. Wählen Sie **Nicht bewertet**, wenn dies noch nicht beurteilt wurde.
Standort	Wo das Asset physisch steht: Halle, Schaltschrank, Rack.
Sicherheitssystem	Ob das Asset Teil eines Sicherheitssystems ist. Wählen Sie **Nicht bewertet**, wenn das noch niemand entschieden hat.
Notizen	Freie Notizen zum Asset.

Feld	Beschreibung
Zone	Die Zone, in der das Asset ist. Wählen Sie **Keine Zone**, um es aus seiner Zone zu nehmen.

Wenn das PROFINET-Funktions-Tag oder das Standort-Tag des Assets einen Wert enthält, den Ihr Team bei der Inbetriebnahme eingetragen hat, bietet das Formular an, diesen als Name oder Standort zu übernehmen. Das Feld wird erst gespeichert, wenn Sie die Übernahme bestätigen und auf **Speichern** klicken.

Jedes Speichern, das etwas ändert, fügt dem **Verlauf** des Assets einen Eintrag hinzu: Er nennt, wer gespeichert hat, und listet jedes geänderte Feld mit seinem Wert vorher und nachher auf.

> TIP
>
> **Kritikalität** und **Sicherheitssystem** haben einen Zustand „noch nicht bewertet", der sich von einem bewussten „nicht kritisch" oder „kein Sicherheitssystem" unterscheidet. Verwenden Sie ihn, bis Ihr Team das Asset geprüft hat — ein nicht geprüfter Eintrag sieht anders aus als ein geprüfter.

Supportende

Hersteller stellen den Support für ihre Module nach einiger Zeit ein: keine Firmware-Updates und keine Sicherheitskorrekturen mehr. Ein Modul nach diesem Datum ist ein Risiko, mit dem Sie planen sollten. Ein Scan kann das Datum nicht vom Gerät lesen, deshalb erfasst Ihr Team es für jedes Modul, aus den Lebenszyklusangaben des Herstellers.

Öffnen Sie dazu das Asset und klicken Sie in der Tabelle **Module** in der Spalte **Supportende** des Moduls auf das Stiftsymbol. Wählen Sie das Datum und klicken Sie auf **Speichern**. Um ein Datum zu entfernen, öffnen Sie es erneut und klicken Sie auf **Datum entfernen**. Die Tabelle zeigt, wer das Datum erfasst hat, und **Nicht erfasst** für ein Modul ohne Datum. Ist die Tabelle zu schmal für die Spalte, etwa auf einem Smartphone, wird sie ausgeblendet; das Asset wird trotzdem gekennzeichnet.

Ab diesem Datum ist das Modul mit **Support beendet** gekennzeichnet, ebenso das Asset: oben auf seiner Seite und in der Spalte **Status** der Asset-Liste. Das Datum gilt in der Zeitzone Ihrer Organisation, die Kennzeichnung erscheint also um Mitternacht Ortszeit, für alle gleich. Ein Modul, dessen Entfernung Scans nachgewiesen haben, kennzeichnet sein Asset nicht. Alle solchen Assets finden Sie in der Liste unter **Filtern** mit **Support beendet**.

Scans ändern das Datum nie. Ein Modul, das durch eines mit anderer Seriennummer im selben Baugruppenträger und Steckplatz ersetzt wird, ist ein neues Modul: Es hat kein Datum, bis Ihr Team eines erfasst. Jede Änderung des Datums fügt dem **Verlauf** des Assets einen Eintrag hinzu, der das Modul nennt, mit dem Datum vorher und nachher.

Wenn zwei Assets zusammengeführt werden, behält jedes Modul sein Datum. Hatten beide Assets dasselbe Modul, behält das zusammengeführte Modul das zuletzt erfasste Datum. Das Aufheben der Zusammenführung gibt jedem Modul sein eigenes Datum zurück, es sei denn, jemand hat es nach der Zusammenführung geändert.

Hat ein anderer Administrator das Datum geändert, während Sie die Seite geöffnet hatten, wird Ihr Speichern nicht übernommen: Die Seite zeigt stattdessen sein Datum, und Sie können es erneut bearbeiten.

Der CSV-Export enthält das Datum in der Spalte **support_end**.

Zonen

Zonen fassen Assets mit denselben Security-Anforderungen zusammen, wie es IEC 62443 vorsieht: nach Risiko und Kritikalität, nicht nach Netzwerk. Ein Asset ist in einer Zone oder in keiner. Das neben **Zonen** in den Einstellungen des Registers erklärt Zonen, Conduits und die Security-Level und verlinkt den kostenlosen Quick Start Guide der ISA Global Cybersecurity Alliance zu IEC 62443.

Administratoren pflegen die Zonen auf dem Tab **Zonen** in den Einstellungen des Registers (**Assets > Einstellungen** in der Seitenleiste). Klicken Sie auf **Zone hinzufügen** und füllen Sie aus:

Feld	Beschreibung
Name	Zum Beispiel „Zelle 2“ oder „Verpackungslinie“. Zonennamen sind in Ihrer Organisation eindeutig, ohne Beachtung der Groß- und Kleinschreibung.
Ziel-Security-Level (SL-T)	Das Security-Level, das die Zone erreichen soll, von 0 bis 4, wie IEC 62443 es definiert, oder **Nicht festgelegt**.
Verantwortlich	Wer für die Zone verantwortlich ist: eine Person, ein Team oder eine Rolle.
Safety-Zone	Ob die Zone als Safety-Zone ausgewiesen ist, also für die funktionale Sicherheit von Mensch und Anlage.
Beschreibung	Freie Notizen zur Zone.

Jede Zone in der Liste zeigt ihre SL-T, ob sie eine Safety-Zone ist, wer für sie verantwortlich ist und wie viele Assets in ihr sind. Klicken Sie auf das Stift-Symbol einer Zone, um sie zu bearbeiten.

Um ein Asset in eine Zone zu legen, öffnen Sie das Asset, klicken unter Ihre Angaben auf **Bearbeiten**, wählen die Zone unter **Zone** und klicken auf **Speichern**. Die Karte zeigt dann die Zone mit ihrer SL-T und, bei einer Safety-Zone, ein Abzeichen **Safety-Zone**. Wie bei jedem anderen Feld dort wird die Änderung im **Verlauf** des Assets festgehalten, mit dem Namen der Zone vorher und nachher. Wird eine Zone später umbenannt, ändert das die schon festgehaltenen Einträge nicht.

Die Zone vieler Assets festlegen

Um viele Assets auf einmal in eine Zone zu legen, verwenden Sie die Asset-Liste:

1. Filtern Sie die Liste auf die gewünschten Assets. Ein Collector steht meist in einem Netzwerksegment, deshalb ist der Filter **Collector** oft ein guter Anfang. Die Assets eines Collectors sind aber keine Zone: Sie entscheiden, in welche Zone sie gehören.
2. Klicken Sie neben **Filter** auf **Auswählen**. Klicken Sie die Assets an, oder haken Sie über der Tabelle **Alle auswählen** an, um alle angezeigten Assets auszuwählen. Halten Sie beim Klicken die Umschalttaste gedrückt, um alle Assets zwischen dem zuletzt angeklickten und diesem auszuwählen.
3. Klicken Sie in der Leiste am unteren Seitenrand auf **Zone festlegen…**, wählen Sie eine Zone oder **Keine Zone** und bestätigen Sie.

Wenn Sie einen Filter ändern, wird die Auswahl aufgehoben, sodass nur Assets geändert werden, die Sie sehen. Bis zu 1000 Assets lassen sich auf einmal festlegen. Mit Esc heben Sie die Auswahl auf, mit einem weiteren Esc oder einem erneuten Klick auf **Auswählen** verlassen Sie den Auswahlmodus. Auf Smartphones gibt es den Auswahlmodus nicht.

Jedes Asset wird gespeichert, als wären seine eigenen Angaben gespeichert worden, und sein **Verlauf** hält die Änderung mit dem Namen der Zone vorher und nachher fest. Ein Asset, das schon in der gewählten Zone ist, bleibt, wie es ist, ohne Eintrag im Verlauf. Ein Asset, das ein anderer Administrator geändert hat, nachdem Sie die Liste geladen haben, wird ebenfalls nicht geändert: Das Ergebnis nennt es, sodass Sie es öffnen, die Änderung prüfen und seine Zone erneut festlegen können. Alle anderen Assets werden gespeichert.

Das Ergebnis nennt, wie viele Assets in die Zone gelegt wurden, wie viele schon in ihr waren und welche inzwischen jemand anderes geändert hat. Pulse legt nie von sich aus eine Zone fest.

Die Asset-Liste zeigt die Zone jedes Assets in ihrer Spalte **Zone** und lässt sich nach Zone filtern. Der CSV-Export enthält die Zone, ihre SL-T und ob sie eine Safety-Zone ist.

Eine Zone, in der Assets sind, lässt sich nicht löschen: Der Lösch-Dialog nennt, wie viele Assets in ihr sind. Nehmen Sie sie zuerst aus der Zone und löschen Sie die Zone dann. Das Löschen einer Zone lässt sich nicht rückgängig machen.

Werden zwei Assets zusammengeführt, behält das zusammengeführte Asset die Zone des Assets, in das Sie das andere zusammengeführt haben, so wie es dessen übrige Angaben behält; die Zone des anderen Assets wird nicht übernommen, ihr Name zum Zeitpunkt der Zusammenführung wird aber im Eintrag der Zusammenführung im **Verlauf** festgehalten und im Änderungsprotokoll. Wird die Zusammenführung aufgehoben, kommt das wiederhergestellte Asset nicht in die Zone zurück, in der es vorher war.

Zusammenführungsvorschläge

Eine CPU und ihr Kommunikationsprozessor antworten jeweils unter einer eigenen Adresse, deshalb führt das Register sie als zwei Assets. Das Register sucht nach solchen Paaren: ein Asset nur mit einer CPU und ein Asset nur mit einem Kommunikationsprozessor, gesehen von derselben Appliance oder demselben Collector, deren IPv4-Adressen im selben /24-Subnetz liegen und einander am nächsten sind, ohne dass ein anderes Asset genauso nah liegt. Findet es ein solches Paar, erscheint ein Banner am Anfang der Asset-Liste.

Jeder Vorschlag zeigt die beiden Assets, das gemeinsame Subnetz, den Adressabstand sowie bei Assets, die über einen Collector gefunden wurden, den Collector, der sie gesehen hat. Der Vorschlag beruht ausschließlich auf der Adressnähe — Asset-Namen werden nicht berücksichtigt.

- Klicken Sie auf **Zusammenführen prüfen…**, um den Zusammenführungsdialog für das Paar zu öffnen (siehe unten).
- Klicken Sie auf **Nicht derselbe Schaltschrank**, um den Vorschlag zu verwerfen. Die beiden Assets werden nicht erneut vorgeschlagen.

Solange Sie nicht handeln, ändert sich nichts — ein Vorschlag ist nur eine Empfehlung.

Assets zusammenführen

Führen Sie zwei Assets zusammen, wenn sie im Register tatsächlich ein Schaltschrank sind — zum Beispiel eine CPU und ihr Kommunikationsprozessor, die jeweils unter einer eigenen Adresse antworten.

Sie können eine Zusammenführung auf zwei Wegen starten:

1. Über einen **Zusammenführungsvorschlag** — klicken Sie auf **Zusammenführen prüfen…** im Vorschlagsbanner.

2. Über die **Asset-Liste** — klicken Sie neben **Filter** auf **Auswählen** und dann auf die beiden Assets. Klicken Sie in der Leiste am unteren Seitenrand auf **Zusammenführen…**. Die Schaltfläche ist verfügbar, wenn genau zwei Assets ausgewählt sind.

Wählen Sie im Zusammenführungsdialog aus, welches Asset erhalten bleiben soll. Das Asset, das Sie behalten, übernimmt die Adressen, MAC-Adressen, ApplicationUris und Module, die die Scans beim anderen gefunden haben, zusammen mit den CVE-Monitoren und CVE-Entscheidungen zu diesen Modulen, den Datenquellen, die vom anderen Asset lesen, und den zu ihm erstellten Vorfällen zu Firmware-Änderungen, entfernten Modulen und neuen Geräten. Das behaltene Asset behält auch seinen eigenen Namen, Verantwortlichen, Kritikalität, Standort, Sicherheitssystem-Markierung und Notizen — Werte des absorbierten Assets werden nicht übernommen, aber im Verlauf des behaltenen Assets festgehalten.

Assets, die von unterschiedlichen Collectors gesehen wurden, können nicht zusammengeführt werden. Dieselbe Adresse hinter zwei Collectors kann zwei verschiedene Geräte bedeuten.

Zusammenführung aufheben

Wenn eine Zusammenführung ein Fehler war, können Sie sie rückgängig machen. Öffnen Sie das Asset, das das andere absorbiert hat, und klicken Sie oben auf der Seite auf **Zusammenführung aufheben…**. Die Schaltfläche hebt die jüngste Zusammenführung in das Asset auf; die Zusammenführung selbst steht in der Karte **Verlauf**.

Das Register legt das absorbierte Asset unter seiner früheren ID wieder an. Seine Adressen, MAC-Adressen, ApplicationUris und Module werden an es zurückgegeben, ebenso die von Ihrem Team für es eingetragenen Werte, sein Verlauf, die Datenquellen, die von ihm lesen, und die zu ihm erstellten Vorfälle. Das behaltene Asset behält die von Ihrem Team eingetragenen Werte — einschließlich Änderungen, die nach der Zusammenführung vorgenommen wurden.

Nur die jüngste Zusammenführung in ein Asset kann aufgehoben werden. Um eine ältere aufzuheben, heben Sie zuerst die neueren auf. Ein Fall lässt sich gar nicht rückgängig machen: Wurde das behaltene Asset später selbst in ein drittes Asset zusammengeführt und diese Zusammenführung aufgehoben, können ältere Zusammenführungen in es nicht mehr aufgehoben werden. Der Dialog zur Aufhebung weist darauf hin.

Offline-Assets

Ein Asset ist **offline**, wenn der letzte abgeschlossene Scan, der seine Adresse abgedeckt hat, es nicht gefunden hat, oder wenn alle Datenquellen, die es lesen, die Verbindung verloren haben (siehe Was Datenquellen dem Register sagen). Pulse kennzeichnet ein Asset nicht als offline, weil Zeit vergangen ist: Anlagen stehen während eines Stillstands wochenlang still, und Pulse scannt nur, wenn jemand einen Scan startet. Findet ein späterer Scan das Asset wieder, ist es von selbst wieder in Betrieb.

Ein Scan deckt ein Asset ab, wenn alles Folgende zutrifft:

- er lief auf derselben Appliance oder demselben Collector, der das Asset gefunden hat;
- er hat die Adresse des Assets mit einer Methode untersucht, die bis zum Ende lief und es hätte finden können — S7 für ein Asset mit S7-Modulen, OPC UA für ein Asset mit OPC-UA-Server;
- der Collector, der ihn ausgeführt hat, hält fest, was er abgedeckt hat. Collectors mit einer älteren Version tun das nicht, und ihre Scans kennzeichnen nie ein Asset als offline.

Ein S7-Scan sucht Steuerungen auf Port 102, dem Standard-Port von S7, sofern ein Eintrag seines **Netzbereichs** keinen anderen Port für einen Host nennt, etwa `192.168.10.5:1102`. Ein Asset mit S7-Modulen deckt er nur auf dem Port ab, auf dem es antwortet: dem Port der S7-Datenquelle, die es liest, oder, wenn keine S7-Datenquelle es liest, dem Port, auf dem ein Scan es zuletzt gefunden hat. Eine Steuerung, die eine Datenquelle auf Port 1102 liest, wird daher nicht von einem Scan als offline gekennzeichnet, der nur auf Port 102 gesucht hat — ihre Datenquelle sagt dem Register weiterhin, ob sie da ist. Dasselbe gilt für eine Steuerung ohne Datenquelle, die ein Scan auf Port 1102 gefunden hat. Damit auch Scans sie beurteilen, nehmen Sie ihren Port in den Netzbereich des Scans auf.

Ein Scan, dessen Methode fehlgeschlagen ist, ein Scan eines anderen Netzes oder ein Scan eines anderen Collectors lässt das Asset, wie es war. Ein Asset, das nur aus der PROFINET-Erkennung bekannt ist, wird nie als offline gekennzeichnet, denn die PROFINET-Erkennung untersucht keine Adressen. Ein aus mehreren zusammengeführtes Asset ist nur offline, wenn der Scan es unter keiner seiner Adressen gefunden hat. Dass ein Scan es nicht gefunden hat, zählt nur, wenn der Scan nach dem letzten Lesen durch eine Datenquelle begonnen hat: Eine Datenquelle, die es seither gelesen hat, sagt, dass es da ist.

Ein Offline-Asset:

- ist in der Liste und oben auf seiner Seite als **Offline** gekennzeichnet;
- zeigt, welcher Scan es nicht gefunden hat, seit wann es offline ist und wann ein Scan es zuletzt abgedeckt hat;

- erhält einen Eintrag in seinem **Verlauf**, festgehalten vom Scan. Ebenso, wenn es zurückkommt.

Offline ist nur so aktuell wie der letzte Scan, der das Asset abgedeckt hat: Das Datum **Zuletzt von einem Scan abgedeckt** auf der Seite des Assets zeigt, wie alt das ist. Um es erneut zu prüfen, scannen Sie das Netz des Assets.

Ein Offline-Asset ist weiterhin in Betrieb, wird aber gesondert hervorgehoben: Die Liste zählt es unter **Offline**, nicht unter **In Betrieb**, und der CSV-Export zeigt `offline` in **lifecycle_status**. Ein Asset, das nicht außer Betrieb genommen ist und nicht offline ist — weder der letzte Scan, der es abgedeckt hat, noch seine Datenquellen melden es als offline —, zeigt auf seiner Seite ein Badge **In Betrieb**; in der Liste bleibt es ungekennzeichnet. Ein außer Betrieb genommenes Asset wird als **Außer Betrieb** angezeigt, was auch immer seine Scans sagen.

Asset außer Betrieb nehmen

Das Register entfernt ein Asset nie von sich aus: Ein Asset, das Scans eine Zeit lang nicht gefunden haben, bleibt gelistet, gekennzeichnet als offline, denn Anlagen stehen mitunter wochenlang still. Wenn ein Gerät tatsächlich außer Betrieb geht, nehmen Sie das Asset außer Betrieb.

Öffnen Sie das Asset und klicken Sie oben auf der Seite auf **Außer Betrieb nehmen…**. Geben Sie den Grund ein (erforderlich, bis zu 1.000 Zeichen) und klicken Sie auf **Außer Betrieb nehmen**. Das Asset:

- bleibt im Register und im CSV-Export, gekennzeichnet als **Außer Betrieb**;
- zeigt oben auf seiner Seite, wer es wann und warum außer Betrieb genommen hat;
- erhält einen Eintrag in seinem **Verlauf**, mit dem Grund.

Scans aktualisieren ein außer Betrieb genommenes Asset weiterhin. Findet ein Scan es erneut, ändert sich sein Datum **Zuletzt gesehen**, es bleibt aber außer Betrieb, bis ein Administrator es wieder in Betrieb nimmt.

Um das Asset wieder in Betrieb zu nehmen, öffnen Sie es und klicken Sie auf **Wieder in Betrieb nehmen**. Das Asset ist dann nicht mehr als außer Betrieb gekennzeichnet; sein **Verlauf** behält sowohl die Außerbetriebnahme mit ihrem Grund als auch die Wiederinbetriebnahme. Wenn ein Scan oder eine Datenquelle das Asset zu diesem Zeitpunkt noch als offline meldet, weist die Bestätigung darauf hin — das Asset ist wieder in Betrieb, wird aber als offline angezeigt, bis ein Scan es findet oder eine Datenquelle es liest.

Wenn Sie ein außer Betrieb genommenes Asset in ein Asset in Betrieb zusammenführen, bleibt das behaltene Asset in Betrieb. Wird diese Zusammenführung aufgehoben, ist das wiederhergestellte Asset wieder außer Betrieb, mit Angabe, wer es wann und warum außer Betrieb genommen hat.

Datenquellen

Eine Datenquelle liest von einem Asset, wenn sie sich über dieselbe Appliance oder denselben Collector mit der Adresse verbindet, unter der das Asset gefunden wurde. Ist die Adresse einer Datenquelle ein Hostname, zählt die Adresse, in die dieser Name aufgelöst wurde: Die Appliance oder der Collector, der die Datenquelle liest, meldet sie nach dem ersten erfolgreichen Lesen. Die Seite des Assets listet diese Datenquellen mit Links auf. Liest keine von ihm, sagt die Seite das: Das Register legt nie eine Datenquelle an. Sie fügen eine über die Gerätesuche oder die Seite der Datenquellen hinzu, und sie erscheint hier, sobald sie vom Asset liest.

Die Seite der Datenquelle selbst zeigt das Asset, von dem sie liest, als **Liest von** mit dem Namen des Assets, verlinkt auf das Asset. Wie das Register wird dieser Link nur Organisationsadministratoren angezeigt.

Was Datenquellen dem Register sagen

Scans laufen nur, wenn jemand einen startet, eine Datenquelle aber liest ihr Asset fortlaufend. Was sie liest, hält das Register zwischen den Scans aktuell:

- **Zuletzt live gesehen.** Die Seite des Assets zeigt, wann eine Datenquelle das Asset zuletzt erfolgreich gelesen hat, und welche, mit Link auf sie. Das wird höchstens einmal pro Minute aktualisiert. Ein Asset, das noch keine Datenquelle gelesen hat, zeigt **Noch von keiner Datenquelle gelesen**; wurde die Datenquelle inzwischen gelöscht, sagt die Seite das. **Zuletzt gesehen** bleibt das Datum, an dem ein Scan das Asset zuletzt gefunden hat.
- **Betriebsart der CPU.** Eine S7-Datenquelle liest mit ihren Werten die Betriebsart der CPU an ihrem Rack und Steckplatz. Liest sie **RUN**, wo das Register **STOP** hielt, oder umgekehrt, hält das Register die neue Betriebsart fest und fügt dem **Verlauf** des Assets einen Eintrag hinzu, gekennzeichnet mit **Live gelesen von** und der Datenquelle. Ein Lesen, das die Betriebsart nicht erkennen kann, ändert nichts, und ein Wert, der älter ist als das, was ein Scan festgehalten hat, ersetzt diesen nie.
- **Firmware.** Eine S7-Datenquelle liest außerdem Bestellnummer, Seriennummer und Firmware der CPU an ihrem Rack und Steckplatz — über die Verbindung, die sie ohnehin hält, nie über eine zweite —, wenn sie sich zum ersten Mal mit dem Gerät verbindet, und danach alle 10 Minuten. Weicht die Firmware von der ab, die das Register führt, hält das Register die neue Firmware fest, fügt dem **Verlauf** des Assets

eine Firmware-Änderung hinzu, gekennzeichnet mit **Live gelesen von** und der Datenquelle, und löst denselben Vorfall aus wie die Firmware-Änderung eines Scans. Das geschieht nur, wenn die Datenquelle die Adresse erreicht hat, über die das Asset verknüpft ist, und Bestellnummer und Seriennummer des Moduls die sind, die das Register führt. Antwortet ein anderes Modul, ändert die Datenquelle nichts: Erst der nächste Scan entscheidet, ob das Gerät ersetzt wurde. Ein Scan, der die alte Firmware las, bevor die Datenquelle die neue las, stellt die alte Firmware nie wieder her. Appliances und Collectors mit einer älteren Pulse-Version lesen die Firmware nicht.

- **Offline und zurück.** Haben alle aktivierten Datenquellen, die das Asset lesen, die Verbindung verloren — das Gerät hat nicht geantwortet, die Verbindung lief in eine Zeitüberschreitung, oder Pulse hält sich bei einem Gerät zurück, das immer wieder fehlschlägt —, wird das Asset als offline gekennzeichnet, ohne auf einen Scan zu warten. Oben auf seiner Seite steht, wann seine Datenquellen die Verbindung verloren haben. Ein Gerät, das geantwortet und abgelehnt hat — ein Lesen, das es zurückgewiesen hat, eine Anmeldung oder ein Zertifikat, das es nicht angenommen hat —, ist da und hält das Asset deshalb in Betrieb. Sobald eine seiner Datenquellen es wieder liest, ist das Asset zurück. Beide Wechsel sind Einträge in seinem **Verlauf**, mit der Datenquelle.

Zwischen Scans und Datenquellen gilt das Neuere: Eine Datenquelle, die antwortet, bringt ein Asset, das ein Scan nicht gefunden hat, nur zurück, wenn sie nach diesem Scan geantwortet hat, und dass ein Scan es nicht gefunden hat, zählt nur, wenn der Scan nach dem letzten Lesen durch eine Datenquelle begonnen hat.

Werden zwei Assets zusammengeführt, zeigt das Asset, das Sie behalten, das spätere seiner beiden Daten **Zuletzt live gesehen**. Ein Asset, das durch das Aufheben einer Zusammenführung wiederhergestellt wird, zeigt keines, bis eine seiner Datenquellen es wieder liest.

Ein Modul auf CVEs überwachen

Mit CVE-Überwachung zeigt die Spalte **CVE-Überwachung** der Tabelle **Module** für jedes Modul:

- **Die CVE-Monitore, die es überwachen**, jeweils verlinkt, mit der Anzahl offener Funde (**Offen** oder **In Bearbeitung**) oder **Keine offenen Funde**.
- **Auf CVEs überwachen**, wenn noch kein Monitor das Modul überwacht.
- **Keine Bestellnummer erfasst, daher kein Abgleich mit Sicherheitsmeldungen möglich**, wenn das Modul keine Bestellnummer hat. Sicherheitsmeldungen werden nach Bestellnummer abgeglichen, daher lässt sich ein solches Modul nicht überwachen.

So starten Sie die Überwachung eines Moduls:

1. Klicken Sie in der Zeile des Moduls auf **Auf CVEs überwachen**.
2. Prüfen Sie den Dialog. Er zeigt das Modul, seine Bestellnummer und seine Firmware. Diese stammen aus dem Asset-Register und folgen dem Modul bei jedem Scan.
3. Passen Sie bei Bedarf den **Namen** an. Vorgegeben ist der Name des Assets, gefolgt von der Bestellnummer.
4. Bestätigen Sie den **Hersteller**. Das Register erfasst keinen Hersteller, daher trägt der Dialog Siemens ein. Sicherheitsmeldungen werden auch nach Hersteller abgeglichen.
5. Wählen Sie eine **Eskalationsrichtlinie** und fügen Sie Tags hinzu, falls Sie welche verwenden.
6. Klicken Sie auf **Überwachung starten**.

Das Ergebnis ist ein gewöhnlicher CVE-Monitor, der sein Gerät von diesem Modul übernimmt. Nur dieser Klick startet einen Monitor: Ein Scan legt nie einen an.

Schwachstellen

Mit CVE-Überwachung beantwortet der Abschnitt **Schwachstellen** auf der Seite des Assets, was zu jeder CVE an diesem Asset entschieden wurde. Eine Entscheidung wird am Modul erfasst, nicht an einem Monitor, und bleibt deshalb hier, auch nachdem der Monitor gelöscht wurde. Siehe Entscheidungen am Modul erfasst.

Wenn ein CVE-Monitor mindestens ein Modul überwacht, beginnt der Abschnitt damit, womit die Module abgeglichen wurden: **Abgeglichen mit N Sicherheitsmeldungen, zuletzt geprüft** und wann die jüngste Prüfung der Monitore dieses Assets lief. Die Anzahl der Sicherheitsmeldungen wird von der stündlichen CVE-Prüfung aktualisiert und kann daher bis zu eine Stunde alt sein. Hat das Pulse-Gateway, das den Schwachstellen-Feed bereitstellt, noch nie geantwortet, entfällt die Anzahl, und die Zeile nennt nur, wann die Module zuletzt geprüft wurden.

Jedes Modul, das ein CVE-Monitor überwacht oder zu dem Entscheidungen erfasst sind, wird mit dem Zeitpunkt seiner letzten Prüfung aufgeführt. Ein Modul, das der jüngste Netzwerk-Scan nicht gefunden hat, ist mit **Beim letzten Scan nicht gesehen** markiert. Seine Entscheidungen werden weiterhin angezeigt, denn eine Entscheidung über ein ausgetauschtes Modul gehört weiterhin zur Dokumentation.

Unter jedem Modul zeigt jede zutreffende CVE ihren Schweregrad und Titel und verlinkt auf den Fund. Außerdem zeigt sie:

- **Die aktuelle Entscheidung** — Status und Begründung, wer sie getroffen hat und wann. Eine Risikoakzeptanz zeigt zusätzlich das Datum, bis zu dem sie gilt. Ohne Entscheidung zeigt die CVE **Keine Entscheidung erfasst**.

- **Durch Firmware-Wechsel behoben** — die CVE trifft nicht mehr zu, weil sich die Firmware des Moduls geändert hat. **Trifft nicht mehr zu** bedeutet, dass sie aus einem anderen Grund nicht mehr zutrifft.
- **Verlauf** — klicken Sie darauf, um jede Entscheidung zu dieser CVE an diesem Modul aufzulisten, die älteste zuerst. Jeder Eintrag zeigt, woher er stammt:
  - **von** und der Name einer Person, für eine Entscheidung, die jemand erfasst hat. Es ist der aktuelle Name des Benutzers, ein umbenannter Benutzer erscheint also mit seinem neuen Namen. Wird dieser Benutzer später aus Pulse entfernt, steht dort **von einem entfernten Benutzer**.
  - **Risikoakzeptanz abgelaufen**, wenn eine Risikoakzeptanz ihr Datum erreicht hat und die CVE wieder auf **Offen** zurückgefallen ist.
  - **Bei Zusammenführung beibehalten**, wenn zwei Assets mit demselben Modul zusammengeführt wurden und beide eine Entscheidung zu dieser CVE hatten. Die Entscheidung des behaltenen Assets bleibt aktuell, und die Entscheidungen des anderen Assets bleiben im Verlauf.

Um eine Entscheidung zu erfassen, klicken Sie neben der CVE auf **Entscheidung erfassen**. Es öffnet sich derselbe Bewertungsdialog wie auf den Seiten unter Schwachstellen, mit denselben Status und Regeln, einschließlich **Mitigiert** für eine Schwachstelle, die eine ausgleichende Maßnahme blockiert. Die Entscheidung erscheint sofort auf den CVE-Seiten. Die Schaltfläche wird angezeigt, solange ein CVE-Monitor das Modul überwacht.

Am Ende des Abschnitts steht die Liste **Nicht auf CVEs geprüfte Module**: jedes Modul des Assets, das kein CVE-Monitor überwacht, mit dem Grund — **Kein CVE-Monitor überwacht dieses Modul** oder keine Bestellnummer für den Abgleich. Der Abgleich deckt nur überwachte Module ab; diese Liste zeigt deshalb klar, was nicht abgedeckt ist.

> **Lizenzvoraussetzung**
>
> Die CVE-Teile der Asset-Seite — die Spalte **CVE-Überwachung** und der Abschnitt **Schwachstellen** — erfordern neben dem Asset-Register auch die CVE-Überwachung in Ihrer Lizenz. Ohne sie werden sie nicht angezeigt.

Vorfälle des Registers weiterleiten

Das Asset-Register löst einen Vorfall aus, wenn ein Scan oder eine S7-Datenquelle auf einem Modul eines registrierten Assets eine andere Firmware liest, wenn Scans belegen, dass ein Modul aus ihm entfernt wurde, oder wenn ein Scan ein neues Gerät findet, wo ein früherer Scan nichts gefunden hat (siehe Firmware-Änderungen an Assets, Aus Assets

entfernte Module und Neue Assets in gescannten Netzwerken). Die Einstellungen des Registers legen fest, wer davon erfährt. Administratoren öffnen sie über **Assets > Einstellungen** in der Seitenleiste.

- **Nur Administratoren benachrichtigen** (Standard) — alle Administratoren und Inhaber der Organisation erhalten eine Benachrichtigung in der App. Niemand wird alarmiert.
- **Eine Eskalationsrichtlinie** — jeder Vorfall des Registers eskaliert zusätzlich über diese Richtlinie, wie ein Vorfall eines Monitors darauf: Ihre Stufen, Empfänger, Schweregrade und Betriebszeiten gelten, und bestätigt niemand den Vorfall, greifen ihre Wiederholungen und ihre Weitergabe. Die Benachrichtigung der Administratoren in der App wird weiterhin gesendet.

Wählen Sie auf dem Tab **Vorfälle** unter **Eskalationsrichtlinie** eine Richtlinie und klicken Sie auf **Speichern**. Die Einstellung gilt für Vorfälle, die nach dem Speichern ausgelöst werden; ein bereits offener Vorfall behält die Weiterleitung, mit der er ausgelöst wurde.

Niemand wird alarmiert, bis ein Administrator hier eine Richtlinie wählt. Die Standard-Eskalationsrichtlinie der Organisation wird für Vorfälle des Registers nicht verwendet.

Solange das Register seine Vorfälle über eine Richtlinie weiterleitet, kann diese Richtlinie nicht gelöscht werden. Wählen Sie zuerst eine andere Richtlinie oder **Nur Administratoren benachrichtigen**.

Beispiel: nur außerhalb der Arbeitszeit alarmieren

Tagsüber ist meist jemand vor Ort, der von einem Firmware-Update weiß; nachts oder am Wochenende ist eine unangekündigte Änderung es wert, jemanden zu wecken. Um nur außerhalb der Arbeitszeit zu alarmieren, legen Sie eine Eskalationsrichtlinie mit zwei Stufen an:

1. Eine **Betriebszeiten**-Stufe: Modus **Werktage**, Zeiten 08:00 bis 17:00, mit eingeschaltetem **Betriebszeiten umkehren**. Umgekehrt lässt die Stufe die Eskalation nur außerhalb dieser Zeiten fortfahren: an Werktagen abends und nachts sowie das ganze Wochenende.
2. Eine Benachrichtigungsstufe (**Schritt hinzufügen**) mit dem Bereitschaftsplan als Empfänger.

Wählen Sie diese Richtlinie dann in den Einstellungen des Registers. Eine Firmware-Änderung, die an einem Dienstag um 10:00 gefunden wird, wartet an der ersten Stufe; der Aktivitätsfeed des Vorfalls zeigt **Eskalation pausiert — außerhalb der Betriebszeiten** und wann sie fortgesetzt wird, um 17:00. Bestätigen und lösen Sie den Vorfall vorher, wird niemand alarmiert. Eine Änderung, die um 22:00 gefunden wird, wartet nicht: Sie geht sofort zur Benachrichtigungsstufe weiter, und der Bereitschaftsplan wird nach deren anfänglicher Verzögerung alarmiert.

Betriebszeiten werden in der Zeitzone der Organisation ausgewertet.

Wartungsfenster

Ein geplantes Firmware-Update oder ein Modultausch muss niemanden alarmieren. Wartungsfenster sind die Zeiten, in denen solche Änderungen vorgenommen werden: Eine Firmware-Änderung, ein entferntes Modul oder ein neues Asset, die vollständig in einem Fenster entstehen, werden wie gewohnt im **Verlauf** des Assets festgehalten, mit dem Fenster, in das sie fielen, als **Im Wartungsfenster** markiert und lösen keinen Vorfall aus.

Administratoren bearbeiten die Fenster auf dem Tab **Wartungsfenster** in den Einstellungen des Registers (**Assets > Einstellungen** in der Seitenleiste). Klicken Sie auf **Fenster hinzufügen**, wählen Sie **Werktage**, **Jeden Tag** oder **Benutzerdefiniert**, legen Sie die Zeiten fest und klicken Sie auf **Speichern**. Um ein Fenster zu entfernen, klicken Sie auf sein Papierkorb-Symbol und speichern. Ein Register hat bis zu 20 Fenster; das Formular weist darauf hin, wenn Sie das Limit erreicht haben. Ohne Fenster, dem Standard, löst jede Änderung einen Vorfall aus. Das Speichern gilt für Änderungen, die ab dann festgehalten werden: Einträge, die schon im Verlauf eines Assets stehen, behalten ihre Markierung. Ein Wechsel zu einem anderen Tab der Einstellungen behält ungespeicherte Änderungen; verlassen Sie die Einstellungen, bevor Sie gespeichert haben, fragt die Seite, ob Ihre Änderungen verworfen werden sollen.

Die Fenster gelten in der Zeitzone der Organisation, die der Tab nennt; ein Fenster von 06:00 bis 14:00 bleibt also auch über eine Zeitumstellung hinweg 06:00 bis 14:00 Ortszeit. Ein Fenster endet an dem Tag, an dem es beginnt, spätestens um **24:00** (Mitternacht); ein Fenster von 22:00 bis 24:00 umfasst also die letzten beiden Stunden des Tages. Gleicher Beginn und gleiches Ende umfassen den ganzen Tag, 24 Stunden ab dem Beginn, und der Tab weist daneben darauf hin.

Wann eine Änderung als im Fenster vorgenommen gilt

Ein Scan sieht eine Änderung nicht, wenn sie vorgenommen wird, sondern erst danach. Pulse fragt deshalb nicht, wann der Scan lief, sondern wann die Änderung vorgenommen worden sein kann: irgendwann zwischen dem Scan, der den alten Stand zuletzt sah, und dem Scan, der den neuen sah.

- **Eine Firmware-Änderung:** vom letzten Lesen der alten Firmware bis zum Lesen der neuen, ob durch einen Scan oder eine S7-Datenquelle.
- **Ein entferntes Modul:** vom letzten Scan, der das Modul fand, bis zum Scan, der die Entfernung festhielt.

- **Ein neues Asset:** vom Beginn des früheren Scans, der seine Adresse leer fand, bis zum Scan, der das Gerät fand.

Die Änderung gilt nur dann als im Fenster vorgenommen, wenn dieser ganze Zeitraum in die Wartungszeit fällt: in ein Fenster oder in Fenster, die lückenlos aneinander anschließen. Ein ganztägiges Fenster am Montag und eines am Dienstag etwa umfassen zusammen auch eine Änderung über Mitternacht.

Beispiel. Ein Fenster umfasst Werktage von 06:00 bis 14:00. Ein Scan am Montag um 08:00 liest auf einer CPU die Firmware 2.8.1, ein Scan um 11:00 liest 2.9.4. Die Änderung wurde zwischen 08:00 und 11:00 vorgenommen, im Fenster am Montag: Sie wird festgehalten, markiert und löst keinen Vorfall aus. Lief der letzte Scan davor dagegen am Sonntag um 20:00 und der nächste am Montag um 09:00, kann die Änderung in der Nacht zum Montag vorgenommen worden sein, außerhalb jedes Fensters: Sie löst einen Vorfall aus, obwohl der Scan, der sie fand, im Fenster lief.

Je dichter Ihre Scans aufeinander folgen, desto genauer weiß Pulse, wann eine Änderung vorgenommen wurde. Ein Scan kurz nach Beginn eines Fensters lässt eine Änderung, die später im Fenster vorgenommen wird, als im Fenster vorgenommen gelten.

Markiert wird nur eine Änderung, die sonst einen Vorfall auslösen würde. Eine Änderung, die ohnehin keinen auslöst — ohne das Asset-Register in Ihrer Lizenz, aus einem Scan, der mehr als 24 Stunden nach seinem Ende ins Register übernommen wird, oder an einem außer Betrieb genommenen Asset —, wird ohne Markierung festgehalten.

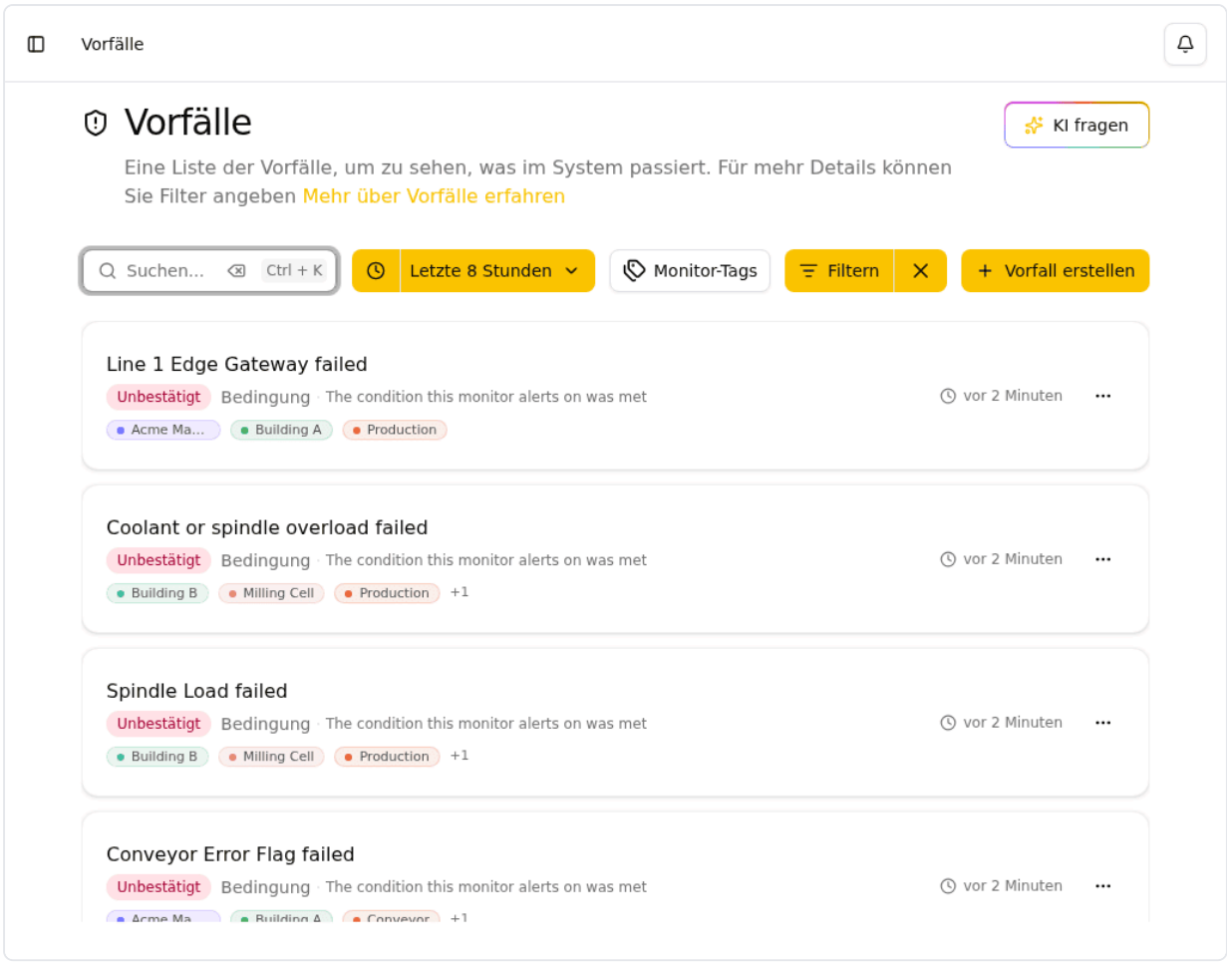
Verwandte Seiten

- Gerätesuche — Scan starten, um das Register zu füllen
- Schwachstellen (CVEs) — CVE-Monitore, Funde und Bewertung
- Lizenzen — Asset-Register im Tarif aktivieren

Teil 3 · Monitoring

3.6 Vorfälle

Vorfälle repräsentieren einen Zeitraum mit beeinträchtigtem oder ausgefallenen Dienst, der Aufmerksamkeit erfordert. Sie werden automatisch erstellt, wenn ein Monitor ein Problem erkennt, oder manuell von einem Teammitglied.



Vorfalllebenszyklus

Jeder Vorfall folgt einem definierten Lebenszyklus:

1. **Unbestätigt** -- Der Vorfall wurde erkannt, aber niemand hat reagiert. Wird mit einem roten Badge **Unbestätigt** angezeigt.
2. **Bestätigt** -- Jemand hat den Vorfall gesehen und arbeitet daran. Wird mit einem gelben Badge **Bestätigt** angezeigt.
3. **Gelöst** -- Das zugrunde liegende Problem wurde behoben. Wird mit einem grünen Badge **Gelöst** angezeigt.

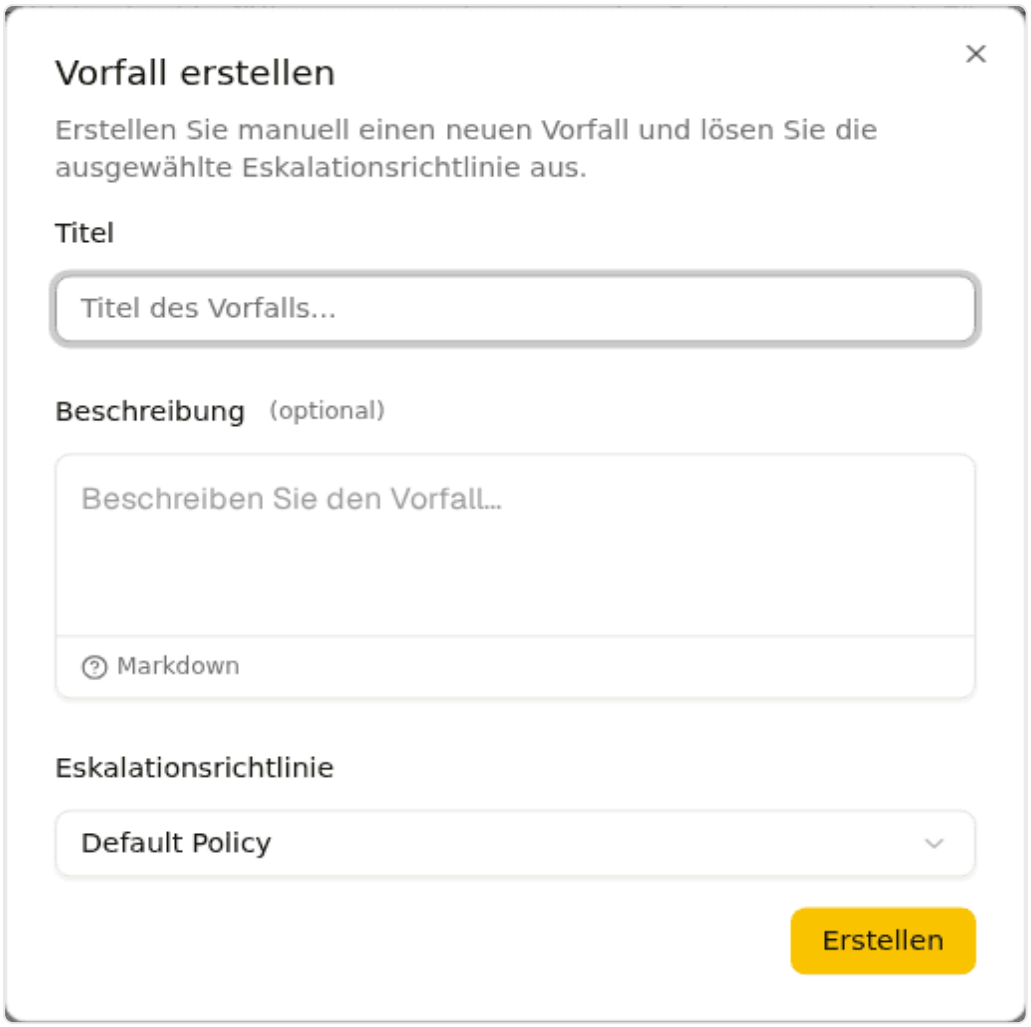
Vorfall manuell erstellen

Sie können auf der Vorfalllistenseite manuell einen Vorfall erstellen. Dies ist nützlich, wenn Sie eine Eskalationsrichtlinie für eine Situation auslösen müssen, die nicht von einem Monitor erkannt wird.

So erstellen Sie einen manuellen Vorfall:

1. Öffnen Sie die Seite **Vorfälle**.
2. Klicken Sie in der Symbolleiste auf **Vorfall erstellen**. Auf mobilen Geräten erscheint diese Schaltfläche als schwebende Aktionsschaltfläche (FAB) unten rechts auf dem Bildschirm.
3. Füllen Sie das Formular aus:
   - **Titel** (erforderlich) — Eine kurze Beschreibung des Vorfalls.
   - **Beschreibung** (optional) — Eine detaillierte Beschreibung, unterstützt Markdown.
   - **Eskalationsrichtlinie** (erforderlich) — Die auszulösende Eskalationsrichtlinie. Die erste verfügbare Richtlinie ist vorausgewählt.
4. Klicken Sie auf **Erstellen**.

Der Vorfall wird sofort erstellt und die ausgewählte Eskalationsrichtlinie ausgelöst. Sie können ihn anschließend wie jeden anderen Vorfall bestätigen und lösen.



Vorfälle anzeigen

Die Vorfallliste zeigt alle Vorfälle mit Statusfilterung. Standardmäßig werden aktive Vorfälle (Unbestätigt + Bestätigt) angezeigt.

Die Seitenleiste zeigt bei **Vorfälle** einen Zähler-Badge, wenn in Ihrer Organisation aktive Vorfälle (unbestätigt oder bestätigt) offen sind, sowie einen separaten Badge bei **Meine Vorfälle** für Vorfälle, die Sie bestätigt, aber noch nicht gelöst haben. Die Badges werden jede Minute aktualisiert; bei einem Zählerstand von null werden sie ausgeblendet. Wenn die Seitenleiste in den Icon-only-Modus eingeklappt ist, schrumpft jeder Badge zu einem kleinen Punkt, der auf offene Aufmerksamkeit hinweist.

Der Eintrag **Meine Vorfälle** in der Seitenleiste ist eine Kurzwahl, die die Vorfallliste vorausgefiltert auf die von Ihnen bestätigten Vorfälle öffnet — eine schnelle Möglichkeit, zu sehen, woran Sie gerade arbeiten.

- **Suche** -- Vorfälle nach Titel oder zugehörigem Monitor-Namen suchen
- **Statusfilter** -- Sichtbarkeit jedes Statustyps umschalten

- **Vorfalltyp** -- Filtern nach der Auslösung: Monitor-Fehler, Systemvorfall oder manueller Vorfall
- **Monitortyp** -- Filtern nach dem Typ des Monitors, der den Vorfall ausgelöst hat (Heartbeat, CVE, Trigger, Bedingung, Ziel, OPC-UA-Alarme & Bedingungen)
- **Tags** -- Nach Tags filtern, die dem Monitor zugewiesen sind, der den Vorfall ausgelöst hat
- **Eskalationsrichtlinie** -- Nach der Eskalationsrichtlinie filtern, nach der der Vorfall eskaliert wird. Diese entspricht der zum Zeitpunkt der Vorfallauslösung verwendeten Richtlinie, nicht einer ggf. später am Monitor zugewiesenen.
- **Bestätigt von** -- Nach dem Teammitglied filtern, das den Vorfall bestätigt hat. Wählen Sie **(ich)**, um von Ihnen bestätigte Vorfälle anzuzeigen.
- **Gelöst von** -- Nach dem Teammitglied filtern, das den Vorfall gelöst hat. Wählen Sie **(ich)**, um von Ihnen gelöste Vorfälle anzuzeigen.
- **Zeitraum** -- Vorfälle nach einem Zeitfenster filtern. Klicken Sie auf das Uhrsymbol, um die Auswahl zu öffnen. Wählen Sie eine Schnellvoreinstellung oder legen Sie einen benutzerdefinierten Datums- und Uhrzeitbereich fest. Zukünftige Daten können nicht ausgewählt werden. Bei einer Schnellvoreinstellung wie **Letzte 8 Stunden** werden noch offene Vorfälle immer angezeigt, egal wie lange sie schon bestehen, sodass die Liste zur Anzahl in der Seitenleiste passt. Ein benutzerdefinierter Zeitraum zeigt nur Vorfälle, die in ihm begonnen haben.
- **Auto-Aktualisierung** -- Die Liste aktualisiert sich automatisch alle 5 Sekunden

Neben den Status-Chips zeigt ein Zähler an, wie viele Vorfälle den aktuellen Filtern entsprechen. Wenn die Liste ihre maximale Größe erreicht, lautet die Anzeige **Neueste N von N+** mit einem Hinweis, die Filter oder den Zeitraum einzuschränken, um ältere Vorfälle zu sehen.

Auf mobilen Geräten ist das Suchfeld standardmäßig ausgeblendet — tippen Sie auf das Suchsymbol in der Symbolleiste, um es einzublenden. Ein erneutes Tippen klappt das Feld ein und löscht die aktive Suche.

Auf mobilen Geräten werden die Filtersteuerelemente durch eine Schaltfläche **Filter** ersetzt, die ein Einschubfeld von unten öffnet. Alle Filtergruppen (Status, Vorfalltyp, Monitortyp, Tags, Eskalationsrichtlinie, Bestätigt von, Gelöst von) erscheinen dort als aufklappbare Abschnitte. Jeder Abschnitt zeigt einen Zähler, wenn Filter ausgewählt sind. Tippen Sie auf **Anwenden**, um die gewählten Filter zu aktivieren, oder auf **Zurücksetzen**, um alle Entwurfsauswahlen zu verwerfen. Aktive Filter werden als Nur-Lese-Chips unterhalb der Suchleiste angezeigt; um eine Auswahl zu ändern, öffnen Sie erneut das Einschubfeld.

Jede Vorfallkarte in der Liste zeigt das Status-Badge, den Monitor-Typ, die dem auslösenden Monitor zugewiesenen Tags und eine kurze Ursache. Wenn die Ursache identisch mit dem Vorfallstitel ist — was bei einfachen Monitor-Alarmen häufig vorkommt — wird die Ursachenzeile weggelassen, um Wiederholungen zu vermeiden.

Ein Systemvorfall hat keinen Monitor, deshalb zeigt seine Karte stattdessen, welche Art von Vorfall er ist — zum Beispiel **Gateway getrennt**, **Firmware geändert**, **Modul entfernt** oder **Neues Asset**. Die Karte eines Vorfalls zum Asset-Register nennt außerdem die betroffene Station und was sich geändert hat: den Namen der Station (oder ihre Adresse, wenn sie keinen hat), ihre Adresse und die Firmware vorher und nachher, die Bestellnummer des entfernten Moduls oder, bei einer neuen Station, ihre Adresse. Alle, die Vorfälle sehen, sehen diese Zeile, ohne Link zur Station, sofern Ihre Lizenz das Asset-Register umfasst.

Vorfalldetails

Klicken Sie auf einen Vorfall, um seine vollständigen Details zu sehen.

Die Detailseite umfasst:

- **Status** -- Aktueller Vorfallzustand, angezeigt als farbiges Text-Badge
- **Zugehöriger Monitor** -- Link zum Monitor, der den Vorfall ausgelöst hat
- **Asset** -- Bei einem Vorfall zu einem Asset im Asset-Register das betroffene Asset, seine Adresse und bei einer Firmware-Änderung die Firmware vorher und nachher und das Modul, an dem sie gelesen wurde — mit Baugruppenträger und Steckplatz (oder **Keine Steckplatzposition** bei einem PROFINET-Gerät), Bestellnummer und Seriennummer —, bei einem entfernten Modul dessen Baugruppenträger und Steckplatz (oder nur **Modul entfernt** bei einem PROFINET-Gerät), Bestellnummer und Seriennummer, bei einem neuen Asset das Modul, als das der Scan es gefunden hat — mit Baugruppenträger und Steckplatz, Bestellnummer und Seriennummer. Alle, die Vorfälle sehen, sehen diese Angaben, nur lesend, damit ein für den Vorfall alarmiertes Mitglied weiß, was es bestätigt. Administratoren sehen außerdem einen Link zum Asset. Nur sichtbar, wenn Ihre Lizenz das Asset-Register umfasst (siehe Firmware-Änderungen an Assets, Aus Assets entfernte Module und Neue Assets in gescannten Netzwerken)
- **Zeitstempel** -- Wann der Vorfall begann, bestätigt und gelöst wurde
- **Bestätigt von** -- Welcher Benutzer den Vorfall bestätigt hat. Klicken Sie auf den Namen, um die Vorfallliste nach allen von dieser Person bestätigten Vorfällen zu filtern.
- **Gelöst von** -- Welcher Benutzer den Vorfall gelöst hat. Klicken Sie auf den Namen, um die Vorfallliste nach allen von dieser Person gelösten Vorfällen zu filtern.

- **Weitere Vorkommen** -- Frühere Vorfälle, die durch dieselbe Ursache ausgelöst wurden (siehe unten)
- **Aktivitätsfeed** -- Chronologisches Protokoll aller Ereignisse

Weitere Vorkommen

Wenn dieselbe Monitor-Bedingung bereits früher Vorfälle ausgelöst hat, erscheint über dem Aktivitätsfeed eine Karte mit diesen früheren Vorkommen. Jede Zeile verlinkt auf den jeweiligen Vorfall und zeigt, wann er begann und wie lange er dauerte (oder **noch offen**, wenn er noch nicht gelöst wurde). Der Abschnitt erscheint nur, wenn mindestens ein früheres Vorkommen vorhanden ist.

Aktivitätsereignisse

Der Aktivitätsfeed zeichnet Ereignisse auf wie:

- Vorfall gestartet
- Vorfall wieder geöffnet (Alarm trat innerhalb des in der Eskalationsrichtlinie konfigurierten Wiedereröffnungsfensters erneut auf)
- Von einem bestimmten Benutzer bestätigt
- Von einem bestimmten Benutzer gelöst
- Monitor-Fehlerdetails
- Monitor-Wiederherstellungsdetails
- E-Mail-Benachrichtigungen gesendet
- SMS-Benachrichtigungen gesendet
- Push-Benachrichtigungen gesendet
- Sprachanruf-Benachrichtigungen gesendet
- Sprachanruf klingelt (Versuch)
- Sprachanruf abgelehnt
- Sprachanruf nicht angenommen
- Warn-E-Mail von einem bestimmten Benutzer geöffnet
- Eskalation pausiert — außerhalb der Betriebszeiten (zeigt an, wann die Eskalation fortgesetzt wird)
- Absenderzeitstempel geändert (eine spätere Zustellung für denselben Trigger-Alarm enthielt einen anderen Quellzeitstempel)
- Manuell an bestimmte Benutzer, Teams oder Bereitschaftspläne eskaliert (siehe unten)

Quellzeitstempel bei Trigger-Vorfällen — Wenn ein Trigger-Monitor eine Regel für den **Quellzeitstempel** konfiguriert hat und das sendende System einen Zeitstempel in den Nutzdaten mitliefert, zeigen die Ereignisse **Vorfall gestartet** und **Vorfall wieder**

geöffnet im Aktivitätsfeed an, wann der Absender laut eigener Angabe den Alarm ausgelöst hat. Daneben zeigt der Feed, wie weit dieser Zeitpunkt vom tatsächlichen Eingang der Zustellung bei Pulse abweicht -- beispielsweise „12 Minuten bevor Pulse ihn empfangen hat" oder „3 Minuten nachdem Pulse ihn empfangen hat -- Uhrzeit des Absenders prüfen". Diese Information dient als Beleg über die Uhr des Absenders; sie verändert nie, wann Pulse den Vorfall als begonnen ansieht. Wie Sie die Extraktion des Quellzeitstempels einrichten, erfahren Sie unter Trigger-Monitor.

Beschreibung bei Trigger-Vorfällen — Wenn die Regel **Vorfallbeschreibung** eines Trigger-Monitors Text aus der Webhook-Nutzlast extrahiert, wird dieser Text auf der Vorfalldetailseite als Markdown gerendert. Der Alarmtext eines Paging-Systems enthält oft Prosa -- Links zum Runbook, eine Liste betroffener Anlagen, Kontext, der nicht in einen Titel passt -- und Markdown lässt diese Formatierung durch. Wenn Beschreibung und Ursache dieselbe Information wiedergeben würden, wird der Ursache-Untertitel ausgeblendet, um Wiederholungen zu vermeiden.

Einen Vorfall manuell eskalieren

Manchmal sind die richtigen Personen nicht die, die die Eskalationsrichtlinie als Nächstes alarmieren würde — ein Operator sieht einen Alarm und weiß, dass das Elektro-Instandhaltungsteam übernehmen muss, oder hat einen Vorfall bereits bestätigt und braucht einen Spezialisten. **Eskalieren** sendet eine direkte, sofortige Benachrichtigung an Personen Ihrer Wahl.

So eskalieren Sie einen Vorfall:

1. Öffnen Sie die Vorfall-Detailseite.
2. Klicken Sie auf **Eskalieren...** (verfügbar, bis der Vorfall behoben ist — auch bei bestätigten Vorfällen).
3. Wählen Sie einen oder mehrere **Benutzer, Teams oder Bereitschaftspläne**. Ein Team benachrichtigt alle seine aktuellen lizenzierten Mitglieder; ein Bereitschaftsplan benachrichtigt diejenigen, die in diesem Moment Bereitschaft haben.
4. Wählen Sie die Kanäle: **Anruf**, **SMS**, **E-Mail** oder **Push-Benachrichtigung**. E-Mail und Push sind vorausgewählt.
5. Klicken Sie auf **Eskalieren**.

Die ausgewählten Empfänger werden sofort benachrichtigt — mit einem Hinweis, wer an sie eskaliert hat — und die Eskalation wird zusammen mit den versendeten Benachrichtigungen im Aktivitätsprotokoll festgehalten.

Wissenswertes:

- Die manuelle Eskalation ist **additiv**: Die automatische Eskalationsrichtlinie läuft nach ihrem eigenen Zeitplan weiter, bis jemand den Vorfall bestätigt. Eskalieren schaltet die Richtlinie nie stumm.
- Eine manuelle Eskalation erreicht die ausgewählten Personen auch außerhalb ihrer konfigurierten Arbeitszeiten — sie ist ein bewusster, namentlicher Ruf.
- Empfänger einer manuellen Eskalation erhalten auch die Folgebenachrichtigungen, wenn der Vorfall später bestätigt und behoben wird.
- Das Aktivitätsprotokoll nennt den Bereitschaftsplan, an den eskaliert wurde, nicht die daraus ermittelten Personen — wer zu diesem Zeitpunkt Bereitschaft hatte, zeigen die darauf folgenden Benachrichtigungseinträge.

Push-Benachrichtigungen

Wenn ein Vorfall erstellt wird und ein Eskalationsschritt mit aktivierten Push-Benachrichtigungen ausgelöst wird, erhalten die Empfänger eine Push-Benachrichtigung auf ihren registrierten Geräten. Wenn der Vorfall später **gelöst** wird, erhalten dieselben Empfänger eine weitere Push-Benachrichtigung zur Bestätigung der Lösung.

Kommentare

Sie können Kommentare zum Aktivitätsverlauf eines Vorfalls hinzufügen, um Aktualisierungen, Kontext oder nächste Schritte mit Ihrem Team zu teilen.

So fügen Sie einen Kommentar hinzu:

1. Öffnen Sie die Vorfalldetailseite.
2. Klicken Sie auf **Kommentar hinzufügen**.
3. Verfassen Sie Ihren Kommentar — Markdown wird unterstützt, einschließlich **Aufgabenlisten-Checkboxen** (`- [ ] Aufgabe` , `- [x] Erledigt`).
4. Klicken Sie auf **Absenden**.

Der Kommentar erscheint im Aktivitätsverlauf und ist für alle Teammitglieder sichtbar.

Aktionen

Von der Vorfalldetailseite können Sie:

- **Bestätigen** -- Den Vorfall als gesehen und in Bearbeitung markieren
- **Lösen** -- Den Vorfall als behoben schließen
- **Monitor anzeigen** -- Zur Detailseite des zugehörigen Monitors navigieren

Wenn Sie einen Vorfall lösen, während der zugehörige Monitor weiterhin fehlerhaft ist, warnt Pulse Sie vor der Ausführung: Das Lösen in diesem Zustand erstellt sofort einen neuen Vorfall, und die Kommentare und der Aktivitätsverlauf des aktuellen Vorfalls verbleiben bei diesem. Die Aktionsschaltfläche ändert sich zu **Trotzdem lösen**, um zu bestätigen, dass Sie fortfahren möchten.

Auf mobilen Geräten erscheint die Schaltfläche **Bestätigen** oder **Lösen** zusätzlich als breite Schaltfläche am unteren Bildschirmrand, die gut mit einer Hand erreichbar ist. Ein Tippen öffnet zunächst ein Bestätigungsfeld, bevor die Aktion ausgeführt wird. Wenn der Monitor weiterhin fehlerhaft ist, zeigt das Bestätigungsfeld dieselbe Warnung. Sobald der Vorfall gelöst ist, verschwindet die Schaltfläche.

Systemvorfälle

Pulse erstellt automatisch Systemvorfälle, wenn betriebliche Probleme erkannt werden, die Administratoren aufmerksam machen. Diese Vorfälle erscheinen in derselben Vorfallliste wie monitorausgelöste Vorfälle und lösen In-App-Benachrichtigungen an alle Organisationsadministratoren aus.

Die meisten Systemvorfälle lösen sich automatisch auf, sobald die zugrundeliegende Bedingung behoben ist — Sie müssen diese nicht manuell lösen. Ausgenommen sind Vorfälle zum Asset-Register: Eine Firmware-Änderung, ein entferntes Modul oder ein neues Gerät ist ein Ereignis, keine Bedingung, die wieder verschwindet. Diese Vorfälle bleiben daher offen, bis jemand sie bestätigt und löst.

Vorfall	Ursache
E-Mail-Zustellung fehlgeschlagen	Ein SMTP-Server konnte eine Benachrichtigungs-E-Mail nicht zustellen.
Niemand für Eskalation verfügbar	Eine Eskalationsrichtlinie wurde ausgelöst, aber kein Empfänger konnte erreicht werden.
Niemand in Bereitschaft für [Zeitplan]	Ein konfigurierter Bereitschaftsplan hat während der aktiven Betriebszeiten keine Abdeckung.
Gateway getrennt	Das Gerät hat die Verbindung zum Pulse-Gateway verloren und konnte keine erneute Verbindung herstellen.

Vorfall	Ursache
Gateway-Registrierung fehlgeschlagen	Das Gerät hat die Gateway-Registrierung nicht abgeschlossen. Dies erscheint während der Ersteinrichtung und löst sich automatisch auf, sobald die Registrierung abgeschlossen ist.
Collector getrennt	Ein Remote-Collector, dem Datenquellen zugeordnet sind, ist seit mehr als zwei Minuten getrennt oder hat sich innerhalb von zehn Minuten nach seiner Registrierung nicht verbunden. Löst sich auf, sobald er sich verbindet.
Keine gültige Lizenz	Die Organisation hat keine aktive Lizenz. Einige Funktionen können eingeschränkt sein.
Lizenz läuft bald ab	Die aktive Lizenz nähert sich ihrem Ablaufdatum.
OPC-UA-Zertifikat läuft bald ab	Das OPC-UA-Client-Zertifikat von Pulse nähert sich seinem Ablaufdatum. Löst sich auf, sobald das aktive Zertifikat wieder deutlich darüber hinaus gültig ist — siehe Rotation.
Firmware an einem Asset geändert	Ein Scan oder eine S7-Datenquelle hat an einem Modul eines Assets im Register eine andere Firmware-Version gelesen. Löst sich nicht von selbst auf. Siehe Firmware-Änderungen an Assets.
Modul aus einem Asset entfernt	Scans haben belegt, dass ein Modul eines Assets im Register nicht mehr in seinem Baugruppenträger steckt. Löst sich nicht von selbst auf. Siehe Aus Assets entfernte Module.
Neues Asset in einem gescannten Netzwerk aufgetaucht	Ein Scan hat ein Gerät an einer Adresse gefunden, die ein früherer Scan desselben Netzwerks abgedeckt und leer vorgefunden hatte. Löst sich nicht von selbst auf. Siehe Neue Assets in gescannten Netzwerken.

Firmware-Änderungen an Assets

Liest eine Gerätesuche oder eine S7-Datenquelle, die das Modul alle 10 Minuten erneut liest (siehe Was Datenquellen dem Register sagen), an einem Modul eine andere Firmware-Version, als das Asset-Register dafür führt, hält das Register die Änderung im **Verlauf** der Station fest, und Pulse erstellt einen Vorfall **Firmware an einem Asset geändert**. Eine ungeplante Firmware-Änderung an einer Steuerung verdient einen Blick: Es kann ein nicht angekündigter Wartungseinsatz sein — oder Schlimmeres.

- **Ein Vorfall je Änderung.** Werden in einem Scan zwei Module aktualisiert, entstehen zwei Vorfälle; ändert sich ein Modul später erneut, entsteht ein neuer.
- **Nur mit dem Asset-Register in Ihrer Lizenz.** Ohne es wird die Änderung weiterhin im Verlauf der Station festgehalten, aber kein Vorfall erstellt.
- **Nur für aktuelle Scans.** Wird ein Scan erst mehr als 24 Stunden nach seinem Ende in das Register übernommen, hält es die Änderung fest, ohne einen Vorfall zu erstellen — sie ist dann Geschichte, keine Neuigkeit mehr. Eine Änderung, die eine Datenquelle liest, ist beim Lesen neu und löst ihren Vorfall dann aus.
- **Nicht für außer Betrieb genommene Stationen.** Eine außer Betrieb genommene Station hält ihre Änderungen weiterhin fest, benachrichtigt aber niemanden.
- **Nicht in einem Wartungsfenster.** Eine Änderung, die vollständig in einem der Wartungsfenster des Registers vorgenommen wurde — vom letzten Lesen der alten Firmware bis zum Lesen der neuen, ob durch einen Scan oder eine Datenquelle —, wird festgehalten, als im Fenster vorgenommen markiert und löst keinen Vorfall aus.
- **Der Titel nennt nur die Art der Änderung.** Alle, die Vorfälle sehen, sehen ihn. Die Vorfallseite zeigt allen, welche Station betroffen ist — ihren Namen, ihre Adresse, die Firmware vorher und nachher und das Modul, an dem die Änderung gelesen wurde, mit Baugruppenträger und Steckplatz, Bestellnummer und Seriennummer —, damit ein für den Vorfall alarmiertes Mitglied weiß, was es bestätigt. Bei einer Station mit mehreren CPUs oder Kommunikationsprozessoren sehen Sie so, welche sich geändert hat. Administratoren sehen außerdem einen Link zur Station, wie das Asset-Register selbst. Die Vorfallliste zeigt allen den Namen und die Adresse der Station und beide Firmware-Versionen, ohne den Link.
- **Er folgt der Station.** Führen Sie die Station mit einer anderen zusammen, geht der Vorfall auf die behaltene Station über; heben Sie die Zusammenführung auf, geht er zurück.

Wie andere Systemvorfälle benachrichtigt er alle Organisationsadministratoren in der App. Standardmäßig eskaliert er nicht; ein Administrator kann in den Einstellungen des Asset-Registers eine Eskalationsrichtlinie für ihn wählen, und er eskaliert dann über diese Richtlinie — zum Beispiel nur außerhalb der Arbeitszeit. Siehe Vorfälle des Registers weiterleiten. Sobald Sie bestätigt haben, dass die Änderung beabsichtigt war, bestätigen und lösen Sie ihn.

Aus Assets entfernte Module

Belegen Gerätesuchen, dass ein Modul nicht mehr auf einer Station im Asset-Register steckt, hält das Register die Entfernung im **Verlauf** der Station fest, und Pulse erstellt einen Vorfall **Modul aus einem Asset entfernt**. Ein aus dem Baugruppenträger gezogenes Modul ist eine Änderung, von der Sie wissen sollten — ob der Austausch geplant war oder nicht.

Dass ein Scan ein Modul einfach nicht findet, genügt nicht. Das Register hält eine Entfernung nur fest, wenn sie belegt ist:

- **An seinem Steckplatz antwortet ein anderes Modul.** Ein Scan liest an Baugruppenträger und Steckplatz des Moduls ein anderes Modul mit eigener Bestellnummer und Seriennummer, über die Adresse, über die das Modul zuletzt gelesen wurde.
- **Zwei Scans verfehlen es.** Zwei Scans, die es hätten sehen können — sie haben die Adresse des Moduls erfasst, die Station erreicht und vom Steckplatz des Moduls eine Antwort erhalten —, haben es nicht gefunden, und kein Scan dazwischen hat es gefunden. Der erste dieser Scans wird vermerkt, der zweite hält die Entfernung fest.

Berücksichtigt werden nur Module mit Bestellnummer und Seriennummer, die über S7 an einem Baugruppenträger und Steckplatz gelesen wurden. Hat eine andere Steuerung die Adresse einer Station übernommen, hält das Register die Station stattdessen als ersetzt fest und erstellt für ihre Module keine Entfernung.

Für den Vorfall gelten dieselben Regeln wie für eine Firmware-Änderung:

- **Ein Vorfall je entferntem Modul.** Werden in einem Scan zwei Module entfernt, entstehen zwei Vorfälle.
- **Nur mit dem Asset-Register in Ihrer Lizenz.** Ohne es wird die Entfernung weiterhin im Verlauf der Station festgehalten, aber kein Vorfall erstellt.
- **Nur für aktuelle Scans.** Wird ein Scan erst mehr als 24 Stunden nach seinem Ende in das Register übernommen, hält es die Entfernung fest, ohne einen Vorfall zu erstellen.
- **Nicht für außer Betrieb genommene Stationen.** Eine außer Betrieb genommene Station hält ihre Entfernungen weiterhin fest, benachrichtigt aber niemanden.
- **Nicht in einem Wartungsfenster.** Eine Entfernung, die vollständig in einem der Wartungsfenster des Registers vorgenommen wurde — vom letzten Scan, der das Modul fand, bis zum Scan, der die Entfernung festhielt —, wird festgehalten, als im Fenster vorgenommen markiert und löst keinen Vorfall aus.
- **Der Titel nennt nur die Art der Änderung.** Die Vorfallseite zeigt allen, welche Station betroffen ist — ihren Namen und ihre Adresse sowie Baugruppenträger, Steckplatz, Bestellnummer und Seriennummer des entfernten Moduls. Administratoren sehen außerdem einen Link zur Station. Die Vorfallliste zeigt allen den Namen und die Adresse der Station und die Bestellnummer des entfernten Moduls, ohne den Link.
- **Er folgt der Station** beim Zusammenführen und beim Aufheben der Zusammenführung.

Er benachrichtigt alle Organisationsadministratoren in der App und eskaliert, sofern ein Administrator eine gewählt hat, über die Eskalationsrichtlinie des Registers (siehe Vorfälle des Registers weiterleiten). Taucht ein Modul in einem späteren Scan wieder auf, hält das Register es als wieder hinzugefügt fest; der Vorfall bleibt offen, bis Sie ihn lösen.

