

ScanDockPub

- [Übersicht](#)
- [Benutzer](#)
 - [Anmelden und Abmelden](#)
 - [Scans ansehen und herunterladen](#)
 - [Scans löschen](#)
 - [Ansicht anpassen](#)
 - [Meldungen und häufige Fragen](#)
- [Verwaltung \(Admins\)](#)
 - [Erste Einrichtung \(Microsoft Entra\)](#)
 - [FTP-Konten und Kopierer einrichten](#)
 - [Wer sieht welche Scans?](#)
 - [Einstellungen](#)
 - [Clientschlüssel erneuern](#)
 - [Journal](#)
 - [Häufige Fragen \(Admins\)](#)
- [Projekt \(Technik\)](#)
 - [Projektbeschreibung](#)
 - [Entscheidung: Architektur 0.0.1](#)
 - [Entscheidung: Gruppen über Microsoft Graph](#)
 - [Entscheidung: Öffentliche und private FTP-Konten](#)
 - [Entscheidung: Dateitypen und Inhaltsprüfung](#)
 - [Entscheidung: Verschlüsselte Ablage und Pseudo-IDs](#)
 - [Entscheidung: Admin-Journal](#)
 - [Changelog](#)
- [Installation, Betrieb & Fehlersuche](#)
 - [Installation \(neuer Server\)](#)
 - [Betrieb & CLI-Befehle](#)

- [Fehlersuche](#)

Übersicht

ScanDock – Hilfe

ScanDock bringt Scans von Kopierern und Multifunktionsgeräten in Ihre Microsoft-365-Umgebung. Die Geräte senden die Scans per FTP an ScanDock. Sie melden sich mit Ihrem Microsoft-Konto an und sehen, laden herunter oder löschen Ihre Scans.

Für wen ist welcher Teil?

Teil	Für wen	Themen
Benutzer	alle Mitarbeiter	Anmelden, Scans ansehen, herunterladen und löschen, Ansicht anpassen, Meldungen verstehen
Verwaltung (Admins)	Administratoren Ihrer Firma	Einrichtung, FTP-Konten und Kopierer, Berechtigungen, Einstellungen, Journal

Ihre persönliche Adresse lautet `https://<ihr-kürzel>.scandock.cloud`, das Kürzel erhalten Sie bei der Einrichtung.

Scans

Alle aufklappen

Alle zuklappen

Scans werden nach 30 Tagen automatisch gelöscht.

▼ Kopierer Empfang öffentlich

16 Scans

17:40 Uhr - „Notizen.docx“ wurde gelöscht: Dateityp „.docx“ ist nicht erlaubt (erlaubt: PDF, JPG, PNG, TIFF).

Rechnung

Rechnung: 10.10.2026 16:55 · 26,4 KB

Herunterladen Löschen

Listenvon

Stundenzettel_KW44.pdf

30.10.2026 14:40 · 22,2 KB

Herunterladen Löschen

Notizen

SCAN0003.pdf

30.10.2026 13:55 · 13,4 KB

Herunterladen Löschen

Scansicht

SCAN0002.pdf

30.10.2026 13:10 · 26 KB

Herunterladen Löschen

Auftragsbestätigung

Rechnung

Auftragsbestätigung

Listenvon

Startseite von ScanDock mit Scan-Liste (Gesamtansicht)

Kontakt

Bei Fragen, die diese Anleitungen nicht beantworten, wenden Sie sich an Ihren ScanDock-Ansprechpartner.

Benutzer

Anleitungen für alle, die sich bei ScanDock anmelden und Scans ansehen, herunterladen oder löschen.

Anmelden und Abmelden

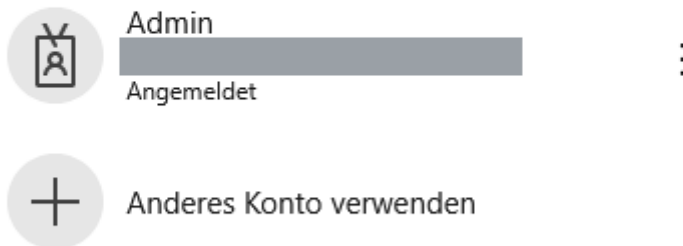
Anmelden und Abmelden

Anmelden

1. Öffnen Sie die Adresse Ihrer Firma, z. B. `https://<ihr-kürzel>.scandock.cloud`.
2. Sie werden zur Anmeldung bei Microsoft weitergeleitet. Melden Sie sich mit Ihrem



Konto auswählen



Microsoft-Anmeldeseite mit

Kontoauswahl

Beim allerersten Mal kann Microsoft fragen, ob ScanDock Ihr Profil lesen darf. Bestätigen Sie mit **Akzeptieren**. Erscheint stattdessen „Administratorgenehmigung erforderlich“, wenden Sie sich an Ihren Administrator.

Ihr Menü

Oben rechts steht Ihre E-Mail-Adresse. Ein Klick öffnet das Menü mit **Darstellung** (Hell, Dunkel, System) und **Abmelden**. Administratoren finden dort zusätzlich FTP-Konten, Einstellungen und Journal. Links daneben führt **Hilfe** zu diesen Anleitungen.

Scans

Scans werden nach 30 Tagen automatisch gelöscht.

▼ **Kopierer Empfang** öffentlich

17:40 Uhr - „Notizen.docx“ wurde gelöscht: Dateityp „.docx“ ist nicht erlaubt (erlaubt: PDF, JPG, PNG, TIFF).

Alle auf

FTP-Konten

Einstellungen

Journal

Darstellung

Hell

Dunkel

System

Abmelden

Kopfzeile mit Logos, Hilfe-Button und geöffnetem Benutzermenü

Abmelden

Menü öffnen → **Abmelden**. Nach 8 Stunden ohne Abmeldung endet die Sitzung automatisch.

Scans ansehen und herunterladen

Scans ansehen und herunterladen

Die Scans sind nach **Geräten (FTP-Konten)** gegliedert, z. B. „Kopierer Empfang“. Sie sehen nur die Geräte, für die Sie freigeschaltet sind. Die neuesten Scans stehen jeweils oben.

 ScanDock  Stefan Kittel IT Solutions  Muster GmbH **Muster GmbH**

Hilfe

anna.admin@muster-gmbh.example ▾

Scans

Alle aufklappen

Alle zuklappen

Scans werden nach 30 Tagen automatisch gelöscht.

▼ **Kopierer Empfang** öffentlich

16 Scans

17:40 Uhr - „Notizen.docx“ wurde gelöscht: Dateityp „.docx“ ist nicht erlaubt (erlaubt: PDF, JPG, PNG, TIFF).

Rechnung

Resultat: Die Rechnung liegt bereit zum Abrufen:

Art	Bezeichnung	Preis	Stückzahl	Netto	Brutto
1	Grundpreis	1,00	1	1,00	1,19
2	Umsatzsteuer	0,00	1	0,00	0,19
3	Netto	1,00	1	1,00	1,19
4	Brutto	1,00	1	1,00	1,19

Das Dokument ist als PDF-Datei erstellt und kann über den Download-Button heruntergeladen werden. Die Datei ist als PDF-Datei erstellt und kann über den Download-Button heruntergeladen werden.

Wartungsbericht_Heizung...
30.10.2026 16:55 · 26,4 KB

Herunterladen Löschen

Leistungschein

Resultat: Hierhergehörige ist nicht zulässig, keine Abrechnung vom Kunden:

Das Dokument ist als PDF-Datei erstellt und kann über den Download-Button heruntergeladen werden. Die Datei ist als PDF-Datei erstellt und kann über den Download-Button heruntergeladen werden.

Stundenzettel_KW44.pdf
30.10.2026 14:40 · 22,2 KB

Herunterladen Löschen

Vertrag

Resultat: Hierhergehörige ist nicht zulässig:

Das Dokument ist als PDF-Datei erstellt und kann über den Download-Button heruntergeladen werden. Die Datei ist als PDF-Datei erstellt und kann über den Download-Button heruntergeladen werden.

SCAN0003.pdf
30.10.2026 13:55 · 13,4 KB

Herunterladen Löschen

GuKarte

Resultat: GuKarte ist nicht zulässig, keine Abrechnung vom Kunden:

Das Dokument ist als PDF-Datei erstellt und kann über den Download-Button heruntergeladen werden. Die Datei ist als PDF-Datei erstellt und kann über den Download-Button heruntergeladen werden.

SCAN0002.pdf
30.10.2026 13:10 · 26 KB

Herunterladen Löschen

Auftragsbestätigung

Resultat: Auftrag ist nicht zulässig, keine Abrechnung vom Kunden:

Das Dokument ist als PDF-Datei erstellt und kann über den Download-Button heruntergeladen werden. Die Datei ist als PDF-Datei erstellt und kann über den Download-Button heruntergeladen werden.

Auftragsbestätigung

Herunterladen Löschen

Rechnung

Resultat: Rechnung ist nicht zulässig, keine Abrechnung vom Kunden:

Das Dokument ist als PDF-Datei erstellt und kann über den Download-Button heruntergeladen werden. Die Datei ist als PDF-Datei erstellt und kann über den Download-Button heruntergeladen werden.

Rechnung

Herunterladen Löschen

Auftragsbestätigung

Resultat: Auftrag ist nicht zulässig, keine Abrechnung vom Kunden:

Das Dokument ist als PDF-Datei erstellt und kann über den Download-Button heruntergeladen werden. Die Datei ist als PDF-Datei erstellt und kann über den Download-Button heruntergeladen werden.

Auftragsbestätigung

Herunterladen Löschen

Leistungschein

Resultat: Leistungschein ist nicht zulässig, keine Abrechnung vom Kunden:

Das Dokument ist als PDF-Datei erstellt und kann über den Download-Button heruntergeladen werden. Die Datei ist als PDF-Datei erstellt und kann über den Download-Button heruntergeladen werden.

Leistungschein

Herunterladen Löschen

Scan-Seite in der Kachelansicht

Ansehen

- Klicken Sie auf das **Vorschaubild** oder den **Dateinamen**. Der Scan öffnet sich in einem neuen Tab.
- PDF, JPG und PNG zeigt der Browser direkt an. TIFF-Scans werden zur Ansicht als PDF geöffnet.

Herunterladen

- **Einzeln:** Button **Herunterladen** am Scan.
- **Mehrere auf einmal:** In die **Listenansicht** wechseln (Symbol mit Zeilen im Kopf des Bereichs), die gewünschten Scans anhaken oder **Alle** wählen und **Ausgewählte herunterladen** klicken. Sie erhalten eine ZIP-Datei.

Kopierer Empfang öffentlich 16 Scans

17:40 Uhr - „Notizen.docx“ wurde gelöscht: Dateityp „.docx“ ist nicht erlaubt (erlaubt: PDF, JPG, PNG, TIFF).

Alle Keine Ausgewählte herunterladen (3) Ausgewählte löschen (3)

	Datei	Eingang	Größe	
☒	 Wartungsbericht_Heizung.pdf	30.10.2026 16:55	26,4 KB	Herunterladen Löschen
☒	 Stundenzettel_KW44.pdf	30.10.2026 14:40	22,2 KB	Herunterladen Löschen
☒	 SCAN0003.pdf	30.10.2026 13:55	13,4 KB	Herunterladen Löschen

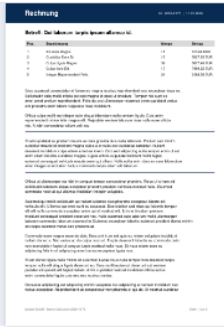
Listenansicht mit Häkchen, Buttons Alle/Keine und „Ausgewählte herunterladen (3)“

Neue Scans

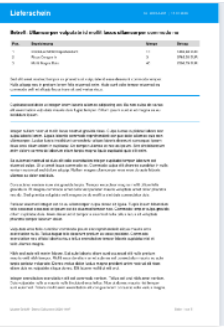
Neue Scans erscheinen nach wenigen Sekunden von selbst, ohne dass Sie die Seite neu laden. Während der Übertragung zeigt eine gestrichelte Kachel „Wird übertragen ...“ bzw. „Wird verarbeitet ...“.



Rechnung_10445.pdf
Wird übertragen ... · 80 KB
ausstehend



Wartungsbericht_Heizung....
30.10.2026 16:55 · 26,4 KB
[Herunterladen](#) [Löschen](#)



Stundenzettel_KW44.pdf
30.10.2026 14:40 · 22,2 KB
[Herunterladen](#) [Löschen](#)



SCAN0003.pdf
30.10.2026 13:55 · 13,4 KB
[Herunterladen](#) [Löschen](#)

Gestrichelte Kachel „Wird übertragen ...“ während eines Scans

Dateinamen

ScanDock vereinheitlicht die Dateinamen der Geräte: Umlaute werden umgeschrieben (ä → ae, ß → ss), Sonderzeichen und Leerzeichen werden zu `_`, sehr lange Namen werden gekürzt und erhalten eine Nummer, z. B. `Uebergabeprotokoll_Grundst0000.pdf`.

Scans löschen

Scans löschen

- **Einzeln:** Button **Löschen** am Scan und bestätigen.
- **Mehrere:** In der **Listenansicht** die Scans anhaken und **Ausgewählte löschen** klicken.

▼

Kopierer Empfang

öffentlich

16 Scans

17:40 Uhr - „Notizen.docx“ wurde gelöscht: Dateityp „.docx“ ist nicht erlaubt (erlaubt: PDF, JPG, PNG, TIFF).

Alle

Keine

Ausgewählte herunterladen (3)

Ausgewählte löschen (3)

	Datei	Eingang	Größe	
☒	 Wartungsbericht_Heizung.pdf	30.10.2026 16:55	26,4 KB	<div>HerunterladenLöschen</div>
☒	 Stundenzettel_KW44.pdf	30.10.2026 14:40	22,2 KB	<div>HerunterladenLöschen</div>
☒	 SCAN0003.pdf	30.10.2026 13:55	13,4 KB	<div>HerunterladenLöschen</div>

Listenansicht mit drei markierten Scans und „Ausgewählte löschen (3)“

Gelöschte Scans lassen sich **nicht wiederherstellen**.

Automatisches Löschen

Scans werden nach einer festen Frist automatisch gelöscht (Standard **30 Tage**, von Ihrem Administrator einstellbar). Die Frist steht oben auf der Scan-Seite. Laden Sie Dokumente, die Sie länger brauchen, rechtzeitig herunter und legen Sie sie z. B. in SharePoint ab.

