

Discovery-Collector – Inventarisierung an entfernten Standorten

Inventarisierung an entfernten Standorten – einrichten, betreiben, aktualisieren

Produktversion 2026.10.03 · Handbuch-Revision 2.1

Stand 03.10.2026 · Plattform .NET 10 / Windows Server

ID-24a Collector

Discovery-Collector – Inventarisierung an entfernten Standorten

Die Scans des Moduls Discovery (ID-24) laufen auf dem Ordavis-Server. Ihre Reichweite endet deshalb an der ersten Netzgrenze: Eine Außenstelle, ein abgeschottetes Produktionsnetz oder das Netz eines betreuten Kunden ist von dort nicht erreichbar.

Der **Discovery-Collector** schließt diese Lücke. Er ist ein kleiner Windows-Dienst, den Sie auf einem Rechner **im** fremden Netz installieren. Er durchsucht die Netzbereiche, die Sie ihm in der Zentrale zuweisen, und meldet seine Funde zurück. Dieses Dokument beschreibt den Collector vollständig: vom Anlegen über Installation und Zugänge bis zu Betrieb, Aktualisierung und Fehlersuche.

INHALT

1 Was der Collector ist

2 Voraussetzungen

2.1 Rechte und vorbelegte Rollen

3 Schritt 1: Einen Collector anlegen

4 Schritt 2: Den Collector am Standort installieren

5 Schritt 3: Prüfen, ob er sich angemeldet hat

6 Erhebungswege schalten und Zugänge hinterlegen

6.1 WinRM und SNMP in der Zentrale schalten

6.2 Scan-Konto und Kennwort ändern

6.3 SNMP-Zugang hinterlegen (v2c oder v3)

6.4 Was die Zielrechner brauchen

7 Was ein Lauf tut

8 Das Client-Inventar: Funde prüfen und übernehmen

8.1 Übernehmen

8.2 Verwerfen und wieder öffnen

9 Betrieb und Überwachung

10 Die Konfigurationsdatei appsettings.json

11 Dateien, Dienste und Protokolle

12 Aktualisieren und entfernen

13 Fehlerbehebung

14 Beispiele aus der Praxis

14.1 Beispiel: Den Bauhof einbinden

14.2 Beispiel: Switches per SNMPv3 erfassen

14.3 Beispiel: Den Standort-Rechner austauschen

14.4 Beispiel: Einen Rechner aus dem Bauhof übernehmen

14.5 Beispiel: Einen gesperrten Collector wieder zulassen

15 Häufige Fragen

Verwandte Themen

1 Was der Collector ist

Die **Verbindung geht immer vom Standort aus**. Der Collector ruft in der Zentrale an, nie umgekehrt. Am Standort ist deshalb **keine eingehende Freigabe** nötig; ein Standort hinter einem NAT-Router funktioniert genauso wie einer mit fester Adresse.

Er **entscheidet nichts selbst**. Alle fünf Minuten holt er seinen Auftrag in der Zentrale ab: welche Netzbereiche, wie oft, welche Wege. Ist ein Lauf fällig, führt er ihn aus und meldet das Ergebnis. Die Zugänge für die Zielrechner – Windows-Konto, SNMP-Gemeinschaft – bleiben dagegen **am Standort**; die Zentrale erfährt sie nie.

Seine **Funde sind Beobachtungen, keine CIs**. Sie landen im **Client-Inventar** zur Prüfung und werden erst durch **Übernehmen** zu Configuration Items (Abschnitt 8).

	Discovery-Scan und Netzsonde (ID-24)	Discovery-Collector
läuft	im Serverdienst der Zentrale	als eigener Dienst am Standort
erreicht	Netze, die der Server erreicht	das Netz, in dem der Collector steht
Zugänge	aus dem Anmeldedaten-Tresor der Zentrale	lokal am Standort, DPAPI-geschützt
Ergebnis	Kandidaten im <i>Scan-Abgleich</i>	Funde im <i>Client-Inventar</i>
Wege	WinRM, SSH, SNMP, LDAP	Ping mit DNS und ARP, WinRM, SNMP

Abbildung 1 zeigt die Einrichtung im Überblick.