Neue Assets in gescannten Netzwerken

Findet eine Gerätesuche ein Gerät an einer Adresse, an der ein früherer Scan desselben Netzwerks nichts gefunden hat, nimmt das Asset-Register es als neue Station auf, mit einem Eintrag in ihrem **Verlauf**, und Pulse erstellt einen Vorfall **Neues Asset in einem gescannten Netzwerk aufgetaucht**. Ein Gerät, das niemand registriert hat und das plötzlich im Anlagennetz auftaucht, verdient einen Blick: Es kann ein Laptop am falschen Switch sein, ein Austausch, den niemand angekündigt hat, oder Schlimmeres.

Neu ist ein Gerät nur, wenn ein früherer Scan es dort hätte sehen können. Pulse erstellt den Vorfall nur, wenn ein früherer, abgeschlossener Scan:

- **auf derselben Appliance oder demselben Collector lief** — ein anderer Collector sieht das Netzwerk von einer anderen Stelle aus, und sein erster Scan findet alles zum ersten Mal;
- **die Adresse des Geräts abgedeckt hat** — bei einer Steuerung auf dem Port, auf dem der Scan sie jetzt gefunden hat. Ein Scan, der nur auf Port 102 gesucht hat, dem Standard-Port von S7, sagt nichts über eine Steuerung, die auf Port 1102 gefunden wurde;
- **mit der Methode gesucht hat, die das Gerät jetzt gefunden hat, und diese Methode bis zum Ende lief** — S7 für eine Steuerung, OPC UA für einen OPC-UA-Server. Ein Scan, dessen S7-Teil fehlgeschlagen ist, sagt nichts über die Adressen, die er scannen sollte.

Der erste Scan eines Netzwerks erstellt daher keinen Vorfall: Jedes Gerät darin ist neu für das Register, aber keines davon ist eine Neuigkeit. Ebenso wenig der erste OPC-UA-Scan eines Netzwerks, das zuvor nur über S7 gescannt wurde, für die OPC-UA-Server, die er findet.

Auch kein Vorfall entsteht für:

- **ein ersetztes Gerät** — eine andere Steuerung antwortet unter der Adresse einer registrierten Station. Das Register hält die Station stattdessen als ersetzt fest.
- **einen Host, den nur die Netzabfrage gesehen hat** — eine Adresse, die auf die Netzabfrage geantwortet hat, aber auf keines der gesuchten Protokolle. Automatisch vergebene Adressen kommen und gehen.
- **ein PROFINET-Gerät** — die PROFINET-Erkennung scannt keine Adressen, daher gibt es keinen früheren Scan zum Vergleich.
- **eine Station neben einer registrierten** — eine neue Station an einer Adresse, an der das Register bereits eine andere Station führt, etwa der eingebaute OPC-UA-Server einer Steuerung, der zum ersten Mal neben der Steuerung antwortet.

Für den Vorfall gelten dieselben Regeln wie für eine Firmware-Änderung:

- **Ein Vorfall je neuer Station.** Zwei neue Geräte in einem Scan erstellen zwei Vorfälle.

- **Nur mit dem Asset-Register in Ihrer Lizenz.** Ohne es wird die Station weiterhin ins Register aufgenommen, aber kein Vorfall erstellt.
- **Nur für aktuelle Scans.** Wird ein Scan erst mehr als 24 Stunden nach seinem Ende in das Register übernommen, nimmt es die Station auf, ohne einen Vorfall zu erstellen.
- **Nicht in einem Wartungsfenster.** Ein Gerät, das vollständig in einem der Wartungsfenster des Registers aufgetaucht ist — vom Beginn des früheren Scans, der seine Adresse leer fand, bis zum Scan, der es fand —, wird aufgenommen, als im Fenster gefunden markiert und löst keinen Vorfall aus.
- **Der Titel nennt nur die Art der Änderung.** Die Vorfallseite zeigt allen, welche Station betroffen ist — ihren Namen und ihre Adresse und bei einer Steuerung das Modul, als das der Scan sie gefunden hat, mit Baugruppenträger und Steckplatz, Bestellnummer und Seriennummer (die CPU, sofern kein anderes Modul die Station identifiziert hat). Ein OPC-UA-Server und eine Station, die erfasst wurde, bevor Pulse dieses Modul nannte, zeigen keines. Administratoren sehen außerdem einen Link zur Station. Die Vorfallliste zeigt allen den Namen und die Adresse der neuen Station, ohne den Link.
- **Er folgt der Station** beim Zusammenführen und beim Aufheben der Zusammenführung.

Er benachrichtigt alle Organisationsadministratoren in der App und eskaliert, sofern ein Administrator eine gewählt hat, über die Eskalationsrichtlinie des Registers (siehe Vorfälle des Registers weiterleiten). Sobald Sie wissen, um welches Gerät es sich handelt, bestätigen und lösen Sie den Vorfall; gehört es nicht ins Netzwerk, nehmen Sie es vom Netz und nehmen Sie seine Station außer Betrieb.

3.7 Ziele

Ein Monitor beantwortet die Frage "ist gerade etwas kaputt". Ein Ziel beantwortet eine andere: **wie viel der Zeit war es in Ordnung, über einen Zeitraum, der Ihnen wichtig ist -- und wie viel Ihres Spielraums für Abweichungen ist noch übrig.**

Diese zweite Frage ist die, in der Verträge geschrieben werden. "Die Linie läuft zu 99,5 % des Monats innerhalb der Grenzwerte" ist ein Versprechen, an dem man Sie messen kann; "das Kühlmittel hat gerade 78 °C" nicht. Ein Ziel ist der Ort, an dem Sie das Versprechen festhalten, damit Pulse Ihnen sagen kann, ob es eingehalten wird -- bevor es jemand anderes tut.

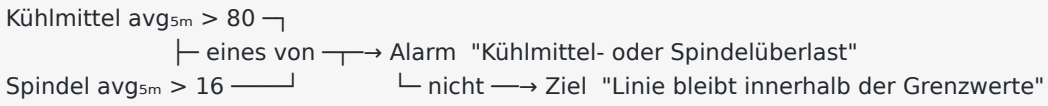
Pulse nennt das ein **Ziel**. Anderswo begegnet Ihnen dieselbe Idee als SLO -- ein Service Level Objective. Es ist dasselbe.

Worüber ein Ziel etwas aussagt

Ein Ziel ist ein Versprechen über eine Bedingung -- genauer: über einen **Ziel**-Knoten im Graphen dieser Bedingung.

Daraus folgt etwas, das man vorab verstanden haben sollte: **die Bedingung legt fest, was "gut" bedeutet, das Ziel legt fest, wie viel gut genug ist.** Beides wird bewusst an verschiedenen Stellen bearbeitet. Ein Zielwert von 99,5 % auf 99,9 % zu ändern ist keine Änderung an der Logik -- der Graph bleibt unberührt, seine Version steigt nicht, und nichts anderes, das denselben Graphen liest, ist davon betroffen.

Ein Ziel-Knoten ist **wahr, wenn alles wie versprochen läuft** -- die umgekehrte Polarität zu einem Alarm-Knoten, der wahr ist, wenn etwas nicht stimmt. Ein Graph mit beidem sieht üblicherweise so aus:



Ein Gatter, zwei Abnehmer, ein `nicht` dazwischen. Genau diese Zeichnung verhindert, dass Alarm und Versprechen sich über die Grenzwerte uneinig werden: Sie ändern den Schwellwert einmal, und beide folgen.

Mehrere Ziele dürfen auf denselben Knoten zeigen. Das ist üblich und sinnvoll -- ein vertragliches Versprechen über einen Monat und ein betriebliches über eine Woche sind verschiedene Versprechen über denselben Indikator.

Ein Ziel anlegen

Über **Ziele → Neues Ziel**, das eine eigene Anlageseite öffnet. Füllen Sie die Versprechen-Felder aus und beschreiben Sie den Indikator inline:

Feld	Bedeutung
Name	Benennt sowohl das Ziel als auch die Bedingung, auf der es gemessen wird
Zielwert	Wie viel der *gemessenen* Zeit die Bedingung halten muss. Zwischen 0 und 100 %
Fenster	Wie weit das Versprechen zurückblickt, rollierend. Zwischen 1 Stunde und 365 Tagen
Abdeckungsuntergrenze	Wie viel des Fensters gemessen sein muss, bevor Pulse überhaupt eine Zahl nennt
Eskalationsrichtlinie	Wer alarmiert wird, wenn das Ziel sein Budget verbrennt — Pflicht, wie bei jedem Monitor
Tags	Optionale Kennzeichnungen, dieselben Tags, die jeder Monitor trägt

Der Abschnitt **Indikator** unterhalb der Versprechen-Felder ermöglicht es Ihnen, das Kriterium in Satzform zu beschreiben -- einen Messwert, der innerhalb eines Bereichs bleibt, oder einen beliebigen Schwellwert, den die Appliance auswerten kann. Für alles, was ein Satz nicht ausdrücken kann, öffnet **Im Graph-Editor bearbeiten** den vollständigen Bedingungseditor; nach dem Speichern der gezeichneten Bedingung bietet der Editor **Ziel erstellen** an, was mit dieser Bedingung als Auswahl auf diese Seite zurückführt. Die Auswahl **Vorhandene Bedingung verwenden** im selben Abschnitt erreicht denselben Zustand für eine bereits gespeicherte Bedingung -- auch für eine, die schon ein Versprechen trägt, denn eine Bedingung kann mehrere Ziele stützen (etwa 99,5 % über dreißig Tage für den Vertrag und 99,9 % über sieben für das Team). Auf beiden Wegen wird die Bedingung nur angezeigt und ausschließlich das Ziel angelegt; der Graph selbst wird weiterhin im Editor bearbeitet, wo auch alles andere sichtbar ist, das ihn verwendet. Nach dem Anlegen des Ziels verweist dessen Seite für Änderungen auf den Bedingungseditor.

Das Fenster ist **rollierend**, nicht kalendarisch: Ein 30-Tage-Ziel bedeutet immer "die letzten 30 Tage", nie "seit dem Ersten des Monats".

Eine **Rückrechnung** erscheint, sobald Zielwert und Abdeckungsuntergrenze ausgefüllt sind. Sie zeigt, wie sich das Ziel anhand der bisherigen Verlaufsdaten der Bedingung verhalten hätte -- nützlich, um vor dem Speichern zu prüfen, ob Fenster und Zielwert auf echten Daten sinnvoll sind.

Nach dem Anlegen navigiert Pulse direkt zur Seite des neuen Ziels -- und **rechnet das Fenster im Hintergrund aus gespeicherten Messwerten nach**. Schon nach wenigen Augenblicken zeigt die Seite einen als *näherungsweise* gekennzeichneten Wert, statt bis zum Aufbau genügend laufender Messung bei "Zu wenig Daten" zu verharren. Der nachgerechnete Abschnitt wandert mit dem rollierenden Fenster hinaus, während echte Messung ihn ersetzt, und mit ihm verschwindet die Kennzeichnung.

Die Zahlen lesen

Die Seite eines Ziels führt mit dem erreichten Prozentwert und der Abdeckung daneben. Darunter:

Zahl	Bedeutung
Fehlerbudget	Wie viel Zeit außerhalb der Vorgabe der Zielwert über dieses Fenster erlaubt
Verbraucht	Wie viel davon aufgebraucht ist
Budget übrig	Was bleibt, in Prozent. Negativ, sobald Sie darüber hinaus sind
Verbrauchsrate	Wie schnell es geht. 1,0 ist genau im Plan; 2,0 verbraucht das Budget eines ganzen Fensters in einem halben
Nicht gemessen	Zeit im Fenster, die Pulse nicht auswerten konnte

Budget übrig ist meist die Zahl, nach der man handelt. "32 % übrig" sagt, was Sie sich noch leisten können; "99,66 %" sagt, wie es bisher gelaufen ist.

Ein Abzeichen **näherungsweise** neben dem Wert bedeutet: Ein Teil des Fensters ist nachgerechnete Historie -- beim Anlegen des Ziels aus gespeicherten Messwerten berechnet statt live gemessen. Die Seite sagt, wie viel des Fensters das betrifft, und die Budget-Kurve zeichnet diesen Abschnitt gestrichelt. Für nachgerechnete Zeit gilt derselbe Vorbehalt wie für eine Rückrechnung: verrauscht, nicht wohlwollend. Sie zählt für die Anzeige -- nie für Budget-Alarme.

Die Abdeckung wird immer gezeigt, und sie ist keine Zierde

Jede Erfüllungszahl in Pulse trägt im selben Atemzug den Anteil des Fensters, auf dem sie gemessen wurde. Das ist Absicht: **der übliche Weg, auf dem eine Verfügbarkeitszahl lügt, ist das stille Weglassen der Zeit, in der niemand hingeschaut hat.** Perfekte 100 %, gemessen an zwei Tagen eines dreißigtägigen Monats, sind kein guter Monat.

Zeit, die Pulse nicht auswerten konnte, wird aus der Rechnung herausgenommen und weder als gut noch als schlecht gezählt. Unbekannt ist kein Fehlschlag -- und auch kein Erfolg.

> **Unterhalb der Abdeckungsuntergrenze gibt es keine Zahl**
>
> Wurde weniger vom Fenster gemessen, als die Abdeckungsuntergrenze verlangt, meldet das Ziel **Nicht genug Daten** statt eines Prozentwerts -- die Zahlen dahinter bleiben sichtbar, die Überschrift ist dann aber der Vorbehalt.
>
> Das ist die ehrliche Antwort, und sie ist einer Zahl vorzuziehen: Ein Versprechen, das auf einem Drittel seines Fensters gemessen wurde, wird weder eingehalten noch gebrochen -- es wird nicht gemessen.

Die Budget-Kurve

Das Diagramm zeigt, wie das Fehlerbudget über das Fenster abschmilzt -- flach, solange die Bedingung hält, mit einer Stufe nach unten, wo sie es nicht tat. Der genaue abgedeckte Zeitraum wird unterhalb des Diagramms angezeigt.

Die Kurve sagt etwas, das der Prozentwert nicht sagen kann: *wann* das Budget verbraucht wurde. Eine einzelne Kante an einem Dienstag ist ein Vorfall, den man untersucht. Ein gleichmäßiges Gefälle ist ein Prozess, der nicht ganz stimmt und dabei nie etwas auslöst.

Benachrichtigt werden

Ein Ziel **ist unter der Haube ein Monitor**: Es trägt eine eigene Eskalationsrichtlinie, eigene Tags und einen eigenen Stummschalter, und seine Alarme erzeugen Vorfälle in derselben Liste wie alles andere. Eine Alarmierung wegen eines Fehlerbudgets funktioniert also genau wie eine wegen einer toten SPS -- nichts Neues musste lernen, wie es Sie erreicht.

Worüber es alarmiert, entscheiden seine **Budget-Alarme** -- die Staffel im gleichnamigen Bereich auf der Seite des Ziels. Ein Ziel ohne Stufen misst und berichtet und weckt niemanden, was völlig in Ordnung ist.

Budget-Alarme lesen **ausschließlich laufende Messung** -- nachgerechnete, näherungsweise Historie alarmiert niemanden. Ein frisch angelegtes Ziel zeigt deshalb sofort einen näherungsweisen Wert, hält seine Alarme aber zurück, bis genügend echte Abdeckung vorliegt -- genau wie es das ohne die Nachrechnung getan hätte.

Warum nicht einfach alarmieren, wenn das Ziel gerissen ist?

Weil es dann zu spät ist, noch etwas zu tun.

Ein 30-Tage-Ziel bei 99,5 % hat rund dreieinhalb Stunden Spielraum. Ein Alarm, der bei aufgebrauchtem Spielraum auslöst, meldet Ihnen einen Monat, den Sie bereits verloren haben. Wissen wollen Sie, dass Sie ihn **zu schnell verbrauchen, um über den Monat zu kommen** -- solange noch Budget da ist, das sich schützen lässt.

Genau darauf schaut ein Budget-Alarm: nicht auf den Stand, sondern auf die **Rate**.

Die Staffel einrichten

Im Bereich **Budget-Alarme** auf der Seite des Ziels:

1. Prüfen Sie, wer alarmiert wird -- die Eskalationsrichtlinie wurde beim Anlegen des Ziels gewählt und lässt sich hier ändern
2. Fügen Sie einen oder mehrere Budget-Alarme hinzu -- oder übernehmen Sie die empfohlene Staffel
3. **Speichern**

Die zwei Arten von Budget-Alarm

Art	Liest sich als
Budget wird zu schnell verbraucht	"Mindestens X % des Budgets sind in den letzten W verbraucht worden"
Zeit, bis das Budget aufgebraucht ist	"Beim aktuellen Tempo ist das Budget innerhalb von N leer"

Budget wird zu schnell verbraucht ist die Art, mit der man anfängt. Sie braucht keine Hochrechnung, und Sie können sie gegen die Budget-Kurve auf derselben Seite prüfen -- was viel wert ist, wenn zu entscheiden ist, ob ein ausgelöster Alarm berechtigt war.

Zeit, bis das Budget aufgebraucht ist lässt sich angenehmer formulieren und läuft unruhiger. Das aktuelle Tempo wird über ein Viertel des angefragten Horizonts gemessen, sodass eine kurze Abweichung auf eine Verletzung hochrechnen kann, die ein längerer Blick nicht vorhergesagt hätte.

Der Prozentwert bezieht sich auf das gesamte Budget, nicht auf das Fenster

"8,5 % innerhalb von 1 Stunde" bedeutet achteinhalb Prozent des Spielraums des *ganzen Monats*, verbraucht innerhalb einer Stunde.

Das macht die Stufen untereinander und gegenüber der Budget-Kurve vergleichbar. Würde jede Stufe gegen den Budgetanteil ihres eigenen Fensters messen, bedeutete jeder Schwellwert etwas anderes, und die Staffel wäre nicht lesbar.

Die empfohlene Staffel

Zwei Stufen, die der Bereich für Sie ausfüllt:

Stufe	Bedeutet typischerweise
8,5 % in 1 Stunde	Gerade läuft etwas ernsthaft schief -- jemanden alarmieren
43,2 % in 3 Tagen	Ein schleichender Verlust, der den Monat kostet -- Ticket

Wichtiger als die genauen Zahlen ist die Form: **eine schnelle Stufe für die Krise, eine langsame für das Schleichende.** Eine einzige Stufe schreit entweder bei jeder Kleinigkeit oder übersieht den schleichenden Verlust vollständig.

Ein Ziel hat eine Eskalationsrichtlinie. Sollen Stufen verschiedene Personen erreichen, zeichnen Sie zwei Ziele über denselben Knoten -- ein schnelles Versprechen an eine Richtlinie, die anruft, ein langsames an eine, die eine E-Mail schreibt.

Was ein Vorfall aussagt

Vorfälle entstehen je Stufe: Zwei ausgelöste Stufen sind zwei Vorfälle, und das Schließen des einen schließt den anderen nicht.

> **Linie 1 bleibt innerhalb der Grenzwerte verbraucht ihr Fehlerbudget** 13,26 % des Fehlerbudgets wurden innerhalb von 1 h verbraucht; 32,3 % des Budgets sind noch übrig.

Benannt ist er nach dem Ziel, nicht nach der Stufe -- das ist der Satz, der für die lesende Person etwas bedeutet. Welche Stufe es war, steht in den Zahlen. Der Vorfall verweist direkt zurück auf die Seite des Ziels.

Vorfälle eskalieren, werden bestätigt und geschlossen wie alle anderen. Wird die Stufe wieder ruhig, schließt sich der Vorfall von selbst.

Ein nicht messbares Ziel hält seine Alarme offen

Fällt das Ziel unter seine Abdeckungsuntergrenze, melden seine Budget-Alarme **Nicht bestimmbar** statt *ruhig*.

Ein bereits offener Vorfall bleibt dann offen und **eskaliert nicht weiter** -- Pulse weckt niemanden zusätzlich für etwas, das es nicht mehr bestätigen kann, und gibt ebenso wenig stillschweigend Entwarnung. Die Eskalation läuft von selbst weiter, sobald die Daten zurück sind.

Bedingungs-Monitore werden genauso behandelt, aus demselben Grund: Ein sterbender Datenpunkt darf nie wie ein behobenes Problem aussehen.

Die Staffel lesen


Die Seite eines Ziels mit den Einhaltungszahlen, der Budget-Kurve und der Budget-Alarm-Staffel

Jede Stufe zeigt, was sie gerade sagt, mitsamt der Zahl dahinter:

Kennzeichnung	Bedeutung
Verbrennt · 13,26 %	Ausgelöst. So viel des Budgets ging innerhalb des Fensters dieser Stufe
13,26 %	Ruhig -- und so nah dran
Nicht bestimmbar	Das Ziel liegt unter seiner Abdeckungsuntergrenze -- siehe oben

Auch ruhige Stufen zeigen ihre Zahl, und zwar bewusst: Der nützliche Blick auf eine Staffel gilt der Frage, *wie nah* die ruhigen Stufen sind -- nicht nur, dass sie ruhig sind.

Die Staffel bearbeiten

Stufen werden gemeinsam bearbeitet und gemeinsam gespeichert. Das Fenster einer Stufe muss mindestens eine Stunde betragen und darf nicht länger als das Fenster des Ziels sein -- eine Stufe kann nicht nach Zeit fragen, die das Versprechen nicht misst.

Wird eine Stufe entfernt und gespeichert, wird sie stillgelegt. Ein von ihr erzeugter Vorfall wird geschlossen, und ihre Kennung wird nicht wiederverwendet -- eine spätere Stufe kann also keinen alten Vorfall erben.

Stummschalten

Stummschalten im Aktionsmenü des Ziels (oder im Zeilenmenü der Liste) bringt es zum Schweigen: Budget-Alarme erzeugen keine Vorfälle, bis die Stummschaltung aufgehoben wird. Die Messung läuft die ganze Zeit weiter -- die Zahlen aktualisieren sich weiterhin, und die Seite sagt deutlich, dass das Ziel stummgeschaltet ist.

Es ist dieselbe Stummschaltung, die jeder Monitor hat -- denn das Ziel ist einer.

Aktionen in der Zielliste

Jedes Ziel in der Liste verfügt über ein Zeilenmenü mit Schnellaktionen:

- **Öffnen** — navigiert zur Detailseite des Ziels.
- **Bedingung öffnen** — öffnet den Bedingungseditor für die Bedingung, auf der dieses Ziel gemessen wird.
- **Stummschalten / Stummschaltung aufheben** — der oben beschriebene Schalter. Ein stummgeschaltetes Ziel ist in der Liste gekennzeichnet.
- **Löschen** — entfernt das Ziel.

Was beim Löschen eines Ziels mit der Bedingung geschieht, hängt davon ab, ob noch etwas anderes auf sie verweist. Verwendet ein Monitor oder ein anderes Ziel dieselbe Bedingung, bleiben die Bedingung und ihre Historie unverändert. Ist dieses Ziel der einzige Verwender, wird die Bedingung mit dem Ziel gelöscht. Der Löschdialog zeigt an, welcher Fall zutrifft, bevor Sie bestätigen.

Rückrechnung

Niemand kann einen Zielwert wählen, den er nie gemessen gesehen hat. Die Rückrechnung ermittelt aus gespeicherten Messwerten, was ein Versprechen über einen vergangenen Zeitraum *gesagt hätte* -- damit Sie einen Zielwert mit Belegen wählen statt zu raten. Sie lebt auf der **Anlegen-Seite**: Sobald das Ziel existiert, ist dieselbe Nachrechnung bereits automatisch gelaufen, und ihr Ergebnis steht als näherungsweise Nachrechnung auf der Seite des Ziels -- eine zweite Karte gibt es dort nicht mehr.

Sie beantwortet außerdem, **wofür das Budget verbraucht wurde**: welcher Zweig der Bedingung falsch war, während das Budget abfloss, als Anteil am Verbrauch. Da mehrere Zweige gleichzeitig falsch sein können, ergeben diese Anteile zusammen nicht 100 %; jeder liest sich als "dieser Teil war während N % des Verbrauchs falsch".

Eine Rückrechnung ist näherungsweise, und die Seite sagt das

Die Neuberechnung tastet auf einem groben Raster ab -- der Schritt steht neben der Zahl. Eine Abweichung, die kürzer als der Schritt ist, wird entweder ganz übersehen oder als ganzer Block gezählt.

Damit ist das Ergebnis **verrauscht, nicht geschönt**: Es über- und unterschätzt gleich wahrscheinlich, und der Fehler sinkt mit der Zahl der Abweichungen, nicht mit der Länge des Zeitraums. Ein Monat mit drei zweiminütigen Verletzungen kann als null oder als dreizehn Minuten zurückkommen.

Nutzen Sie sie, um einen Zielwert zu wählen. Zitieren Sie sie nie als Messung -- die aufgezeichnete Zahl darüber ist die Messung.

Die Rückrechnung reicht so weit zurück, wie Messwerte vorgehalten werden; deshalb sind die angebotenen Zeiträume begrenzt.

In Berichten

Vorfallberichte enthalten einen Abschnitt zu Zielen: was jedes Versprechen **über den Zeitraum des Berichts** gemeldet hat, nicht über sein eigenes rollierendes Fenster.

Genau darauf kommt es an. "Wurde das im Juni eingehalten" ist die Frage an einen Monatsbericht, und eine rollierende 30-Tage-Zahl vom Tag der Erstellung würde stillschweigend den Juli einschließen und den größten Teil des Juni auslassen.

Was Pulse hier noch nicht kann

Wissenswert, bevor Sie jemandem etwas versprechen:

- **Geplante Stillstände werden nicht erkannt.** Pulse kennt genau eine Ausnahme -- fehlende Daten -- und kann einen geplanten Stillstand nicht von einem toten Netzwerk unterscheiden. Eine Anlage, die jedes Wochenende steht, liegt unter ihrer Abdeckungsuntergrenze und meldet *Nicht genug Daten* statt einer Zahl. **Wenn Ihre Anlage nicht durchgehend läuft, lesen Sie das, bevor Sie eine Abdeckungsuntergrenze setzen.**
- **Budget-Alarme werden einmal pro Minute ausgewertet**, nicht in der Fünf-Sekunden-Schleife der Monitore. Das kürzeste zulässige Stufenfenster ist eine Stunde -- eine Minute liegt also deutlich innerhalb der Auflösung, die die Frage hat.
- **Fenster sind ausschließlich rollierend.** Ein vertraglicher "Kalendermonat" lässt sich noch nicht ausdrücken.

- **Eine Bedingung je Ziel.** Versprechen über mehrere Dinge gleichzeitig zeichnet man als eine Bedingung mit einem `alle von`-Gatter, nicht als mehrere Ziele.
- **Die Bedingung kann sich innerhalb eines Fensters ändern.** Passiert das, meldet die Seite *Die Bedingung wurde in diesem Zeitraum geändert* -- die Zahl umfasst dann zwei verschiedene Definitionen von "gut". Das ist nicht falsch, sollte aber bekannt sein, bevor man sie zitiert.

3.8 Berichte

Vorfallsberichte ermöglichen es Betreibern, wiederkehrende, teilbare Zusammenfassungen ihrer Vorfälle zu planen. Jeder Bericht deckt einen vollständigen Zeitraum ab — einen Tag, eine Woche oder einen Monat — und wird automatisch an die Personen zugestellt, die ihn sehen müssen.

Berichtsvorlagen

Berichte werden auf der Seite **Berichte** (`/app/reports`) erstellt und verwaltet. Das Erstellen, Bearbeiten und Löschen von Berichtsvorlagen ist Administratoren vorbehalten. Die Liste zeigt für jede Vorlage den Rhythmus, den nächsten geplanten Zeitpunkt und die Empfängeranzahl. Vorlagen mit externen E-Mail-Empfängern sind mit dem Label **Extern** gekennzeichnet.

Eine Berichtsvorlage definiert:

- **Berichtsname** — Eine kurze Bezeichnung für den Bericht.
- **Rhythmus** — **Täglich**, **Wöchentlich** oder **Monatlich**. Der Bericht deckt den letzten vollständigen Zeitraum für diesen Rhythmus ab, ausgewertet in der Zeitzone der Organisation.
- **Versandstunde** — Die Tageszeit (0–23, Zeitzone der Organisation), zu der der Bericht erstellt und versendet wird.
- **Link-Gültigkeit (Tage)** — Wie lange ein geteilter Berichtslink gültig bleibt.
- **Filter** — Beschränken, welche Vorfälle im Bericht erscheinen. Sie können nach **Vorfallsstatus**, **Monitor-Typen**, **Datenquellen** und **Tags** filtern. Jeder Filter ist optional; wird einer leer gelassen, gilt für diese Dimension keine Einschränkung. Der Filter **Datenquellen** beschränkt den Bericht auf Vorfälle von Monitoren, die die ausgewählten Datenquellen lesen -- nützlich für gerätesspezifische Berichte. Beim **Tag-Filter** gilt: Innerhalb einer Tag-Kategorie genügt ein übereinstimmendes Tag (ODER); kategorieübergreifend muss ein Monitor in jeder ausgewählten Kategorie mindestens ein Tag tragen (UND).
- **Empfänger** — Zwei Arten. **E-Mail-Empfänger** sind externe Personen ohne Pulse-Anmeldung; ihr Exemplar wird über eine passwortgeschützte, öffentliche URL zugestellt, die ihnen per E-Mail geschickt wird. **Pulse-Benutzer und Teams** sind Mitglieder Ihrer Organisation; wählen Sie ein Team aus, erhalten alle seine Mitglieder den Bericht. Die Team-Mitglieder werden bei jeder Erstellung des Berichts neu ermittelt — wer einem Team später beitritt, wird also automatisch berücksichtigt.

- **Aktiviert** — Wenn deaktiviert, wird die Vorlage gespeichert, aber nicht automatisch gemäß dem Rhythmus erstellt. Sie können den Bericht weiterhin manuell erstellen.

Erstellung

Berichte werden automatisch gemäß ihrem Rhythmus zur konfigurierten Versandstunde erstellt. Administratoren können außerdem das Menü **Aktionen** einer Vorlage öffnen und **Jetzt erstellen** wählen, um sofort einen Bericht zu erzeugen. Dasselbe Menü **Aktionen** enthält die Option **Löschen**, um eine Vorlage zu entfernen.

Berichtsverlauf

Jeder erstellte Bericht ist **eingefroren** — er erfasst die Vorfallsdaten zum Zeitpunkt der Erstellung und ändert sich danach nie mehr, auch wenn die zugrunde liegenden Vorfälle bestätigt, gelöst oder bearbeitet werden.

Die vergangenen Berichte einer Vorlage werden auf ihrer Detailseite unter **Letzte Berichte** aufgelistet, jeweils mit Zeitraum, Erstellungszeitpunkt und Ablaufdatum. Die Liste zeigt zuerst die neuesten Berichte; mit **Ältere** und **Neuere** blättern Sie durch die Übersicht.

Berichte werden bis zu ihrem Ablauf aufbewahrt. Sobald ein Bericht das neben ihm angezeigte Ablaufdatum überschreitet — die **Link-Gültigkeit (Tage)** seiner Vorlage, gerechnet ab der Erstellung —, wird er automatisch entfernt, sowohl aus dieser Liste als auch aus dem geteilten Link, den seine Empfänger besitzen. Wenn ein Bericht länger verfügbar bleiben soll, erhöhen Sie die **Link-Gültigkeit (Tage)** der Vorlage, bevor die betreffenden Berichte erstellt werden.

Was ein Bericht enthält

Jeder Bericht fasst die Vorfälle seines Zeitraums in mehreren Abschnitten zusammen:

- **Kennzahlen** — Eröffnete, gelöste und weiterhin offene Vorfälle sowie MTTA und MTTR.
- **Volumen & Trends** — Wie sich das Vorfallsvolumen über den Zeitraum verändert hat.
- **Status am Ende des Zeitraums** — Wie viele Vorfälle zum Abschluss des Zeitraums unbestätigt, bestätigt oder gelöst waren.
- **Wann Vorfälle beginnen** — Onset-Heatmap aufgeschlüsselt nach Wochentag und Stunde.

- **Wo Vorfälle häufen** — Vorfälle gruppiert nach Monitor-Typ, nach Tag und nach den häufigsten Monitoren.
- **Auslastung der Bereitschaft** — Wie sich die Reaktionslast über Ihr Team verteilt hat.
- **Zuverlässigkeit** — Zuerst die Ziele: je Ziel der versprochene Zielwert, der erreichte Wert, wie viel des Zeitraums überhaupt gemessen wurde und wie viel des Fehlerbudgets verbraucht ist. Wurde ein Ziel auf zu wenig des Zeitraums gemessen, weist es **Nicht genug Daten** aus statt einer Zahl. Unter jedem Ziel steht sein **Verlauf des Fehlerbudgets**: die Linie beginnt beim vollen Budget und fällt nur — ihre Steigung ist also die Verbrauchsrate, und die Nulllinie markiert den Punkt, an dem das Versprechen aufgebraucht war. Danach wiederkehrende Monitore und Systemereignisse über den Zeitraum.
- **Vorfalldetails** — Eine filterbare, sortierbare und exportierbare Tabelle der einzelnen Vorfälle.

Einen Bericht anzeigen

Wie ein Bericht geöffnet wird, hängt davon ab, wer ihn ansieht.

Pulse-Benutzer — einzeln oder über ein Team ausgewählt — öffnen Berichte in der App in einer angemeldeten Ansicht, die kein Passwort benötigt. Der Bericht ist über die Berichtsliste der Vorlage erreichbar und wird direkt aus der In-App-Benachrichtigung und der E-Mail verlinkt, die sie erhalten.

Externe E-Mail-Empfänger öffnen Berichte über einen passwortgeschützten geteilten Link. Jeder Empfänger erhält sein eigenes, individuelles Zufallspasswort, das ihm einmalig per E-Mail zugesandt wird — es wird niemals gespeichert. Beim Öffnen des Links wird nach diesem Passwort gefragt und anschließend der Bericht angezeigt. Der öffentliche Berichtsbetrachter enthält eine **Sprachumschaltung** (DE / EN), mit der Empfänger die Anzeigesprache des Berichts wechseln können. Links laufen nach der **Link-Gültigkeit (Tage)** der Vorlage ab.

Zustellung

Wenn ein Bericht erstellt wird:

1. **E-Mail-Empfänger** erhalten ihren persönlichen geteilten Link zusammen mit ihrem Passwort per E-Mail.
2. **Pulse-Benutzer** — einschließlich der Mitglieder jedes ausgewählten Teams — erhalten eine In-App-Benachrichtigung und eine E-Mail, die auf die angemeldete In-App-Ansicht verweist. Wer sowohl einzeln ausgewählt ist als auch zu einem ausgewählten Team gehört, wird einmal benachrichtigt, nicht doppelt.

Siehe Vorfälle für Details zu den Vorfällen, die diese Berichte speisen.

3.9 Schwachstellen

Pulse gleicht veröffentlichte CVEs (Common Vulnerabilities and Exposures) mit Ihrem Geräteinventar ab und stellt jeden Treffer als **Fund** dar, den Sie bewerten können. Anders als ein Vorfall — der ein Ausfallen oder Wiederanlaufen eines Monitors abbildet — löst sich eine Schwachstelle selten von selbst. Sie erfordert eine Entscheidung: Betrifft sie dieses Gerät, wird das Gerät auf eine Weise eingesetzt, die es angreifbar macht, und wie gehen Sie damit um? Schwachstellen sind deshalb ein eigenständiger Bereich in Pulse mit eigenem Lebenszyklus, eigener Aktivitätshistorie und eigener Berichterstattung, getrennt von Vorfällen.

CVE-Monitore

Ein **CVE-Monitor** steht für ein Gerät in Ihrem Inventar, das auf bekannte Schwachstellen geprüft werden soll. Sie legen ihn mit der Geräteidentität an:

- **Hersteller** — der Gerätehersteller (zum Beispiel Siemens).
- **Bestellnummer** — die Bestellnummer des Herstellers (die Siemens-MLFB, zum Beispiel `6ES7515-2AN03-0AB0`). Der genaueste Schlüssel: Eine Meldung, die genau dieses Teil nennt, passt.
- **Produktname** — das Produkt oder der Modultyp in der Schreibweise der Hersteller-Sicherheitsmeldungen (zum Beispiel `SIMATIC S7-1500 CPU 1518-4 PN/DP` oder `AC500 V3`). So werden Meldungen abgeglichen, die ein Produkt statt einer Bestellnummer nennen — alle Hersteller außer Siemens sowie Siemens' eigene Softwareprodukte und Produktfamilien.
- **Firmware** (optional) — die installierte Firmware-Version, damit versionsspezifische Sicherheitsmeldungen präzise ausgewertet werden können.

Ein Monitor braucht eine Bestellnummer oder einen Produktnamen; mit beidem passen Meldungen, die eines von beiden nennen. Hersteller und Produktname werden nach einer Normalisierung von Groß-/Kleinschreibung, Schreibvarianten und Firmenzusätzen verglichen — `PHOENIX CONTACT` und `Phoenix Contact GmbH & Co. KG` sind derselbe Hersteller —, der Produktname muss aber das exakte Produkt sein: `AC500 V2` und `AC500 V3` sind zwei Produkte mit unterschiedlichen betroffenen Versionen.

CVE-Monitore befinden sich neben Ihren übrigen Monitoren unter **CVE-Monitore**. Sie können einen Monitor dort anlegen oder für ein Modul von der Seite seiner Station im Asset-Register aus starten.

Pulse prüft jeden CVE-Monitor regelmäßig erneut gegen den Schwachstellenkatalog. Ein Monitor wird als **fehlerhaft** angezeigt, solange er einen Fund mit dem Status **Offen** oder **In Bearbeitung** enthält, und als fehlerfrei, sobald zu jedem Fund eine Entscheidung vorliegt oder keine Schwachstellen zutreffen.

Gerät aus dem Asset-Register übernehmen

Wenn Ihre Organisation das Asset-Register nutzt, kann ein CVE-Monitor Bestellnummer und Firmware von einem Modul im Register übernehmen, statt sie von Hand eingetragen zu bekommen. Wählen Sie im CVE-Monitor-Formular unter **Asset aus dem Register** das Asset und dann das **Modul**. Bestellnummer und Firmware werden ausgefüllt und schreibgeschützt angezeigt, mit dem Hinweis, dass sie aus dem Register stammen.

Von da an folgen sie dem Modul. Findet ein späterer Netzwerk-Scan eine neue Firmware darauf, wird der Monitor bei seiner nächsten Prüfung gegen die neue Version abgeglichen, ohne dass Sie ihn bearbeiten. Ein Firmware-Update, das eine Schwachstelle beseitigt, erscheint auf der Seite der Station als **Durch Firmware-Wechsel behoben**.

- **Hersteller** bleibt ein Wert, den Sie bestätigen. Das Register erfasst keinen Hersteller; das Formular trägt deshalb bei der Wahl eines Moduls Siemens ein, sofern der Hersteller noch leer ist. Korrigieren Sie ihn bei Bedarf. Sicherheitsmeldungen werden auch nach Hersteller abgeglichen.
- **Produktname** wird nicht aus dem Register übernommen. Tragen Sie ihn ein, wenn zusätzlich nach Produktname abgeglichen werden soll.
- Ein Modul ohne Bestellnummer kann keinen Monitor tragen. Das Formular weist darauf hin, und Sie tragen das Gerät stattdessen von Hand ein.
- Um das Gerät wieder von Hand einzutragen, wählen Sie **Keine (Gerät von Hand eintragen)**.

Die Stationsauswahl wird Organisationsadministratoren angezeigt, wenn Ihre Lizenz das Asset-Register enthält. Geräte, die das Register nicht enthält, etwa OPC-UA-Server oder Gateways, tragen Sie wie bisher von Hand ein.

Funde und ihr Lebenszyklus

Jede zutreffende CVE wird zu einem **Fund**, der seinem CVE-Monitor zugeordnet ist. Ein Fund trägt die Details der Sicherheitsmeldung (CVSS-Wert und Schweregrad, betroffenes Produkt und betroffene Version, Hinweise zur Behebung und einen Link zur Quellmeldung) sowie einen **Bewertungsstatus**:

- **Offen** — neu erkannt, noch nicht bewertet.
- **In Bearbeitung** — wird aktiv untersucht oder behoben.

- **Behoben** — die Schwachstelle wurde behoben.
- **Wird nicht behoben** — eine tatsächliche Schwachstelle, aber die bewusste Entscheidung, sie nicht zu beheben (akzeptiertes Risiko). Erfordert eine Begründung.
- **Nicht betroffen** — als nicht zutreffend bewertet (zum Beispiel wird die betroffene Funktion nicht genutzt, oder der Versionsabgleich war ein Fehlalarm). Erfordert eine Begründung.
- **Risiko akzeptiert** — vorübergehend bis zu einem von Ihnen gewählten Datum akzeptiert. Verstreicht dieses Datum, kehrt der Fund automatisch zu **Offen** zur erneuten Bewertung zurück. Erfordert eine Begründung und ein Ablaufdatum in der Zukunft.
- **Mitigiert** — die Schwachstelle trifft zu, aber eine ausgleichende Maßnahme blockiert sie, zum Beispiel ein geschlossener Port, eine Firewall-Regel oder ein abgetrenntes VLAN. Erfordert eine Begründung: Nennen Sie die Maßnahme. Der Status hat kein Ablaufdatum.

Nur **Offen** und **In Bearbeitung** wirken sich auf den Zustand des Monitors aus. Jeder andere Status ist eine Entscheidung und lässt den Monitor fehlerfrei.

Die Entscheidungsstatus unterscheiden sich darin, was sie über die Schwachstelle aussagen:

Status	Trifft sie auf das Gerät zu?	Was steht zwischen ihr und einem Angreifer	Endet von selbst?
Nicht betroffen	Nein	Nichts nötig	Nein
Behoben	Nicht mehr	Sie wurde behoben, zum Beispiel durch ein Firmware-Update	Nein
Mitigiert	Ja	Eine Maßnahme, die Sie umgesetzt haben	Nein
Risiko akzeptiert	Ja	Nichts — Sie akzeptieren das Risiko befristet	Ja, am Datum
Wird nicht behoben	Ja	Nichts — Sie belassen sie bewusst	Nein

Bewertungsentscheidungen sind **beständig**: Sie bleiben über erneute Prüfungen hinweg erhalten. Verschwindet eine Schwachstelle aus einer Prüfung und taucht später wieder auf, wird die frühere Bewertungsentscheidung beibehalten statt zurückgesetzt.

Entscheidungen am Modul erfasst

Wenn ein CVE-Monitor sein Gerät aus dem Asset-Register übernimmt, wird die Bewertungsentscheidung am Modul und an der CVE erfasst, nicht am Monitor. Das Modul überdauert jeden Monitor, und damit auch die Entscheidung:

- **Ein zweiter Monitor auf demselben Modul zeigt dieselbe Entscheidung.** Ändern Sie den Status am Fund des einen Monitors, ändert er sich auch am Fund des anderen.
- **Ein gelöschter und neu angelegter Monitor bringt die Entscheidung zurück.** Findet der neue Monitor die CVE wieder, beginnt der Fund mit der erfassten Entscheidung statt mit **Offen**.
- **Der Verlauf bleibt beim Modul**, auch wenn zwei Stationen des Registers zusammengeführt werden oder eine Zusammenführung rückgängig gemacht wird.

Einzelbewertung, Sammelbewertung und der automatische Ablauf einer Risikoakzeptanz werden alle auf diese Weise erfasst. Die Seite der Station zeigt jede Entscheidung mit ihrem Verlauf; siehe Schwachstellen auf der Stationsseite. Monitore, deren Gerät Sie von Hand eingetragen haben, behalten ihre Entscheidungen wie bisher am Monitor.

Um diese Entscheidungen weiterzugeben, etwa an eine Prüferin oder einen Prüfer, exportieren Sie sie auf der Assets-Seite: eine Zeile je Modul und CVE, offen oder geschlossen, mit der geltenden Entscheidung und wer sie getroffen hat. Siehe Schwachstellenstatus exportieren.

Funde werden nie gelöscht. Erkennt eine erneute Prüfung eine CVE nicht mehr, wird der Fund als **nicht mehr erkannt** markiert und aufbewahrt, damit Historie und Trends vollständig bleiben. Verwenden Sie den Filter **Nicht mehr erkannte anzeigen**, um diese in der Liste einzublenden.

Einen Fund bewerten

Öffnen Sie einen Fund, um seine vollständige Sicherheitsmeldung, das Bewertungsfeld und die Liste der betroffenen Geräte zu sehen.

Das Panel **Betroffene Geräte** listet alle Geräte in Ihrer Organisation auf, die einen Fund zur selben CVE aufweisen — nicht nur das gerade angezeigte. Jeder Eintrag zeigt den Gerätenamen, den Bewertungsstatus und ob die CVE noch erkannt wird. Klicken Sie auf ein Gerät, um direkt zu dessen Fund zu gelangen. Das aktuell angezeigte Gerät ist mit *(dieses Gerät)* gekennzeichnet und nicht verlinkt. Nutzen Sie dieses Panel, um die Reichweite einer CVE in Ihrer Geräteflotte einzuschätzen und einheitlich zu bewerten.

Administratoren können den Bewertungsstatus über die Aktion **Bewertung ändern** anpassen:

1. Wählen Sie den neuen **Status**.
2. Geben Sie bei **Wird nicht behoben**, **Nicht betroffen**, **Risiko akzeptiert** oder **Mitigiert** eine **Begründung** ein. Nennen Sie bei **Mitigiert** die ausgleichende Maßnahme.
3. Wählen Sie bei **Risiko akzeptiert** das Datum, an dem die Akzeptanz abläuft.
4. Speichern Sie.

Derselbe Dialog öffnet sich über **Entscheidung erfassen** auf der Seite einer Station im Asset-Register. Eine dort erfasste Entscheidung erscheint sofort auf den CVE-Seiten.

Jedes Mitglied kann einem Fund **Kommentare** hinzufügen, um Untersuchungsnotizen festzuhalten.

Aktivitätshistorie

Jeder Fund führt eine chronologische **Aktivitätshistorie** über alles, was mit ihm geschehen ist — automatische Prüfereignisse (erkannt, nicht mehr erkannt, wieder aufgetaucht, Risikoakzeptanz abgelaufen) und Aktionen von Personen (Bewertungsänderungen mit vorherigem und neuem Status sowie Begründung, und Kommentare). Prüfungsbedingte Einträge werden *System* zugeordnet; Einträge von Personen zeigen, wer sie vorgenommen hat.

Der Reiter **Aktivität** auf der Schwachstellen-Seite zeigt dieselben Ereignisse über alle Funde Ihrer Organisation hinweg, die neuesten zuerst, sodass Sie die jüngste Bewertungs- und Erkennungsaktivität auf einen Blick sehen.

Die Schwachstellen-Seite

Die Seite **Schwachstellen** hat vier Reiter:

- **Übersicht** — ein Überblicks-Dashboard mit Anzahl nach Bewertungsstatus und Schweregrad, einem 30-Tage-Trend für Erkannt vs. behoben und den am stärksten betroffenen Geräten.
- **CVEs** — eine aufklappbare Zeile pro eindeutiger CVE, zusammengefasst über alle Ihre Geräte. Jede Zeile zeigt die CVE-Kennung, den Titel, die Anzahl der betroffenen Geräte, den Schweregrad sowie eine Aufschlüsselung der Bewertungsstatus über alle Funde dieser CVE. Klicken Sie auf eine Zeile, um sie aufzuklappen und die einzelnen Funde direkt einzusehen.
- **Funde** — eine Zeile pro einzelnem Fund (eine flache Liste).
- **Aktivität** — die organisationsweite Aktivitätshistorie (siehe Aktivitätshistorie).

Filtern und suchen

Die Reiter **CVEs** und **Funde** teilen sich dieselben Filter- und Suchoptionen:

- **Suche** — nach CVE-Kennung, Titel oder betroffenem Produkt.
- **Filter** — nach Bewertungsstatus, Schweregrad und Monitor-Tags; und ob nicht mehr erkannte Funde angezeigt werden.

Sammelbewertung

In der **CVEs**-Ansicht können Organisationsadministratoren alle Funde einer CVE auf einmal bewerten, ohne jeden Fund einzeln öffnen zu müssen. Klicken Sie auf das ⋯-Menü einer CVE-Zeile und wählen Sie **Alle bewerten**. Der Dialog funktioniert genauso wie der Bewertungsdialog für einen einzelnen Fund — wählen Sie einen Status, fügen Sie bei Bedarf eine Begründung hinzu und bestätigen Sie. Die Entscheidung wird auf jeden Fund dieser CVE über alle Geräte Ihrer Organisation angewendet.

Sind beim Öffnen des Sammelbewertungs-Dialogs Filter aktiv, weist ein Hinweis darauf hin, dass die Aktion organisationsweit gilt — nicht nur für den gefilterten, aktuell sichtbaren Ausschnitt.

Sammelbewertungs-Ereignisse erscheinen in der Aktivitätshistorie mit der Bezeichnung **Sammelbewertung**, sodass Sie sie von Bewertungsänderungen einzelner Funde unterscheiden können.

Untersuchung mit KI-Canvas

Auf der Detailseite eines CVE-Funds öffnet die Schaltfläche **KI fragen** den KI-Canvas mit einer vorausgefüllten Frage zu dieser spezifischen CVE und diesem Gerät. Der Assistent erklärt die Schwachstelle verständlich — worum es geht, wie schwerwiegend sie ist und was ein Angreifer damit tun könnte — und analysiert anschließend, wie sie den jeweiligen überwachten Monitor betrifft: ob er in einer OT-Umgebung wahrscheinlich ausnutzbar ist und welche konkreten Behebungs- oder Minderungsmaßnahmen ergriffen werden sollten.

Sie können den KI-Canvas auch ohne Öffnen eines bestimmten Funds nach Schwachstellen befragen. Aus dem Canvas heraus kann der Assistent Ihre CVE-Funde nach Bewertungsstatus, Schweregrad, betroffenem Gerät und weiteren Filtern abfragen — zum Beispiel: „Welche meiner Geräte haben kritische offene CVEs?" oder „Gib mir einen Schwachstellenbericht für meine Siemens-Geräte."

Berichterstattung

Pulse versendet wöchentlich eine **Schwachstellen-Zusammenfassung** per E-Mail an die Administratoren der Organisation: Anzahl nach Bewertungsstatus sowie die Anzahl neuer Funde mit kritischem und hohem Schweregrad aus der vergangenen Woche. Es ist keine Konfiguration erforderlich.

Lizenzierung

Die Schwachstellen-Funktion wird pro Organisation durch Ihre Lizenz freigeschaltet. Ohne sie stehen CVE-Monitore und Funde nicht zur Verfügung.

3.10 KI-Canvas

KI-Canvas ist ein interaktiver Untersuchungsbereich, in dem Sie Fragen zu Ihrem System stellen und der Assistent seine Ergebnisse auf einem räumlichen Canvas darstellt. Jede Frage startet ein neues Canvas; die Erkenntnisse des Assistenten — abgefragte Vorfälle, geprüfte Monitore, abgerufene Zeitreihendaten — erscheinen als Karten, die Sie verschieben und zoomen können.

> **INFO**
>
> KI-Canvas erfordert eine aktive Lizenz mit aktiviertem KI-Canvas-Feature. Ist KI-Canvas nicht in Ihrer Lizenz enthalten, erscheint der Eintrag **Canvas** nicht in der Seitenleiste. Wenden Sie sich an Ihren Administrator, um Ihre Lizenz zu erweitern.

Erste Schritte

Navigieren Sie zu **Canvas** in der Seitenleiste, um die Canvas-Liste zu öffnen. Geben Sie eine Frage in das Eingabefeld ein und drücken Sie **Fragen** (oder **Eingabe**), um ein neues Canvas zu starten. Pulse sendet die Frage an den KI-Assistenten und öffnet das Canvas, während der Assistent arbeitet.

Sie können ein Canvas auch von der **Abfrage**-Seite aus starten: Klicken Sie auf die Schaltfläche **KI um Hilfe bitten** (✦) in der Werkzeugleiste des Abfrage-Editors, um ein neues Canvas mit einer vorausgefüllten Eingabe zu öffnen, die den Assistenten dabei unterstützt, eine Zeitreihenabfrage für Sie zu erstellen.

Sie können Fragen zu allem stellen, was Ihr überwachtes System betrifft — zum Beispiel:

- „Gibt es aktive Vorfälle in der Produktionslinie?"
- „Zeig mir den Signalverlauf für Sine0 in der letzten Stunde."
- „Welche Monitore sind derzeit nicht in Ordnung?"
- „Welche meiner Geräte haben kritische offene CVEs?"

Das Canvas

Sobald der Assistent Ergebnisse zurückgeliefert hat, öffnet sich das Canvas in einer geteilten Ansicht mit zwei separaten Bereichen:

- **Links — Untersuchungs-Board**: Die Ergebnisse des Assistenten erscheinen als Karten auf einer freien räumlichen Arbeitsfläche. Jede Karte steht für ein Werkzeugergebnis — eine Datenabfrage, Vorfallsliste, Monitorliste oder CVE-Funde. Karten erscheinen, sobald der Assistent sie anheftet, und bleiben zwischen Sitzungen auf dem Board erhalten.
- **Rechts — Unterhaltung**: Das Chat-Panel zeigt das vollständige Gespräch: Ihre Fragen und die Textantworten des Assistenten. Werkzeugaufrufe des Assistenten sind hier über die Schaltfläche **Werkzeugaufrufe anzeigen** zugänglich.

Wenn das Board leer ist — bevor der Assistent etwas angeheftet hat — zeigt es die Meldung **Noch nichts angeheftet** als Hinweis, dass Ergebnisse hier erscheinen und die Unterhaltung im Chat bleibt.

Der Assistent verwendet beim Verfassen von Antworten und Berichten die konfigurierte Zeitzone Ihrer Organisation. Intern arbeitet er mit UTC; die Umrechnung erfolgt automatisch.

Karten

Jede Karte auf dem Board zeigt das Ergebnis eines Werkzeugaufrufs des Assistenten:

Kartentyp	Inhalt
Datenabfrage	Ein Zeitreihendiagramm aus einer Datenpunktabfrage
Vorfälle	Vorfälle, die der Assistent gefunden hat
Monitore	Monitore, die der Assistent gefunden hat
CVE-Funde	Schwachstellenfunde, die der Assistent gefunden hat
Tags	Tags, die der Assistent gefunden hat

Jede Karte zeigt einen Zeitstempel, wann sie erfasst wurde. Datenabfrage-Karten haben drei Reiter — **Diagramm**, **Übersicht** und **Werte** — für unterschiedliche Ansichten desselben Ergebnisses. Wenn ein Werkzeug mehr Zeilen zurückgegeben hat, als es anzeigen kann, erscheint am unteren Rand der Karte ein Hinweis.

Vorfälle, Monitore und CVE-Funde in Karten verlinken direkt auf ihre Detailseiten. Bei langen Ergebnislisten können Sie die vollständige Liste über **Weitere anzeigen** aufklappen.

Sie können jede Karte über das Breitensteuerfeld in der Kopfzeile anpassen: **Schmal**, **Breit** oder **Extra breit**.

Navigation auf dem Board

Aktion	So geht es
Verschieben	Leere Board-Fläche ziehen oder **Leertaste** halten und ziehen
Zoomen	Strg / ⌘ + Scrollrad oder Pinch-Geste auf dem Trackpad
Scrollen (Verschieben ohne Zoom)	Scrollrad (ohne Strg / ⌘)
Rein-/Rauszoomen	Schaltflächen **+** / **−** in der Werkzeugleiste
Alle Karten in die Ansicht einpassen	Schaltfläche □ (Einpassen) in der Werkzeugleiste
Zoom auf 100 % zurücksetzen	**Zoom zurücksetzen** in der Werkzeugleiste

Der aktuelle Zoomgrad wird als Prozentwert zwischen den Zoom-Schaltflächen angezeigt.

Board-Werkzeugleiste

Die Werkzeugleiste am unteren Rand des Boards bietet zwei Interaktionsmodi:

- **Auswählen** — Karten anklicken, um sie auszuwählen; Karten ziehen, um sie auf dem Board neu zu positionieren.
- **Verschieben** — Ziehen zum Verschieben des Boards, ohne Karten auszuwählen oder zu bewegen. Nützlich, wenn viele Karten nah beieinander liegen.

Wechseln Sie zwischen den Modi über die Schaltflächen **Auswählen** und **Verschieben** in der Werkzeugleiste. Das Halten der **Leertaste** wechselt vorübergehend in den Verschiebe-Modus, unabhängig vom aktiven Modus.

Board aufräumen ordnet alle Karten in einem übersichtlichen Raster an — nützlich nach einer langen Sitzung, in der Karten verstreut wurden. Die Positionen nach dem Aufräumen werden wie jede andere Verschiebung gespeichert.

Karten anordnen

Karten können frei an beliebige Positionen auf dem Board gezogen werden. Ihre Positionen werden automatisch gespeichert und sind für alle sichtbar, die dasselbe Canvas aufrufen.

Auf Touch-Geräten und kleinen Bildschirmen ist das Board schreibgeschützt — Karten können weder gezogen noch in ihrer Größe verändert werden. Die vollständige Anordnung ist weiterhin sichtbar; für Änderungen sind eine Maus und ein größerer Bildschirm erforderlich.

Canvas umbenennen

Canvas-Eigentümer können ein Canvas umbenennen, indem sie auf den Titel in der Kopfzeile klicken. Bearbeiten Sie den Namen und drücken Sie **Eingabe** zum Speichern oder **Escape** zum Abbrechen.

Pulse benennt das Canvas auch automatisch in zwei Stufen: Sobald Sie die erste Nachricht senden, erhält das Canvas einen Namen aus der ersten Zeile Ihrer Frage, sodass es während des laufenden Durchgangs erkennbar ist. Nach erfolgreichem Abschluss des Durchgangs ersetzt der Assistent diesen Zwischennamen durch einen kurzen, aussagekräftigen Titel, der aus dem gesamten Gesprächsverlauf abgeleitet wird. Eine manuelle Umbenennung sperrt den Namen — keine der automatischen Stufen überschreibt ihn.

Ein Canvas, das noch keinen automatischen Titel erhalten hat, erscheint als **Unbenanntes Canvas** in der Liste, im Umschalter und in der Titelleiste. Beim Klick auf den Titel zum Umbenennen beginnen Sie mit einem leeren Eingabefeld, ohne den Platzhaltertext erst löschen zu müssen.

Der automatisch generierte Titel wird in der Sprache des Gesprächs verfasst — Fragen auf Deutsch ergeben einen deutschen Titel.

Zwischen Canvases wechseln

Die Kopfzeile des Canvas-Editors enthält rechts eine Schaltfläche **Canvas wechseln** (Stapel-Symbol). Klicken Sie darauf, um ein Seitenpanel mit allen Ihren Canvases zu öffnen. Wählen Sie eine Zeile aus, um direkt zu diesem Canvas zu wechseln, oder klicken Sie unten auf **Neues Canvas**, um zur Canvas-Liste zurückzukehren und ein neues zu starten.

Board- und Chat-Reiter (kleine Bildschirme)

Auf kleinen Bildschirmen, auf denen Board und Chat nicht nebeneinander angezeigt werden können, erscheinen zwei Umschaltschaltflächen — **Canvas** und **Chat** — unterhalb der Kopfzeile. Verwenden Sie sie, um zwischen dem Untersuchungs-Board und dem Gesprächsbereich zu wechseln. Auf größeren Bildschirmen sind beide Bereiche immer sichtbar und die Umschaltung ist ausgeblendet.

Untersuchung fortsetzen

Eigentümer können weitere Fragen über das Texteingabefeld am unteren Rand des Chat-Panels stellen. Drücken Sie **Eingabe** zum Senden (oder **Umschalt+Eingabe** für einen Zeilenumbruch). Der Assistent führt einen weiteren Lauf durch und fügt neue Karten zum Canvas hinzu.

Nicht-Eigentümer sehen am unteren Rand des Chat-Panels einen Hinweis auf den Lesezugriff, der den Eigentümer des Canvas nennt und einen Link zum Erstellen eines eigenen Canvas anbietet. Wenn der Eigentümer die Organisation verlassen hat, weist der Hinweis darauf hin.

Canvases verwalten

Die Canvas-Listenseite zeigt alle Canvases, die Sie besitzen oder einsehen können. Jede Zeile zeigt den Canvas-Namen, den Eigentümer und den Zeitpunkt der letzten Aktualisierung. Ein farbiges Statusabzeichen erscheint neben dem Zeitstempel für Canvases, die gerade ausgeführt werden (pulsierendes Bernstein) oder bei deren letztem Lauf ein Fehler aufgetreten ist (Rot).

Sobald Ihre Liste eine gewisse Anzahl an Canvases überschreitet, erscheint oberhalb der Liste ein **Filter**-Eingabefeld. Geben Sie einen Teil des Canvas-Namens ein, um die Liste einzugrenzen. Der Filter greift nur auf die geladene Liste zu — er durchsucht nicht den Server.

Um ein Canvas zu löschen, öffnen Sie das Aktionsmenü der Zeile (⋯) und wählen Sie **Löschen**. Bestätigen Sie die Löschung im Dialogfeld. Das Löschen ist dauerhaft — der Canvas-Verlauf und alle Ergebnisse werden entfernt.

Verwandte Dokumentation

- Abfrage — Erstellen Sie direkt Ad-hoc-Zeitreihenabfragen auf Ihren Monitordaten.
- Monitore — Die Monitore, die der Assistent in Ihrem Auftrag abfragen kann.
- Vorfälle — Die Vorfälle, die der Assistent suchen und zusammenfassen kann.
- Schwachstellen — CVE-Funde, die der Assistent abfragen und analysieren kann.

3.11 Abfrage

Auf der Abfrage-Seite erkunden Sie die Zeitreihendaten, die Pulse von Ihren Datenquellen erfasst — OPC-UA-Servern, S7-SPS, Prometheus-Endpunkten und Heartbeats. Statt einen einzelnen Monitor zu betrachten, erstellen Sie eine oder mehrere Ad-hoc-Abfragen — wählen Sie die Datenpunkte, legen Sie die Aggregation fest und sehen Sie das Ergebnis als Diagramme oder als Tabelle.

Dies ist eine reine Auswertung. Abfragen ändern niemals Ihre Monitore, Schwellenwerte oder Vorfälle.

Aufbau einer Abfrage

Jede Abfrage ist eine Zeile im Bereich **Definieren** und wird aus drei Teilen zusammengesetzt, die nebeneinander angezeigt werden:

- **SELECT** — die zu berechnende Aggregation (z. B. Durchschnitt, Maximum, ein Perzentil).
- **WHERE** — die einzubeziehenden Datenpunkte.
- **GROUP BY** — wie die Ergebnisse in einzelne Datenreihen aufgeteilt werden.

Zeitraum und Granularität legen Sie über das Uhrsymbol in der Kopfzeile des Bereichs fest; sie gelten für **alle** Abfragen der Seite, sodass sich alle Diagramme eine Zeitachse teilen und zum selben Zeitpunkt gelesen werden können. Klicken Sie auf **Abfrage ausführen** (oder drücken Sie **⌘ Eingabe** / **Strg Eingabe**), um sie auszuführen, oder auf **Abbrechen**, um die aktuellen Ergebnisse zu löschen.

Mit dem Ausführen erhält das Ergebnis außerdem eine eigene Adresse: Die URL der Seite benennt nun diesen Lauf. Wer sie später öffnet — oder von Ihnen erhält — sieht die Zahlen dieses Laufs, statt die Frage erneut über einen neueren Zeitraum zu stellen. Klicken Sie wieder auf **Abfrage ausführen**, wenn Sie aktuelle Zahlen möchten: Das ist ein neuer Lauf mit eigener URL, sodass ein bereits geteilter Link weiterhin dasselbe zeigt. Ein Ergebnis wird 30 Tage aufbewahrt; danach bittet sein Link darum, die Abfrage erneut auszuführen.

Mehrere Abfragen vergleichen

Über **+ Abfrage hinzufügen** fügen Sie eine weitere Zeile hinzu, bis zu sechs. Jede Zeile fragt nach ihrem eigenen Gegenstand — eigene Datenpunkte und Tags, eigene Gruppierung, eigene Aggregationen. So vergleichen Sie unterschiedliche Größen: die

Temperatur einer Linie mit dem Durchsatz einer anderen, oder den Wert eines Sensors mit der Latenz der Verbindung, die ihn liest.

Mehrere Aggregationen *desselben Gegenstands* brauchen keine zweite Abfrage — legen Sie sie in dieselbe Zeile, und sie werden gemeinsam abgefragt (siehe SELECT unten).

Eine neue Zeile startet leer. Das Menü ⋮ einer Zeile bietet:

- **Duplizieren** — eine Kopie der Zeile, bereit, zum Vergleichsobjekt umgebaut zu werden.
- **Entfernen** — die Zeile löschen. Die letzte verbleibende Abfrage lässt sich nicht entfernen.

Jede Abfrage wird durch einen Buchstaben (A, B, C …) gekennzeichnet, der auf ihrer Zeile und auf ihrem Diagramm erscheint. Klicken Sie auf den Buchstaben, um der Abfrage stattdessen einen Namen zu geben — hilfreich, wenn zwei Abfragen sonst gleich aussähen. Der Name erscheint in der Diagrammüberschrift, in der Übersicht und in der Abfrageauswahl der Registerkarte Tabelle, und er bleibt erhalten, wenn Sie den Link zur Seite teilen.

> **KI um Hilfe bitten**
>
> Klicken Sie auf die Schaltfläche **KI um Hilfe bitten** (✦) in der Werkzeugleiste, um KI-Canvas mit einer vorausgefüllten Eingabe zu öffnen, die den Assistenten durch die Erstellung einer Abfrage führt. Der Assistent fragt, was Sie herausfinden möchten, erstellt die Abfrage und zeigt Ihnen die Ergebnisse.

SELECT — die Aggregation

Eine Aggregation verdichtet alle Messwerte eines Zeitintervalls zu einer einzigen Zahl. Eine Abfrage trägt **eine bis vier** davon, und jede erhält ihr eigenes Diagramm — Durchschnitt *und* Maximum eines Sensors sind also eine Abfrage, eine Anfrage und zwei Grafiken.

Eine Aggregation ist eine Funktion, die auf ein Feld angewendet wird:

- **Funktionen** — Anzahl, Summe, Durchschnitt, Min, Max, Neuester sowie Perzentile (P1, P5, P10, P25, P50/Median, P75, P90, P95, P99 und feinere Stufen wie P0,1 und P99,9).
- **Felder** — der aggregierte Wert:
  - **Wert** — der numerische Messwert des Datenpunkts. Boolesche Messwerte zählen als `0` oder `1`.
  - **Latenz** — wie lange der Lesevorgang gedauert hat, in Millisekunden. Nützlich, um langsame oder sich verschlechternde Verbindungen zu erkennen.

`Anzahl` benötigt kein Feld — sie zählt die Anzahl der Messwerte in jedem Intervall. `Neuester` gibt den Wert des Messvorgangs mit dem größten Zeitstempel im Intervall zurück — nützlich, wenn Sie den aktuellsten Messwert statt eines Aggregats wie Durchschnitt oder Maximum benötigen.

Um die Aggregation festzulegen, beginnen Sie, einen Funktionsnamen einzugeben. Geben Sie die Funktion gefolgt von `(` ein, um ein Feld zu wählen — zum Beispiel `avg(` und dann **Wert** oder **Latenz**. Das Ergebnis wird als Chip wie `avg(value)` oder `max(latency)` angezeigt.

Wählen Sie erneut, um eine weitere hinzuzufügen; jede erscheint als eigener Chip, und das × eines Chips entfernt ihn — genauso, wie das WHERE-Feld Datenpunkte aufnimmt und wieder freigibt. Vier ist die Grenze, denn so viele kann eine einzelne Anfrage tragen; eine fünfte Aggregation gehört in eine zweite Abfrage.

> **TIP**
>
> Nur erfolgreiche Lesevorgänge werden einbezogen. Ein Messwert wird nur gezählt, wenn die Quelle einen guten Status gemeldet hat (OPC-UA-Status *Good*, S7-Lesestatus *OK*). Fehlgeschlagene oder veraltete Lesevorgänge werden ausgeschlossen, sodass die Aggregate nur fehlerfreie Daten widerspiegeln.

WHERE — Datenpunkte und Tags

Das Feld WHERE wählt aus, welche Datenpunkte in die Abfrage einfließen.

Beginnen Sie, den Namen einer Datenquelle einzugeben, um sie zu finden, und wählen Sie dann einen ihrer Datenpunkte — einen OPC-UA-Knoten, eine S7-Adresse, eine Prometheus-Zeitreihe oder einen Heartbeat. Mit `*` beziehen Sie alles ein, was diese Quelle misst. Ausgewählte Datenpunkte werden als Chips angezeigt; entfernen Sie einen Datenpunkt über das × oder mit der Rücktaste.

Sie können Datenpunkte aus mehreren Quellen beliebiger Art kombinieren. Sie werden gemeinsam abgefragt und zu einem Ergebnis zusammengeführt.

> **Was `*` auslässt**
>
> `*` erfasst, was eine Quelle misst, nicht ihre Zustandssignale. Die Erreichbarkeit der Quelle selbst und jeder OPC-UA-Knoten, der auf sein Vorhandensein statt auf seinen Wert überwacht wird, bleiben außen vor — beide melden einen konstanten Wert, und ein Durchschnitt neben einer Temperatur würde dadurch verflacht. Wählen Sie eines von beiden namentlich aus, um es einzeln darzustellen.

Sie können auch nach **Monitor-Tags** filtern — den Bezeichnungen, die Sie Ihren Monitoren zuweisen. Tags erscheinen im selben Dropdown, nach Kategorie geordnet. Wählen Sie einen oder mehrere Tags aus, um die Abfrage auf Daten von Monitoren zu beschränken, die diese Tags tragen. Tag-Chips zeigen die Tag-Farbe und den Namen neben den ausgewählten Datenpunkt-Chips an. Entfernen Sie einen Tag-Chip über das × oder mit der Rücktaste. Eine Abfrage kann auch ausschließlich Tags verwenden, ohne bestimmte Datenpunkte auszuwählen.

> **WARNING**
>
> Für jede Abfrage der Seite ist mindestens ein Datenpunkt oder Tag erforderlich. Eine Abfrage mit leerem WHERE-Feld wird nicht ausgeführt, und der Fehler wird an der betreffenden Zeile angezeigt.

GROUP BY — Aufteilung in Datenreihen

Standardmäßig werden alle von einer Abfrage ausgewählten Datenpunkte zu einer einzigen Datenreihe zusammengefasst. GROUP BY teilt diese Reihe in mehrere auf:

- **Monitor** — eine Datenreihe pro Bedingungsmonitor, der die ausgewählten Datenpunkte liest.
- **Datenpunkt** — eine Datenreihe pro Datenpunkt.
- **Datenquelle** — eine Datenreihe pro Datenquelle.

Sie können sie kombinieren. `avg(value)` gruppiert nach **Datenpunkt** erzeugt eine Linie pro Datenpunkt — der schnellste Weg, Messwerte miteinander zu vergleichen. Ergänzen Sie **Monitor**, um jeden Datenpunkt nach dem überwachenden Monitor aufzuschlüsseln; ein Datenpunkt, den zwei Monitore lesen, erscheint dann unter jedem einmal.

Zeitraum und Granularität

Öffnen Sie das **Uhrsymbol** in der Kopfzeile des Bereichs, um Folgendes festzulegen:

- **Zeitraum** — ein Schnellbereich (letzte 15 Minuten bis letzte 30 Tage) oder ein benutzerdefinierter Start- und Endzeitpunkt.
- **Granularität** — die Größe der einzelnen Zeitintervalle (10 Sekunden bis 1 Woche). Belassen Sie die Einstellung auf **Automatisch**, damit Pulse ein passendes Intervall für den gewählten Zeitraum wählt. Wird die Granularität nicht ausdrücklich festgelegt, fasst Pulse die Daten stündlich zusammen.

Eine feinere Granularität liefert mehr Details, aber auch mehr Punkte; eine gröbere Granularität glättet die Daten und ist über lange Zeiträume schneller.

Mit einem früheren Zeitraum vergleichen

Öffnen Sie das **Uhrsymbol** in der Kopfzeile des Bereichs und scrollen Sie zum Abschnitt **Mit vorherigem Zeitraum vergleichen**. Wählen Sie einen Abstand — wie weit der zweite Zeitraum zurückliegt — und die Seite ruft sowohl das aktuelle Fenster als auch das gleichlange, um diesen Abstand zurückversetzte Fenster ab und stellt sie gemeinsam dar.

Die verfügbaren Abstände hängen vom gewählten Zeitraum ab: Es werden nur Abstände angeboten, die mindestens so lang wie das Fenster sind, damit sich die beiden Zeiträume nicht überschneiden. Bei einem 7-Tage-Fenster stehen beispielsweise „Vorherige 7 Tage" und „Vorherige 28 Tage" zur Auswahl, nicht aber „Vorherige Stunde".

Zum Deaktivieren des Vergleichs klicken Sie im selben Abschnitt auf **Aus**.

Überlagerung und nebeneinander

Während der Vergleich aktiv ist, erscheint unterhalb der Abstände ein Schalter **Als Überlagerung anzeigen**:

- **Aus (Standard)** — jedes Diagramm teilt sich in zwei Bereiche auf, einen pro Zeitraum, jeder mit eigener Zeitachse. Beim Ablesen über beide Bereiche hinweg ist Intervall *i* der gleiche Abstand in beiden Zeiträumen.
- **Ein** — beide Zeiträume werden in einem Diagramm auf einer gemeinsamen Zeitachse gezeichnet. Der aktuelle Zeitraum verwendet durchgezogene Linien, der frühere gestrichelte Linien in derselben Farbe. Nützlich für einen schnellen visuellen Vergleich, bei dem die genaue Intervall-Ausrichtung weniger wichtig ist als die Gesamtform.

Diagrammansicht pro Diagramm

Wenn ein Vergleich läuft, zeigt der Kopf jedes Diagramms einen Schalter **Aktuell / Vergleich**. Damit wechseln Sie dieses einzelne Diagramm zwischen dem aktuellen und dem früheren Zeitraum — ohne die Vergleichseinstellungen der gesamten Seite zu ändern.

Wie Abstände angewendet werden

PQL richtet Zeitintervalle an der Epoche aus. Wenn der gewählte Abstand keine ganze Anzahl von Intervallen ergibt — etwa „Vorherige 30 Tage" bei wöchentlicher Granularität — wird er auf die nächste ganze Intervallanzahl gerundet. Die Zeitraumbezeichnungen in den Diagrammen und in der Übersicht zeigen den tatsächlich angewendeten Abstand an, sodass Sie immer wissen, welchen Zeitraum die frühere Periode abdeckt.