Benutzer

Ansicht anpassen

Ansicht anpassen

Alle Einstellungen auf dieser Seite werden für Ihr Konto gespeichert und gelten auch auf anderen Geräten.

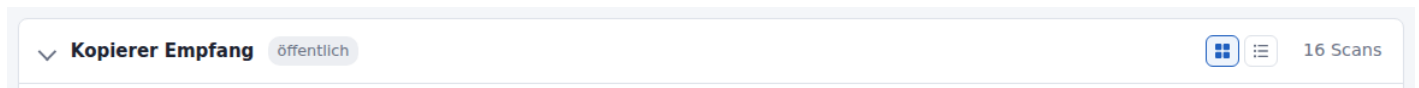
Bereiche auf- und zuklappen

Klicken Sie auf den Kopf eines Bereichs (Gerätename). Oben gibt es **Alle aufklappen** und **Alle zuklappen**.

Kacheln oder Liste

Im Kopf jedes Bereichs, links neben der Anzahl, stehen zwei Symbole:

- **Kacheln:** große Vorschaubilder
- **Liste:** kompakt, mit Häkchen zum Herunterladen oder Löschen mehrerer Scans



Kopf eines Bereichs mit den beiden Ansichts-Symbolen

Hell oder dunkel

Menü (Ihre E-Mail-Adresse oben rechts) → **Darstellung:** **Hell**, **Dunkel** oder **System** (folgt der Einstellung Ihres Computers).

Meldungen und häufige Fragen

Meldungen und häufige Fragen

Farbige Hinweise

Hinweis	Bedeutung	Was tun?
Gelb: „... wurde gelöscht: ...“ im Bereich eines Geräts	Eine Datei des Kopierers wurde nicht angenommen, der Grund steht dabei (z. B. falscher Dateityp, größer als 50 MB, beschädigt, verdächtiger Inhalt). Der Hinweis verschwindet nach 1 Stunde.	Scan erneut senden, ggf. als PDF und mit geringerer Auflösung. Bei Wiederholung den Administrator informieren.
Rot: „Der Empfang von Scans ist gesperrt“	Auf dem Server ist vorübergehend zu wenig Speicherplatz frei. Kopierer können nicht senden, vorhandene Scans sind weiter verfügbar.	Nichts, der Empfang wird automatisch wieder freigegeben.
Gelb: „Ihre Gruppenmitgliedschaften konnten nicht aktualisiert werden“	Microsoft war kurz nicht erreichbar. Freigaben über Gruppen gelten vorübergehend nicht.	Neu anmelden klicken.

17:40 Uhr - „Notizen.docx“ wurde gelöscht: Dateityp „.docx“ ist nicht erlaubt (erlaubt: PDF, JPG, PNG, TIFF).

Gelber Hinweis zu einer abgelehnten Datei im Bereich eines Geräts

Häufige Fragen

Mein Scan erscheint nicht. Warten Sie etwa 30 Sekunden. Erscheint ein gelber Hinweis, steht dort der Grund. Erscheint nichts, hat der Kopierer die Datei vermutlich nicht gesendet (Fehlermeldung am Gerät prüfen).

Ich sehe ein Gerät nicht, obwohl Kollegen es sehen. Das Gerät ist privat und Sie sind (noch) nicht freigeschaltet. Bitte wenden Sie sich an Ihren Administrator. Änderungen wirken nach spätestens 5 Minuten.

„Ihnen ist noch kein Gerät zugeordnet.“ Für Sie ist noch kein Gerät freigegeben. Wenden Sie sich an Ihren Administrator.

Warum heißt meine Datei anders als am Kopierer eingestellt? ScanDock vereinheitlicht Dateinamen (siehe *Scans ansehen und herunterladen*).

Verwaltung (Admins)

Anleitungen für Administratoren: Einrichtung, FTP-Konten und Kopierer, Berechtigungen, Einstellungen und Journal.

Erste Einrichtung (Microsoft Entra)

Erste Einrichtung (Microsoft Entra)

Sie erhalten von Ihrem ScanDock-Ansprechpartner einen **Start-Link**. Er führt Schritt für Schritt durch die Anbindung an Ihr Microsoft Entra ID (früher Azure AD). Sie benötigen die Rolle **Anwendungsadministrator** oder **Globaler Administrator**.



ScanDock



Stefan Kittel
IT Solutions



Muster GmbH Muster GmbH

Einrichtung für Muster GmbH

Damit sich Ihre Mitarbeiter mit ihrem Microsoft-365-Konto anmelden können, legen Sie in Ihrem Microsoft Entra ID eine App-Registrierung an. Dafür benötigen Sie die Rolle *Anwendungsadministrator* oder *Globaler Administrator*.

1. App registrieren

1. Öffnen Sie entra.microsoft.com → *Identität* → *Anwendungen* → *App-Registrierungen* und klicken Sie auf **Neue Registrierung**.
2. Name: `ScanDock`
3. Unterstützte Kontotypen: **Nur Konten in diesem Organisationsverzeichnis** (einzelner Mandant)
4. Umleitungs-URI: Plattform **Web**, Wert:
`https://demo.scandock.cloud/auth/callback`
5. Auf **Registrieren** klicken.

2. Werte notieren

Auf der Übersichtsseite der App finden Sie die **Anwendungs-ID (Client)** und die **Verzeichnis-ID (Mandant)**.

3. Geheimen Clientschlüssel erstellen

1. **Zertifikate & Geheimnisse** → **Geheime Clientschlüssel** → **Neuer geheimer Clientschlüssel**
2. Beschreibung `ScanDock`, Ablauf z. B. 24 Monate. Das Ablaufdatum tragen Sie unten mit ein.
3. Kopieren Sie den **Wert** (nicht die Geheimnis-ID). Er wird nur einmal angezeigt.

4. API-Berechtigung prüfen

1. Unter **API-Berechtigungen** muss **Microsoft Graph** → **User.Read** (delegiert) eingetragen sein. Bei neuen Registrierungen ist das bereits der Fall.
2. Empfohlen: **Administratorzustimmung für <Ihre Organisation> erteilen** klicken. Dann werden Ihre Mitarbeiter bei der ersten Anmeldung nicht nach ihrer Zustimmung gefragt.

Mit User.Read liest ScanDock bei jeder Anmeldung nur die Gruppenmitgliedschaften des angemeldeten Benutzers (auch Microsoft-365-Gruppen und verschachtelte Gruppen). Darüber vergeben Sie Rechte (Admin-Gruppe, Zugriff auf FTP-Konten). Eine Tokenkonfiguration ist nicht nötig.

Einrichtungsassistent nach Öffnen des Start-Links

Ablauf

1. **App registrieren:** In entra.microsoft.com → *Identität* → *Anwendungen* → *App-Registrierungen* → *Neue Registrierung*. Name z. B. „ScanDock“, *Nur Konten in diesem Organisationsverzeichnis*, Umleitungs-URI (Plattform *Web*) so, wie sie im Assistenten angezeigt wird.

2. **Werte notieren:** *Anwendungs-ID (Client)* und *Verzeichnis-ID (Mandant)* von der Übersichtsseite der App.
3. **Geheimen Clientschlüssel erstellen:** *Zertifikate & Geheimnisse* → *Neuer geheimer Clientschlüssel*. Den **Wert** (nicht die Geheimnis-ID) kopieren und das **Ablaufdatum** notieren.
4. **Berechtigung prüfen:** *API-Berechtigungen: Microsoft Graph* → *User.Read* (delegiert) ist bei neuen Apps bereits vorhanden. Empfohlen: **Administratorzustimmung erteilen**.
5. **Werte im Assistenten eintragen** und speichern. ScanDock prüft die Angaben sofort bei Microsoft.
6. **Mit Microsoft anmelden.** Klappt die Anmeldung, ist die Einrichtung abgeschlossen und der Start-Link ungültig.

Home > Unternehmensanwendungen | Alle Anwendungen > ScanDock | Übersicht > App-Registrierungen

ScanDock

Suche

Deaktivieren Löschend Endpunkte

Übersicht

Schnellstart

Integrations-Assistent

Diagnose und Problembehandlung

Verwalten

Branding und Eigenschaften

Authentication (Preview)

Haben Sie einen Moment Zeit? Wir würden uns sehr über Ihr Feedback zur Microsoft Identity Platform (früher Azure AD für Entwickler) freuen. →

Zusammenfassung

Anzeigenname : ScanDock

Anwendungs-ID (Client) :

Objekt-ID :

Verzeichnis-ID (Mandant) :

Unterstützte Kontotypen : Nur meine Organisation

Clientanmeldeinformatio... : 0 Zertifikat, 1 Geheimnis

Umleitungs-URIs : 1 vom Typ "Web", 0 vom Typ "SPA", 0 vom Typ "öffentl...

Anwendungs-ID-URI : Anwendungs-ID-URI hinzufügen

Verwaltete Anwendung i... : ScanDock

Zustand : Aktiviert

Entra: Übersichtsseite der App mit Anwendungs-ID und Verzeichnis-ID

Home > Unternehmensanwendungen | Alle Anwendungen > ScanDock | Übersicht > App-Registrierungen > ScanDock

ScanDock | API-Berechtigungen

Suche

AktualisierenHaben Sie Feedback für uns?

Übersicht

Schnellstart

Integrations-Assistent

Diagnose und Problembehandlung

Verwalten

Branding und Eigenschaften

Authentication (Preview)

Zertifikate & Geheimnisse

Tokenkonfiguration

API-Berechtigungen

Eine API verfügbar machen

App-Rollen

Besitzer

Rollen und Administratoren

Manifest

Support + Problembehandlung

Neue Supportanfrage

Durch das Erteilen einer mandantenweiten Einwilligung können Berechtigungen widerrufen werden, die bereits mandantenweit für diese Anwendung erteilt wurden. Berechtigungen, die Benutzer bereits in ihrem eigenen Namen erteilt haben, sind davon nicht betroffen. [Weitere Informationen](#)

In der Spalte "Administratoreinwilligung erforderlich," wird der Standardwert für eine Organisation angezeigt. Die Benutzereinwilligung kann jedoch pro Berechtigung, Benutzer oder App angepasst werden. Diese Spalte zeigt möglicherweise nicht den Wert für Ihre Organisation oder für Organisationen, in denen diese App verwendet wird. [Weitere Informationen](#)

Konfigurierte Berechtigungen

Anwendungen sind zum Aufruf von APIs autorisiert, wenn ihnen im Rahmen des Zustimmungsprozesses Berechtigungen von Benutzern/Administratoren erteilt werden. Die Liste der konfigurierten Berechtigungen muss alle Berechtigungen enthalten, die die Anwendung benötigt. [Weitere Informationen zu Berechtigungen und Zustimmung](#)

Berechtigung hinzufügen

Administratorzustimmung für Ihre Organisation

erteilen

API/Berechtigungsname	Typ	Beschreibung	Administratoreinwill...	Status	
Microsoft Graph (6)					
email	Delegiert	E-Mail-Adresse von Benutzern anzeigen	Nein	Gewährt für *	...
Group.ReadBasic.All	Anwendung	Read all groups' basic property	Ja	Gewährt für *	...
openid	Delegiert	Benutzer anmelden	Nein	Gewährt für *	...
profile	Delegiert	Grundlegendes Profil von Benutzern anzeigen	Nein	Gewährt für *	...
User.Read	Delegiert	Anmelden und Benutzerprofil lesen	Nein	Gewährt für *	...
User.Read.All	Anwendung	Read all users' full profiles	Ja	Gewährt für *	...

Entra: API-Berechtigungen mit „Administratorzustimmung erteilen“

Optional: Vorschläge aus dem Verzeichnis

Damit ScanDock beim Freigeben von Geräten Personen und Gruppen aus Ihrem Verzeichnis vorschlägt: *API-Berechtigungen* → *Berechtigung hinzufügen* → *Microsoft Graph* →

Anwendungsberechtigungen: `User.Read.All` und `Group.ReadBasic.All`, danach

Administratorzustimmung erteilen. Ohne diese Berechtigungen geben Sie Anmeldenamen bzw. Gruppen-IDs von Hand ein.

Nach der Einrichtung

Zunächst haben **alle** angemeldeten Benutzer Admin-Rechte. Legen Sie deshalb gleich eine Admin-Gruppe fest (siehe *Einstellungen*). Den Start-Link verloren oder abgelaufen? Ihr ScanDock-Ansprechpartner stellt einen neuen aus.

FTP-Konten und Kopierer einrichten

FTP-Konten und Kopierer einrichten

Jeder Kopierer (oder Standort) erhält ein eigenes **FTP-Konto**. Die Scans eines Kontos erscheinen in der Weboberfläche als eigener Bereich.

Konto anlegen

Menü → **FTP-Konten** → Bezeichnung eingeben (z. B. „Kopierer Empfang“), **privat** oder **öffentlich** wählen → **FTP-Konto anlegen**.

 ScanDock

 Stefan Kittel
IT Solutions

 Muster GmbH

Muster GmbH

Hilfe

anna.admin@muster-gmbh.example ▾

FTP-Konten

Jeder Kopierer (oder Standort) erhält ein eigenes FTP-Konto. Über das Konto können nur Scans hochgeladen werden (PDF, JPG, PNG oder TIFF, höchstens 50 MB pro Datei).

☒ privat ☐ öffentlich FTP-Konto anlegen

Öffentlich: alle Benutzer sehen die Scans. **Privat:** nur die eingetragenen Personen und Gruppen – auch Administratoren nur, wenn sie eingetragen sind.

Bezeichnung	Sichtbarkeit	Benutzername	Status	Scans
Kopierer Empfang	öffentlich	demo-kkj74c	aktiv	16
Kopierer Geschäftsführung	privat	demo-g3jdw	aktiv	4

Seite FTP-Konten mit Formular „FTP-Konto anlegen“ und Liste der Konten

Zugangsdaten für den Kopierer

Feld am Kopierer	Wert
Server / Host	ftp.scandock.cloud
Port	21 (FTP oder FTPS explizit „AUTH TLS“) oder 990 (FTPS implizit)
Benutzername	wie angezeigt, z. B. firma-ab12cd
Passwort	wie angezeigt (siehe unten)
Verzeichnis / Pfad	/ oder leer
Modus	Passiv (PASV)

Feld am Kopierer	Wert
Dateiformat	PDF empfohlen (auch JPG, PNG, TIFF möglich)

Das **Passwort** wird nur direkt nach dem Anlegen bzw. nach **Neues Passwort** im Klartext angezeigt. Danach steht dort , das **Augen-Symbol** zeigt es bei Bedarf an.