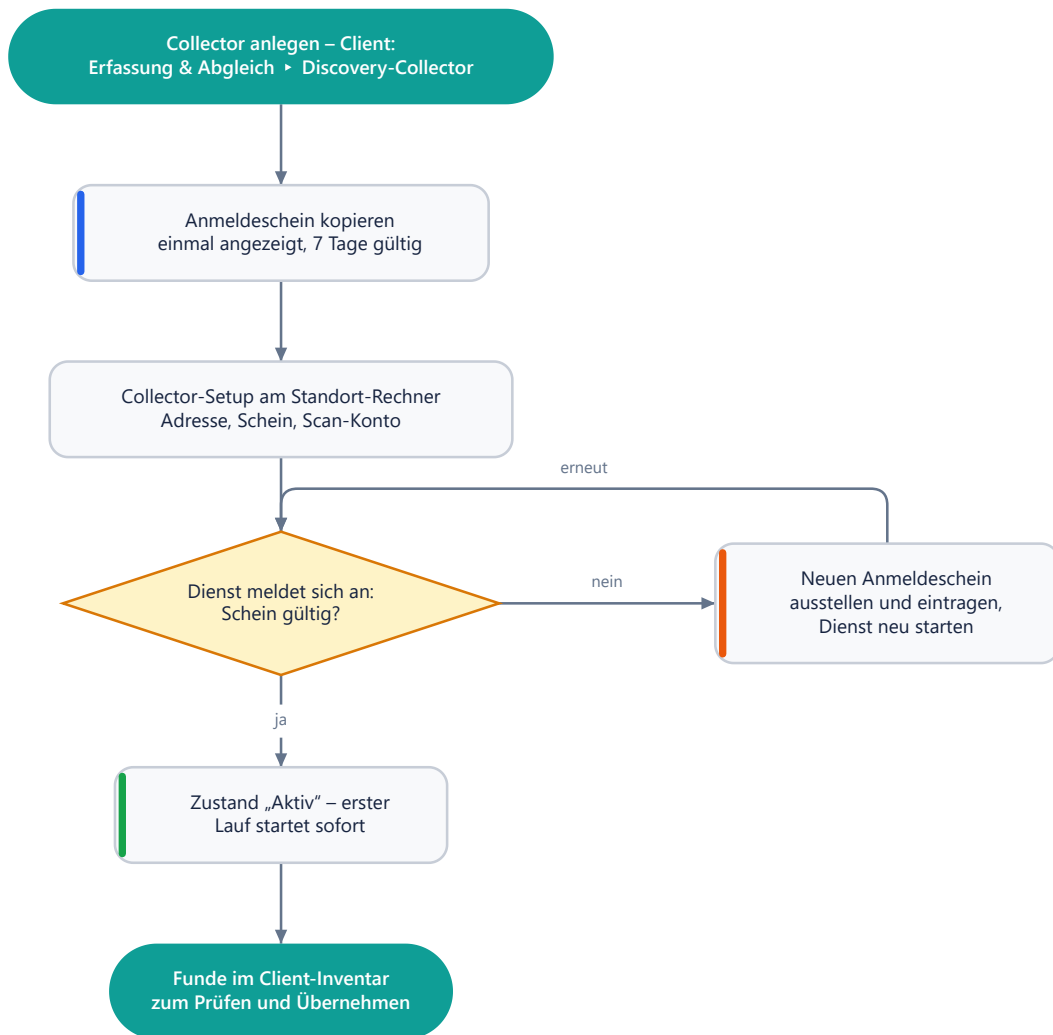


Abb. 1 – Einen Collector einrichten. Der Seitenweg ist nötig, wenn der Anmeldeschein abgelaufen, schon eingelöst oder vertippt ist.

2 Voraussetzungen

Was	Anforderung
Standort-Rechner	Windows 10 ab 1809 oder Windows Server 2019 und neuer, 64 Bit (x64) , dauerhaft eingeschaltet. Eine .NET-Laufzeit ist nicht nötig.
Rechte für die Installation	lokaler Administrator (der Collector wird als Dienst eingerichtet).
Verbindung zur Zentrale	ausgehendes HTTPS zur Ordvis-Schnittstelle – dieselbe Adresse wie für die Clients, mit dem Port aus dieser Adresse. Ein eigener Proxy-Schalter existiert nicht.
Verbindungen ins Zielnetz	ICMP-Echo (Ping) in alle zugewiesenen Bereiche; DNS über den Resolver des Rechners; TCP 5985 (WinRM über HTTP) zu Windows-Rechnern; UDP 161 (SNMP) zu Netzgeräten.
PowerShell	Windows PowerShell 5.1 auf dem Standort-Rechner (für die WinRM-Erhebung).
Scan-Konto (optional)	ein Windows-Konto, das sich per PowerShell-Remoting an den Zielrechnern anmelden darf (Abschnitt 6.4).
Recht in Ordvis	<code>discovery.collector.manage</code> zum Anlegen und Verwalten; <code>discovery.read</code> zum Ansehen.

Wichtig: Ein Rechner trägt genau **einen** Collector, und ein Collector gehört zu genau **einem** Mandanten. Für einen zweiten Mandanten brauchen Sie einen zweiten Rechner.