Ergebnisse lesen

Nach einem Lauf erscheinen die Diagramme unterhalb des Editors, darunter eine **Übersicht** und eine **Tabelle** in einer Registerkartenleiste. Eine kurze Zusammenfassungszeile zeigt, wie lange die langsamste Abfrage gedauert hat, die Anzahl der zurückgegebenen Zeitintervalle und die tatsächlich angewendete Granularität.

Diagramme

Die Diagramme werden immer angezeigt. Jede Aggregation jeder Abfrage erhält ihr **eigenes Diagramm**, in der Reihenfolge ihrer Definition, sodass unterschiedliche Einheiten und Skalen sich nie eine Achse teilen — eine Abfrage mit `count` und `avg(value)` erzeugt zwei Grafiken. Innerhalb jedes Diagramms wird jede GROUP-BY-Datenreihe als eigene Linie dargestellt.

Jedes Diagramm trägt als Überschrift den Buchstaben oder Namen der Abfrage, ihre Aggregation und eine Zeile, die benennt, was sie liest — wichtig, sobald zwei Diagramme beide mit `avg(value)` überschrieben sind und verschiedene Sensoren meinen.

Wenn Sie den Zeiger irgendwo über den Stapel bewegen, wird in **jedem** Diagramm ein Fadenkreuz zum selben Zeitpunkt gezeichnet, sodass sich ein Moment über alle hinweg ablesen lässt. Alle Diagramme teilen sich den Zeitraum der Seite; wo eine Abfrage zu einem Zeitpunkt keinen Messwert hat, zeigt sie eine Lücke statt einer Linie durch einen nie gelesenen Wert.

Schlägt eine Abfrage fehl oder liefert sie nichts, sagen das nur ihre eigenen Diagramme; die übrigen beantworten weiterhin ihre Fragen.

Die Farben werden durch die Übersichtstabelle darunter erklärt, in der jede Zeile dieselbe Farbe wie ihre Linie trägt.

Wenn eine Abfrage mehr als eine Aggregation liefert, zeichnet das Bewegen des Mauszeigers über die Diagramme ein **gemeinsames Fadenkreuz** — eine senkrechte Linie am selben Zeitintervall in allen Aggregationsdiagrammen gleichzeitig. Dies erleichtert den Vergleich, zum Beispiel von Durchschnitts- und Maximalwerten zum gleichen Zeitpunkt. Das Fadenkreuz folgt dem Mauszeiger überall in der Diagrammspalte, einschließlich in den Lücken zwischen Diagrammen und auf den Achsenbeschriftungen. Ein Werte-Tooltip erscheint nur bei dem Diagramm, über dem sich der Mauszeiger direkt befindet.

Vorfallmarkierungen

Vorfälle, die während des Zeitraums aufgetreten sind, werden in jedem Diagramm an derselben Stelle als vertikale Markierungen dargestellt, eingefärbt nach Status (unbestätigt, bestätigt, behoben). Über die Schaltfläche **Vorfälle** oberhalb der

Diagramme können Sie einzelne Vorfälle ein- oder ausblenden — praktisch, um eine Spitze in einer Abfrage mit einem Einbruch in einer anderen und mit dem folgenden Vorfall in Beziehung zu setzen.

Übersicht

Die Registerkarte **Übersicht** fasst den gesamten Zeitraum zusammen, mit einem Block je **Abfrage** — nicht je Diagramm — unter ihrem Buchstaben oder Namen und darin **einer Zeile pro Gruppe**. Die Aggregationen einer Abfrage sind hier Spalten, wo sie oben getrennte Bilder sind. Wenn Sie nach Monitor, Datenpunkt oder Datenquelle gruppieren, erscheinen auch diese als Spalten, und ein farbiger Punkt in jeder Zeile entspricht der Linie dieser Gruppe in den Diagrammen.

Eine Abfrage ohne GROUP BY hat eine einzige Zeile, die alles Ausgewählte abdeckt; statt einer Gruppenspalte trägt sie deshalb eine Spalte **Liest**, die ihren Gegenstand benennt.

Diese Summen werden über **alle** Messwerte im Zeitraum berechnet — `avg(value)` ist also der echte Durchschnitt über den Zeitraum, Perzentile sind exakt und `count` ist die Gesamtzahl — und nicht eine Kombination der Werte pro Intervall.

Wenn ein Vergleich aktiv ist, erhält jede Aggregationsspalte zwei weitere: **Vorher**, denselben Aggregatwert für den früheren Zeitraum, und **Δ**, die prozentuale Änderung vom früheren zum aktuellen Wert — positiv in Grün, negativ in Amber. Ein Gedankenstrich bedeutet, dass kein früherer Messwert vorhanden ist oder der frühere Wert null war.

Eingrenzen aus der Übersicht

Jede Zeile der Übersicht trägt rechts eine ⋯-Schaltfläche (oder kann per Rechtsklick geöffnet werden). Das Menü bietet je nach Gruppierung der Zeile folgende Aktionen:

- **Auf diesen Datenpunkt eingrenzen** — schreibt das WHERE der Abfrage auf diesen einzelnen Datenpunkt um und führt sie sofort erneut aus. Verfügbar, wenn die Abfrage nach Datenpunkt oder Datenquelle gruppiert ist.
- **Auf diesen Monitor eingrenzen** — schreibt das WHERE der Abfrage auf diesen einzelnen Monitor um und führt sie sofort erneut aus. Verfügbar, wenn die Abfrage nach Monitor gruppiert ist.

Eine Aktion ist **deaktiviert**, wenn die Abfrage bereits auf dieses Element eingegrenzt ist — die Seite zeigt bereits die engere Antwort, ein erneutes Drücken würde nichts ändern.

Wenn eine Abfrage auf einen Monitor eingegrenzt ist, zeigt das WHERE-Feld einen Chip mit dem Monitornamen neben den Datenpunkt- und Schlagwort-Chips. Entfernen Sie ihn mit dem × am Chip, um den Gegenstand wieder zu erweitern.

Tabelle

Die Registerkarte **Tabelle** zeigt die zeitliche Aufschlüsselung — eine Zeile pro Zeitintervall und Gruppe. Die Spalten sind sortierbar. Verwenden Sie die Tabelle, wenn Sie die exakten Werte pro Intervall statt eines Trends oder einer Gesamtsumme benötigen. Bei mehr als einer Abfrage auf der Seite wählen Sie über die Auswahl oberhalb der Tabelle, welche sie zeigt.

Vorgeschlagene Abfragen

Unterhalb des Editors bietet **Vorgeschlagene Abfragen** fertige Ausgangspunkte für häufige Fragestellungen, etwa Durchschnittswert pro Datenpunkt, Spitzenwerte, Abruf-Latenz, die langsamsten Datenquellen und das Stichprobenvolumen pro Datenquelle.

Wenn Sie einen Vorschlag auswählen, werden SELECT, GROUP BY, Granularität und Zeitraum für Sie ausgefüllt, während die bereits gewählten Datenpunkte erhalten bleiben. Ein Vorschlag, der mehr als eine Frage stellt — etwa der Betriebsbereich, der sowohl Minimum als auch Maximum will — wird zu einer Abfrage je Frage, alle auf denselben Datenpunkten. Falls Sie noch keinen Datenpunkt ausgewählt haben, wählen Sie zuerst einen im WHERE-Feld und führen Sie dann den Vorschlag aus.

Die Vorschläge verschwinden, sobald Sie eine Abfrage ausführen, und kehren zurück, wenn Sie auf **Abbrechen** klicken.

Auf mobilen Geräten wird der Bereich durch eine Schaltfläche **Vorgeschlagene Abfragen** ersetzt. Tippen Sie darauf, um ein Einschubfeld von unten zu öffnen, das alle Vorschläge mit Namen und Beschreibung auflistet. Tippen Sie auf einen Vorschlag, um ihn sofort auszuführen.

Verwandte Dokumentation

- Monitore — die Bedingungsmonitore, die auf den hier abgefragten Messwerten alarmieren.
- OPC UA, Siemens S7 und Heartbeat — wie die zugrunde liegenden Daten erfasst werden.
- KI-Canvas — bitten Sie den Assistenten, Abfragen in Ihrem Auftrag zu erstellen und auszuführen.

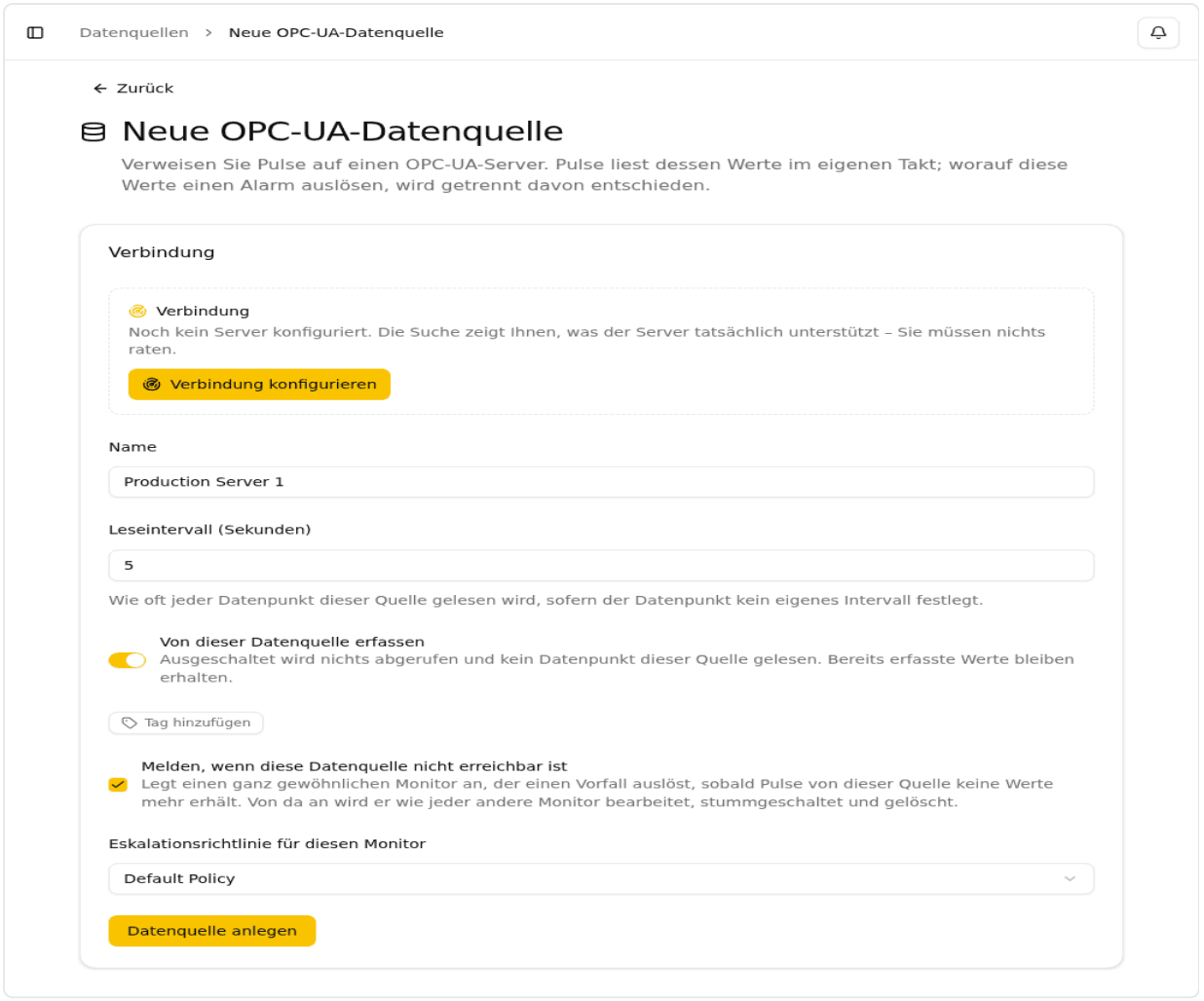
Teil 4 · Monitortypen

4.1 OPC UA

OPC UA (Open Platform Communications Unified Architecture) ist ein industrielles Kommunikationsprotokoll für sicheren, zuverlässigen Datenaustausch. Pulse bindet einen OPC-UA-Server als **Datenquelle** ein und liest dessen Werte.

OPC-UA-Datenquelle anlegen

Eine Datenquelle bündelt alles zu einer Serververbindung an einer Stelle: die Adresse, die Absicherung des Kanals, die Authentifizierung und das Leseintervall.



1. Navigieren Sie im Seitenbereich zu **Datenquellen → OPC UA** — dort sind alle OPC-UA-Server aufgeführt, die Pulse liest — und klicken Sie auf **Neue Datenquelle**
2. Wählen Sie **OPC UA**
3. Konfigurieren Sie die Datenquelle:

Feld	Beschreibung	Beispiel
Name	Ein beschreibender Name für die Datenquelle	`Produktionsserver 1`
Verbindung	Endpunkt-URL, Sicherheitsmodus und -richtlinie, Authentifizierung und das gepinnte Serverzertifikat — gemeinsam konfiguriert	`opc.tcp://192.168.1.100:4840`
Leseintervall (Sekunden)	Wie oft jeder Datenpunkt dieser Quelle gelesen wird	`10`
Von dieser Datenquelle erfassen	Ausgeschaltet wird nichts abgefragt, ohne dass Sie die Quelle löschen müssen	
Tags	Datenquelle kategorisieren; jeder Datenpunkt erbt ihre Tags	
Melden, wenn diese Datenquelle nicht erreichbar ist	Legt zusammen mit der Quelle einen Monitor an (siehe unten)	

Klicken Sie auf **Verbindung konfigurieren**, um den Verbindungsdialog zu öffnen. Dort werden Endpunkt-URL, Sicherheitsmodus, Sicherheitsrichtlinie, Authentifizierung und das gepinnte Serverzertifikat gemeinsam festgelegt. Das Formular zeigt anschließend eine Zusammenfassung; über **Bearbeiten** öffnen Sie den Dialog erneut.

Anlegen über die Geräteerkennung

Wenn Sie über die Geräteerkennung hierher gelangen, indem Sie bei einem gefundenen Gerät auf **Hinzufügen** klicken, sind **Name** und Endpunkt-URL bereits aus den Scan-Ergebnissen vorausgefüllt. Prüfen Sie die Angaben und fahren Sie mit den übrigen Feldern fort.

Sicherheitseinstellungen

Sicherheitsmodus, Sicherheitsrichtlinie, Authentifizierung, Endpunkt-Erkennung und die beiden an der Verbindung beteiligten Zertifikate werden ausführlich in OPC-UA-Sicherheit erklärt. Kurz gefasst: Verwenden Sie im Produktivbetrieb **Signieren & Verschlüsseln** mit **Basic256Sha256** oder stärker, und lassen Sie **Endpunkte erkennen** die stärkste Konfiguration Ihres Servers vorauswählen.

NETZWERKANFORDERUNGEN

Stellen Sie sicher, dass Ihre Firewall TCP-Verbindungen auf dem OPC-UA-Port (Standard: 4840) zwischen dem Pulse-Server und Ihren OPC-UA-Servern erlaubt.

Alarm bei nicht erreichbarem Server

Melden, wenn diese Datenquelle nicht erreichbar ist ist beim Anlegen einer Datenquelle vorausgewählt. Damit entsteht ein Bedingungsmonitor, der nach der Quelle benannt ist — *Produktionsserver 1 nicht erreichbar* — und einen Vorfall auslöst, sobald Pulse keine Werte mehr von ihr erhält. Die zu verwendende Eskalationsrichtlinie wählen Sie im Feld unter dem Kontrollkästchen.

Von da an ist es ein ganz gewöhnlicher Monitor: Sie benennen ihn um, schalten ihn stumm, ändern seine Eskalationsrichtlinie, bearbeiten seine Bedingung oder löschen ihn — alles in der Monitorliste. Entfernen Sie den Haken, wenn für diesen Server niemand alarmiert werden soll.

Datenpunkte hinzufügen

Die einzelnen Werte eines Servers sind **Datenpunkte** der Datenquelle. Die Detailseite der Datenquelle listet jeden Datenpunkt auf, den Pulse liest — mit Knoten-ID, letztem Wert, Zeitpunkt der letzten Messung und Qualität der Messung. Lange Adressen werden in der Tabelle abgeschnitten; klicken Sie auf eine Adresse, um sie vollständig in einem Popover anzuzeigen — mit einer Schaltfläche zum Kopieren in die Zwischenablage, etwa für ein SPS-Projekt oder einen OPC-UA-Client.

Um einen neuen Datenpunkt zu deklarieren, öffnen Sie die Detailseite der Datenquelle und wählen Sie über der Tabelle **Datenpunkte** die Aktion **Datenpunkt hinzufügen**. Der Dialog (auf Mobilgeräten ein Drawer) bietet zwei Registerkarten:

- **Durchsuchen** — verbindet sich mit dem OPC-UA-Server und ermöglicht das Navigieren durch seine Knoten. Setzen Sie einen oder mehrere Haken und tippen Sie auf **Hinzufügen**. Bereits auf dieser Quelle deklarierte Knoten werden markiert und übersprungen.
- **Manuell eingeben** — geben Sie die OPC-UA-Kennung des Knotens direkt ein, z. B. `ns=2;s=Temperature` oder `ns=2;i=1001`.

Der Datentyp des Datenpunkts wird mit der ersten Messung festgelegt. Pulse beginnt beim nächsten Abruf der Quelle mit dem Lesen des neuen Knotens.

Durchsuchen auf dem Smartphone

Auf dem Smartphone zeigt die Registerkarte **Durchsuchen** immer eine Ebene des Knotenbaums. Tippen Sie auf einen Ordner, um ihn zu öffnen; der Pfad zurück zur Wurzel ist im Breadcrumb über der Liste stets sichtbar. Werte lassen sich auf jeder Tiefenebene auswählen — die Auswahl bleibt erhalten, wenn Sie zwischen Ordnern wechseln.

Jede Ebene hat ein Filterfeld, das Namen und Knoten-IDs der sichtbaren Ebene durchsucht. Zwei Umschalter grenzen die Liste weiter ein: **Nur Werte** blendet Ordner aus, sodass nur auswählbare Knoten erscheinen, und **Bereits vorhandene ausblenden** verbirgt Knoten, die bereits auf dieser Quelle deklariert sind.

Die Fußleiste zeigt an, wie viele Knoten ausgewählt sind, sowie einen Link **Auswahl aufheben**. Beim Tippen auf **Hinzufügen** zählt eine Fortschrittsanzeige jede einzelne Anfrage ab („*X von Y*") mit einer **Abbrechen**-Schaltfläche, die die Schleife nach der laufenden Anfrage stoppt — die noch nicht verarbeiteten ausgewählten Knoten bleiben für einen erneuten Versuch markiert.

Datenpunkte suchen

Wenn eine Datenquelle viele Datenpunkte hat, finden Sie einen bestimmten Knoten mit dem Suchfeld über der Tabelle — nach Name, Adresse oder Beschreibung. Die Suche läuft serverseitig und erreicht alle Datenpunkte der Quelle, nicht nur die aktuelle Seite. Der Suchbegriff wird in der URL gespeichert, sodass ein geteilter oder gespeicherter Link direkt zur gefilterten Ansicht führt.

Auf einen Wert alarmieren

Um auf einen Datenpunkt zu alarmieren, erstellen Sie eine Bedingung und hängen einen Bedingungsmonitor daran. Eine Bedingung vergleicht Messwerte mit Schwellwerten, aggregiert sie über ein Zeitfenster und kann mehrere davon verknüpfen — auch einen Messwert und die Erreichbarkeit seiner Datenquelle in einer Regel. Ein gezogenes Kabel löst dann den einen Vorfall aus, der genau das sagt, statt einen pro Wert, der darüber gelesen wird.

Die Detailseite der Datenquelle zeigt einen Abschnitt **Monitore** mit allen Bedingungsmonitoren, die auf einen Datenpunkt dieser Datenquelle alarmieren. Klicken Sie auf einen Monitor, um seine Detailseite zu öffnen. Eine Datenquelle ohne Monitore alarmiert auf nichts; der Abschnitt sagt das ausdrücklich — eine nützliche Erinnerung daran, dass Messwerte erfasst werden, aber niemand alarmiert wird, wenn sie aus dem Ruder laufen.

Jede Zeile in der Datenpunkttabelle zeigt außerdem, welche Monitore auf genau diesen Knoten alarmieren. Ein einzelner Monitor erscheint als Schaltfläche, die ihn direkt öffnet; alarmieren zwei oder mehr Monitore auf denselben Knoten, zeigt die Schaltfläche die Anzahl und öffnet eine Auswahl mit den Namen.

Jede Zeile hat außerdem die Aktion **In Abfrage öffnen** im Kontextmenü (Rechtsklick oder die Schaltfläche ⋮), die Sie zur Seite Abfrage führt, die auf diesen Datenpunkt voreingestellt ist, damit Sie dessen Messverlauf erkunden können, ohne die Abfrage von Grund auf aufzubauen.

Datenpunkte bauen nur dann einen Verlauf auf, wenn Sie sie aufbewahren. Verwenden Sie **Aufbewahren** auf der Detailseite der Datenquelle für die Werte, die Sie langfristig auswerten wollen; die übrigen bleiben 24 Stunden lang lesbar.

OPC-UA-Alarme & Bedingungen

OPC-UA-Alarme & Bedingungen (A&C) ist ein Standardmechanismus, mit dem Server Ereignis- und Alarmbenachrichtigungen an Clients senden. Wenn eine OPC-UA-Datenquelle eine A&C-Ereignisbenachrichtigung empfängt, erstellt Pulse automatisch einen Vorfall.

Jeder aus einem A&C-Ereignis erstellte Vorfall:

- Verwendet die Alarmmeldung vom OPC-UA-Server als Vorfallstitel
- Zeigt dieselbe Alarmmeldung in der Vorfalldetailansicht als Beschreibung an, sodass der vollständige Alarmtext stets in Benachrichtigungen und Vorfalldetails sichtbar ist

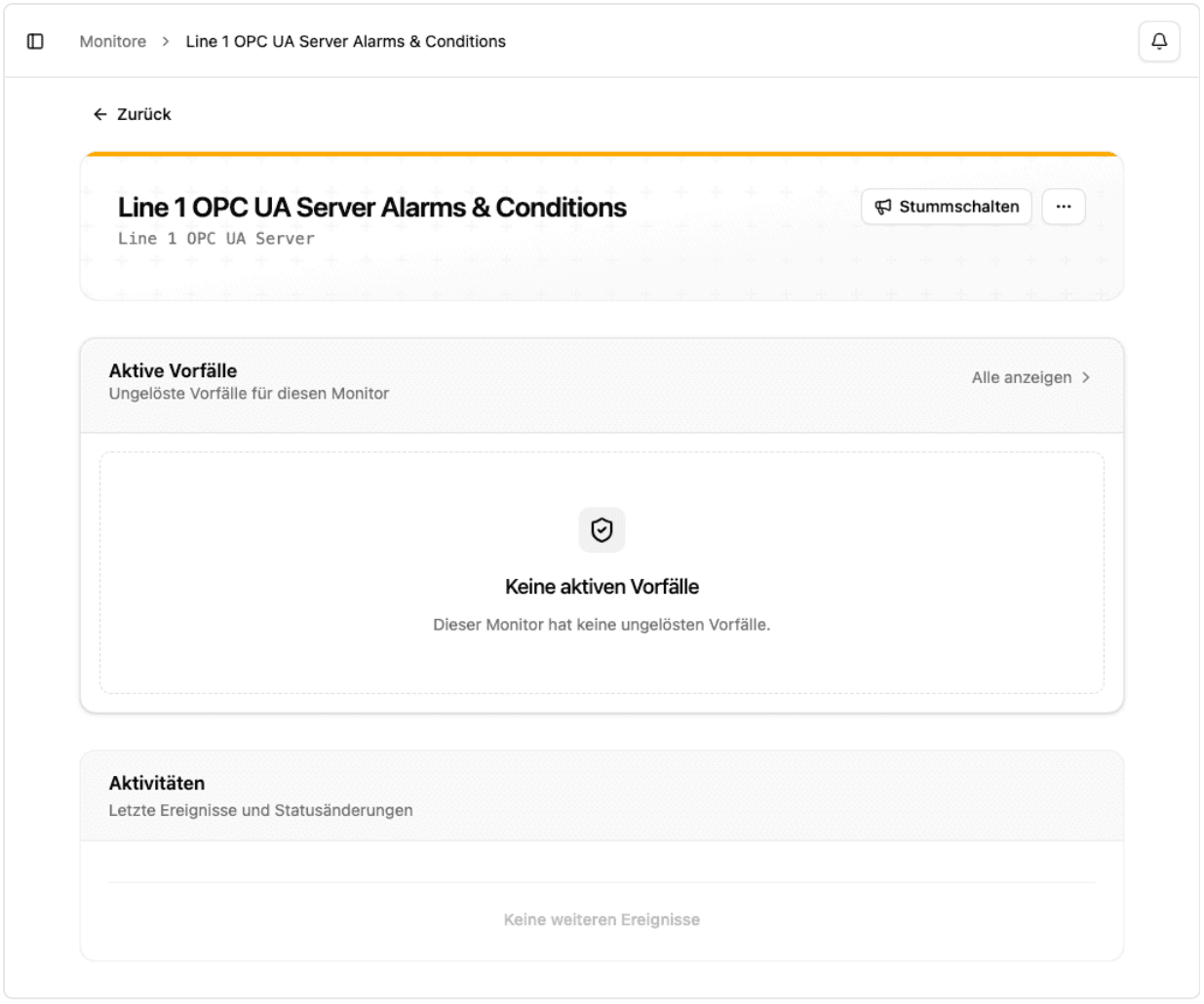
Vorfälle aus A&C-Ereignissen werden dedupliziert: Wenn dieselbe Bedingung mehrfach ausgelöst wird, wird pro Bedingung nur ein offener Vorfall erstellt.

Alarms & Conditions ist ein Schalter auf der Bearbeitungsseite der Datenquelle, bei einer neuen Quelle standardmäßig eingeschaltet. Ausgeschaltet unterhält Pulse für diesen Server kein A&C-Abonnement und zeichnet keine seiner Ereignisse auf — Datenpunkte werden weiterhin wie bisher gelesen, denn Erfassung und Alarmierung sind voneinander unabhängig. Schalten Sie ihn wieder ein, abonniert Pulse erneut und gleicht über den OPC-UA-Mechanismus `ConditionRefresh` jede noch auf dem Server aktive Bedingung ab, sodass Alarme, die während der Abschaltung ausgelöst wurden, beim nächsten Abgleich erfasst werden.

Der Alarms-&-Conditions-Monitor

Beim ersten Einschalten des A&C-Schalters einer Quelle legt Pulse dafür einen eigenen Monitor an, benannt *<Quelle> Alarms & Conditions*. Jeder Alarmvorfall dieser Quelle wird gegen diesen Monitor erstellt — niemals gegen den Monitor für die Nichterreichbarkeit

der Quelle, sodass ein hängender Ventilalarm und ein gekapptes Netzwerkkabel stets zwei getrennte Probleme an zwei getrennten Stellen bleiben. Ein Badge auf der Detailseite der Datenquelle verlinkt direkt dorthin.



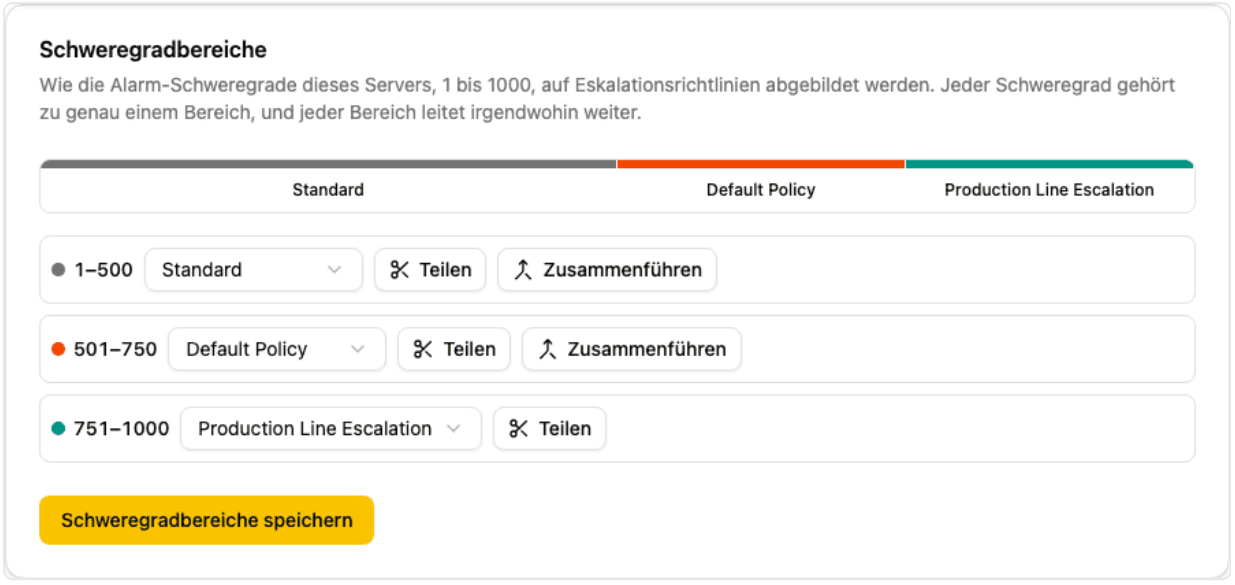
Der Monitor ist **Fehlerhaft**, solange ein Alarm der Quelle aktiv ist, und wird **Gesund**, sobald der letzte Alarm behoben ist. Ansonsten verhält er sich wie jeder andere Monitor: Sie können ihn stummschalten, taggen, und er hat seine eigene Eskalationsrichtlinie — welche Richtlinie tatsächlich greift, entscheidet jedoch pro Alarm der Schweregrad weiter unten, nicht allein diese eine Einstellung.

Das Ausschalten von A&C, das Deaktivieren der Quelle oder ihr Löschen löscht diesen Monitor nie — er wird **deaktiviert**, sodass seine Konfiguration, Tags und Vorfallshistorie einen Ein-Aus-Zyklus überstehen. Wird A&C wieder eingeschaltet, reaktiviert Pulse denselben Monitor, statt einen neuen anzulegen. Eine direkte Folge davon, dass der Schalter unabhängig vom Abonnement ist: **Ein Alarmvorfall, der beim Ausschalten von A&C noch offen ist, bleibt offen.** Niemand überwacht den Server mehr, um ihn zu schließen, also lässt er sich bis zum nächsten `ConditionRefresh` — beim erneuten Einschalten — nur von Hand schließen; dieser Abgleich teilt Pulse dann mit, welche zugrunde liegenden Bedingungen bereits erloschen sind, während niemand zuhörte.

Weiterleitung nach Schweregrad

Jeder OPC-UA-Alarm trägt einen **Schweregrad** von 1 bis 1000, und die **Schweregradbereiche** einer Quelle entscheiden, welche Eskalationsrichtlinie ein Alarm mit diesem Schweregrad verwendet. Die Bereiche bilden eine strikte Partition des gesamten Bereichs 1–1000: Jeder Schweregrad gehört zu genau einem Bereich, und jeder Bereich leitet irgendwohin weiter — entweder an eine von Ihnen gewählte Richtlinie oder an **Standard**, was an die eigene Eskalationsrichtlinie des A&C-Monitors verweist.

Bearbeiten Sie die Bereiche im Panel **Schweregradbereiche** auf der Bearbeitungsseite der Datenquelle, das nur aktiv ist, während Alarms & Conditions eingeschaltet ist:



Der Balken ist das Steuerelement. Ziehen Sie den Griff zwischen zwei Bereichen, um ihre gemeinsame Grenze zu verschieben (oder verwenden Sie die Pfeiltasten, sobald der Griff den Fokus hat). Tippen oder klicken Sie auf einen Bereich, um sein Panel zu öffnen:

- **Richtlinienauswahl** — weist dem Bereich eine Eskalationsrichtlinie zu, oder **Standard**
- **Untere und obere Grenze** — der genaue Schwereradbereich als editierbare Zahl; wird beim Verlassen des Felds oder mit Eingabe übernommen und geklemmt, sodass jeder Bereich mindestens einen Schweregrad breit bleibt
- **Teilen** — teilt den Bereich in zwei gleich große Hälften, die beide die ursprüngliche Richtlinie übernehmen
- **Mit [benachbartem Bereich] zusammenführen** — vereint den Bereich mit dem darauffolgenden und behält die Richtlinie dieses Bereichs

Jede Operation hält den Bereich konstruktionsbedingt lückenlos und überlappungsfrei, sodass es keinen ungültigen Zustand zum Speichern gibt.

Schweregrad entscheidet nur über die Weiterleitung, nie über den Zustand

Ein Bereich wählt, welche Eskalationsrichtlinie der Vorfall eines Alarms verwendet. Er ändert nicht, ob der Monitor Gesund oder Fehlerhaft ist — **jeder** aktive Alarm macht den A&C-Monitor Fehlerhaft, unabhängig von seinem Schweregrad. Eine Quelle mit nur niedrig priorisierten offenen Meldungen ist genauso fehlerhaft wie eine mit einem einzigen kritischen Alarm.

Die Richtlinie wird beim ersten Auslösen des Alarms festgelegt

Die Eskalationsrichtlinie eines Alarms wird einmalig festgelegt — aus dem Bereich, in den sein Schweregrad im Moment des Auslösens fiel — und bleibt für die gesamte Lebensdauer dieses Vorfalls fest. Meldet der Server dieselbe Bedingung später mit höherem Schweregrad — steigt er etwa von 300 auf 900 —, eskaliert der Vorfall weiterhin über die Richtlinie, die der Bereich bei 300 vorgab; er wechselt nicht in den Bereich bei 900. Das ist beabsichtigt, kein Fehler: Einen laufenden Vorfall mitten in der Eskalation umzuleiten, ist derzeit nicht vorgesehen.

Anwendungsinstanz-Zertifikat

Um einen sicheren Kanal zu öffnen (**Signieren** oder **Signieren & Verschlüsseln**), präsentiert Pulse ein **Anwendungsinstanz-Zertifikat** — eine selbstsignierte X.509-Identität, eine pro Organisation, die von allen OPC-UA-Datenquellen gemeinsam genutzt wird. Jeder OPC-UA-Server muss diesem Zertifikat **vertrauen**, bevor er eine sichere Verbindung akzeptiert.

Die Verwaltung des Zertifikats — Herunterladen, Hinterlegen auf Ihren Servern und Widerrufen bei Kompromittierung — wird in OPC-UA-Sicherheit — Anwendungsinstanz-Zertifikat beschrieben.

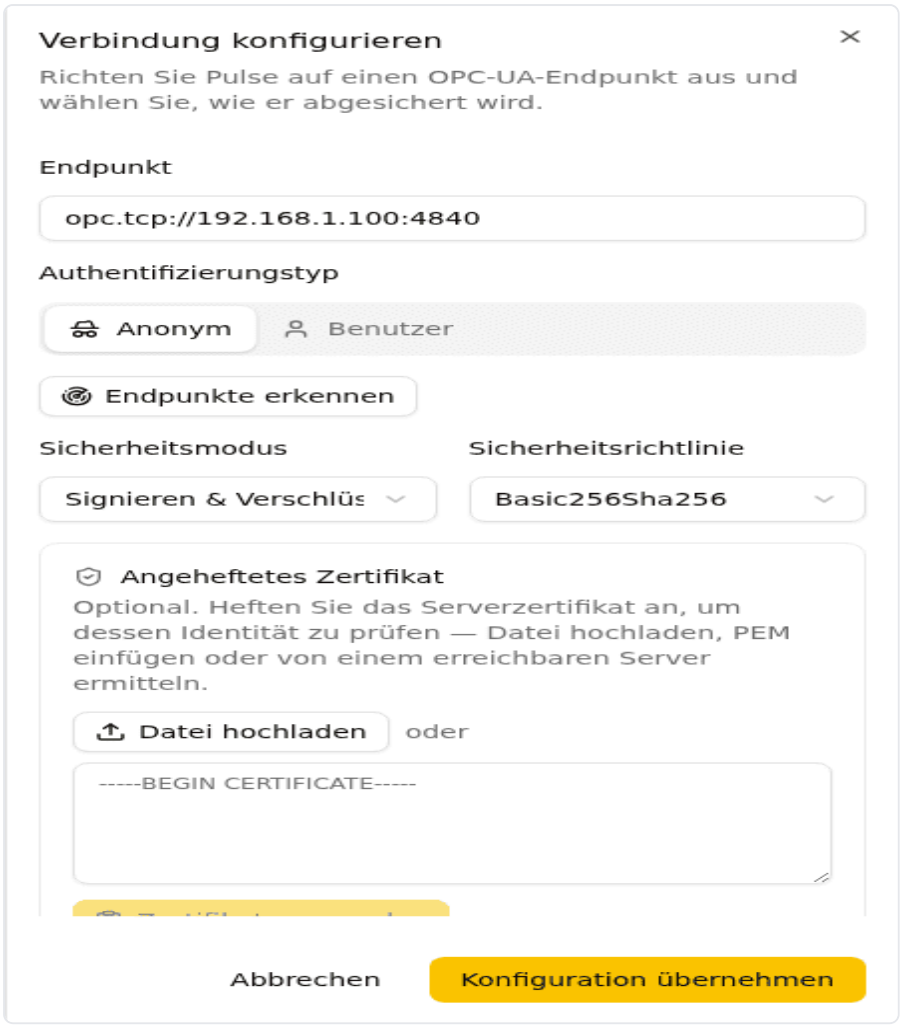
Rotation — ein ablaufendes Zertifikat ersetzen

Da ein Ersatzzertifikat eine neue Identität ist, rotiert Pulse mit einem **Überlappungsfenster**: Ein Ersatz wird vorab erstellt, Sie vertrauen ihm auf jedem Server, während die Überwachung über das alte Zertifikat weiterläuft, und schließen die Rotation dann ab. Der vollständige Ablauf ist in OPC-UA-Sicherheit — Rotation beschrieben.

Teil 4 · Monitortypen

4.2 OPC-UA-Sicherheit

Jede OPC-UA-Datenquelle legt fest, wie ihre Verbindung zum Server abgesichert wird. Diese Seite erklärt die Bausteine dieser Entscheidung: den **Sicherheitsmodus** und die **Sicherheitsrichtlinie**, die Nachrichten auf dem Übertragungsweg schützen, die **zwei beteiligten Zertifikate** — die Identität von Pulse und die des Servers — sowie die **Authentifizierung** der Sitzung.



So funktioniert eine sichere Verbindung

Eine OPC-UA-Verbindung wird auf zwei Ebenen abgesichert:

1. **Sicherer Kanal** — die Transportebene. Pulse und der Server tauschen X.509-Zertifikate aus und signieren und/oder verschlüsseln je nach Sicherheitsmodus jede Nachricht. Pulse präsentiert sein Anwendungsinstanz-Zertifikat; der Server präsentiert sein eigenes Zertifikat, das Pulse anheften kann.

2. **Sitzung** — innerhalb des Kanals authentifiziert sich Pulse als Benutzer: anonym oder mit Benutzername und Passwort. Siehe Authentifizierung.

Daraus folgen zwei praktische Konsequenzen:

- Für **Signieren** oder **Signieren & Verschlüsseln** muss der Server dem **Zertifikat von Pulse vertrauen**, bevor eine Verbindung zustande kommt.
- Verschlüsselung allein prüft nicht, **mit wem** Sie sprechen. Das leistet nur das Anheften des Serverzertifikats.

Sicherheitsmodus

Der Sicherheitsmodus bestimmt, was der sichere Kanal mit jeder Nachricht tut:

Modus	Wirkung	Einsatz
Keiner	Nachrichten werden im Klartext gesendet; keine Zertifikate werden getauscht.	Nur in isolierten Netzen mit vertrauenswürdigem Übertragungsweg.
Signieren	Nachrichten werden signiert — Manipulation fällt auf, Inhalte bleiben lesbar.	Wenn Integrität zählt, Vertraulichkeit aber nicht.
Signieren & Verschlüsseln	Nachrichten werden signiert und verschlüsselt.	Empfohlen für den Produktivbetrieb.

Modus und Richtlinie sind gekoppelt: Der Modus **Keiner** erzwingt die Richtlinie **Keine** (und umgekehrt); beim Wechsel auf einen sicheren Modus wird **Basic256Sha256** vorausgewählt.

Sicherheitsrichtlinie

Die Sicherheitsrichtlinie ist die Algorithmen-Suite für Signierung und Verschlüsselung:

Richtlinie	Status	Hinweise
None	—	Keine Kryptografie. Nur mit Sicherheitsmodus „Keiner" gültig.
Basic128Rsa15	Veraltet	Alte SHA-1-basierte Suite. Nur für Altserver, die nichts anderes anbieten.

Richtlinie	Status	Hinweise
Basic256	Veraltet	Alte SHA-1-basierte Suite. Nur für Altserver, die nichts anderes anbieten.
Basic256Sha256	Aktueller Standard	Empfohlener Standard — breit unterstützt.
Aes128Sha256RsaOaep	Aktuell	Moderne Alternative zu Basic256Sha256.
Aes256Sha256RsaPss	Aktuell	Stärkste Suite — verwenden Sie sie, wenn der Server sie anbietet.

> **TIP**
>
> Wählen Sie die stärkste Richtlinie, die Ihr Server unterstützt. Die Erkennung nimmt Ihnen das ab: Sie listet nur Kombinationen auf, die der Server tatsächlich anbietet, und wählt die stärkste vor.

Die passende Konfiguration per Erkennung finden

Statt zu raten, was der Server unterstützt, lassen Sie Pulse nachfragen. Klicken Sie bei ausgefüllter `opc.tcp://`-Endpunkt-URL im Verbindungsdialog auf **Endpunkte erkennen**. Pulse fragt den Server ab und zeigt:

- **Sicherheitskonfiguration** — die realen Modus-Richtlinien-Kombinationen des Servers, stärkste zuerst. Die stärkste ist als **Empfohlen** markiert; Kombinationen ohne Signierung oder Verschlüsselung tragen eine Warnung.
- **Serverzertifikat** — Antragsteller, Aussteller, Gültigkeitsdaten und Thumbprint des vom Server präsentierten Zertifikats, mit Hinweisen auf abgelaufene oder bald ablaufende Zertifikate. Bei einer sicheren Konfiguration wird dieses Zertifikat zum Anheften angeboten.

Ist der Server nicht erreichbar, können Sie Sicherheitsmodus und Richtlinie weiterhin manuell wählen — die Erkennung ist eine Erleichterung, keine Voraussetzung.

Die zwei Zertifikate

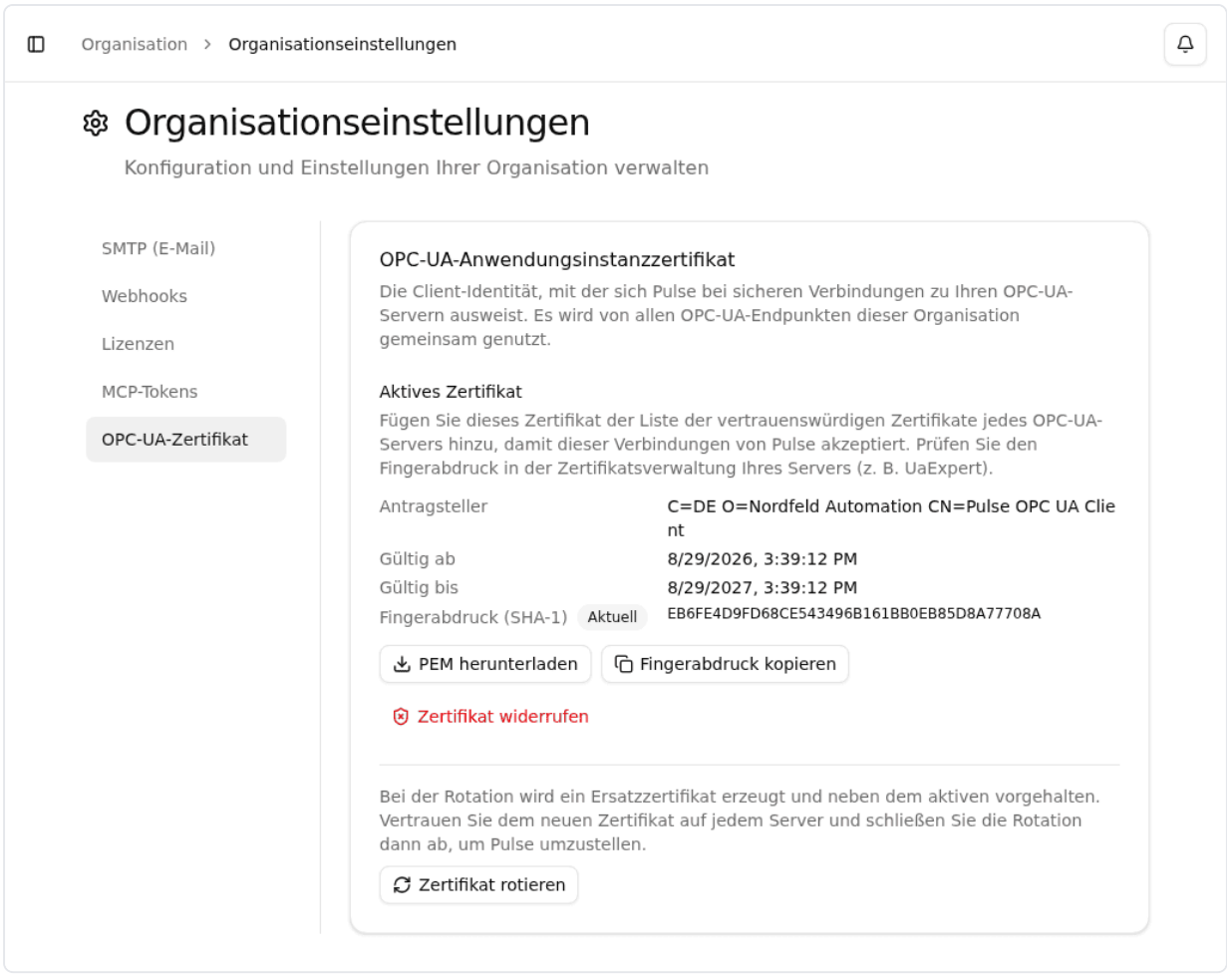
An sicheren OPC-UA-Verbindungen ist je Seite ein Zertifikat beteiligt, und jede Seite muss der anderen vertrauen:

Zertifikat	Wer es präsentiert	Wer ihm vertrauen muss
Anwendungsinstanz-Zertifikat	Pulse	Ihre OPC-UA-Server — sonst lehnen sie die Verbindung ab.
Serverzertifikat	Der Server	Pulse — geprüft nur, wenn Sie es an der Datenquelle anheften.

Anwendungsinstanz-Zertifikat

Um einen sicheren Kanal zu öffnen (**Signieren** oder **Signieren & Verschlüsseln**), präsentiert Pulse ein **Anwendungsinstanz-Zertifikat** — eine selbstsignierte X.509-Identität, eine pro Organisation, die von allen OPC-UA-Datenquellen gemeinsam genutzt wird. Jeder OPC-UA-Server muss diesem Zertifikat **vertrauen**, bevor er eine sichere Verbindung akzeptiert.

Sie verwalten das Zertifikat unter **Organisation → Einstellungen → OPC-UA-Zertifikat**. Pulse stellt es automatisch bereit, sobald eine sichere Verbindung es benötigt — oder Sie klicken vorab auf **Zertifikat erzeugen**, um ihm auf Ihren Servern zu vertrauen, bevor Sie Datenquellen anlegen.



Eigenschaft	Wert
Antragsteller	`Pulse OPC UA Client` (selbstsigniert)
Schlüssel	RSA 2048 Bit, SHA-256-Signatur
Gültigkeit	Ein Jahr; Rotations-Ersatz ca. 14 Monate, damit nach dem Wechsel ein volles Jahr verbleibt
Thumbprint	SHA-1 des Zertifikats, Großbuchstaben-Hex

Auf der Einstellungsseite können Sie das Zertifikat mit **PEM herunterladen** exportieren und mit **Fingerabdruck kopieren** den Thumbprint übernehmen, um ihn mit der Vertrauensliste Ihres Servers abzugleichen.

Das Zertifikat auf Ihren Servern hinterlegen

Die genauen Schritte hängen von Ihrem OPC-UA-Server ab, das Muster ist jedoch immer gleich:

1. Laden Sie das Zertifikat unter **Organisation → Einstellungen → OPC-UA-Zertifikat** herunter.

2. Importieren Sie es in den Speicher der **vertrauenswürdigen Zertifikate** des Servers (in UaExpert und vielen Servern ist dies der Ordner „Trusted" bzw. „PKI").
3. Bestätigen Sie, dass der vom Server angezeigte Thumbprint mit dem in Pulse übereinstimmt.

Solange dem Zertifikat nicht vertraut wird, schlagen sichere Verbindungsaufbauten zu diesem Server fehl.

Rotation — ein ablaufendes Zertifikat ersetzen

Da ein Ersatzzertifikat eine **neue Identität** ist, muss jeder Server, der dem alten Zertifikat vertraut hat, auch dem neuen vertrauen — daher rotiert Pulse mit einem **Überlappungsfenster** statt mit einem harten Wechsel:

1. **Ein Ersatz wird vorab vorbereitet.** Etwa 60 Tage vor Ablauf (oder sofort, wenn Sie **Zertifikat rotieren** klicken) erstellt Pulse ein **ausstehendes** Zertifikat und stellt weiterhin das aktuelle bereit. Die Einstellungsseite zeigt dann beide an, Pulse erzeugt einen Vorfall, und die Administratoren Ihrer Organisation erhalten eine E-Mail.
2. **Sie hinterlegen das neue Zertifikat überall.** Kopieren Sie den Thumbprint des ausstehenden Zertifikats und fügen Sie es dem vertrauenswürdigen Speicher auf jedem OPC-UA-Server hinzu — genau wie beim aktuellen Zertifikat. Die Überwachung läuft währenddessen weiter über das alte Zertifikat.
3. **Sie schließen die Rotation ab.** Sobald jeder Server dem neuen Zertifikat vertraut, klicken Sie auf **Rotation abschließen**. Pulse stuft das ausstehende Zertifikat auf aktiv hoch und entfernt das alte. Neue sichere Kanäle verwenden sofort die neue Identität.

> **WARNING**
>
> Schließen Sie die Rotation erst ab, **nachdem** jeder Server dem neuen Zertifikat vertraut. Ein zu früher Abschluss unterbricht sichere Verbindungen zu jedem Server, der ihm noch nicht vertraut.

Rotation versehentlich gestartet? **Ersatz verwerfen** löscht das ausstehende Zertifikat; das aktive bleibt unverändert.

Läuft ein Zertifikat ab, bevor Sie die Rotation abschließen, stuft Pulse den wartenden Ersatz automatisch hoch — das alte Zertifikat ist zu diesem Zeitpunkt ohnehin unbrauchbar, sodass dies die Überwachung nur wiederherstellen und niemals unterbrechen kann. Damit Verbindungen sich erholen, müssen Sie dem neuen Zertifikat dennoch auf Ihren Servern vertraut haben.

Wenn das Zertifikat kompromittiert ist

Zertifikat widerrufen verwirft das aktive Zertifikat sofort und erzeugt eine neue Identität. Jeder OPC-UA-Server weist Pulse ab, bis Sie dem neuen Zertifikat dort vertrauen — die sichere Überwachung bleibt so lange unterbrochen. Verwenden Sie dies nur bei einem kompromittierten Schlüssel; für einen geplanten Austausch vermeidet die Rotation den Ausfall.

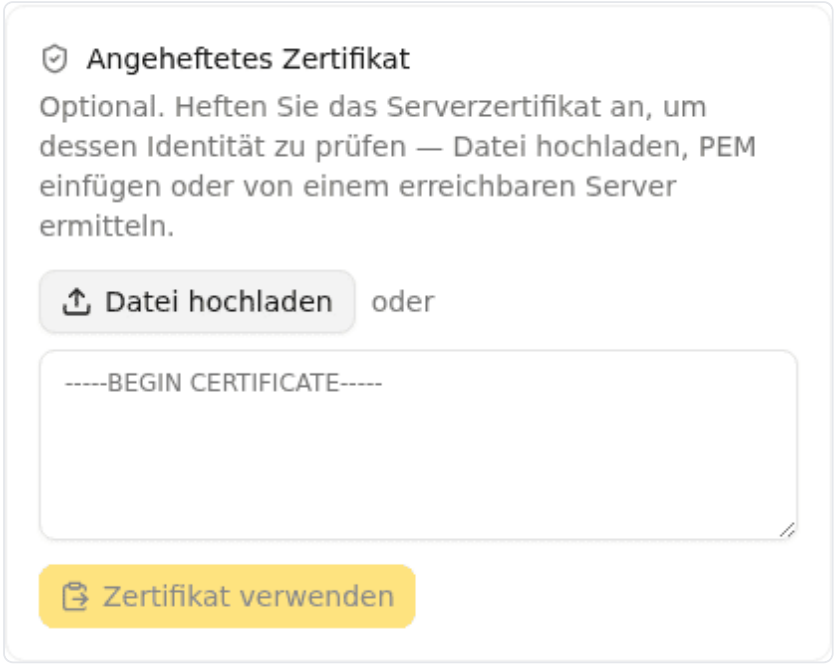
Serverzertifikat anheften

Das Anheften ist der Weg, wie Pulse die Identität des **Servers** prüft — die zweite Hälfte der Vertrauensbeziehung.

Ohne angeheftetes Zertifikat akzeptiert Pulse jedes Zertifikat, das der Server präsentiert. Der Kanal bleibt unter Signieren & Verschlüsseln zwar verschlüsselt — das schützt vor Mitlesen, aber nicht vor Vortäuschung: Alles, was unter dieser Adresse antwortet, könnte die Verbindung entgegennehmen. Mit angeheftetem Zertifikat müssen künftige Verbindungen **genau** dieses Zertifikat vorweisen, sonst schlägt die Verbindung fehl.

Das Anheften ist optional und verfügbar, sobald der Sicherheitsmodus Signieren oder Signieren & Verschlüsseln ist. Es gibt drei Wege:

- **Erkennung** — führen Sie die Erkennung aus; das aktuelle Zertifikat des Servers wird zum Anheften angeboten. Empfohlen, wenn der Server erreichbar ist.
- **Datei hochladen** — laden Sie eine PEM- oder DER-Zertifikatsdatei hoch.
- **PEM einfügen** — fügen Sie den Zertifikatstext ein und klicken Sie auf **Zertifikat verwenden**.



Nach dem Anheften zeigt der Bereich Thumbprint und Gültigkeit des Zertifikats. **Ersetzen** hinterlegt ein anderes Zertifikat; **Lösen** entfernt es (nach einer Bestätigung, da damit der Schutz vor einem Man-in-the-Middle entfällt).

Wenn sich das Serverzertifikat ändert

Führen Sie die Erkennung an einer Datenquelle mit angeheftetem Zertifikat aus, vergleicht Pulse beide und zeigt an, ob das angeheftete Zertifikat mit dem aktuell präsentierten **übereinstimmt** oder davon **abweicht**. Eine Abweichung kann eine legitime Zertifikatsrotation auf dem Server bedeuten — oder einen Man-in-the-Middle. Die Übernahme des neuen Zertifikats ist deshalb immer eine bewusste Aktion: Prüfen Sie, ob die Änderung erwartet ist, und klicken Sie dann auf **Ermitteltes Zertifikat verwenden**.

> **WARNING**
>
> Ändern Sie die Endpunkt-URL, während ein Zertifikat angeheftet ist, gehört das Zertifikat zum vorherigen Server und wird beim Speichern entfernt — eine Warnung im Formular stellt sicher, dass dies nie unbemerkt geschieht. Dasselbe gilt beim Wechsel des Sicherheitsmodus auf „Keiner". Heften Sie das Zertifikat nach der Änderung erneut an.

Anheften und gespeicherte Anmeldedaten

Verwendet eine Datenquelle **Benutzername/Passwort-Authentifizierung** über einen signierten oder verschlüsselten Kanal **ohne** angeheftetes Zertifikat, zeigt das Formular eine Warnung: Die Identität des Servers ist nicht verifiziert, ein Man-in-the-Middle könnte die Anmeldedaten abfangen. Das Anheften des Serverzertifikats schließt diese Lücke — verstehen Sie die Warnung als Aufforderung zum Anheften, nicht als Hintergrundrauschen.

Authentifizierung

Unabhängig von der Transportsicherheit kann der Server verlangen, dass sich Pulse als Benutzer authentifiziert:

- **Anonym** — keine Anmeldedaten; der Server muss anonyme Sitzungen zulassen.
- **Benutzer** — Benutzername und Passwort. Anmeldedaten werden in Pulse als benannte, organisationsweite Einträge gespeichert und pro Datenquelle ausgewählt; Organisations-Administratoren können neue direkt im Verbindungsdialog anlegen.

TIP

Betreiben Sie Verbindungen mit Benutzername/Passwort-Authentifizierung mit **Signieren & Verschlüsseln** und einem angehefteten Serverzertifikat, damit Anmeldedaten weder mitgelesen noch einem Angreifer präsentiert werden können.

Netzwerkanforderungen

Pulse verbindet sich über das binäre `opc.tcp://`-Protokoll — die Endpunkt-URL muss dieses Schema verwenden. Stellen Sie sicher, dass Ihre Firewall TCP-Verbindungen vom Pulse-Server zum Port des OPC-UA-Servers erlaubt (üblicherweise **4840**; Server können jedoch beliebige Ports verwenden — maßgeblich ist der Port aus Ihrer Endpunkt-URL).

Fehlerbehebung

Symptom	Wahrscheinliche Ursache	Lösung
Sichere Verbindung schlägt direkt nach Aktivieren von Signieren / Signieren & Verschlüsseln fehl	Der Server vertraut dem Zertifikat von Pulse noch nicht	Anwendungsinstanz-Zertifikat auf dem Server hinterlegen
Verbindung schlägt nach Wartungsarbeiten fehl (Datenquelle mit angeheftetem Zertifikat)	Das Serverzertifikat wurde rotiert	Verbindungsdialog öffnen, Erkennung ausführen, neues Zertifikat prüfen und übernehmen
Sichere Verbindungen schlagen nach Abschluss einer Rotation fehl	Ein Server wurde beim Hinterlegen des neuen Zertifikats übersehen	Dem neuen Thumbprint auf diesem Server vertrauen
Authentifizierungsfehler	Falsche Anmeldedaten oder fehlende Rechte des Serverkontos	Gespeicherte Anmeldedaten und Berechtigungen des Kontos auf dem Server prüfen

Symptom	Wahrscheinliche Ursache	Lösung
Die gewählte Sicherheitskonfiguration wird abgelehnt	Der Server bietet diese Modus-Richtlinien-Kombination nicht mehr an	Erkennung erneut ausführen und eine angebotene Konfiguration wählen
Server nicht erreichbar	Netzwerkpfad oder Firewall	Endpunkt-URL, Port und Firewall-Regeln prüfen

Verwandte Themen

- OPC-UA-Konfiguration — eine OPC-UA-Datenquelle anlegen
- Monitore — Monitor-Konzepte aller Typen

4.3 Siemens S7

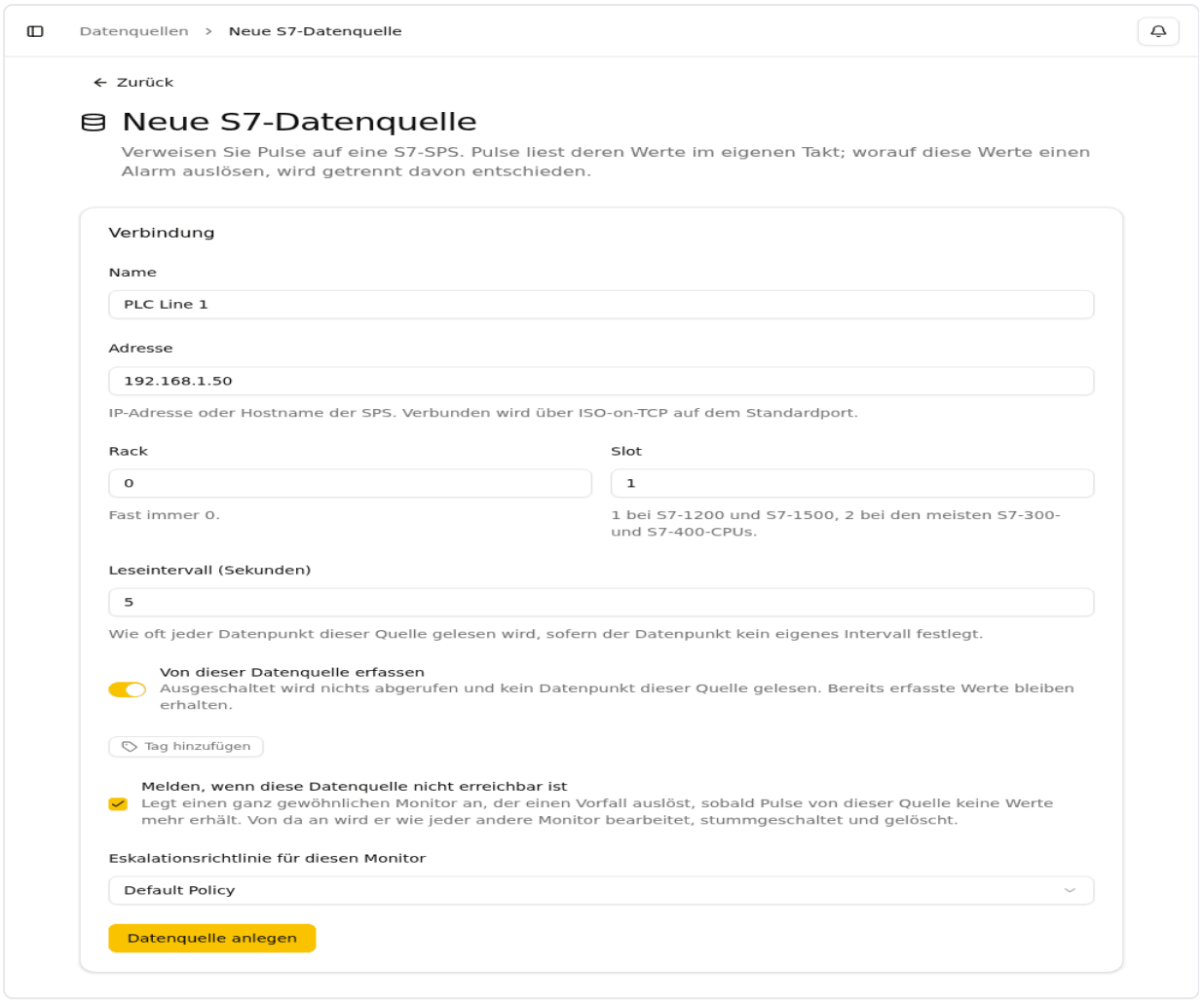
Pulse liest Siemens-SIMATIC-S7-SPS über das S7-Kommunikationsprotokoll. Eine SPS wird als **Datenquelle** angelegt: eine Verbindung, über die alle Werte dieser Maschine gelesen werden.

Es gibt zwei S7-Modi, und dies ist der klassische

Diese Seite beschreibt das Lesen einer SPS über **absolute Adressen** (`DB1.DBD4`). Das funktioniert bei jeder S7-Familie und setzt voraus, dass die PUT/GET-Kommunikation an der Steuerung freigegeben ist.

Eine S7-1200 ab Firmware V4.5 oder eine S7-1500 ab V2.9, deren Projekt mit TIA Portal V17 oder neuer geladen wurde, lässt sich stattdessen **über Symbolnamen** lesen — `"DB_Line".Speed` — ohne dass etwas freigeschaltet werden muss, und mit durchsuchbarem Symbolbaum. Siehe Symbolisches S7.

S7-Datenquelle anlegen



1. Navigieren Sie im Seitenbereich zu **Datenquellen → S7** und klicken Sie auf **Neue Datenquelle**
2. Wählen Sie im Menü **Siemens S7**. Im anschließenden Dialog wählen Sie **Klassisch — über absolute Adresse**
3. Konfigurieren Sie die Verbindung:

Feld	Beschreibung	Typischer Wert
Name	Ein beschreibender Name für die Datenquelle	`SPS Linie 1`
Adresse	IP-Adresse oder Hostname der SPS	`192.168.1.50`
Rack	SPS-Rack-Nummer	`0`
Slot	SPS-Slot-Nummer	`1`

Feld	Beschreibung	Typischer Wert
Leseintervall (Sekunden)	Wie oft jeder Datenpunkt dieser Quelle gelesen wird	`10`
Von dieser Datenquelle erfassen	Ausgeschaltet wird nichts abgefragt, ohne dass Sie die Quelle löschen müssen	
Tags	Datenquelle kategorisieren; jeder Datenpunkt erbt ihre Tags	
Melden, wenn diese Datenquelle nicht erreichbar ist	Legt zusammen mit der Quelle einen Monitor an (siehe unten)	

Pulse verbindet sich über ISO-on-TCP auf dem Standardport; ein Port muss daher nicht konfiguriert werden.

Anlegen über die Geräteerkennung

Wenn Sie über die Geräteerkennung hierher gelangen, indem Sie bei einem gefundenen Gerät auf **Hinzufügen** klicken, sind **Name**, **Adresse**, **Rack** und **Slot** bereits aus den Scan-Ergebnissen vorausgefüllt. Prüfen Sie die Angaben und fahren Sie mit den übrigen Feldern fort.

Rack- und Slot-Werte

Gängige Konfigurationen für Siemens-SPS:

SPS-Typ	Rack	Slot
S7-1200	0	1
S7-1500	0	1
S7-300	0	2
S7-400	0	2 oder 3

Alarm bei nicht erreichbarer SPS

Melden, wenn diese Datenquelle nicht erreichbar ist ist beim Anlegen einer Datenquelle vorausgewählt. Damit entsteht ein Bedingungsmonitor, der nach der Quelle benannt ist — *SPS Linie 1 nicht erreichbar* — und einen Vorfall auslöst, sobald Pulse keine Werte mehr von ihr erhält. Die zu verwendende Eskalationsrichtlinie wählen Sie im Feld unter dem Kontrollkästchen.

Von da an ist es ein ganz gewöhnlicher Monitor: Sie benennen ihn um, schalten ihn stumm, ändern seine Eskalationsrichtlinie, bearbeiten seine Bedingung oder löschen ihn — alles in der Monitorliste. Entfernen Sie den Haken, wenn für diese SPS niemand alarmiert werden soll.

Datenpunkte hinzufügen

Die einzelnen Werte im SPS-Speicher sind **Datenpunkte** der Datenquelle. Die Detailseite der Datenquelle listet jeden Datenpunkt auf, den Pulse liest — mit S7-Adresse, letztem Wert, Zeitpunkt der letzten Messung und Qualität der Messung.

Um einen neuen Datenpunkt zu deklarieren, öffnen Sie die Detailseite der Datenquelle und wählen Sie über der Tabelle **Datenpunkte** die Aktion **Datenpunkt hinzufügen**. Der Dialog fragt nach:

- **Adresse** — die S7-Adresse in der Syntax, die auch der Sampler liest, z. B. `I0.0`, `MW10` oder `DB1.DBD4`.
- **Datentyp** — wie Pulse den rohen SPS-Speicher an dieser Adresse interpretiert (siehe Datentypen unten).

Adresse und Datentyp müssen zusammenpassen: Eine `DBW`-Adresse (Word) enthält einen 16-Bit-Wert und passt daher zu **Word** oder **Int**, nicht zu **Real**. Pulse beginnt beim nächsten Abruf der Quelle mit dem Lesen des neuen Datenpunkts.

Um viele Datenpunkte auf einmal aus einer Tabelle zu deklarieren, verwenden Sie **Importieren** aus dem Aktionsmenü (⋯) direkt daneben. Die vollständige Spaltenreferenz — einschließlich der optionalen Schwellwertspalten, die je Datenpunkt einen Bedingungsmonitor anlegen — finden Sie unter Import aus CSV.

Mit dem Suchfeld über der Datenpunkttabelle finden Sie einen bestimmten Datenpunkt nach Adresse oder Name. Die Suche läuft serverseitig und erreicht alle deklarierten Datenpunkte, nicht nur die aktuelle Seite.

Auf einen Tag-Wert alarmieren

Um auf einen Datenpunkt zu alarmieren, erstellen Sie eine Bedingung und hängen einen Bedingungsmonitor daran. Eine Bedingung vergleicht Messwerte mit Schwellwerten, aggregiert sie über ein Zeitfenster und kann mehrere davon verknüpfen — auch einen Messwert und die Erreichbarkeit seiner Datenquelle in einer Regel. Eine SPS, die aus dem Netz fällt, löst dann den einen Vorfall aus, der genau das sagt, statt einen pro Wert, der von ihr gelesen wird.

Die Detailseite der Datenquelle zeigt einen Abschnitt **Monitore** mit allen Bedingungsmonitoren, die auf einen Datenpunkt dieser Datenquelle alarmieren. Klicken Sie auf einen Monitor, um seine Detailseite zu öffnen. Eine Datenquelle ohne Monitore alarmiert auf nichts; der Abschnitt sagt das ausdrücklich — eine nützliche Erinnerung daran, dass Messwerte erfasst werden, aber niemand alarmiert wird, wenn sie aus dem Ruder laufen.

Jede Zeile in der Datenpunkttabelle zeigt außerdem, welche Monitore auf genau diesen Datenpunkt alarmieren. Ein einzelner Monitor erscheint als Schaltfläche, die ihn direkt öffnet; alarmieren zwei oder mehr Monitore auf denselben Datenpunkt, zeigt die Schaltfläche die Anzahl und öffnet eine Auswahl mit den Namen.

Jede Zeile hat außerdem die Aktion **In Abfrage öffnen** im Kontextmenü (Rechtsklick oder die Schaltfläche ⋮), die Sie zur Seite Abfrage führt, die auf diesen Datenpunkt voreingestellt ist, damit Sie dessen Messverlauf erkunden können, ohne die Abfrage von Grund auf aufzubauen.

Datenpunkte bauen nur dann einen Verlauf auf, wenn Sie sie aufbewahren. Verwenden Sie **Aufbewahren** auf der Detailseite der Datenquelle für die Werte, die Sie langfristig auswerten wollen; die übrigen bleiben 24 Stunden lang lesbar.

S7-Adressformat

S7-Adressen folgen dem Muster `DBx.DByz` wobei:

- `DB` -- Datenbaustein-Präfix
- `x` -- Datenbaustein-Nummer
- `y` -- Datentyp: `B` (Byte), `W` (Wort/2 Bytes), `D` (Doppelwort/4 Bytes)
- `z` -- Byte-Offset innerhalb des Datenbausteins

Beispiele:

Adresse	Beschreibung
`DB1.DBW0`	Wort an Offset 0 in Datenbaustein 1
`DB2.DBD4`	Doppelwort an Offset 4 in Datenbaustein 2
`DB10.DBB0`	Byte an Offset 0 in Datenbaustein 10

Datentypen

Jeder S7-Datenpunkt trägt einen Datentyp, der festlegt, wie Pulse den rohen SPS-Speicher an seiner Adresse interpretiert:

Datentyp	Beschreibung
Bit	Einzelner boolescher Wert (0/1)
Byte	Vorzeichenloser 8-Bit-Ganzzahlwert
Word	Vorzeichenloser 16-Bit-Ganzzahlwert
DWord	Vorzeichenloser 32-Bit-Ganzzahlwert
Int	Vorzeichenbehafteter 16-Bit-Ganzzahlwert
DInt	Vorzeichenbehafteter 32-Bit-Ganzzahlwert
Real	32-Bit-Gleitkommazahl

Adresse und Datentyp müssen zusammenpassen: Eine `DBW`-Adresse (Word) enthält einen 16-Bit-Wert und passt daher zu **Word** oder **Int**, nicht zu **Real**.

TIP

Beachten Sie die Dokumentation Ihres SPS-Programms für die korrekten Datenbaustein-Nummern, Offsets und Datentypen der zu lesenden Werte.

Teil 4 · Monitortypen

4.4 Symbolisches S7 (S7-1200/1500)

Pulse liest neuere SIMATIC-Steuerungen **über Symbolnamen** — `"DB_Line".ThroughputPerMinute` — statt über absolute Adressen. Es ist dieselbe Siemens-S7-Familie wie im klassischen Modus, nur über ein anderes Protokoll erreicht: S7CommPlus, das Protokoll, mit dem auch das TIA Portal selbst mit einer SPS spricht.

Warum sich der Wechsel lohnt:

- **Namen statt Offsets.** Ein klassischer Datenpunkt ist ein Byte-Offset in einem Datenbaustein — und er bedeutet stillschweigend etwas anderes, sobald jemand das Programm neu übersetzt und sich das Layout verschiebt. Ein Symbol übersteht das, denn es ist der Name, den das Programm selbst benutzt.
- **Nichts freizuschalten.** Der klassische Modus braucht die PUT/GET-Kommunikation auf der SPS — eine Einstellung, die viele Anlagen bewusst ausgeschaltet lassen. S7CommPlus ist die Schnittstelle, die das TIA Portal ohnehin verwendet.
- **Durchsuchbar.** Pulse kann die SPS fragen, was sie hat. Sie wählen Werte aus einem Baum aus, statt eine Symboltabelle abzutippen.

Welchen Modus brauche ich?

Beide Modi sind gemeinsam unter **Datenquellen → S7** in der Seitenleiste aufgeführt — jede Zeile in der Liste trägt ein Badge mit ihrem Modus. Um eine neue Quelle anzulegen, klicken Sie auf **Neue Datenquelle** und wählen **Siemens S7**: Der Dialog nennt jeden Modus und seine Voraussetzungen. Im Zweifel: zuerst symbolisch versuchen und auf klassisch zurückfallen, wenn Ihre SPS älter ist als der Bereich unten.

Was die SPS mitbringen muss

Voraussetzung	S7-1500	S7-1200
Firmware	V2.9 oder neuer	V4.5 oder neuer
Projekt	Mit TIA Portal V17 oder neuer geladen	Mit TIA Portal V17 oder neuer geladen
Schutzstufe	Lesezugriff erlaubt, oder eine Leserolle zum Anmelden	Lesezugriff erlaubt, oder eine Leserolle zum Anmelden

Firmware und TIA-Version sind zwei getrennte Bedingungen, und beide müssen erfüllt sein: Die Firmware bringt das TLS-Protokoll mit, und das Projekt muss von einer TIA-Version geladen worden sein, die es verwendet.