Zugangsdaten für den Kopierer

Server ftp.scandock.cloud

Port 21 FTP oder FTPS (explizit, „AUTH TLS“) · 990 FTPS implizit

Benutzername demo-kkj74c

Passwort 

Verzeichnis / Pfad / (leer lassen, falls möglich)

Modus Passiv (PASV)

Wenn der Kopierer es unterstützt, FTPS verwenden. Unverschlüsseltes FTP überträgt Passwort und Dokumente im Klartext. Das Konto kann nur Scans hochladen (PDF, JPG, PNG oder TIFF, höchstens 50 MB), aber keine Dateien auflisten, lesen oder löschen.

Neues Passwort
Sperren
Löschen

Detailseite eines FTP-Kontos mit Zugangsdaten und Augen-Symbol

Empfehlung: Nutzen Sie **FTPS**, wenn der Kopierer es unterstützt. Bei unverschlüsseltem FTP werden Passwort und Dokumente im Klartext übertragen.

Was ein Kopierer darf

Das Konto kann **nur hochladen**: keine Dateien auflisten, lesen oder löschen. Ein mitgelesenes Passwort verrät deshalb keine Scans.

Regeln für Dateien

- Erlaubt: **PDF, JPG/JPEG, PNG, TIFF**. Andere Dateien werden gelöscht und gemeldet.
- Maximal **50 MB** pro Datei (übliche Scans: 0,5–5 MB). Größere Übertragungen bricht der Server ab, der Kopierer meldet einen Fehler, in ScanDock erscheint ein Hinweis.
- Jede Datei wird auf echten Inhalt und Schadcode (z. B. HTML/Skript in PDFs) geprüft.
- Dateinamen werden vereinheitlicht (Umlaute → ae/oe/ue/ss, Sonderzeichen → , max. 30 Zeichen).

ScanDock ist für Kopierer gedacht, nicht zum Austausch beliebiger Dateien.

Konto verwalten

Auf der Detailseite: **Neues Passwort** (altes gilt sofort nicht mehr, Kopierer umstellen!),
Sperren/Aktivieren, Löschen (löscht auch **alle Scans** des Kontos).

Wer sieht welche Scans?

Wer sieht welche Scans?

Jedes FTP-Konto ist entweder **öffentlich** oder **privat**. Einstellung auf der Detailseite des Kontos unter *Wer sieht die Scans?*.

Sichtbarkeit	Wer sieht die Scans
Öffentlich	alle angemeldeten Benutzer Ihrer Firma
Privat	nur die eingetragenen Personen und Mitglieder der eingetragenen Gruppen

Wichtig: Auch Administratoren sehen private Scans **nur**, wenn sie selbst oder eine ihrer Gruppen eingetragen sind. Verwalten (Zugangsdaten, Freigaben) können Admins jedes Konto.

Wer sieht die Scans?

☐ Öffentlich – alle Benutzer sehen die Scans

☒ Privat – nur die unten eingetragenen Personen und Gruppen sehen die Scans

Auch Administratoren sehen private Scans nur, wenn sie selbst oder eine ihrer Gruppen eingetragen sind.

Typ	Name	Kennung	
Person	Anna Admin	anna.admin@muster-gmbh.example	Entfernen
Gruppe	Geschäftsführung	d0d0d0d0-0000-4000-8000-000000000002	Entfernen

Person oder Gruppe hinzufügen

Name, Anmeldename oder Gruppe suchen ...

Hinzufügen

Vorschläge kommen aus Ihrem Microsoft-Verzeichnis, sofern ScanDock die Anwendungsberechtigungen *User.Read.All* und *Group.ReadBasic.All* hat. Sonst werden Personen vorgeschlagen, die sich schon angemeldet haben. Sie können auch direkt einen Anmeldennamen (name@firma.de) oder die Objekt-ID einer Gruppe eingeben.

Bereich „Wer sieht die Scans?“ mit Auswahl öffentlich/privat und Liste der Freigaben

Personen oder Gruppen hinzufügen

Im Feld *Person oder Gruppe hinzufügen* tippen, ab 2 Zeichen erscheinen Vorschläge. Auswählen → **Hinzufügen**.

- Ohne Vorschläge aus dem Verzeichnis (siehe *Erste Einrichtung*, optional) geben Sie den **Anmeldenamen** (`name@firma.de`) oder die **Objekt-ID** einer Entra-Gruppe ein.
- Personen werden intern über ihre feste Microsoft-ID erkannt. Eine spätere Umbenennung schadet nicht, und ein neuer Mitarbeiter mit einer wiederverwendeten Adresse erhält **keinen** Zugriff.
- Gruppenänderungen in Entra wirken nach spätestens etwa 5 Minuten.

Hinzufügen

Bernd Beispiel

Person · bernd.beispiel@muster-gmbh.example

Objekt-ID einer Gruppe eingeben.

basic.All hat.

de) oder die

Eingabefeld mit Vorschlagsliste (Personen und Gruppen)

Entfernen

Entfernen neben dem Eintrag. Wird ein privates Konto öffentlich, bleiben die Einträge gespeichert und gelten wieder, sobald es erneut privat wird.

Verwaltung (Admins)

Einstellungen

Einstellungen

Menü → **Einstellungen**.

Firma

Firmenname und **Logo** (PNG, JPG, WebP oder SVG, max. 1 MB). Beides erscheint oben links neben dem ScanDock-Logo.



The screenshot shows a settings panel titled 'Firma'. It contains a text input field for 'Firmenname (Anzeigename)' with the value 'Muster GmbH'. Below it is a section for the 'Logo (PNG, JPG, WebP oder SVG, max. 1 MB)' with a 'Choose File' button and the text 'No file chosen'. A preview of the current logo is shown as a green square with a white triangle and the text 'Muster GmbH', with the caption 'Aktuelles Logo – eine neue Datei ersetzt es.' Below the logo section are two buttons: a blue 'Speichern' button and a red 'Logo entfernen' button.

Einstellungen, Abschnitt Firma mit Logo-Vorschau

Admin-Gruppe

Objekt-ID einer Entra-Gruppe. Nur deren Mitglieder haben dann Admin-Rechte. Solange keine Gruppe eingetragen ist, sind **alle** angemeldeten Benutzer Admins, darauf weist ein gelber Hinweis hin.

- Die Objekt-ID finden Sie in Entra unter *Gruppen → Gruppe → Übersicht*.
- Sind Sie selbst nicht Mitglied, warnt ScanDock, bevor Sie sich aussperren.

Aufbewahrung

Anzahl Tage (1-999, Standard 30), nach denen Scans automatisch gelöscht werden.

Geheimer Clientschlüssel

Siehe *Clientschlüssel* erneuern.

Clientschlüssel erneuern

Clientschlüssel erneuern

Der geheime Clientschlüssel der Entra-App läuft ab (meist nach 24 Monaten). Danach kann sich **niemand** mehr anmelden. ScanDock warnt Admins **30 Tage vorher** mit einem gelben Hinweis, nach Ablauf mit einem roten.

 ScanDock |  Stefan Kittel
IT Solutions |  **Muster GmbH** **Muster GmbH**

Hilfe

anna.admin@muster-gmbh.example ▾

Der geheime Clientschlüssel der Entra-App läuft in 12 Tagen ab (11.11.2026). Danach kann sich niemand mehr anmelden. [Jetzt erneuern](#)

Scans

Alle aufklappen

Alle zuklappen

Scans werden nach 30 Tagen automatisch gelöscht.

Gelber Hinweis „Der geheime Clientschlüssel ... läuft in 12 Tagen ab“

So geht's

1. In Entra: *App-Registrierungen* → ScanDock → Zertifikate & Geheimnisse → **Neuer geheimer Clientschlüssel**.
2. In ScanDock: Menü → **Einstellungen** → **Geheimer Clientschlüssel: Wert** und **Ablaufdatum** eintragen → **Schlüssel prüfen und speichern**. ScanDock prüft den Schlüssel sofort bei Microsoft.
3. Erst danach den alten Schlüssel in Entra löschen.

Schon abgelaufen? Wenden Sie sich an Ihren ScanDock-Ansprechpartner. Er stellt einen neuen Start-Link aus, über den Sie den Schlüssel erneuern. Die Kopierer senden in der Zwischenzeit weiter.

Journal

Journal

Menü → **Journal** (nur für Admins). Hier ist nachvollziehbar, wer wann was geändert hat:

- **Einstellungen:** Admin-Gruppe, Aufbewahrung, Firmenname, Logo, Clientschlüssel
 - **FTP-Konten:** angelegt, gelöscht, Passwort erneuert, gesperrt/aktiviert, Sichtbarkeit, Personen/Gruppen
 - **Scans:** eingegangen, abgelehnt (mit Grund), gelöscht (von Hand oder nach Ablauf der Frist)
 - **System:** z. B. Empfang wegen Speichermangel gesperrt/freigegeben
- Jeder Eintrag enthält Zeitpunkt, Person (bzw. „System“) und IP-Adresse. **Nicht** protokolliert werden Anmeldungen, das Ansehen und das Herunterladen von Scans. Einträge werden nach **einem Jahr** gelöscht.

 ScanDock

 Stefan Kittel
IT Solutions

 **Muster GmbH** **Muster GmbH**

Hilfe

anna.admin@muster-gmbh.example ▾

Journal

FTP-Konten ▾

Änderungen an Einstellungen und FTP-Konten sowie eingegangene, abgelehnte und gelöschte Scans. Anmeldungen und Downloads werden nicht protokolliert. Einträge werden nach einem Jahr gelöscht.

Zeitpunkt	Bereich	Vorgang	Durch	IP-Adresse
30.10.2026 17:40:12	FTP-Konten	FTP-Konto „Kopierer Geschäftsführung“: Person „Anna Admin (anna.admin@muster-gmbh.example)“ hinzugefügt	Anna Admin (anna.admin@muster-gmbh.example)	
30.10.2026 17:40:12	FTP-Konten	FTP-Konto „Kopierer Geschäftsführung“: Gruppe „Geschäftsführung“ hinzugefügt	Anna Admin (anna.admin@muster-gmbh.example)	
30.10.2026 17:40:12	FTP-Konten	FTP-Konto „Kopierer Geschäftsführung“ angelegt (privat)	Anna Admin (anna.admin@muster-gmbh.example)	

Journal mit Filter „Bereich“ und einigen Einträgen

Häufige Fragen (Admins)

Häufige Fragen (Admins)

Der Kopierer meldet einen Fehler beim Senden. Zugangsdaten und Einstellungen prüfen (Host `ftp.scandock.cloud`, Port, **Passiv**-Modus, Pfad `/`). Zu große Dateien (über 50 MB) bricht der Server ab, dann am Kopierer Auflösung oder Farbe reduzieren. Bei FTPS-Problemen testweise Port 990 bzw. 21 probieren.

Der Kopierer meldet Erfolg, aber der Scan fehlt. Im Bereich des Geräts bzw. im **Journal** nach „abgelehnt“ suchen, der Grund steht dabei.

Anmeldung schlägt fehl (Meldung mit „AADSTS...“). Häufige Ursachen: abgelaufener Clientschlüssel, falsche Umleitungs-URI in der App-Registrierung, fehlende Zustimmung. Die Meldung nennt den Grund. Sonst Ihren ScanDock-Ansprechpartner kontaktieren.

Ein Kollege sieht ein privates Gerät nicht. Ist er (oder eine seiner Gruppen) beim Gerät eingetragen? Gruppenänderungen in Entra wirken nach etwa 5 Minuten.

Ich habe meine Admin-Rechte verloren. Ist eine Admin-Gruppe eingetragen, braucht man deren Mitgliedschaft. Ein anderer Admin kann helfen, sonst Ihr ScanDock-Ansprechpartner.

Roter Hinweis „Empfang gesperrt“. Speicherplatz auf dem Server knapp. Der Betreiber kümmert sich darum, der Empfang wird automatisch wieder freigegeben.

Projekt (Technik)

Hintergrund für Interessierte und Entwickler: Projektbeschreibung, Entscheidungen und Änderungen. Für die Bedienung von ScanDock nicht nötig.

Projektbeschreibung

Projektbeschreibung ScanDock

Stand: 2026-10-31 · Version 0.0.34 (erster Kunde aktiv; bis 0.0.18 hieß das Projekt ScanKai)

Problem

Kunden mit Kopierern/MFPs ziehen in die Cloud (Microsoft 365). Selbst neue Geräte können nicht nach SharePoint oder auf SMB-Freigaben in der Cloud scannen. Viele Geräte können außerdem nur unverschlüsseltes FTP.

Lösung

ScanDock ist ein mandantenfähiger Scan-Eingang:

1. Am Kopierer wird ein FTP-Ziel eingerichtet (FTP unverschlüsselt oder FTPS), mit Zugangsdaten von ScanDock.
2. Gescannte Dokumente (PDF, JPEG, PNG, TIFF) landen auf dem ScanDock-Server. Jede Datei wird auf echten Inhalt und Schadcode (HTML/Skript, aktive PDF-Inhalte) geprüft, andere Dateien werden gelöscht.
3. Benutzer melden sich mit ihrem Microsoft-365-Konto (Entra ID) unter `<slug>.scandock.cloud` an, sehen die PDFs mit Vorschau und laden sie herunter.
4. Dateien werden nach n Tagen automatisch oder vorher manuell gelöscht.

Abgrenzung

ScanDock ist für **Kopierer und Multifunktionsgeräte** gedacht, nicht als Plattform zum Dateiaustausch. Übliche Scans sind 0,5 bis 5 MB groß, die Grenze von 50 MB liegt beim Zehnfachen.

Mandanten

- Jeder Kunde hat einen Slug, z. B. `kunde.scandock.cloud` .

- Der Betreiber legt Kunden per CLI über SSH an. Dabei entstehen der vHost mit Let's-Encrypt-Zertifikat und ein Start-Link.
- Der Start-Link führt den Kunden durch die Anbindung an Entra: Anleitung, die einzutragenden Werte (z. B. Redirect-URI) und die Eingabe der Werte aus Entra (Tenant-ID, Client-ID, Secret).
- Sobald die Anmeldung über Entra einmal funktioniert hat, ist der Start-Link ungültig.

