15 – Überwachung, Benachrichtigungen und REST-API

Betrieb überwachen

Übersicht und Benachrichtigungen

Die Überwachung bewertet Dienst, Versandwege, Ausgangsordner, offene/fehlerhafte Vorgänge, Eingang, ERP Suite Connect und Filialverbund. Über **Benachrichtigung** aktivieren, Empfänger, Wartezeit und Wiederholung festlegen. Standard: 30 Minuten Wartezeit, Wiederholung nach 240 Minuten, optional Wieder-in-Ordnung-Mail. 0 als Wiederholung bedeutet einmalige Meldung.

Wochentage und Zeitfenster können Meldungen beschränken. Außerhalb werden Probleme gesammelt und später gemeldet. Fehlerhafte unbearbeitete Vorgänge werden standardmäßig nach 60 Minuten relevant; Warnungen nur bei aktivierter Option. Für Connect-Wartezeiten und Filialzustände gelten eigene Einstellungen. Letzte Meldung/Fehler sowie eine Testmail kontrollieren.

Die Benachrichtigung benötigt einen funktionierenden Mailtransport. Ein Ausfall dieses Wegs kann nicht zuverlässig über denselben Weg gemeldet werden; für den Dienstzustand ist zusätzlich externe Überwachung sinnvoll.

Eigene API-Schlüssel

Unter **REST-API** einen benannten Schlüssel mit nur den benötigten Rechten erstellen. Der Klartext wird einmal angezeigt; geschützt im Zielsystem hinterlegen. Belegpost speichert einen Hash. Schlüssel deaktivieren, wenn das Zielsystem nicht mehr verwendet wird. Keine echten Schlüssel in Beispiele oder Protokolle schreiben.

Recht	Zweck
status	Monitoring-Status abfragen
pruefen	Dokumente über die Prüfschnittstelle validieren
austausch	Standortgebundene Dateien und Client-Konfiguration im Filialverbund

Authentifizierung über **X-Api-Key** oder **Authorization: Bearer**. HTTPS mit gültigem Serverzertifikat verwenden. Status kann außerdem ein angemeldeter Portaladministrator lesen.

Endpunkte und Ergebnisse

Aufruf	Ergebnis
GET /api/v1/ping	Einfacher Erreichbarkeitscheck ohne Anmeldung; keine Gesamtbewertung
GET /api/v1/status	Gesamtstatus; 200 bei ok/warnung, 503 bei fehler
GET /api/v1/status/ausgang	Bereichsstatus; ebenso für versandwege, vorgaenge, eingang, connect und filialverbund
GET /api/v1/status-liste	Verfügbare Statusziele auflisten
POST /api/v1/pruefen	Datei validieren; 200 bei Annahme/ohne Fehler, 406 bei Ablehnung/Fehlern
/api/v1/austausch/...	Standortgebundene Konfiguration, Lebenszeichen, Dateien und Quittungen

`?immer200=1` liefert auch bei inhaltlich fehlerhaftem Status HTTP 200; dann muss das Überwachungssystem den Inhalt auswerten. `?details=0` verkürzt die Statusausgabe. Bei der Prüfung liefert `?text=1` einen Textbericht. Dateien als Rohinhalt mit passendem Content-Type oder als Multipart-Feld **datei** senden. Prüfgrößenlimit: 50 MB. Fehlender/ungültiger Schlüssel ergibt 401, fehlendes Recht 403.

Beispiel für einen Techniker, ohne echtes Geheimnis:

```
$portal = 'https://belegpost.kunde.example:5444'
$headers = @{ 'X-Api-Key' = '<API-SCHLUESSEL>' }
Invoke-RestMethod -Uri "$portal/api/v1/status" -Headers $headers
```

Das Muster erst nach Einsetzen einer kontrollierten Adresse und des geschützten Schlüssels ausführen. Schlüssel nicht im produktiven Skript oder in Git ablegen; im Zielsystem eine geeignete Geheimnisverwaltung verwenden. Für Prüf-Uploads und Filial-Importe das zugehörige Recht und die fachlichen Folgen gesondert abnehmen.

Created 2026-11-17 23:44:14 CET by Access MCP API
Updated 2026-11-17 23:44:14 CET by Access MCP API