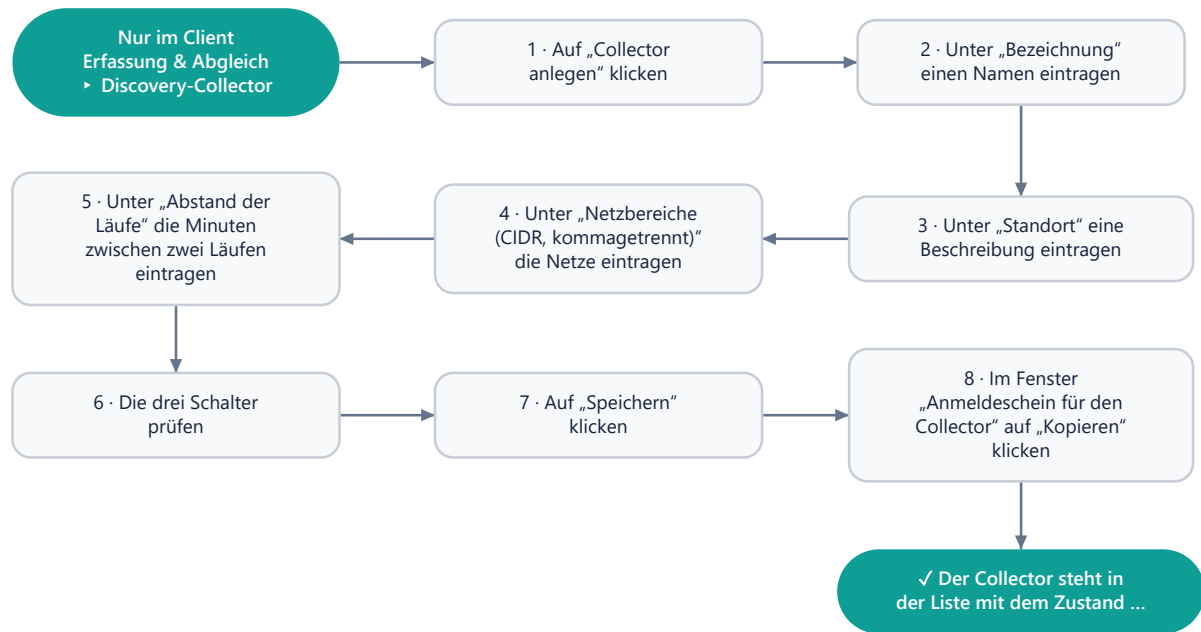
2.1 Rechte und vorbelegte Rollen

Recht	Erlaubt
<code>discovery.read</code>	die Menüpunkte <i>Discovery-Collector</i> und <i>Client-Inventar</i> sehen, Liste und Funde lesen
<code>discovery.collector.manage</code>	Collector anlegen, bearbeiten, Anmeldeschein ausstellen, sperren, entsperren, löschen
<code>discovery.result.review</code>	Funde übernehmen, verwerfen und wieder öffnen
<code>discovery.collector.report</code>	trägt nur der Zugang des Collectors selbst; lässt sich nicht von Hand vergeben

Vorbelegt haben *System Administrator* und *IT-Administrator* alle Rechte, der *Netzwerk-Administrator* `discovery.read`, `discovery.manage`, `discovery.collector.manage` und `discovery.result.review`, der *CMD-Administrator* nur `discovery.read`. Die Menüpunkte erscheinen außerdem nur, wenn das Modul Discovery für den Mandanten eingeschaltet ist (ID-40).

3 Schritt 1: Einen Collector anlegen

 **Nur im Client:** *Erfassung & Abgleich* ▶ *Discovery-Collector* ·  `discovery.collector.manage` — Das Portal bietet keine Collector-Verwaltung; dieselbe Seite steht auch unter *Einstellungen* ▶ *Discovery-Collector*.



Klickweg – Schritt 1: Einen Collector anlegen

Pflichtreihenfolge — der Anmeldeschein entsteht **beim Speichern** und wird nur einmal angezeigt.

1. Klicken Sie auf *Collector anlegen*.
2. Tragen Sie unter *Bezeichnung* einen Namen ein, zum Beispiel **Collector Bauhof** – am besten den, unter dem der Standort im Alltag bekannt ist.
3. Tragen Sie unter *Standort* eine Beschreibung ein, zum Beispiel **Bauhof, Industriestraße 5**.
4. Tragen Sie unter *Netzbereiche (CIDR, kommagetrennt)* die Netze ein, zum Beispiel **10.20.0.0/24, 10.20.10.0/24**.
5. Tragen Sie unter *Abstand der Läufe* die Minuten zwischen zwei Läufen ein (Vorgabe **1440** = täglich).
6. Prüfen Sie die Schalter *Geplante Läufe aktiv*, *Windows per WinRM erheben* und *Geräte ohne Windows per SNMP befragen*.
7. Klicken Sie auf *Speichern*.
8. Klicken Sie im Fenster *Anmeldeschein für den Collector* auf *Kopieren* und legen Sie den Schein sicher ab.

✓ **Ergebnis:** Der Collector steht in der Liste mit dem Zustand *Anmeldung ausstehend*. Der Schein beginnt mit **ifd_** und ist bis zum angezeigten Zeitpunkt (*Gültig bis*) einlösbar – **sieben Tage**, genau einmal.

Feld	Bedeutung
<i>Bezeichnung</i>	Pflicht, je Mandant eindeutig.
<i>Standort</i>	rein beschreibend.
<i>Netzbereiche (CIDR, kommagetrennt)</i>	mindestens ein Netz in CIDR-Schreibweise. Nur die Schreibweise wird geprüft.
<i>Abstand der Läufe (Minuten, 0 = keine Läufe)</i>	Minuten zwischen zwei Läufen, Vorgabe 1440 (einmal am Tag). Bei 0 läuft kein Scan; einen Anstoß von Hand gibt es nicht.
<i>Geplante Läufe aktiv</i>	aus = der Collector meldet nur Lebenszeichen, scannt aber nicht.
<i>Windows per WinRM erheben</i>	Tiefen-Scan der Windows-Rechner (Vorgabe an).

Feld	Bedeutung
Geräte ohne Windows per SNMP befragen	SNMP für Switches, Drucker, USV (Vorgabe aus).