Rollen

- Anfangs sind alle Benutzer Admins.
- In den Einstellungen kann eine Entra-Gruppe als Admin-Gruppe festgelegt werden.
- Admins legen FTP-Konten an (Anzeige: Host, Port, Zugangsdaten). Ein Konto ist **öffentlich** (alle sehen die Scans) oder **privat** (nur zugeordnete Personen und Entra-Gruppen, Auswahl mit Autovervollständigung).
- Admins verwalten alle Einstellungen, sehen private Scans aber nur, wenn sie selbst zugeordnet sind.

Weitere Funktionen

- Admin-Journal mit allen Änderungen und Datei-Vorgängen (ohne Anmeldungen/Downloads), nur für Admins.
- Listenansicht mit Mehrfachauswahl zum Löschen oder Herunterladen als ZIP.
- Scans verschlüsselt gespeichert (ein Schlüssel pro Kunde), Pseudo-IDs in allen URLs.
- Tägliche lokale Datensicherung (letzte 30), externe Sicherung als ToDo.
- Maximal 50 MB pro Datei, durchgesetzt vom FTP-Server. Abgebrochene Uploads werden wie andere abgelehnte Dateien angezeigt. Unter 10 GB freiem Speicher wird der Empfang automatisch gesperrt (Hinweis für alle Benutzer).
- Dateinamen werden normalisiert (Umlaute → ae/oe/ue/ss, nur a-z/A-Z/0-9, max. 30 Zeichen ohne Endung).

Hilfe für Kunden

Button **Hilfe** in der Anwendung → öffentliches Support-Wiki

<https://wiki.skit.center/books/scandockpub> (Deutsch; Teile *Benutzer* und *Verwaltung (Admins)*). Die CLI ist nur für den Betreiber und wird dort nicht beschrieben.

Eckdaten

Punkt	Wert
-------	------

Domain	<code>scandock.cloud</code> , Wildcard <code>*.scandock.cloud</code> → <Server-IP>
SSL	Let's Encrypt, ein Zertifikat pro Hostname (HTTP-01), kein Wildcard
Stack	Codelgniter 4, Apache, PHP 8.5, MariaDB 11.8, ProFTPD
FTP	<code>ftp.scandock.cloud</code> , Port 21 (FTP/FTPS explizit), 990 (FTPS implizit), nur Hochladen; PDF/JPEG/PNG/TIFF mit Inhaltsprüfung
Aufbewahrung	Standard 30 Tage, pro Kunde einstellbar
Code	https://github.com/Skittel/scandock (öffentlich), Code und Doku auf Englisch
Lizenz	MIT plus Pflicht zum Verweis auf das GitHub-Repo in der README
Versionierung	n.n.n, jede Stelle 0–999

Entscheidung: Architektur 0.0.1

Entscheidung: Architektur ScanKai 0.0.1

2026-10-30

FTP-Server: ProFTPD mit MariaDB

- **Gewählt:** ProFTPD 1.3.9 mit mod_sql (virtuelle Benutzer aus der Datenbank) und mod_tls.
- **Begründung:** Kann unverschlüsseltes FTP, explizites FTPS (Port 21) und implizites FTPS (Port 990). Konten verwaltet die Web-App direkt in der Datenbank, ohne Systembenutzer. pure-ftpd kann kein implizites FTPS.
- ProFTPD liest nur die View `ftp_users` mit einem eigenen DB-Benutzer, der nur Leserechte hat. Gesperrte Konten und Kunden, die nicht aktiv sind, können sich nicht anmelden.
- Passwörter: SHA-512-crypt für ProFTPD. Zusätzlich verschlüsselt gespeichert, damit Admins sie anzeigen können (Vorgabe).

FTP nur zum Hochladen

- Erlaubt sind nur STOR/STOU sowie Verzeichniswechsel. Lesen, Löschen, Umbenennen, Verzeichnisse anlegen usw. sind gesperrt.
- LIST liefert eine leere Liste ohne Dateinamen. Das ist besser verträglich mit Kopierern, die nach dem Upload ein LIST schicken.
- Nur `*.pdf`, max. 200 MB pro Datei, kein Überschreiben, Uploads werden als versteckte Datei geschrieben, bis sie vollständig sind.
- Schutz vor Brute-Force: mod_ban (3 Fehlversuche in 10 Minuten führen zu 1 Stunde Sperre) und fail2ban.
- Begründung: Bei unverschlüsseltem FTP kann das Passwort mitgelesen werden. Ein Angreifer kann damit keine Scans abrufen.

FTP-Host

- Gemeinsamer Host `ftp.scan kai . site` mit eigenem Let's-Encrypt-Zertifikat, da ProFTPD Zertifikate pro Hostname nur schlecht unterstützt. Der Slug `ftp` und weitere Namen sind für Kunden gesperrt.

Import der Scans

- Ein systemd-Timer importiert alle 20 Sekunden fertige Uploads: PDF-Signatur prüfen, in den Speicher kopieren, Vorschaubild (pdftoppm) erzeugen, Datenbankeintrag schreiben und erst dann die Quelle löschen. So geht bei einem Fehler kein Scan verloren.
- Ein täglicher Timer um 03:15 löscht Scans nach Ablauf der Frist (Standard 30 Tage, pro Kunde einstellbar).

Anmeldung: Entra ID

- Jeder Kunde legt eine eigene App-Registrierung für einen einzelnen Mandanten an. Der Start-Link führt mit Anleitung durch die Einrichtung.
- OpenID Connect mit Autorisierungscode und PKCE. Geprüft werden Signatur, Aussteller, Zielgruppe, Mandant und Nonce des ID-Tokens.
- Gruppen kommen aus dem `groups`-Claim (Tokenkonfiguration). Bei mehr als 200 Gruppen übermittelt Entra keine Liste, dann gibt es einen Hinweis.
- Die erste erfolgreiche Anmeldung aktiviert den Kunden und macht den Start-Link ungültig. Gespeichert wird nur ein Hash des Tokens.

Rechte

- Ohne Admin-Gruppe ist jeder angemeldete Benutzer Admin. Sobald eine Gruppe eingetragen ist, sind nur deren Mitglieder Admins. Ein Schutz verhindert, dass man sich versehentlich selbst aussperrt.
- Admins sehen alle Scans. Andere Benutzer sehen nur Scans der FTP-Konten, denen sie als Person (UPN) oder über eine Entra-Gruppe zugeordnet sind.

Server

- Pro Hostname ein Apache-vHost und ein Let's-Encrypt-Zertifikat (HTTP-01, webroot). Port 80 beantwortet nur die Prüfungen von Let's Encrypt und leitet alles andere auf HTTPS weiter.
- Privilegierte Aktionen erledigt nur `/usr/local/sbin/scankai-site`, das den Hostnamen streng prüft. www-data darf genau dieses Skript per sudo ausführen.
- Firewall öffentlich: 80, 443, 21, 990, 40000-40100/tcp (freigegeben durch den Projektinhaber).
- Server-Konfiguration als Kopie im Repo unter `deploy/`.

Entscheidung: Gruppen über Microsoft Graph

Entscheidung: Gruppen über Microsoft Graph statt Tokenkonfiguration

2026-10-30 · Version 0.0.5

Ausgangslage

Bis 0.0.4 kamen die Gruppen nur aus dem `groups`-Claim des ID-Tokens (Tokenkonfiguration der App-Registrierung). Nachteile:

- muss vom Kunden zusätzlich eingerichtet werden und wird leicht vergessen
- „Sicherheitsgruppen“ enthält keine Microsoft-365-Gruppen
- maximal 200 Gruppen, sonst kommt gar keine Liste
- Änderungen werden erst bei der nächsten Anmeldung sichtbar

Optionen

Variante	Berechtigung	Admin-Zustimmung	Bewertung
Gruppen-Claim (Tokenkonfiguration)	keine	nein	Nachteile siehe oben
Graph <code>/me/transitiveMemberOf</code>	User.Read (delegiert)	nein (empfohlen, damit keine Abfrage beim Benutzer)	nur eigene Gruppen, alle Gruppenarten, auch verschachtelt
Graph mit Group.Read.All / GroupMember.Read.All	erhöht	ja	darf alle Gruppen des Mandanten lesen, mehr als nötig

Entscheidung

- Bei der Anmeldung wird `User.Read` angefordert. ScanKai liest die Gruppen des Benutzers über `/me/transitiveMemberOf` und vereinigt sie mit einem eventuell vorhandenen Gruppen-Claim.
- **Abgleich beim Speichern:** Ist der Admin laut Datenbank nicht Mitglied der neuen Admin-Gruppe, werden seine Gruppen sofort bei Microsoft abgefragt, solange das Zugriffstoken der Sitzung (ca. 1 Stunde) noch gilt. Ist es abgelaufen, folgt eine stille Anmeldung (`prompt=none`), danach wird das Speichern automatisch fortgesetzt. Ist er dann immer noch kein Mitglied, wird gewarnt.
- Der Gruppen-Claim ist optional, eine Tokenkonfiguration ist nicht mehr nötig.
- Gespeichert werden nur Gruppen-IDs. Gruppennamen liefert `User.Read` nicht.

Entscheidung: Öffentliche und private FTP-Konten

Entscheidung: Öffentliche und private FTP-Konten

2026-10-30 · Version 0.0.6 · Vorgabe des Projektinhabers

Regeln

- Jedes FTP-Konto ist **öffentlich** (alle Benutzer des Kunden sehen die Scans) oder **privat** (nur eingetragene Personen und Entra-Gruppen).
- **Admins** dürfen alle Einstellungen sehen und ändern: Konten, Zugangsdaten, Sichtbarkeit, Mitglieder, Einstellungen. Sie sehen öffentliche Scans, **private Scans aber nur, wenn sie selbst oder eine ihrer Gruppen eingetragen sind.**
- Neue Konten sind standardmäßig privat, öffentlich ist per Auswahl beim Anlegen möglich. Bestehende Konten ohne Mitglieder wurden bei der Migration öffentlich, Konten mit Mitgliedern privat.
- Wird ein privates Konto öffentlich, bleiben die eingetragenen Mitglieder gespeichert und gelten wieder, sobald das Konto erneut privat wird.

Zuordnung mit Autovervollständigung

- Ein einziges Eingabefeld für Personen und Gruppen, Vorschläge erscheinen ab 2 Zeichen.
- Quellen:
 1. **Entra-Verzeichnis** über Microsoft Graph mit App-Token (Client Credentials).
Optional, benötigt die Anwendungsberechtigungen `User.Read.All` und `Group.ReadBasic.All` mit Administratorzustimmung. Ohne Berechtigung pausiert die Abfrage für 10 Minuten.
 2. **Lokal:** Benutzer, die sich schon angemeldet haben, und Gruppen, die bereits zugeordnet sind.
- Freie Eingabe bleibt möglich: Eine E-Mail-Adresse wird als Person (UPN) gespeichert, eine GUID als Gruppe.
- Begründung für die Anwendungsberechtigungen statt delegierter: Die Suche läuft serverseitig und unabhängig von der Sitzung des Admins, und normale Benutzer müssen

bei der Anmeldung keinen zusätzlichen Berechtigungen zustimmen.

Entscheidung: Dateitypen und Inhaltsprüfung

Entscheidung: Erlaubte Dateitypen und Inhaltsprüfung

2026-10-30 · Version 0.0.15 · Anlass: Virus in einer PDF-Datei mit HTML-Inhalt

Erlaubt

PDF, JPEG (`.jpg`, `.jpeg`), PNG, TIFF (`.tif`, `.tiff`). Alle anderen Dateien werden beim Import sofort gelöscht.

Der PDF-Filter in ProFTPD wurde dafür entfernt. Sonst würde der FTP-Server unerwünschte Dateien schon beim Upload ablehnen, und ScanKai könnte nicht anzeigen, dass und warum eine Datei verworfen wurde.

Prüfungen beim Import (App\Libraries\FileInspector)

1. **Endung erlaubt?**
2. **Datei nicht leer?**
3. **Signatur passt zur Endung:** `%PDF-`, JPEG `FF D8 FF`, PNG-Signatur, TIFF `II*` / `MM*`. Bei Abweichung wird genannt, was tatsächlich erkannt wurde (z. B. HTML-Dokument, Windows-Programm, ZIP/Office, E-Mail/MHT).
4. **Kein HTML- oder Skript-Code** im Rohinhalt: `<html`, `<script`, `<iframe`, `<object`, `<!doctype html`, `<meta http-equiv`, `<?php`, `javascript:`, `vbscript:`, `MIME-Version: 1.0`, `Content-Type: text/html`. Es werden bewusst nur lange, eindeutige Muster verwendet. Kurze Muster wie `<svg` würden in komprimierten Bilddaten zufällig vorkommen.
5. **PDF:**
 - `pdfinfo` muss die Datei lesen können.
 - Struktur über `qpdf --json` ohne Stream-Daten, inklusive Objekten in komprimierten Objekt-Streams. Abgelehnt bei `/JavaScript`, `/JS`, `/Launch`, `/EmbeddedFile`,

`/RichMedia`, `/XFA`, `/SubmitForm`, `/ImportData`, `/GoToE`.

- Entpackte Streams (`qpdf --qdf`) werden erneut auf HTML/Skript geprüft.

6. **Bilder:** `getimagesize` muss ein gültiges Bild des erwarteten Typs liefern.

Anzeige

- Abgelehnte Dateien werden gelöscht und in `scan_rejections` protokolliert. Der Grund steht eine Stunde lang als Balken im Abschnitt des FTP-Kontos (nur für Benutzer, die dieses Konto sehen). Die Einträge bleiben 30 Tage gespeichert.
- TIFF: Für die Anzeige im Browser wird eine PDF-Fassung erzeugt (`tiff2pdf`, Rückfallebene ImageMagick). Heruntergeladen wird immer das Original.

Getestet

14 präparierte Dateien, darunter HTML als PDF, PDF mit angehängtem HTML, PDF-JavaScript (auch versteckt im Objekt-Stream), HTML in einem komprimierten Stream, EXE als JPG und JPEG mit Skript-Kommentar: alle korrekt erkannt. Keine Fehlalarme bei 20 Demo-PDFs, einer 29-MB-Bild-PDF und Rausch-Bildern (JPEG, PNG, TIFF).

Kein Virens Scanner

Entscheidung des Projekthinhabers (2026-10-30): **kein ClamAV**. Begründung: Ein Angreifer braucht zumindest gültige FTP-Zugangsdaten. Die Inhaltsprüfung deckt Tarnung (falsche Endung, HTML/Skript) und aktive PDF-Inhalte ab.