Eine ältere SPS ist nicht verloren. Eine S7-1500 unter V2.9, eine S7-1200 unter V4.5 sowie jede S7-300 und S7-400 lassen sich als klassische S7-Datenquelle mit aktiviertem PUT/GET lesen — oder über den eigenen OPC-UA-Server der SPS, den S7-1500 ab V2.0 und S7-1200 ab V4.4 mitbringen (er braucht eine Runtime-Lizenz auf der SPS). Die Gerätesuche sagt Ihnen für jede gefundene Steuerung, welcher der drei Wege gilt.

Schutzstufe und Legitimierung

Die Schutzstufe einer SPS entscheidet, ob ein nicht angemeldeter Client sie lesen darf. Erlaubt die Stufe den Lesezugriff, braucht Pulse nichts weiter. Erlaubt sie ihn nicht, erwartet die SPS, dass sich ein Client legitimiert — mit dem Passwort der Schutzstufe oder mit einem UMAC-Benutzer, der eine Leserolle hat.

Verweigert eine SPS den Lesezugriff, meldet die Datenquelle **Lesen verweigert** auf ihrer Detailseite. Das ist die Schutzstufe, kein Netzwerkproblem: Geben Sie Pulse in den Schutzeinstellungen der SPS Lesezugriff, oder richten Sie eine Leserolle dafür ein.

Eine symbolische S7-Datenquelle anlegen

1. **Datenquellen → Neue Datenquelle → Siemens S7**, dann **Symbolisch** wählen.
2. Verbindung ausfüllen:

Feld	Bedeutung	Typischer Wert
Name	Wie diese SPS in Pulse heißt	`SPS Linie 1`
Adresse	IP-Adresse oder Hostname der SPS, optional `host:port`	`192.168.1.50`
Leseintervall (Sekunden)	Wie oft jeder Datenpunkt dieser Quelle gelesen wird	`5`
Von dieser Datenquelle erfassen	Ausschalten, um das Lesen zu stoppen, ohne die Quelle zu löschen	
Tags	Die Quelle kategorisieren; jeder Datenpunkt erbt ihre Tags	

Feld	Bedeutung	Typischer Wert
Benachrichtigen, wenn diese Quelle nicht erreichbar ist	Legt einen Condition-Monitor mit dem Namen der Quelle an	

Kein Baugruppenträger und kein Steckplatz. Der klassische Modus fragt danach, weil eine klassische Verbindung eine Baugruppe eines Racks adressiert. S7CommPlus adressiert die SPS selbst, es gibt hier also nichts zu konfigurieren — wenn Sie gewohnt sind, `0` und `1` einzutragen: Ihr Fehlen ist richtig so.

Fünf Sekunden sind das voreingestellte Leseintervall, und das aus gutem Grund: Ein symbolischer Lesevorgang ist eine gebündelte Anfrage auf einer offenen Sitzung, ein Fünf-Sekunden-Takt kostet die SPS also sehr wenig. Für langsam veränderliche Werte dürfen es ruhig mehr sein.

Dem Zertifikat der SPS vertrauen



S7CommPlus ist TLS, und eine SIMATIC-SPS signiert ihr Zertifikat selbst — es gibt keine Stelle, gegen die man es prüfen könnte. Pulse macht es deshalb wie das TIA Portal: Es zeigt Ihnen, was die SPS vorgelegt hat, und bittet Sie, es **einmal** zu bestätigen. Bis dahin wird nichts von der SPS gelesen.

1. Öffnen Sie die Seite der neuen Datenquelle. Das Panel **Vertrauenswürdiges SPS-Zertifikat** zeigt den aktuellen Zustand — eine farbkodierte Kopfzeile gibt auf einen Blick an, ob das Zertifikat bestätigt ist, auf eine Bestätigung wartet oder nicht übereinstimmt.
2. Klicken Sie auf **Zertifikat der SPS abrufen**. Pulse baut eine TLS-Verbindung auf, liest das vorgelegte Zertifikat, schließt wieder und zeigt Ihnen Inhaber, Gültigkeit und den **SHA-256-Fingerabdruck**.

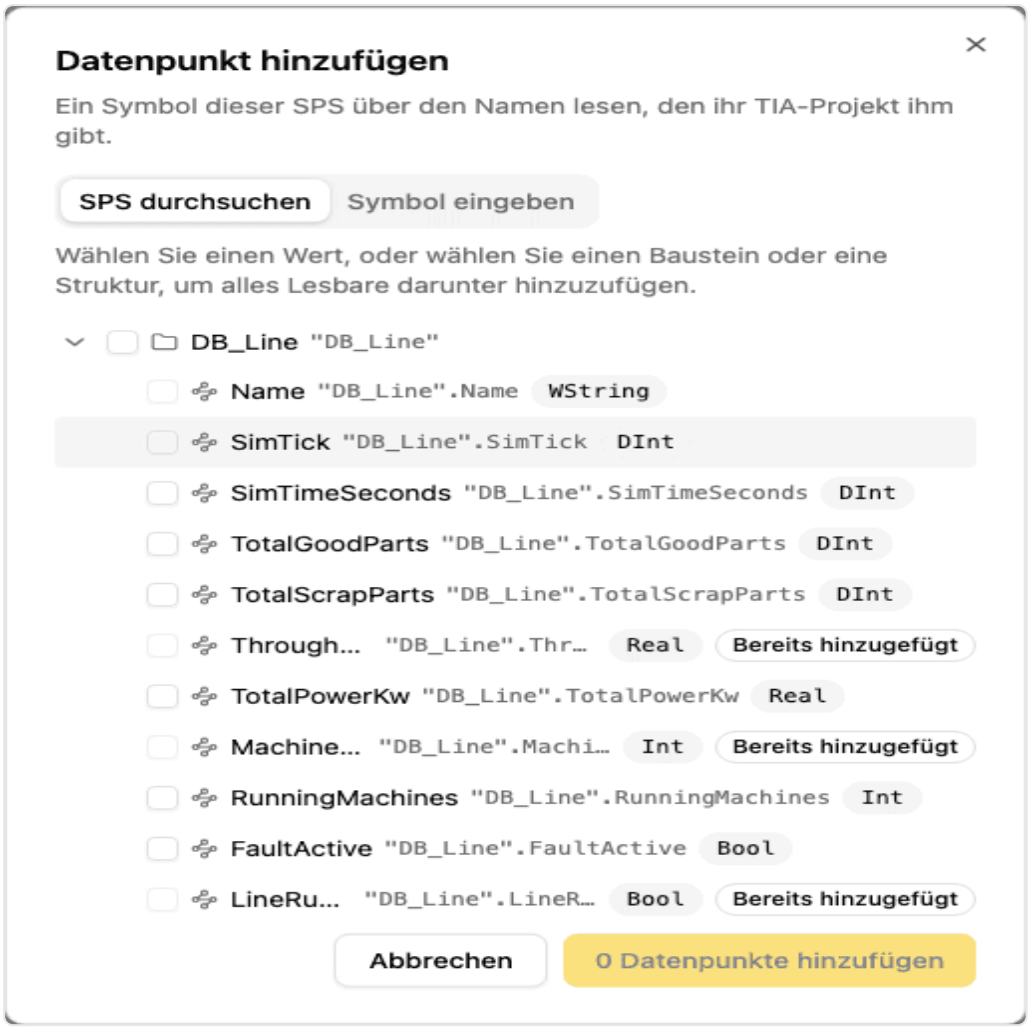
3. Vergleichen Sie diesen Fingerabdruck mit dem, den das TIA Portal für dieselbe SPS anzeigt (in den Schutzeinstellungen der SPS), oder mit dem, den Ihre Steuerungstechnik Ihnen nennt.
4. Klicken Sie auf **Diesem Zertifikat vertrauen**. Ab diesem Moment liest die Quelle.

Ist ein Zertifikat bereits bestätigt, zeigt die Kopfzeile des Panels den Kurzfingerabdruck sowie einen Umschalter **Details anzeigen**, über den Sie die vollständigen Zertifikatsdaten aufklappen können.

> **Vergleichen Sie den Fingerabdruck, bevor Sie bestätigen**
>
> Das Bestätigen ist hier die gesamte Sicherheit. Ein nicht geprüfter Fingerabdruck ist eine nicht authentifizierte Verbindung — das Zertifikat könnte zu irgendeiner Maschine gehören, die unter dieser Adresse geantwortet hat.

Legt die SPS später ein anderes Zertifikat vor, hört Pulse auf zu lesen. Die Kopfzeile des Panels zeigt den Nicht-Übereinstimmungs-Zustand. Klicken Sie auf **Erneut abrufen**, vergleichen Sie den neuen Fingerabdruck und bestätigen Sie ihn, um das Lesen fortzusetzen. Das Zertifikat einer SPS ändert sich, wenn sie getauscht, auf Werkseinstellungen zurückgesetzt oder neu ausgestellt wird — jeder dieser Fälle ist einen Blick wert.

Datenpunkte anlegen



Öffnen Sie die Quelle und wählen Sie **Datenpunkt hinzufügen**. Der Dialog hat zwei Reiter.

SPS durchsuchen ist der Weg der Wahl. Pulse fragt die SPS nach ihrem Programm und ordnet die Symbole in Ordner: **Datenbausteine**, **Eingänge**, **Ausgänge**, **Merker**, **Zeiten** und **Zähler**. Die Zahl neben einem Ordner, einem Baustein oder einer Struktur zeigt, wie viele Datenpunkte er anlegt — sehen Sie, was Sie anhaken, bevor Sie es tun. Haken setzen, **Hinzufügen** klicken.

- **Einen Wert anhaken**, um genau dieses Symbol zu lesen.
- **Einen Baustein, eine Struktur oder ein Array anhaken**, um alles Lesbare darunter zu lesen, ohne es zu öffnen. Ein Haken auf einer Struktur mit elf Elementen legt elf Datenpunkte an.
- **Große Arrays** zeigen die ersten zehn Elemente; klicken Sie auf **X weitere anzeigen**, um den Rest einzublenden, oder suchen Sie nach dem gewünschten Element.
- **Wählen Sie mehr als 50 Datenpunkte auf einmal aus**, erscheint ein Bestätigungsschritt, bevor die Aktion ausgeführt wird — damit ein breiter Haken auf einer großen Struktur eine bewusste Entscheidung bleibt.

- Eine Auswahl von mehr als 1.000 Datenpunkten wird abgelehnt — öffnen Sie sie und wählen Sie einen kleineren Teil.
- Symbole, die Pulse noch nicht speichern kann — Datums- und Zeitwerte — werden angezeigt, lassen sich aber nicht anhaken; so sehen Sie, dass die SPS sie hat.
- Ein Symbol, das diese Quelle bereits liest, ist mit **Bereits hinzugefügt** gekennzeichnet.
- Klicken Sie auf den Namen eines Symbols, um seinen vollständigen Pfad in die Zwischenablage zu kopieren.
- Sind einige Auswahlen beim Klicken auf **Hinzufügen nicht mehr im Programm der SPS** — weil das Programm zwischen dem Durchsuchen und dem Hinzufügen neu übersetzt wurde — nennt Pulse sie, entfernt sie aus der Auswahl und fügt nichts hinzu. Prüfen Sie die verbleibende Auswahl und klicken Sie erneut auf **Hinzufügen**.

Suche: Geben Sie mindestens zwei Zeichen in das Suchfeld ein, um den vollständigen Symbolkatalog der SPS zu durchsuchen, ohne im Baum zu navigieren. Jedes Ergebnis zeigt seinen übergeordneten Pfad in einer zweiten Zeile, damit Sie sehen, wo es sich befindet. Datenbausteine zeigen ihre Nummer (zum Beispiel **DB4**), damit Sie sie auf einen Blick mit der Baustein-Liste im TIA Portal abgleichen können. Leeren Sie die Suche, um zum Baum in seinem bisherigen Zustand zurückzukehren.

Symbol eingeben ist der Rückfallweg, für eine SPS, die noch nicht erreichbar ist oder deren Zertifikat noch niemand bestätigt hat. Geben Sie das Symbol genau so ein, wie das TIA Portal es schreibt, mit Anführungszeichen, und sagen Sie, welche Art von Wert es enthält:

Gelesen als	Siemens-Typen
Dezimalzahl	`Real`, `LReal`
Ganze Zahl	`Int`, `DInt`, `SInt`, `LInt`, `UInt`, `UDInt`, `USInt`, `ULInt`, `Byte`, `Word`, `DWord`, `LWord`
Ein oder aus	`Bool`
Text	`String`, `WString`, `Char`, `WChar`

Schreibweise der Symbole

Ein Symbol ist der Pfad, den das TIA Portal anzeigt, und Pulse schickt ihn unverändert an die SPS — Anführungszeichen, Groß- und Kleinschreibung inklusive.

Symbol	Was es ist
`"DB_Line".ThroughputPerMinute`	Ein Wert in einem Datenbaustein
`"DB_Motor".Limits.MaxRpm`	Ein Element einer Struktur
`"DB_Stations".Station[0].TemperatureC`	Ein Element eines Array-Elements

Das letzte ist die Form, die keine klassische S7-Adresse ausdrücken kann, ohne Bytes zu zählen.

Eine Symboltabelle importieren

Um viele auf einmal anzulegen, nutzen Sie **Importieren** im Aktionsmenü (⋯) der Datenpunkte. Ein symbolischer Import liest zwei Spalten:

- **symbol** — der Name, wie oben.
- **Gelesen als** — welche Art von Wert es enthält. **Leer lassen heißt „die SPS fragen“**: Pulse schlägt das Symbol dann im Katalog nach, typisiert es aus der Deklaration der SPS und legt — wenn die Zeile einen Baustein oder eine Struktur nennt — einen Punkt je lesbarem Symbol darunter an.

Eine Zeile, die ihren Typ angibt, braucht gar keine SPS; eine Symboltabelle lässt sich also importieren, bevor die Steuerung erreichbar ist. Eine Zeile, die ihn leer lässt, ist zugleich die einzige, die ein Symbol melden kann, das die SPS nicht hat: Unbekannte Symbole lassen ihre eigene Zeile scheitern, der Rest der Datei wird trotzdem importiert. Den Assistenten selbst beschreibt Import aus CSV.

Auf einen Wert alarmieren

Ein symbolischer Datenpunkt verhält sich wie jeder andere: Bauen Sie eine Bedingung darüber und hängen Sie einen Condition-Monitor daran. In der Sensorauswahl des Bedingungseditors steht die Quelle unter **Siemens S7 (symbolisch)**, ihre Punkte sind nach Symbol aufgeführt.

Eine Sitzung je SPS

Pulse hält **eine einzige** S7CommPlus-Sitzung je SPS und bündelt alle Datenpunkte der Quelle in eine Anfrage pro Takt. Das ist Absicht: Eine S7-1200 hat sehr wenige Verbindungsressourcen, und eine Engineering-Station, ein HMI und ein

Überwachungssystem können sie zu dritt aufbrauchen. Wenn das TIA Portal nicht online gehen kann, während Pulse liest, sind die Verbindungen der SPS erschöpft — nicht weil Pulse mehr als seine eine hält.

Aus demselben Grund ist eine Quelle je SPS die richtige Form. Zwei Quellen auf dieselbe Steuerung bedeuten zwei Sitzungen.

Wenn eine Quelle nicht mehr liest

Die Detailseite der Quelle zeigt den Grund in einem Banner, und der Vorfall des **Nicht-erreichbar**-Monitors trägt denselben Text. Die Gründe, die es nur in diesem Modus gibt:

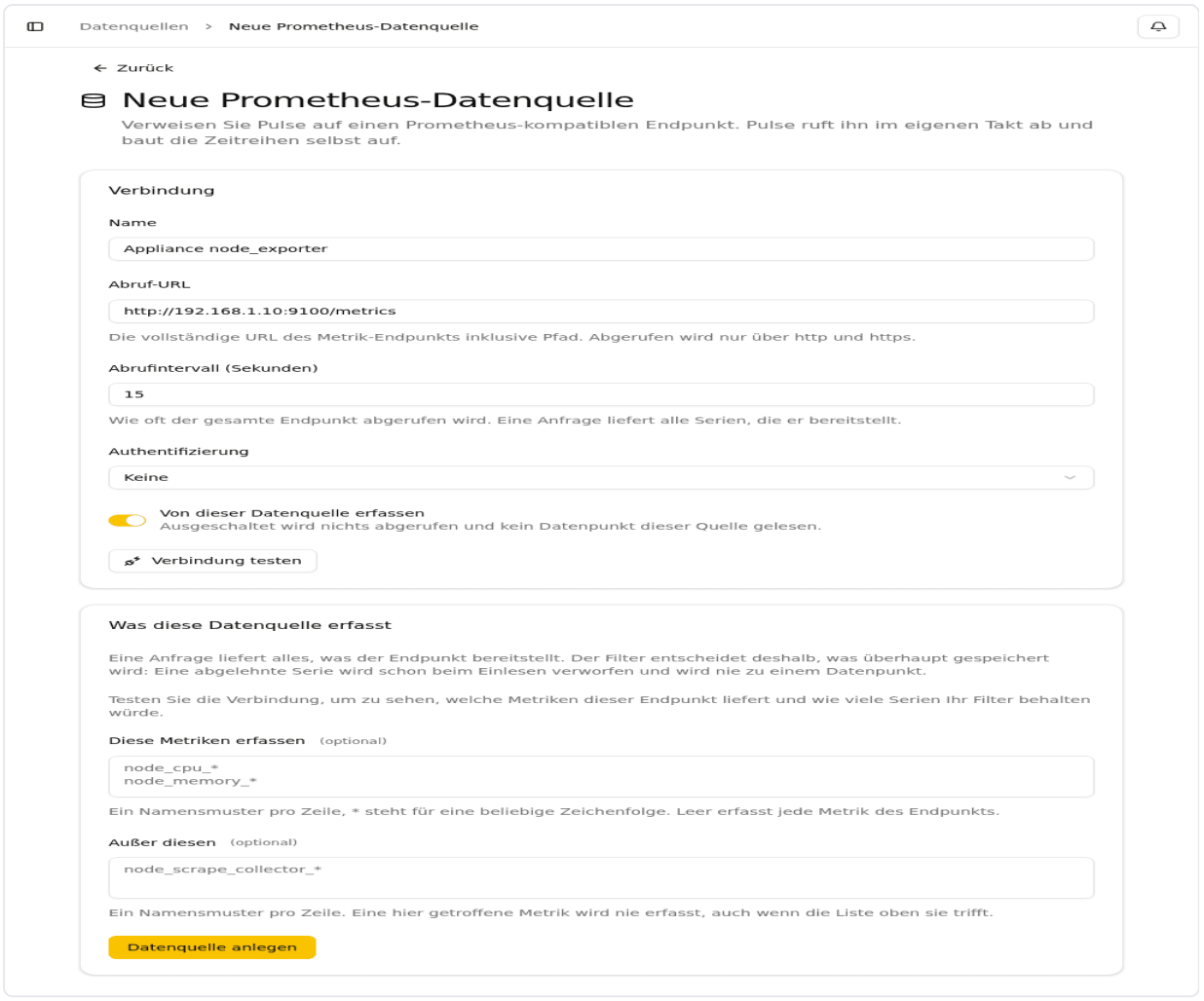
Grund	Was er bedeutet
Zertifikat abgelehnt (kein Pin)	Pulse hat für diese SPS noch kein Zertifikat bestätigt. Öffnen Sie das Zertifikat-Panel, rufen Sie das Zertifikat ab und bestätigen Sie es.
Zertifikat abgelehnt (Abweichung)	Die SPS legt ein anderes Zertifikat vor als das, dem Pulse vertraut. Öffnen Sie das Zertifikat-Panel, rufen Sie das neue Zertifikat ab, vergleichen Sie es und bestätigen Sie es.
Sicherheits-Handshake fehlgeschlagen	Der TLS-Handshake kam nicht zustande. Meist eine SPS, deren Firmware älter ist als das Protokoll — lesen Sie sie als klassische Quelle.
Authentifizierung fehlgeschlagen	Die Schutzstufe der SPS verlangt, dass sich der Client legitimiert, und Pulse konnte es nicht. Richten Sie Lesezugriff oder eine Leserolle ein.
Lesen verweigert	Die Sitzung steht und die SPS hat das Lesen verweigert — ihre Schutzstufe erlaubt es nicht.
Firmware nicht unterstützt	Die Firmware liegt außerhalb des Bereichs, den dieses Protokoll unterstützt. Nutzen Sie den klassischen Modus oder den OPC-UA-Server der SPS.
Collector kann dieses Protokoll nicht lesen	Der dieser Quelle zugewiesene Collector ist zu alt für das symbolische S7-Protokoll. Aktualisieren Sie den Collector oder weisen Sie die Quelle einem anderen zu.

Die vollständige Liste steht in Monitore.

4.5 Prometheus

Pulse verbindet sich als **Datenquelle** mit einem Prometheus-kompatiblen Metrik-Endpunkt. Pulse ruft den Endpunkt im eigenen Takt ab, speichert die zurückgegebenen Zeitreihen als Datenpunkte und macht sie für Conditions und Diagramme verfügbar.

Prometheus-Datenquelle hinzufügen



1. Navigieren Sie zu **Datenquellen → Prometheus** in der Seitenleiste und klicken Sie auf **Neue Datenquelle**
2. Wählen Sie **Prometheus**
3. Konfigurieren Sie die Datenquelle:

Feld	Beschreibung	Beispiel
Name	Ein beschreibender Name für die Datenquelle	`node_exporter der Appliance`
Abruf-URL	Die vollständige URL des Metrik-Endpunkts inklusive Pfad	`http://localhost:9100/metrics`
Abrufintervall (Sekunden)	Wie oft der Endpunkt abgerufen wird; eine Anfrage liefert alle Serien, die er bereitstellt	`15`
Von dieser Datenquelle erfassen	Ausschalten, um den Abruf zu stoppen, ohne die Quelle zu löschen	
Authentifizierung	Wie Pulse sich am Endpunkt anmeldet (siehe unten)	

Authentifizierung

Drei Modi stehen zur Verfügung:

Modus	Einsatz
Keine	Der Endpunkt ist offen oder durch Netzwerkkontrollen geschützt
Bearer-Token	Der Endpunkt erfordert einen `Authorization: Bearer <token>`-Header
Basic Auth	Der Endpunkt erfordert Benutzername und Passwort

Geheimnisse (Tokens und Passwörter) werden nur zum Schreiben gespeichert: Pulse zeigt sie nach dem Speichern nicht mehr an. Lassen Sie das Feld beim Bearbeiten leer, um das gespeicherte Geheimnis beizubehalten; geben Sie einen neuen Wert ein, um es zu ersetzen.

Verbindung testen

Klicken Sie auf **Verbindung testen**, bevor Sie speichern. Pulse ruft den Endpunkt einmal ab und gibt an, wie viele Serien über wie viele Metriken gefunden wurden. Dieser Schritt ist wichtig: Eine Abrufanfrage kann Hunderte von Serien zurückliefern, und Sie möchten sehen, was Sie behalten, bevor die Erfassung beginnt.

Was diese Datenquelle erfasst

Jeder Prometheus-Abruf liefert alle Serien, die der Endpunkt bereitstellt. Der **Metrikfilter** entscheidet, welche dieser Serien als Datenpunkte gespeichert werden; abgelehnte Serien werden bereits beim Einlesen verworfen und werden nie zu Datenpunkten oder verbrauchen Speicher.

Der Filter hat zwei Listen:

Liste	Verhalten
Diese Metriken erfassen	Ein Namensmuster pro Zeile. `*` steht für eine beliebige Zeichenfolge. Leer lassen, um alle Metriken des Endpunkts zu erfassen.
Außer diesen	Ein Namensmuster pro Zeile. Eine hier getroffene Metrik wird nie erfasst, auch wenn die obige Liste sie trifft.

Nachdem Sie **Verbindung testen** ausgeführt haben, zeigt das Filterpanel eine Live-Anzahl, wie viele Serien Ihr aktueller Filter von der Gesamtzahl behalten würde. Passen Sie die Muster an und beobachten Sie, wie sich die Anzahl ändert, bevor Sie speichern.

> **Erst weit, dann enger**
>
> Lassen Sie den Filter beim ersten Speichern leer, sehen Sie sich auf der Detailseite der Datenquelle an, was erfasst wird, und bearbeiten Sie die Quelle dann, um eine Ablehnliste für nicht benötigte Serien hinzuzufügen. Das ist einfacher als Muster für Metriken zu schreiben, die Sie noch nie gesehen haben.

Datenpunkte und Verlauf

Sobald eine Datenquelle erfasst, wird jede einzelne Zeitreihe zu einem **Datenpunkt**, der auf der Detailseite der Datenquelle angezeigt wird. Die Seite zeigt:

- Den Metriknamen und etwaige Labels
- Den zuletzt gelesenen Wert und den Zeitpunkt des letzten Lesens
- Ob die Lesequalität Gut, Schlecht oder Keine Daten ist

Datenpunkte bauen nur dann einen Verlauf auf, wenn Sie sie aufbewahren. Verwenden Sie **Aufbewahren** auf der Detailseite der Datenquelle für Serien, die Sie langfristig grafisch darstellen oder abfragen möchten; die übrigen bleiben 24 Stunden lesbar und werden dann gelöscht.

Mit dem Suchfeld über der Tabelle können Sie eine bestimmte Serie nach Name oder Beschreibung finden. Die Suche läuft serverseitig und erreicht alle Datenpunkte der Quelle — hilfreich, wenn ein Prometheus-Endpunkt Hunderte oder Tausende von Serien bereitstellt.

Auf einen Wert aufmerksam machen

Um bei Überschreitung eines Prometheus-Schwellenwerts einen Alarm auszulösen, erstellen Sie eine Condition mit einem **Sensor**-Knoten, der auf den Datenpunkt zeigt. Eine Condition kann mehrere Datenpunkte in einer Regel kombinieren — zum Beispiel: Alarm, wenn die CPU-Auslastung den gelernten Normalwert überschreitet.

Metriktypen

Pulse speichert Prometheus-Metriktypen so, wie sie ankommen, und macht sie für Abfragen verfügbar:

Typ	Beschreibung
Counter	Ein monoton wachsender Zähler; verwenden Sie einen **Anstiegsrate**-Knoten in einer Condition, um ihn in eine Rate pro Sekunde umzuwandeln
Gauge	Ein Wert, der steigen und fallen kann
Histogram	Eine Stichprobenverteilung mit Anzahl-, Summen- und Bucket-Serien
Summary	Eine vorberechnete Quantilverteilung
Ohne Typ	Metriken, die der Endpunkt nicht typisiert hat

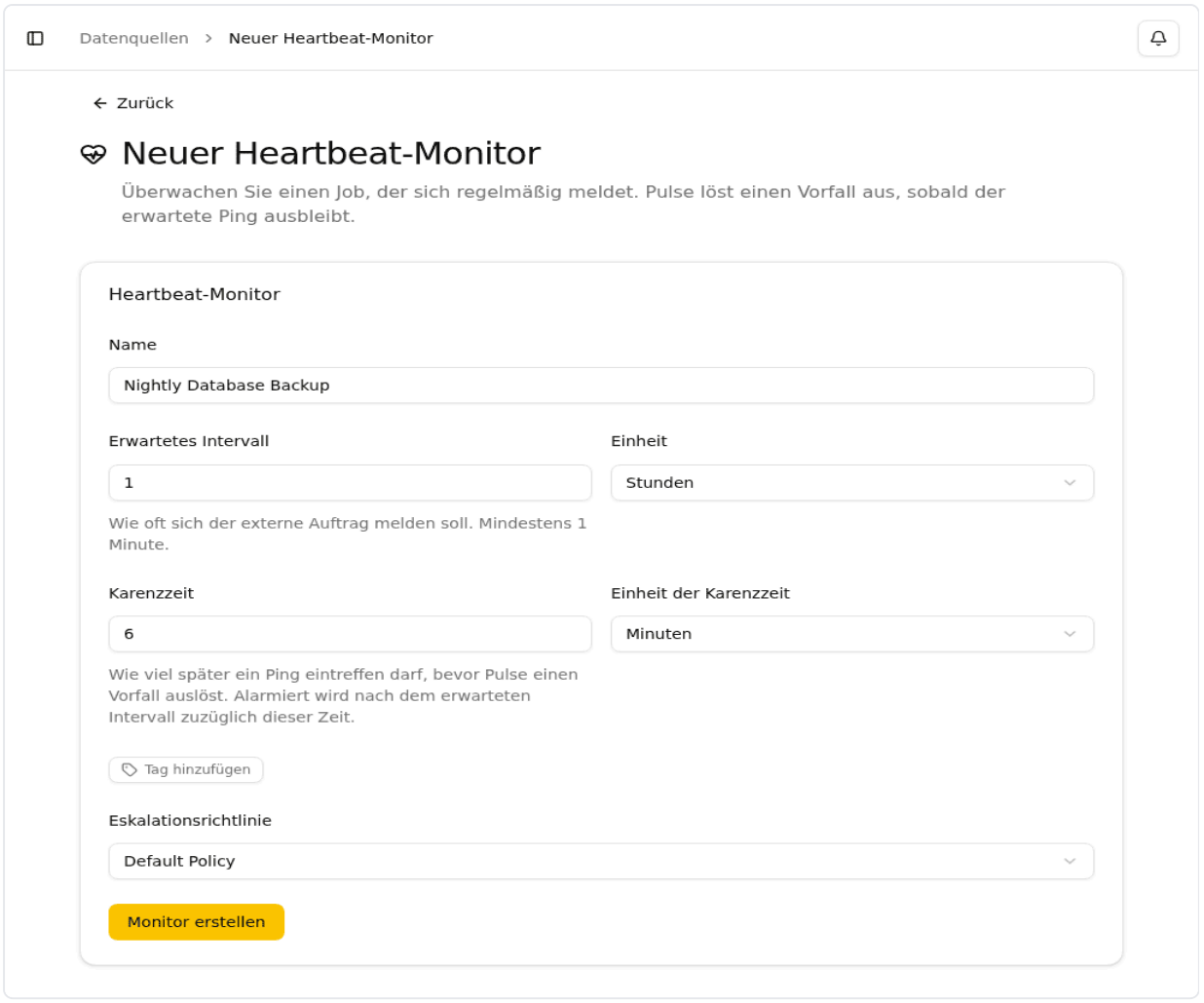
4.6 Heartbeat

Ein Heartbeat-Monitor überwacht einen Job, der nach Zeitplan läuft -- ein nächtliches Backup, einen stündlichen Export, ein Edge-Gerät, das sich regelmäßig meldet. Der Job ruft nach jedem erfolgreichen Durchlauf eine URL auf, und Pulse löst einen Vorfall aus, sobald dieser Aufruf ausbleibt.

Dieser Monitortyp funktioniert als einziger umgekehrt: Pulse baut keine Verbindung auf. Pulse wartet, und das Schweigen ist der Alarm. Damit ist er die richtige Wahl für alles, was Pulse nicht direkt erreichen kann -- einen Cron-Job hinter einer Firewall, ein Skript auf einem Notebook, ein Gateway an einem entfernten Standort.

Ein Heartbeat ist eine **Datenquelle**: Pulse erfasst von ihr genau ein Signal -- "ein Ping ist eingetroffen" -- und ein gewöhnlicher Monitor alarmiert, wenn dieses Signal verstummt. Ihre Heartbeats finden Sie unter **Datenquellen**, den zugehörigen Monitor in der Monitorliste neben allen anderen.

Heartbeat erstellen



1. Öffnen Sie **Datenquellen** und klicken Sie auf **Neu** -- oder nutzen Sie **Erstellen** in der Monitorliste
2. Wählen Sie **Heartbeat**
3. Füllen Sie die Felder aus:

Feld	Beschreibung
Name	Ein aussagekräftiger Name, üblicherweise der Name des Jobs (z. B. `Nächtliches Backup`)
Erwartetes Intervall	Wie oft der externe Auftrag sich melden soll. Mindestens 1 Minute
Einheit	Minuten, Stunden oder Tage

Feld	Beschreibung
Karenzzeit	Wie viel später ein Ping eintreffen darf, bevor Pulse einen Vorfall auslöst. Alarmiert wird nach dem erwarteten Intervall zuzüglich dieser Zeit
Einheit der Karenzzeit	Sekunden, Minuten oder Stunden
Eskalationsrichtlinie	Welche Eskalationsrichtlinie greift, wenn der Ping ausbleibt
Tags	Kategorisierung des Heartbeats

Mit dem Heartbeat entsteht zugleich sein Monitor, benannt nach ihm. Dieser Monitor ist ein ganz gewöhnlicher: Sie können ihn stummschalten, einem Team zuordnen, seine Eskalationsrichtlinie ändern oder ihn öffnen und neben der Ping-Prüfung eine eigene Bedingung ergänzen.

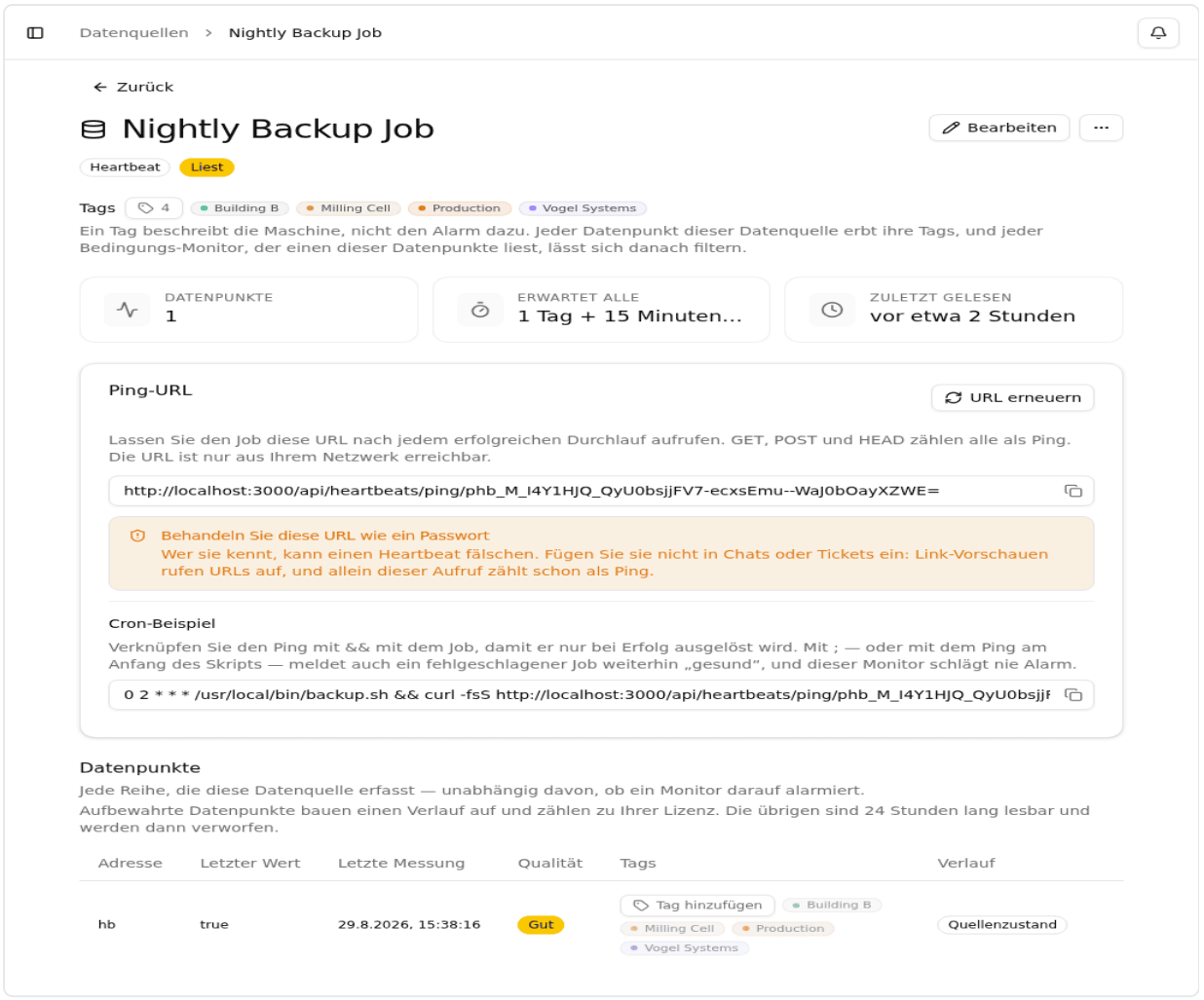
Das **erwartete Intervall** entspricht dem Zeitplan, nach dem Ihr Job läuft. Stellen Sie es so ein, wie oft der Job tatsächlich läuft -- nicht großzügiger.

Die **Karenzzeit** deckt Schwankungen in der Laufzeit des Auftrags ab. Ein Backup, das stündlich läuft, gelegentlich aber einige Minuten länger braucht, sollte mit einer Karenzzeit dieser paar Minuten eingerichtet werden, damit ein langsamer Durchlauf keinen Alarm auslöst. Pulse löst einen Vorfall erst aus, wenn sowohl das erwartete Intervall als auch die Karenzzeit ohne Ping verstrichen sind. Eine Karenzzeit von null bedeutet, dass Pulse sofort alarmiert, sobald das erwartete Intervall überschritten ist.

Die Uhr läuft ab dem Anlegen des Monitors, nicht ab dem ersten Ping. Bleibt jeder Ping aus, löst der Monitor seinen ersten Vorfall aus, sobald das erwartete Intervall zuzüglich der Karenzzeit abgelaufen ist. Bis zum ersten Ping oder bis zu dieser ersten Frist hat der Monitor den Status **Unbekannt**.

Die Ping-URL

Jeder Heartbeat erhält eine eigene Ping-URL, die auf seiner Seite unter **Datenquellen** angezeigt wird.



Klicken Sie auf die Schaltfläche neben der URL, um sie in die Zwischenablage zu kopieren. `GET`, `POST` und `HEAD` zählen alle als Ping -- Sie können also verwenden, was auf dem Zielsystem ohnehin vorhanden ist: `curl`, `wget`, eine geplante Aufgabe oder ein zweizeiliges Skript.

Die URL ist nur aus Ihrem Netzwerk erreichbar. Ein Job auf einem System, das Pulse nicht erreicht, kann auch nicht pingen.

Behandeln Sie die Ping-URL wie ein Passwort

Wer die URL kennt, kann einen Heartbeat fälschen -- und ein gefälschter Heartbeat bedeutet, dass ein fehlgeschlagener Job als gesund gemeldet wird.

Fügen Sie die URL nicht in Chat-Nachrichten, Tickets, Wiki-Seiten oder gemeinsam genutzte Dokumente ein. Chat-Werkzeuge und Ticketsysteme erzeugen Link-Vorschauen, indem sie **die URL aufrufen** -- und allein dieser Aufruf zählt bereits als Ping. Ein an bequemer Stelle eingefügter Link kann den Monitor also unbemerkt auf Grün halten, solange die Vorschau aktualisiert wird.

Hinterlegen Sie die URL dort, wo bei Ihnen ohnehin Geheimnisse liegen: in der Konfigurationsverwaltung, in einem Secrets-Manager oder direkt im Skript des Jobs auf dem ausführenden System.

Ping-URL erneuern

Wenn die URL nach außen gelangt ist, klicken Sie auf der Heartbeat-Seite unter **Datenquellen** auf **URL erneuern**. Die alte URL funktioniert sofort nicht mehr -- hinterlegen Sie die neue also unverzüglich. Ein Job, der weiterhin die alte URL aufruft, zählt nicht mehr als Ping, und der Monitor löst nach Ablauf des erwarteten Intervalls einen Vorfall aus.

Das Erneuern tauscht ausschließlich die URL. Historie, erwartetes Intervall und ein eventuell offener Vorfall bleiben unverändert.

Einbindung in Cron

Setzen Sie den Ping **hinter** den Job und verknüpfen Sie beide mit `&&`:

```
0 2 * * * /usr/local/bin/backup.sh && curl -fsS https://pulse.example.com/api/heartbeats/ping/ihr-toke
```

`&&` bedeutet „nur wenn der vorherige Befehl erfolgreich war". Schlägt das Backup fehl, läuft der Ping nicht, Pulse hört nichts -- und Sie bekommen genau den Vorfall, den Sie haben wollten.

Es gibt drei typische Fehler, die alle dazu führen, dass ein Monitor dauerhaft „gesund" meldet, obwohl der Job kaputt ist:

- **Verknüpfung mit `;` statt `&&`.** Ein Semikolon führt den Ping aus, unabhängig davon, ob der Job erfolgreich war.
- **Der Ping steht vorne.** `curl ... && /usr/local/bin/backup.sh` pingt, bevor der Job überhaupt etwas getan hat.

- **Der Ping steht am Anfang des Skripts.** Dasselbe Problem, nur eine Datei weiter weg und im Review deutlich schwerer zu erkennen.

Die Regel ist einfach: Der Ping ist das Erfolgssignal des Jobs. Es darf also nichts pingen, bevor der Job durchgelaufen und erfolgreich war.

Die Optionen `-fsS` sorgen dafür, dass `curl` bei Erfolg still bleibt und bei einem HTTP-Fehler fehlschlägt -- ein Netzwerk- oder Serverproblem taucht dadurch in Ihrer Cron-Mail auf, statt unbemerkt zu bleiben.

Eine *vertippte oder rotierte* Ping-URL erscheint dort allerdings nicht: Der Ping-Endpunkt antwortet immer mit `200 OK`, unabhängig davon, ob das Token gültig ist -- so kann niemand darüber prüfen, ob ein gefundenes Token noch aktiv ist. Eine falsche URL fällt genauso auf wie ein Job, der nicht mehr läuft: Der Monitor hört nichts mehr von Ihnen und löst nach Ablauf des erwarteten Intervalls einen Vorfall aus. Prüfen Sie nach dem Einrichten oder Rotieren einer URL den **Letzten Ping** des Monitors, um sicherzugehen, dass er angekommen ist.

Wenn Ihr Job ein längeres Skript statt eines einzelnen Befehls ist, setzen Sie den Ping in die letzte Zeile und sorgen Sie dafür, dass das Skript bei einem Fehler vorzeitig abbricht:

```
#!/bin/sh
set -e
run_the_backup
verify_the_backup
curl -fsS https://pulse.example.com/api/heartbeats/ping/ihr-token
```

Mit `set -e` bricht jeder fehlgeschlagene Schritt das Skript ab, bevor es den Ping erreicht.

Wenn der Ping ausbleibt

Sobald das erwartete Intervall zuzüglich der Karenzzeit ohne Ping verstreicht, wechselt der Monitor auf **Ungesund** und Pulse öffnet einen nach dem Monitor benannten Vorfall. Ab diesem Punkt folgt der Vorfall wie jeder andere seiner Eskalationsrichtlinie, sodass die richtigen Personen über die gewohnten Kanäle benachrichtigt werden.

Der nächste eintreffende Ping stellt den Monitor wieder her und löst den Vorfall automatisch auf.

Aktivitätsverlauf

Pings werden im Aktivitätsverlauf des Monitors festgehalten. So beantworten Sie die Frage „Ist das Backup diesen Monat wirklich jede Nacht gelaufen?" direkt in Pulse. Aufeinanderfolgende Pings werden zu einem Eintrag zusammengefasst -- klicken Sie auf **Alle N anzeigen**, um ihn aufzuklappen.

Pings, die weniger als 30 Sekunden auseinanderliegen, werden nur einmal festgehalten. Ein Job, der kurz hintereinander erneut versucht zu pingen, erzeugt daher einen einzelnen Eintrag statt einen pro Versuch. Auf die Gesundheit des Monitors hat das keinen Einfluss: Jeder Ping setzt die Frist zurück, auch wenn er keinen neuen Eintrag erzeugt.

Da ein Heartbeat-Monitor bis zu einmal pro Minute gepingt werden kann, werden Ping-Einträge für die Aufbewahrungsdauer Ihrer Organisation gespeichert und danach entfernt. Statuswechsel -- also das Ausfallen und Wiederherstellen des Monitors -- bleiben als langfristiger Nachweis erhalten.

Hinweise

- Heartbeat-Monitore lassen sich nicht über den CSV-Import anlegen. Jeder von ihnen trägt eine eigene geheime URL, die an den pingenden Job verteilt werden muss -- deshalb werden sie einzeln angelegt.
- Heartbeat-Monitore lassen sich in geplante Berichte aufnehmen, indem Sie im Monitortyp-Filter des Berichts **Heartbeat** auswählen.
- Filtern, Stummschalten, Tags und alles andere, was für jeden Monitortyp gilt, finden Sie unter Monitore.

4.7 Anomalieerkennung

Ein Schwellwert-Monitor setzt voraus, dass Sie die Zahl kennen. Die Anomalieerkennung nicht: Pulse misst, was ein Datenpunkt normalerweise tut, und achtet dann darauf, dass er etwas anderes tut.

Das hilft genau dort, wo Schwellwerte nicht helfen. Niemand kennt die richtige Obergrenze für vierhundert Tags, und die alarmwürdigen sind oft genau die, an die niemand gedacht hat. Ein Datenpunkt, der unbemerkt abgedriftet, festgefahren oder verstummt ist, ist ein Fehler -- ob jemand eine Grenze dafür aufgeschrieben hat oder nicht.

Sie erhalten dabei keinen neuen Monitortyp. Jede Prüfung, die Pulse anlegt, ist ein gewöhnlicher Bedingungs-Monitor -- Sie können ihn öffnen, die Logik lesen, ändern oder löschen wie jeden anderen.

Einrichtung

Die Anomalieerkennung sitzt in der Datenpunkttabelle einer Datenquelle, direkt neben der Entscheidung, aus der sie folgt: Ein Datenpunkt, der einen Verlauf aufbaut, ist ein Datenpunkt, an dem sich ein Normalzustand lernen lässt.

Beim Einschalten von Verlauf. Schalten Sie **Verlauf** für einen Datenpunkt ein, werden seine Messwerte aufbewahrt -- und Pulse bietet daraufhin an, ihn zu überwachen. Lehnen Sie das Angebot ab, behält der Datenpunkt seinen Verlauf genau wie sonst auch.

Jederzeit danach. Jeder Datenpunkt, der bereits einen Verlauf aufbaut, trägt in seiner Zeile eine Schaltfläche **Anomalien erkennen**. Das ist der Weg für längst übernommene Datenpunkte und für die, bei denen das Angebot weggeklickt wurde.

Anschließend wählen Sie in beiden Fällen eine Empfindlichkeit, wählen die anzulegenden Prüfungen aus und bestätigen.

Pulse ermittelt, welche Prüfungen für genau diesen Datenpunkt sinnvoll sind. Was nicht möglich ist, wird mit Begründung genannt -- siehe Wann eine Prüfung wartet und wann sie nicht angeboten wird.

Sie müssen nicht auf die Messung warten

Jede Prüfung lässt sich sofort einschalten, auch an einem Datenpunkt, der vor einer Minute übernommen wurde. Die Prüfungen, die eine Messung brauchen, werden jetzt angelegt und mit **Aktiv nach der Messung** gekennzeichnet: Sie bleiben still und melden **Unbekannt**, statt gegen einen Normalzustand zu urteilen, den niemand gemessen hat, und beginnen nach der nächsten nächtlichen Messung von selbst zu überwachen. Sie müssen dafür nichts nachholen.

Beginnen Sie mit ausgeschalteten Prüfungen

Das Kontrollkästchen **Direkt aktivieren** ist standardmäßig aus, und es ausgeschaltet zu lassen ist der günstigste Weg herauszufinden, ob die Prüfungen zu Ihrer Anlage passen.

Ausgeschaltet laufen die Prüfungen mit und zeichnen auf, was sie getan hätten, ohne jemanden zu benachrichtigen. Schauen Sie in einer Woche nach, was ausgelöst worden wäre. Sieht es richtig aus, aktivieren Sie die Prüfungen aus der Monitorliste; ist es zu unruhig, senken Sie die Empfindlichkeit oder löschen Sie sie. Währenddessen wird niemand alarmiert.

Die fünf Prüfungen

Prüfung	Löst aus, wenn	Braucht eine Messung
Meldet keine Werte mehr	15 Minuten lang kein aktueller Messwert eingeht	Nein
Außerhalb des normalen Bereichs	Der Messwert den üblichen Bereich verlässt und draußen bleibt	Ja
Ändert sich nicht mehr	Weiterhin gemeldet wird, der Wert sich aber nicht bewegt	Ja
Ungewöhnliche Bewegung	Deutlich stärker geschwankt oder gestiegen wird als bei diesem Datenpunkt üblich	Ja
Entfernt sich von seiner Referenz	Das Niveau des letzten Tages hat sich von dem entfernt, was beim Einrichten festgehalten wurde	Ja

Meldet keine Werte mehr funktioniert immer. Diese Prüfung braucht keine Messung und steht daher auch bei einem heute angelegten Datenpunkt zur Verfügung -- und sie ist es, die das Schweigen der anderen aussagekräftig macht. Ein Datenpunkt, für den sich kein Normalbereich bilden ließ, wird weiterhin auf Verstummen überwacht; so bleiben „nichts alarmiert" und „nichts schaut hin" unterscheidbare Zustände.

Ändert sich nicht mehr ist nicht dasselbe wie **Meldet keine Werte mehr**, und der Unterschied zählt, wenn Sie nachts davon geweckt werden. Ein feststehender Wert bedeutet: Der Datenpunkt meldet weiterhin, und die Zahl dahinter ist eingefroren -- ein festsitzendes Ventil, ein eingefrorener Scan-Zyklus, ein zwischengespeicherter Wert. Das Gerät ist in Ordnung, die Messung nicht.

Ungewöhnliche Bewegung deckt einen schnellen Anstieg und eine unruhige Schwingung mit einer Prüfung ab. Beides ist dieselbe Aussage über das Zeitfenster -- es hat deutlich mehr Bereich überstrichen als üblich -- und eine Trennung bräuchte eine Richtung, die diese Prüfung bewusst ignoriert.

Entfernt sich von seiner Referenz erkennt langsame Veränderungen, die die anderen Prüfungen als normal lernen würden. Diese Prüfungen aktualisieren ihre Messungen jede Nacht und nennen die jüngste Geschichte normal; ein Datenpunkt, der sich über Wochen langsam verschoben hat, sieht für sie unverändert aus. Die Drift-Prüfung vergleicht stattdessen das Niveau des letzten Tages mit einer festen Referenz -- der Messung, wie sie beim Einrichten der Prüfung vorlag, oder der ersten überhaupt erhobenen, falls der Datenpunkt damals noch nicht vermessen war. Diese Referenz verschiebt sich nicht von selbst. Verwenden Sie sie für Anlagen, bei denen ein langsamer Trend zählt: eine Pumpe, die lautlos an Effizienz verloren hat, oder ein SPS-Ausgang, der sich von seinem ursprünglichen Betriebspunkt entfernt hat.

Empfindlichkeit

Einstellung	Bedeutung
Niedrig	Nur das Offensichtliche. Breiter Bereich, langes Halten vor dem Auslösen
Mittel	Der empfohlene Ausgangspunkt
Hoch	Erkennt früher und löst häufiger aus

Die Empfindlichkeit ändert zwei Dinge zugleich: wie weit außerhalb des Normalen als weit gilt, und wie lange es dort bleiben muss. Beides ist beabsichtigt -- eine Abweichung über zehn Sekunden ist meist der Prozess, eine über fünfzehn Minuten meist nicht.

Hoch ist keine flächendeckende Einstellung

Hoch ist eine sinnvolle Wahl für einen Datenpunkt, um den Sie sich ohnehin sorgen. Über einige Hundert Datenpunkte hinweg entstehen mehr Vorfälle, als jemand lesen kann -- und eine Warteschlange, die niemand liest, entspricht gar keiner Überwachung.

Die Empfindlichkeit einer bestehenden Prüfung ändern Sie, indem Sie ihren Bedingungs-Monitor öffnen und die Werte direkt bearbeiten.

Was Pulse misst

Jede Nacht misst Pulse den jüngsten Verlauf jedes Datenpunkts und speichert das Ergebnis: das Niveau, auf dem der Datenpunkt liegt, wie weit er üblicherweise davon abweicht, wie stark er sich innerhalb weniger Minuten bewegt und wie grob seine kleinste tatsächliche Änderung ist.

Daraus folgen drei Dinge, die Sie kennen sollten, bevor Sie eine fehlende Prüfung suchen:

- **Ein neuer Datenpunkt hat keine Messung.** Die darauf angewiesenen Prüfungen werden trotzdem angelegt -- sie melden bis zur nächsten nächtlichen Messung **Unbekannt** und beginnen danach zu überwachen. **Meldet keine Werte mehr** funktioniert sofort.
- **Eine Messung bleibt erhalten, bis eine bessere sie ersetzt.** Einen Monitor drei Wochen für Wartungsarbeiten zu pausieren zerstört seine Messung nicht.
- **Eine veraltete Messung stoppt die Prüfung.** Ist die nächtliche Messung über eine Woche ausgeblieben, melden die darauf angewiesenen Prüfungen **Unbekannt**, statt gegen eine Zahl zu urteilen, für die niemand mehr geradesteht.

Wann eine Prüfung wartet und wann sie nicht angeboten wird

Der Dialog gibt hier zwei verschiedene Antworten, und sie bedeuten das Gegenteil voneinander. Die eine ist eine Prüfung, die Sie haben; die andere eine, die Sie nicht haben können.

Aktiv nach der Messung

Die Prüfung ist angelegt und läuft. Sie hat nur noch nichts, woran sie messen kann, und meldet bis dahin **Unbekannt**. Das löst sich von selbst:

Begründung	Bedeutung
Pulse hat diesen Datenpunkt noch nicht vermessen	Normal für einen heute angelegten Datenpunkt. Nach der nächsten nächtlichen Messung beginnt die Überwachung
Noch zu wenig Verlauf, um zu sagen, was normal ist	Der Datenpunkt liefert Daten, aber zu wenige
Schwankt nicht so, dass sich ein Normalbereich darum bilden ließe	Ein Tag, das auf einem Wert steht oder zwischen wenigen springt. Beginnt es sich zu bewegen, beginnt die Prüfung zu greifen

Der letzte Fall ist der interessante. Etwa die Hälfte aller industriellen Tags liegt in einem Regelkreis und bewegt sich kaum -- und ein Bereich um ein Signal, das nicht schwankt, ist ein Bereich, außerhalb dessen alles liegt. Statt viertausend Alarme zu erzeugen, hält Pulse die Prüfung still, bis das Tag etwas zu messen gibt.

Für diesen Datenpunkt nicht verfügbar

Daran ändert keine Messung etwas, deshalb wird die Prüfung gar nicht erst angelegt:

Begründung	Bedeutung
Dieser Datenpunkt ist ein Ein/Aus-Signal	Ein Normalbereich hat für ein zweiwertiges Signal keine Bedeutung. **Meldet keine Werte mehr** wird weiterhin angeboten
Dieser Datenpunkt liefert keine Zahlen	Es kann nichts überwacht werden, auch **Meldet keine Werte mehr** nicht
Der Zustands-Datenpunkt liefert keine Zahlen	Das zum Schlüsseln der Prüfungen gewählte Zustandssignal ist kein numerischer Datenpunkt

Vorfälle

Ein Anomalie-Vorfall nennt den gemessenen Wert und das, wogegen gemessen wurde, statt „Die Bedingung ist eingetreten":

> **Kühlmitteltemperatur liegt außerhalb ihres normalen Bereichs** Gemessen 91,4, außerhalb des gelernten Normalbereichs 76,8–82,4, durchgehend seit 15 Min.

> **Vordruck ändert sich nicht mehr** Meldet weiterhin, steht aber seit 30 Min. auf 4,02.

> **Antriebsstrom hat sich von seiner Referenz entfernt** Niveau des letzten Tages 18,4, außerhalb des Referenzbereichs 11,2–15,6, der beim Einrichten dieser Prüfung festgehalten wurde.

Die Dauer ist die konfigurierte Haltezeit der Prüfung und damit eine Aussage über den Auslösemoment, keine mitlaufende Uhr -- die Vorfallsliste zeigt das laufende Alter separat.

Vorfälle aus diesen Prüfungen eskalieren über Ihre Eskalationsrichtlinie wie alle anderen und werden genauso bestätigt und behoben.

Eine nicht bewertbare Prüfung eskaliert nicht weiter

Verstummt der Datenpunkt hinter einem offenen Vorfall, steigt Pulse die Eskalationsrichtlinie nicht weiter hinauf, statt weitere Personen für etwas zu wecken, das es nicht mehr bestätigen kann. Der Vorfall bleibt offen, und die Eskalation wird von selbst fortgesetzt, sobald der Datenpunkt zurückkehrt.

Die erste Benachrichtigung wird davon nie zurückgehalten -- dass der Vorfall existiert, erfahren Sie immer.

Einschränkungen

Wissenswert, bevor Sie sich auf diese Prüfungen verlassen:

- **Keine Maßeinheiten.** Pulse weiß nicht, ob ein Tag Grad oder bar ist, daher nennt ein Vorfall nackte Zahlen.
- **Keine Schicht- oder Tageszeitabhängigkeit.** Ein Datenpunkt, dessen Normalzustand sich zwischen Tag- und Nachtschicht unterscheidet, wird als eine Grundgesamtheit gemessen -- sein Normalbereich wird dadurch breiter als der jeder einzelnen Schicht.
- **Zyklische Signale werden abgelehnt.** Ein Tag, das regelmäßig schwingt, lässt sich nicht durch einen festen Bereich beschreiben, und Pulse lehnt ab, statt zu raten.
- **Geplante Stillstände werden nicht erkannt.** Ein Anlagenstillstand sieht für diese Prüfungen wie ein Fehler aus. Pausieren Sie die Monitore, oder rechnen Sie mit Auslösungen.

4.8 Nachrichtenvorlagen

Eine Nachrichtenvorlage ist der eigene Text, den Pulse in die Vorfälle eines Monitors schreibt — anstelle einer allgemeinen Meldung. Sie wird einmal am Monitor hinterlegt und bei jedem Vorfall dieses Monitors verwendet.

Wo Sie eine Vorlage hinterlegen

Monitor	Wo die Nachricht geschrieben wird
CVE-Monitor	Die Spalte `incidentMessageTemplate` beim CSV-Import
Bedingungsmonitor	Das Feld **Was passiert ist** am Alarm-Knoten der Bedingung, im Bedingungseditor

Ein Heartbeat ist eine Datenquelle, und die Bedingung, über die er Vorfälle auslöst, ist ein Bedingungsmonitor wie jeder andere — dessen eigenes Bearbeitungsformular hat kein Nachrichtenvorlage-Feld, aber **Im Editor öffnen** auf dieser Seite öffnet den Bedingungseditor, wo dasselbe Feld **Was passiert ist** am Alarm-Knoten gilt.

Eine Bedingung kann mehrere Alarm-Knoten enthalten, jeder mit eigenem Vorfallnamen und eigener Beschreibung — so löst eine Bedingung für verschiedene Fehlerbilder unterschiedlich benannte Vorfälle aus. Siehe Bedingungen.

Die Nachricht schreiben

Die Nachricht wird genau so angezeigt, wie Sie sie schreiben — im Vorfall und in der Benachrichtigung dazu. Markdown für Hervorhebungen, Listen und Links wird unterstützt, siehe Markdown-Referenz.

Wirksame Nachrichten schreiben

- Halten Sie die Nachricht prägnant, aber informativ.
- Benennen Sie die Anlage, um die es geht, damit ein Bereitschaftshabender weiß, wohin er muss, ohne Pulse zu öffnen.
- Ergänzen Sie, welche Bedingung verletzt wurde und was zuerst zu prüfen ist.
- Verwenden Sie klare, nicht-technische Sprache für Operatoren. :::

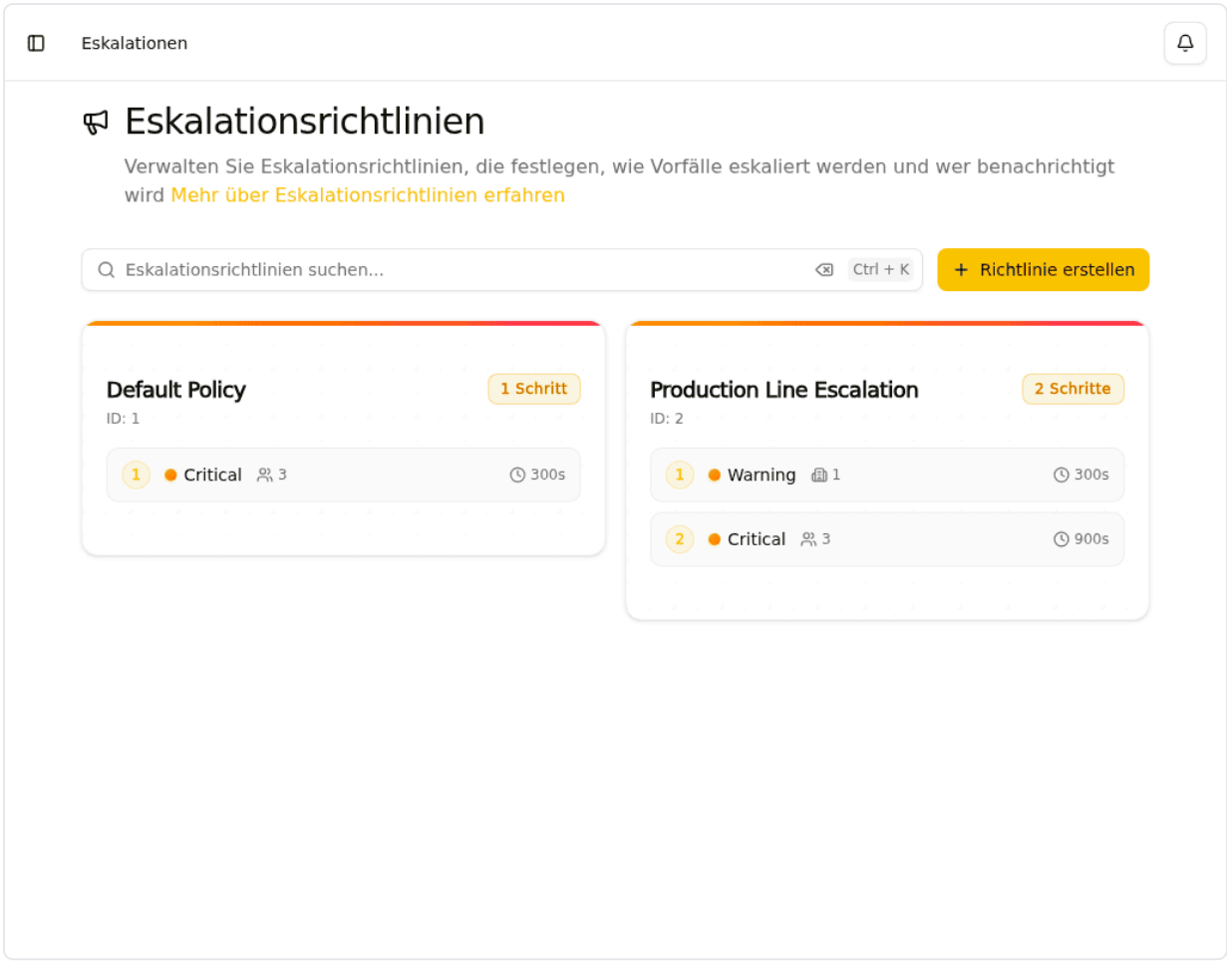
Verwandte Themen

- Markdown-Referenz
- Monitore
- OPC-UA-Konfiguration
- Siemens-S7-Konfiguration

Teil 5 · Alarmierung

5.1 Eskalationsrichtlinien

Eskalationsrichtlinien definieren, wie Vorfälle an Ihr Team kommuniziert werden. Sie legen fest, wer benachrichtigt wird, über welche Kanäle und in welcher Reihenfolge.



Wie Eskalation funktioniert

Wenn ein Vorfall erstellt wird, folgt Pulse der zugewiesenen Eskalationsrichtlinie:

1. Die erste Eskalationsstufe wird sofort (oder nach einer konfigurierten Verzögerung) ausgelöst
2. Benachrichtigungen werden an die angegebenen Empfänger über die Benachrichtigungskanäle des Schweregrads gesendet
3. Wenn der Vorfall nicht innerhalb der konfigurierten Zeit bestätigt wird, wird die nächste Stufe ausgelöst
4. Stufen können eine bestimmte Anzahl von Malen wiederholt werden, bevor zur nächsten Ebene eskaliert wird

Wird eine **Betriebszeiten**-Stufe außerhalb des konfigurierten Zeitfensters erreicht, pausiert die Eskalation und wartet. Im Aktivitätsfeed des Vorfalls wird das Ereignis **Eskalation pausiert — außerhalb der Betriebszeiten** vermerkt und angezeigt, wann die Eskalation fortgesetzt wird.

Eskalationsrichtlinie erstellen

1. Navigieren Sie zu **Eskalationen** in der Seitenleiste
2. Klicken Sie auf **Eskalationsrichtlinie erstellen**
3. Konfigurieren Sie den Richtliniennamen und die Stufen

Stufen konfigurieren

Es gibt zwei Arten von Stufen:

Benachrichtigungsstufe — Sendet Benachrichtigungen an die konfigurierten Empfänger.

Feld	Beschreibung
Schweregrad	Der Schweregrad, der die Benachrichtigungskanäle bestimmt
Anfangsverzögerung	Sekunden bis zur Auslösung dieser Stufe
Wiederholungen	Wie oft diese Stufe wiederholt wird, bevor eskaliert wird
Empfänger	Benutzer, Teams und/oder Bereitschaftspläne, die benachrichtigt werden

Betriebszeiten-Stufe — Pausiert die Eskalation, bis das konfigurierte Zeitfenster gilt. Erreicht die Eskalation diese Stufe außerhalb der konfigurierten Zeiten, wartet sie, bis die Betriebszeiten wieder beginnen, und fährt dann mit dem nächsten Schritt fort.

Feld	Beschreibung
Modus	Werktage, Täglich oder Benutzerdefiniert (tagesweiser Zeitplan)
Zeiten	Start- und Endzeit des Fensters
Umkehren	Wenn aktiviert, hält das Tor während der Zeiten an und fährt außerhalb davon fort

Betriebszeiten werden in der Zeitzone der Organisation ausgewertet (konfiguriert in Einstellungen).

Verwenden Sie eine Betriebszeiten-Stufe, um die Eskalation je nach Tageszeit unterschiedlich weiterzuleiten — beispielsweise das Bereitschaftsteam sofort zu alarmieren, den Manager aber nur während der Geschäftszeiten.

> **TIP**
>
> Beginnen Sie mit einem niedrigeren Schweregrad für die erste Stufe und eskalieren Sie zu höheren Schweregraden. Dies verhindert Benachrichtigungsmüdigkeit und stellt gleichzeitig sicher, dass kritische Probleme die richtigen Personen erreichen.

Was passiert, wenn niemand bestätigt

Nachdem alle Eskalationsstufen durchlaufen wurden, können Sie konfigurieren, was Pulse tut, wenn niemand den Vorfall bestätigt hat:

- **Nicht wiederholen** -- Nach der letzten Stufe stoppen. Es werden keine weiteren Benachrichtigungen gesendet.
- **N-mal wiederholen** -- Die Eskalationssequenz bis zu N-mal neu starten (maximal 20). Jeder vollständige Zyklus durchläuft alle Stufen erneut.
- **Dann eskalieren an** -- Nach Erschöpfung der Wiederholungen an eine andere Eskalationsrichtlinie übergeben. Dies ermöglicht das Verketten von Richtlinien — beispielsweise eine Teamrichtlinie zweimal zu wiederholen und dann an eine Management-Richtlinie zu eskalieren.

Diese Einstellungen werden im Abschnitt **Was passiert, wenn niemand bestätigt** des Eskalationsrichtlinien-Formulars konfiguriert.

Die Detailseite einer bestehenden Richtlinie zeigt eine Zusammenfassung dieser Konfiguration.

Wenn ein gelöster Alarm zurückkehrt

Das **Wiedereröffnungsfenster** legt fest, was passiert, wenn derselbe Trigger-Monitor kurz nach dem Lösen eines Vorfalls erneut auslöst.

Einstellung	Verhalten
0 (deaktiviert)	Jeder erneute Alarm startet einen komplett neuen Vorfall mit eigenem Bearbeiter und Eskalation ab dem ersten Schritt

Einstellung	Verhalten
N Sekunden	Löst derselbe Alarm innerhalb von N Sekunden nach dem Lösen erneut aus, wird der ursprüngliche Vorfall wieder geöffnet, statt einen neuen anzulegen

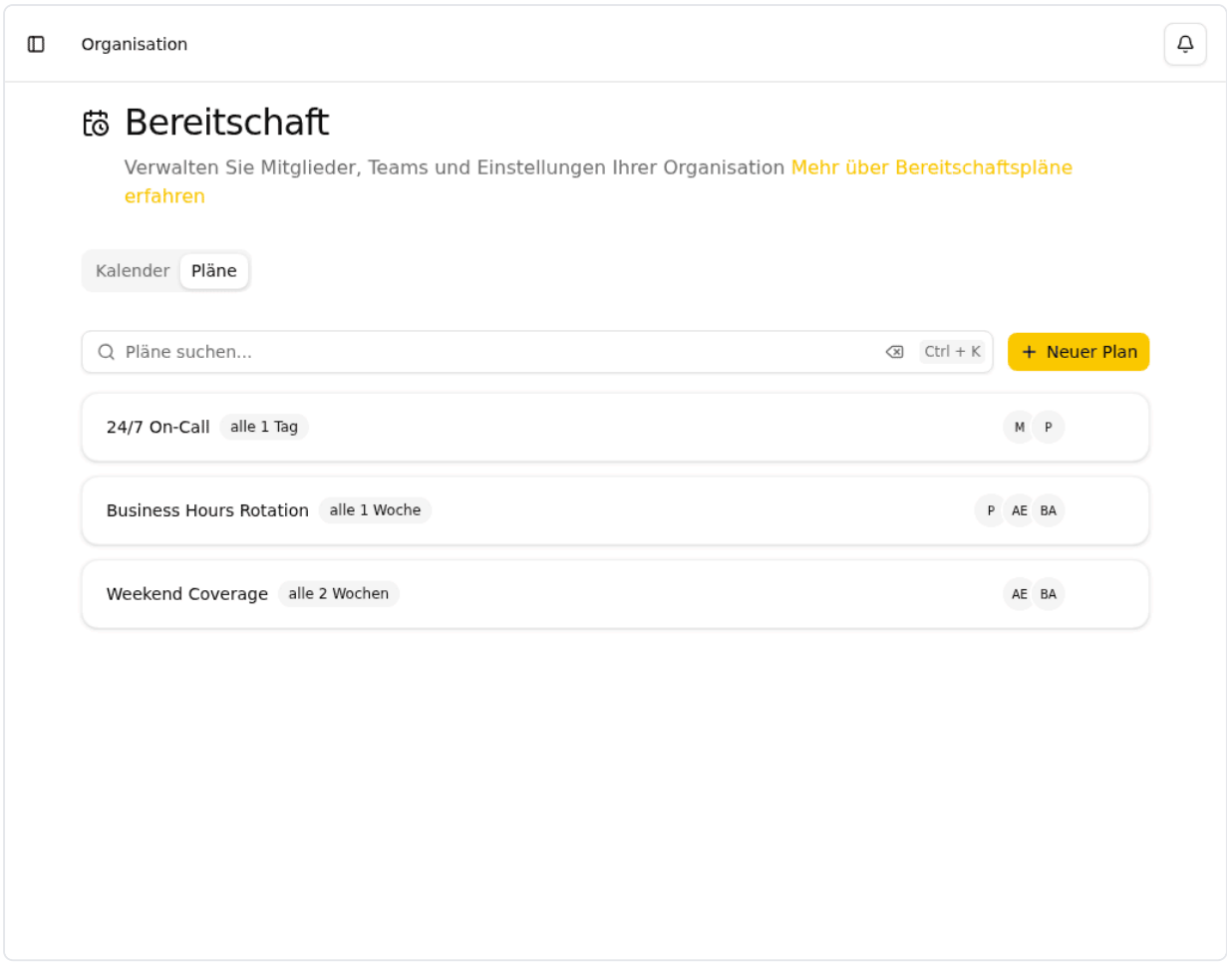
Bei einer Wiedereröffnung behält der Vorfall seinen Bearbeiter, seine Kommentare und seinen Eskalationsstand — niemand, der bereits bestätigt hat, wird erneut alarmiert. Die Lösungsbenachrichtigung wird ebenfalls um denselben Zeitraum zurückgehalten, sodass eine Wiedereröffnung innerhalb des Fensters nie als behoben gemeldet wird.

Richten Sie ein Wiedereröffnungsfenster ein, wenn eine flatternde Quelle ein Problem immer wieder auf mehrere Vorfälle aufteilt. Setzen Sie es auf 0, um bei jedem erneuten Auslösen immer einen neuen Vorfall zu starten.

Die Detailseite der Richtlinie zeigt eine Zusammenfassung dieser Einstellung unter **Wenn ein gelöster Alarm zurückkehrt**.