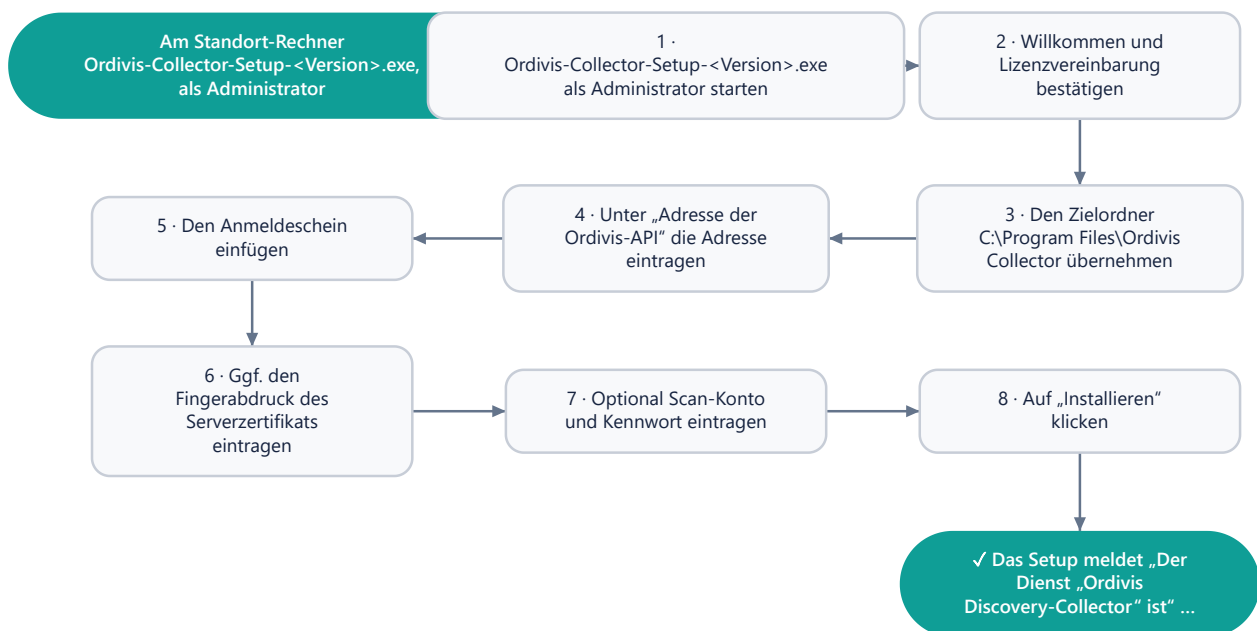
Schein nicht kopiert? Kein Grund, den Collector neu anzulegen: Die Schaltfläche *Anmeldeschein* in der Zeile stellt einen neuen aus (Abschnitt 9).

4 Schritt 2: Den Collector am Standort installieren

Verwenden Sie das eigenständige Paket **Ordivis-Collector-Setup-*<Version>*.exe** (rund 70 MB). Es enthält nur den Collector und seinen Aktualisierungsdienst – keinen Server, keine Datenbank, keinen Client.

 **Am Standort-Rechner:** **Ordivis-Collector-Setup-*<Version>*.exe** , als Administrator •  lokaler Administrator

Voraussetzung: Sie haben den Anmeldeschein aus Schritt 1 und die Adresse der Ordivis-Schnittstelle.



Klickweg – Schritt 2: Den Collector am Standort installieren

1. Starten Sie **Ordivis-Collector-Setup-*<Version>*.exe** als Administrator.
2. Bestätigen Sie Willkommen und Lizenzvereinbarung.
3. Übernehmen Sie den Zielordner **C:\Program Files\Ordivis Collector**.
4. Tragen Sie auf der Seite *Verbindung zur Zentrale* unter *Adresse der Ordivis-API* die Adresse ein, zum Beispiel **https://ordivis.musterstadt.local:5001**.
5. Fügen Sie unter *Anmeldeschein* (einmalig, aus der Collector-Verwaltung) den Schein ein.
6. Tragen Sie unter *SHA-256-Fingerabdruck des Serverzertifikats* nur dann etwas ein, wenn der Server ein eigenes Zertifikat ohne Zertifizierungsstelle trägt (64 Hex-Zeichen; Doppelpunkte, Leerzeichen und Bindestriche sind

erlaubt).

7. Tragen Sie auf der Seite *Anmeldedaten für den Tiefen-Scan* unter *Konto* (DOMAENE\benutzer) das Scan-Konto und darunter das *Kennwort* ein – oder lassen Sie beides leer.

8. Klicken Sie auf *Installieren* und schließen Sie den Assistenten.

✓ **Ergebnis:** Das Setup meldet „Der Dienst „Ordavis Discovery-Collector“ ist eingerichtet.“ Diese Meldung kommt nur, wenn der Dienst nach dem Start wirklich **läuft**. Kurz darauf steht der Collector in der Zentrale auf *Aktiv* (Schritt 3).

Statt der Erfolgsmeldung kann eine von drei Fehlermeldungen kommen – jede nennt, was zu tun ist:

Meldung des Setups	Bedeutung	Was Sie tun
„... ist eingerichtet, läuft aber NICHT (Zustand: ...)“	Der Dienst steht, startet aber nicht.	Ursache in <code>%ProgramData%\InfraDesk\setup-logs\collector.log</code> und im Protokoll des Dienstes lesen (Abschnitt 13).
„... ist eingerichtet, aber NICHT gestartet: Es ist keine Adresse der Ordavis-API hinterlegt.“	Es gibt keine Serveradresse.	Adresse in der <code>appsettings.json</code> unter <code>ServerUrl</code> eintragen und den Dienst starten – oder das Setup erneut ausführen.
„... konnte NICHT eingerichtet werden.“	Das Einrichtungsskript ist gescheitert.	Ursache in <code>collector.log</code> lesen, beheben, Setup erneut.