Entscheidung: Verschlüsselte Ablage und Pseudo-IDs

Entscheidung: Verschlüsselte Ablage und Pseudo-IDs

2026-10-30 · Version 0.0.18 · Vorgabe des Projektinhabers

Verschlüsselung der Dateien

- **Ziel:** Dateien liegen nur verschlüsselt auf dem Laufwerk. Es geht nicht um Ende-zu-Ende-Verschlüsselung, der Server kann die Dateien zum Anzeigen entschlüsseln.
- **Verfahren:** libsodium secretstream (XChaCha20-Poly1305), in Blöcken von 64 KiB, damit große Dateien nicht in den Arbeitsspeicher geladen werden müssen. Dateiformat: `SKE1` + Header + Blöcke, Dateiendung `.enc`.
- **Schlüssel:** einer pro Kunde (`tenants.storage_key`), selbst verschlüsselt mit dem Anwendungsschlüssel `encryption.key` aus `/var/www/scankai/.env`. Er wird beim ersten Gebrauch erzeugt.
- **Verschlüsselt werden:** Original (`<uuid>.<ext>.enc`), Vorschaubild (`<uuid>.thumb.png.enc`), TIFF-Ansicht (`<uuid>.view.pdf.enc`). Firmenlogos bleiben unverschlüsselt.
- **Unverschlüsselt kurzzeitig:** Die Datei liegt nur im FTP-Eingang, bis zum Import (ca. 1 Sekunde). Vorschaubild und Ansicht entstehen in `/dev/shm` (RAM). Zum Anzeigen und Herunterladen wird ebenfalls in den RAM entschlüsselt, die Kopie wird danach gelöscht.
- **Bestehende Scans:** `scankai scans:encrypt` verschlüsselt sie und prüft vor dem Löschen der unverschlüsselten Datei die SHA-256-Prüfsumme. Bei Kunde 1 wurden 25 Scans umgestellt und einzeln geprüft.
- **Wichtig für Backups:** Ohne `encryption.key` aus der `.env` sind alle Scans **unwiederbringlich** verloren. `.env`, Datenbank und `/srv/scankai/storage` gehören immer zusammen in die Sicherung.

Pseudo-IDs in URLs

- Scans, FTP-Konten und Berechtigungseinträge haben eine zufällige `public_id` (16 Zeichen aus `a-z` ohne `l/o` und `2-9`, ca. 80 Bit).

- Sie wird verwendet in URLs (`/scans/<id>/view`, `/admin/ftp/<id>`), Formularen, Blätter-Parametern (`?page_a<id>`) und Hintergrund-Anfragen (Auf-/Zuklappen, Ansicht, Mehrfach-Löschen).
- Datenbank-IDs erscheinen nicht mehr nach außen. Aus den Nummern lässt sich nicht ablesen, wie viele Scans oder Konten es gibt.

Entscheidung: Admin-Journal

Entscheidung: Admin-Journal

2026-10-30 · Version 0.0.23 · Vorgabe des Projektinhabers

Jeder Kunde hat ein Journal unter **Menü → Journal** (`/admin/journal`). **Nur Admins** sehen es, normale Benutzer erhalten 403 und haben keinen Menüpunkt.

Protokolliert

Bereich	Vorgänge
Einstellungen	Admin-Gruppe (alt → neu), Aufbewahrung (alt → neu), Firmenname (alt → neu), Logo hochgeladen/entfernt, Clientschlüssel erneuert (mit Ablaufdatum)
FTP-Konten	angelegt (Sichtbarkeit), gelöscht (mit Anzahl gelöschter Scans), neues Passwort, gesperrt/aktiviert, Sichtbarkeit (alt → neu), Person/Gruppe hinzugefügt/entfernt
Scans	eingegangen (Konto, Größe), abgelehnt und gelöscht (Grund), von Hand gelöscht (auch Mehrfach-Löschen, je Datei ein Eintrag), nach Ablauf der Aufbewahrung gelöscht
System	Einrichtung abgeschlossen, Aktionen des Betreibers per CLI (Umbenennen, Sperren/Entsperren, neuer Start-Link)

Je Eintrag: Zeitpunkt, Bereich, Beschreibung, wer (Name und UPN zum Zeitpunkt der Aktion, „System (FTP)“, „System“ oder „Betreiber (CLI)“) und die IP-Adresse bei Web-Aktionen.

Nicht protokolliert

Anmeldungen, Ansehen und Herunterladen von Scans (auch als ZIP), persönliche Einstellungen (Darstellung, Auf-/Zuklappen, Listen-/Kachelansicht).

Technik

Tabelle `audit_log` (`tenant_id`, `user_id`, `actor`, `category`, `action`, `details` als JSON, `ip`, `created_at`). Die Texte entstehen aus Aktionscode und Details (`App\\Libraries\\AuditLog::ACTIONS`). Einträge werden **ein Jahr** aufbewahrt. Der tägliche Löschlauf (03:15 Uhr) entfernt ältere (`Config\\ScanDock::$auditRetentionDays = 365` , seit 0.0.24).

Ebenfalls in 0.0.23: ZIP-Download

In der Listenansicht lädt „Ausgewählte herunterladen (n)“ die markierten Scans als ZIP: entschlüsselt im RAM, eindeutige Dateinamen, höchstens 1 GB, nur Scans mit Zugriffsrecht. Downloads erscheinen bewusst nicht im Journal.

Changelog

Changelog

Kurzform aller wesentlichen Änderungen und Entscheidungen an ScanDock. Langform der Entscheidungen: Kapitel [Projekt \(Technik\)](#). Anleitungen: Kapitel [Benutzer](#) und [Verwaltung \(Admins\)](#).

Einträge sind für die Öffentlichkeit bereinigt (keine Kundennamen, IDs oder IP-Adressen).

2026-10-30

- Projektname: **ScanKai**. Domain `scankai.site`, Mandanten per Subdomain-Slug (`<slug>.scankai.site`).
- Stack: CodeIgniter 4, Apache, PHP 8.5 (Ubuntu 26.04, erfüllt 8.4+), MariaDB 11.8.
- SSL: Let's Encrypt pro Hostname.
- GitHub: <https://github.com/Skittel/scankai> (öffentlich).
- Lizenz: freie private und gewerbliche Nutzung, Pflicht nur: Verweis auf das GitHub-Repo in der README.
- Firewall (ufw) aktiv: eingehend nur von den Admin-Adressen des Betreibers.
- Versionierung n.n.n (je 0-999), Start 0.0.1.
- LAMP installiert: Apache 2.4.66, PHP 8.5.4, MariaDB 11.8.6, Composer 2.9.5, Certbot 4.0.0.
- Ports 80 und 443 öffentlich freigegeben (Freigabe durch Projektinhaber). Port 80 beantwortet nur Let's-Encrypt-Prüfungen und leitet alles andere per 301 auf HTTPS weiter.
- Kein Wildcard-Zertifikat: keine Live-Änderungen am DNS (kritische Infrastruktur). Ein Zertifikat pro Hostname per HTTP-01 (webroot `/var/www/letsencrypt`), anfangs 3-4 Kunden.
- GitHub-Zugang über Deploy-Key (`~ubuntu/.ssh/scankai_deploy` , SSH-Alias `github-scankai`).
- Zweck festgelegt: Scan-Eingang per FTP/FTPS für Kopierer, Ansicht und Download nach Anmeldung über Entra (siehe Projektbeschreibung).
- FTP: ProFTPD mit MariaDB, Host `ftp.scankai.site` , Ports 21/990/40000-40100 öffentlich (Freigabe durch Projektinhaber), **nur Hochladen**, nur PDF.
- Löschfrist Standard 30 Tage, pro Kunde einstellbar.
- Lizenz: MIT mit Pflicht zum README-Verweis (bestätigt).
- **Version 0.0.1** umgesetzt und getestet (FTP/FTPS/implizit, Upload-Sperren, Import, Rechte, CSRF, Löschfrist, Token-Prüfung); nach GitHub gepusht, Tag v0.0.1.
- Erster Kunde angelegt (Status: Einrichtung), Start-Link an den Projektinhaber übergeben.
- Langform: [Entscheidung: Architektur 0.0.1](#)
- **Version 0.0.2:**

- Ablaufdatum des Entra-Clientschlüssels wird erfasst. Admins werden 30 Tage vorher gewarnt und können den Schlüssel in den Einstellungen erneuern. Der Schlüssel wird vor dem Speichern bei Microsoft geprüft.
- Start-Link wird zusätzlich verschlüsselt gespeichert. `tenant:link` zeigt ihn an, `tenant:link-renew` erzeugt einen neuen. Ein aktiver Kunde bleibt dabei aktiv, FTP läuft weiter (ersetzt `--reset`).
- Statische Landingpage für scankai.site und www.scankai.site (deutsch/englisch), Skittel-Logo lokal eingebunden (keine Anfragen an fremde Server), Links auf Impressum und Datenschutz von skittel.de, alle Links öffnen in einem neuen Tab.
- ScanKai-Logo als Vektorgrafik nachgebaut (Vorlage war nur ein JPEG). Die Welle bewegt sich sehr langsam und steht still, wenn Nutzer reduzierte Bewegung eingestellt haben. Dazu Favicon. Schriftzug aus Nunito Black (SIL OFL).
- Öffentliches Wiki <https://wiki.skit.center/books/scankai-ZE7>: Kapitel **Deutsch** und **English** mit je einer Übersichtsseite angelegt, Anleitungen folgen.
- Neue Seite CLI-Befehle.
- **Version 0.0.3:** Logo durch den SVG-Entwurf des Projektinhabers ersetzt. Der Schriftzug ist in Pfade umgewandelt (Liberation Sans Bold, gleiche Maße wie Arial, SIL OFL), die Welle bewegt sich sehr langsam (ein Zyklus in 20 Sekunden), Favicon neu erzeugt.
- Kunde 1 ist eingerichtet und aktiv (erste Anmeldung über Entra 11:19).
- **Version 0.0.4:** Klarere Hinweise zu Gruppen. Microsoft übermittelt Gruppen nur bei der Anmeldung (nach Änderungen ab- und wieder anmelden). Der Gruppenanspruch „Sicherheitsgruppen“ enthält keine Microsoft-365-Gruppen, dafür „Alle Gruppen“ wählen.
- **Version 0.0.5:** Gruppen werden bei der Anmeldung über Microsoft Graph gelesen (Berechtigung User.Read, ohne Tokenkonfiguration). Beim Speichern der Admin-Gruppe werden die Gruppen mit Microsoft abgeglichen. Langform: [Entscheidung: Gruppen über Microsoft Graph](#)
- Gruppenabfrage über Graph in der Praxis bestätigt: Bei Kunde 1 ist die Admin-Gruppe `<Gruppen-ID>` gesetzt, der Abgleich beim Speichern hat funktioniert.
- **Version 0.0.6:** FTP-Konten sind öffentlich oder privat. Admins sehen private Scans nur, wenn sie eingetragen sind. Personen und Gruppen werden über ein Feld mit Autovervollständigung zugeordnet (Verzeichnissuche optional über Anwendungsberechtigungen). das erste FTP-Konto des ersten Kunden ist durch die Migration öffentlich. Langform: [Entscheidung: Öffentliche und private FTP-Konten](#)
- **Version 0.0.7:** Das FTP-Passwort steht nur direkt nach dem Anlegen bzw. nach „Neues Passwort“ im Klartext da, danach als •••••• mit Augen-Symbol zum Anzeigen (wird erst beim Klick geladen).
- **Version 0.0.8:** Fehler behoben: Die Autovervollständigung blieb ohne Treffer stumm, und nach einer neuen Admin-Zustimmung wurde bis zu einer Stunde ein altes App-Token ohne Berechtigungen benutzt. Jetzt erscheint „Keine Treffer“ bzw. ein Hinweis auf fehlende Berechtigungen, eine eingetippte UPN oder Gruppen-ID wird direkt angeboten, und bei einer Ablehnung wird das Token verworfen. Bei Kunde 1 sind User.Read.All und Group.ReadBasic.All jetzt erteilt.
- **Version 0.0.9:** Die Scan-Seite ist nach FTP-Konten gegliedert, ein aufklappbarer Abschnitt pro Konto. Standardmäßig sind alle offen, dazu „Alle aufklappen“/„Alle zuklappen“. Der Zustand wird pro Benutzer dauerhaft gespeichert, Blättern geht pro

Konto. Entscheidung: Der CSRF-Token gilt jetzt pro Sitzung statt pro Anfrage, damit Speichern im Hintergrund die übrigen Formulare der Seite nicht ungültig macht.