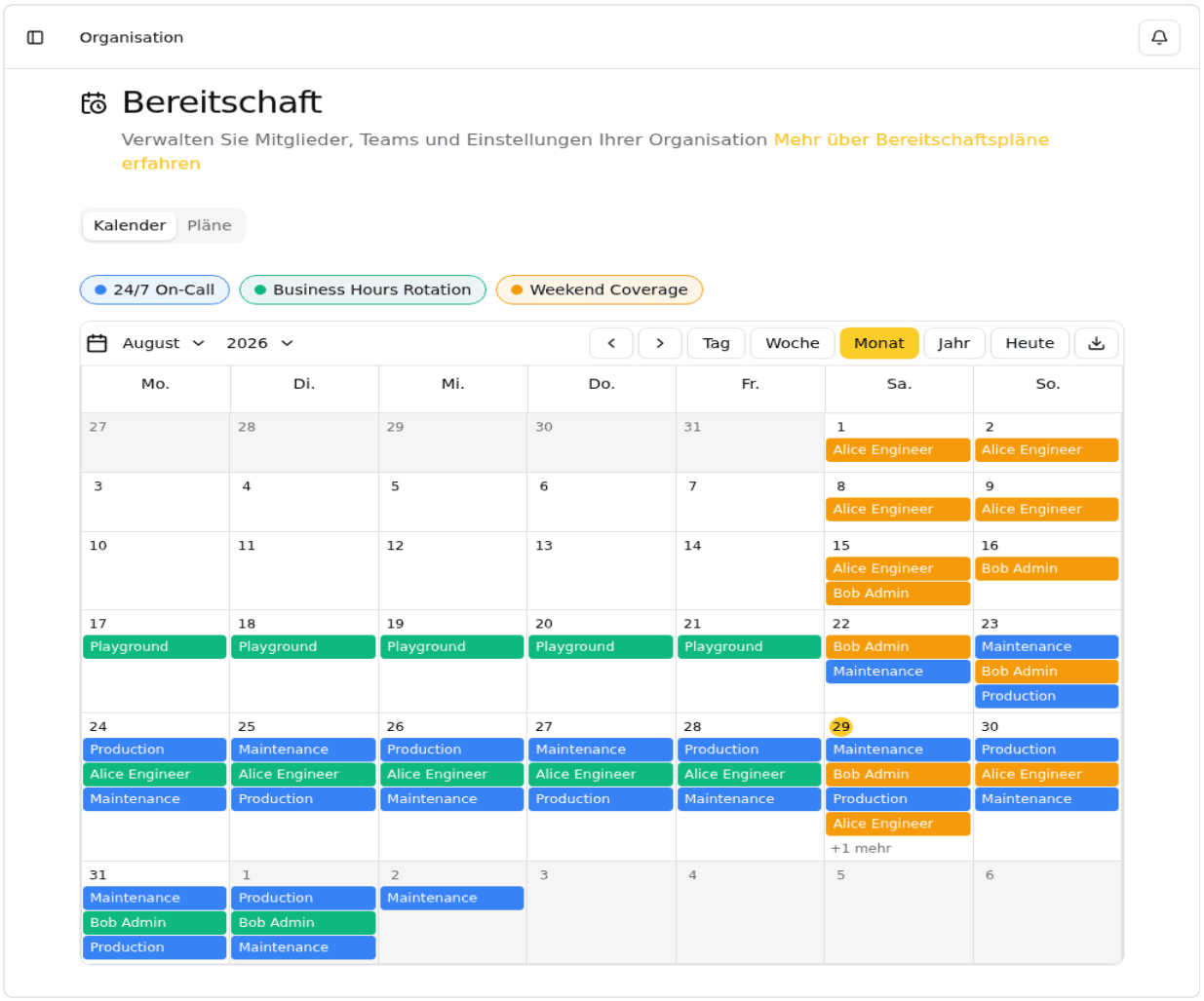
5.2 Bereitschaftspläne

Bereitschaftspläne legen fest, wer wann für die Reaktion auf Vorfälle verfügbar ist. Pläne werden auf Organisationsebene unter **Organisation > Bereitschaft** in der Seitenleiste verwaltet.



Reiter Kalender

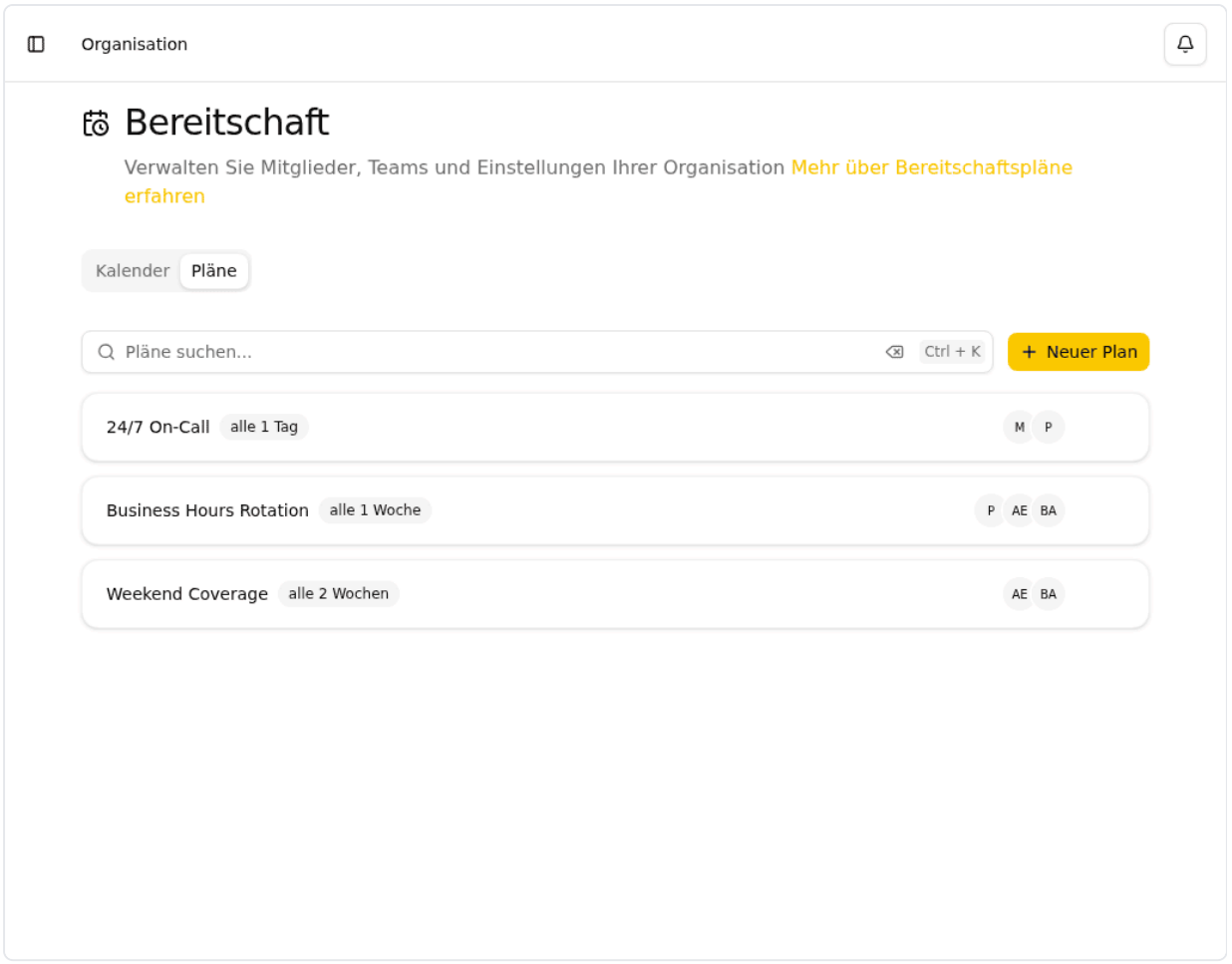
Der Reiter **Kalender** bietet eine visuelle Übersicht aller Bereitschaftspläne Ihrer Organisation.



Über den Ansichtsumschalter kann der Kalender in der **Tages-**, **Wochen-**, **Monats-** oder **Jahresansicht** angezeigt werden. Die gewählte Ansicht wird in der URL gespeichert (z.B. `?view=month`), sodass Links geteilt oder als Lesezeichen gespeichert werden können, die den Kalender direkt in der gewünschten Ansicht öffnen. Auf mobilen Geräten wird oberhalb des Kalenders eine beschriftete **Ansicht**-Auswahlliste angezeigt; die Ansichtspräferenzen für Mobilgeräte und Desktop werden getrennt gespeichert, sodass ein Wechsel zur Tagesansicht auf dem Smartphone die Desktop-Einstellung nicht verändert.

Reiter Pläne

Der Reiter **Pläne** listet alle Bereitschaftspläne auf. Jeder Plan zeigt seinen Namen, das Rotationsintervall und die zugewiesenen Bereitschaftspersonen.



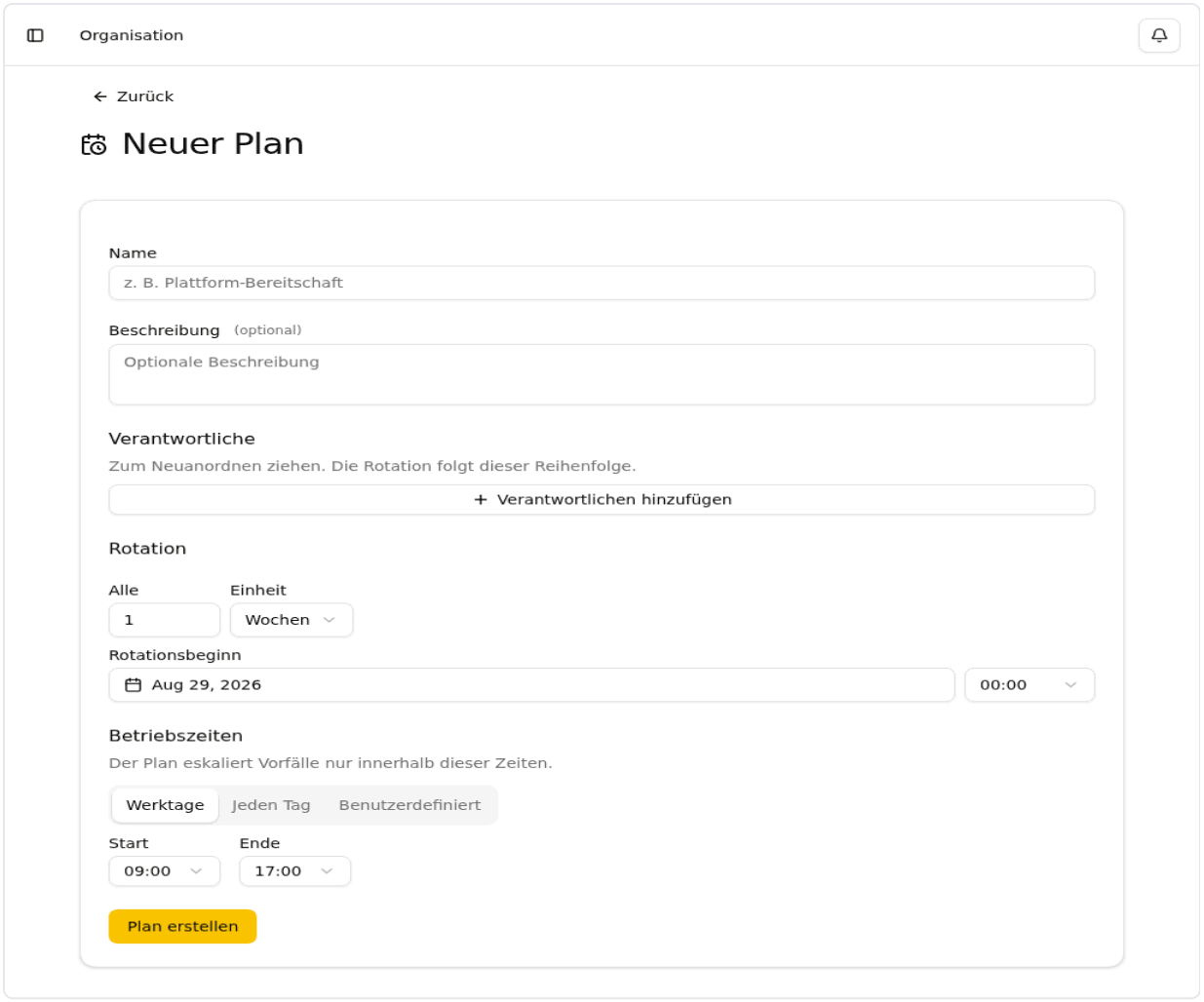
- **Suche** -- Pläne nach Namen filtern
- **Neuer Plan** -- Einen neuen Bereitschaftsplan erstellen (nur Admin)

Einen Plan erstellen

Klicken Sie auf **Neuer Plan**, um das Planformular zu öffnen. Konfigurieren Sie Folgendes:

Feld	Beschreibung
Name	Ein beschreibender Name für den Plan (z.B. "Plattform-Bereitschaft")
Beschreibung	Optionale Beschreibung
Bereitschaftler	Benutzer oder Teams, die an der Rotation teilnehmen. Ziehen zum Neuordnen.
Rotation	Wie oft die Bereitschaft rotiert (Minuten, Stunden, Tage oder Wochen)
Rotationsstart	Wann die erste Rotation beginnt

Feld	Beschreibung
Betriebszeiten	Zeitfenster, in dem der Plan aktiv ist. Außerhalb dieser Zeiten werden „Niemand im Bereitschaftsdienst"-Warnungen unterdrückt.



TIP

Die Rotation folgt der Reihenfolge der Bereitschaftsliste. Ziehen Sie Einträge, um die Rotationsreihenfolge zu ändern.

TIP

Wenn die **Betriebszeiten** auf `00:00–00:00` gesetzt sind (Start gleich Ende), wird dies als **ganzer Tag** interpretiert — der Plan ist für volle 24 Stunden aktiv.

INFO

Wenn Ihre Bereitschaft beginnt, benachrichtigt Pulse Sie per Push-Benachrichtigung und E-Mail: **„Sie sind jetzt in Bereitschaft für [Planname]."** Wenn Ihre Bereitschaft endet, erhalten Sie eine zweite Benachrichtigung und E-Mail: **„Ihre Bereitschaft für [Planname] ist beendet."** Die Benachrichtigungen werden in Ihrer bevorzugten Sprache gesendet. Wenn Sie aufeinanderfolgende Bereitschaftsschichten haben, erhalten Sie zu Beginn jeder Schicht eine Startbenachrichtigung. Die E-Mail enthält einen direkten Link zum Bereitschaftskalender für diesen Plan.

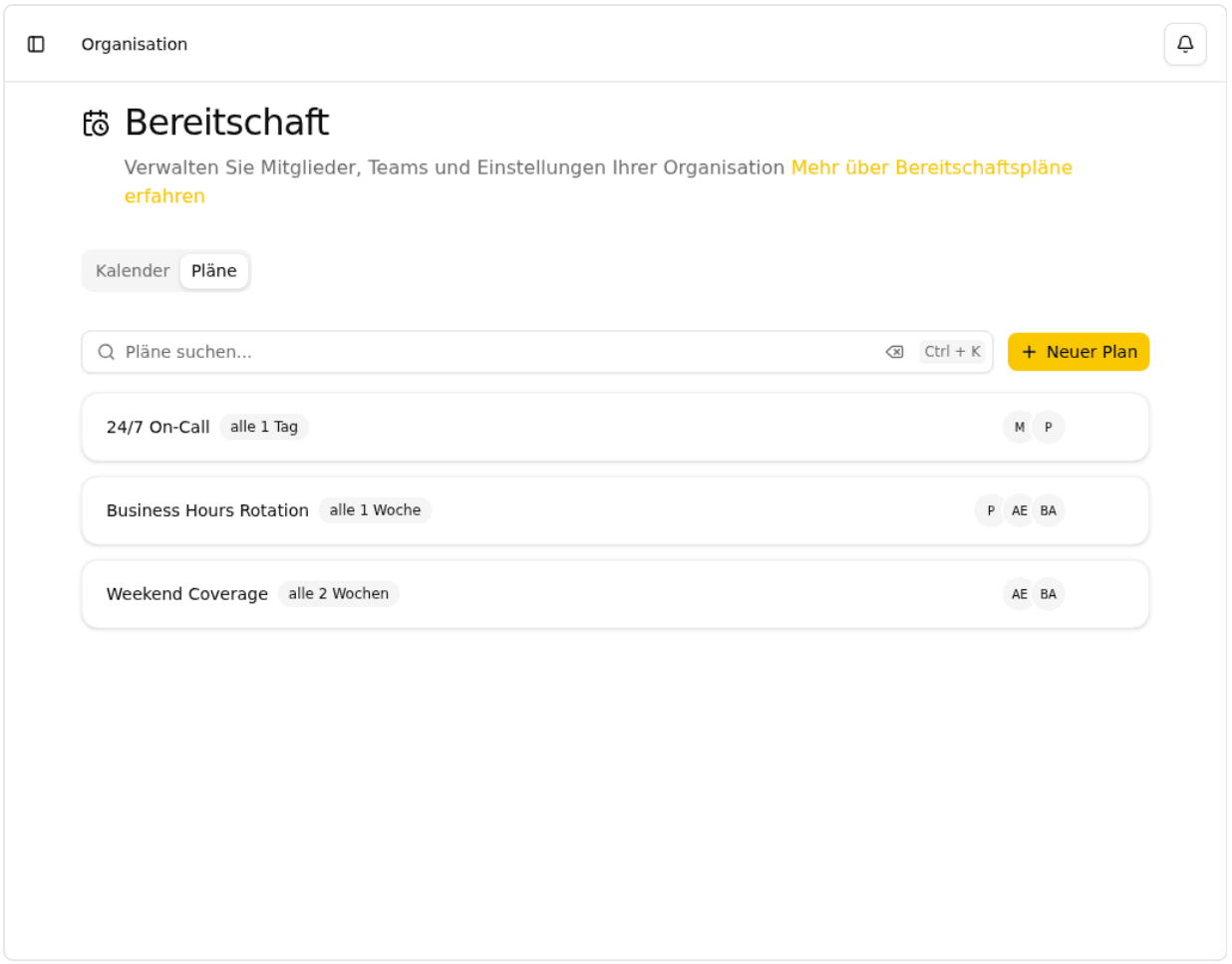
INFO

Wenn während der konfigurierten Betriebszeiten niemand im Bereitschaftsdienst ist, löst Pulse einen Systemvorfall mit dem Namen **„Niemand in Bereitschaft für [Planname]"** aus, um das Team zu informieren. Der Planname ist enthalten, damit Sie sofort erkennen können, welcher Plan eine Abdeckungslücke hat. Außerhalb der Betriebszeiten wird diese Warnung unterdrückt — Lücken in der Abdeckung sind dort erwartet und werden nicht gemeldet.

Pläne verwalten

Klicken Sie auf einen Plan, um die Detailseite mit zwei Reitern anzuzeigen:

- **Konfiguration** -- Plan-Name, Bereitschaftler, Rotation und Betriebszeiten bearbeiten



Wann eine Änderung wirksam wird

Am Ende des Konfigurationsformulars legt **Wirksam ab** fest, ab wann Ihre Änderungen gelten:

Auswahl	Was passiert
Jetzt (Standard)	Die neue Rotation, das neue Intervall und die neuen Betriebszeiten gelten ab dem Speichern.
Geplant	Die Änderung wartet bis zum gewählten Zeitpunkt und wird dann automatisch wirksam.

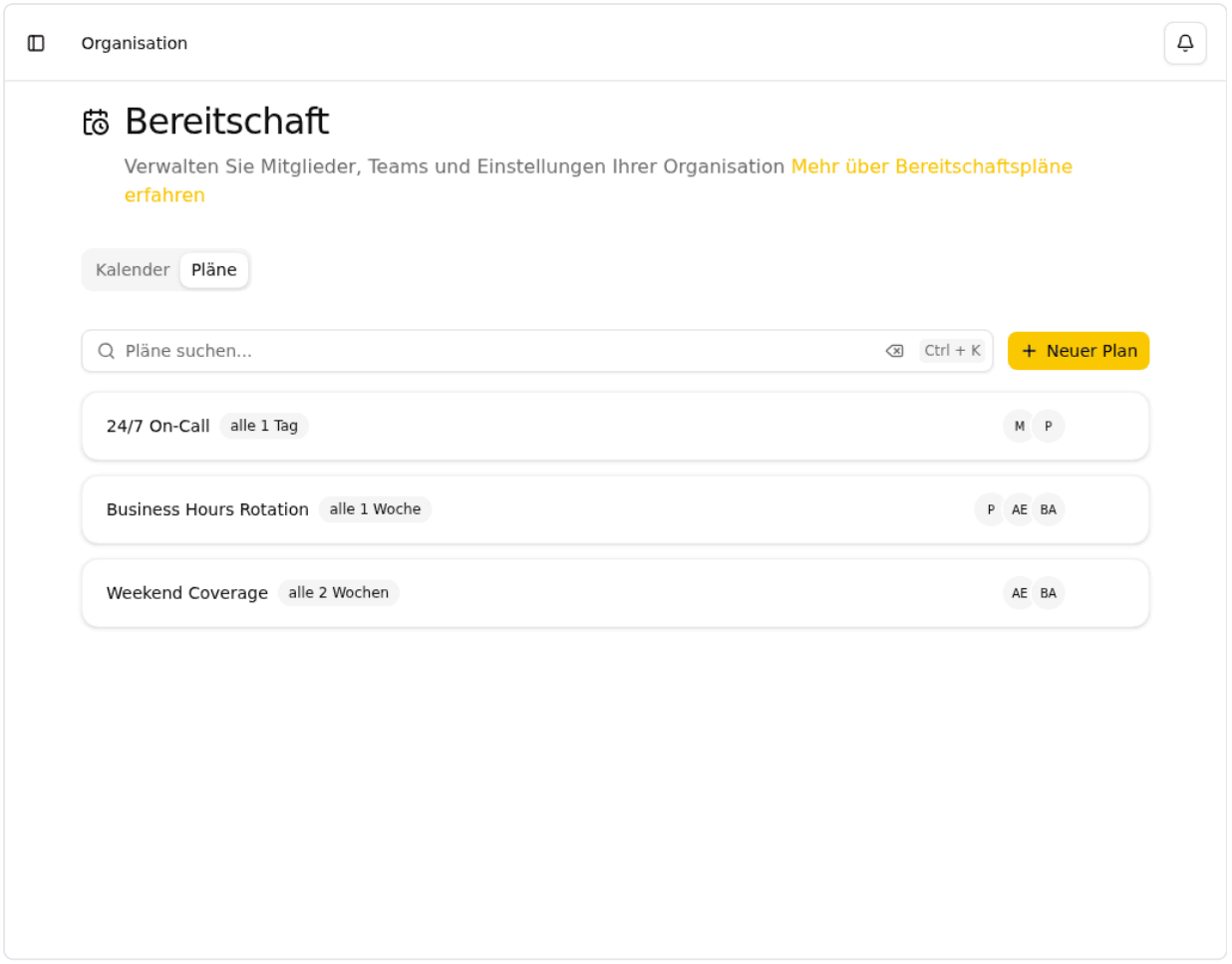
In beiden Fällen gilt: **Die Vergangenheit ändert sich nie.** Wenn Sie im Kalender zurückblättern, sehen Sie immer, wer damals tatsächlich Bereitschaft hatte — ermittelt aus den Einstellungen, die zu diesem Zeitpunkt galten, und nicht aus den heutigen. Die Reihenfolge der Rotation zu ändern, das Intervall anzupassen oder die Betriebszeiten einzuschränken wirkt sich ausschließlich auf die Zukunft aus.

Ein Plan kann **eine geplante Änderung** gleichzeitig vorhalten. Wenn bereits eine wartet, öffnet sich das Formular mit dieser Änderung und weist darauf hin — eine weitere Bearbeitung passt also diese Änderung an, statt eine zweite dahinter einzureihen.

Änderung verwerfen löscht sie; die aktuell gültige Rotation bleibt unberührt. Eine geplante Änderung erscheint im Kalender ab dem Zeitpunkt, an dem sie wirksam wird — Sie sehen ihre Auswirkung also, bevor sie eintritt.

> **INFO**
>
> Einen Plan umzubenennen oder seine Beschreibung zu bearbeiten wird immer sofort wirksam, unabhängig von der gewählten Option. Beides ändert nicht, wer Bereitschaft hat.

- **Überschreibungen** -- Temporäre Überschreibungen erstellen, um für einen bestimmten Zeitraum eine andere Bereitschaftsperson zuzuweisen. Überschreibungen sind nicht auf die Betriebszeiten des Plans beschränkt — sie gelten für das gesamte angegebene Zeitfenster.



Status-Badges für Überschreibungen:

- **Aktiv** -- Derzeit in Kraft
- **Bevorstehend** -- Für die Zukunft geplant
- **Vergangen** -- Bereits abgelaufen

Aktionen für Überschreibungen

Welche Aktionen für eine Überschreibung verfügbar sind, hängt davon ab, wo sie zeitlich liegt:

Status	Verfügbare Aktionen
Bevorstehend	Bearbeiten (nur Admin), Löschen
Aktiv	Ab jetzt ersetzen, Jetzt beenden
Vergangen	Keine – Vergangene Bereitschaft kann nicht geändert werden

Ab jetzt ersetzen — Weist die Bereitschaft ab dem aktuellen Moment bis zum Ende der aktiven Überschreibung neu zu. Ein Dialog fordert zur Auswahl der neuen Bereitschaftsperson auf. Der bereits abgelaufene Teil der Überschreibung bleibt unverändert.

Jetzt beenden — Beendet die aktive Überschreibung sofort. Die Bereitschaft kehrt ab diesem Zeitpunkt zur normalen Rotation zurück. Der abgelaufene Teil bleibt erhalten.

> **INFO**
>
> Überschreibungen, die bereits begonnen haben oder abgelaufen sind, können nicht gelöscht werden. Um eine aktive Überschreibung vorzeitig zu stoppen, verwenden Sie **Jetzt beenden** oder **Ab jetzt ersetzen**.

> **INFO**
>
> Die Aktionen **Ab jetzt ersetzen** und **Jetzt beenden** sind auch im Kalender-Ereignis-Popover verfügbar. Klicken Sie auf ein beliebiges Überschreibungsereignis im Kalender, um darauf zuzugreifen.

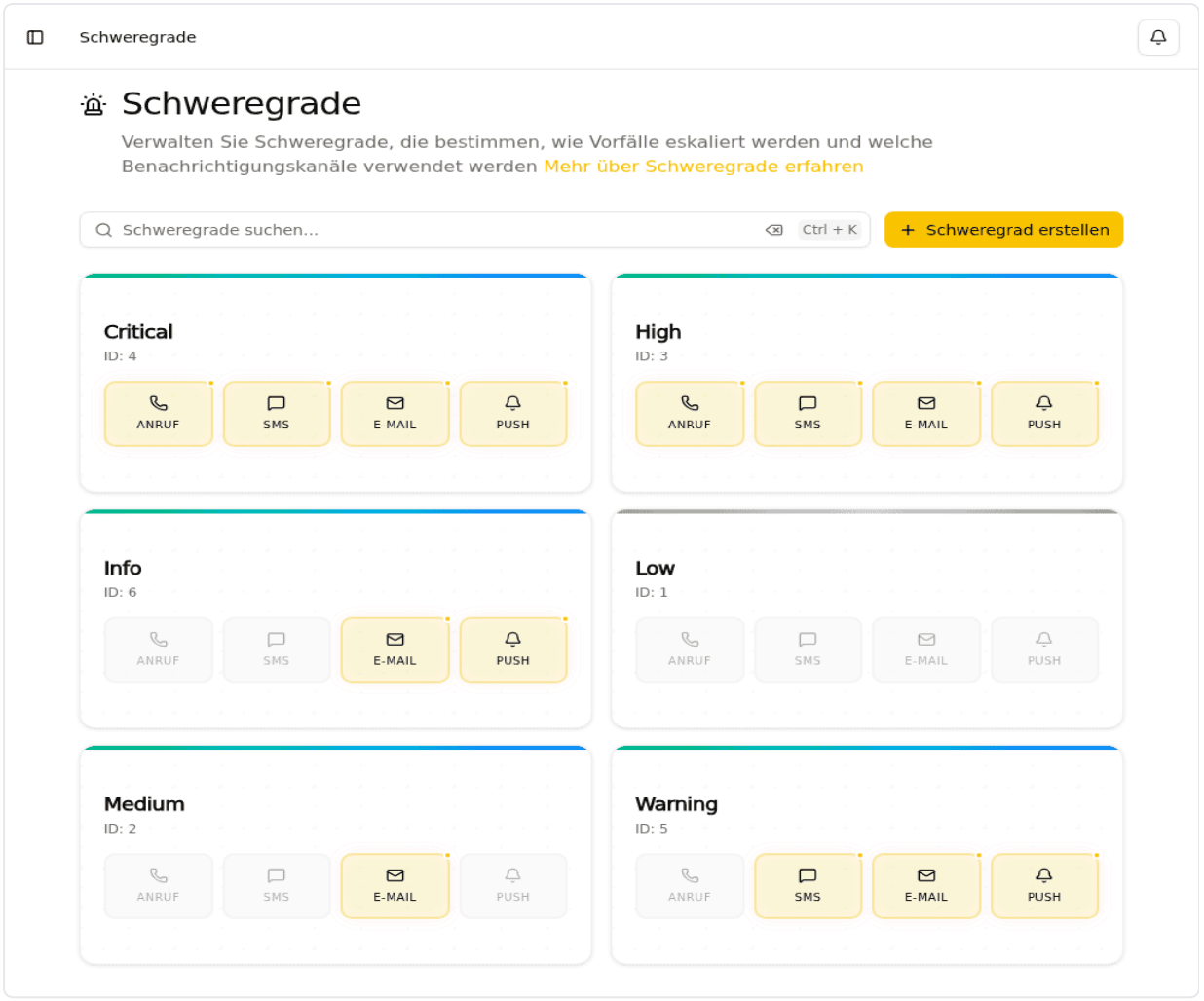
Verwandte Seiten

- Eskalationsrichtlinien -- Vorfall-Eskalation konfigurieren
- Teams -- Teammitgliedschaft verwalten

Teil 5 · Alarmierung

5.3 Schweregrade

Schweregrade definieren die Wichtigkeitsstufe von Vorfällen und bestimmen, welche Benachrichtigungskanäle bei der Eskalation verwendet werden.



Benachrichtigungskanäle

Jeder Schweregrad kann mit einem oder mehreren Benachrichtigungskanälen konfiguriert werden:

Kanal	Beschreibung
E-Mail	E-Mail-Benachrichtigungen an Empfänger senden
SMS	Textnachricht-Benachrichtigungen senden

Kanal	Beschreibung
Push	Mobile Push-Benachrichtigungen senden
Anruf	Telefonanruf-Benachrichtigungen auslösen

Push-Benachrichtigungen

Push-Benachrichtigungen werden über die Pulse Dispatch Mobile App zugestellt. Empfänger benötigen die App auf ihrem Smartphone — sie ist im App Store für iPhone und iPad verfügbar.

Schweregrad erstellen

1. Navigieren Sie zu **Schweregrade** in der Seitenleiste
2. Klicken Sie auf **Schweregrad erstellen**
3. Geben Sie einen Namen ein und wählen Sie die Benachrichtigungskanäle

TIP

Erstellen Sie Schweregrade, die zu den Vorfallreaktionsverfahren Ihrer Organisation passen. Gängige Muster sind: Niedrig (nur E-Mail), Mittel (E-Mail + SMS), Hoch (E-Mail + SMS + Anruf).

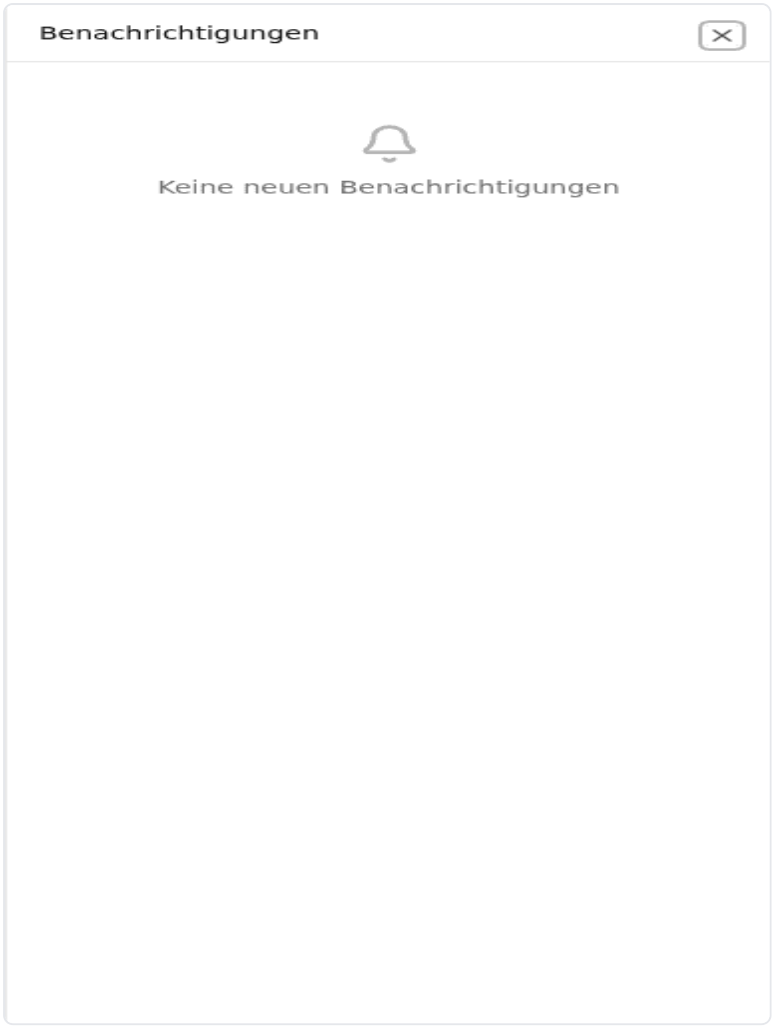
Schweregrade in Eskalationsrichtlinien

Schweregrade werden in Eskalationsrichtlinien-Stufen referenziert. Jede Stufe gibt einen Schweregrad an, der bestimmt, wie Empfänger in dieser Eskalationsstufe benachrichtigt werden.

Siehe Eskalationsrichtlinien für Details.

5.4 Benachrichtigungen

Das Benachrichtigungscenter zeigt Systemwarnungen und wichtige Aktualisierungen für Ihre Organisation an. Es ist über das Glockensymbol im Header auf jeder Seite zugänglich.



Benachrichtigungscenter öffnen

Klicken Sie auf das **Glockensymbol** oben rechts im Header, um das Benachrichtigungs-Drawer zu öffnen. Gibt es ungelesene Benachrichtigungen, wird auf dem Symbol ein rotes Badge mit der Anzahl angezeigt.

Benachrichtigungen verwalten

Jede Benachrichtigung zeigt:

- **Titel** — eine kurze Beschreibung des Ereignisses
- **Details** — zusätzlicher Kontext (falls vorhanden)
- **Zeit** — wie lange die Benachrichtigung bereits vorliegt

Um eine einzelne Benachrichtigung zu verwerfen, klicken Sie auf die ×-Schaltfläche auf der rechten Seite der Benachrichtigung.

Um alle Benachrichtigungen auf einmal zu verwerfen, klicken Sie auf **Alle verwerfen** am unteren Rand des Drawers.

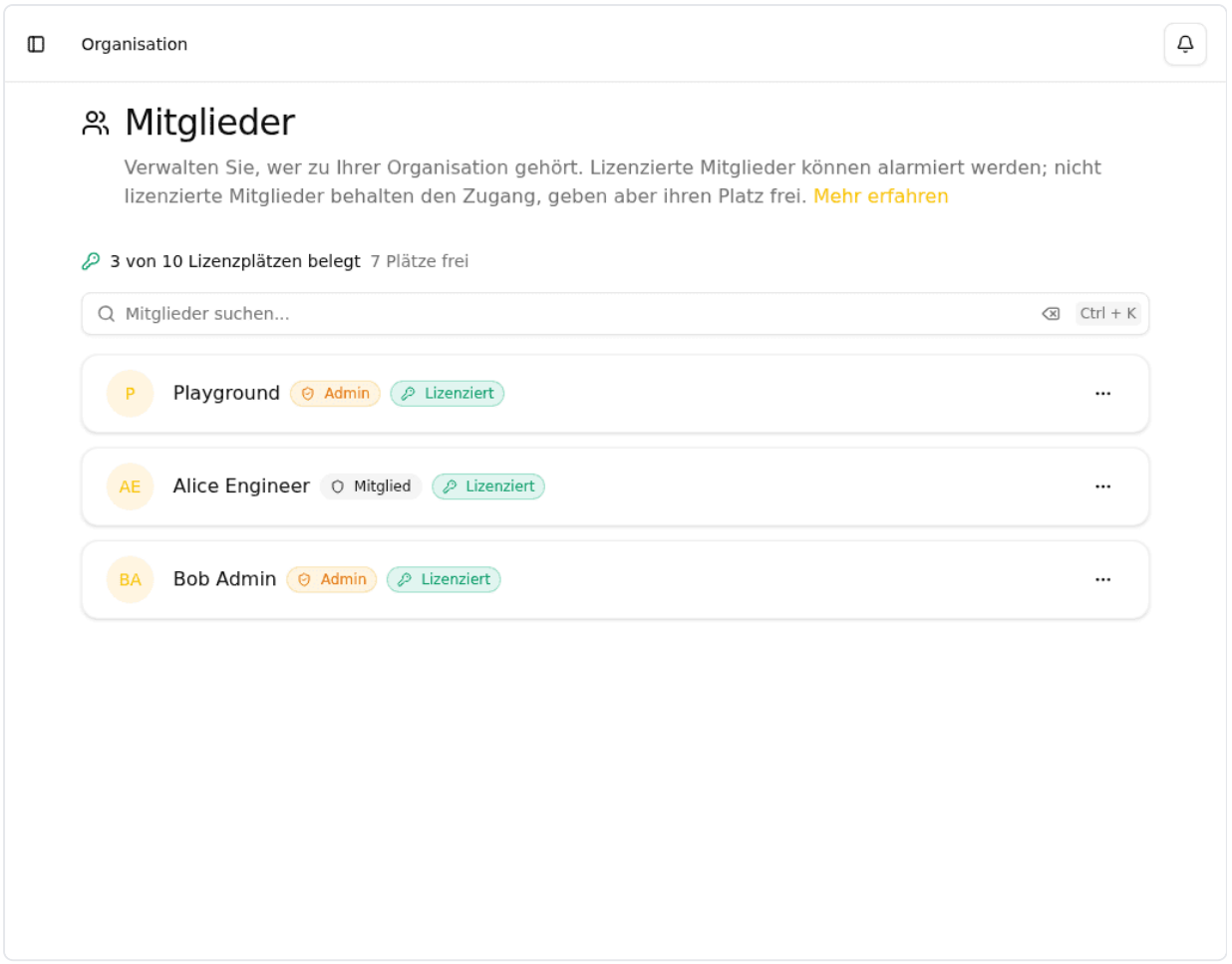
Verwandte Seiten

- Vorfälle — Aktive Vorfälle anzeigen und verwalten
- Bereitschaftspläne — Konfigurieren, wer Bereitschaftsbenachrichtigungen erhält
- Mobile Benachrichtigungen — Bedeutung der Symbole in Push-Benachrichtigungen

Teil 6 · Verwaltung

6.1 Mitglieder & Rollen

Pulse verwendet ein rollenbasiertes Zugriffskontrollsystem, das um Organisationen und Teams organisiert ist. Die Seite **Mitglieder** zeigt alle Benutzer Ihrer Organisation mit Anzeigenamen und Rollen.



- **Suche** -- Filtern Sie die Mitgliederliste nach Namen
- **Platzzusammenfassung** -- Zeigt, wie viele Lizenzplätze belegt sind und wie viele frei bleiben
- **Rollen-Badges** -- Jedes Mitglied zeigt ein **Admin**- oder **Mitglied**-Badge
- **Lizenz-Badges** -- Jedes Mitglied zeigt ein **Lizenziert**- oder **Nicht lizenziert**-Badge

Organisationsrollen

Rolle	Berechtigungen
Admin	Monitore, Tags, Schweregrade, Eskalationsrichtlinien und Teams erstellen und verwalten. Voller Konfigurationszugriff.
Mitglied	Monitore und Vorfälle anzeigen. Vorfälle bestätigen und lösen. Team-Informationen einsehen.

Mitgliederrollen verwalten

Als Admin klicken Sie auf das Aktionsmenü neben einem Mitglied, um:

- **Zum Admin befördern** -- Vollständigen Konfigurationszugriff gewähren
- **Zum Mitglied herabstufen** -- Auf Lesezugriff beschränken
- **Mitglied entfernen** -- Den Benutzer aus der Organisation entfernen

> **WARNING**
>
> Das Entfernen eines Mitglieds kann nicht rückgängig gemacht werden. Der Benutzer verliert sofort den Zugriff auf alle Organisationsressourcen.

Lizenzplätze

Jedes Mitglied ist entweder **lizenziert** oder **nicht lizenziert**. Ein lizenziertes Mitglied belegt einen der Lizenzplätze Ihrer Organisation; die Anzahl der Plätze wird durch Ihre Lizenz festgelegt.

Status	Bedeutung
Lizenziert	Belegt einen Platz und kann alarmiert werden -- erhält Benachrichtigungen und kann als Empfänger zu Eskalationsrichtlinien und Bereitschaftsplänen hinzugefügt werden.
Nicht lizenziert	Behält den Zugang zum Anmelden und Ansehen der Konfiguration, gibt aber den Platz frei und wird nie alarmiert. Kann nicht zu Eskalationsrichtlinien oder Plänen hinzugefügt werden.

Die Mitgliederseite zeigt, wie viele Plätze belegt sind und wie viele frei bleiben. Wenn alle Plätze belegt sind, wird das Zuweisen einer Lizenz an ein bestehendes, nicht lizenziertes Mitglied blockiert, bis Sie einen Platz freigeben oder das Limit erhöhen. Das Annehmen

einer Einladung ist weiterhin möglich — das neue Mitglied tritt ohne Lizenz bei, anstatt abgewiesen zu werden. Sie können ihm eine Lizenz zuweisen, sobald ein Platz frei wird.

Lizenzstatus eines Mitglieds ändern

Verwenden Sie als Admin das Aktionsmenü neben einem Mitglied, um **Lizenz zuweisen** oder **Lizenz entfernen** auszuwählen. Das Entfernen einer Lizenz wird verweigert, solange das Mitglied direkt als Empfänger auf einer Eskalationsrichtlinie oder einem Bereitschaftsplan genannt wird -- entfernen Sie zuerst diese Verweise.

Team-Rollen

Rolle	Fähigkeiten
Team-Admin	Teammitglieder und Team-Einstellungen verwalten
Team-Mitglied	Am Team teilnehmen und Benachrichtigungen erhalten

---

Benutzer einladen

Team-Admins können neue Benutzer in ihr Team einladen:

1. Navigieren Sie zur Team-Detailseite
2. Kopieren Sie den Einladungslink
3. Teilen Sie den Link mit der Person, die Sie einladen möchten
4. Der eingeladene Benutzer kann ein neues Konto erstellen oder sich mit einem bestehenden anmelden

> **TIP**
>
> Benutzer, die einen Einladungslink erhalten, werden aufgefordert, sich entweder anzumelden oder ein neues Konto zu erstellen, bevor sie dem Team beitreten.

Organisation erstellen

Bei der erstmaligen Registrierung werden Sie aufgefordert, eine Organisation zu erstellen. Sie müssen angeben:

- **Organisationsname** -- Ein beschreibender Name für Ihre Organisation
- **Zeitzone** -- Die Standard-Zeitzone für Datums-/Zeitanzeigen

Organisation wechseln

Wenn Sie mehreren Organisationen angehören, können Sie über das Benutzermenü in der Seitenleiste zwischen ihnen wechseln.

1. Klicken Sie auf Ihren Namen in der unteren linken Ecke der Seitenleiste
2. Wählen Sie **Organisation auswählen**
3. Wählen Sie die Organisation, in der Sie arbeiten möchten

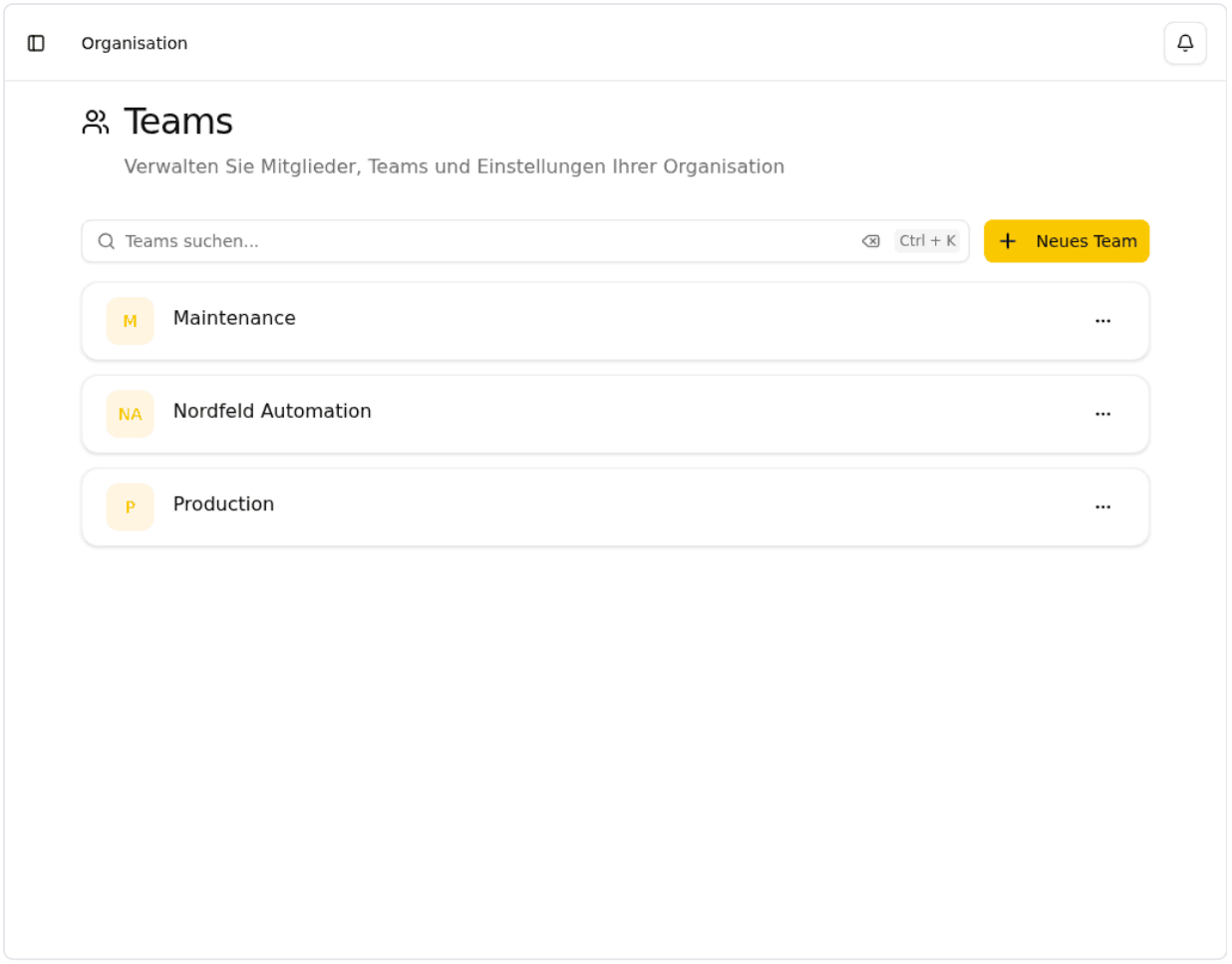
Verwandte Seiten

- Teams -- Teammitgliedschaft verwalten
- Organisationseinstellungen -- SMTP-Server und Webhooks
- Lizenzen -- Lizenzschlüssel, Plan-Limits und Nutzung
- Einstellungen -- Persönliche Benachrichtigungseinstellungen

Teil 6 · Verwaltung

6.2 Teams

Teams fassen Benutzer für die Benachrichtigungsweiterleitung und Zugriffskontrolle zusammen.



Team erstellen

1. Navigieren Sie zu **Teams** in der Seitenleiste
2. Klicken Sie auf **Team erstellen** (erfordert Admin-Rolle)
3. Geben Sie einen Teamnamen und eine Beschreibung ein

Teammitglieder verwalten

Auf der Team-Detailseite sehen Sie alle aktuellen Mitglieder mit ihren Rollen.

Mitglieder einladen

1. Öffnen Sie die Team-Detailseite
2. Klicken Sie auf **Einladungslink kopieren**
3. Teilen Sie den Link mit der Person, die Sie einladen möchten

Der eingeladene Benutzer sieht eine Einladungsseite, auf der er die Einladung durch Anmelden oder Erstellen eines neuen Kontos annehmen kann.

Teams in Eskalationsrichtlinien

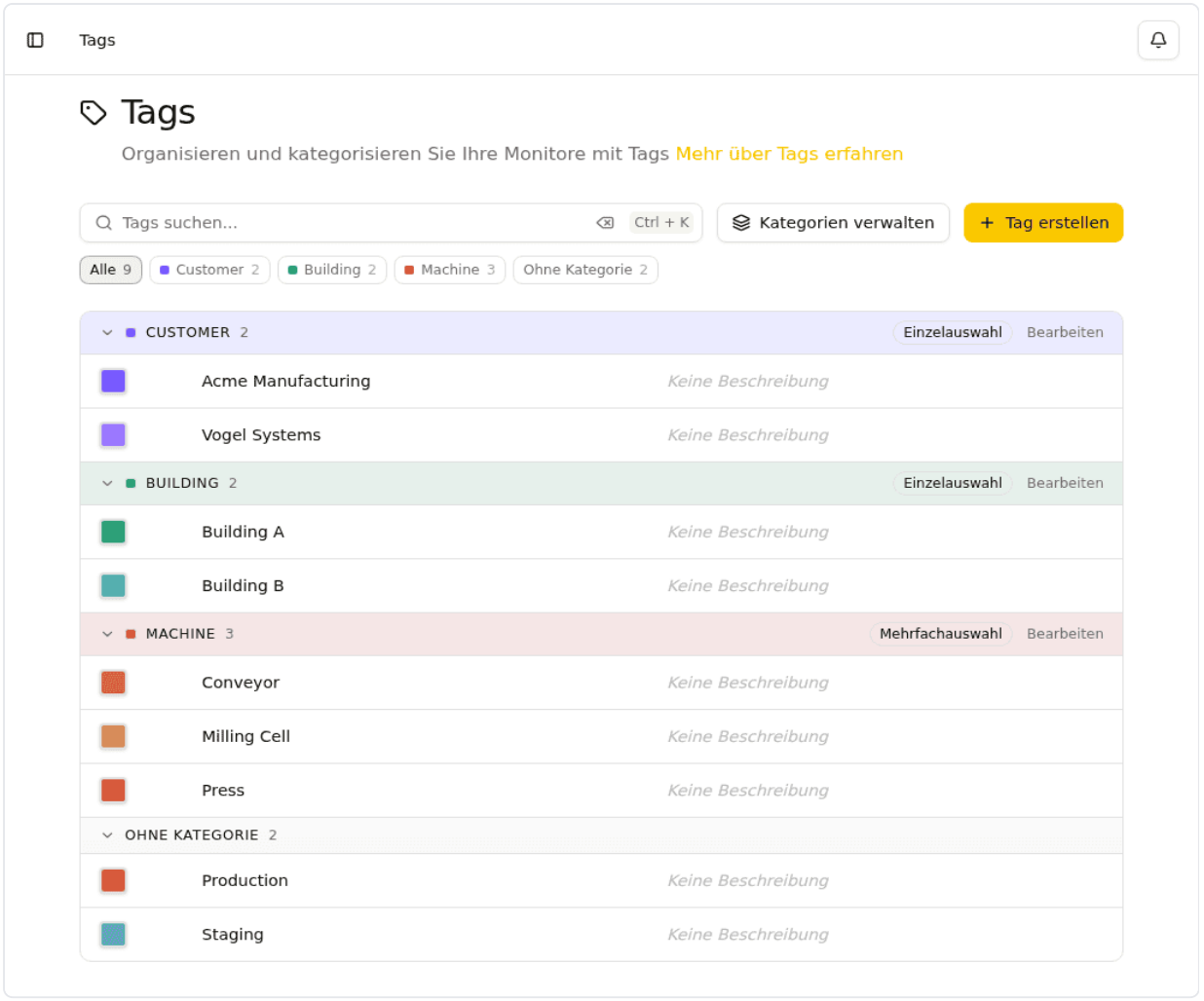
Teams können als Empfänger in Eskalationsrichtlinien-Stufen hinzugefügt werden. Wenn eine Eskalationsstufe ein Team anvisiert, werden alle Mitglieder dieses Teams benachrichtigt, die sich innerhalb ihrer Betriebszeiten befinden.

Siehe Eskalationsrichtlinien für Details zur Konfiguration teambasierter Benachrichtigungen.

Teil 6 · Verwaltung

6.3 Tags

Tags helfen Ihnen, Ihre Monitore zu organisieren und zu kategorisieren. Sie können Tags Monitoren zuweisen und die Monitor-Liste nach Tags filtern.



Tag-Liste

Wenn Tags zu Kategorien gehören, wird die Liste nach Kategorie gruppiert. Jede Gruppe zeigt den Kategorienamen und die Anzahl der Tags und kann durch Klicken auf den Gruppenheader ein- oder ausgeklappt werden. Eine Zeile mit Filterchips über der Liste ermöglicht die Einschränkung auf eine einzelne Kategorie. Bei der Suche nach Namen wechselt die Ansicht in eine flache alphabetische Liste mit einer Spalte **Kategorie**, damit Sie auf einen Blick sehen, zu welcher Kategorie jeder Tag gehört.

Tag erstellen

1. Navigieren Sie zu **Tags** in der Seitenleiste
2. Klicken Sie auf **Tag erstellen**
3. Konfigurieren Sie den Tag:

Feld	Beschreibung
Label	Der Anzeigename des Tags
Beschreibung	Optionale Beschreibung, wofür dieser Tag steht
Farbe	Eine Farbe zur visuellen Identifikation
Kategorie	Optionale Dimension, zu der dieser Tag gehört

Tag bearbeiten

Organisations-Admins können Label, Beschreibung und Farbe eines vorhandenen Tags bearbeiten. Klicken Sie auf einen Tag in der Liste, um die Detailseite zu öffnen, nehmen Sie Ihre Änderungen vor und klicken Sie auf **Änderungen speichern**.

Tag löschen

Organisations-Admins können einen Tag über die Detailseite löschen. Klicken Sie auf **Tag löschen**, bestätigen Sie die Aktion im Dialog, und der Tag wird dauerhaft entfernt.

> **WARNING**
>
> Ein Tag, der noch einem oder mehreren Monitoren zugewiesen ist, kann nicht gelöscht werden. Entfernen Sie den Tag zuerst von allen Monitoren und löschen Sie ihn danach.

Tags verwenden

Nach dem Erstellen von Tags können Sie diese Monitoren beim Erstellen oder Bearbeiten zuweisen. Auf der Monitor-Listenseite verwenden Sie den Tag-Filter, um Monitore mit bestimmten Tags schnell zu finden.

TIP

Verwenden Sie Tags, um Monitore nach Standort (z.B. "Gebäude A", "Linie 3"), nach Kritikalität (z.B. "Sicherheit", "Produktion") oder nach Gerätetyp zu gruppieren.

Tags in Kategorien organisieren

Sobald mehr als eine Handvoll Tags zusammenkommt, sortieren Sie diese in Kategorien — Kunde, Projekt, Standort. Die Tag-Auswahl gruppiert sie dann nach Dimension, und Filter lassen sich über mehrere Dimensionen hinweg kombinieren.

Siehe Tag-Kategorien.

6.4 Tag-Kategorien

Eine Tag-Kategorie ist eine Dimension, in die Sie Ihre Tags einsortieren — Kunde, Projekt, Standort, Linie. Die Tags selbst bleiben flach und unabhängig; die Kategorie sagt Pulse, welche Tags zur selben Frage gehören. So können Sie Ihre Monitore über mehrere Dimensionen gleichzeitig filtern.

Kategorien sind optional. Ein Tag ohne Kategorie erscheint als **Ohne Kategorie** und funktioniert unverändert weiter.

Wozu Kategorien

In einer Anlage mit 400 Monitoren entsteht schnell eine ungeordnete Liste aus 40 Tags — Kundennamen neben Linienbezeichnungen neben Kritikalitäten. Kategorien lösen das auf drei Wegen:

- **Tags sind dort gruppiert, wo Sie sie auswählen.** Die Tag-Auswahl und jeder Tag-Filter zeigen eine Gruppe pro Kategorie. "Welcher Kunde?" und "Welche Linie?" sind damit zwei getrennte Fragen statt einer langen Liste.
- **Filter kombinieren über Dimensionen hinweg.** Die Auswahl `Acme` unter Kunde zusammen mit `Linie 3` und `Linie 4` unter Standort beantwortet "alles, was ich für Acme auf Linie 3 oder 4 betreibe" in einem Filter.
- **Manche Dimensionen erlauben nur eine Antwort.** Ein Monitor gehört zu genau einem Kunden. Schalten Sie die Mehrfachauswahl für diese Kategorie ab, dann ersetzt ein zweiter Kunde den ersten — der Fehler kann gar nicht erst passieren.

> **TIP**
>
> Gute Kategorien sind die Achsen, nach denen Sie eine Tabelle sortieren würden: Kunde, Projekt, Standort, Gerätetyp. Alles, was den Zustand oder die Dringlichkeit eines Monitors beschreibt — etwa `Kritisch` —, bleibt meist besser ohne Kategorie oder wird über Schweregrade abgebildet.

Kategorie erstellen

Organisations-Admins können Kategorien erstellen.

1. Navigieren Sie zu **Tags** in der Seitenleiste

2. Klicken Sie auf **Kategorien verwalten**
3. Klicken Sie auf **Kategorie erstellen**
4. Konfigurieren Sie die Kategorie:

Feld	Beschreibung
Name	Die Dimension, für die diese Kategorie steht, z. B. Kunde, Projekt oder Standort
Beschreibung	Optionaler Hinweis, was in diese Kategorie gehört
Farbe	Eine Farbe zur visuellen Identifikation
Mehrere Tags pro Monitor zulassen	Aktiviert kann ein Monitor mehrere Tags dieser Kategorie tragen. Deaktiviert höchstens eines

Kategorienamen müssen innerhalb Ihrer Organisation eindeutig sein.

Tags einer Kategorie zuordnen

Ein Tag gehört zu höchstens einer Kategorie. Öffnen Sie einen Tag in der **Tags**-Liste und wählen Sie im Feld **Kategorie** eine Kategorie aus, oder belassen Sie es bei **Ohne Kategorie**.

Tag-Bezeichnungen müssen nur innerhalb ihrer Kategorie eindeutig sein. Sie können `Linie 3` unter Standort und `Linie 3` unter Projekt anlegen, ohne dass es zu einem Konflikt kommt.

Einzelauswahl und Mehrfachauswahl

Der Schalter **Mehrere Tags pro Monitor zulassen** bestimmt, wie sich die Tag-Auswahl für diese Kategorie verhält:

- **Mehrfachauswahl** (Standard) — ein Monitor kann beliebig viele Tags der Kategorie tragen. Sinnvoll für Dimensionen, die sich tatsächlich stapeln, etwa Gerätetyp.
- **Einzelauswahl** — ein neu gewähltes Tag ersetzt das bisher gewählte Tag derselben Kategorie, wie bei einem Radiobutton. Sinnvoll für Dimensionen mit genau einer richtigen Antwort, etwa Kunde.

Über Dimensionen hinweg filtern

Kategorien ändern, wie der Tag-Filter in den Listen für Monitore, Vorfälle und Schwachstellen Ihre Auswahl kombiniert:

- **Innerhalb einer Kategorie werden Tags mit ODER verknüpft.** `Linie 3` und `Linie 4` unter Standort trifft auf Monitore beider Linien zu.
- **Über Kategorien hinweg wird mit UND verknüpft.** Ergänzen Sie `Acme` unter Kunde, schränkt das die Treffer auf die Monitore von Acme auf Linie 3 oder 4 ein.

Genau das macht mehrere Dimensionen gleichzeitig nutzbar: Jede zusätzliche Kategorie schränkt das Ergebnis ein, jedes zusätzliche Tag innerhalb einer Kategorie erweitert es.

Geführte Zuweisung

Sowohl der Tag-Filter als auch die Tag-Auswahl am Monitor sortieren die Tags danach, was bereits im Einsatz ist. Sobald Sie ein Tag auswählen, rücken alle Tags, die auf denselben Monitoren vorkommen, mit der Anzahl der passenden Monitore an den Anfang ihrer Gruppe. Tags ohne gemeinsame Verwendung rutschen darunter und werden ausgegraut — anklickbar bleiben sie, sodass Sie die Auswahl jederzeit erweitern können.

In der Praxis: Wählen Sie `Acme` unter Kunde, zeigt die Gruppe Standort sofort die Standorte, die Acme tatsächlich hat, vor denen, die Acme nicht hat.

> **TIP**
>
> Die Zahlen erscheinen auch ohne Auswahl — dann zeigt jedes Tag, wie viele Monitore es tragen. Ein schneller Weg, um ungenutzte Tags zu finden.

Kategorie bearbeiten und löschen

Organisations-Admins können Name, Beschreibung, Farbe und die Mehrfachauswahl einer Kategorie auf deren Detailseite ändern.

Beim Löschen einer Kategorie bleiben ihre Tags erhalten. Sie werden zu **Ohne Kategorie**; die Monitore behalten ihre Zuweisungen. Sie können die Tags jederzeit einer anderen Kategorie zuordnen.

WARNING

Das Löschen einer Kategorie kann nicht rückgängig gemacht werden. Ihre Tags verlieren die Gruppierung und müssen einzeln neu zugeordnet werden.

Weiterführend

- Tags — Tags erstellen, bearbeiten und zuweisen
- Monitore — Tags beim Erstellen oder Bearbeiten eines Monitors zuweisen

Teil 6 · Verwaltung

6.5 Organisationseinstellungen

Die Organisationseinstellungen ermöglichen Admins die Konfiguration von Infrastruktur-Optionen. Navigieren Sie zu **Organisation > Einstellungen** in der Seitenleiste.

Allgemein

Der Reiter **Allgemein** enthält die Einstellungen der Organisation selbst. Er wird angezeigt, wenn Sie **Organisation > Einstellungen** öffnen.

Automatisches Onboarding

Normalerweise treten Kolleginnen und Kollegen Ihrer Organisation über einen Team-Einladungslink bei. Das automatische Onboarding erspart diesen Schritt: Aktivieren Sie **Alle aufnehmen, die sich mit einer @Ihre-Domain-Adresse registrieren**, und wer ein Pulse-Konto mit einer E-Mail-Adresse Ihrer Firmendomain anlegt, wird bei der Registrierung automatisch Mitglied dieser Organisation.

Die Domain geben Sie nicht selbst ein — Pulse übernimmt sie aus Ihrer eigenen E-Mail-Adresse. Eine Organisation kann damit nur eine Domain beanspruchen, die ihre Admins auch tatsächlich verwenden.

Situation	Was Sie sehen
Ihre Adresse liegt auf einer Firmendomain	Das Kontrollkästchen mit dieser Domain
Ihre Adresse liegt bei einem öffentlichen Anbieter (Gmail, GMX …)	Das Kontrollkästchen ist deaktiviert — ein öffentlicher Anbieter sagt nichts darüber aus, mit wem Sie zusammenarbeiten
Sie sind Mitglied, nicht Admin	Die aktuelle Einstellung, schreibgeschützt

Vor dem Aktivieren sollten Sie wissen:

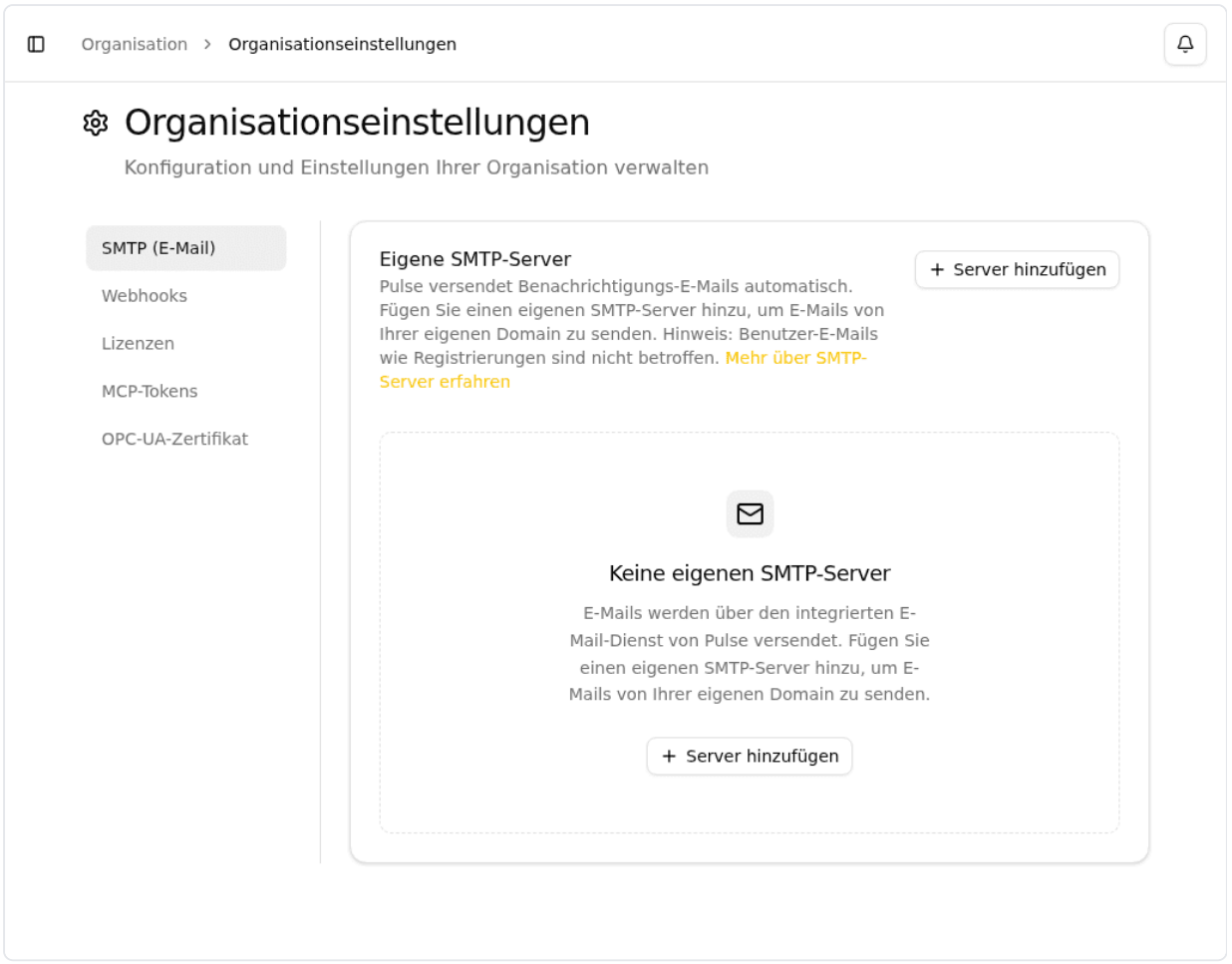
- Neue Mitglieder erhalten immer die Rolle **Mitglied**, nie Admin-Rechte. Rollen ändern Sie unter Mitglieder & Rollen.
- Die Einstellung gilt **nur für neue Registrierungen**. Bestehende Pulse-Konten sind nicht betroffen, und ein späteres Deaktivieren entfernt niemanden, der zwischenzeitlich beigetreten ist.

- Ein neues Mitglied **erhält eine Lizenz, sofern eine frei ist**, und wird damit ab dem ersten Tag alarmiert. Sind alle Plätze belegt, tritt es ohne Lizenz bei — es kann sich anmelden und die Konfiguration einsehen, wird aber erst alarmiert, wenn Sie unter Mitglieder & Rollen eine Lizenz zuweisen. Abgewiesen wird wegen eines fehlenden Platzes niemand.
- Beigetretene Mitglieder entfernen Sie unter Mitglieder & Rollen wie jedes andere Mitglied.

> **WARNING**
>
> Wer eine Adresse auf Ihrer Mail-Domain registrieren kann, wird Mitglied, sieht Ihre Monitore und deren Konfiguration und belegt einen Ihrer Lizenzplätze, sofern noch welche frei sind. Lassen Sie die Option deaktiviert, wenn Adressen Ihrer Domain auch an Personen außerhalb Ihres Teams vergeben werden.

Eigene SMTP-Server (E-Mail)

Konfigurieren Sie eigene SMTP-Server für ausgehende E-Mail-Benachrichtigungen.



Pulse versendet Benachrichtigungs-E-Mails automatisch über den integrierten E-Mail-Dienst. Fügen Sie einen eigenen SMTP-Server hinzu, um E-Mails von Ihrer eigenen Domain zu senden. Sind mehrere eigene SMTP-Server konfiguriert, probiert Pulse sie **in der angezeigten Reihenfolge** und verwendet den ersten, der erfolgreich antwortet.

Klicken Sie auf **Server hinzufügen**, um einen neuen SMTP-Server zu konfigurieren:

Feld	Beschreibung
Host	SMTP-Server-Hostname
Port	SMTP-Server-Port (z.B. 587 für TLS)
Benutzername	Authentifizierungs-Benutzername
Passwort	Authentifizierungs-Passwort
Absenderadresse	E-Mail-Adresse, die als Absender verwendet wird
Absendername	Anzeigename, der als Absender verwendet wird
TLS verwenden	TLS-Verschlüsselung für die Verbindung aktivieren

TIP

Um die Einstellungen zu validieren, können Sie test E-Mails absetzen.

INFO

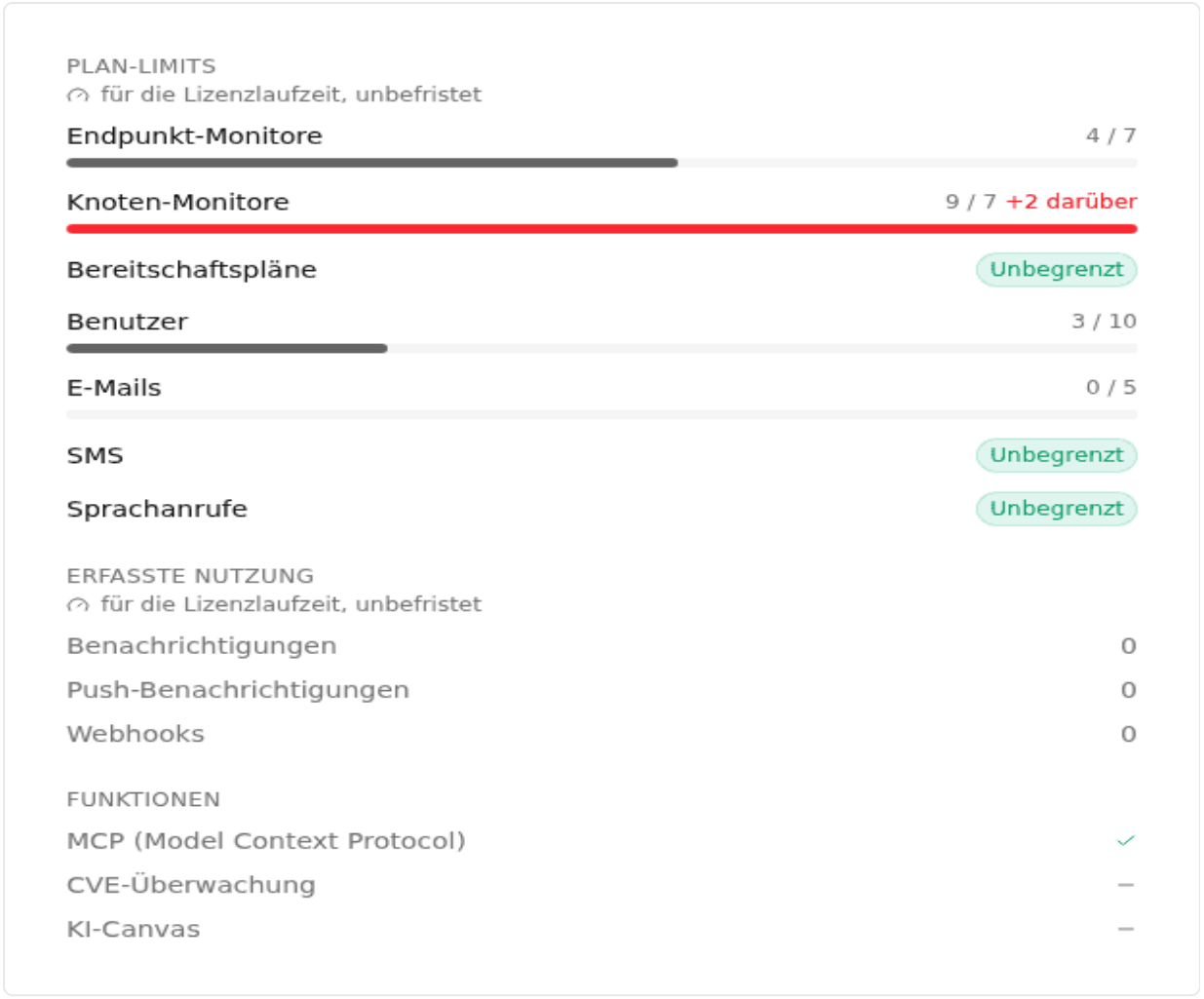
SMTP-Server werden nur für Benachrichtigungs-E-Mails verwendet. Benutzer-E-Mails wie Registrierungen sind nicht betroffen.

Lizenzen

Lizenzen haben eine eigene Seite. Unter Lizenzen können Sie einen Lizenzschlüssel hinzufügen, Ihre Plan-Limits und Nutzung einsehen und mehr über das Lizenzstatus-Banner erfahren.

Lizenznutzung

Das Nutzungspanel zeigt, wie der aktuelle Verbrauch Ihrer Organisation mit den Limits Ihrer aktiven Lizenz verglichen wird – gemessen über die gesamte Lizenzlaufzeit.



Das Panel ist in zwei Gruppen unterteilt:

Plan-Limits — Dimensionen mit einem Kontingent, dargestellt als Fortschrittsbalken:

Dimension	Beschreibung
Endpunkt-Monitore	Konfigurierte Datenquellen im Verhältnis zum Plan-Limit
Knoten-Monitore	Aufbewahrte Datenpunkte im Verhältnis zum Plan-Limit
Bereitschaftspläne	Aktive Bereitschaftspläne im Verhältnis zum Plan-Limit
E-Mails	Während der Lizenzlaufzeit versendete E-Mails
SMS	Während der Lizenzlaufzeit versendete SMS-Nachrichten
Sprachanrufe	Während der Lizenzlaufzeit getätigte Sprachanrufe

Die Balkenfarbe gibt Auskunft über den Kapazitätsstatus:

- **Grau** — innerhalb der Limits (unter 80 %)
- **Gelb / Limit fast erreicht** — Kontingent wird bald ausgeschöpft (80 – 99 %)

- **Gelb / Limit erreicht** — Nutzung liegt genau am Kontingent (100 %)
- **Rot / +N darüber** — Kontingent überschritten

Dimensionen, die nicht im Plan enthalten sind, werden mit dem Badge **„nicht in Ihrem Plan"** gekennzeichnet. Wenn trotzdem Nutzung anfällt, wechselt der Badge auf Rot.