Was das Setup im Hintergrund tut:

- Es verschlüsselt das Kennwort mit dem Windows-Maschinenschlüssel (DPAPI) und schreibt Adresse, Schein, Konto, Kennwort und Fingerabdruck in `C:\Program Files\Ordavis Collector\collector\appsettings.json`. Das Kennwort erscheint dabei weder auf einer Kommandozeile noch in einem Protokoll. Misslingt die Verschlüsselung, werden Konto und Kennwort gar nicht gespeichert.
- Es richtet den Dienst `InfraDesk.Discovery.Collector` ein (Anzeigename *Ordavis Discovery-Collector*, Konto *LocalSystem*, Start *Automatisch* (verzögert), bei Fehlern Neustart nach 60, 60 und 300 Sekunden).
- Es richtet den Aktualisierungsdienst `InfraDesk.CollectorUpdate` ein (Abschnitt 12).
- Es legt im Startmenü unter *Ordavis IT* die Einträge *Ordavis Collector — Einstellungen* (öffnet die `appsettings.json` im Editor), *Ordavis Collector — Protokoll* (öffnet den Ordner, in den der Dienst tatsächlich schreibt) und *Ordavis Collector deinstallieren* an.

Hinweis: Bei einer Neuinstallation sind Adresse und Anmeldeschein Pflicht. Läuft das Setup über eine bestehende Installation, behält jedes leer gelassene Feld seinen bisherigen Wert – auch die Adresse; der Dienst wird mit ihr gestartet.

Hinweis: Der Collector lässt sich auch mit dem Hauptsetup installieren – als Installationstyp *Collector-Installation* oder als Zusatzhaken *Discovery-Collector zusätzlich installieren*. Die Seite *Discovery-Collector* fragt dort dieselben Angaben ab, einschließlich des Zertifikat-Fingerabdrucks. Auf einem Server aktualisiert ihn dann das Plattform-Update (ID-50a).

5 Schritt 3: Prüfen, ob er sich angemeldet hat

 **Nur im Client:** *Erfassung & Abgleich* ▶ *Discovery-Collector* ·  `discovery.read` — Das Portal zeigt keine Collector.



Klickweg – Schritt 3: Prüfen, ob er sich angemeldet hat

1. Öffnen Sie *Erfassung & Abgleich* ▶ *Discovery-Collector*.
2. Suchen Sie die Zeile Ihres Collectors.
3. Prüfen Sie die Spalten *Zustand* und *Zuletzt gesehen*.

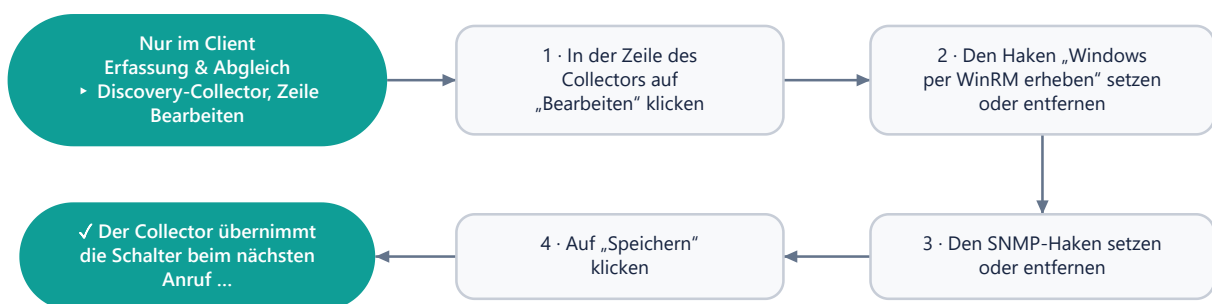
✓ **Ergebnis:** *Zustand* zeigt *Aktiv*, *Zuletzt gesehen* ist höchstens fünf Minuten alt. Der erste Lauf beginnt sofort nach der Anmeldung; nach dessen Ende stehen Werte unter *Letzter Lauf* und *Offene Funde*.

Am Standort-Rechner bestätigt das Protokoll die Anmeldung mit „Als "" angemeldet“ (Abschnitt 11).

6 Erhebungswege schalten und Zugänge hinterlegen

6.1 WinRM und SNMP in der Zentrale schalten

 **Nur im Client:** *Erfassung & Abgleich* ▶ *Discovery-Collector, Zeile Bearbeiten* ·  `discovery.collector.manage` — Das Portal bietet keine Collector-Verwaltung.



Klickweg – WinRM und SNMP in der Zentrale schalten

1. Klicken Sie in der Zeile des Collectors auf *Bearbeiten*.
2. Setzen oder entfernen Sie den Haken *Windows per WinRM erheben*.
3. Setzen oder entfernen Sie den Haken *Geräte ohne Windows per SNMP befragen*.
4. Klicken Sie auf *Speichern*.

✓ **Ergebnis:** Der Collector übernimmt die Schalter beim nächsten Anruf, spätestens nach fünf Minuten – niemand muss an den Standort.