- **Version 0.0.10:** Fehler behoben: Gruppenmitgliedschaften wurden nur bei der Anmeldung gelesen. Wer danach einer Gruppe beitrug, sah das freigegebene Konto erst nach erneuter Anmeldung. Jetzt werden die Gruppen angemeldeter Benutzer alle 5 Minuten aktualisiert (App-Token über Graph, sonst das Token der Sitzung).
- **Version 0.0.11:** Admins pflegen unter Einstellungen → Firma den Anzeigenamen und laden ein Firmenlogo hoch (PNG/JPG/WebP/SVG, max. 1 MB, SVGs mit Skripten werden abgelehnt). Die Kopfzeile zeigt ScanKai-Logo, Kundenlogo und Firmennamen. Neuer CLI-Befehl `tenant:rename`. Fehler behoben: Radiobuttons standen über dem Text.
- **Version 0.0.12:** Kopfzeile in der Reihenfolge ScanKai-Logo, Skittel-Logo (Link auf skittel.de, öffnet im neuen Tab), Kundenlogo und Firmenname. Betreiber-Logo, -Name und -URL sind in `Config\\ScanKai` einstellbar.
- **Version 0.0.13:** Nach einem Upload erscheint sofort ein Platzhalter mit Dateiname und Status („Wird übertragen ...“ / „Wird verarbeitet ...“), die Scan-Seite aktualisiert sich selbst. Ein neuer Dateiwächter (inotify, Dienst `scankai-upload-watch`) startet den Import direkt nach dem Upload: gemessen 1,3 Sekunden statt bisher bis zu 30. Der Timer bleibt als Rückfallebene.
- **Version 0.0.14:** Oben rechts steht die E-Mail-Adresse des Benutzers und öffnet ein Menü mit FTP-Konten und Einstellungen (nur Admins), Darstellung Hell/Dunkel/System und Abmelden. Den Menüpunkt „Scans“ gibt es nicht mehr, das Logo führt zu den Scans. Dunkelmodus kam neu hinzu und wird pro Benutzer gespeichert. Scans sind nach Eingang sortiert, die neuesten oben (bei gleicher Sekunde nach Import-Reihenfolge).
- **Version 0.0.15:** Erlaubt sind nur noch PDF, JPG/JPEG, PNG und TIFF, alle anderen Dateien werden sofort gelöscht. Jede Datei wird auf echten Inhalt, HTML- und Skript-Code (auch versteckt in PDF-Streams) und aktive PDF-Inhalte geprüft. Abgelehnte Dateien erscheinen eine Stunde lang mit Grund als Balken im Konto. Langform: [Entscheidung: Dateitypen und Inhaltsprüfung](#)
- Entscheidung: **kein Virenschanner (ClamAV)**, weil ein Angreifer zumindest gültige FTP-Zugangsdaten bräuchte.
- **Version 0.0.16:** Jeder Konto-Abschnitt hat links neben der Anzahl zwei Symbole zum Umschalten zwischen Vorschau (Kacheln) und Liste. Die Wahl wird pro Benutzer und Konto gespeichert.
- **Version 0.0.17:** In der Listenansicht hat jeder Scan eine Checkbox, dazu „Alle“, „Keine“ und „Ausgewählte löschen (n)“ mit Rückfrage. Gelöscht werden nur Scans, auf die der Benutzer Zugriff hat.
- **Version 0.0.18:** Scans, Vorschaubilder und TIFF-Ansichten liegen verschlüsselt auf dem Laufwerk, mit einem Schlüssel pro Kunde. Zwischenschritte laufen nur im Arbeitsspeicher. Die 25 bestehenden Scans von Kunde 1 sind umgestellt und per Prüfsumme kontrolliert. Alle URLs verwenden zufällige Pseudo-IDs statt Datenbank-IDs. **Backup-Hinweis:** Ohne den `encryption.key` aus der `.env` sind die Scans verloren. Langform: [Entscheidung: Verschlüsselte Ablage und Pseudo-IDs](#)
- **Version 0.0.19: Umbenennung in ScanDock** mit der Domain `scandock.cloud`. Umgestellt sind Code, Datenbank, Pfade, Systembenutzer, Dienste, Zertifikate und

Hostname, Altes ist entfernt. Vorher wurde nach `/root/backup` gesichert. Langform:
Entscheidung: Umbenennung ScanKai → ScanDock

- Umbenennung abgeschlossen: Das GitHub-Repo heißt jetzt Skittel/scandock (Push umgestellt), die Umleitungs-URI in der Entra-App des ersten Kunden ist angepasst, und `ftp.scandock.cloud` ist auch über die öffentlichen Resolver per IPv4 erreichbar.
- **Abschlusstest 0.0.20:** Infrastruktur, FTP, Inhaltsprüfung, Verschlüsselung, Rechte, Admin-Funktionen und Sicherheit sind geprüft, alles ok. Gefunden und behoben: Der Server-Header verrät die Apache-Version (`zz-scandock-security.conf`). Langform: Testprotokoll Abschlusstest 0.0.20
- **Version 0.0.21:** Tägliche Datensicherung um 03:00 Uhr nach `/backup` (Skript `scandock-backup`, Cron). Archiv und Log heißen `yyyymmdd-hhiiss`, das Log endet mit einer Zusammenfassung. Erste Sicherung `20261030-125956` (8,7 MB, 4470 Dateien) mit Status OK. Eine Probe-Wiederherstellung der Datenbank ergab identische Zeilenzahlen.
- **Version 0.0.22:** Es werden die letzten 30 Sicherungen behalten. Ältere werden nur nach einer erfolgreichen Sicherung gelöscht. Neue Seite ToDo mit dem offenen Punkt **externe Datensicherung**.
- **Version 0.0.23:** Neues Admin-Journal (nur für Admins). Es protokolliert Änderungen an Einstellungen und FTP-Konten sowie eingegangene, abgelehnte und gelöschte Scans, ohne Anmeldungen und Downloads. Außerdem lassen sich markierte Scans in der Listenansicht als ZIP herunterladen. Langform: [Entscheidung: Admin-Journal](#)
- **Version 0.0.24:** Journal-Einträge werden ein Jahr aufbewahrt, der tägliche Löschlauf entfernt ältere.
- ChatGPT-Review (Stand 0.0.24) am Code geprüft und ausgewertet. Echte Funde: möglicher Scan-Verlust bei vollem Datenträger, ignorierte Löschfehler, Temp-Datei der PDF-Prüfung auf der Platte, veraltete Gruppen bei Graph-Ausfall, Freigaben per UPN statt Objekt-ID, fehlende automatisierte Tests, falsche Composer-Metadaten. Langform: Auswertung ChatGPT-Review 30.10.26
- **Version 0.0.25:** Review-Punkte 1–4 umgesetzt: kein Datenverlust bei vollem Datenträger, verlässliches Löschen mit Wiederholung, Freigaben per Entra-Objekt-ID, Höchstalter für Gruppen, Temp-Dateien im RAM, Composer-Metadaten. Neu: **Speicherwächter** (unter 10 GB frei wird FTP gestoppt, Balken für alle Benutzer, ab 11 GB automatische Freigabe) und **maximal 50 MB pro Datei**. Details mit Testergebnissen in der Auswertung.
- **Version 0.0.26:** Dateinamen von FTP werden normalisiert: Jedes Zeichen außer a-z, A-Z, 0-9 wird zu `_`. Namen sind maximal 20 Zeichen lang, längere werden auf 16 Zeichen gekürzt und bekommen einen Zähler ab `0000`. Die Endung bleibt und darf höchstens 4 Zeichen haben. Das gilt für Scans, Ablehnungen, Journal und Platzhalter. Die übrigen Review-Punkte werden derzeit nicht benötigt und stehen in der ToDo-Liste.
- **Version 0.0.27:** Dateinamen dürfen jetzt bis zu 30 Zeichen lang sein, längere werden auf 26 Zeichen gekürzt und bekommen den Zähler. Umlaute werden umgeschrieben (ä→ae, ö→oe, ü→ue, Ä→Ae, Ö→Oe, Ü→Ue, ß→ss), auch in zerlegter Form, wie sie von macOS kommt. Beispiel: „Übergabeprotokoll Grundstücksverkauf.pdf“ → `Uebergabeprotokoll_Grundst0000.pdf`.
- **Version 0.0.28:** Neuer CLI-Befehl `scans:normalize-names` zum Umbenennen vorhandener Scans. Bei Kunde 1 war nichts zu tun, alle 3 Scans entsprechen bereits den Regeln.

Festgelegt: Die 30 Zeichen gelten ohne Endung.

- **Version 0.0.29:** Die Grenze von 50 MB setzt jetzt der FTP-Server selbst durch. Er bricht größere Uploads während der Übertragung ab (Fehler 552), der Kopierer meldet dann „Senden fehlgeschlagen“, und es wird nichts gespeichert. Diese Abbrüche meldet `scandock-ftplog` alle 15 Sekunden als abgelehnte Datei (Balken und Journal). Das SQL-Debug-Log von ProFTPD ist abgeschaltet.
- **Festgehalten (Projekthinhaber):** Übliche Scans sind 0,5 bis 5 MB groß, 50 MB ist schon das Zehnfache. ScanDock ist für Kopierer gedacht, **nicht als Plattform zum Dateiaustausch**.
- Projekt-Dokumentation aus dem Wiki ins Repository übernommen (`docs/`, dieses CHANGELOG, `INSTALL.md` – ungetestet). Admin-Adressen in `deploy/fail2ban` durch Platzhalter ersetzt.
- **Version 0.0.30:** Button **Hilfe** oben rechts (links vom Benutzermenü) öffnet die Benutzer-Anleitungen im öffentlichen Support-Wiki (`Config\ScanDock:$helpUrl`). Das Support-Wiki ist neu aufgebaut, nur auf Deutsch, in den Teilen **Benutzer** und **Verwaltung (Admins)**, mit Platzhaltern für Screenshots. Die CLI wird dort nicht beschrieben, sie ist nur für den Betreiber.
- **Version 0.0.31:** Dauerhafter Demo-Kunde „Muster GmbH“ (`demo.scandock.cloud`) mit erfundenen Daten. Er ist nur von den Adressen des Betreibers erreichbar (`scandock.demoAllowedIps` in der `.env`, nicht im Repository) und meldet ohne Microsoft automatisch als Demo-Admin an, `?demo_user=<upn>` wechselt den Benutzer. `scandock demo:seed` setzt die Demo zurück (3 Benutzer, 2 Geräte, 20 Scans, 1 abgelehnte Datei, Journal). Fehler behoben: Die Import-Sperre lag nur im CLI-Befehl, ein direkter Aufruf von `ingestAll()` konnte parallel zum Dateiwächter importieren (doppelte Scans). Die Sperre sitzt jetzt in `ingestAll()` selbst.
- **Version 0.0.32:** Darstellungsfehler, die beim ersten Blick auf die echte Oberfläche (Screenshots mit Playwright) aufgefallen sind: In der Kachelansicht ragte „Löschen“ über den Kachelrand. Das Augen-Symbol beim Passwort erschien durchgestrichen, weil `hidden` auf SVG-Elementen in Chrome nicht wirkt. Das Eingabefeld für Personen und Gruppen war zu schmal. Die Hinweise auf den FTP-Seiten nannten noch „nur PDF“. Das Demo-Logo ist breiter.
- **Version 0.0.33:** Log-Rotation für die ProFTPD-Logs `auth.log`, `tls.log`, `ban.log` und `stor.log` (wöchentlich, 8 Wochen, `copytruncate`, geprüft mit Upload und dem Melde-Dienst nach der Rotation). Das alte SQL-Debug-Log ist entfernt. Der tägliche Löschlauf entfernt Anwendungslogs, die älter als 90 Tage sind.
- **Tagesabschluss 2026-10-30:** Stand 0.0.33. Alle Dienste laufen, keine offenen Fehler im Betrieb (die Log-Einträge des Tages stammen aus Tests und bereits behobenen Fehlern). Datensicherung erstellt.
- **Dokumentation (2026-10-31):** Projektbeschreibung, Entscheidungen und dieses Changelog stehen jetzt im öffentlichen Wiki (Kapitel *Projekt (Technik)*). Das GitHub-Repository verweist darauf und enthält neben dem Code nur noch README und `INSTALL.md`.
- **Dokumentation (2026-10-31):** Neues Kapitel *Installation, Betrieb & Fehlersuche* im öffentlichen Wiki: Installationsanleitung (jetzt auf Deutsch), alle CLI-Befehle und eine neue Seite zur Fehlersuche (Logs, Kopierer-Fehler, Import, Extra-Fehlercodes, Speicherplatz, Zertifikate, Sicherung). `INSTALL.md` ist aus dem Repository entfernt, die README verlinkt

das Wiki.

- **Version 0.0.34:** Kundennamen aus Beispielen im Code entfernt (Hilfetext von `tenant:create`, Kommentare). Grundlage: Regel des Betreibers, dass Namen, Kundeninformationen, Benutzernamen, Kennwörter, Token und IP-Adressen nicht öffentlich sind.

Installation, Betrieb & Fehlersuche

Für Betreiber eines eigenen ScanDock-Servers: Installation, CLI-Befehle, Logs und Fehlersuche. Der Quellcode liegt öffentlich auf [GitHub](#).

Installation (neuer Server)

ScanDock auf einem leeren Ubuntu-Server installieren

⚠ **UNGETESTET.** Diese Anleitung ist aus der Konfiguration des Produktivservers entstanden (Ubuntu 26.04 LTS, ScanDock 0.0.33). Sie wurde noch **nicht** vollständig auf einem neuen Server durchgespielt. Einzelheiten können abweichen.

ScanDock ist für Kopierer und Multifunktionsgeräte gedacht (übliche Scans 0,5–5 MB, Grenze 50 MB). Es ist keine Plattform zum Dateiaustausch.

Der Quellcode und alle hier genannten Konfigurationsdateien liegen öffentlich auf GitHub: <https://github.com/Skittel/scandock> (Ordner `deploy/`). Die Befehle werden als Benutzer mit `sudo` ausgeführt.

Weiter: [Betrieb & CLI-Befehle](#) · [Fehlersuche](#)

0. Voraussetzungen

- Ubuntu 26.04 LTS (PHP 8.5 aus der Distribution; ScanDock braucht PHP ≥ 8.4 mit `sodium` und `intl`), root-Zugang, öffentliche IPv4-Adresse (IPv6 optional).
- Eine Domain mit DNS-Einträgen auf den Server: `example.com` und `*.example.com` (A und, falls vorhanden, AAAA). Kunden erreichen ScanDock unter `<slug>.example.com`, FTP unter `ftp.example.com`.
- Eine E-Mail-Adresse für Let's Encrypt.
- Pro Kunde: ein Microsoft-Entra-Mandant, in dem ein Admin eine App-Registrierung anlegen darf (der Start-Link führt durch die Einrichtung).

In dieser Anleitung ersetzen:

Platzhalter	Bedeutung
<code>example.com</code>	eigene Basis-Domain (Produktivsystem: <code>scandock.cloud</code>)

Platzhalter	Bedeutung
admin@example.com	Kontakt für Let's Encrypt
203.0.113.10	IP-Adressen, die den Server verwalten dürfen (SSH usw.)