Erfasste Nutzung — Dimensionen ohne Kontingent-Limit, als reine Zähler für die Lizenzlaufzeit:

Dimension	Beschreibung
Benachrichtigungen	Versendete In-App-Benachrichtigungen
Push-Benachrichtigungen	Versendete mobile Push-Benachrichtigungen
Webhooks	Durchgeführte Webhook-Zustellungen

Funktionen — lizenzierte Fähigkeiten, angezeigt als aktiviert (✓) oder nicht enthalten (—):

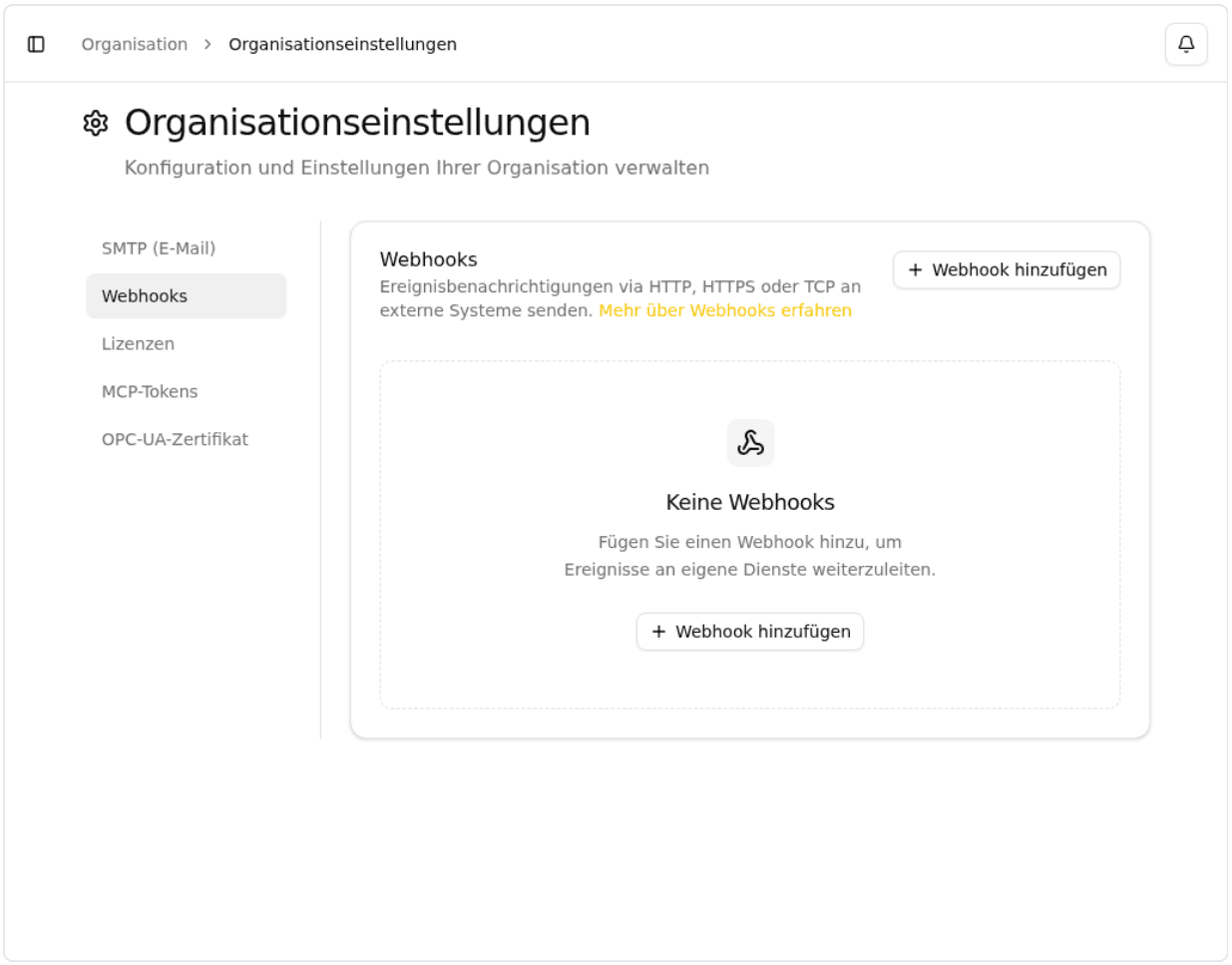
Funktion	Beschreibung
MCP (Model Context Protocol)	Ob sich MCP-Clients mit Ihrer Organisation verbinden können
CVE-Überwachung	Ob CVE-Monitore erstellt werden können und Scans durchführen
KI-Canvas	Ob der KI-Canvas-Untersuchungsbereich aktiviert ist

Ist keine aktive Lizenz mit der Organisation verknüpft, zeigt das Panel stattdessen einen Hinweis an. Wenden Sie sich an Ihren Administrator, um einen Lizenzschlüssel hinzuzufügen.

Webhooks

Webhooks ermöglichen es Pulse, bei bestimmten Ereignissen Echtzeit-Benachrichtigungen per HTTP(S) oder TCP an externe Systeme zu senden.

Navigieren Sie zu **Organisation > Einstellungen > Webhooks**, um Webhooks zu verwalten.



Klicken Sie auf **Webhook hinzufügen**, um einen neuen Webhook zu erstellen:

Feld	Beschreibung
Anzeigename	Eine Bezeichnung zur Identifikation dieses Webhooks
Endpunkt-URL	Ziel-URL – unterstützt die Schemata `https://`, `http://` oder `tcp://`
Aktiv	Aktivieren oder deaktivieren Sie die Zustellung
Ereignistypen	Wählen Sie aus, welche Ereignisse diesen Webhook auslösen

WARNING

Pulse zeigt eine Warnung „Unverschlüsselter Transport" an, wenn Sie eine `tcp://`- oder `http://`-URL eingeben. Reines TCP und reines HTTP verschlüsseln Payloads während der Übertragung nicht – verwenden Sie diese Schemata nur für Altsysteme, die kein HTTPS unterstützen.

INFO

TCP-Payloads werden mit Leerzeichen aufgefüllt, sodass die Gesamtlänge der Nachricht (JSON + Padding + Zeilenumbruch) immer ein Vielfaches von **64 Bytes** beträgt. Dies unterstützt festgroße Stream-Puffer auf SPS-Steuerungen, die in 64-Byte-Blöcken lesen.

So funktioniert die Zustellung

Jedes Ereignis löst pro passendem Webhook eine Zustellung aus. Zustellungen an denselben Endpunkt werden **der Reihe nach** und einzeln verarbeitet, sodass ein langsamer Endpunkt niemals dafür sorgt, dass Ereignisse außerhalb der Reihenfolge ankommen.

Schlägt eine Zustellung fehl — Verbindungsfehler, HTTP-Antwort ohne 2xx-Status oder Timeout — wiederholt Pulse sie bis zu **insgesamt 3 Versuchen** mit exponentiellem Backoff zwischen den Versuchen. Nach dem dritten gescheiterten Versuch wird das Ereignis für diesen Endpunkt verworfen. Für darüber hinausgehende Ausfallsicherheit richten Sie den Webhook auf eine eigene Warteschlange oder einen Reverse-Proxy.

HTTP(S)-Transport

HTTP(S)-Endpunkte erhalten ein `POST` mit den folgenden Headern:

Header	Wert
`Content-Type`	`application/json`
`User-Agent`	`Pulse-Webhook/1.0`
`X-Pulse-Signature`	`sha256=<hex>` — nur vorhanden, wenn Signierung aktiv

Der Anfragetext ist die JSON-Ereignis-Payload — unverändert, ohne abschließenden Zeilenumbruch.

TCP-Transport

TCP-Endpunkte erhalten jeden Frame in der Reihenfolge **JSON-Payload → ASCII-Leerzeichen-Auffüllung (`0x20`) → ein einzelner Zeilenumbruch (`\n`)** — die Leerzeichen stehen also zwischen der Payload und dem abschließenden Zeilenumbruch, der stets das letzte Byte ist. Die Auffüllung ist so bemessen, dass die **Gesamtlänge des Frames (Payload + Leerzeichen + Zeilenumbruch) ein Vielfaches von 64 Bytes** beträgt. Pulse öffnet pro Zustellung eine frische TCP-Verbindung, sendet den aufgefüllten Frame, schließt anschließend die Schreibseite des Sockets und beendet die Verbindung.

NOTE

Es handelt sich um **reines TCP**, nicht um WebSockets. Es gibt keinen HTTP-Upgrade-Handshake, keine Opcode-Frames und keine persistente Sitzung — jedes Ereignis ist eine eigene kurzlebige Verbindung. Die 64-Byte-Auffüllung existiert, damit SPS und ähnliche Steuerungen in festen Blockgrößen lesen können. Der nachgestellte Zeilenumbruch und die Leerzeichen sind gemäß der JSON-Spezifikation (RFC 8259, wonach `JSON-text = ws value ws` gilt und `ws` das Leerzeichen `0x20` sowie den Zeilenumbruch `0x0A` umfasst) unbedeutender Leerraum, sodass jeder spezifikationskonforme JSON-Parser den aufgefüllten Frame unverändert akzeptiert — ein Abschneiden ist nicht erforderlich. Ist Ihr Parser strenger als die Spezifikation, lesen Sie bis zum Ende des Streams und schneiden Sie den nachgestellten Leerraum vor dem Parsen ab.

Signaturen prüfen

Wenn Sie für einen Webhook ein oder mehrere **Signaturgeheimnisse** konfigurieren, enthält jede HTTP(S)-Zustellung einen `X-Pulse-Signature`-Header mit einem HMAC-SHA256 des Anfragetexts.

Der Header-Wert ist eine durch Kommas getrennte Liste aus `sha256=<hex>`-Einträgen — einer pro Geheimnis, in der Reihenfolge, in der die Geheimnisse beim Webhook hinterlegt sind. Mehrere Einträge ermöglichen es Ihnen, **Geheimnisse zu rotieren, ohne Zustellungen zu verlieren**: neues Geheimnis hinzufügen, neuen Verifizierer ausrollen (der beide Geheimnisse akzeptiert), dann das alte Geheimnis entfernen.

Eine Zustellung verifizieren:

1. Lesen Sie den **rohen Anfragetext** als Bytes — parsen und re-serialisieren Sie das JSON nicht. Schon unbedeutende Whitespace-Unterschiede verändern den Hash.
2. Berechnen Sie `HMAC-SHA256(geheimnis, body)` und formatieren Sie das Ergebnis als kleingeschriebene Hexadezimalzeichenkette.
3. Vergleichen Sie Ihren berechneten Wert `sha256=<hex>` mit **mindestens einem** der Einträge in `X-Pulse-Signature`. Verwenden Sie einen zeitkonstanten Vergleich, um Timing-Lecks zu vermeiden.
4. Stimmt mindestens ein Eintrag überein, ist die Zustellung authentisch. Stimmt keiner überein, lehnen Sie die Anfrage ab.

Node.js-Beispiel:

```
import crypto from "node:crypto";

// `body` muss der rohe Anfragetext als Bytes sein, kein geparstes Objekt.
function verifyPulseWebhook(body, header, secrets) {
  const expected = secrets.map((secret) => {
    const hex = crypto.createHmac("sha256", secret).update(body).digest("hex");
    return `sha256=${hex}`;
  });

  const received = header.split(",").map((s) => s.trim());

  return received.some((r) =>
    expected.some(
      (e) =>
        e.length === r.length &&
        crypto.timingSafeEqual(Buffer.from(e), Buffer.from(r)),
    ),
  );
}
```

Python-Beispiel:

```
import hmac
import hashlib

def verify_pulse_webhook(body: bytes, header: str, secrets: list[str]) -> bool:
    expected = [
        f"sha256={hmac.new(s.encode(), body, hashlib.sha256).hexdigest()}"
        for s in secrets
    ]
    received = [s.strip() for s in header.split(",")]
    return any(hmac.compare_digest(e, r) for e in expected for r in received)
```

WARNING

Verwenden Sie stets einen zeitkonstanten Vergleich (`crypto.timingSafeEqual` , `hmac.compare_digest` oder Äquivalent). Ein normaler String-Vergleich mit `==` kann die erwartete Signatur Byte für Byte über Timing-Unterschiede preisgeben.

Ereignistypen

Jeder Ereignistyp wird durch seinen `event.type` -Schlüssel in der Webhook-Payload identifiziert:

`event.type`	Beschreibung
`incident.created`	Vorfall erstellt

event.type	Beschreibung
incident.acknowledged	Vorfall bestätigt
incident.resolved	Vorfall behoben
oncall.rotation	Bereitschaftswechsel oder Betriebszeiten geändert
notification.email_scheduled	E-Mail-Benachrichtigung eingeplant
notification.sms_scheduled	SMS-Benachrichtigung eingeplant
notification.push_scheduled	Push-Benachrichtigung eingeplant
notification.call_scheduled	Anruf eingeplant

Webhook-Payload-Struktur

Jede Webhook-Zustellung ist ein JSON-Objekt. Pulse fügt das Feld `event_type` auf oberster Ebene zusammen mit den ereignisspezifischen Feldern ein:

```
{
  "event_type": "incident.created",
  ...ereignisspezifische Felder
}
```

Incident-Event-Payloads

Die Ereignisse `incident.created`, `incident.acknowledged` und `incident.resolved` verwenden die gleiche Payload-Struktur:

Feld	Typ	Beschreibung
event_type	string	Eines von `incident.created`, `incident.acknowledged`, `incident.resolved`
incident_id	integer	ID des Vorfalls
title	string	Titel des Vorfalls
status	string	Vorfallstatus — `"created"`, `"acknowledged"` oder `"resolved"`

Benachrichtigungs-Event-Payloads

Die Ereignisse `notification.email_scheduled`, `notification.sms_scheduled`, `notification.push_scheduled` und `notification.call_scheduled` verwenden die gleiche Payload-Struktur:

Feld	Typ	Beschreibung
`event_type`	string	Eines von `notification.email_scheduled`, `notification.sms_scheduled`, `notification.push_scheduled`, `notification.call_scheduled`
`incident_id`	integer	ID des Vorfalls, der die Benachrichtigung ausgelöst hat
`channel`	string	Benachrichtigungskanal — `"email"`, `"sms"`, `"push"` oder `"call"`
`recipients`	array	Liste der Benachrichtigungsempfänger

Jeder Eintrag in `recipients` enthält:

Feld	Typ	Beschreibung
`display_name`	string	Anzeigename des Empfängers
`email`	string|null	E-Mail-Adresse, falls vorhanden
`phone_number`	string|null	Telefonnummer, falls vorhanden

`oncall.rotation`-Payload

Das Ereignis `oncall.rotation` wird ausgelöst, wenn sich die aktiven Bereitschaftspersonen ändern oder sich der Betriebszeiten- oder Override-Status eines Zeitplans ändert:

Feld	Typ	Beschreibung
`event_type`	string	Immer `"oncall.rotation"`
`schedule_id`	integer	ID des Bereitschaftsplans
`schedule_name`	string	Name des Bereitschaftsplans
`previous_responders`	array	Bereitschaftspersonen vor der Änderung
`current_responders`	array	Bereitschaftspersonen nach der Änderung
`in_operating_hours`	boolean	Ob der Zeitplan aktuell innerhalb der Betriebszeiten liegt
`is_override`	boolean	Ob aktuell eine Ausnahme (Override) aktiv ist

Jeder Eintrag in `previous_responders` und `current_responders` enthält:

Feld	Typ	Beschreibung
`id`	integer	Login-ID
`name`	string	Anzeigename oder E-Mail-Adresse
`email`	string	E-Mail-Adresse
`phone`	string|null	Mobilnummer, falls hinterlegt

Verbundene MCP-Clients

KI-Assistenten und Automatisierungswerkzeuge verbinden sich über das Model Context Protocol per OAuth mit Pulse: Jeder Benutzer autorisiert einen Client im Browser, pro Organisation. Es müssen keine Tokens mehr erstellt oder kopiert werden — der Client erkennt den Autorisierungsserver von Pulse, registriert sich selbst und leitet Sie zu einem Zustimmungsdialog.

> **INFO**
>
> Der MCP-Zugriff erfordert eine aktive Lizenz, die MCP einschließt. Der Zustimmungsdialog bietet nur Organisationen an, deren Lizenz MCP enthält; qualifiziert sich keine Ihrer Organisationen, wenden Sie sich an Ihren Administrator, um die Lizenz zu erweitern.

Einen Client verbinden

Der MCP-Endpunkt ist unter `/mcp` auf Ihrer Pulse-Instanz verfügbar. Die Registerkarte **MCP-Clients** in den Einstellungen zeigt die genaue URL mit einer Kopierschaltfläche.

> **Voraussetzung**
>
> `CS_BASEURL` muss auf die extern erreichbare Basis-URL Ihrer Pulse-Instanz gesetzt sein (z.B. `https://pulse.example.com`). Die OAuth-Discovery-Metadaten und die URL des Autorisierungsendpunkts werden daraus abgeleitet — mit dem Standardwert können Clients auf anderen Rechnern den Ablauf nicht abschließen.

Claude Code

```
claude mcp add --transport http pulse https://<ihre-domain>/mcp
```

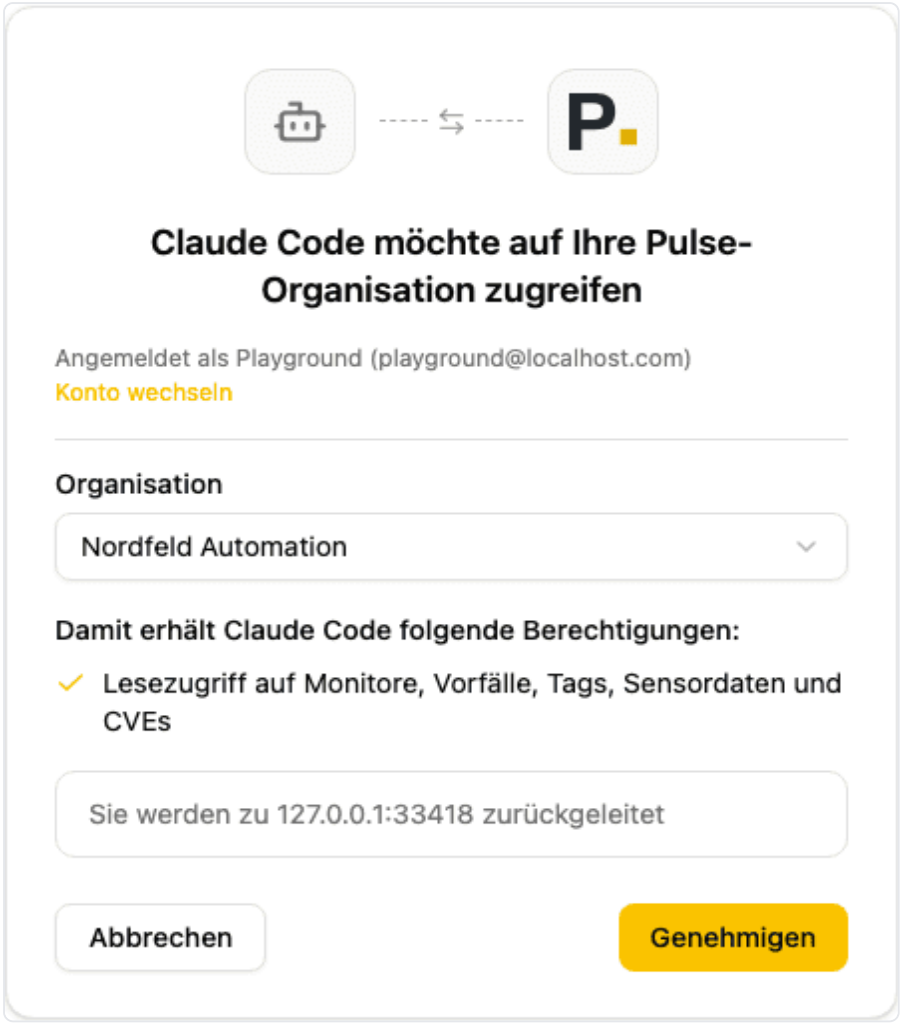
Ersetzen Sie `<ihre-domain>` durch den Host, unter dem Ihre Pulse-Instanz erreichbar ist — derselbe Wert wie `CS_BASEURL`. Fügen Sie `--scope user` hinzu, um den Server in jedem Projekt auf Ihrem Rechner verfügbar zu machen und nicht nur im aktuellen.

Die erste Werkzeugnutzung (oder `/mcp` in Claude Code) öffnet Ihren Browser: Melden Sie sich bei Pulse an, wählen Sie die zu verbindende Organisation und genehmigen Sie den Zugriff. Tokens werden von da an automatisch verwaltet.

claude.ai, Cursor und andere MCP-Clients

Fügen Sie einen Remote-MCP-Server (HTTP) mit der URL `https://<ihre-domain>/mcp` hinzu. Der Client erkennt die OAuth-Konfiguration, registriert sich automatisch und öffnet den Pulse-Zustimmungsdialog in Ihrem Browser.

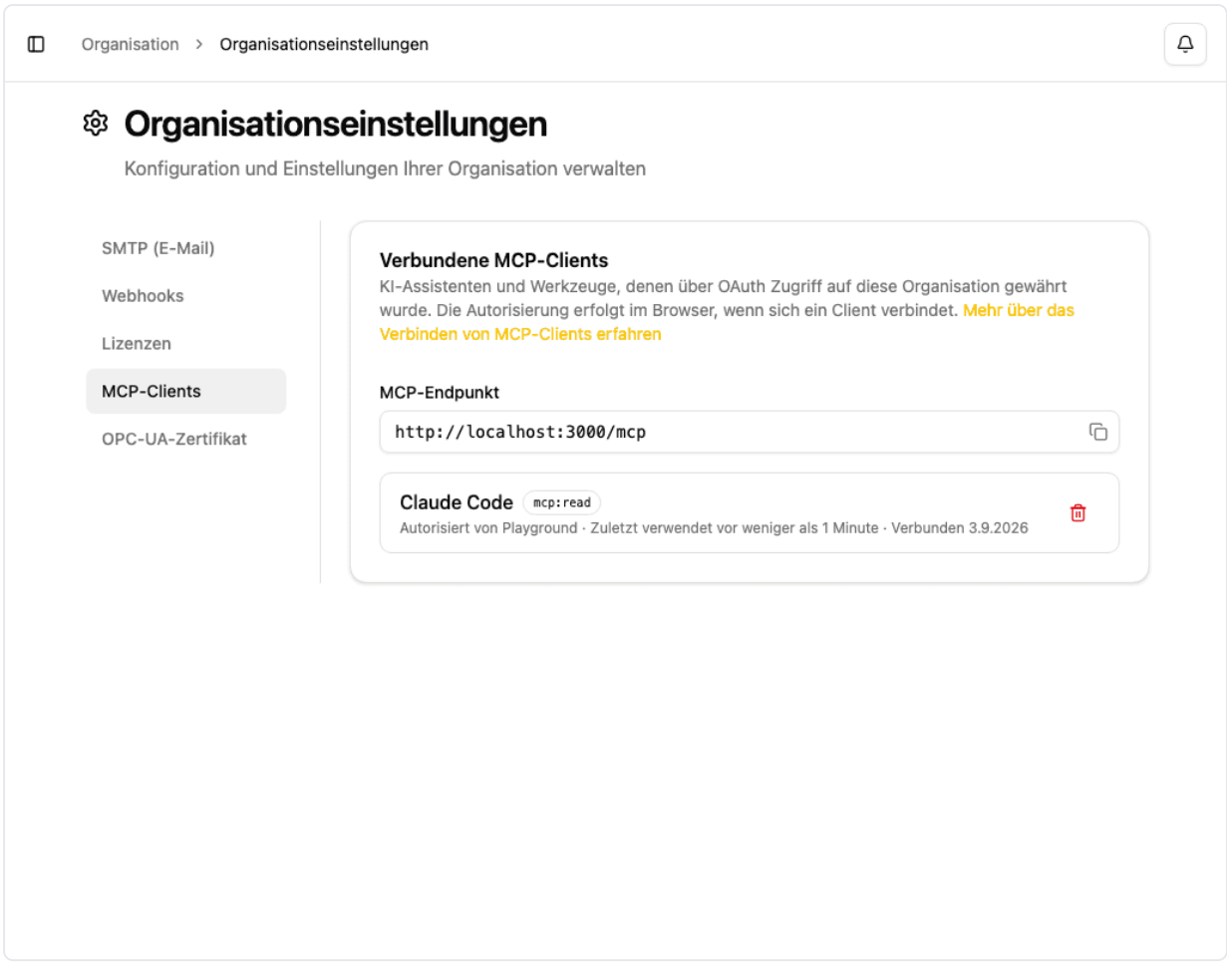
Der Zustimmungsdialog



Der Zustimmungsdialog benennt den Client, lässt Sie die zu verbindende Organisation wählen und listet auf, welchen Zugriff er erhält (Lesezugriff auf Monitore, Vorfälle, Tags, Sensordaten und CVEs). Er zeigt außerdem, wohin Sie nach der Genehmigung zurückgeleitet werden — prüfen Sie vor dem Klick auf **Genehmigen**, dass dieser Host zu dem Werkzeug passt, aus dem Sie die Verbindung gestartet haben.

Verbundene Clients verwalten

Navigieren Sie zu **Organisation > Einstellungen > MCP-Clients**, um alle Clients zu sehen, denen Zugriff auf die Organisation gewährt wurde.



Jede Zeile zeigt den Client, wer ihn autorisiert hat, wann er zuletzt verwendet und wann er verbunden wurde. Um den Zugriff zu widerrufen, klicken Sie auf das Löschen-Symbol und bestätigen Sie.

> **WARNING**
>
> Der Widerruf erfolgt sofort — die nächste Anfrage des Clients wird abgelehnt, auch wenn sein aktuelles Token noch nicht abgelaufen ist. Widerrufen Sie Clients, die Sie nicht mehr verwenden.

Verfügbare MCP-Werkzeuge

Der Pulse-MCP-Server stellt verbundenen Clients die folgenden Werkzeuge bereit. Die Parameter sind selbstbeschreibend — Ihr KI-Assistent erkennt sie automatisch über das MCP-Schema.

- `list_monitors` — Monitore der Organisation auflisten und filtern.

- `list_incidents` — Vorfälle auflisten und filtern.
- `query_data` — Zeitreihendaten mit Aggregationen abfragen, dargestellt als ASCII-Graph oder Tabelle. Die Ergebnisse können nach Monitor, Datenpunkt oder Datenquelle gruppiert werden.
- `query_cves` — CVE-Funde über die überwachten Geräte hinweg abfragen.
- `list_tags` — Die Tags der Organisation auflisten.
- `list_data_sources` — Datenquellen auflisten und optional ihre einzelnen Datenpunkte: Adressen, Namen und Beschreibungen, letzte Messwerte und die Monitore, die sie lesen. So findet ein Assistent die Namen der Quellen und die Adressen der Datenpunkte, nach denen `query_data` filtert — und es ist das einzige Werkzeug, das einen Datenpunkt zeigen kann, für den kein Monitor alarmiert.
- `get_condition` — Den Bedingungsgraphen lesen, auf den ein Bedingungsmonitor alarmiert, samt dem aktuellen Wert jedes Knotens und dem Zeitpunkt, ab dem dieser Wert gilt. Ein Bedingungsmonitor hat keinen einzelnen Schwellenwert — dies beantwortet, welcher Eingang ihn ausgelöst hat.
- `list_incident_events` — Den Verlauf eines Vorfalls lesen: wann der Monitor ausgefallen ist und sich erholt hat, jede zugestellte Benachrichtigung und an wen, Bestätigungen, Auflösungen und Eskalationsschritte.

Collectors

Navigieren Sie zu **Organisation > Einstellungen > Collectors**.

Remote-Collectors laufen in abgeschotteten Netzwerkzonen und bauen eine ausgehende Verbindung zur Appliance auf, um S7- und OPC-UA-Geräte abzufragen, die die Appliance nicht direkt erreicht. Damit kann eine Pulse-Appliance Geräte in isolierten Segmenten überwachen, ohne eingehende Firewall-Öffnungen zu benötigen.

Collector-Liste

Die Tabelle zeigt jeden registrierten Collector:

Spalte	Beschreibung
Name	Die von Ihnen vergebene Bezeichnung
Status	Aktueller Verbindungsstatus (siehe unten)
Zuletzt verbunden	Wann der Collector sich zuletzt mit der Appliance verbunden hat; leer für einen Collector, der sich noch nie verbunden hat

Spalte	Beschreibung
Host	Hostname und Software-Version des Collectors, soweit bekannt; zeigt außerdem die Adresse, von der er zuletzt gekoppelt wurde
Quellen	Anzahl der diesem Collector zugewiesenen Datenquellen

Status-Werte:

Status	Bedeutung
Verbunden	Collector ist aktiv mit der Appliance verbunden
Offline	Collector war zuvor verbunden, ist aber aktuell nicht erreichbar
Wartet auf erste Verbindung	Collector wurde angelegt, hat sich aber noch nie verbunden
Widerrufen	Collector wurde widerrufen; er kann sich erst nach Ausgabe eines neuen Pairing-Codes wieder verbinden

Collector hinzufügen

Klicken Sie auf **Collector hinzufügen**. Geben Sie einen **Namen** an — etwas, das Betreiber wiedererkennen, wie die Zone oder der Schaltschrank, in dem er läuft. Optional können Sie einen oder mehrere **IP-Bereiche** (CIDRs, Host-Bereiche oder Hostnamen) angeben, die der Collector erreichen kann. Diese dienen als Vorschläge bei der Zuweisung von Quellen und zur Eingrenzung von Erkundungsscans.

Nach dem Speichern öffnet sich der Dialog **Collector koppeln**. Er zeigt die Collector-Adresse, einen einmalig gültigen Pairing-Code mit Ablaufzeit und — sofern diese Instanz ein eigenes Zertifikat für Collectors besitzt — den Appliance-Fingerabdruck, den Sie zusammen mit dem Code auf dem Collector eingeben. Das Zertifikat von Pulse Cloud ist öffentlich vertrauenswürdig, daher ist dort keine Pinnung nötig. Geben Sie den Pairing-Code beim Einrichten auf dem Collector ein, bevor er abläuft — er wird nur dieses eine Mal angezeigt. Sie können bei Bedarf über das Aktionsmenü des Collectors einen neuen Pairing-Code erzeugen.

Collectors verwalten

Das Dropdown-Menü jeder Zeile bietet:

Aktion	Beschreibung
Bearbeiten	Collector umbenennen oder IP-Bereiche aktualisieren

Aktion	Beschreibung
Neuen Pairing-Code erzeugen…	Neuen einmaligen Pairing-Code für den Collector ausgeben. Der aktuelle Schlüssel des Collectors bleibt gültig, bis der neue Code eingelöst wird. Könnte dieser Schlüssel kompromittiert sein, widerrufen Sie den Collector zuerst.
Widerrufen…	Collector trennen; er kann sich erst nach Ausgabe eines neuen Pairing-Codes wieder verbinden
Löschen	Collector entfernen — alle seine Datenquellen müssen zuerst einem anderen Collector zugewiesen werden

Collector einer Datenquelle zuweisen

Sobald mindestens ein Collector registriert ist, zeigen die Formulare für S7- und OPC-UA-Datenquellen ein Feld **Erfasst über**. Wählen Sie **Diese Appliance** für eine direkte Abfrage oder wählen Sie einen bestimmten Collector. Ist der gewählte Collector offline, wartet auf die erste Verbindung oder wurde widerrufen, erscheint eine Warnung; Speichern ist dennoch möglich, und die Erfassung wird automatisch fortgesetzt, sobald sich der Collector verbindet.

Erkundung vom Collector aus starten

Die Seite Geräte entdecken zeigt eine Auswahl **Scannen von**, wenn Collectors registriert sind. Wählen Sie einen Collector, um den Netzwerkscan von dessen Standpunkt aus durchzuführen — nützlich, um ein Segment zu erreichen, das von der Appliance isoliert ist. Ein Scan kann nicht gestartet werden, wenn der gewählte Collector nicht aktiv verbunden ist, widerrufen wurde oder aus der Organisation entfernt wurde.

OPC-UA-Zertifikat

Navigieren Sie zu **Organisation > Einstellungen > OPC-UA-Zertifikat**, um das **Anwendungsinstanzzertifikat** zu verwalten — die gemeinsame X.509-Identität, mit der sich Pulse beim Aufbau sicherer OPC-UA-Kanäle (Modus Sign oder Sign & Encrypt) ausweist. Eine konzeptionelle Übersicht und den vollständigen Rotationsablauf finden Sie unter OPC-UA-Sicherheit — Anwendungsinstanz-Zertifikat.

Die Registerkarte zeigt den Antragsteller des aktiven Zertifikats, die Gültigkeitsdaten und den SHA-1-Fingerabdruck. Läuft eine Rotation, werden sowohl das aktive als auch das ausstehende Zertifikat angezeigt. Jeder Fingerabdruck ist gekennzeichnet — **Aktuell** für das aktive Zertifikat und **Neu – vor Abschluss der Rotation vertrauen** für das ausstehende — damit die beiden nicht verwechselt werden.

Aktionen

Aktion	Verfügbar wenn	Beschreibung
PEM herunterladen	Aktives Zertifikat vorhanden	Zertifikatsdatei herunterladen, um sie auf Ihren OPC-UA-Servern zu installieren
Fingerabdruck kopieren	Aktives Zertifikat vorhanden	SHA-1-Fingerabdruck kopieren, um ihn in der Zertifikatsverwaltung Ihres Servers zu überprüfen
Zertifikat generieren	Kein aktives Zertifikat vorhanden	Zertifikat vorab bereitstellen (Pulse stellt es auch automatisch bei der ersten sicheren Verbindung bereit)
Zertifikat rotieren	Aktives Zertifikat vorhanden, keine Rotation in Gang	Ersatzzertifikat erstellen, um die Überlappungsrotation zu starten
Rotation abschließen	Ausstehende Zertifikat vorhanden	Ausstehendes Zertifikat als aktiv übernehmen — erst nach Vertrauen auf jedem Server
Ersatz verwerfen	Ausstehendes Zertifikat vorhanden	Laufende Rotation abbrechen und das ausstehende Zertifikat entfernen — ein Bestätigungsdialog erscheint
Zertifikat widerrufen	Aktives Zertifikat vorhanden	Nur im Notfall: aktives Zertifikat sofort durch eine neue Identität ersetzen

> **WARNING**
>
> **Zertifikat widerrufen** verursacht einen sofortigen Ausfall der gesamten sicheren OPC-UA-Überwachung — jeder Server weist Pulse zurück, bis Sie das neue Zertifikat dort als vertrauenswürdig eingetragen haben. Verwenden Sie für einen geplanten, unterbrechungsfreien Austausch stattdessen die Rotation.

Verwandte Seiten

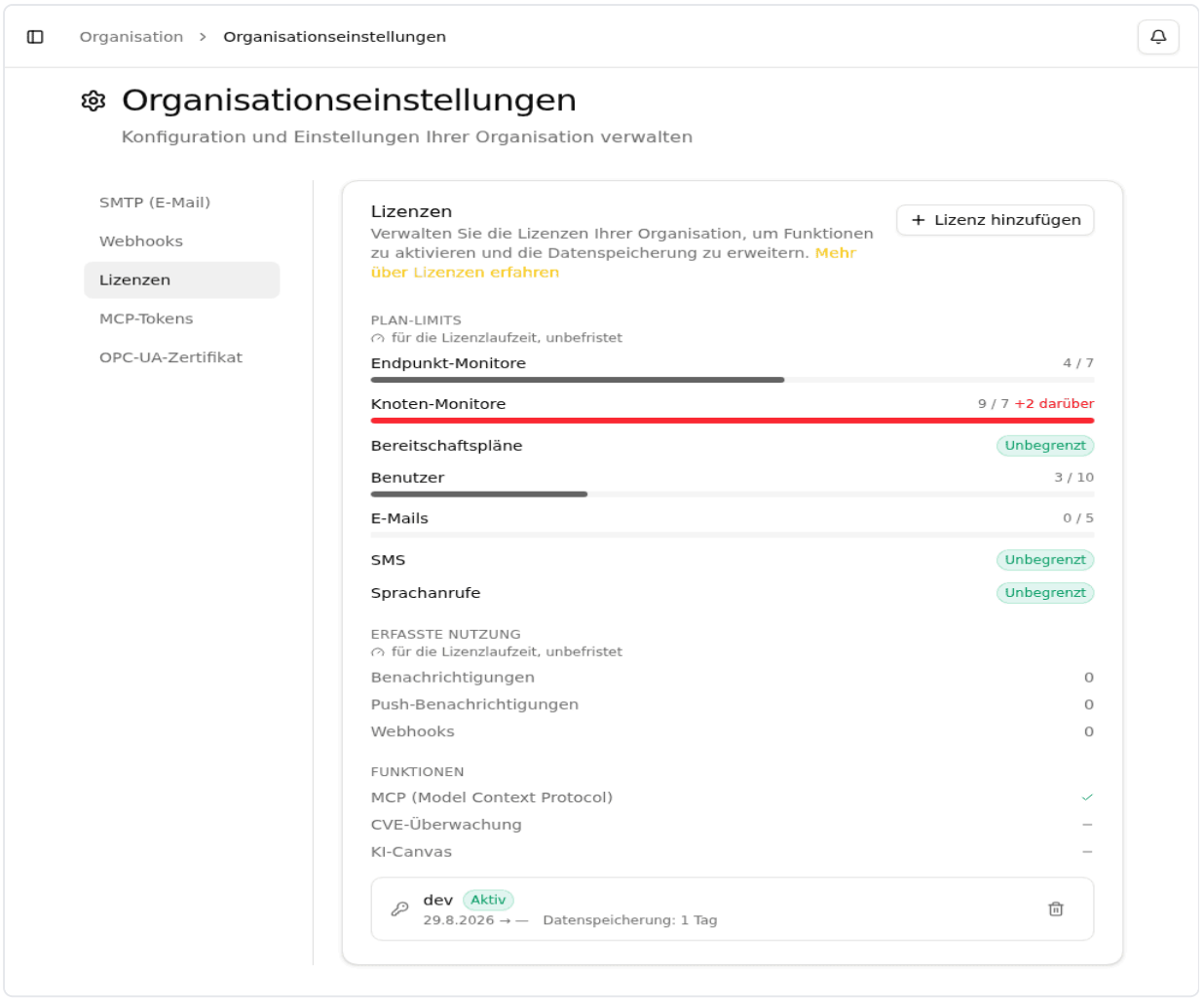
- Mitglieder & Rollen -- Organisationsmitglieder verwalten
- Einstellungen -- Persönliche Benachrichtigungseinstellungen
- OPC-UA-Konfiguration -- OPC-UA-Monitore und das Anwendungsinstanzzertifikat

- Geräte entdecken -- Netzwerkbereich nach S7-, OPC-UA- und PROFINET-Controllern durchsuchen

Teil 6 · Verwaltung

6.6 Lizenzen

Lizenzen aktivieren Pulse-Funktionen für Ihre Organisation, legen die Kapazitätsgrenzen Ihres Plans fest und steuern, wie lange Monitoring-Daten gespeichert werden. Verwalten Sie sie unter **Organisation > Einstellungen > Lizenzen**.



Lizenz hinzufügen

1. Navigieren Sie zu **Organisation > Einstellungen > Lizenzen**.
2. Klicken Sie auf **Lizenz hinzufügen**.
3. Fügen Sie Ihren Schlüssel in das Feld **Lizenzschlüssel** ein und klicken Sie auf **Lizenz hinzufügen**.

Ihr Lizenzschlüssel wird Ihnen von Pulse bereitgestellt und ist ein langer Token, der mit `eyJ` beginnt. Wird der Schlüssel abgelehnt, zeigt Pulse eine dieser Meldungen:

- **Der Lizenzschlüssel ist ungültig.** -- Der Schlüssel ist fehlerhaft oder kein Lizenz-Token.
- **Der Lizenzschlüssel konnte nicht verifiziert werden.** -- Die Signatur des Schlüssels stimmte nicht. Prüfen Sie, ob Sie den vollständigen Schlüssel eingefügt haben.

Lizenzdetails

Jede Lizenz in der Liste zeigt:

Feld	Beschreibung
Instanz-ID	Die Pulse-Instanz, für die die Lizenz ausgestellt wurde.
Status	**Aktiv** (die Lizenz, die aktuell die Kontingente steuert), **Reserve** (aktuell gültig, aber nicht die wirksame Lizenz), **Abgelaufen** (Enddatum überschritten) oder **Ausstehend** (Startdatum liegt in der Zukunft).
Gültigkeitszeitraum	Start- → Enddatum. Ein fehlendes Datum bedeutet, dass es in dieser Richtung keine Begrenzung gibt (unbefristet).
Datenspeicherung	Wie viele Tage Pulse Ihre Monitoring-Daten aufbewahrt, bevor sie automatisch gelöscht werden.

Um eine Lizenz zu entfernen, klicken Sie auf das Papierkorb-Symbol und bestätigen Sie.

> **WARNING**
>
> Das Löschen einer Lizenz kann Ihrer Organisation den Zugriff auf lizenzierte Funktionen kosten, und die Anwendung ist möglicherweise nicht mehr vollständig nutzbar. Löschen Sie nur eine Lizenz, die Sie ersetzen möchten.

Nutzung und Plan-Limits

Das Nutzungspanel oben im Tab „Lizenzen" vergleicht Ihre aktuelle Nutzung mit der aktiven Lizenz. Jede Gruppe ist mit der Lizenzlaufzeit beschriftet -- **für die Lizenzlaufzeit, endet am {Datum}** oder **für die Lizenzlaufzeit, unbefristet**, wenn die Lizenz kein Enddatum hat.

Plan-Limits

Diese Kapazitäten werden durch Ihren Plan geregelt. Jede wird als Anzeige der Nutzung im Verhältnis zu Ihrem Kontingent dargestellt:

Limit	Was gezählt wird
Endpunkt-Monitore	Konfigurierte Datenquellen.
Knoten-Monitore	Datenpunkte, für die Sie einen Verlauf aufbewahren.
Bereitschaftspläne	Bereitschaftspläne in Ihrer Organisation.
Benutzer	Aktive Mitglieder in Ihrer Organisation.
E-Mails	Während der Lizenzlaufzeit gesendete E-Mail-Benachrichtigungen.
SMS	Während der Lizenzlaufzeit gesendete SMS-Benachrichtigungen.

Eine Anzeige erscheint in einer von drei Formen:

- **Ein Balken mit Zähler** (zum Beispiel `12 / 20`) -- Ihre Nutzung im Verhältnis zum Kontingent. Der Balken ist normalerweise neutral, wird bei 80 % oder mehr **gelb** mit dem Hinweis *Limit fast erreicht* und **rot** mit dem Hinweis *+N darüber*, sobald Sie das Kontingent überschreiten.
- **Unbegrenzt** -- Ihr Plan setzt für diese Kapazität keine Obergrenze.
- **nicht in Ihrem Plan** -- diese Kapazität ist nicht Teil Ihres aktuellen Plans. Jegliche Nutzung wird rot angezeigt, als Hinweis darauf, dass sie außerhalb der Grenzen Ihres Plans liegt.

Funktionen

Je nach Plan können bestimmte Funktionen für Ihre Organisation aktiviert oder deaktiviert sein. Der Abschnitt **Funktionen** im Nutzungspanel listet jede Funktion und gibt an, ob sie in der aktuellen Lizenz enthalten ist:

Funktion	Beschreibung
MCP (Model Context Protocol)	Stellt Pulse-Daten über das Model Context Protocol für KI-Assistenten bereit.
CVE-Überwachung	Verfolgt bekannte Schwachstellen für die Firmware-Versionen, die Pulse von Ihren Steuerungen liest.

Funktion	Beschreibung
KI-Canvas	KI-gestützter Arbeitsbereich für die Vorfallsanalyse.
S7-Gerätesuche	Durchsucht einen Netzbereich nach Siemens-S7-Steuerungen.
OPC-UA-Gerätesuche	Durchsucht einen Netzbereich nach OPC-UA-Servern.
PROFINET-Gerätesuche	Durchsucht ein Netzsegment nach PROFINET-Geräten.
Asset-Register	Dauerhaftes Verzeichnis aller durch Scans gefundenen Stationen, von einem Scan zum nächsten gespeichert. Siehe Asset-Register.

Jeder Eintrag wird als **aktiviert** oder **deaktiviert** entsprechend der aktiven Lizenz angezeigt. Die Gerätesuche wird pro Protokoll lizenziert — Ihr Tarif kann eine beliebige Kombination aus S7, OPC UA und PROFINET umfassen.

Erfasste Nutzung

Pulse meldet zusätzlich das Nachrichtenvolumen, das **gezählt, aber nicht begrenzt** wird, über dieselbe Lizenzlaufzeit:

- **Benachrichtigungen**
- **Push-Benachrichtigungen**
- **Webhooks**

Diese Werte sind informativ -- sie blockieren keine Aktivität, wenn sie ansteigen.

Benachrichtigungen bei niedrigem Kontingent

Wenn Ihr E-Mail- oder SMS-Kontingent auf 10 % oder weniger des lizenzierten Limits sinkt, sendet Pulse automatisch eine In-App-Benachrichtigung an alle Organisations-Administratoren und -Inhaber:

- **E-Mail-Kontingent fast aufgebraucht** -- Sie haben X von Y Nachrichten im aktuellen Lizenzzeitraum verbraucht. Laden Sie Ihr Kontingent auf, um Zustellausfälle zu vermeiden.
- **SMS-Kontingent fast aufgebraucht** -- Sie haben X von Y Nachrichten im aktuellen Lizenzzeitraum verbraucht. Laden Sie Ihr Kontingent auf, um Zustellausfälle zu vermeiden.

Die Benachrichtigung wird einmal pro Lizenz gesendet. Bei Installation einer neuen Lizenz (z. B. nach einer Aufstockung) wird die Warnung für den neuen Zeitraum erneut aktiviert.

Lizenzstatus-Banner

Wenn die Lizenz Ihrer Organisation Aufmerksamkeit erfordert, zeigt Pulse oben auf jeder Seite einen Warnhinweis:

- **Keine gültige Lizenz** -- „Diese Organisation verfügt über keine gültige Lizenz. Einige Funktionen können eingeschränkt sein."
- **Lizenz läuft bald ab** -- „Ihre Lizenz läuft bald ab. Bitte erneuern Sie diese, um Dienstunterbrechungen zu vermeiden."

Der Banner verschwindet automatisch, sobald eine gültige, nicht ablaufende Lizenz aktiv ist.

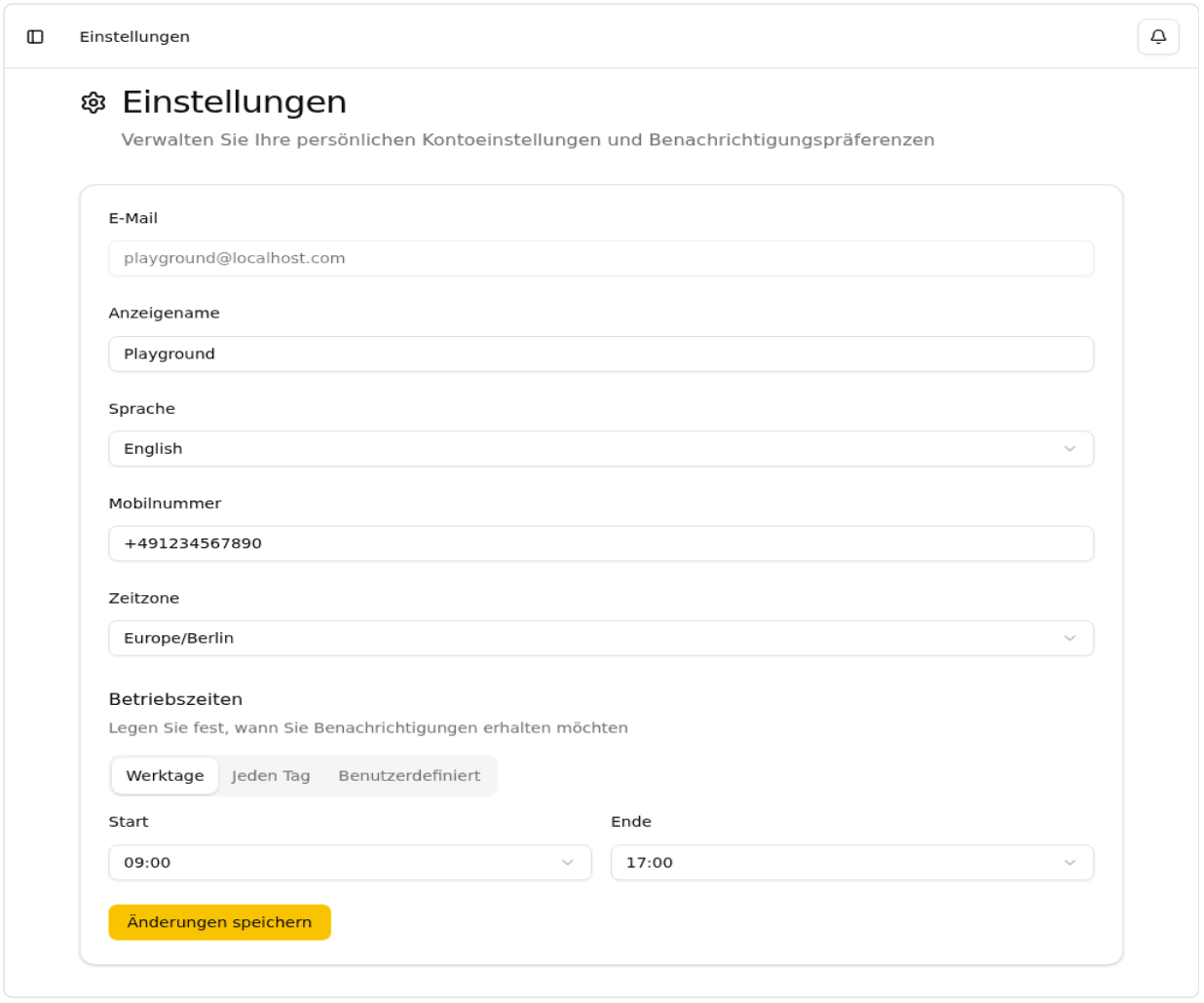
Verwandte Seiten

- Organisationseinstellungen -- SMTP-Server und Webhooks
- Mitglieder & Rollen -- Wer die Organisation verwalten darf
- Monitore -- Die Monitore, die auf Ihren Plan angerechnet werden

Teil 6 · Verwaltung

6.7 Einstellungen

Die Einstellungsseite ermöglicht es Ihnen, Ihre persönlichen Pulse-Einstellungen anzupassen.



Verfügbare Einstellungen

Einstellung	Beschreibung
Anzeigename	Ihr Name, wie er anderen Teammitgliedern angezeigt wird
E-Mail	Ihre E-Mail-Adresse (schreibgeschützt)
Sprache	Oberflächen-Sprache: Englisch oder Deutsch
Mobilnummer	Telefonnummer für SMS- und Sprachanruf-Benachrichtigungen

Einstellung	Beschreibung
Zeitzone	Ihre lokale Zeitzone für die Anzeige von Datum und Uhrzeit
Betriebszeiten	Wann Sie für Benachrichtigungen erreichbar sind

WARNING

Wenn eine Schwere in Ihrer Organisation SMS- oder Sprachanruf-Benachrichtigungen verwendet, wird ein Warnhinweis angezeigt, bis Sie eine Mobilnummer hinterlegen. Ohne Mobilnummer können diese Benachrichtigungskanäle Sie nicht erreichen.

Mobile App koppeln

Sie können die Pulse Dispatch Mobile App mit Ihrem Konto koppeln, ohne Anmeldedaten manuell einzugeben. Diese Funktion ist über das Benutzermenü in der Seitenleiste auf dem Desktop verfügbar.

So koppeln Sie die Mobile App:

1. Öffnen Sie das Benutzermenü am unteren Rand der Seitenleiste.
2. Wählen Sie **Mobile App koppeln**.
3. Scannen Sie den angezeigten QR-Code mit der Pulse Dispatch App.

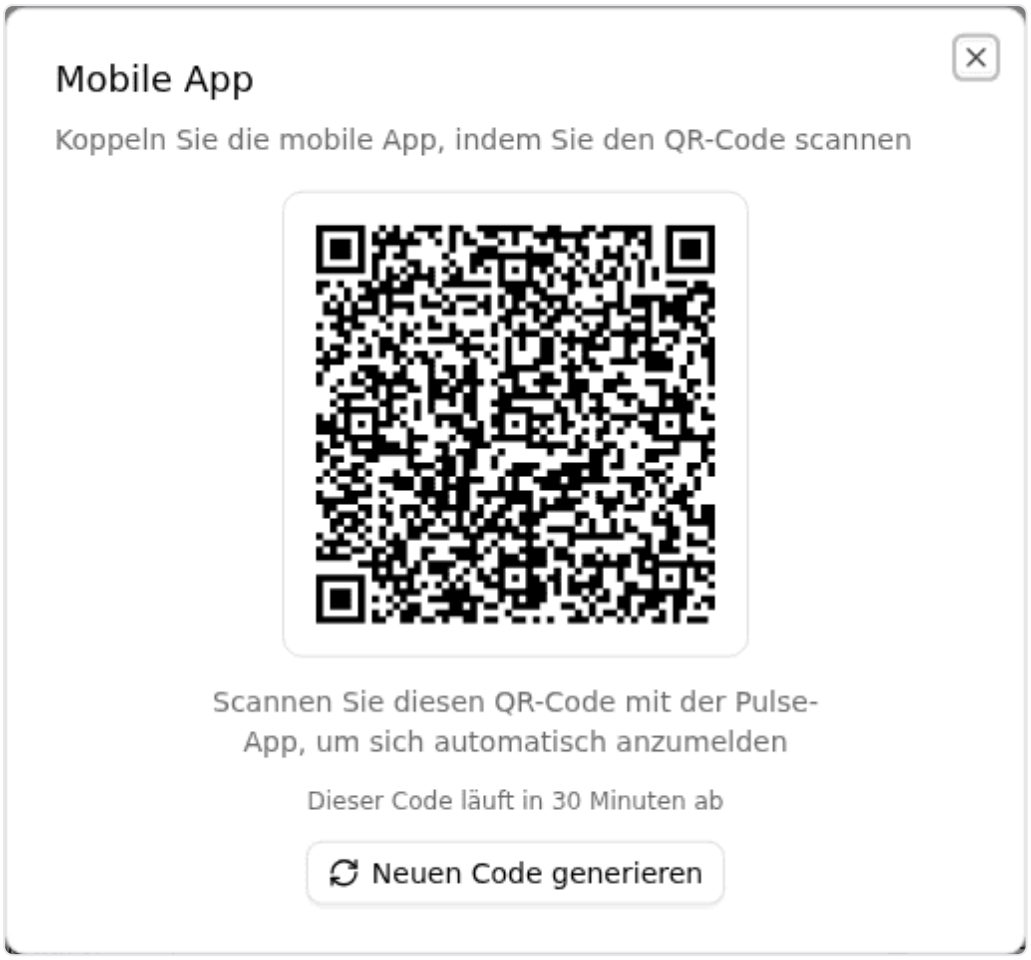
Der QR-Code läuft nach 30 Minuten ab. Falls er abläuft, bevor Sie ihn scannen, klicken Sie auf **Neuen Code generieren**, um einen neuen zu erhalten.

TIP

Die App noch nicht installiert? Pulse Dispatch ist im App Store für iPhone und iPad verfügbar. Informationen zur Verfügbarkeit und Einrichtung finden Sie unter Mobile App.

Zertifikats-Fingerabdruck

Bei der Kopplung zeigt das Dialogfeld einen **Zertifikats-Fingerabdruck** — eine kurze Zeichenfolge, die aus dem TLS-Zertifikat des Geräts abgeleitet wird. Ihr Smartphone zeigt während der Kopplung denselben Fingerabdruck an. Überprüfen Sie, ob beide übereinstimmen, bevor Sie die Verbindung bestätigen. Falls sie abweichen, fahren Sie nicht fort.



Betriebszeiten

Betriebszeiten definieren, wann Sie für Vorfallbenachrichtigungen kontaktiert werden können. Außerhalb der Betriebszeiten werden Benachrichtigungen zurückgestellt oder an andere Teammitglieder weitergeleitet.

Modi

- **Werktage** -- Montag bis Freitag mit gleichen Zeiten jeden Tag
- **Täglich** -- Gleiche Zeiten jeden Tag einschließlich Wochenende
- **Benutzerdefiniert** -- Unterschiedliche Zeiten für jeden Wochentag

Betriebszeiten umkehren

Aktivieren Sie **Betriebszeiten umkehren**, um das Fenster umzukehren: Benachrichtigungen kommen dann *außerhalb* der ausgewählten Zeiten an, nicht während dieser. Dies ist nützlich, wenn Sie abends und am Wochenende erreichbar sein möchten, aber nicht während der regulären Geschäftszeiten.

Standardkonfiguration

Die Standard-Betriebszeiten sind Montag bis Freitag, 09:00 bis 17:00 Uhr in Ihrer konfigurierten Zeitzone.

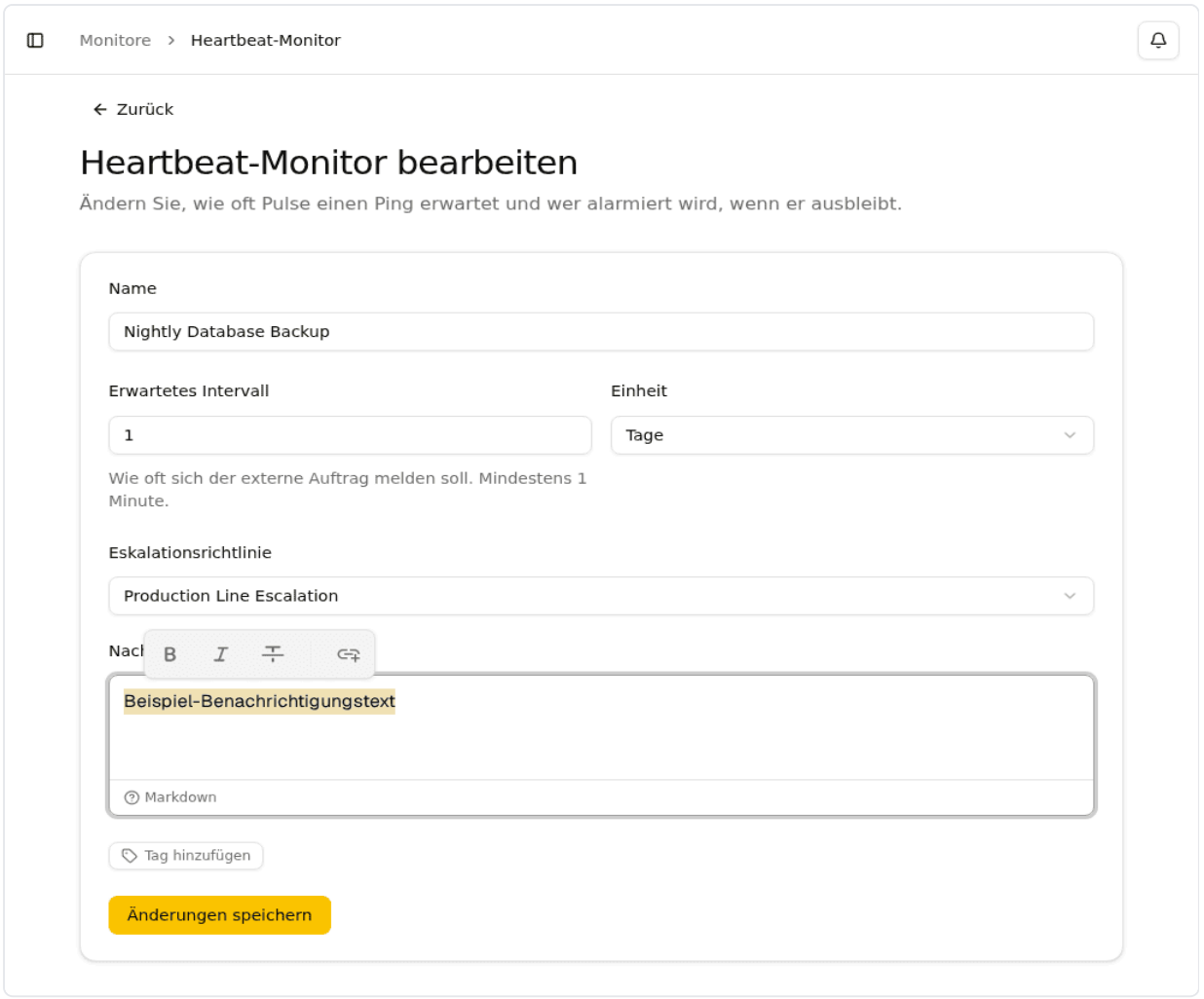
TIP

Konfigurieren Sie Ihre Betriebszeiten passend zu Ihrem tatsächlichen Arbeitsplan. So stellen Sie sicher, dass Sie nur Benachrichtigungen erhalten, wenn Sie darauf reagieren können.

Teil 7 · Referenz

7.1 Markdown

Der Nachrichtenvorlagen-Editor in Pulse unterstützt Markdown-Formatierung. Verwenden Sie die Symbolleiste für schnelle Formatierung oder geben Sie die Markdown-Syntax direkt ein.



Textformatierung

Syntax	Ergebnis
`**fetter Text**`	**fetter Text**
`*kursiver Text*`	*kursiver Text*
`` `Inline-Code` ``	`Inline-Code`

TIP

Markieren Sie Text im Editor, um die schwebende Symbolleiste mit den Schaltflächen **Fett**, **Kursiv** und **Code** anzuzeigen.

Überschriften

```
# Überschrift 1

## Überschrift 2

### Überschrift 3

#### Überschrift 4

##### Überschrift 5
```

Listen

Aufzählungsliste:

```
- Erster Punkt
- Zweiter Punkt
- Dritter Punkt
```

Nummerierte Liste:

```
1. Erster Schritt
2. Zweiter Schritt
3. Dritter Schritt
```

Links

```
[Linktext](https://example.com)
```

WARNING

Es werden nur `https://` - und `http://` -Links unterstützt.

Zitate

```
> Dies ist ein Zitat.
```

Code-Blöcke

```
```
Inhalt des Code-Blocks
```
```

Bilder

```
![Beschreibung](https://example.com/bild.png)
```

Absätze

Trennen Sie Absätze durch eine Leerzeile.

```
Erster Absatz.

Zweiter Absatz.
```

Verwandte Themen

- Nachrichtenvorlagen

7.2 Fehlerbehebung

Häufige Probleme und deren Lösungen bei der Arbeit mit Pulse.

Verbindungsprobleme

OPC-UA-Server nicht erreichbar

Symptome: Die Datenquelle zeigt „Liest nicht", und der Monitor, der ihre Nichterreichbarkeit meldet, ist fehlerhaft.

Mögliche Ursachen:

- Firewall blockiert TCP-Port 4840 (oder benutzerdefinierten Port)
- OPC-UA-Server läuft nicht
- Falsche Endpunkt-URL

Lösungen:

1. Prüfen Sie, ob der OPC-UA-Server auf dem Zielrechner läuft
2. Überprüfen Sie die Firewall-Regeln zwischen Pulse und dem OPC-UA-Server
3. Bestätigen Sie, dass die Endpunkt-URL korrekt ist, einschließlich Protokoll und Port

S7-SPS nicht erreichbar

Symptome: Die Datenquelle zeigt „Liest nicht", und der Monitor, der ihre Nichterreichbarkeit meldet, ist fehlerhaft.

Mögliche Ursachen:

- Netzwerk-Konnektivitätsproblem
- Falsche IP-Adresse, Rack- oder Slot-Konfiguration
- SPS befindet sich im STOP-Modus

Lösungen:

1. Prüfen Sie die Netzwerkkonnektivität zur SPS (IP-Adresse anpingen)
2. Überprüfen Sie, ob Rack- und Slot-Werte mit Ihrer SPS-Hardware übereinstimmen
3. Stellen Sie sicher, dass die SPS im RUN-Modus ist

Authentifizierungsprobleme

OPC-UA-Authentifizierung fehlgeschlagen

Symptome: Die Datenquelle kann sich nicht verbinden und meldet einen Authentifizierungsfehler.

Lösungen:

1. Überprüfen Sie, ob Benutzername und Passwort korrekt sind
2. Stellen Sie sicher, dass Sicherheitsmodus und -richtlinie mit der Serverkonfiguration übereinstimmen
3. Bei Zertifikatsauthentifizierung stellen Sie sicher, dass das Zertifikat gültig und vom Server vertrauenswürdig ist

---

Benachrichtigungsprobleme

Keine Benachrichtigungen erhalten

Mögliche Ursachen:

- Betriebszeiten falsch konfiguriert
- Nicht der Eskalationsrichtlinie zugewiesen
- Benachrichtigungskanal nicht im Schweregrad konfiguriert

Lösungen:

1. Überprüfen Sie Ihre Betriebszeiten in den Einstellungen
2. Stellen Sie sicher, dass Sie oder Ihr Team als Empfänger in der Eskalationsrichtlinie aufgeführt sind
3. Bestätigen Sie, dass der Schweregrad die erwarteten Benachrichtigungskanäle enthält
4. Überprüfen Sie, ob Ihre Mobilnummer für SMS-/Anrufbenachrichtigungen korrekt eingetragen ist

7.3 SBOM

Jeder ausgelieferte Pulse-Build enthält eine Software-Stückliste (SBOM): ein maschinenlesbares Verzeichnis aller im Produkt enthaltenen Drittanbieter-Komponenten.

Pulse veröffentlicht seine SBOM im CycloneDX-JSON-Format. Es handelt sich um ein einzelnes zusammengeführtes Dokument, das alle ausgelieferten Komponenten abdeckt:

- Das Haskell-Backend (aus dem festgelegten Abhängigkeitssatz aufgelöst)
- Die Go-Dienste — den OPC-UA-Kollektor, den S7-Kollektor und die Appliance-CLI
- Die Web- und Mobile-Oberflächen (npm-Abhängigkeiten)

Download

Pulse-SBOM herunterladen (CycloneDX JSON)

Sie können die Datei auch im Browser öffnen.

Verwendung der SBOM

Die CycloneDX-Datei kann von gängigen Supply-Chain- und Schwachstellen-Tools eingelesen werden — zum Beispiel Dependency-Track, Grype oder Trivy —, um Lizenzen zu prüfen und die von Pulse ausgelieferten Komponenten auf bekannte Schwachstellen zu untersuchen.

Teil 8 · Mobile-App

8.1 Übersicht

Die Pulse Mobile-App ist die Begleit-App zur Pulse Web-Anwendung. Sobald sie mit Ihrem Pulse-Server verbunden ist, können Sie Ihre OT-Infrastruktur überwachen und Alarmbenachrichtigungen unterwegs empfangen.

Verfügbarkeit

Pulse Dispatch steht im App Store bereit. Installieren Sie die App auf dem Gerät, auf dem Sie alarmiert werden möchten, und richten Sie sie anschließend auf Ihren Pulse-Server aus — siehe Einrichtung & Verbindung.

Pulse Dispatch im App Store →

Unterstützte Plattformen

- **iOS** — iPhone und iPad, aus dem App Store. Erfordert iOS 15.1 oder neuer. Verfügbar im deutschen, österreichischen und Schweizer App Store.
- **Android** — *in Kürze verfügbar*. Die Android-Version ist in Entwicklung und steht noch nicht zur Installation bereit.

Die Oberfläche passt sich automatisch an die helle oder dunkle Darstellung Ihres Geräts an.

Was Sie damit machen können

Die Mobile-App bietet Ihnen die gleiche Pulse-Erfahrung wie im Browser. Vom Smartphone aus können Sie:

- Das Dashboard mit dem Live-Status aller Monitore aufrufen
- Monitore durchsuchen und prüfen
- Vorfälle verfolgen und bestätigen
- Das Benachrichtigungscenter öffnen, um aktuelle Alarme einzusehen

Anmeldung, Wechsel der Organisation und Teamverwaltung erfolgen in derselben Pulse-Oberfläche, die Sie bereits kennen — es gibt keine separate mobile Anmeldung.

Was die Mobile-App zusätzlich bietet

Drei Aufgaben übernimmt die mobile Hülle anstelle der Web-Anwendung:

- Serverkopplung — Sie richten die App beim ersten Start auf Ihren Pulse-Server aus und können diesen später jederzeit ändern.
- Push-Benachrichtigungen — Sie empfangen Alarme direkt auf Ihrem Gerät, gesteuert durch Ihre bestehenden Bereitschaftspläne und Eskalationsrichtlinien.

Verwandte Themen

- Einrichtung & Verbindung — App mit Ihrem Pulse-Server verbinden
- Benachrichtigungen & Einstellungen — Alarme aktivieren und Serveradresse später ändern
- Dashboard — Übersicht über alle Monitore
- Vorfälle — aktive Vorfälle untersuchen und bestätigen

8.2 Einrichtung & Verbindung

Bevor Sie die Pulse Mobile-App nutzen können, müssen Sie sie installieren und auf Ihren Pulse-Server ausrichten.

App installieren

Installieren Sie **Pulse Dispatch** aus dem App Store auf dem iPhone oder iPad, auf dem Sie alarmiert werden möchten:

Pulse Dispatch im App Store →

Die App erfordert iOS 15.1 oder neuer. Eine Android-Version ist in Entwicklung — siehe Mobile-App.

Erstmalige Kopplung

Wenn Sie die App zum ersten Mal öffnen, fragt der Bildschirm **Mit Pulse verbinden** nach der Adresse Ihres Pulse-Servers.

1. Geben Sie die Serveradresse ein — zum Beispiel `pulse.ihreFirma.de`.
2. Tippen Sie auf **Verbinden**. Die App prüft, ob der Server erreichbar ist, bevor sie fortfährt.
3. Ist die Prüfung erfolgreich, lädt die App Ihren Pulse-Server und führt Sie direkt zur Anmeldung.

> **TIP**
>
> `https://` können Sie weglassen — die App ergänzt es automatisch.

Sollten Sie noch keine eigene Serveradresse haben, tippen Sie auf **Pulse Cloud verwenden (app.pulsehq.de)**, um die App auf den gehosteten Pulse Cloud-Dienst auszurichten.

Kann die Adresse nicht erreicht werden, zeigt die App eine Fehlermeldung an und bietet die Option **Diese Adresse trotzdem verwenden** an. Verwenden Sie diese, wenn Sie wissen, dass der Server aus Ihrem Netzwerk erreichbar ist, obwohl die initiale Prüfung fehlgeschlagen ist (zum Beispiel in internen Netzen, die den Prüfaufruf blockieren).

Anmeldung

Sobald die App mit einem Server gekoppelt ist, funktioniert die Anmeldung genauso wie in der Pulse Web-Anwendung. Verwenden Sie dieselbe E-Mail-Adresse und dasselbe Passwort wie im Browser. Wechsel zwischen Organisationen, Verwaltung Ihres Profils und Beitritt zu Teams erfolgen in derselben Oberfläche — siehe Mitglieder & Rollen und Teams.

Serveradresse später ändern

Sie können die Serveradresse jederzeit aus der App heraus ändern:

1. Halten Sie auf dem Startbildschirm **den kleinen Anfasser am oberen Bildschirmrand** etwa 1,5 Sekunden lang gedrückt. Das Sheet **Serverkonfiguration** wird von unten eingeblendet.
2. Bearbeiten Sie die Serveradresse und tippen Sie auf **Verbinden**, um sie zu prüfen und zu speichern.
3. Um zum gehosteten Dienst zurückzukehren, tippen Sie auf **Standard wiederherstellen**.
4. Um die App komplett mit einem anderen Server neu zu koppeln, tippen Sie auf **Trennen und neu konfigurieren**. Damit gelangen Sie zurück zum Bildschirm der erstmaligen Kopplung.

Wenn das Gerät offline ist

Verliert Ihr Smartphone die Netzwerkverbindung oder ist Ihr Pulse-Server kurzzeitig nicht erreichbar, zeigt die App den Bildschirm **Verbindung unterbrochen** anstelle der Hauptoberfläche an.

- Die App versucht die Verbindung automatisch erneut herzustellen — mit einer kurzen Wartezeit zwischen den Versuchen.
- Tippen Sie auf **Erneut versuchen**, um sofort einen neuen Versuch auszulösen.
- Tippen Sie auf **Serverkonfiguration**, um dasselbe Einstellungs-Sheet wie oben beschrieben zu öffnen — nützlich, wenn die Serveradresse selbst geändert werden muss.
- Klappen Sie **Details** aus, um genau zu sehen, welchen Server die App zu erreichen versucht und welcher Fehler zuletzt aufgetreten ist (zum Beispiel ein HTTP-Statuscode oder eine Netzwerk-Zeitüberschreitung).

Sobald das Netzwerk wieder verfügbar ist oder der Server wieder erreichbar wird, stellt die App die Verbindung automatisch wieder her — Sie müssen nichts unternehmen.

> **TIP**
>
> Auch das Zurückholen der App in den Vordergrund (etwa nach einem Wechsel zu einer anderen App) löst sofort einen erneuten Verbindungsversuch aus.

Fingerabdruck der Appliance prüfen

Wenn Sie die App mit einer selbst betriebenen Pulse-Appliance koppeln statt mit Pulse Cloud, fragt Sie die App nach der ersten Verbindung gegebenenfalls, einen SHA256-Fingerabdruck zu bestätigen. Vergleichen Sie den auf dem Bildschirm angezeigten Wert mit dem Wert aus dem Bildschirm TLS-Zertifikate der Appliance — sie müssen Zeichen für Zeichen übereinstimmen, bevor Sie fortfahren.

Verwandte Themen

- Benachrichtigungen & Einstellungen — Push-Benachrichtigungen aktivieren und auf das Einstellungs-Sheet zugreifen
- TLS-Zertifikate — der Bedienerbildschirm, auf dem der bei der Kopplung verwendete Fingerabdruck angezeigt wird
- Fehlerbehebung — allgemeine Hilfe bei Anmelde- und Verbindungsproblemen

8.3 Benachrichtigungen & Einstellungen

Die Mobile-App kann Alarmbenachrichtigungen direkt auf Ihr Gerät senden, sodass Sie die Pulse Web-Anwendung nicht geöffnet halten müssen, um zu erfahren, wann Ihre Aufmerksamkeit gefragt ist.

Berechtigung für Benachrichtigungen erteilen

Wenn die App Ihren Pulse-Server zum ersten Mal lädt, fragt Ihr Betriebssystem, ob Pulse Ihnen Benachrichtigungen senden darf. Tippen Sie auf **Erlauben**, um Push-Benachrichtigungen auf diesem Gerät zu aktivieren.

Lehnen Sie die Abfrage ab, funktioniert die App weiterhin, aber es werden keine Push-Benachrichtigungen ausgeliefert. Sie können diese Entscheidung später in den Geräteeinstellungen ändern — siehe Benachrichtigungen erneut aktivieren unten.