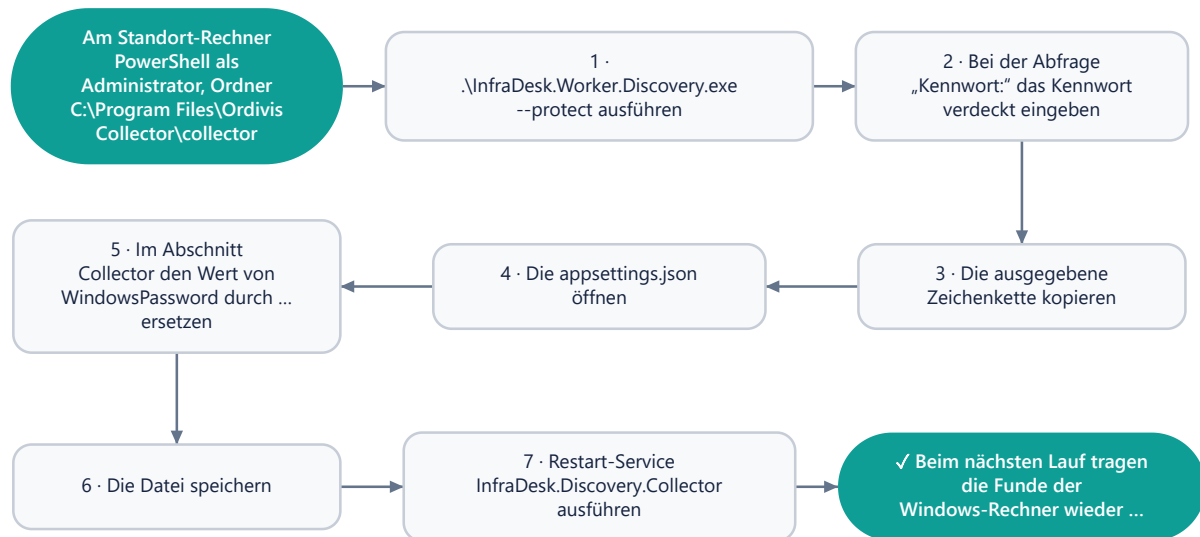
Zugänge bleiben am Standort. Die Zentrale schaltet nur, *welcher* Weg läuft. Windows-Kennwort, SNMP-Gemeinschaft und SNMPv3-Kennwörter erfährt sie nie. Der Collector führt außerdem nur die Abfragen aus, die er selbst mitbringt – die Zentrale kann ihm keine Skripte schicken.

6.2 Scan-Konto und Kennwort ändern

Das Scan-Kennwort steht verschlüsselt (DPAPI:...) in der `appsettings.json`. Ein Klartext-Kennwort wird abgewiesen: Der Tiefen-Scan bleibt dann aus, das Protokoll meldet es.

⚙️ **Am Standort-Rechner:** PowerShell als Administrator, Ordner `C:\Program Files\Ordivis Collector\collector` · 🔑 lokaler Administrator

🔒 **Pflichtreihenfolge** — das verschlüsselte Kennwort gilt nur auf **diesem** Rechner; der Dienst liest es nur beim Start.



Klickweg – Scan-Konto und Kennwort ändern

1. Führen Sie `.\InfraDesk.Worker.Discovery.exe --protect` aus.
2. Geben Sie bei der Abfrage *Kennwort:* das Kennwort verdeckt ein.
3. Kopieren Sie die ausgegebene Zeichenkette, die mit `DPAPI:` beginnt.
4. Öffnen Sie die `appsettings.json` (Startmenü *Ordivis Collector* — *Einstellungen*).
5. Ersetzen Sie im Abschnitt `Collector` den Wert von `WindowsPassword` durch die kopierte Zeichenkette (bei einem neuen Konto zusätzlich `WindowsUsername`).
6. Speichern Sie die Datei.
7. Führen Sie `Restart-Service InfraDesk.Discovery.Collector` aus.

✓ **Ergebnis:** Beim nächsten Lauf tragen die Funde der Windows-Rechner wieder Betriebssystem, Hardware und Anwendungen.

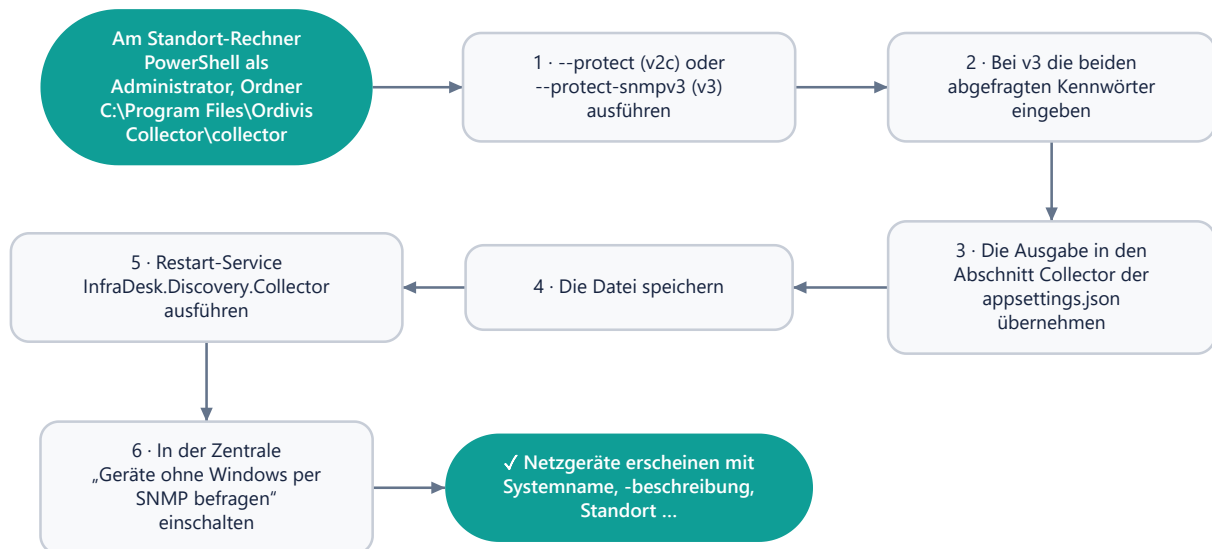
Tipp: Statt von Hand können Sie das Setup erneut laufen lassen und Konto und Kennwort dort neu eintragen. Leer gelassene Felder behalten ihren bisherigen Wert.