1. Pakete

```
sudo apt-get update
sudo apt-get install -y \
    apache2 libapache2-mod-php8.5 \
    php8.5 php8.5-cli php8.5-mysql php8.5-intl php8.5-mbstring php8.5-curl \
    php8.5-xml php8.5-zip php8.5-gd \
    mariadb-server composer git unzip \
    certbot \
    proftpd-core proftpd-mod-mysql \
    poppler-utils qpdf libtiff-tools imagemagick inotify-tools \
    fail2ban ufw
```

2. Systembenutzer und Verzeichnisse

```
sudo groupadd scandock
sudo useradd -r -g scandock -d /srv/scandock -s /usr/sbin/nologin scandock
sudo usermod -aG scandock www-data

sudo mkdir -p /srv/scandock/incoming /srv/scandock/storage /var/www/letsencrypt/.well-known/acme-challenge /backup
sudo chown scandock:scandock /srv/scandock/incoming && sudo chmod 2770 /srv/scandock/incoming
sudo chown www-data:www-data /srv/scandock/storage && sudo chmod 0750 /srv/scandock/storage
sudo chmod 0755 /srv/scandock
sudo chmod 0700 /backup

id scandock    # uid und gid notieren, sie werden für ProFTPD gebraucht (Schritt 8)
```

3. Code

```
sudo mkdir -p /var/www/scandock && sudo chown "$USER":www-data /var/www/scandock
git clone https://github.com/Skittel/scandock.git /var/www/scandock
cd /var/www/scandock
composer install --no-dev --optimize-autoloader
sudo chown -R www-data:www-data writable
sudo find writable -type d -exec chmod 2775 {} + ; sudo find writable -type f -exec chmod 664 {} +
```

Domain anpassen

Die Produktiv-Domain `scandock.cloud` steht in diesen Dateien und muss durch die eigene Domain ersetzt werden:

```
grep -rln 'scandock\.cloud' app/Config deploy
# app/Config/ScanDock.php, deploy/apache/000-redirect-http.conf,
# deploy/apparmor/local-proftpd, deploy/proftpd/proftpd.conf, deploy/sbin/scandock-site
```

In `app/Config/ScanDock.php` außerdem prüfen: `letsEncryptEmail`, `operatorLogo`, `operatorName`, `operatorUrl`, `helpUrl` und die Grenzen (`maxUploadBytes`, `minFreeBytes`, `defaultRetentionDays`). In `deploy/sbin/scandock-site` `EMAIL` setzen, in `deploy/fail2ban/scandock.conf` `ADMIN_IPS_HERE` durch die eigenen Admin-Adressen ersetzen.

4. Datenbank

```
APP_PW=$(openssl rand -base64 30 | tr -d '/+=' | cut -c1-32)
FTP_PW=$(openssl rand -base64 30 | tr -d '/+=' | cut -c1-32)
sudo mariadb <<SQL
CREATE DATABASE scandock CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
CREATE USER 'scandock'@'localhost' IDENTIFIED BY '$APP_PW';
GRANT ALL PRIVILEGES ON scandock.* TO 'scandock'@'localhost';
CREATE USER 'scandock_ftp'@'127.0.0.1' IDENTIFIED BY '$FTP_PW';
FLUSH PRIVILEGES;
SQL
sudo install -d -m 700 /root/.secrets
printf 'DB_APP_USER=scandock\nDB_APP_PASS=%s\nDB_FTP_USER=scandock_ftp\nDB_FTP_PASS=%s\n'
"$APP_PW" "$FTP_PW" \
    | sudo tee /root/.secrets/scandock-db.env >/dev/null
sudo chmod 600 /root/.secrets/scandock-db.env
```

ProFTPD verbindet sich per TCP mit `127.0.0.1` (ein Unix-Socket funktioniert nach dem chroot nicht), deshalb wird der FTP-Datenbankbenutzer für `127.0.0.1` angelegt.

5. Anwendungskonfiguration (`.env`)

```
cd /var/www/scandock
KEY=$(php -r 'echo "hex2bin:".bin2hex(random_bytes(32));')
cat > .env <<EOF
CI_ENVIRONMENT = production

app.baseURL = 'https://example.com/'
app.forceGlobalSecureRequests = true

database.default.hostname = localhost
database.default.database = scandock
database.default.username = scandock
database.default.password = $APP_PW
database.default.DBDriver = MySQLi
database.default.charset = utf8mb4
database.default.DBCollat = utf8mb4_unicode_ci

encryption.key = $KEY

session.driver = 'CodeIgniter\Session\Handlers\FileHandler'
session.cookieName = 'scandock_session'
session.expiration = 28800
cookie.secure = true
cookie.httponly = true
cookie.samesite = 'Lax'
EOF
chmod 640 .env && sudo chgrp www-data .env
```

“ Der `encryption.key` schützt alle gespeicherten Scans (der Dateischlüssel jedes Kunden ist damit verschlüsselt). Ohne ihn lassen sich die Scans nicht mehr entschlüsseln. Eine Kopie gehört außerhalb des Servers, z. B. in einen Passwort-Manager.

Schema anlegen und dem FTP-Benutzer Lesezugriff auf seine View geben:

```
sudo -u www-data php spark migrate
sudo mariadb -e "GRANT SELECT ON scandock.ftp_users TO 'scandock_ftp'@'127.0.0.1'; FLUSH
PRIVILEGES;"
```

6. Apache und PHP

```
D=/var/www/scandock/deploy
sudo a2enmod rewrite ssl headers
sudo a2dissite 000-default
sudo install -m 644 $D/apache/000-redirect-http.conf /etc/apache2/sites-available/
sudo install -m 644 $D/apache/zz-scandock-security.conf /etc/apache2/conf-available/
sudo a2ensite 000-redirect-http && sudo a2enconf zz-scandock-security
sudo install -m 644 $D/apache/php-99-scandock.ini /etc/php/8.5/apache2/conf.d/99-scandock.ini
sudo install -m 644 $D/apache/php-99-scandock.ini /etc/php/8.5/cli/conf.d/99-scandock.ini
sudo systemctl restart apache2
```

Port 80 beantwortet nur Let's-Encrypt-Anfragen und leitet alles andere auf HTTPS um. Jeder Hostname bekommt einen eigenen HTTPS-vHost (nächster Schritt). Die Sicherheitskonfiguration heißt `zz-...`, damit sie nach Ubuntu's `security.conf` geladen wird.

7. Hilfsskripte, CLI und Zertifikate

```
sudo install -m 755 $D/sbin/scandock-site /usr/local/sbin/
sudo install -m 755 $D/sbin/scandock /usr/local/bin/          # CLI-Wrapper: startet spark als
www-data
sudo install -m 440 $D/sudoers/scandock /etc/sudoers.d/ && sudo visudo -cf
/etc/sudoers.d/scandock
sudo install -m 755 $D/letsencrypt/scandock-reload.sh /etc/letsencrypt/renewal-hooks/deploy/

# Startseite (Basis-Domain + www) und FTP-Zertifikat
sudo /usr/local/sbin/scandock-site add example.com
sudo /usr/local/sbin/scandock-site add www.example.com
sudo certbot certonly --webroot -w /var/www/letsencrypt -d ftp.example.com \
--email admin@example.com --agree-tos --no-eff-email -n
```

`scandock-site` legt vHost und Zertifikat für einen Hostnamen an; Kunden-Hostnamen legt `scandock tenant:create` automatisch an. Der Benutzer `www-data` darf genau dieses Skript per `sudo`

ausführen.

8. FTP-Server (ProFTPD)

```
source <(sudo cat /root/.secrets/scandock-db.env)
sudo cp /etc/proftpd/proftpd.conf /etc/proftpd/proftpd.conf.dist
sed "s/CHANGE_ME_PASSWORD/$DB_FTP_PASS/" $D/proftpd/proftpd.conf | sudo tee
/etc/proftpd/proftpd.conf >/dev/null
sudo chmod 600 /etc/proftpd/proftpd.conf
```

In `/etc/proftpd/proftpd.conf` in beiden `SQLNamedQuery`-Zeilen `999, 1001` durch uid und gid des Benutzers `scandock` ersetzen (Schritt 2).

Ubuntu schränkt ProFTPD und qpdf mit AppArmor ein; ScanDock braucht ein paar zusätzliche Regeln:

```
sudo install -m 644 $D/apparmor/local-proftpd /etc/apparmor.d/local/proftpd
sudo install -m 644 $D/apparmor/local-qpdf /etc/apparmor.d/local/qpdf
sudo apparmor_parser -r /etc/apparmor.d/proftpd /etc/apparmor.d/qpdf
sudo proftpd -t && sudo systemctl restart proftpd
```

Was die Konfiguration macht: virtuelle Benutzer aus der Datenbank-View, nur Hochladen (kein Auflisten von Inhalten, kein Herunterladen, Umbenennen oder Löschen), FTP und explizites FTPS auf Port 21, implizites FTPS auf Port 990, passive Ports 40000-40100, höchstens 50 MB pro Datei, Schutz gegen Passwort-Raten (`mod_ban`) und ein Upload-Protokoll für abgebrochene Uploads.

9. Hintergrunddienste

```
sudo install -m 755 $D/sbin/scandock-upload-watch $D/sbin/scandock-diskguard \
    $D/sbin/scandock-ftplog $D/sbin/scandock-backup /usr/local/sbin/
sudo install -m 644 $D/systemd/scandock-* /etc/systemd/system/
sudo systemctl daemon-reload
sudo systemctl enable --now scandock-upload-watch.service \
    scandock-ingest.timer scandock-purge.timer scandock-diskguard.timer scandock-ftplog.timer
sudo install -m 644 $D/cron/scandock-backup /etc/cron.d/scandock-backup
sudo install -m 644 $D/fail2ban/scandock.conf /etc/fail2ban/jail.d/ && sudo systemctl restart
fail2ban
sudo install -m 644 $D/logrotate/scandock-proftpd /etc/logrotate.d/scandock-proftpd
```

Dienst	Zweck
<code>scandock-upload-watch</code>	importiert einen Upload etwa 1 s nach dem Ende der Übertragung (inotify)
<code>scandock-ingest.timer</code>	Rückfallebene: Import alle 20 s
<code>scandock-purge.timer</code>	täglich 03:15: Aufbewahrungsfrist, fehlgeschlagene Löschungen, verwaiste Dateien, alte Journal-Einträge, Anwendungslogs älter als 90 Tage
<code>scandock-diskguard.timer</code>	jede Minute: unter 10 GB frei → FTP stoppen, Hinweis für alle Benutzer; ab 11 GB → wieder freigeben
<code>scandock-ftplog.timer</code>	alle 15 s: meldet Uploads, die der FTP-Server abgebrochen hat (über 50 MB)
cron <code>scandock-backup</code>	täglich 03:00: Datensicherung nach <code>/backup</code> , die letzten 30 bleiben

10. Firewall

```

sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw allow from 203.0.113.10          # Admin-Zugang (je Adresse/Netz wiederholen)
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp
sudo ufw allow 21/tcp
sudo ufw allow 990/tcp
sudo ufw allow 40000:40100/tcp
sudo ufw enable

```

Vor dem Einschalten sicherstellen, dass die eigene SSH-Verbindung von einer erlaubten Adresse kommt.

11. Erster Kunde

```
scandock tenant:create <slug> --name "Firmenname"
```

Das stellt das Zertifikat aus, legt den vHost an und gibt einen **Start-Link** aus. Der Entra-Admin des Kunden öffnet ihn und folgt dem Assistenten (App-Registrierung, Umleitungs-URI, Clientschlüssel, Berechtigungen). Nach der ersten erfolgreichen Anmeldung wird der Link ungültig. Danach legt ein Admin in der Weboberfläche FTP-Konten an und trägt Host, Port, Benutzername und Passwort im Kopierer ein (siehe Kapitel *Verwaltung (Admins)*).

Weitere Befehle: [Betrieb & CLI-Befehle](#) oder `scandock list` (Gruppe ScanDock).

12. Prüfen

```
systemctl is-active apache2 proftpd mariadb fail2ban scandock-upload-watch \  
    scandock-ingest.timer scandock-purge.timer scandock-diskguard.timer scandock-ftplog.timer  
sudo certbot renew --dry-run  
curl -I https://example.com/  
sudo /usr/local/sbin/scandock-backup && sudo ls /backup
```

Eine kleine PDF mit den Zugangsdaten eines FTP-Kontos hochladen; sie sollte nach wenigen Sekunden auf der Scan-Seite erscheinen. Wenn nicht: [Fehlersuche](#).

13. Aktualisieren

```
cd /var/www/scandock  
git pull  
composer install --no-dev --optimize-autoloader  
sudo -u www-data php spark migrate
```

`deploy/` mit den installierten Kopien vergleichen und geänderte Dateien neu installieren (danach `daemon-reload` bzw. den betroffenen Dienst neu starten).

14. Aus einer Datensicherung wiederherstellen (Kurzform)

1. Pakete, Benutzer und Verzeichnisse wie oben einrichten.
2. Archiv nach `/` entpacken (enthält Code mit `.env`, Scans, Konfiguration, Zertifikate, Zugangsdaten).
3. `sudo mariadb < database.sql` und `sudo mariadb < database-users.sql` (beide im Archiv).
4. `sudo apparmor_parser -r /etc/apparmor.d/proftpd /etc/apparmor.d/qpdf`, `sudo systemctl daemon-reload`, Dienste aktivieren (Schritt 9), Apache und ProFTPD neu starten.

Betrieb & CLI-Befehle

Betrieb & CLI-Befehle

Für Betreiber eines ScanDock-Servers. Die CLI erreicht nur, wer per SSH auf dem Server arbeitet; Kunden bedienen ScanDock ausschließlich über die Weboberfläche.

Siehe auch: [Installation](#) · [Fehlersuche](#)

Alle Befehle per SSH auf dem Server ausführen. `scandock` ist ein Wrapper, der `php spark` als Benutzer `www-data` startet (`/usr/local/bin/scandock`).

Kunden

Befehl	Zweck
<code>scandock tenant:create <slug> --name "Firma"</code>	Legt einen Kunden an: Let's-Encrypt-Zertifikat, Apache-vHost, Datenbankeintrag. Gibt den Start-Link aus.
<code>scandock tenant:link <slug></code>	Zeigt den aktuellen Start-Link an.
<code>scandock tenant:link-renew <slug></code>	Erzeugt einen neuen Start-Link, der alte wird ungültig. Bei aktiven Kunden laufen Anmeldung und FTP weiter, z. B. zum Erneuern eines abgelaufenen Clientschlüssels.
<code>scandock tenant:list</code>	Übersicht aller Kunden: Status, Benutzer, FTP-Konten, Scans, Aufbewahrung, Ablauf des Clientschlüssels (gelb: ≤ 30 Tage, rot: abgelaufen).
<code>scandock tenant:rename <slug> "Firmenname"</code>	Ändert den Anzeigenamen (Firmenname) eines Kunden. Kunden-Admins können ihn auch selbst unter <i>Einstellungen</i> → <i>Firma</i> ändern.
<code>scandock tenant:status <slug> disable</code>	Sperrt einen Kunden (Weboberfläche und FTP).
<code>scandock tenant:status <slug> enable</code>	Entsperrt einen Kunden.

Regeln für Slugs: `a-z`, `0-9`, `-`, max. 63 Zeichen. Gesperrt sind u. a. `www`, `ftp`, `admin`, `api`, `mail`, `setup`, `test`.