Was Sie empfangen

Push-Benachrichtigungen folgen denselben Regeln wie alle anderen Pulse-Alarmkanäle. Ob Ihr Gerät bei einem bestimmten Vorfall alarmiert wird, hängt ab von:

- Dem Schweregrad des Vorfalls
- Der Eskalationsrichtlinie, die für den betroffenen Monitor gilt
- Wer aktuell im Bereitschaftsplan eingetragen ist

Welche Kanäle (Push, E-Mail, SMS, Telefon) Sie für jeden Schweregrad empfangen möchten, legen Sie im Benachrichtigungscenter oder in Ihren Konto-Einstellungen fest — diese Einstellungen werden zwischen Web-Anwendung und Mobile-App geteilt.

Symbole in Benachrichtigungen

Jede Push-Benachrichtigung beginnt mit einem Symbol, das Ihnen bereits vor dem Öffnen zeigt, was geschehen ist — hilfreich, wenn sich mehrere Benachrichtigungen zum selben Vorfall auf dem Sperrbildschirm stapeln:

Titel	Bedeutung
□ *Vorfallname*	Ein neuer Vorfall wurde ausgelöst und Sie werden dafür alarmiert.

Titel	Bedeutung
□ *Vorfallname* bestätigt	Jemand hat den Vorfall übernommen. Der Text nennt die Person — Sie müssen nicht ebenfalls reagieren.
□ *Vorfallname* behoben	Der Vorfall ist abgeschlossen. Es bleibt nichts zu tun.
□ *Vorfallname*	Eine Kollegin oder ein Kollege hat diesen Vorfall persönlich an Sie eskaliert, außerhalb der automatischen Eskalationsrichtlinie. Der Text nennt die absendende Person.

Eine □-Alarmierung wird auch dann zugestellt, wenn der Vorfall bereits bestätigt wurde oder Sie sich außerhalb Ihrer konfigurierten Betriebszeiten befinden, denn jemand hat Sie bewusst ausgewählt — wie das Eskalieren funktioniert, beschreibt Vorfälle.

Die Symbole erscheinen in den Push-Benachrichtigungen auf Ihrem Gerät. Das Benachrichtigungscenter in der Web-Anwendung listet andere Meldungen auf und verwendet sie nicht.

Benachrichtigungstöne

Pulse-Benachrichtigungen haben eigene Töne, sodass Sie sie von anderen Apps unterscheiden können, ohne auf das Display zu sehen:

Ton	Erklingt bei
Ein kurzer Zweiklang	□ bestätigt und □ behoben sowie Beginn und Ende Ihrer Bereitschaft — für Sie bleibt nichts zu tun
Derselbe Zweiklang, gefolgt von drei Alarmstößen	□ neue Vorfälle und □ persönliche Eskalationen — alles, wofür Sie alarmiert werden

Die Töne folgen den Toneinstellungen Ihres Geräts. Ein stummgeschaltetes Telefon unterdrückt sie; Pulse kann den Stummschalter nicht übergehen. Benachrichtigungen, die Sie alarmieren (□, □), werden als zeitkritisch zugestellt: Sie durchbrechen Fokus-Modi und werden nie in eine geplante Zusammenfassung verschoben — es sei denn, Sie schalten **Zeitkritische Mitteilungen** für Pulse Dispatch in den Einstellungen aus. Die Benachrichtigungen mit Zweiklang respektieren den Fokus wie jede andere Benachrichtigung. Wenn Sie bei kritischen Vorfällen auch nachts erreichbar sein müssen, aktivieren Sie für diese Schweregrade zusätzlich den Telefonkanal in Ihren Einstellungen.

Um die Benachrichtigungen zu behalten, aber die Töne abzuschalten, öffnen Sie **Einstellungen**, scrollen Sie zu **Pulse Dispatch**, tippen Sie auf **Mitteilungen** und deaktivieren Sie **Töne**.

Benachrichtigungen erneut aktivieren

Wenn Sie die Berechtigungsabfrage zuvor abgelehnt haben oder Benachrichtigungen später wieder einschalten möchten, tun Sie dies in den Geräteeinstellungen:

- **iOS** — öffnen Sie **Einstellungen**, scrollen Sie zu **Pulse Dispatch**, tippen Sie auf **Mitteilungen** und aktivieren Sie **Mitteilungen erlauben**.

Kehren Sie anschließend zur Pulse-App zurück; der neue Berechtigungsstatus wird automatisch übernommen.

Einstellungs-Sheet

Die mobile Hülle hat nur wenige eigene Einstellungen. Sie sind über das Sheet **Serverkonfiguration** erreichbar:

1. Halten Sie auf dem Startbildschirm den kleinen Anfasser am oberen Bildschirmrand etwa 1,5 Sekunden lang gedrückt.
2. Das Sheet wird von unten eingeblendet und bietet:
   - **Server-URL** — den Pulse-Server ändern, mit dem dieses Gerät gekoppelt ist.
   - **Verbinden** — die neue Adresse prüfen und speichern.
   - **Standard wiederherstellen** — zum gehosteten Pulse Cloud-Dienst zurückkehren.
   - **Trennen und neu konfigurieren** — die gespeicherte Adresse löschen und zum Bildschirm der erstmaligen Kopplung zurückkehren.

Eine vollständige Anleitung zum Koppeln und erneuten Koppeln der App finden Sie unter Einrichtung & Verbindung.

Verwandte Themen

- Benachrichtigungen — das Benachrichtigungscenter in der App
- Schweregrade — wählen, welche Kanäle pro Schweregrad genutzt werden
- Einstellungen — E-Mail, SMS und Telefonkanäle einrichten
- Einrichtung & Verbindung — App mit Ihrem Pulse-Server verbinden

Teil 9 · Appliance

9.1 Übersicht

Die Pulse-Appliance ist ein schlüsselfertiges NixOS-Gerät, auf dem der Pulse-Server vorinstalliert läuft. Anlagenbediener und IT-Personal vor Ort verwalten das Gerät über eine textbasierte Bedienoberfläche (TUI) auf der Konsole — Sie müssen sich nicht in eine Shell einloggen oder Konfigurationsdateien von Hand bearbeiten.

So erreichen Sie die TUI

- **Über die Konsole**: Die Appliance meldet sich auf tty1 automatisch als Benutzer `pulse` an und startet direkt die TUI. Schließen Sie einen Monitor und eine Tastatur an, um sie lokal zu bedienen.
- **Über das Netzwerk**: Melden Sie sich per SSH als Benutzer `pulse` an der Appliance an. Die TUI startet beim Login automatisch.

In diesem Abschnitt

- Installation — Installieren Sie die Appliance vom ISO-Abbild und schließen Sie die Erstkonfiguration ab.
- Netzwerk — Konfigurieren Sie IP-Adresse, Gateway und DNS-Server der Appliance.
- TUI-Referenz — Jeder Menüeintrag, den der Bediener auf der Konsole sieht, an einer Stelle.
- TLS-Zertifikate — Verwalten Sie das Zertifikat, das die Weboberfläche im Browser ausliefert.
- SFTP-Zugang — Richten Sie SFTP-Schlüssel für den Dateiaustausch mit Kunden ein.
- SSH-Zugang — Gewähren Sie Support-Mitarbeitern Shell-Zugriff auf die Appliance.
- Systemupdates — Spielen Sie ein signiertes Update-Bundle von USB, CD/DVD-ROM oder SFTP ein, mit automatischem Backup und Rollback.
- Betrieb — Erstellen Sie Datenbank-Sicherungen und setzen Sie auf eine vorherige Version zurück.

9.2 Bereitstellungsoptionen

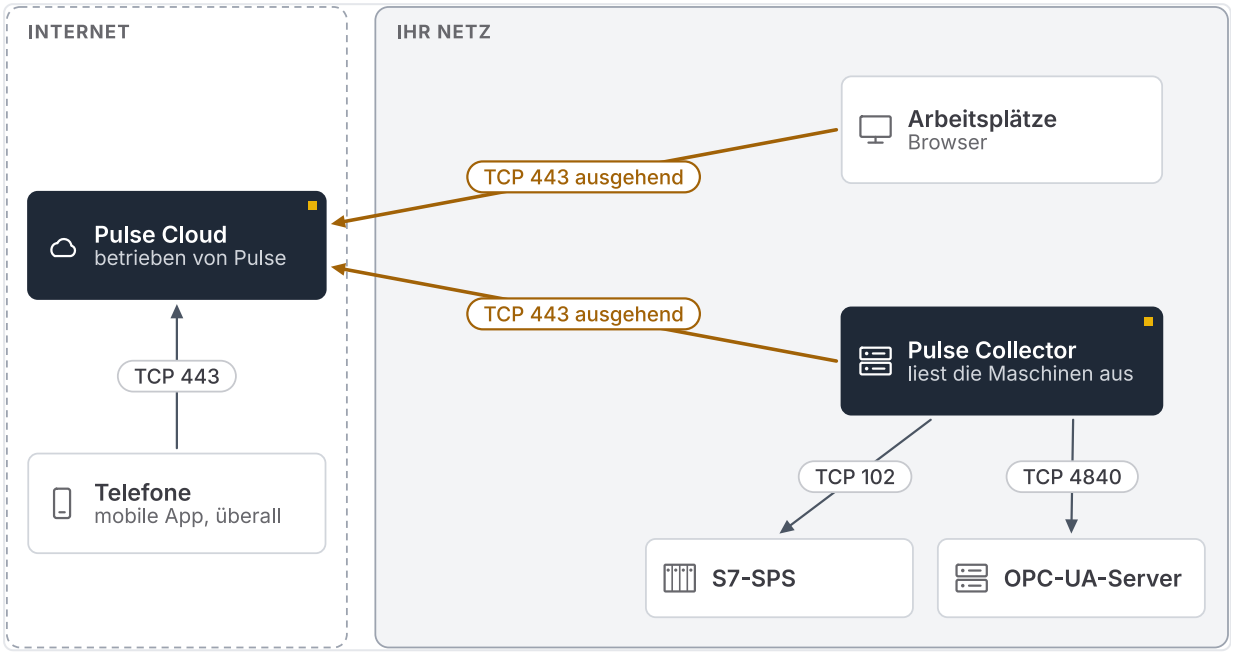
Pulse läuft wahlweise als gehosteter Dienst oder als Appliance in Ihrem eigenen Netz. Diese Seite erklärt, was jede Variante von Ihrem Netz verlangt, damit Sie Ihrer IT- und Sicherheitsabteilung schon vor dem Installationstermin die passende Antwort geben können.

Entscheidend ist meist nicht, wo die Software läuft, sondern **welche Seite die jeweilige Verbindung aufbaut**. Genau darauf antwortet jedes Diagramm auf dieser Seite.

Pulse Cloud

Pulse Cloud ist der gehostete Dienst: Wir betreiben und aktualisieren die Anwendung, Sie warten keinen Server, und die mobile App funktioniert von überall. Eine kleine Komponente läuft dennoch bei Ihnen vor Ort, denn Ihre Maschinen werden ausschließlich aus Ihrem eigenen Netz heraus ausgelesen.

Ein **Collector** läuft in Ihrem eigenen Netz. Er liest Ihre Maschinen lokal aus und baut eine einzige Verbindung nach außen zu Pulse Cloud auf — in dieselbe Richtung wie die Appliance und aus demselben Grund. Er wird einmalig mit einem Code an Pulse gekoppelt, siehe Collector-Kopplung.



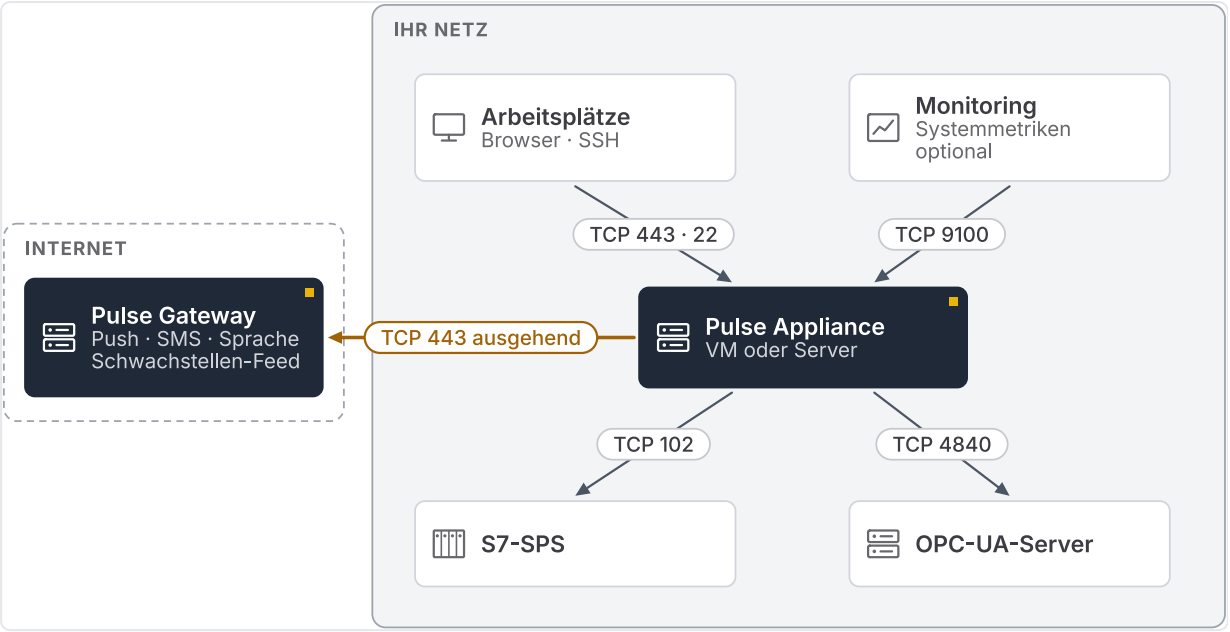
Pfeile zeigen weg von der Seite, die die Verbindung aufbaut. Ihre Maschinen werden ausschließlich von innen erreicht, und jede Verbindung zur Cloud wird von innen nach außen aufgebaut.

Daraus folgen zwei Dinge. In Ihr Produktionsnetz wird nie von außen hineingegriffen: Das Einzige, was mit Ihren Maschinen spricht, steht in Ihrem Netz und gehört Ihnen. Und weil die Verbindung zur Cloud von innen aufgebaut wird, ist **zu keinem Zeitpunkt eine eingehende Freigabe nötig** — dieselbe Eigenschaft, die die Appliance heute schon hat.

Pro Standort läuft ein Collector, und mehrere Standorte laufen in einer gemeinsamen Ansicht zusammen — genau das, was die Appliance nicht leisten kann.

Appliance im eigenen Netz

Die Appliance ist Pulse als einzelne virtuelle Maschine oder als Server, den Sie selbst betreiben. Sie liest die Maschinen von innen aus, und die Messwerte bleiben dort. Stehen Ihre Maschinen in einem eigenen Produktionsnetz, liest ein Pulse Collector sie dort aus und gibt die Messwerte an die Appliance weiter — siehe Getrennte IT- und OT-Netze.



Pfeile zeigen weg von der Seite, die die Verbindung aufbaut. Eine Verbindung verlässt Ihr Netz, aufgebaut von der Appliance. Von außen baut nichts eine Verbindung auf, und die Messwerte bleiben vor Ort.

Aus Ihrem eigenen Netz **zur Appliance hin** brauchen Sie zwei Ports: **443** für die Weboberfläche und **22** für Administration und Dateiaustausch. Port 80 antwortet ausschließlich mit einer Weiterleitung auf 443. Die Systemmetriken der Appliance sind aus dem Netz nicht erreichbar; Pulse liest sie lokal unter `http://localhost:9100/metrics`, wenn Sie sie als Prometheus-Datenquelle anlegen.

Nach außen baut die Appliance eine einzige Verbindung zum Pulse Gateway auf Port **443** auf. Über sie laufen Push-Benachrichtigungen, SMS- und Sprachalarme sowie der Schwachstellen-Feed. Alarme und die Aktionen **Bestätigen** und **Lösen** kommen über

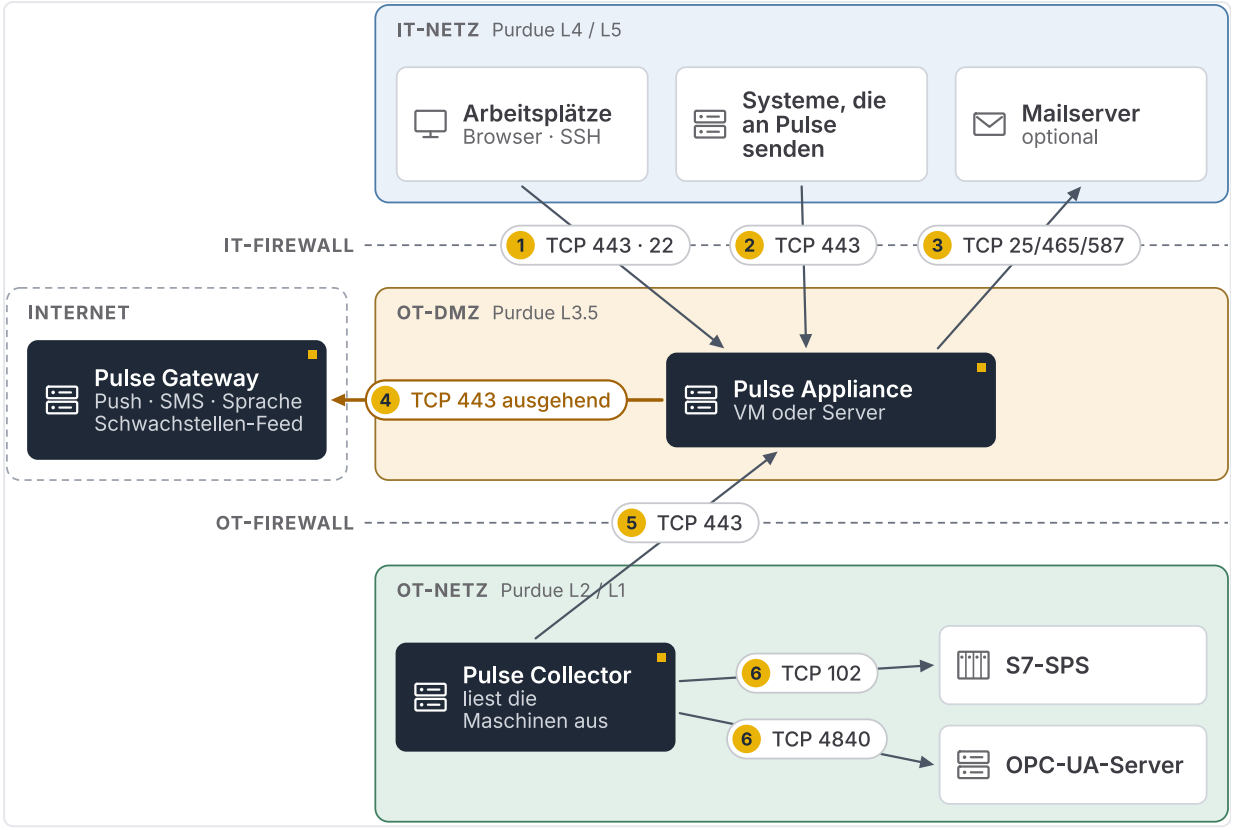
dieselbe Verbindung zurück — deshalb ist dafür nie eine eingehende Freigabe nötig.

Sie können diese Verbindung auch vollständig sperren. Die Appliance meldet den Ausfall als Vorfall, überwacht weiter und alarmiert weiterhin per E-Mail und Webhook. Zusammen mit Ihrem eigenen Mailserver, der Offline-Lizenzierung und Updates von Wechselmedien ist ein vollständig abgekoppelter Betrieb damit eine unterstützte Betriebsart.

Getrennte IT- und OT-Netze

Wo Produktions- und Büronetz strikt getrennt sind, gehört die Appliance in die demilitarisierte Zone dazwischen, und ein Pulse Collector liest die Maschinen im Produktionsnetz aus. Der Collector baut eine einzige Verbindung hinauf zur Appliance auf, deshalb muss ins Produktionsnetz hinein nichts freigegeben werden.

Das entspricht der Struktur, die eine Sicherheitsprüfung erwartet. Arbeitet Ihre Prüfung mit **Zonen und Conduits** — dem Modell der IEC 62443 —, dann sind die drei Netzebenen unten die Zonen und die nummerierten Firewall-Regeln die Conduits dazwischen. Jede Regel gilt in eine Richtung und benennt genau einen Port, sodass sie einzeln geprüft werden kann. Pulse ist auf dieses Modell hin entworfen; zertifiziert nach der Norm ist es nicht, und die Tabelle unten beschreibt die Installation, sie ist keine Konformitätsaussage.



Pfeile zeigen weg von der Seite, die die Verbindung aufbaut, und die Nummern entsprechen den Firewall-Regeln unten. Die Farbe steht für die Vertrauensstufe: Büronetz, kontrollierte DMZ, geschütztes Produktionsnetz.

Die kleinere Alternative: eine Appliance in beiden Netzen

Wo die Trennung weniger strikt ist — ein einzelnes Werk, ein Team, keine DMZ, in die sich etwas stellen ließe — kann eine Appliance mit zwei Ethernet-Anschlüssen selbst in beiden Netzen hängen und die Maschinen direkt auslesen statt über einen Collector. Geben Sie ihr einen Anschluss im Büronetz und einen im Produktionsnetz; den zweiten richten Sie nach der Installation über den Bildschirm Network Configuration ein, beschrieben unter Netzwerk.

Pulse bietet am Anschluss zum Produktionsnetz weder die Weboberfläche noch SSH an. Nur der Anschluss im Büronetz antwortet auf 443 und 22 — im Produktionsnetz steht damit weiterhin keine administrative Schnittstelle, und Regel 1 unten beschreibt nach wie vor den einzigen Weg hinein.

Zwei Gründe sprechen dennoch für die Collector-Topologie: Sie ist die einzige Variante, die funktioniert, wenn zwischen beiden Netzen eine Firewall steht und kein Host beide verbinden darf, und sie ist die einzige, die mehrere Standorte in einer gemeinsamen Ansicht abdeckt.

Gegenüber einer Prüfung nach Zonen und Conduits ist sie außerdem die schwächere Antwort. Eine Appliance in beiden Netzen stellt einen Host in zwei Zonen; damit wird der Host selbst zum Conduit, und die Frage der Prüfung verschiebt sich von „welche Regeln verbinden diese Zonen" zu „was kann diese Maschine passieren". Was Pulse dazu sagen kann: Zwischen beiden Netzen wird nichts weitergeleitet, und der Anschluss zum Produktionsnetz antwortet auf keinem Port — weder Weboberfläche noch SSH. Der Conduit transportiert Messwerte in eine Richtung und bietet in die andere nichts an. Ob das akzeptabel ist, entscheidet die Prüfung; klären Sie es besser, bevor die Appliance eingebaut wird, als danach.

Notwendige Firewall-Regeln

#	Von	Nach	Port	Wofür
1	Arbeitsplätze	Appliance	TCP 443	Die Weboberfläche
1	Administration	Appliance	TCP 22	Konsolenzugriff und Dateiaustausch
2	Systeme, die an Pulse senden	Appliance	TCP 443	Trigger- und Heartbeat-Monitore
3	Appliance	Ihr Mailserver	TCP 25, 465 oder 587	E-Mail-Alarme

#	Von	Nach	Port	Wofür
4	Appliance	Pulse Gateway	TCP 443, ausgehend	Push, SMS, Sprache und der Schwachstellen-Feed
5	Pulse Collector	Appliance	TCP 443	Weitergabe der Messwerte an die Appliance
6	Pulse Collector	S7-SPS	TCP 102	Auslesen Ihrer Maschinen
6	Pulse Collector	OPC-UA-Server	TCP 4840	Auslesen Ihrer Maschinen
	Administration im OT-Netz	Pulse Collector	TCP 22	*(Optional)* Konsolenzugriff und Dateiaustausch, nur solange SSH in der TUI eingeschaltet ist
	IT-Netz und DMZ	OT-Netz	—	Nichts. Ins Produktionsnetz hinein ist keine Verbindung nötig.
	Internet	Appliance	—	Nichts. Es ist keine eingehende Freigabe aus dem Internet nötig.

Jede Regel gilt nur in eine Richtung. Auf die letzten beiden Zeilen kommt es bei einer Sicherheitsprüfung meist an.

Auf welchem Port Ihre OPC-UA-Server lauschen, haben Sie selbst festgelegt; 4840 ist der übliche Standard. S7 nutzt seinen Standardport und ist nicht konfigurierbar — siehe Siemens S7 und OPC UA.

Wenn etwas an Pulse sendet

Trigger-Monitore und Heartbeat-Monitore arbeiten umgekehrt zu den Monitoren, die Pulse ausliest: Das sendende System baut die Verbindung auf und schickt seine Daten an Port 443 der Appliance. Zeile 2 deckt Sender im IT-Netz ab. Ein Sender im Produktionsnetz braucht eine eigene Regel — Produktionsnetz zur Appliance, TCP 443.

Die meisten Standorte vermeiden diese Regel, indem sie solche Sender dorthin stellen, wo die Appliance ohnehin schon steht: in die DMZ oder ins IT-Netz. Muss ein Sender im Produktionsnetz bleiben, beschränken Sie die Regel auf diesen einen Host und diesen einen Port.

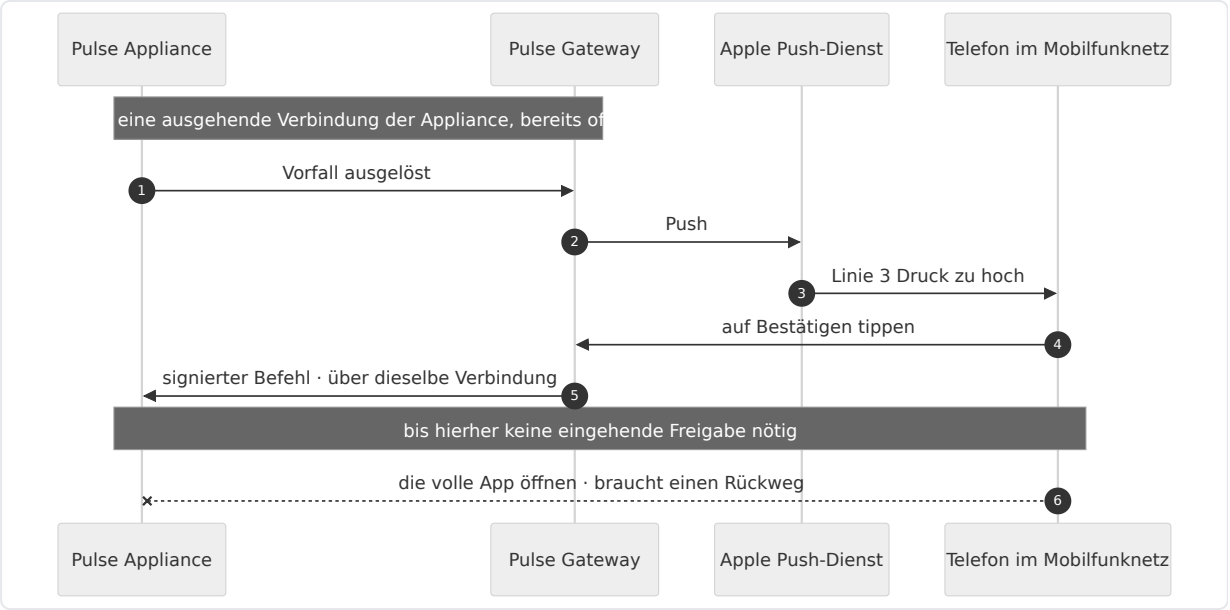
Was Ihr Netz verlässt

Mit der Appliance bleiben die Überwachungsdaten vor Ort. Ihre Messwerte, die Konfiguration Ihrer Monitore und Ihre Tags werden nirgendwohin übertragen. Was das Netz verlässt, beschränkt sich auf den Alarmierungsweg — und ein Alarm muss benennen, worum es geht, also reisen Namen mit:

Verlässt das Netz	Enthält
Push-Benachrichtigung	Titel und Text des Vorfalls, die den Vorfall und den auslösenden Monitor benennen, seinen Schweregrad, einen Link zurück auf den Vorfall in Ihrer Appliance sowie die Kennung des zu benachrichtigenden Geräts
SMS und Sprachanrufe	Rufnummer der Empfängerin und den Nachrichtentext
E-Mail	Nur, wenn kein eigener Mailserver hinterlegt ist. Hinterlegen Sie einen unter Einstellungen, versendet die Appliance direkt
Schwachstellenabgleich	Bestellnummer und Firmware-Version eines Geräts, damit Sicherheitshinweise dazu zugeordnet werden können
Geteilte Berichte	Vor dem Versand verschlüsselt und verschlüsselt gespeichert. Nur das Passwort der Empfängerin öffnet den Bericht, und dieses Passwort steht in derselben E-Mail wie der Link

Mobilgeräte außerhalb des Standorts

Eine Appliance in Ihrem Netz ist aus dem Mobilfunknetz nicht erreichbar. Das wiegt weniger schwer, als es zunächst klingt, denn alarmiert zu werden und zu reagieren setzt das nicht voraus.



Die Schritte 1 bis 5 kommen ohne eingehende Freigabe aus. Nur Schritt 6 braucht eine.

Benachrichtigungen erreichen ein Telefon überall, weil die Appliance sie über die bereits von ihr aufgebaute Verbindung hinausschickt. **Auch das Bestätigen und Lösen eines Vorfalls direkt aus der Benachrichtigung funktioniert überall** — ohne dass das Telefon Ihr Netz überhaupt erreicht.

Die Ausnahme ist das Öffnen der vollständigen App: Sie lädt die Pulse-Oberfläche von Ihrer Appliance, das Telefon braucht dafür also einen Weg dorthin. Drei übliche Antworten, in der Reihenfolge, in der sich die meisten Standorte entscheiden:

1. **Die Trennung akzeptieren.** Ihre Rufbereitschaft wird überall alarmiert und kann den Vorfall sofort übernehmen; untersucht wird später im Firmennetz.
2. **Ihr vorhandenes Mobilgerätemanagement nutzen**, um der App eine VPN-Verbindung mitzugeben.
3. **Die Weboberfläche über Ihren eigenen Reverse Proxy veröffentlichen**, mit Ihrem Zertifikat und Ihrer Authentifizierung davor.

Wie Sie die App auf Ihren Server zeigen lassen, steht unter Einrichtung & Kopplung.

Weiterführend

- Collector-Kopplung — einen Collector mit der Appliance verbinden, bei der er sich meldet
- Collector-Status — was der Bildschirm eines Collectors zeigt, wenn er die Appliance nicht erreicht
- Installation — die Appliance installieren, wenn Sie sich für diesen Weg entschieden haben

- Netzwerk — der Appliance eine feste Adresse geben
- TLS-Zertifikate — das Zertifikat, das die Weboberfläche vorzeigt
- Systemupdates — aktualisieren ohne Internetverbindung

9.3 Installation

Diese Seite beschreibt die Installation von Pulse auf einer frischen Maschine — entweder als **Appliance** oder als **Collector**, der sich bei einer Appliance meldet. Der Ablauf ist derselbe, ob das Ziel ein kleiner Industrie-PC, ein Rackserver oder eine virtuelle Maschine ist — booten Sie das ISO-Abbild, wählen Sie eine Rolle, beantworten Sie einige Fragen in der Installer-TUI und warten Sie, bis die Maschine in die Bedienoberfläche neu startet.

Die Schritte unten entsprechen der Reihenfolge des Installations-Assistenten, den Sie auf der Konsole sehen, exakt.

Hardware-Anforderungen

Die Appliance ist bewusst genügsam:

- **CPU**: 2 Kerne (x86_64). Jede moderne Intel- oder AMD-CPU ist geeignet.
- **Arbeitsspeicher**: mindestens 4 GB, empfohlen 8 GB für Standorte mit mehr als wenigen hundert Monitoren.
- **Festplatte**: mindestens 32 GB. SSD wird ausdrücklich empfohlen — die Datenbank erzeugt genug zufällige I/O-Last, dass eine konventionelle Festplatte die Weboberfläche spürbar verlangsamt.
- **Firmware**: UEFI oder Legacy-BIOS — beides wird unterstützt. Das ISO-Abbild ist ein Hybrid-Image und startet in beiden Modi.
- **Netzwerk**: mindestens ein Ethernet-Anschluss. Ein zweiter Anschluss wird unterstützt und lohnt sich, wenn die Maschinen in einem eigenen Netz stehen. WLAN wird nicht unterstützt.

Die Zielfestplatte wird während der Installation **vollständig gelöscht**. Wenn die Maschine mehrere Festplatten besitzt, können Sie im Installer auswählen, welche verwendet wird — alle Daten auf der ausgewählten Festplatte gehen jedoch verloren, sobald Sie die Installation bestätigen.

ISO-Abbild auf einen USB-Stick schreiben

Sie benötigen einen USB-Stick mit mindestens 4 GB. Jedes Werkzeug, das eine rohe Blockkopie des ISO auf den Stick anlegt, ist geeignet — das Abbild ist direkt bootfähig, ein Partitionieren oder Formatieren entfällt.

- **Linux / macOS**: `sudo dd if=pulse.iso of=/dev/sdX bs=4M status=progress conv=fsync` (ersetzen Sie `/dev/sdX` durch das tatsächliche Gerät — `lsblk` bzw. `diskutil list` zeigen es an). Wenn Sie das falsche Gerät angeben, löschen Sie die falsche Festplatte; prüfen Sie sorgfältig, bevor Sie bestätigen.
- **Windows**: nutzen Sie Rufus im Modus **DD-Image** (nicht ISO-Modus). Wählen Sie das ISO, wählen Sie den USB-Stick, klicken Sie auf Start.
- **Plattformübergreifende GUI**: Balena Etcher läuft auf allen drei Betriebssystemen und versteckt die manuelle Geräteauswahl.

Der erstellte USB-Stick bootet sowohl auf UEFI- als auch auf Legacy-BIOS-Systemen, sodass Sie denselben Stick für jedes Ziel verwenden können.

Erster Start

Stecken Sie den USB-Stick in die Zielmaschine und schalten Sie sie ein. Möglicherweise müssen Sie während der Firmware-Startanzeige eine Taste drücken, um das Bootmenü zu öffnen — übliche Tasten sind `F12`, `F11`, `F10`, `F2`, `Esc` oder `Entf`, je nach Hersteller.

Wählen Sie im Bootmenü den USB-Stick aus. Das Appliance-ISO lädt und führt Sie nach wenigen Sekunden in die Installer-TUI auf tty1. Es gibt keinen grafischen Installer — die gesamte Einrichtung erfolgt tastaturgesteuert über die Konsole.

Wenn die Maschine stattdessen in das vorhandene Betriebssystem bootet, ist die Bootreihenfolge in der Firmware falsch konfiguriert. Starten Sie neu, öffnen Sie das Firmware-Setup und ändern Sie entweder die Bootpriorität oder verwenden Sie erneut das Einmal-Bootmenü.

Installations-Assistent

Der Assistent führt Sie in einer festen Abfolge von Bildschirmen durch die Einrichtung. Der erste Bildschirm legt die Rolle fest, und diese Wahl entscheidet, welche der folgenden Bildschirme Sie sehen — Festplatte, Netzwerk und NTP sind bei beiden Rollen gleich, was danach kommt nicht. Navigieren Sie mit den Pfeiltasten (oder `j` / `k`), bestätigen Sie mit `Enter` und gehen Sie mit `Esc` einen Schritt zurück. `Strg+C` bricht die Installation vollständig ab.

Role

Als Erstes fragt der Installer, welche Rolle Sie installieren: **Appliance** oder **Collector**. Wählen Sie mit den Pfeiltasten und bestätigen Sie mit `Enter`.

- **Appliance** ist ein eigenständiger Pulse-Server. Diese Rolle beschreibt der Rest dieser Seite, sofern ein Schritt nichts anderes sagt.
- **Collector** meldet sich bei einer Appliance, statt selbst die Weboberfläche zu betreiben. Er überspringt den Basis-URL-Schritt und fragt stattdessen nach der Appliance, bei der er sich meldet, und einem Pairing-Code — wie diese Kopplung funktioniert, beschreibt Collector-Kopplung.

Welcome

Der Startbildschirm benennt den Assistenten und fasst kurz zusammen, was für die gewählte Rolle folgt: Festplattenauswahl, Netzwerkkonfiguration, optionaler NTP-Server und danach entweder eine Basis-URL (Appliance) oder eine Appliance-Adresse und ein Pairing-Code (Collector). Er weist Sie zudem darauf hin, dass die Zielfestplatte gelöscht wird. Drücken Sie `Enter`, um zu beginnen, oder `Strg+C`, um abzubrechen.

Disk

Der Installer ermittelt alle Festplatten, auf die installiert werden kann, und listet sie auf. Jede Zeile zeigt den Gerätenamen (zum Beispiel `/dev/sda`), die Größe und die Modellbezeichnung, die die Firmware meldet. Markieren Sie das Ziel mit den Pfeiltasten und bestätigen Sie mit `Enter`.

Warnung. Die hier ausgewählte Festplatte wird vollständig gelöscht. Sobald die Installation beginnt, gibt es kein Zurück mehr. Wenn die Maschine sowohl eine Betriebssystem-Festplatte als auch eine separate leere Festplatte besitzt, vergewissern Sie sich kurz, welche welche ist — Modellbezeichnung und Größe reichen normalerweise zur Unterscheidung.

Network

Hat die Maschine mehr als einen Ethernet-Anschluss, beginnt der Bildschirm mit einer Liste dieser Anschlüsse. Wählen Sie den Anschluss, über den die Appliance erreicht werden soll — den, der im Netz der Personen steckt, die Pulse nutzen. Jeder Eintrag zeigt die Hardware-Adresse, ob ein Kabel eingesteckt ist, und eine eventuell schon bezogene Adresse. Genügt das nicht, um zwei baugleiche Anschlüsse zu unterscheiden, drücken Sie `d` und ziehen das Kabel des gewünschten Anschlusses ab und wieder ein — der Installer erkennt ihn und wählt ihn aus. Bei einer Maschine mit nur einem Anschluss entfällt dieser Schritt.

Während der Installation wird ausschließlich dieser eine Anschluss konfiguriert. Braucht die Appliance zusätzlich einen Anschluss in einem zweiten Netz, richten Sie diesen nach dem ersten Start über den Bildschirm Network Configuration ein — siehe Netzwerk.

Wählen Sie anschließend, wie die Appliance ihre IP-Adresse bezieht:

- **DHCP** — das Netz vergibt Adressen automatisch. Die meisten internen LANs und viele Anlagennetze funktionieren so. Wählen Sie diese Option, wenn Sie unsicher sind.
- **Statische IP** — das LAN-Team hat eine feste IP-Adresse für die Appliance reserviert. Diese Wahl blendet drei zusätzliche Felder ein: die IP-Adresse (in CIDR-Notation, z. B. `192.168.1.100/24`), das Gateway und einen DNS-Server.

Die Eingaben werden vor dem nächsten Schritt validiert — Tippfehler oder unmögliche Werte erzeugen eine Fehlermeldung, und Sie bleiben auf der Seite, bis sie korrigiert sind. Siehe Netzwerk für Hinweise zur Wahl der statischen IP und zum späteren Wechsel des Modus.

NTP

Optional. Lassen Sie das Feld leer, um die standardmäßigen öffentlichen NTP-Server zu verwenden — das genügt, wenn die Appliance Internetzugang hat. Wenn der Standort einen internen Zeitserver nutzt, tragen Sie hier seinen Hostnamen oder seine IP ein, dann synchronisiert sich die Appliance gegen diesen Server. Drücken Sie `Enter`, um fortzufahren.

BaseURL

Dieser Schritt erscheint nur für die Rolle **Appliance**. Ein Collector hat keine eigene Basis-URL — siehe Appliance-Adresse weiter unten.

Die URL, unter der die Weboberfläche und die Kopplung der Mobile-App die Appliance erreichen. Das ist die Adresse, die Bediener im Browser eingeben und die die Mobile-App beim Koppeln eines Telefons speichert.

- Wenn die Appliance einen DNS-Namen im LAN hat, verwenden Sie diesen (`https://pulse-system.example.local`).
- Andernfalls verwenden Sie die im vorigen Schritt vergebene IP-Adresse (`https://192.168.1.100`).
- Geben Sie immer das Schema mit an (`https://`). Reine Hostnamen werden abgelehnt.

Eine fehlerhafte Basis-URL können Sie später in der TUI ändern; vorher gekoppelte Mobile-Geräte müssen jedoch neu gekoppelt werden — eine korrekte Eingabe spart also Aufwand.

Appliance-Adresse

Dieser Schritt und der Pairing-Code-Schritt danach ersetzen bei der Rolle **Collector** den Basis-URL-Schritt.

Geben Sie die IP-Adresse oder den Hostnamen der Appliance ein, optional gefolgt von einem Port nach einem Doppelpunkt — lassen Sie den Port weg, nimmt der Installer `443` an. Meist ist das eine IP-Adresse; alles Weitere, um die Appliance zu erreichen, ermittelt der Collector selbst.

Verbindet sich der Collector nicht mit einer Appliance, sondern mit Pulse Cloud, geben Sie auf dieselbe Weise die Domain ein, die unter **Organisation > Einstellungen > Collectors** angezeigt wird — zum Beispiel `app.pulsehq.de`.

Pairing-Code

Geben Sie den auf der Appliance angezeigten Pairing-Code im Format `XXXX-XXXX-XXXX` ein. Groß- und Kleinschreibung spielen keine Rolle, und die Bindestriche sind optional — `ab12cd34ef56` und `AB12-CD34-EF56` werden beide akzeptiert. Den Code erhalten Sie über den Dialog **Organisation > Einstellungen > Collectors > Collector hinzufügen** der Appliance; siehe Collector-Kopplung dafür, woher der Code kommt und was zu tun ist, wenn er bis hierhin schon abgelaufen ist.

Ein falsch eingegebener Code wird sofort abgelehnt, mit einem Hinweis, ihn zu prüfen und es erneut zu versuchen — Sie müssen dafür nicht bis zum Confirm-Bildschirm warten.

Confirm

Der Assistent zeigt alle eingegebenen Werte auf einem Bildschirm zusammengefasst, damit Sie sie prüfen können, bevor irgendetwas auf die Festplatte geschrieben wird. Der Hinweis auf das Löschen der Festplatte wird wiederholt. Drücken Sie `Enter`, um die eigentliche Installation zu starten, oder `Esc`, um eine Antwort zu ändern.

- **Appliance**: Festplatte, Netzwerkmodus (und gegebenenfalls die Details der statischen IP), NTP-Server und Basis-URL.
- **Collector**: Rolle, Festplatte, Netzwerkmodus (und gegebenenfalls die Details der statischen IP), NTP-Server, Appliance-Adresse und Pairing-Code.

Progress

Nach der Bestätigung partitioniert der Installer die Festplatte, kopiert das Systemabbild für die gewählte Rolle und schreibt die Konfiguration. Fortschrittszeilen erscheinen laufend auf dem Bildschirm. Drücken Sie jederzeit `l`, um das vollständige Installer-Log einzublenden — hilfreich, wenn der Assistent bei einem langwierigen Schritt zu pausieren scheint und Sie wissen wollen, was tatsächlich passiert.

Die Installation dauert auf einer SSD typischerweise wenige Minuten; konventionelle Festplatten benötigen wegen Partitionierung und Kopiervorgang deutlich länger. Schalten Sie die Maschine in dieser Phase nicht aus.

Done

Wenn der Installer fertig ist, erscheint der **Done**-Bildschirm. Bei Erfolg bestätigt er die abgeschlossene Installation und bietet einen Neustart an — drücken Sie `Enter`, um neu zu starten, und ziehen Sie den USB-Stick während des BIOS-POST ab, damit die Maschine von der frisch installierten Festplatte startet.

Schlägt die Installation fehl, zeigt der Bildschirm stattdessen die Fehlermeldung; `l` öffnet das Log, damit Sie nachsehen können, was schiefgegangen ist, und `Esc` bringt Sie zurück zum Confirm-Schritt, um eine Antwort anzupassen und es erneut zu versuchen. `Strg+C` beendet, ohne neu zu starten.

Nach dem Neustart erscheint eine Appliance mit der TUI als Standardkonsole und ist betriebsbereit. Ein Collector erscheint stattdessen auf seinem Collector-Status-Bildschirm und koppelt sich im Hintergrund mit der eingegebenen Adresse und dem Code an die Appliance — siehe Collector-Kopplung dafür, was danach passiert, einschließlich eines inzwischen abgelaufenen Codes.

9.4 Netzwerk

Diese Seite beschreibt die Netzwerkänderungen im laufenden Betrieb — wie Sie eine Appliance zwischen DHCP und einer festen IP-Adresse umschalten, was die Felder im statischen Modus bedeuten, wie Sie eine Appliance einrichten, die an zwei Netzen gleichzeitig hängt, und wie die Anwenden- und Zurücksetzen-Schritte verhindern, dass Sie sich selbst aussperren. Der hier beschriebene Bildschirm ist **Network Configuration** in der TUI.

Den Netzwerkmodus wählen Sie auch während der Installation. Auf einer laufenden Appliance ändern Sie ihn jedoch über diesen Bildschirm und nicht durch eine Neuinstallation.

DHCP oder statisch — wann was sinnvoll ist

Der Bildschirm Network Configuration zeigt oben zwei Modi an: **DHCP (automatic)** und **Static IP**. Er startet immer in dem Modus, den die Appliance gerade verwendet; mit den Pfeiltasten wechseln Sie zwischen den beiden.

- **DHCP** ist der Standard und die richtige Wahl, wenn das Netz Adressen automatisch vergibt. Die meisten Büro-LANs und viele Anlagennetze funktionieren so. Sie müssen sonst nichts eingeben — der DHCP-Modus hat keine weiteren Felder.
- **Statische IP** ist erforderlich, wenn im Netz kein DHCP-Server vorhanden ist oder die Appliance eine feste Adresse braucht. Zwei Situationen machen die statische Konfiguration unvermeidlich: Die Mobile-App speichert die Adresse der Appliance auf jedem gekoppelten Telefon — wechselt der DHCP-Lease unbemerkt, sind alle Kopplungen ungültig. Und jedes externe Monitoring oder ein Reverse-Proxy, der auf die Appliance zeigt, braucht eine Adresse, die sich nicht ändert.

Der Moduswechsel ist nicht destruktiv — die vorherige Konfiguration wird gesichert, bevor etwas geschrieben wird. Sie können also zwischen DHCP und statisch hin- und herwechseln und bei Bedarf zurücksetzen. Siehe Anwenden, zurücksetzen und Sicherungen.

Die drei Felder für die statische IP

Wenn Sie Static IP wählen, erscheinen drei Felder unter der Modusauswahl. Mit `Tab` (oder den Pfeiltasten) wechseln Sie zwischen den Feldern.

- **IP Address** — die Adresse der Appliance in CIDR-Notation: Adresse und Präfixlänge der Subnetzmaske, getrennt durch einen Schrägstrich. Beispiel: `192.168.1.100/24`. Der `/24`-Teil ist Pflicht — ohne Präfixlänge kann die Appliance nicht ermitteln, welche anderen Hosts zum selben Subnetz gehören.
- **Gateway** — die IP-Adresse des Routers, der den Verkehr aus dem lokalen Subnetz hinausleitet. Ohne diesen Eintrag erreicht die Appliance zwar andere Hosts im LAN, aber weder das Internet noch andere Netze. Fragen Sie Ihr LAN-Team nach der Gateway-Adresse; sie ist meist die erste oder letzte nutzbare Adresse im Subnetz (z. B. `192.168.1.1` oder `192.168.1.254`).
- **DNS Server** — die IP-Adresse des Resolvers, mit dem die Appliance Hostnamen in IP-Adressen auflöst. Wenn am Kundenstandort ein interner DNS-Server existiert, ist dieser meist die bessere Wahl, weil er auch standortinterne Namen (Dateiserver, Anlagensysteme) auflösen kann, die öffentliche Resolver nicht kennen. Ein öffentlicher Resolver wie `8.8.8.8` funktioniert als Fallback, wenn kein interner Resolver verfügbar ist.

Die TUI weist offensichtlich fehlerhafte Eingaben zurück: eine IP-Adresse ohne Präfixlänge oder einen Gateway- bzw. DNS-Eintrag, der keine gültige IPv4-Adresse ist (Hostnamen wie `dns.example.com` werden nicht akzeptiert — verwenden Sie die IP des Resolvers). Die Fehlermeldung erscheint rot unter den Feldern, und die Änderung wird nicht übernommen — korrigieren Sie den Wert und drücken Sie erneut auf Anwenden.

Appliances mit mehr als einem Netzwerkanschluss

Manche Appliances hängen an zwei Netzen gleichzeitig — typischerweise an einem zum Büronetz, über das die Weboberfläche erreicht wird, und an einem zum Produktionsnetz, in dem die Maschinen stehen. Hat die Appliance mehr als einen Ethernet-Anschluss, öffnet Network Configuration zuerst eine Liste dieser Anschlüsse statt direkt der Modusauswahl:

```
> enp1s0    primary     static 192.168.1.100/24
  enp2s0    additional  static 10.10.0.5/24 · no services
  enp3s0    —           not configured
```

Mit den Pfeiltasten wählen Sie einen Anschluss aus, mit `Enter` konfigurieren Sie ihn. `Esc` führt zurück zur Liste. Bei einer Appliance mit nur einem Anschluss entfällt die Liste — es gibt nichts auszuwählen.

Bei einer Appliance, die installiert wurde, bevor dieser Bildschirm Anschlüsse unterscheiden konnte, ist kein Anschluss als primärer hinterlegt. Beim ersten Öffnen ermittelt Pulse, welcher das ist, markiert ihn und nennt den Anschluss samt Begründung:

- Er trägt die Adresse, mit der die Appliance konfiguriert ist, oder
- er führt die Standardroute — der Anschluss, über den der Verkehr der Appliance das Gerät tatsächlich verlässt, und genau das macht den primären Anschluss aus, oder
- er ist der einzige Anschluss mit einer Adresse.

Bis Sie anwenden, wird nichts geschrieben; mit `p` auf einem anderen Anschluss überschreiben Sie die Auswahl.

Trifft nichts davon zu — mehrere Anschlüsse mit Adresse und keine Standardroute darunter —, wird kein Anschluss markiert, und die Liste weist darauf hin. Zusätzliche Anschlüsse lassen sich erst konfigurieren, wenn einer markiert ist: Markieren Sie den Anschluss, über den Pulse erreicht wird, und drücken Sie `p`.

Herausfinden, welcher Anschluss welcher ist

Anschlüsse werden danach benannt, wo ihre Karte im Gerät sitzt, und diese Reihenfolge muss nicht der Anordnung der Buchsen auf der Rückseite entsprechen. Bei einem Server mit vier baugleichen Buchsen kann die Zuordnung zwischen Namen und Buchsen beliebig sein.

Drücken Sie `d`, und die Appliance ermittelt es für Sie: Ziehen Sie das Kabel des gewünschten Anschlusses ab und stecken Sie es wieder ein — dieser Anschluss wird ausgewählt. Die Liste aktualisiert sich innerhalb von ein bis zwei Sekunden und bestätigt, welcher erkannt wurde. Sie müssen vorher nichts anderes abziehen; erkannt wird nur der Anschluss, an dem sich etwas ändert.

Wird kein Kabel bewegt, bricht die Suche nach etwa einer Minute ab und meldet das; mit `Esc` beenden Sie sie früher. In beiden Fällen können Sie den Anschluss weiterhin von Hand aus der Liste wählen — jeder Eintrag zeigt seine Hardware-Adresse, die meist mit einer Beschriftung auf der Karte übereinstimmt, und ob gerade ein Kabel steckt.

Wenn eine Netzwerkkarte getauscht oder umgesteckt wird

Anschlüsse werden danach benannt, wo ihre Karte im Gerät sitzt. Wird eine Karte in einen anderen Steckplatz gesetzt — oder das Mainboard getauscht —, kann sich der Name daher ändern. Pulse merkt sich, um welche Karte es sich bei jedem konfigurierten Anschluss handelt, und folgt ihr: Beim nächsten Start bindet sich die Konfiguration an den neuen Namen, und die Appliance ist wieder unter derselben Adresse erreichbar wie zuvor.

Dabei wird nichts umbenannt, und an Ihrer Konfiguration ändert sich nichts. Öffnen Sie danach Network Configuration, zeigt die Liste den neuen Namen zu den unveränderten Einstellungen.

Das gilt für Anschlüsse, die über diesen Bildschirm oder während der Installation konfiguriert wurden. Eine Appliance, die vor dieser Erfassung eingerichtet wurde, übernimmt sie, sobald Sie das nächste Mal eine Netzwerkänderung anwenden.

Primärer und zusätzliche Anschlüsse

Ein Anschluss ist der **primäre** (`primary`). Er führt Gateway und DNS-Server, und über seine Adresse wird Pulse erreicht: die Weboberfläche, gekoppelte Telefone und alle Collectors nutzen sie. Er bietet immer Weboberfläche und SSH an.

Jeder weitere Anschluss ist ein **zusätzlicher** (`additional`). Er existiert, damit Pulse Maschinen in einem zweiten Netz lesen kann. Er erhält eine Adresse, aber kein eigenes Gateway und keinen eigenen DNS-Server, weil nur ein Anschluss diese bereitstellen kann. Eine zweite Standardroute ist die häufigste Ursache dafür, dass eine Appliance an zwei Netzen den Kontakt zum ersten verliert.

Um die primäre Rolle auf einen anderen Anschluss zu verschieben, markieren Sie ihn und drücken `p` . Der bisherige primäre Anschluss behält seine Adresse und wird zu einem zusätzlichen. Tragen Sie Gateway und DNS-Server für den neuen primären Anschluss ein — die alten Werte beschrieben das alte Netz und werden deshalb geleert.

Die drei Modi eines zusätzlichen Anschlusses

- **DHCP (automatic)** — das zweite Netz vergibt eine Adresse. Ein dort ebenfalls angebotenes Gateway und ein DNS-Server werden ignoriert.
- **Static IP** — Sie vergeben eine feste Adresse. Es erscheint nur das Adressfeld, kein Gateway- und kein DNS-Feld.
- **No address (PROFINET only)** — der Anschluss bleibt aktiv, erhält aber überhaupt keine Adresse. Die PROFINET-Gerätesuche findet Steuerungen in diesem Segment trotzdem, weil sie keine Adresse benötigt. In diesem Zustand startet ein Anschluss, bevor Sie ihn konfigurieren, und er ist die richtige Wahl für ein Segment, das Sie nur nach PROFINET-Geräten durchsuchen wollen.

Jeder Anschluss braucht sein eigenes Subnetz. Zwei Anschlüsse im selben Subnetz werden beim Anwenden abgelehnt: Pulse kann dann nicht entscheiden, welcher zu verwenden ist, und der zweite würde nicht als eigenes durchsuchbares Netz erscheinen.

Maschinen hinter einem Router erreichen

Ein zusätzlicher Anschluss erreicht sein eigenes Subnetz ohne weiteres Zutun. Stehen die Maschinen in einem anderen Subnetz, hinter einem Router innerhalb des Produktionsnetzes, ergänzen Sie eine Route, damit die Appliance den Weg dorthin kennt. Das Feld **Routes** erscheint, sobald der Anschluss eine feste Adresse hat:

```
10.10.5.0/24 via 10.10.0.1
```

Zu lesen als: „um das Netz `10.10.5.0/24` zu erreichen, gib den Verkehr an den Router `10.10.0.1` ". Mehrere Routen trennen Sie durch Kommas. Lassen Sie das Feld leer, wenn die Maschinen im selben Subnetz wie der Anschluss stehen — das ist der Regelfall.

Das Gateway einer Route muss selbst im Subnetz des Anschlusses liegen. Ein Router, den der Anschluss nicht direkt erreicht, kann für ihn nichts weiterleiten; die Appliance lehnt die Route deshalb ab, statt eine Einstellung zu übernehmen, die wirkungslos bliebe.

Eine Route auf `0.0.0.0/0` ist hier nicht möglich. Das wäre eine zweite Standardroute, und die hat nur der primäre Anschluss — siehe Primärer und zusätzliche Anschlüsse. Routen gibt es außerdem nur an einem Anschluss mit fester Adresse: Vergeben Sie zuerst eine statische IP, wenn der Anschluss Routen braucht.

Weboberfläche und SSH an einem zusätzlichen Anschluss

Ein zusätzlicher Anschluss bietet **weder** Weboberfläche **noch** SSH an. Das ist Absicht — ein Anschluss zum Produktionsnetz soll dort keine administrative Schnittstelle bereitstellen. Die Liste zeigt den Zustand ausdrücklich an, `no services` oder `serves web UI and SSH`, damit Sie ihn nie vermuten müssen.

Wenn Pulse an einem Standort doch aus dem zweiten Netz erreichbar sein soll, markieren Sie den Anschluss und drücken `s`. Ein erneutes `s` schaltet es wieder ab. Der primäre Anschluss ist davon nicht betroffen; er bietet beides immer an.

Was die Appliance durchsucht

Sobald ein zusätzlicher Anschluss eine Adresse hat, erscheint dessen Netz in der Weboberfläche auf der Seite **Assets > Geräte suchen** als durchsuchbares Netz. Sie müssen das Subnetz nicht eintippen — die Appliance kennt es bereits. Ein Anschluss im Modus **No address** erscheint dort nicht, die PROFINET-Suche erreicht ihn aber trotzdem.

Anwenden, zurücksetzen und Sicherungen

Am unteren Bildschirmrand finden Sie die verfügbaren Tastenkürzel:

```
tab navigate • ctrl+s apply • ctrl+r revert • esc back
```

`Strg-S` **übernimmt die Änderung.** Vor dem Schreiben der neuen Konfiguration legt die Appliance eine Sicherung der vorherigen an. Wenn anschließend alles erwartungsgemäß funktioniert — das Gateway antwortet auf Ping, DNS löst auf, die Weboberfläche ist

erreichbar — sind Sie fertig. Unter dem Formular erscheint die kurze Bestätigung `Network configuration applied`.

`Strg-R` **setzt auf die vorherige Konfiguration zurück.** Das ist Ihr Sicherheitsnetz für den Fall, dass Sie sich selbst ausgesperrt haben. Wiederhergestellt wird der primäre Anschluss — der, über den Sie sich aussperren können; zusätzliche Anschlüsse behalten ihre aktuellen Einstellungen. Ein typisches Szenario: Ein Bediener wechselt auf statische IP, vertippt sich beim Gateway, und die Appliance ist von der Arbeitsstation aus nicht mehr erreichbar. Die TUI auf der lokalen Konsole ist trotzdem verfügbar — melden Sie sich dort an, öffnen Sie Network Configuration und drücken Sie `Strg-R`; die vorherigen (funktionierenden) Einstellungen sind wiederhergestellt. Den erfolgreichen Rollback meldet der Bildschirm mit `Reverted to previous network configuration`.

Unter dem Meldungsbereich zeigt der Bildschirm, wie viele frühere Konfigurationen für ein Rollback aufbewahrt werden (z. B. `2 previous config(s) available for rollback`). Der Zähler steigt mit jeder übernommenen Änderung — ein schneller Test, ob Ihre Änderung tatsächlich geschrieben wurde, ist, nach dem Anwenden zu prüfen, ob der Zähler um eins gestiegen ist.

Mit `Esc` verlassen Sie den Bildschirm, ohne zu übernehmen. Die Eingaben in den Feldern werden verworfen — nichts wird geschrieben, bevor `Strg-S` gedrückt wird.

Eine sichere Reihenfolge für eine statische IP-Änderung

Wenn Sie keinen physischen Konsolenzugriff haben und über SSH arbeiten, ist der Zurücksetzen-Pfad der Unterschied zwischen einer Fünf-Minuten-Änderung und einem Vor-Ort-Termin. Wir empfehlen folgende Reihenfolge:

1. Stellen Sie sicher, dass Sie die Konsole erreichen können — entweder physisch an der Appliance oder über ein Remote-KVM/iLO/iDRAC, falls die Hardware das unterstützt. Die TUI auf der Konsole funktioniert unabhängig von der Netzwerkkonfiguration.
2. Notieren Sie sich die aktuellen Einstellungen auf einem Stück Papier, bevor Sie beginnen, damit Sie wissen, wie der funktionierende Zustand aussah.
3. Wechseln Sie auf statisch, füllen Sie die drei Felder aus und drücken Sie `Strg-S`.
4. Prüfen Sie von einer zweiten Arbeitsstation aus (nicht von der, an der Sie per SSH angemeldet sind), ob die Appliance unter der neuen IP-Adresse erreichbar ist — per Ping, durch Aufruf der Weboberfläche oder beides.
5. Wenn etwas nicht stimmt, melden Sie sich an der Konsole an und drücken Sie `Strg-R`. Die vorherige Konfiguration wird wiederhergestellt, und die Appliance ist wieder erreichbar.

Wo die Konfiguration liegt

Wird von der TUI verwaltet — nicht von Hand bearbeiten

Die Netzwerkeinstellungen werden in `/var/pulse/site.env` persistiert. Behandeln Sie diese Datei als TUI-verwaltet: Jede Änderung sollte über den Bildschirm Network Configuration laufen, damit die Sicherung angelegt und die abhängigen Dienste (networkd, die Basis-URL der Weboberfläche) in der richtigen Reihenfolge neu geladen werden. Eine direkte Bearbeitung der Datei umgeht beides, und die nächste Übernahme aus der TUI überschreibt Ihre Änderungen ohnehin.

Wenn Sie vermuten, dass die Datei beschädigt oder nicht mehr aktuell ist, ist der sicherste Weg zur Wiederherstellung derselbe wie oben beschrieben — `Strg-R` setzt auf die vorherige funktionierende Sicherung zurück, statt dass Sie die Datei von Hand bearbeiten müssen.

Verwandte Bildschirme

Der Bildschirm Network Configuration kümmert sich ausschließlich um IP-Einstellungen. Zwei verwandte Themen liegen an anderer Stelle in der TUI:

- **NTP Configuration** — legt den Zeitserver fest. Zeit und IP sind voneinander unabhängig: Eine Änderung des Netzwerkmodus ändert die NTP-Einstellung nicht und umgekehrt.
- **TLS Certificates** — verwaltet das Zertifikat, das die Weboberfläche im Browser ausliefert. Die Subject Alternative Names (SANs) des Zertifikats enthalten die IP-Adresse der Appliance — nach einer statischen IP-Änderung sollten Sie das Zertifikat daher gegebenenfalls neu erzeugen oder neu installieren, damit es zur neuen Adresse passt. Zusätzliche Anschlüsse mit fester Adresse sind automatisch enthalten; für einen Anschluss im DHCP-Modus tragen Sie dessen Adresse auf jenem Bildschirm in die SAN-Liste ein.

Siehe die TUI-Referenz für die vollständige Liste der Menüeinträge und die Seite Installation für den entsprechenden Netzwerkschritt während der Erstkonfiguration.

9.5 TLS-Zertifikate

Diese Seite beschreibt, wie Sie als Bediener das TLS-Zertifikat verwalten, das die Appliance auf ihrer Weboberfläche ausliefert. Der hier beschriebene Bildschirm ist **TLS Certificates** in der TUI.

Der Bildschirm besteht aus zwei Bereichen.

- Der **Statusbereich** oben zeigt Betreff, Aussteller, den Gültigkeitszeitraum (mit einer Warnung in der Zeile, sobald das Zertifikat in weniger als 30 Tagen abläuft), die IP- und DNS-SANs, die das Zertifikat abdeckt, den SHA256-Fingerabdruck sowie eine `Typ:`-Zeile, die ausweist, ob das aktive Zertifikat selbstsigniert oder kundenseitig bereitgestellt ist.
- Die **Aktionsliste** unten bietet **CSR erstellen**, **Zertifikat hochladen** und **Selbstsigniertes Zertifikat wiederherstellen** an — sowie **CSR abbrechen**, sobald eine Anfrage auf die Signatur wartet.

Befinden sich beim Öffnen des Bildschirms bereits Zertifikatsdateien im SFTP-Austauschverzeichnis, erscheint unter dem Statusbereich ein Hinweis wie `1 Zertifikat im SFTP bereit — Hochladen zum Anwenden` als Erinnerung, dass noch Arbeit ansteht.

Mit `r` aktualisieren Sie die Hauptansicht jederzeit — nützlich, wenn ein Kunde gerade Dateien per SFTP hochgeladen hat und der Hinweis erscheinen soll, ohne dass Sie den Bildschirm verlassen.

Auslieferungszustand

Eine frisch installierte Appliance erzeugt beim ersten Start ein **selbstsigniertes** Zertifikat und liefert es auf der Weboberfläche aus. Eine öffentliche CA ist nicht beteiligt, daher warnen Browser beim ersten Besuch — das ist so erwartet.

Für reine LAN- oder Headless-Installationen reicht das selbstsignierte Zertifikat oft aus: Die Mobile-App ist nicht auf eine öffentliche CA angewiesen. Sie verifiziert die Appliance stattdessen über den **Fingerabdruck**, sodass eine Kopplung auch mit selbstsigniertem Zertifikat sicher ist. Den Ablauf finden Sie unten unter Fingerabdruck und Kopplung mit der Mobile-App.

Möchten Sie, dass Browser das Zertifikat ohne Warnung akzeptieren — oder gibt es Vorgaben, ein kundenseitiges Zertifikat einzuspielen — verwenden Sie wie unten beschrieben **Zertifikat hochladen**. Um jederzeit zum Appliance-eigenen Zertifikat zurückzukehren, verwenden Sie **Selbstsigniertes Zertifikat wiederherstellen**.

Ein CA-signiertes Zertifikat anfordern

Signiert Ihre CA Zertifikate auf Basis einer Zertifikatsignierungsanfrage (CSR), kann die Appliance die Anfrage und den passenden privaten Schlüssel für Sie erzeugen — der private Schlüssel verlässt die Appliance dabei nie.

1. Wählen Sie auf dem Bildschirm **TLS Certificates CSR erstellen** und bestätigen Sie. Das aktive Zertifikat liefert weiter aus; es wird lediglich ein neuer ausstehender Schlüssel angelegt. Die Anfrage übernimmt die IP- und DNS-Namen der Appliance, damit das signierte Zertifikat dieselben Adressen abdeckt.
2. Verbinden Sie sich per SFTP und laden Sie `pulse-csr.pem` aus dem Ordner `downloads/` herunter; reichen Sie die Datei dann bei Ihrer CA ein. Den SFTP-Zugang richten Sie auf dem Bildschirm SFTP-Zugang ein.
3. Solange die Anfrage auf die Signatur wartet, zeigt der Statusbereich den Hinweis `CSR wartet auf CA-Signierung` an, und es erscheint die Aktion **CSR abbrechen**.
4. Wenn die CA das signierte Zertifikat zurückgibt, spielen Sie es mit **Zertifikat hochladen** ein (siehe unten). Da eine Anfrage aussteht, prüft die Appliance das Zertifikat automatisch gegen den ausstehenden Schlüssel — Sie laden keinen Schlüssel hoch.

Existiert bereits eine Anfrage und Sie erzeugen eine weitere, wird der ausstehende Schlüssel ersetzt und ein bereits eingereichter CSR ungültig. Um eine Anfrage zu verwerfen, ohne etwas einzuspielen, wählen Sie **CSR abbrechen** — das entfernt ausstehenden Schlüssel und Anfrage und lässt das aktive Zertifikat unberührt.

Eigenes Zertifikat hochladen

Die Aktion **Zertifikat hochladen** nimmt ein PEM-kodiertes Zertifikat und optional einen PEM-kodierten privaten Schlüssel entgegen. Zwei Lieferwege werden unterstützt: ein USB-Stick, der an die Appliance angeschlossen wird, oder Dateien, die im SFTP-Austauschverzeichnis bereitgestellt werden. Validierung, Installation und Reload laufen in beiden Fällen identisch ab — nur die Quellauswahl unterscheidet sich.

Beide Wege akzeptieren ausschließlich PEM-kodierte Eingaben. Lässt sich eine Datei nicht als PEM parsen oder passen Zertifikat und Schlüssel nicht zusammen, meldet die TUI den Fehler direkt und installiert **nichts**; das bisherige aktive Zertifikat bleibt im Einsatz.

Die Abfrage nach dem Schlüssel passt sich daran an, ob zuvor ein CSR erzeugt wurde:

- Liegt ein ausstehender Schlüssel in `tls-key-pending.pem` (Sie haben einen CSR erzeugt und installieren nun das signierte Zertifikat, das von der CA zurückkam), wird das hochgeladene Zertifikat allein gegen den ausstehenden Schlüssel geprüft.

- Andernfalls wird das Zertifikat gegen den aktuell aktiven Schlüssel geprüft — sinnvoll, wenn nur das Zertifikat selbst rotiert wird.
- Wählen Sie zusätzlich eine Schlüsseldatei aus, wird das Zertifikats-/Schlüsselpaar gemeinsam geprüft, bevor irgendetwas auf die Festplatte geschrieben wird.

Per USB

Diesen Weg verwenden Sie, wenn Sie mit einem Stick vor Ort an der Appliance stehen.

1. Kopieren Sie das PEM-Zertifikat (und den privaten Schlüssel, falls Sie ihn rotieren) auf einen USB-Stick, der mit FAT32 oder ext4 formatiert ist. Dateien müssen die Endung `.pem` tragen, damit die Auswahl sie findet.
2. Stecken Sie den Stick in die Appliance. Die TUI hängt ihn schreibgeschützt unter `/mnt/usb` ein.
3. Wählen Sie auf dem Bildschirm **TLS Certificates** zunächst **Zertifikat hochladen** und dann **USB** als Quelle.
4. Werden mehrere USB-Geräte erkannt, wählen Sie das richtige aus. Die TUI durchsucht den Stick dann nach `.pem`-Dateien und zeigt eine Auswahl. Werden keine `.pem`-Dateien gefunden, kehrt die Ansicht mit einer Fehlermeldung zur Quellauswahl zurück — kopieren Sie die Dateien in das Wurzelverzeichnis oder ein oberstes Verzeichnis und versuchen Sie es erneut.
5. Wählen Sie die Zertifikatsdatei aus und drücken Sie `Enter`. Die TUI parst das PEM. Schlägt das Parsen fehl, erscheint eine rote Fehlermeldung und die Auswahl bleibt offen — korrigieren Sie die Datei und versuchen Sie es erneut.
6. Anschließend fragt die TUI, ob Sie auch eine neue Schlüsseldatei hochladen möchten. Wählen Sie den Schlüssel vom selben Stick aus, oder überspringen Sie, wenn Sie den aktuell aktiven Schlüssel (oder, falls zuvor ein CSR erstellt wurde, den ausstehenden Schlüssel in `tls-key-pending.pem`) weiterverwenden.
7. Bei Erfolg wird das Zertifikat installiert, nginx mit dem neuen Paar neu geladen und die Hauptansicht erscheint mit grüner Bestätigung. Der Stick wird automatisch wieder ausgehängt.

Drücken Sie unterwegs `Esc` — etwa nachdem Sie die falsche Zertifikatsdatei ausgewählt haben — geht die TUI einen Schritt zurück. Aus der Zertifikatsauswahl bringt `Esc` Sie zurück in die Quellauswahl und hängt den Stick aus; aus der Schlüsselabfrage bringt `Esc` Sie zurück in die Zertifikatsauswahl, um eine andere Datei zu wählen.

Per SFTP

Diesen Weg verwenden Sie, wenn der Kunde das Zertifikat lieber über das Netzwerk liefert, statt einen USB-Stick zu transportieren. Voraussetzung: Der Kunde kann sich am SFTP-Austausch anmelden — per SSH-Schlüssel oder mit dem Passwort der Appliance;

siehe SFTP-Zugang, wie Sie das einrichten.

1. Der Kunde lädt das Zertifikat (und den Schlüssel, falls getrennt) in das Austauschverzeichnis unter `uploads/certificates/`. Aus seiner Sicht verbindet er sich per SFTP als Benutzer `pulse-transfer` mit der Appliance und legt die Dateien mit `put` ab.
2. Liegen Dateien bereit, zeigt der Bildschirm TLS Certificates einen Hinweis wie `1 Zertifikat im SFTP bereit — Hochladen zum Anwenden` an. Wählen Sie **Zertifikat hochladen** und dann **Aus SFTP-Austausch** als Quelle.
3. Die TUI listet jede `.pem`-Datei unter `uploads/certificates/` auf. Wählen Sie das Zertifikat aus, beantworten Sie die Schlüsselabfrage und bestätigen Sie. Die Validierungsregeln sind dieselben wie beim USB-Weg.
4. Bei Erfolg werden die übernommenen Dateien aus dem Austauschverzeichnis entfernt und ein Audit-Eintrag geschrieben, damit später nachvollziehbar bleibt, welche kundenseitige Datei wann angewendet wurde.

Ist eine Datei im Austauschverzeichnis kein gültiges PEM, meldet die TUI das und überspringt die Installation — die Datei bleibt unter `uploads/certificates/` liegen, damit der Kunde sie ersetzen kann. Dasselbe gilt für Zertifikats-/Schlüssel-Inkonsistenzen: Es wird nichts installiert, und die bereitgestellten Dateien bleiben erhalten, damit der Kunde korrigieren und erneut hochladen kann.

Erreichen Sie diesen Bildschirm und die SFTP-Liste ist leer, liegt das meist daran, dass der Kunde in das falsche Unterverzeichnis hochgeladen hat. Dateien für diese Auswahl müssen genau unter `uploads/certificates/` landen; Bundles oder andere PEM-Dateien an anderen Stellen des Austauschverzeichnisses werden vom Bildschirm TLS Certificates ignoriert.

Selbstsigniertes Zertifikat wiederherstellen

Die Aktion **Selbstsigniertes Zertifikat wiederherstellen** erzeugt ein neues, von der Appliance kontrolliertes selbstsigniertes Zertifikat und schaltet die Weboberfläche wieder darauf um. Greifen Sie darauf zurück, wenn:

- Das eingespielte Kundenzertifikat sich als falsch herausstellt (falscher Betreff, vor der Installation abgelaufen, von der falschen CA signiert).
- Das eingespielte Zertifikat abgelaufen ist und kein Ersatz bereitsteht — das Wiederherstellen des selbstsignierten Zertifikats versetzt die Appliance in einen funktionierenden HTTPS-Zustand, damit Sie die Weboberfläche weiter erreichen.
- Sie eine kundenspezifische Konfiguration entfernen, bevor die Appliance anderswo erneut bereitgestellt wird.