Achtung: Der Maschinenschlüssel schützt vor dem Kopieren auf einen anderen Rechner, nicht vor Programmen auf **demselden** Rechner: Jeder Prozess auf dem Standort-Rechner kann die **DPAPI: -Werte** entschlüsseln. Lassen Sie am Standort-Rechner deshalb nur Administratoren zu und nutzen Sie ihn für nichts anderes.

6.3 SNMP-Zugang hinterlegen (v2c oder v3)

Das Setup fragt keine SNMP-Daten ab; sie stehen nicht in der ausgelieferten `appsettings.json` und werden von Hand ergänzt. Ohne Eintrag fragt der Collector mit der Gemeinschaft `public`.

 **Am Standort-Rechner:** PowerShell als Administrator, Ordner `C:\Program Files\Ordvis Collector\collector` ·  lokaler Administrator



Klickweg – SNMP-Zugang hinterlegen (v2c oder v3)

1. Führen Sie für **v2c** `.\InfraDesk.Worker.Discovery.exe --protect` aus und geben Sie die Gemeinschaft verdeckt ein – oder für **v3** `.\InfraDesk.Worker.Discovery.exe --protect-snmpv3 <Benutzer> <Hashverfahren> <Verschlüsselung>`.
2. Geben Sie bei v3 die beiden abgefragten Kennwörter ein (je mindestens 8 Zeichen).
3. Übernehmen Sie die Ausgabe in den Abschnitt `Collector` der `appsettings.json`: bei v2c als `"SnmpGeheimnis": "DPAPI:..."`, bei v3 beide ausgegebenen Zeilen `SnmpBenutzer` und `SnmpGeheimnis`.
4. Speichern Sie die Datei.
5. Führen Sie `Restart-Service InfraDesk.Discovery.Collector` aus.
6. Schalten Sie in der Zentrale *Geräte ohne Windows per SNMP befragen* ein (Abschnitt 6.1).

 **Ergebnis:** Netzgeräte erscheinen mit Systemname, -beschreibung, Standort und Laufzeit; am Fund steht `erhoben_ueber = SNMP`.

Für v3 erlaubt `--protect-snmpv3` als Hashverfahren `Sha1`, `Sha256`, `Sha384` oder `Sha512` und als Verschlüsselung `Keine`, `Aes128`, `Aes192` oder `Aes256` (Groß- und Kleinschreibung egal). MD5 und DES werden nicht unterstützt.

6.4 Was die Zielrechner brauchen

Ping. Gefunden wird nur, wer auf ICMP-Echo antwortet. Rechner mit gesperrtem Ping bleiben unsichtbar.

MAC-Adresse. Der Collector liest sie aus der ARP-Tabelle seines Rechners – das klappt nur für Geräte im **selben Segment**. Hinter einem Router bleibt die MAC leer. Deshalb steht der Collector *im* Netz: Die MAC ist das Merkmal, das einen Rechner über einen Adresswechsel hinweg wiedererkennt.

WinRM (Tiefen-Scan Windows). Der Collector meldet sich mit dem Scan-Konto per PowerShell-Remoting an (TCP 5985, ohne SSL) und führt ein festes, nur lesendes Inventarskript aus. Dafür muss:

- WinRM am Zielrechner eingeschaltet sein (per Gruppenrichtlinie oder `Enable-PSRemoting`),
- das Scan-Konto Remoting nutzen dürfen – Windows erlaubt das standardmäßig nur Administratoren oder Mitgliedern der Gruppe *Remoteverwaltungsbenutzer*,
- der Zielname auflösbar sein: Der Collector spricht den Rechner über den Namen aus der Rückwärtsauflösung (PTR) an – aber nur, wenn derselbe Name vorwärts wieder auf diese Adresse zeigt. Ohne PTR oder bei einem Namen, der woandershin zeigt, nimmt er die IP-Adresse; dann muss der Standort-Rechner das Ziel in seiner WinRM-Liste *TrustedHosts* führen.

Achtung: Das Scan-Konto meldet sich an **jedem** antwortenden Rechner der Bereiche an. Nehmen Sie ein eigenes Konto mit so wenig Rechten wie möglich, nie ein Domänen-Administratorkonto.

Tipp: Ein veralteter PTR-Eintrag führt nicht mehr zum falschen Rechner – der Fund bleibt dann aber ohne Namen, und der Tiefen-Scan braucht *TrustedHosts*. Halten Sie die Rückwärtszonen deshalb sauber (ID-22).