Der Start-Link wird ungültig, sobald sich jemand darüber erfolgreich mit Entra angemeldet hat.

Scans

Befehl	Zweck
<code>scandock scans:ingest</code>	Importiert fertige FTP-Uploads. Läuft automatisch direkt nach jedem Upload (Dienst <code>scandock-upload-watch</code>), zusätzlich alle 20 Sekunden als Rückfallebene (<code>scandock-ingest.timer</code>).
<code>scandock scans:encrypt</code>	Verschlüsselt Scans, die noch unverschlüsselt gespeichert sind (Umstellung auf 0.0.18). Prüft jede Datei per Prüfsumme, bevor das Original gelöscht wird. Wirkt auf alle Kunden.
<code>scandock scans:normalize-names --tenant <slug> [--dry-run]</code>	Benennt vorhandene Scans nach den Dateinamen-Regeln um (Umlaute, nur a-z/A-Z/0-9, max. 30 Zeichen). Jede Umbenennung steht im Journal.
<code>scandock scans:ftp-rejected <ftp-benutzer> <bytes> <dateiname></code>	Trägt einen vom FTP-Server abgebrochenen Upload als abgelehnte Datei ein (Balken und Journal). Wird von <code>scandock-ftplog</code> aufgerufen, nicht von Hand nötig.
<code>scandock scans:purge</code>	Löscht Scans nach Ablauf der Aufbewahrungsfrist. Läuft täglich um 03:15 Uhr (<code>scandock-purge.timer</code>).

System

Befehl	Zweck
<code>scandock system:receive-block on off <freie GB></code>	Trägt Sperre bzw. Freigabe des Empfangs ins Journal aller Kunden ein. Wird vom Speicherwächter aufgerufen, nicht von Hand nötig.

Datenbank

Befehl	Zweck
<code>scandock migrate</code>	Spielt neue Datenbank-Migrationen ein (nach einem Update).
<code>scandock migrate:status</code>	Zeigt den Stand der Migrationen.

Server (root)

Befehl	Zweck
<code>sudo /usr/local/sbin/scandock-site add <host></code>	vHost und Zertifikat für einen Hostnamen anlegen (wird von <code>tenant:create</code> aufgerufen).

Befehl	Zweck
<code>sudo /usr/local/sbin/scandock-site remove <host></code>	vHost und Zertifikat entfernen.
<code>systemctl list-timers 'scandock-*'</code>	Status der Timer.
<code>journalctl -u scandock-ingest -n 50</code>	Log des Imports.
<code>journalctl -t scandock-ftplog</code> / <code>sudo tail /var/log/proftpd/stor.log</code>	Upload-Protokoll des FTP-Servers. Abbrüche wegen mehr als 50 MB (Code 552) meldet <code>scandock-ftplog</code> alle 15 s an ScanDock.
<code>journalctl -t scandock-diskguard</code>	Log des Speicherwächters (Sperrung/Freigabe des FTP-Empfangs).
<code>cat /run/scandock/ftp-blocked</code>	Existiert, solange der Empfang wegen Speichermangel gesperrt ist.
<code>sudo /usr/local/sbin/scandock-diskguard</code>	Speicherwächter sofort ausführen (läuft sonst jede Minute; Sperrung unter 10 GB, Freigabe ab 11 GB).
<code>systemctl status scandock-upload-watch</code>	Status des Dateiwächters, der den Import sofort startet.
<code>sudo tail -f /var/log/proftpd/proftpd.log</code>	FTP-Log (Anmeldungen, Fehler).
<code>sudo fail2ban-client status proftpd</code>	Gesperrte IPs (FTP).
<code>sudo fail2ban-client set proftpd unbanip <ip></code>	IP entsperren.

Datensicherung

Befehl / Ort	Zweck
<code>sudo /usr/local/sbin/scandock-backup</code>	Sicherung sofort ausführen
<code>/etc/cron.d/scandock-backup</code>	automatisch täglich um 03:00 Uhr
Aufbewahrung	die letzten 30 Sicherungen; ältere werden nach einer erfolgreichen Sicherung gelöscht
<code>/backup/<yyyymmdd-hhiiss>.tgz</code>	Archiv: Datenbank-Dump inkl. DB-Benutzer, Scans (verschlüsselt), Projekt inkl. <code>.env</code> (Schlüssel!), Server-Konfiguration, Zertifikate, Zugangsdaten
<code>/backup/<yyyymmdd-hhiiss>.log</code>	Protokoll aller Schritte mit Zusammenfassung (Status OK/FEHLER, Größe, Anzahl Dateien, Scans, Dauer, freier Platz, SHA-256)
<code>sudo tail -12 /backup/\$(sudo ls /backup grep log\$ tail -1)</code>	Zusammenfassung der letzten Sicherung

Wiederherstellen (Kurzform): Archiv nach `/` entpacken, `mariadb < database.sql`, `mariadb < database-users.sql`, Dienste neu starten. Ohne die `.env` aus dem Archiv lassen sich die Scans nicht entschlüsseln. Archiv und Schlüssel gehören zusammen und müssen entsprechend geschützt werden.

Demo-Kunde und Screenshots

Befehl / Ort	Zweck
<code>https://<demo-slug>.<domain></code>	Demo-Kunde „Muster GmbH“ mit erfundenen Daten (Slug: <code>Config\ScanDock::\$demoSlug</code>). Nur von den Adressen in <code>scandock.demoAllowedIps</code> (<code>.env</code>) erreichbar, automatische Anmeldung als Demo-Admin, <code>?demo_user=<upn></code> wechselt den Benutzer (<code>bernd.beispiel@...</code> = normaler Benutzer, <code>clara.chef@...</code> = Geschäftsführung).
<code>scandock demo:seed</code>	Setzt den Demo-Kunden zurück und befüllt ihn neu.
<code>resources/demo/</code>	Demo-PDFs (<code>mkdemo.py</code>), Demo-Logo, Screenshot-Skript <code>screenshots.py</code> (Playwright in <code>/opt/scandock-tools</code>).

Fehlersuche

Fehlersuche

Für Betreiber eines ScanDock-Servers. Die meisten Prüfungen brauchen SSH-Zugang. Probleme, die Admins eines Kunden selbst lösen können, stehen unter *Verwaltung (Admins)* → *Häufige Fragen*.

Siehe auch: [Installation](#) · [Betrieb & CLI-Befehle](#)

Wo stehen die Logs?

Log	Inhalt
<code>/var/www/scandock/writable/logs/log-<datum>.log</code>	Anwendung: Import, Prüfung, Anmeldung, Fehler (90 Tage)
<code>journalctl -u scandock-ingest</code> / <code>journalctl -u scandock-upload-watch</code>	Import nach dem Upload
<code>/var/log/proftpd/proftpd.log</code>	FTP: Verbindungen, Fehler
<code>/var/log/proftpd/auth.log</code>	FTP: Anmeldungen
<code>/var/log/proftpd/tls.log</code>	FTPS: TLS-Aushandlung
<code>/var/log/proftpd/stor.log</code>	FTP: Uploads mit Ergebnis (552 = zu groß abgebrochen)
<code>/var/log/proftpd/ban.log</code>	FTP: Sperren durch mod_ban
<code>journalctl -t scandock-diskguard</code> / <code>journalctl -t scandock-ftplog</code>	Speicherwächter, Meldung abgebrochener Uploads
<code>/var/log/apache2/</code>	Weboberfläche
<code>/backup/<zeitstempel>.log</code>	Datensicherung mit Zusammenfassung

Schnellcheck aller Dienste:

```
systemctl is-active apache2 proftpd mariadb fail2ban scandock-upload-watch \  
scandock-ingest.timer scandock-purge.timer scandock-diskguard.timer scandock-ftplog.timer
```

Kopierer: „Senden fehlgeschlagen“

1. **Zugangsdaten:** In der Weboberfläche prüfen, ob das FTP-Konto existiert und aktiv ist; ggf. „Neues Passwort“ und im Kopierer neu eintragen. In `/var/log/proftpd/auth.log` steht, ob die Anmeldung ankommt und abgelehnt wird.
2. **Gesperrte IP:** Nach 3 Fehlversuchen in 10 Minuten sperrt ProFTPD (`mod_ban`) die Adresse für 1 Stunde; fail2ban sperrt nach 5 Fehlversuchen in 10 Minuten für 1 Stunde.

```
sudo fail2ban-client status proftpd
sudo fail2ban-client set proftpd unbanip <ip>
sudo tail /var/log/proftpd/ban.log      # Sperren durch mod_ban (laufen nach 1 Stunde
ab)
```

3. **Passiver Modus:** Der Kopierer muss passives FTP nutzen; die Ports 40000–40100 müssen in der Firewall offen sein (`sudo ufw status`). Typisches Bild: Anmeldung klappt, Übertragung hängt.
4. **FTPS:** Port 21 = FTP oder explizites FTPS, Port 990 = implizites FTPS (dort ist TLS Pflicht). Ältere Kopierer können manchmal nur TLS 1.0/1.1 – ScanDock erlaubt nur TLS 1.2 und 1.3. Fehler stehen in `/var/log/proftpd/tls.log`. Zertifikat prüfen: `sudo certbot certificates`.
5. **Datei zu groß:** Über 50 MB bricht der FTP-Server die Übertragung ab (Code 552). Die Datei erscheint als abgelehnt mit Grund im Konto. Abhilfe am Kopierer: geringere Auflösung, Graustufen oder Schwarz-Weiß, Dokument aufteilen.
6. **Empfang gesperrt:** Bei weniger als 10 GB freiem Speicher ist der FTP-Server gestoppt, alle Benutzer sehen einen Hinweis. Siehe Abschnitt *Speicherplatz* weiter unten.

Upload klappt, aber der Scan erscheint nicht

1. **Abgelehnt?** Abgelehnte Dateien erscheinen eine Stunde lang mit Grund als Balken im Konto und dauerhaft im Journal. Gründe: falsche Endung (erlaubt: PDF, JPG/JPEG, PNG, TIFF), Inhalt passt nicht zur Endung, HTML-/Skript-Code oder aktive PDF-Inhalte (JavaScript, Programmstart, eingebettete Dateien, XFA-Formulare usw.), über 50 MB.
2. **Import läuft?**

```
systemctl status scandock-upload-watch
journalctl -u scandock-ingest -n 50
scandock scans:ingest          # Import sofort von Hand
```

3. **Noch in Übertragung:** Während des Uploads heißt die Datei `.in.<name>.` (HiddenStores) und wird nicht importiert. Bleibt sie liegen, wurde die Übertragung abgebrochen.
4. **Sichtbarkeit:** Bei einem *privaten* FTP-Konto sehen nur zugeordnete Personen und Gruppen die Scans – auch Admins nur, wenn sie zugeordnet sind.

Anmeldung mit Microsoft schlägt fehl

ScanDock zeigt die Meldung von Entra mit Code an. Häufige Codes:

Code	Bedeutung	Abhilfe
AADSTS7000222	Clientschlüssel abgelaufen	ein Admin des Kunden erstellt in Entra einen neuen Schlüssel und trägt ihn unter <i>Einstellungen</i> → <i>Clientschlüssel</i> ein; kann sich kein Admin mehr anmelden: <code>scandock tenant:link-renew <slug></code> und den neuen Start-Link schicken (FTP läuft weiter)
AADSTS7000215	Clientschlüssel ungültig	den Wert des Schlüssels eintragen, nicht die Geheimnis-ID
AADSTS700016	Anwendungs-ID nicht gefunden	Client-ID oder Mandant falsch eingetragen
AADSTS90002 / AADSTS900023	Mandant nicht gefunden / ungültig	Verzeichnis-ID (Mandant) prüfen
AADSTS50011	Umleitungs-URI passt nicht	in der App-Registrierung <code>https://<slug>.<domain>/auth/callback</code> eintragen (genau wie im Assistenten angezeigt)

Den Ablauf der Clientschlüssel aller Kunden zeigt `scandock tenant:list` (gelb: ≤ 30 Tage, rot: abgelaufen); Admins sehen vor dem Ablauf einen Hinweis mit Link zum Erneuern.

Ist ein Kunde gesperrt (`scandock tenant:status <slug> disable`), funktionieren weder Anmeldung noch FTP.

Hinweis „Gruppenmitgliedschaften konnten nicht aktualisiert werden“

ScanDock liest Gruppen über Microsoft Graph und gleicht sie alle 5 Minuten ab. Gruppen, die älter als 1 Stunde sind, geben keine Rechte mehr. Ursachen: Graph nicht erreichbar, Anwendungsberechtigungen (`User.Read.All`, `Group.ReadBasic.All`) ohne Administratorzustimmung oder Clientschlüssel abgelaufen. Details im Anwendungslog.

Hinweis „Es ist keine Admin-Gruppe festgelegt“

Solange keine Admin-Gruppe gesetzt ist, sind alle angemeldeten Benutzer Admin. Ein Admin trägt unter *Einstellungen* eine Entra-Gruppe ein.

Speicherplatz

```
df -h /srv/scandock
journalctl -t scandock-diskguard -n 20
ls -l /run/scandock/ftp-blocked      # existiert, solange der Empfang gesperrt ist
```

Unter 10 GB frei stoppt der Speicherwächter den FTP-Server, ab 11 GB gibt er ihn automatisch wieder frei (Prüfung jede Minute, sofort: `sudo /usr/local/sbin/scandock-diskguard`). Platz schaffen: alte Sicherungen in `/backup`, Aufbewahrungsfrist der Kunden prüfen (`scandock tenant:list`), Logs.

Zertifikate

```
sudo certbot certificates
sudo certbot renew --dry-run
```

Port 80 muss für Let's Encrypt erreichbar sein. Nach einer Erneuerung lädt der Hook `scandock-reload.sh` Apache und ProFTPD neu.

Demo-Kunde zeigt „403“

Der Demo-Kunde ist nur von den Adressen in `scandock.demoAllowedIps` (`.env`) erreichbar. Eigene Adresse ergänzen (IPv4, IPv6 oder CIDR, kommasetrennt).

Datensicherung fehlgeschlagen

```
sudo tail -12 /backup/$(sudo ls /backup | grep 'log$' | tail -1)
```

Die Zusammenfassung zeigt Status, Größe und Fehler. Bei Fehlern werden keine alten Sicherungen gelöscht. Ohne den `encryption.key` aus der `.env` lassen sich gesicherte Scans nicht entschlüsseln.