Die Bestätigungsabfrage warnt, dass das aktuelle Zertifikat ersetzt wird und nginx neu geladen wird. Ein eventuell ausstehender CSR wird im Zuge der Wiederherstellung aufgeräumt — eine veraltete `tls-key-pending.pem` aus einem nicht abgeschlossenen CSR-Vorgang wird best-effort entfernt. Ist das aktive Zertifikat bereits selbstsigniert, bietet die Abfrage an, es trotzdem neu zu erzeugen; das ergibt einen frischen Fingerabdruck bei unverändertem `Typ: Selbstsigniert`.

Das neue selbstsignierte Zertifikat wird mit der aktuellen Site-IP der Appliance (gelesen aus `/var/pulse/site.env`) als einer der SANs erzeugt. Im DHCP-Modus kann die Site-IP leer sein, in diesem Fall wird der IP-SAN weggelassen; das ist normal und beeinträchtigt die Kopplung mit der Mobile-App nicht, da diese den Fingerabdruck und nicht den SAN verwendet.

Entfernte Collectors sind nicht betroffen

Ein entfernter Collector verwendet nicht das Zertifikat auf diesem Bildschirm. Er verifiziert die Appliance stattdessen über sein eigenes, dediziertes Collector-Zertifikat, das einmalig bei der ersten Kopplung des Collectors geprüft wird — siehe Fingerabdruck prüfen.

Da die beiden Zertifikate unabhängig voneinander sind, unterbricht das Erstellen eines CSR, das Hochladen eines Zertifikats oder das Wiederherstellen des selbstsignierten Zertifikats auf diesem Bildschirm nie die Verbindung zu einem bereits gekoppelten Collector.

Fingerabdruck und Kopplung mit der Mobile-App

Die Zeile **Fingerabdruck** im Statusbereich von TLS Certificates zeigt den SHA256-Fingerabdruck des aktiven Zertifikats, mit Doppelpunkten als Trennzeichen (zum Beispiel `AB:CD:EF:...`). Diesen Wert fragt die Pulse Mobile-App bei der erstmaligen Kopplung zum Abgleich ab.

Da die Appliance häufig ein selbstsigniertes Zertifikat ausliefert, kann sich die Mobile-App nicht auf eine öffentliche CA stützen, um den Server zu authentifizieren. Stattdessen zeigt die App den Fingerabdruck des Zertifikats, das sie empfangen hat, und bittet Sie, ihn mit dem auf diesem Bildschirm angezeigten Wert zu vergleichen. Sie müssen Zeichen für Zeichen übereinstimmen. Stimmen sie nicht überein, brechen Sie die Kopplung ab — entweder wird die Verbindung mitgelesen, oder Sie betrachten die falsche Appliance.

Der Fingerabdruck ändert sich, sobald sich das Zertifikat ändert — also auch bei jeder Verwendung von **Selbstsigniertes Zertifikat wiederherstellen**, weil dabei das Schlüsselpaar neu erzeugt wird. Nach einer Wiederherstellung (oder nach dem Hochladen

eines neuen Zertifikats) zeigen bereits gekoppelte Mobilgeräte beim nächsten Verbindungsaufbau eine Fingerabdruck-Warnung an; bestätigen Sie den neuen Fingerabdruck dann erneut über diesen Bildschirm.

Verwandte Bildschirme

- SFTP-Zugang — autorisiert den Kunden, per SSH-Schlüssel oder mit dem Passwort der Appliance, für den oben beschriebenen SFTP-Weg.
- Mobile-App: Einrichtung & Verbindung — wie die Mobile-App den auf diesem Bildschirm angezeigten Fingerabdruck zur Prüfung der Appliance nutzt.
- Collector-Kopplung — wie ein entfernter Collector diese Appliance verifiziert und ihr vertraut, über sein eigenes, separates Zertifikat.
- TUI-Referenz — das vollständige Bediener-Menü.

9.6 SFTP-Zugang

Diese Seite beschreibt, wie Sie als Bediener Personen außerhalb der Appliance autorisieren — einen Hersteller, einen Kundenadministrator oder einen Bereitschaftsmitarbeiter im Support — Dateien per SFTP auf der Appliance abzulegen. Der hier beschriebene Bildschirm ist **SFTP Access** in der TUI.

Der Zugang hier autorisiert ausschließlich das *Hochladen von Dateien* — gleich, ob die Gegenseite sich mit ihrem eigenen SSH-Schlüssel oder mit dem SFTP-Passwort der Appliance verbindet. Keine der beiden Methoden gewährt einen Shell-Zugang auf der Appliance — das ist ein eigener Bereich, der über den Bildschirm SSH-Zugang verwaltet wird.

Wann brauchen Sie das

SFTP-Zugang ist die Antwort, wenn eine Datei auf der Appliance landen soll und ein USB-Stick nicht praktikabel ist. Zwei wiederkehrende Situationen:

- **Ein Hersteller muss ein Update-Bundle aus der Ferne liefern.** Der Pulse-Support hat einen neuen Systemtarball gebaut und signiert, und Sie möchten nicht zur Anlage fahren, nur um einen USB-Stick einzustecken. Wenn Sie den öffentlichen Schlüssel des Herstellers hier autorisieren, kann er das Bundle per SFTP in das Austauschverzeichnis hochladen; Sie übernehmen es anschließend über den Bildschirm Update System.
- **Ein Kunde möchte sein eigenes TLS-Zertifikat einspielen.** Die CA des Kunden hat ein frisches Zertifikat- und Schlüsselpaar für die Weboberfläche der Appliance ausgestellt, und der Kunde möchte es lieber per Netzwerk hochladen als einen USB-Stick zum Rack zu tragen. Wenn Sie den Schlüssel des Kunden hier autorisieren, kann er die PEM-Dateien per SFTP in das Austauschverzeichnis legen; Sie installieren sie anschließend über den Bildschirm TLS Certificates.

In beiden Fällen erhält die autorisierte Gegenseite niemals eine Shell — sie kann nur Dateien in das Austauschverzeichnis legen. Die TUI ist die Grenze, an der entschieden wird, was mit diesen Dateien geschieht.

Passwort-Anmeldung

Nicht jede Gegenseite besitzt einen SSH-Schlüssel, und nur für eine einzelne Lieferung einen einzurichten, ist oft mehr Aufwand, als es sich lohnt. Für diese Fälle akzeptiert die Appliance auch ein Passwort, das mit jedem grafischen SFTP-Client funktioniert —

FileZilla, WinSCP, Cyberduck und dergleichen.

Die Appliance erzeugt ihr eigenes SFTP-Passwort beim ersten Start und zeigt es oben auf dem Bildschirm **SFTP Access** unter **Passwort-Anmeldung (beliebiger SFTP-Client)** an:

- **Host** — die IP-Adresse der Appliance.
- **Port** — `22`.
- **Benutzer** — `pulse-transfer`.
- **Passwort** — angezeigt als fünf Vierergruppen (`xxxx-xxxx-xxxx-xxxx-xxxx`), direkt von der Konsole ablesbar.

Geben Sie diese vier Werte über einen vertrauenswürdigen Kanal an die Gegenseite weiter, und sie kann sich sofort verbinden — ein Schlüsselaustausch ist nicht nötig. Die Sitzung ist genauso eingeschränkt wie beim Schlüssel-Zugang: chroot-eingesperrt im Austauschverzeichnis, ohne Shell und ohne Weiterleitung.

Es gibt ein Passwort pro Appliance, das sich alle teilen, die sich auf diesem Weg anmelden — das ist der Kompromiss gegenüber Schlüsseln. Ein Schlüssel kennzeichnet eine einzelne Partei und lässt sich einzeln widerrufen; das Passwort ist ein einziges gemeinsames Geheimnis. Bevorzugen Sie Schlüssel, wenn Sie mehrere Parteien unabhängig autorisieren müssen, und greifen Sie zum Passwort, wenn einfach nur eine Lieferung schnell erfolgen soll.

Das Passwort neu erzeugen

Drücken Sie `g`, um ein frisches Passwort zu erzeugen. Existiert bereits eines, fragt die TUI zuerst nach einer Bestätigung, denn **das aktuelle Passwort funktioniert ab dem Moment der Neuerzeugung sofort nicht mehr** — jeder Client, der es nutzt, auch Ihre eigenen, muss mit dem neuen Wert aktualisiert werden. Bei Erfolg kehrt der Bildschirm mit `SFTP-Passwort neu erzeugt.` und dem angezeigten neuen Passwort zur Liste zurück.

Erzeugen Sie das Passwort neu, sobald eine Lieferung abgeschlossen ist, oder immer dann, wenn Sie vermuten, dass es sich weiter verbreitet hat als beabsichtigt.

Einen Schlüssel einfügen

Der Bildschirm listet die aktuell autorisierten Schlüssel unterhalb des Passwort-Bereichs auf. Die Tastenleiste am unteren Rand zeigt, was verfügbar ist:

```
a Schlüssel einfügen • u von USB • d entfernen • g Passwort neu erzeugen • esc zurück
```

Es gibt zwei Wege, einen Schlüssel hinzuzufügen. Wählen Sie den, der zum Arbeitsablauf passt — das Ergebnis ist identisch.

Den Schlüssel direkt einfügen

Drücken Sie `a`. Ein Eingabefeld erscheint mit dem Platzhalter `ssh-ed25519 AAAA... user@host`.

1. Fragen Sie die Gegenseite nach ihrem öffentlichen SSH-Schlüssel. Es ist der Inhalt einer `.pub`-Datei — eine einzige Zeile, die mit dem Algorithmusnamen beginnt (`ssh-ed25519`, `ssh-rsa`, `ecdsa-sha2-nistp256`), gefolgt vom base64-kodierten Schlüsselmaterial und einem optionalen Kommentar wie `alice@vendor.com`.
2. Fügen Sie die ganze Zeile in das Feld ein. Das Terminal muss Einfügen unterstützen — die meisten modernen Terminal-Emulatoren tun das, und an der Appliance-Konsole fügen Sie üblicherweise mit `Strg-Umschalt-V` oder per mittlerem Mausklick ein, je nach Terminal.
3. Drücken Sie `Enter` zur Bestätigung. Die TUI prüft die Zeile mit `ssh-keygen`. Ist der Schlüssel fehlerhaft, erscheint eine rote Fehlermeldung unter dem Feld und nichts wird hinzugefügt — korrigieren Sie ihn und versuchen Sie es erneut. Ist der Schlüssel bereits in der Liste, weist die TUI ihn mit dem vorhandenen Fingerabdruck zurück, damit Sie wissen, welchen Eintrag Sie ansehen müssen.
4. Bei Erfolg kehrt der Bildschirm zur Liste zurück, der neue Schlüssel erscheint mit seinem SHA256-Fingerabdruck und Kommentar, und eine grüne Statuszeile bestätigt `Key added: SHA256:...`.

Mit `Esc` brechen Sie ab, ohne etwas hinzuzufügen.

Eine `.pub`-Datei von einem USB-Stick auswählen

Drücken Sie `u`. Die TUI durchsucht den eingehängten USB-Stick nach Dateien mit der Endung `.pub` und zeigt eine Auswahl an.

1. Stecken Sie einen USB-Stick mit der `.pub`-Datei der Gegenseite in die Appliance. Die TUI hängt das Laufwerk automatisch unter `/mnt/usb` ein.
2. Drücken Sie zurück im Bildschirm SFTP Access die Taste `u`. Werden keine `.pub`-Dateien gefunden, kehrt der Bildschirm mit der roten Meldung `no .pub files found on USB drive` zur Liste zurück — kopieren Sie die Datei in das Wurzelverzeichnis des USB-Sticks und versuchen Sie es erneut.
3. Wählen Sie mit den Pfeiltasten (oder `j` / `k`) die richtige Datei aus und drücken Sie `Enter`. Die TUI liest die Datei, validiert sie und fügt den Schlüssel hinzu.
4. Wie beim Einfügen kehrt der Bildschirm bei Erfolg mit einer grünen Bestätigung und dem neuen Fingerabdruck zur Liste zurück.

Mit `Esc` brechen Sie an jeder Stelle ab, ohne einen Schlüssel hinzuzufügen.

Die USB-Auswahl ist der richtige Weg, wenn der Kunde Ihnen einen Stick persönlich übergeben hat oder wenn der Schlüssel per E-Mail kam und auf einen Stick statt in die Zwischenablage gespeichert wurde.

Schlüssel auflisten und entfernen

Die Hauptansicht listet jeden autorisierten Schlüssel zeilenweise auf. Jeder Eintrag zeigt den SHA256-Fingerabdruck und das Kommentarfeld des Schlüssels — meist eine E-Mail-Adresse oder eine Hostkennung wie `alice@vendor.com`. Verwenden Sie den Fingerabdruck, um auseinanderzuhalten, welcher Schlüssel welcher ist, wenn mehrere ähnlich aussehen; der Kommentar allein ist nicht beweiskräftig, weil dort beliebiger Text stehen kann.

So entfernen Sie einen Schlüssel:

1. Bewegen Sie die Auswahl mit `↑` / `↓` (oder `k` / `j`) auf die Zeile, die Sie entfernen möchten.
2. Drücken Sie `d`. Eine Bestätigungsabfrage erscheint mit dem Fingerabdruck und dem Kommentar des zu entfernenden Schlüssels.
3. Drücken Sie `y` zur Bestätigung oder `n` (oder `Esc`) zum Abbrechen.

Nach der Bestätigung wird der Schlüssel aus der `authorized_keys`-Datei der Appliance entfernt, und der Bildschirm kehrt mit `Key removed` zur Liste zurück. Die Entfernung wirkt sofort — eine bereits offene SFTP-Sitzung des Schlüsselinhabers bleibt bis zur Trennung verbunden, eine neue Sitzung kann er aber nicht mehr aufbauen.

Was die autorisierte Gegenseite tun kann

Beide Authentifizierungsmethoden — ein autorisierter Schlüssel oder das Passwort — führen zu genau einem SFTP-Benutzer: dem `pulse-transfer`-Prinzipal. Dieser Benutzer ist im Austauschverzeichnis der Appliance chroot-eingesperrt, hat keine Shell, und `AllowTcpForwarding`, `X11Forwarding` sowie `PermitTunnel` sind alle abgeschaltet. Effektiv kann jeder, der sich authentifiziert:

- Sich per SFTP verbinden (Port 22, Benutzername `pulse-transfer`).
- Dateien in den Unterbaum `uploads/` des Austauschverzeichnisses ablegen.
- Dateien aus dem Unterbaum `downloads/` abholen (genutzt für Dateien, die die Appliance zum Download bereitstellt, etwa Backup-Archive und einen erzeugten CSR).
- Sich nicht auf einer interaktiven Shell anmelden.
- Keine TCP-Weiterleitung, keine X11-Sitzung und keinen Tunnel aufbauen.

Den Shell-Zugang auf Bedienerebene — für Support-Mitarbeiter, die Probleme an der Appliance selbst beheben — verwalten Sie getrennt auf dem Bildschirm SSH-Zugang. Die beiden Bildschirme sind voneinander unabhängig: Ein hier autorisierter Schlüssel gewährt keinen Shell-Zugang, und ein dort autorisierter Schlüssel berechtigt nicht zum SFTP-Upload.

Wo die Dateien landen

Per SFTP hochgeladene Dateien landen in `/var/pulse-exchange/uploads/`, aufgeteilt nach Art in Unterverzeichnisse: `updates/` für System-Update-Bundles und `certificates/` für TLS-PEM-Dateien. Die genauen Pfade gehören zur chroot-Sicht des SFTP-Benutzers — die Gegenseite sieht sie als Wurzel ihrer Sitzung.

Sie konsumieren die Dateien nicht von diesem Bildschirm aus. Stattdessen:

- **Update System** bietet die Quelle **SFTP Upload**, die die unter `uploads/updates/` bereitgestellten Bundles auflistet und Sie eines davon zur Installation auswählen lässt.
- **TLS Certificates** bietet die Quelle **From SFTP exchange**, die die unter `uploads/certificates/` bereitgestellten PEM-Dateien auflistet und Sie ein Zertifikat-/Schlüssel-Paar zur Installation auswählen lässt.

Ein wöchentlicher Aufräum-Timer entfernt Dateien, die älter als sieben Tage sind, aus dem Austauschverzeichnis — ein Upload, der dort lange ungenutzt liegt, wird irgendwann eingesammelt. Wenn etwas länger Bestand haben muss, übernehmen Sie es vorher über den zuständigen TUI-Bildschirm.

Verwandte Bildschirme

- SSH-Zugang — verwaltet den Shell-Zugang auf Bedienerebene. Eigenes Prinzipal, eigene Schlüsselliste.
- TUI-Referenz — das vollständige Menü, einschließlich der SFTP-source-Optionen in Update System und TLS Certificates.
- Installation — die Erstkonfiguration, bei der die Appliance bereitgestellt wird, aber noch keine SFTP-Schlüssel konfiguriert sind.

9.7 SSH-Zugang

Diese Seite erklärt, wie Shell-Zugang zur Appliance gewährt wird. SSH-Zugang dient dem Hersteller-Support und dem Dateitransfer — er ist nicht Teil des täglichen Betriebs. Die textbasierte Bedienoberfläche (TUI) erledigt die Routineaufgaben direkt auf der Konsole, und SSH ist nur für jene Fälle vorgesehen, die die TUI nicht abdecken kann. Ein Collector verwendet dieselben Zertifikate und Prinzipale, schaltet SSH aber ein und aus, statt es dauerhaft erreichbar zu lassen — siehe SSH auf einem Collector.

Warum es SSH-Zugang gibt

Die Pulse-Appliance ist so entworfen, dass 99 % aller Vorgänge über die TUI erledigt werden. Sie installieren Updates, verwalten TLS-Zertifikate, konfigurieren das Netzwerk und richten SFTP-Schlüssel ein, ohne jemals eine Shell zu öffnen. Das hält das System schmal und nachvollziehbar.

Es gibt zwei Situationen, in denen Shell-Zugang dennoch nötig ist:

- **Hersteller-Support im Notfall.** Wenn etwas unterhalb der TUI schiefläuft — ein Kernel-Problem, ein hängender Dienst, ein Fehler im Appliance-Image selbst — braucht ein Pulse-Support-Mitarbeiter eine Shell auf der Appliance, um zu untersuchen. SSH ist der Kanal dafür. Der Hersteller signiert ein kurzlebiges Zertifikat für den Schlüssel des Support-Mitarbeiters; Sie müssen im Voraus nichts bereitstellen.
- **Der SFTP-Prinzipal** `pulse-transfer`. Die Schlüssel, die Sie auf dem Bildschirm SFTP-Zugang verwalten, autorisieren eine externe Gegenseite, Dateien in das Austauschverzeichnis der Appliance abzulegen. Diese Gegenseite verbindet sich als `pulse-transfer` über denselben SSH-Dienst — die SFTP-Zustellung läuft also auf dem hier beschriebenen SSH-Stack.

In beiden Fällen vertraut die Appliance Zertifikaten, die von der SSH-Zertifizierungsstelle (CA) der Appliance signiert wurden. Auf der Appliance gibt es keine Liste einzelner Benutzerschlüssel zu pflegen — das Vertrauen ist an denjenigen delegiert, der den privaten CA-Schlüssel besitzt.

Die zwei Prinzipale

Jedes signierte Zertifikat trägt ein oder mehrere *Prinzipale*. Ein Prinzipal ist eine Kennung, anhand derer der SSH-Server entscheidet, welche Art von Zugang das Zertifikat gewährt. Die Appliance kennt genau zwei:

`pulse` — Bedienerrolle (SSH + TUI)

Wer sich als `pulse` anmeldet, landet in der Bediener-TUI. Das ist dieselbe Ansicht, die Sie auf der lokalen Konsole sehen. Von dort aus verwalten Sie Netzwerk, Zertifikate, Updates und so weiter. Der Benutzer `pulse` ist **unprivilegiert**: Er hat keine Root-Shell, kann keine Systemdateien direkt bearbeiten und die TUI nicht umgehen, um den Zustand der Appliance zu verändern. Alles, was geändert werden muss, läuft über die Menüs, die im Hintergrund privilegierte Wrapper aufrufen.

Verwenden Sie `-n pulse`, wenn Sie einen Schlüssel für einen Support-Mitarbeiter signieren, der die Appliance genauso bedienen soll, wie es der Bediener vor Ort tut.

`pulse-transfer` — nur SFTP

Der Prinzipal `pulse-transfer` autorisiert eine im chroot eingesperrte SFTP-Sitzung und nichts weiter: keine interaktive Shell, keine TCP-Weiterleitung, kein X11, keinen Tunnel. Der Inhaber eines `pulse-transfer`-Zertifikats kann Dateien in `uploads/` ablegen und Dateien aus `downloads/` abholen — das ist die gesamte ihm zur Verfügung stehende Oberfläche. Es ist der Prinzipal, der von den Schlüsseln genutzt wird, die Sie auf dem Bildschirm SFTP-Zugang eintragen.

Verwenden Sie `-n pulse-transfer`, wenn Sie einen Schlüssel signieren, dessen einzige Aufgabe das Übertragen von Dateien in und aus dem Austauschverzeichnis ist.

Ein einzelnes Zertifikat kann beide Prinzipale gleichzeitig tragen, wenn dieselbe Person beide Rollen tatsächlich benötigt — zum Beispiel ein Support-Mitarbeiter, der während derselben Sitzung auch ein Update-Bundle hochladen wird.

Wie der Hersteller einen Kundenschlüssel signiert

Das Signieren geschieht **außerhalb der Appliance**, auf einer Workstation, die den privaten CA-Schlüssel verwahrt. Die Appliance sieht den privaten CA-Schlüssel nie; sie kennt nur den dazugehörigen öffentlichen Schlüssel als Vertrauensanker.

Der gesamte Ablauf:

1. Sie als Bediener (oder wer auch immer Zugang benötigt) erzeugen auf Ihrer Workstation ein SSH-Schlüsselpaar, sofern Sie noch keines haben. Der öffentliche Teil liegt unter `~/.ssh/id_ed25519.pub`.
2. Sie übermitteln dem Hersteller diese `.pub`-Datei über einen passenden Kanal — E-Mail, Ticket-Anhang, sichere Kurznachricht. Der private Teil verlässt Ihren Rechner nicht.
3. Der Hersteller signiert den öffentlichen Schlüssel mit dem privaten CA-Schlüssel über `ssh-keygen -s` und wählt den Prinzipal, der dem zu gewährenden Zugang entspricht.

4. Der Hersteller schickt Ihnen die signierte Zertifikatsdatei zurück. Per Konvention heißt sie `id_ed25519-cert.pub` (derselbe Basisname wie der Schlüssel, mit angehängtem `-cert`).
5. Sie legen das signierte Zertifikat neben Ihren Schlüssel — üblicherweise unter `~/.ssh/id_ed25519-cert.pub`. Der SSH-Client liest es beim nächsten Verbindungsaufbau automatisch ein.

Die vom Hersteller ausgeführten Signaturbefehle sind:

Bedienerrolle (Prinzipal `pulse`)

```
ssh-keygen -s /path/to/ca_private_key -I "description" -n pulse -V +365d ~/.ssh/id_ed25519.pub
```

SFTP-Transferrolle (Prinzipal `pulse-transfer`)

```
ssh-keygen -s /path/to/ca_private_key -I "description" -n pulse-transfer -V +365d ~/.ssh/id_ed25519.
```

Beide Prinzipale in einem Zertifikat

```
ssh-keygen -s /path/to/ca_private_key -I "description" -n pulse,pulse-transfer -V +365d ~/.ssh/id_ed2
```

In jedem Fall wird das signierte Zertifikat unter `~/.ssh/id_ed25519-cert.pub` abgelegt und vom SSH-Client automatisch verwendet.

Der Schalter `-I` setzt eine frei wählbare Identität, die im Zertifikat festgehalten wird — nützlich für die Nachvollziehbarkeit. Eine kurze Beschreibung wie `support-mitarbeiter-jane-2026-05` oder die Ticketnummer, die zur Signatur führte, ist die richtige Detailtiefe.

Gültigkeitsfenster

Der Schalter `-V +365d` in den obigen Beispielen begrenzt die Gültigkeit des Zertifikats auf ein Jahr ab Signaturzeitpunkt. Danach läuft das Zertifikat ab, und der SSH-Server lehnt es ab — auch wenn der zugrunde liegende Schlüssel unverändert ist.

Dieser Ablauf ist **bewusst gewählt**:

- Er begrenzt den Schaden, falls ein Schlüssel verloren geht. Ein entwendetes Zertifikat verliert von selbst seine Wirkung; niemand muss es suchen und widerrufen.
- Er erzwingt einen wiederkehrenden Signaturvorgang, der zugleich der natürliche Anlass ist, die Frage zu stellen: „Braucht diese Person den Zugang noch?"

- Er passt zum Betriebsrhythmus einer verwalteten Appliance: Ein Jahr ist lang genug, dass das erneute Signieren keine ständige Last ist, und kurz genug, dass längst ausgeschiedene Mitarbeiter keinen dauerhaften Zugang behalten.

Kürzere Fenster sind für einzelne Support-Einsätze sinnvoll — `-V +1d` oder `-V +1w` für einen einzigen Vorgang, nach dessen Ende das Zertifikat tot ist. Verwenden Sie kürzere Gültigkeiten, wenn der Zugang an eine konkrete Aufgabe gebunden ist; reservieren Sie das Ein-Jahres-Fenster für Schlüssel, die wiederholt benutzt werden.

Der Ablauf des Zertifikats ist unabhängig vom SSH-Schlüssel selbst. Der Schlüssel bleibt gültig; nur die Signatur darauf läuft ab.

Was der Bediener nicht erhält

Ein signiertes `pulse`-Zertifikat gewährt dem Benutzer eine Shell auf der Appliance, aber diese Shell ist dieselbe eingegrenzte Umgebung, in der auch der lokale Bediener arbeitet:

- Der Benutzer `pulse` ist **unprivilegiert**. Er hat kein `sudo` für beliebige Befehle. Er kann Systemkonfigurationsdateien nicht direkt bearbeiten, Systemdienste nicht aus der Shell neu starten und die geschützten Geheimnisse der Appliance weder lesen noch schreiben.
- Konfigurationsänderungen laufen über die TUI. Die TUI selbst ruft eine kleine Menge geprüfter privilegierter Wrapper auf, um den Zustand der Appliance zu ändern. Daran führt kein Weg vorbei.
- Ein `pulse-transfer`-Zertifikat ist noch enger gefasst: gar keine Shell, nur SFTP in das Austauschverzeichnis.

Mit anderen Worten: SSH-Zugang ist ein Weg, die Bedienerrolle *aus der Ferne zu erreichen*, kein Weg, *darüber hinaus zu eskalieren*. Wer den Zustand der Appliance ändern will, tut das weiterhin über die TUI — er sieht sie nur per SSH statt auf der lokalen Konsole.

SSH auf einem Collector

Ein Collector verwendet dieselben Zertifikate und Prinzipale wie oben beschrieben — nur ist SSH hier nicht dauerhaft erreichbar wie auf der Appliance. Ein Collector steht im OT-Netz, und von außen verbindet sich nichts in dieses Netz hinein — daran ändert auch das Einschalten von SSH nichts. Es ermöglicht Administratorinnen und Administratoren, die bereits im OT-Netz sind, den Collector über SSH zu erreichen; ein Bediener schaltet SSH an der Konsole des Collectors selbst ein, und bis dahin lehnt Port 22 jede Verbindung ab.

Das geschieht auf dem Bildschirm **SSH / SFTP-Zugang** im Menü des Collectors. Er zeigt, ob SSH gerade an- oder ausgeschaltet ist, und, solange es an ist, wie viel Zeit bis zum automatischen Abschalten bleibt; auf demselben Bildschirm schalten Sie SSH auch von Hand ein und aus, und dort verwalten Sie die Kunden-SSH-Schlüssel für diesen Collector. SSH schaltet sich nach 24 Stunden von selbst wieder aus, falls es niemand vorher abschaltet, und nach einem Neustart ist SSH immer aus — unabhängig davon, welchen Zustand es vor dem Neustart hatte.

Solange es an ist, funktioniert die Authentifizierung genau wie auf der Appliance: keine Passwort-Anmeldung, nur Zertifikate, die von der Pulse-Support-SSH-CA signiert sind, sowie die auf demselben Bildschirm hinterlegten Kundenschlüssel. `pulse-transfer`-Uploads landen im Austauschverzeichnis des Collectors genauso wie auf der Appliance — siehe SFTP-Zugang für Details zu diesem Prinzipal und seinen Uploads — und ein auf diesem Weg bereitgestelltes Bundle wird, solange SSH an ist, als Update-Quelle auf dem Collector angeboten, genau wie auf der Appliance; siehe Einen Collector aktualisieren.

Jeder Wechsel — SSH einschalten, ausschalten und das automatische Abschalten nach 24 Stunden — wird im Audit-Log festgehalten.

Solange SSH an ist, zeigt der Bildschirm Collector-Status des Collectors eine Zeile dazu an, sodass ein Blick auf diesen Bildschirm sofort verrät, ob die Box gerade über SSH erreichbar ist.

Verwandte Bildschirme

- SFTP-Zugang — verwalten Sie die kundenseitigen SFTP-Schlüssel, die als `pulse-transfer` authentifiziert werden.
- TUI-Referenz — das Bedienermenü, in dem der `pulse`-Benutzer nach dem SSH-Login landet.
- Installation — die Erstkonfiguration, einschließlich des SSH-CA-Vertrauensankers, der signierte Zertifikate erst akzeptierbar macht.
- Collector-Status — der Konsolenbildschirm des Collectors; zeigt eine Zeile an, solange SSH eingeschaltet ist.

9.8 TUI-Referenz

Die Pulse-Appliance wird über eine textbasierte Bedienoberfläche (TUI) gesteuert, die sich automatisch auf der Konsole (tty1) und über SSH öffnet. Das Hauptmenü hat zwölf Einträge. Verwenden Sie die Pfeiltasten (oder `j` / `k`), um zwischen ihnen zu wechseln, `Enter`, um einen Eintrag zu öffnen, und `q`, um die TUI zu beenden.

System Status

Zeigt die Software-Version, die Laufzeit, die IP-Adresse, den Zustand der einzelnen Kerndienste, die Festplattenauslastung und den Zeitpunkt des letzten Backups an. Öffnen Sie diesen Eintrag zuerst, wenn ein Benutzer meldet, dass die Anwendung langsam, nicht erreichbar oder auffällig ist — so prüfen Sie am schnellsten, ob die Appliance selbst gesund ist.

Network Configuration

Konfiguriert die IPv4-Adresse, das Gateway und die DNS-Server der Appliance und wechselt zwischen DHCP- und statischem IP-Betrieb. Öffnen Sie diesen Eintrag bei der Erstinbetriebnahme, wenn Sie die Appliance in ein anderes Netz umziehen oder wenn das LAN-Team eine geänderte IP zuweist.

NTP Configuration

Legt fest, welchen Zeitserver die Appliance für die Synchronisation verwendet. Öffnen Sie diesen Eintrag, wenn die Uhr abdriftet, wenn Ihr Standort einen internen NTP-Server statt des öffentlichen Pools nutzt oder nachdem Sie die Appliance in ein Netz ohne Internet-Zugang umgezogen haben.

Update System

Spielt ein signiertes Systemupdate von einem USB-Stick, aus dem SFTP-Austausch oder von einem CD/DVD-ROM-Laufwerk ein. Öffnen Sie diesen Eintrag, wenn ein neues Pulse-Release angekündigt wird, wenn ein Sicherheitsupdate erforderlich ist oder wenn der Support vor Ort ein Update-Paket zum Einspielen bereitgestellt hat.

SFTP Access

Verwaltet, wie sich Kunden für den SFTP-Dateiaustausch mit der Appliance anmelden — sowohl die SSH-Public-Keys als auch das automatisch erzeugte Passwort der Appliance. Öffnen Sie diesen Eintrag, wenn Sie eine neue Kundenintegration einrichten, einen Schlüssel oder das Passwort rotieren oder den Zugriff am Ende einer Geschäftsbeziehung entfernen.

Backup / Restore

Erstellt eine vollständige Datenbanksicherung oder stellt die Appliance aus einer früheren Sicherung wieder her. Öffnen Sie diesen Eintrag vor riskanten Aktionen (Updates, Konfigurationsänderungen), in regelmäßigen Abständen im Normalbetrieb oder zur Wiederherstellung nach Datenverlust oder einem fehlgeschlagenen Update.

View Logs

Zeigt aktuelle System- und Anwendungsprotokolle aus journald und vom Pulse-Server an. Öffnen Sie diesen Eintrag, wenn Sie einem Dienst auf die Spur kommen wollen, der nicht startet, einer ausgebliebenen Alarmierung nachgehen oder Informationen für eine Support-Anfrage sammeln müssen.

Restart Services

Startet den Pulse-Server, PostgreSQL oder nginx einzeln neu. Öffnen Sie diesen Eintrag, wenn ein Dienst hängt — zum Beispiel wenn die Weboberfläche 502-Fehler liefert, die Appliance ansonsten aber gesund ist — und Sie nur einen einzelnen Dienst neu starten möchten statt die ganze Appliance neu zu starten.

TLS Certificates

Verwaltet das TLS-Zertifikat, das die Weboberfläche im Browser ausliefert. Öffnen Sie diesen Eintrag, um zwischen selbstsigniertem Zertifikat und kundenseitig bereitgestelltem Zertifikat zu wechseln, eine Zertifikatsanforderung (CSR) für die Signatur durch die Kunden-CA zu erzeugen oder ein erneuertes Zertifikat einzuspielen, bevor das aktuelle abläuft.

Rollback

Setzt die Appliance auf eine frühere Systemgeneration zurück. Öffnen Sie diesen Eintrag unmittelbar nach einem Update, wenn sich die neue Version auffällig verhält — der Rollback ist das Sicherheitsnetz, mit dem der Bediener ohne Hilfe des Supports zu einem bekanntermaßen funktionierenden Zustand zurückkehrt.

Expert Shell

Öffnet eine interaktive System-Shell auf der Appliance, abgesichert durch ein Passwort. Öffnen Sie diesen Eintrag nur dann, wenn der Support Sie ausdrücklich dazu auffordert: Er umgeht die Schutzmechanismen der TUI, und Änderungen, die Sie hier vornehmen, sind im restlichen Menü nicht sichtbar.

Reboot System

Startet die Appliance neu. Öffnen Sie diesen Eintrag nach einem Update, das einen Kernel-Neustart erfordert, auf Anweisung des Supports oder als letzten Ausweg, wenn die Appliance offensichtlich gestört ist und Sie neu starten wollen.

9.9 Systemupdates

Pulse wird als signiertes Update-Bundle ausgeliefert, das vom Hersteller erzeugt wird. Der Bildschirm **Update System** — in der Appliance-TUI und derselbe Bildschirm auf der Konsole eines Collectors — spielt ein solches Bundle in das laufende System ein. Der Assistent ist immer derselbe, egal auf welchem Weg das Bundle es erreicht — nur der erste Schritt, die Quelle, unterscheidet sich.

Diese Seite ist die vollständige Anleitung. Für Datenbank-Backups und das Zurücksetzen auf eine vorherige Version siehe Betrieb.

Was ein Update-Bundle ist

Jedes Bundle ist von Pulse signiert. Die Appliance prüft die Signaturkette, bevor überhaupt etwas angezeigt wird, und verweigert die Verarbeitung, wenn das Bundle unsigniert, manipuliert oder mit einem Schlüssel signiert ist, der nicht zum öffentlichen Schlüssel des laufenden Systems passt. Es gibt keinen Weg, ein unsigniertes Bundle über die TUI einzuspielen — genau das ist der Zweck der Signaturkette.

Ein gültiges Bundle enthält ein Manifest mit Versionsangabe, Build-Zeitstempel, einer kurzen Liste der Änderungen und einem Marker, ob die neue Version einen Neustart erfordert. All das sehen Sie auf dem Bildschirm **Update Available**, bevor Sie sich für das Einspielen entscheiden.

Den Lieferweg wählen

Es gibt drei Wege, ein Bundle auf die Appliance zu bringen. Wählen Sie danach, wie die Appliance betrieben wird:

Betrieb	Empfohlener Weg	Warum
Virtualisiert (VMware ESXi/vSphere, Proxmox, Hyper-V, …)	**CD/DVD-ROM**	Hängen Sie das Update-ISO in das virtuelle optische Laufwerk der VM ein — dieselbe Geste wie bei der Installation. Kein USB-Passthrough nötig.

Betrieb	Empfohlener Weg	Warum
Physische / Bare-Metal-Appliance	**USB-Stick**	Kein Hypervisor, daher ist ein per Hand mitgebrachter Wechseldatenträger der einfachste Weg.
Remote / unbeaufsichtigt oder vom Support bereitgestellt	**SFTP-Upload**	Der Support liefert das Bundle über das Netzwerk; niemand muss zum Rack gehen.

Alle drei münden in denselben Assistenten und dasselbe unten beschriebene Sicherheitsnetz — die Tabelle betrifft die Bequemlichkeit, nicht den Funktionsumfang.

Wie ein Update eingespielt wird

Sobald Sie bestätigen, führt die Appliance eine feste Abfolge aus. Es lohnt sich zu wissen, was passiert, denn das meiste davon ist automatische Absicherung:

1. **Prüfen** — Signatur und Prüfsumme werden erneut kontrolliert.
2. **Datenbank sichern** — es wird ein frisches PostgreSQL-Backup erstellt, *bevor* irgendetwas angefasst wird, sodass der Zustand vor dem Update jederzeit wiederherstellbar ist.
3. **Importieren und umschalten** — das neue System wird entpackt und das Boot-Profil darauf umgestellt.
4. **Health-Check** — es wird bis zu 60 Sekunden gewartet, bis Pulse an seinem Health-Endpunkt antwortet.
5. **Automatisches Rollback bei Fehler** — schlägt das Umschalten oder der Health-Check fehl, setzt sich die Appliance automatisch auf die vorherige Version zurück und meldet den Fehler. Sie bleiben auf einem funktionierenden System zurück, nicht auf einem kaputten.
6. **Aufräumen** — die fünf neuesten Systemgenerationen werden behalten, ältere entfernt.

Wenn das Manifest einen Neustart verlangt (typischerweise eine Kernel-Änderung), teilt der Schlussbildschirm Ihnen das mit; starten Sie dann bei Gelegenheit über das Hauptmenü neu.

TIP

Weil die Appliance die Datenbank sichert und sich bei einem fehlgeschlagenen Health-Check selbst zurücksetzt, korrigiert sich ein fehlerhaftes Update weitgehend von selbst. Die manuellen Wiederherstellungswerkzeuge auf der Seite Betrieb sind für Probleme gedacht, die *nach* dem Einspielen im laufenden Betrieb auftreten.

Einen Collector aktualisieren

Ein Collector wird über dasselbe signierte Bundle wie die Appliance aktualisiert, über denselben Bildschirm **Update System** — geöffnet über die eigene Konsole des Collectors statt über die der Appliance. Ein USB-Stick oder eine virtuelle CD/DVD funktionieren an einem Collector jederzeit, genau wie oben beschrieben. Auch SFTP-Upload funktioniert, aber nur aus dem OT-Netz heraus, solange SSH an der Konsole dieses Collectors eingeschaltet ist. Sie aktualisieren Collectors einzeln, jeweils über die eigene Konsole des Collectors, nicht über die Appliance.

Ein Update auf einem Collector unterscheidet sich in einigen Punkten von einem Appliance-Update:

- **Kein Datenbank-Backup-Schritt.** Ein Collector hat keine Datenbank, daher geht der Assistent direkt vom Prüfen des Bundles zum Importieren und Umschalten über.
- **Das Umschalten setzt nicht voraus, dass die Appliance erreichbar ist.** Sobald die neue Version wieder hochgefahren ist und erneut ihren Status meldet, gilt das Update als erfolgreich — unabhängig davon, welcher Status das ist: verbunden, noch beim Versuch, die Appliance zu erreichen, oder wartend auf Kopplung. Keiner dieser Zustände erfordert ein Zurücksetzen, daher können Sie einen Collector auch dann aktualisieren, wenn seine Appliance gerade nicht erreichbar ist.
- **Ein kürzeres, automatisches Sicherheitsnetz.** Meldet die neue Version innerhalb von drei Minuten keinen frischen Status oder startet sie wiederholt nicht, setzt sich der Collector von selbst auf die zuvor laufende Version zurück.

Erfordert das Bundle einen Neustart, wird das genauso vorgemerkt wie bei einer Appliance: Schließen Sie den Assistenten ab und starten Sie den Collector bei Gelegenheit über das Hauptmenü neu.

Um nach einem Update zu prüfen, wie es einem Collector geht — verbunden, in der Wiederverbindung oder wartend auf Kopplung — öffnen Sie Collector-Status.

Vor dem Update

Eine kurze Checkliste hält ein Update unspektakulär:

- **Stellen Sie sicher, dass die Appliance jetzt gesund ist** — die Weboberfläche lädt und das System verhält sich normal. Ein Update auf einem kranken System erschwert die Fehlersuche.
- **Sorgen Sie für Konsolenzugang** — lokaler Monitor und Tastatur oder SSH als `pulse`-Benutzer. Sie möchten den Fortschritt verfolgen und bei Bedarf neu starten.
- **Planen Sie einen möglichen Neustart ein** — manche Updates erfordern einen. Wählen Sie ein Zeitfenster, in dem ein kurzer Neustart vertretbar ist.
- **Halten Sie das Bundle am richtigen Ort bereit** für den gewählten Weg (siehe die einzelnen Wege unten).
- *(Optional)* **Erstellen Sie ein manuelles Backup** über den Bildschirm Backup / Restore. Das Update erstellt zwar automatisch eines, aber ein zusätzlicher bekannter guter Stand ist vor einem großen Sprung eine günstige Absicherung.

Lieferwege im Detail

Virtualisierte Appliance — CD/DVD-ROM

Das ist der empfohlene Weg für jede Appliance, die als VM läuft.

1. Kopieren Sie das Update-ISO (`pulse-update-<version>.iso`) in den Datastore Ihres Hypervisors.
2. Bearbeiten Sie die Einstellungen der VM und richten Sie deren **CD/DVD-Laufwerk** auf dieses ISO. In VMware vSphere/ESXi setzen Sie das Laufwerk auf **Datastore ISO File**, wählen das ISO aus und — diesen Schritt übersieht man leicht — setzen den Haken bei **Connected** (und **Connect At Power On**). Andere Hypervisoren haben dieselben zwei Punkte: das ISO auswählen und sicherstellen, dass das Laufwerk tatsächlich verbunden ist.
3. Öffnen Sie auf der Appliance oder dem Collector **Update System → CD/DVD-ROM**. Die TUI hängt das virtuelle Laufwerk ein, findet das Bundle und prüft es.

> **WARNING**
>
> Meldet die TUI keinen Datenträger, ist das Laufwerk fast immer angehängt, aber nicht **Connected**. Die Erkennung richtet sich danach, ob der Datenträger tatsächlich eingehängt ist, nicht nur danach, ob er in der VM-Konfiguration vorhanden ist. Setzen Sie den Haken bei **Connected** und wiederholen Sie den Vorgang.

Trennen Sie den Datenträger nicht, während das Update läuft — der Bildschirm **Updating…** weist in Gelb darauf hin. Das Laufwerk wird nach Abschluss des Updates automatisch ausgehängt.

Physische Appliance — USB-Stick

1. Formatieren Sie einen USB-Stick als **FAT32** oder **ext4**.
2. Kopieren Sie die Bundle-Dateien in das **Wurzelverzeichnis des Sticks** (ein einzelnes Unterverzeichnis wie `updates/` funktioniert ebenfalls). Legen Sie sie nicht tiefer ab.
3. Stecken Sie ihn in die Appliance oder den Collector und öffnen Sie **Update System → USB Drive**. Die TUI sucht nach Wechseldatenträgern:
   - Ein Laufwerk gefunden → es wird automatisch eingehängt und durchsucht.
   - Mehrere gefunden → der Schritt **Select USB Device** lässt Sie das richtige auswählen.
   - Keines gefunden → es meldet `no USB drive found (format must be FAT32 or ext4)` und wartet.

Ziehen Sie den Stick nicht ab, während das Update läuft — das Bundle wird während des Einspielens davon gelesen, und der Bildschirm **Updating…** weist in Gelb darauf hin. Er wird nach Abschluss automatisch ausgehängt.

Remote / vom Support bereitgestellt — SFTP-Upload

1. Die Gegenseite, die das Bundle liefert, muss bereits ein autorisierter SFTP-Benutzer sein — siehe SFTP-Zugang, wie Sie sie autorisieren, per SSH-Schlüssel oder mit dem Passwort der Appliance.
2. Sie lädt das Bundle in das Austauschverzeichnis unter `uploads/updates/` hoch.
3. Öffnen Sie auf der Appliance, oder an einem Collector mit eingeschaltetem SSH, **Update System → SFTP Upload**. Die TUI durchsucht das Austauschverzeichnis und prüft das Gefundene.

An einem Collector funktioniert das nur aus dem OT-Netz heraus — SSH nimmt dort nie eine Verbindung von außerhalb an — und nur per autorisiertem Schlüssel; die Passwort-Option der Appliance bietet ein Collector nicht.

Ein erfolgreich eingespieltes SFTP-Bundle wird danach aus dem Austauschverzeichnis entfernt, damit es nicht zweimal eingespielt werden kann.

Der Assistent, Schritt für Schritt

Welche Quelle Sie auch wählen, der Rest ist identisch:

1. **Quelle** — wählen Sie USB Drive, SFTP Upload oder CD/DVD-ROM. Die TUI sucht, hängt ein (USB und CD/DVD-ROM) und prüft das Bundle.
2. **Manifest-Prüfung** — der Bildschirm **Update Available** zeigt Version, Build-Zeitstempel, Änderungen und ob ein Neustart erforderlich ist. Lesen Sie das. Drücken Sie `Esc`, um sauber abzubrechen, ohne etwas einzuspielen.
3. **Bestätigung** — drücken Sie auf dem Manifest-Bildschirm `Enter`, um zu starten. Es folgt keine zweite Ja/Nein-Abfrage; der Manifest-Bildschirm *ist* die Bestätigung.
4. **Fortschritt** — der Bildschirm **Updating…** zeigt den Fortschritt, während das Bundle geprüft, gesichert, importiert und aktiviert wird. Solange ein Wechseldatenträger noch eingehängt ist, weist er in Gelb darauf hin, diesen nicht zu entfernen.
5. **Fertig** — der Schlussbildschirm zeigt `Update Successful!` (grün) oder `Update Failed` (rot) mit der zugrunde liegenden Fehlermeldung. Drücken Sie `Esc`, um ins Hauptmenü zurückzukehren.

Nach dem Update

- Hat das Manifest einen Neustart angezeigt, starten Sie über den Eintrag **Reboot System** im Hauptmenü neu.
- Prüfen Sie, dass die Weboberfläche wieder erscheint und die Version die erwartete ist.
- Wenn Sie zufrieden sind, erstellen Sie über Backup / Restore ein frisches Backup, damit Ihr nächster bekannter guter Stand nach dem Update liegt.

Fehlerbehebung

Was Sie sehen	Wahrscheinliche Ursache	Was zu tun ist
`no USB drive found (format must be FAT32 or ext4)`	Stick ist nicht FAT32/ext4 oder wurde nicht erkannt	Als FAT32 oder ext4 neu formatieren, Stick neu einstecken, erneut versuchen
USB wird eingehängt, aber kein Bundle gefunden	Bundle liegt nicht im Wurzelverzeichnis oder Dateien unvollständig	`manifest.json` + `system.tar` (und die `.sha256` / `.sig`-Dateien) ins **Wurzelverzeichnis oder einen einzelnen Unterordner direkt im Wurzelverzeichnis** (z. B. `updates/`) legen — nicht tiefer verschachteln

Was Sie sehen	Wahrscheinliche Ursache	Was zu tun ist
CD/DVD-ROM: kein Datenträger erkannt	ISO nicht angehängt oder angehängt, aber nicht **Connected**	ISO anhängen, Haken bei **Connected** / **Connect At Power On** setzen, erneut versuchen
SFTP: kein Bundle gefunden	Nicht nach `uploads/updates/` hochgeladen oder Absender nicht autorisiert	Upload-Pfad prüfen; Absender (SSH-Schlüssel oder Passwort) über SFTP-Zugang autorisieren
Prüf-/Signaturfehler	Bundle ist unsigniert, beschädigt oder mit falschem Schlüssel signiert	Ein korrekt signiertes Bundle von Pulse anfordern; dieselbe Datei erneut einzuspielen hilft nicht
`Dieses Update-Bundle enthält kein Collector-System.` (auf einem Collector)	Bundle ist eine ältere Version oder wurde nur für die Appliance erstellt	Ein Bundle anfordern, das ein Collector-System enthält, und es erneut versuchen
Update Failed während des Einspielens	Umschalten oder Health-Check fehlgeschlagen — die Appliance hat bereits automatisch zurückgesetzt	Sie sind zurück auf der vorherigen Version. Fehler festhalten und damit den Support kontaktieren
Web-App nach einem Neustart nicht erreichbar	Neue Version ist nicht gesund	Auf die vorherige Generation zurücksetzen, danach bei Bedarf ein Backup wiederherstellen

Wenn ein Update schiefgeht

Ein fehlgeschlagenes Update setzt sich während des Einspielens automatisch zurück (siehe die Tabelle zur Fehlerbehebung oben). Tritt ein Problem erst im laufenden Betrieb der neuen Version auf, verwenden Sie Rollback, um auf die vorherige Systemgeneration zurückzukehren. Rollback wirkt nur auf Systemebene — die Datenbank und andere Daten unter `/var` bleiben unberührt. Siehe Betrieb für Backups, Wiederherstellung und Rollback in voller Länge.

9.10 Betrieb

Diese Seite beschreibt die Bedienerabläufe zum Schützen und Wiederherstellen von Appliance-Daten: das Erstellen und Wiederherstellen von Datenbank-Backups und das Zurücksetzen auf die vorherige Systemgeneration, wenn ein Update Probleme bereitet. Das Einspielen eines Systemupdates hat eine eigene Seite — siehe Systemupdates. Jeder Abschnitt ist an einen TUI-Bildschirm gebunden, sodass Sie den Assistenten am Bildschirm den hier beschriebenen Schritten zuordnen können.

Systemupdate einspielen

Das Einspielen eines signierten Update-Bundles hat eine eigene Seite — siehe Systemupdates für die vollständige Anleitung: welcher Lieferweg für virtualisierte gegenüber physischen Appliances zu verwenden ist, das eingebaute Sicherheitsnetz aus Backup und Rollback sowie die Fehlerbehebung.

Backup und Wiederherstellung

Der Bildschirm **Backup / Restore** verwaltet Datenbank-Backups. Die Appliance erstellt nach Zeitplan automatische Backups; Sie können außerdem vor riskanten Aktionen ein zusätzliches Backup anlegen und aus jedem vom Bildschirm gelisteten Backup wiederherstellen.

Was Sie sehen

Das oberste Menü hat zwei Einträge:

- **Create Backup** — führt sofort ein Backup aus. Der Bildschirm zeigt bei Erfolg eine grüne Statuszeile mit der Ausgabe des Backup-Befehls oder bei Fehlschlag einen roten Fehler.
- **List / Restore Backups** — öffnet die unten beschriebene Auswahl.

Wählen Sie **List / Restore Backups**, sehen Sie jede auf der Appliance vorhandene Backup-Datei zeilenweise mit Dateinamen, Größe (KB, MB oder GB) und Änderungszeitpunkt. Das zuletzt geänderte Backup ist üblicherweise das, das Sie zur Wiederherstellung möchten; die älteren Einträge sind die rollierenden automatischen Backups.

Ein Ad-hoc-Backup erstellen

Bevor Sie etwas Riskantes tun — ein Update, eine größere Konfigurationsänderung, einen Kundenimport — wählen Sie **Create Backup** und warten Sie auf die grüne Bestätigung. Das Ergebnis ist eine frische Backup-Datei neben den automatischen, und sie liefert Ihnen einen bekannt guten Rücksetzpunkt für die Datenbank, der nicht von der nächsten geplanten Sicherung abhängt.

Ein Backup wiederherstellen

Eine Wiederherstellung überschreibt die laufende Datenbank mit dem Inhalt der gewählten Backup-Datei. Der Bildschirm nimmt das ernst:

1. Bewegen Sie in **List / Restore Backups** den Cursor auf das gewünschte Backup und drücken Sie `Enter`.
2. Ein Bestätigungsbildschirm erscheint mit einer gelben Warnung — `WARNING: This will replace the current database!` — und dem Namen der Backup-Datei. Drücken Sie `y` zur Bestätigung oder `n` / `Esc` zum Abbrechen.
3. Bei Bestätigung läuft die Wiederherstellung, und der Bildschirm zeigt `Database restored successfully` (grün) oder den zugrunde liegenden Fehler (rot).

Während die Wiederherstellung läuft, wird die Datenbank vollständig ersetzt: Zeilen, die seit dem gewählten Backup geschrieben wurden, gehen verloren, und jeder in der Weboberfläche angemeldete Benutzer sieht seine Sitzung im Moment des Datenbankwechsels abbrechen. Eine Wiederherstellung ist kein teilweiser oder zusammenführender Vorgang — es ist ein vollständiger Austausch, und genau deshalb ist die Warnung deutlich.

Hatte die ausgetauschte Appliance Collectors gekoppelt, reicht die reine Datenbank-Wiederherstellung nicht aus, um sie automatisch wieder anzubinden — siehe Ein Backup vor dem Austausch einer Appliance wiederherstellen.

Backup vs. Rollback

Backups decken die *Datenbank* ab. Das System selbst — die NixOS-Generation, die Konfiguration, die installierte Software — wird durch Rollback abgedeckt. Beide ergänzen sich: Ein Backup bringt keinen alten Kernel zurück, und ein Rollback bringt keine gelöschten Datensätze zurück. Sind Sie unsicher, was Sie brauchen, lesen Sie den nächsten Abschnitt.

Rollback

Der Bildschirm **Rollback** wechselt die Appliance auf eine vorherige Systemgeneration. Verwenden Sie ihn, wenn ein Update Probleme bereitet und Sie schnell die alte Version zurückbrauchen.

Was Rollback tut

Der Bildschirm listet jede NixOS-Generation, die die Appliance noch vorhält, neueste zuerst, mit Nummer, Build-Datum und einer grünen Markierung `(current)` auf der laufenden Generation. Bewegen Sie den Cursor mit den Pfeiltasten (oder `j` / `k`), drücken Sie `r`, um die Liste zu aktualisieren, und drücken Sie `Enter` auf einer nicht aktuellen Generation, um den Wechsel zu starten.

Eine Bestätigungsabfrage erscheint mit der Frage `Switch to generation N (date)?`. Drücken Sie `y` zur Bestätigung oder `n` / `Esc` zum Abbrechen. Bei Bestätigung aktualisiert die Appliance ihre Bootkonfiguration und meldet `Switched to selected generation`. **Ein Neustart ist nötig, damit die Änderung wirksam wird** — die laufenden Dienste laufen weiterhin auf der alten (nun neueren) Generation, bis die Appliance neu startet. Starten Sie über den Menüeintrag **Reboot System** im Hauptmenü neu, sobald der Rollback bestätigt ist.

Was Rollback bewahrt — und was nicht

Rollback ist eine System-, keine Datenoperation. Konkret:

- **Ersetzt**: die Wurzelpartition. Der Nix-Store, der Kernel, die Systemkonfiguration und die installierte Software werden auf den Stand der vorherigen Generation zurückgesetzt.
- **Bewahrt**: `/var` und alles darunter. Das umfasst die PostgreSQL-Datenbank von Pulse, Ihre Datenbank-Backups, Logdateien, das SFTP-Austauschverzeichnis und jede über die TUI geschriebene Konfiguration (TLS-Zertifikate, SFTP-Schlüssel, Netzwerkeinstellungen). Nichts davon wird durch den Generationswechsel berührt.

In der Praxis macht ein Rollback den *Software*-Anteil des letzten Updates rückgängig, behält aber jedes Byte an Kundendaten, das die Appliance seither angesammelt hat.

Wann Rollback, wann ein Backup zurückspielen

Die beiden Wiederherstellungswerkzeuge decken unterschiedliche Fehlerbilder ab; die richtige Wahl ist wichtig.

- **Rollback** wenn die neue Software das Problem ist: ein Dienst, der nicht startet, eine Verhaltensregression, ein durch das Update eingeschleppter Kernelfehler, ein abstürzender TUI-Bildschirm. Die Daten sind in Ordnung, der Code nicht. Rollback stellt die vorherige Generation wieder her, ohne Datenbankzeilen zu verlieren.

- **Backup zurückspielen** wenn die Daten das Problem sind: Korruption, ein versehentlicher Massenlöschvorgang, ein fehlerhafter Import, der das Schema verschmutzt hat. Der Code ist in Ordnung, die Daten nicht. Die Backup-Wiederherstellung bringt die Datenbank auf einen bekannt guten Stand zurück.

Werden beide benötigt — ein Update ging schief *und* hat den Zustand auf dem Weg nach draußen beschädigt — spielen Sie zuerst ein Rollback ein, damit die Appliance wieder auf einer funktionierenden Softwareversion läuft, und stellen Sie dann das jüngste Backup vor dem Update wieder her.

Generationen, die nicht mehr erscheinen

NixOS behält nur eine begrenzte Anzahl Generationen auf der Platte. Ältere Generationen werden im normalen Zeitplan der Appliance entfernt, die Liste wächst also nicht endlos. Ist die gewünschte Generation nicht mehr aufgelistet, sind Sie jenseits des Punktes, an dem Rollback helfen kann, und die Appliance muss neu installiert oder durch den Support repariert werden — der Rollback-Bildschirm ist ein kurzfristiges Sicherheitsnetz, kein langfristiges Wiederherstellungsarchiv.

Nach einem erfolgreichen Rollback

Sobald die Appliance auf der vorherigen Generation neu gestartet ist und Sie bestätigt haben, dass das System wieder gesund ist, erstellen Sie über den Bildschirm Backup und Wiederherstellung ein frisches Datenbank-Backup. Der Zustand nach dem Rollback ist nun Ihre bekannte gute Grundlage; ihn ausdrücklich festzuhalten bedeutet, dass der nächste riskante Vorgang einen sauberen Schnappschuss zum Zurückfallen hat statt der älteren automatischen Backups, die noch vor dem gerade ausgestandenen Problem entstanden sind.

War das Update, das den Rollback ausgelöst hat, per SFTP geliefert, ist das Bundle bereits durch den Aufräumvorgang nach dem *ursprünglichen* (fehlgeschlagenen) Versuch entfernt worden. War es ein USB-Update, ist der Stick nicht mehr eingehängt — ziehen Sie ihn ab, klären Sie mit dem Support, was an diesem Bundle nicht stimmte, und versuchen Sie es erst dann erneut, wenn ein korrigierter Build verfügbar ist. War es ein CD/DVD-ROM-Update, wurde das Laufwerk automatisch ausgehängt und Sie können das ISO sicher von der VM trennen. Es bringt nichts, dasselbe Bundle erneut einzuspielen, das beim letzten Mal fehlgeschlagen ist.

10.1 Collector-Status

Die Konsole eines Collectors zeigt heute einen Bildschirm: **Systemstatus**. Er zeigt Ihnen, was der Collector gerade tut — und, falls er nicht mit seiner Appliance verbunden ist, warum. Öffnen Sie ihn jederzeit, um zu prüfen, ob ein Collector gesund ist, oder um mit der Fehlersuche bei einem zu beginnen, der es nicht ist.

Neben der Kopfzeile zeigt der Bildschirm alles, was gerade bekannt ist: seit wann der aktuelle Status besteht, die Adresse der Appliance, mit der sich der Collector verbinden soll, seine eigene Softwareversion, seine Seriennummer und den Fingerabdruck des Appliance-Zertifikats. Braucht der Support mehr Details als die Kopfzeile hergibt, zeigt der Bildschirm zusätzlich eine kurze technische Zeile, die Sie ihm vorlesen können. Der Bildschirm aktualisiert sich automatisch alle paar Sekunden — Sie müssen ihn also nicht neu öffnen, um eine Änderung zu sehen.

Verbindung zur Appliance wird aufgebaut…

Der Collector versucht gerade, sich zu verbinden. Das ist normal, direkt nachdem der Dienst gestartet ist oder nachdem eine Verbindung neu aufgebaut wird, und sollte zügig vorübergehen. Bleibt der Bildschirm länger als ein bis zwei Minuten auf dieser Meldung stehen, behandeln Sie es wie Die Appliance ist nicht erreichbar.

Mit der Appliance verbunden

Der Collector ist verbunden und sendet Daten. Kein Handlungsbedarf.

Die Appliance ist nicht erreichbar

Der Collector kann keine Netzwerkverbindung zu seiner Appliance aufbauen. Möglicherweise ist die Appliance ausgeschaltet, die eingetragene Adresse ist falsch, oder etwas auf dem Netzwerkpfad zwischen beiden blockiert die Verbindung.

Prüfen Sie, ob die Appliance eingeschaltet und im Netzwerk erreichbar ist, und ob die für den Collector eingetragene Adresse stimmt. Der Collector versucht es von selbst immer wieder erneut — sobald das Problem behoben ist, verbindet er sich ohne weiteres Zutun neu.

Die gesicherte Verbindung zur Appliance ist fehlgeschlagen

Der Collector hat die Appliance erreicht, aber die verschlüsselte Verbindung zwischen beiden kam nicht zustande. Das deutet meist auf ein Zertifikatsproblem an der Appliance, eine aus dem Takt geratene Uhr oder ein Netzwerkgerät hin, das die Verbindung stört.

Prüfen Sie das Zertifikat der Appliance und die Uhrzeit des Collectors. Klärt sich das Problem nicht von selbst, wenden Sie sich an den Support und lesen Sie ihm die technische Detailzeile auf dem Bildschirm vor.

Das Zertifikat der Appliance stimmt nicht mit dem hinterlegten überein

Der Collector merkt sich seit der Kopplung, welche Appliance es sein soll — und die Appliance weist sich jetzt mit einer anderen Identität aus als der, die der Collector kennt.

Wurde das Zertifikat der Appliance absichtlich erneuert oder ersetzt, ist das erwartbar — koppeln Sie den Collector erneut, damit er dem neuen Zertifikat vertraut. Haben Sie diese Änderung nicht selbst vorgenommen, koppeln Sie noch nicht neu: Wenden Sie sich zuerst an den Support, denn das kann auch bedeuten, dass der Collector mit der falschen Appliance spricht.

Die Appliance hat die Anmeldedaten dieses Collectors abgelehnt

Die Appliance akzeptiert die Anmeldedaten, die dieser Collector vorlegt, nicht. Koppeln Sie den Collector erneut, damit er von der Appliance neue Anmeldedaten erhält.

Die Appliance hat die Anmeldedaten dieses Collectors widerrufen

Eine Administratorin oder ein Administrator hat an der Appliance den Zugriff dieses Collectors ausdrücklich entzogen — zum Beispiel, weil der Collector außer Betrieb genommen oder ersetzt wurde.

Soll dieser Collector weiterhin verbunden sein, koppeln Sie ihn erneut über die Appliance. Wird er stillgelegt, ist kein Handeln nötig.

Die Appliance hat den Identitätsnachweis dieses Collectors abgelehnt

Die Appliance erkennt diesen Collector, konnte seine Identität beim Verbindungsversuch jedoch nicht bestätigen.

Koppeln Sie den Collector erneut, damit er eine neue Identität erhält, die die Appliance akzeptiert.

Dieser Collector ist noch mit keiner Appliance gekoppelt

Das ist ein frisch installierter Collector ohne eingerichtete Verbindung. Koppeln Sie ihn mit seiner Appliance, um loszulegen.

Der Pairing-Code wurde abgelehnt

Der bei der Einrichtung eingegebene Pairing-Code wurde nicht akzeptiert — er wurde möglicherweise falsch eingetippt, bereits verwendet oder für einen anderen Collector ausgestellt. Holen Sie sich an der Appliance einen neuen Pairing-Code und versuchen Sie es erneut.

Der Pairing-Code ist abgelaufen

Der Pairing-Code war gültig, aber bis zum Abschluss der Einrichtung ist zu viel Zeit vergangen. Erzeugen Sie einen neuen Pairing-Code und schließen Sie die Einrichtung diesmal zügig ab.

Der Collector-Dienst ist fehlgeschlagen

Der Hintergrunddienst des Collectors ist unerwartet gestoppt. Diese Meldung hat Vorrang vor jeder anderen, die der Bildschirm sonst zeigen würde. Wenden Sie sich an den Support — möglicherweise muss der Dienst neu gestartet oder das Problem genauer untersucht werden.

Der Collector-Dienst läuft nicht

Das kann zwei Ursachen haben: Entweder ist der Collector noch nicht gekoppelt, sodass der Dienst absichtlich ausgeschaltet bleibt (siehe Dieser Collector ist noch mit keiner Appliance gekoppelt), oder der Dienst eines zuvor funktionierenden Collectors wurde gestoppt.

Handelt es sich um einen neuen Collector, koppeln Sie ihn. Lief er zuvor, klären Sie, warum der Dienst gestoppt wurde, und starten Sie ihn neu.

Der Collector wird gestartet…

Der Dienst startet gerade und hat seinen Status noch nicht gemeldet. Das sollte innerhalb weniger Sekunden vorübergehen. Bleibt es dabei, wenden Sie sich an den Support.

Unbekannter Collector-Status (diese pulse-cli-Version ist möglicherweise älter als der Collector)

Der Collector hat einen Status gemeldet, den die Software auf dieser Konsole noch nicht kennt — meist, weil der Collector auf eine neuere Version aktualisiert wurde als die Konsolensoftware. Bringen Sie die Konsolensoftware auf denselben Stand. Bis dahin zeigt die technische Detailzeile auf dem Bildschirm, was der Collector tatsächlich meldet.

Siehe auch

- Collector-Kopplung — einen Collector koppeln und einen Collector neu koppeln, dessen Anmeldedaten oder Pairing-Code abgelehnt wurden.
- Bereitstellungsoptionen — die Firewall-Regeln, die ein Collector benötigt, wenn eine Meldung hier auf den Netzwerkpfad zur Appliance hindeutet.

10.2 Collector-Kopplung

Die Kopplung verbindet einen Collector mit der Appliance, bei der er sich meldet. Sie erfolgt einmalig, mit einem kurzlebigen Code, den Sie auf der Appliance erzeugen; danach merkt sich der Collector die Appliance und verbindet sich von selbst wieder mit ihr.

Die Verbindung läuft immer in eine Richtung: Der Collector wählt sich bei der Appliance ein. Von außerhalb seines eigenen Netzwerks muss nie etwas den Collector erreichen — deshalb kann er in einer abgeschotteten Zone laufen, die die Appliance selbst nicht erreicht. Wo ein Collector in den einzelnen Netzwerk-Topologien sitzt — und welche Firewall-Regeln dazugehören — beschreibt Bereitstellungsoptionen.

Einen Pairing-Code erhalten

Pairing-Codes kommen von der Appliance, nicht vom Collector.

1. Öffnen Sie in der Weboberfläche der Appliance **Organisation > Einstellungen > Collectors** und klicken Sie auf **Collector hinzufügen**.
2. Geben Sie dem Collector einen Namen und klicken Sie auf **Collector erstellen**.
3. Pulse zeigt den Dialog **Diesen Collector koppeln** mit allem, was der Installer abfragt:
   - **Collector-Adresse** — die Adresse, die Sie im Installer beim Schritt Appliance-Adresse eingeben.
   - **Pairing-Code**, daneben **Läuft ab**. Der Code ist nur einmal gültig und 30 Minuten lang.
   - **Appliance-Fingerabdruck** — heben Sie ihn sich auf; siehe Fingerabdruck prüfen weiter unten.

Lassen Sie den Dialog geöffnet, oder notieren Sie sich die Werte, bis Sie die passenden Schritte im Installer erreichen.

Eingabe während der Einrichtung

Wählen Sie im Installer die Rolle **Collector** und durchlaufen Sie wie gewohnt Festplatte, Netzwerk und NTP. Geben Sie bei Appliance-Adresse die Adresse aus dem Dialog ein. Geben Sie bei Pairing-Code den Code genau wie angezeigt ein — Groß- und Kleinschreibung spielen keine Rolle, und der Bindestrich ist optional. Ein falsch eingegebener Code wird sofort abgelehnt, bevor Sie zum Confirm-Bildschirm weitergehen können.

Kopplung beim ersten Start

Der Collector koppelt sich nicht während der Installation selbst — die Live-Installer-Umgebung hat möglicherweise nicht die Netzwerkeinstellungen, mit denen die fertig installierte Maschine am Ende läuft. Stattdessen erfolgt die Kopplung beim ersten Start des frisch installierten Systems: Es verbindet sich zu der angegebenen Appliance-Adresse und legt den Pairing-Code vor.

Wenn der Code abgelaufen ist

Ein Pairing-Code ist nur 30 Minuten lang gültig. Vergeht bis zum ersten Start des Collectors mehr Zeit — eine langsame Installation, ein verzögerter Neustart, Hardware, die eine Weile zum Hochfahren braucht —, funktioniert der Code nicht mehr, und der Statusbildschirm des Collectors zeigt, dass der Pairing-Code abgelaufen ist.

Einen neuen Code erhalten Sie auf demselben Weg wie den ersten: Öffnen Sie auf der Appliance **Organisation > Einstellungen > Collectors**, suchen Sie den Collector — er wird als **Wartet auf erste Verbindung** angezeigt — und wählen Sie **Neuen Pairing-Code erzeugen…**.

Fingerabdruck prüfen

Vergleichen Sie nach der Kopplung die Fingerabdrücke, um sicherzustellen, dass der Collector mit der Appliance spricht, die Sie erwarten:

- Der Statusbildschirm des Collectors zeigt den Fingerabdruck, den er sich bei der Kopplung gemerkt hat.
- Die Seite **Organisation > Einstellungen > Collectors** der Appliance zeigt für denselben Collector denselben Fingerabdruck, formatiert als hexadezimale Großbuchstaben in Vierergruppen (zum Beispiel `A1B2 C3D4 …`).

Sie müssen exakt übereinstimmen. Tun Sie das nicht, vertrauen Sie der Verbindung nicht — wenden Sie sich an den Support, oder widerrufen Sie den Collector und koppeln Sie ihn neu.

Einen Collector neu koppeln

Beim Neukoppeln wird die gesamte gespeicherte Verbindung eines Collectors ersetzt — die Anmeldedaten, die er der Appliance vorlegt, und der Fingerabdruck, den er sich gemerkt hat — durch einen neuen Satz, genau wie bei der ersten Kopplung. Das geschieht auf der Konsole des Collectors selbst, auf dem reinen Collector-Bildschirm **Appliance-Verbindung** (direkt nach SSH / SFTP-Zugang im Hauptmenü).

Koppeln Sie neu, wenn:

- der Statusbildschirm des Collectors ein nicht übereinstimmendes Zertifikat, abgelehnte oder widerrufene Anmeldedaten, einen abgelehnten oder abgelaufenen Pairing-Code oder einen abgelehnten Identitätsnachweis anzeigt. Drücken Sie auf diesem Bildschirm `p`, um direkt in das Neukopplungs-Formular zu springen.
- Sie diesen Collector absichtlich mit einer anderen Appliance verbinden möchten.

Einen neuen Pairing-Code erhalten Sie an derselben Stelle wie den ersten: Öffnen Sie in der Weboberfläche der Appliance **Organisation > Einstellungen > Collectors**, suchen Sie den Collector, und wählen Sie **Neuen Pairing-Code erzeugen…** (siehe Einen Pairing-Code erhalten weiter oben für das, was dieser Dialog zeigt).

Drücken Sie auf dem Bildschirm **Appliance-Verbindung** `p` für **Neu koppeln**, geben Sie die Adresse ein (vorausgefüllt mit der aktuell verwendeten — ändern Sie sie auch, wenn Sie den Collector auf eine andere Appliance verweisen wollen) und den neuen Code, und bestätigen Sie dann. Der Bildschirm warnt, dass die aktuelle Kopplung ersetzt wird, bevor er fortfährt. Nach der Bestätigung verwirft der Collector seine gespeicherten Anmeldedaten und den hinterlegten Fingerabdruck, speichert die neue Adresse und den neuen Code und verbindet sich neu — er koppelt sich also genau wie beim ersten Start erneut.

Die Appliance-Adresse ändern

Wenn eine Appliance zu einer neuen IP-Adresse oder einem neuen Hostnamen wechselt und sich sonst nichts ändert, verwenden Sie **Adresse ändern** auf dem Bildschirm **Appliance-Verbindung** des Collectors, statt neu zu koppeln. Geben Sie die neue Adresse ein; die bestehende Kopplung und der hinterlegte Fingerabdruck der Appliance bleiben beide erhalten, es ist also kein neuer Pairing-Code nötig — der Collector wählt sich einfach mit den Anmeldedaten, denen er bereits vertraut, unter der neuen Adresse ein.

Ein Backup vor dem Austausch einer Appliance wiederherstellen

Ein Backup, das erstellt wurde, nachdem Collectors eingerichtet waren, enthält das, was eine Ersatz-Appliance braucht, um sie verbunden zu halten: den dedizierten Collector-TLS-Schlüssel der Appliance und den Datenbankeintrag jedes gekoppelten Collectors. Die Datenbank allein wiederherzustellen reicht dafür aber nicht aus — die gespeicherte Konfiguration der Appliance, einschließlich dieses TLS-Schlüssels, muss ebenfalls zurückkommen, sonst erzeugt die Ersatz-Appliance beim ersten Start ihren eigenen, neuen Schlüssel, und jeder bereits gekoppelte Collector lehnt ihn als nicht

übereinstimmendes Zertifikat ab. Die Konfiguration zusammen mit der Datenbank wiederherzustellen ist über den geführten Bildschirm **Backups anzeigen / Wiederherstellen** heute nicht möglich; wenden Sie sich an den Support, bevor Sie eine Ersatz-Appliance in Betrieb nehmen, damit Collectors nicht neu gekoppelt werden müssen.

Ohne ein brauchbares Backup — oder nach einer reinen Datenbank-Wiederherstellung — zeigt jeder Collector auf seinem eigenen Statusbildschirm ein nicht übereinstimmendes Zertifikat oder abgelehnte Anmeldedaten an und muss einzeln neu gekoppelt werden; seine Datenquellen müssen in der Weboberfläche erneut zugewiesen werden.

Siehe auch

- Bereitstellungsoptionen — wo ein Collector in den einzelnen Netzwerk-Topologien sitzt und welche Firewall-Regeln er benötigt.
- Installation — der Installations-Assistent, einschließlich des Collector-Pfads.
- Collector-Status — was jede Statusmeldung bedeutet, einschließlich Kopplungsfehlern.
- Betrieb — Backups und Datenbank-Wiederherstellung.