SNMP. UDP 161; der Collector fragt nur Geräte, die **kein** Windows-Ergebnis geliefert haben.

7 Was ein Lauf tut

Abbildung 2 zeigt, wann ein Lauf stattfindet und in welcher Folge er arbeitet.

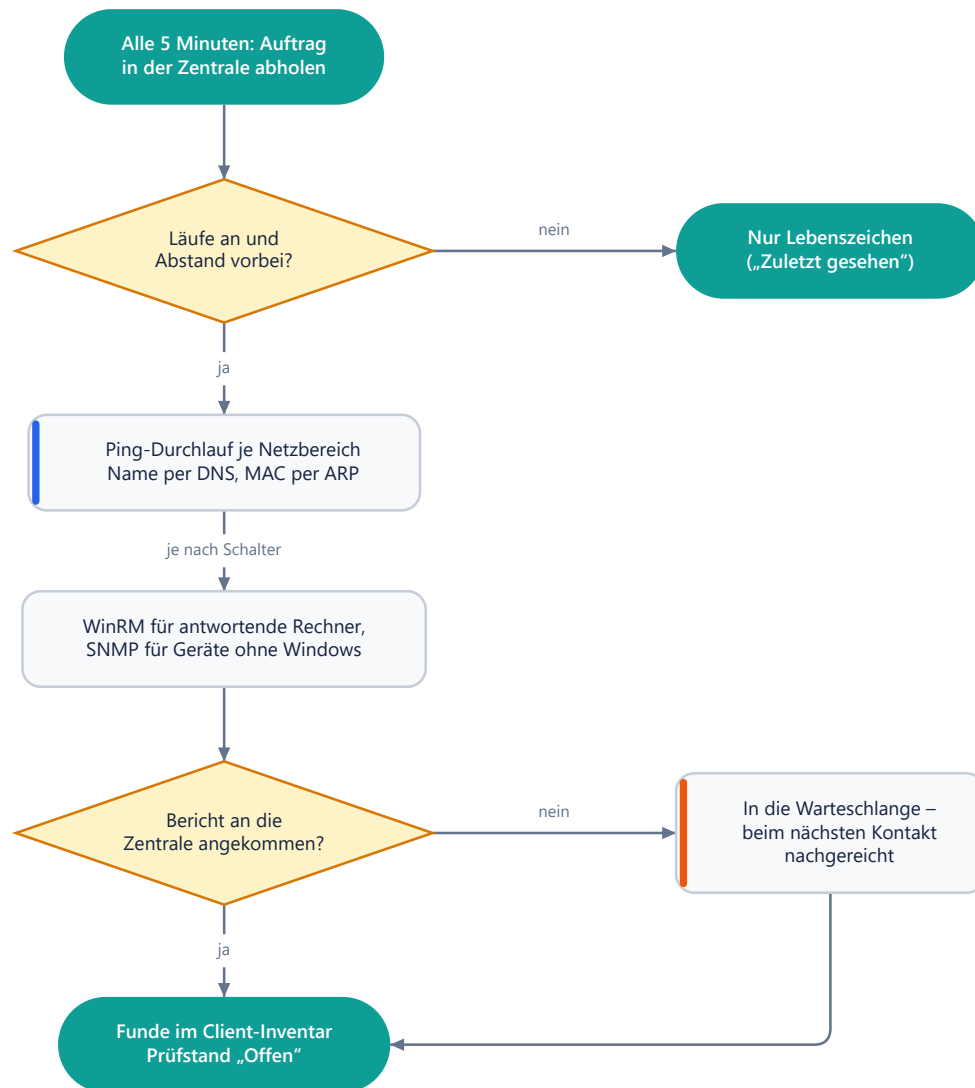


Abb. 2 – Ein Lauf des Collectors. Ohne Verbindung zur Zentrale gibt es keinen neuen Lauf; ein fertiger Bericht wird bei einem Abriss nachgereicht.

Wann. Alle fünf Minuten (`HeartbeatSeconds` = 300) holt der Collector seinen Auftrag. Ein Lauf ist fällig, wenn *Geplante Läufe aktiv* gesetzt ist und seit dem letzten Lauf mindestens der *Abstand der Läufe* vergangen ist – gemessen an der Uhr des Standort-Rechners. Der erste Lauf startet direkt nach der Anmeldung.

In welcher Folge:

Stufe	Erhebt	Voraussetzung
1. Ping-Durchlauf	antwortende Adressen, Antwortzeit (<code>rtt_ms</code>), Name per Rückwärtsauflösung	keine
2. ARP	MAC-Adresse (nur im eigenen Segment)	keine
3. WinRM	<code>os</code> , <code>os_version</code> , <code>os_arch</code> , <code>manufacturer</code> , <code>model</code> , <code>logical_cpus</code> , <code>ram_bytes</code> , <code>serial_number</code> , <code>firmware</code> , <code>disk_gb</code> , je Netzwerkkarte <code>if.<Name>.mac/.type/.speed</code> , installierte Anwendungen	Scan-Konto, Schalter <i>Windows per WinRM erheben</i> , <code>DeepScanWindows</code>

Stufe	Erhebt	Voraussetzung
4. SNMP	sysDescr , sysName , sysLocation , sysContact , sysUpTime	Schalter Geräte ohne Windows per SNMP befragen; nur Geräte ohne Windows-Ergebnis

Am Fund steht, auf welchem Weg er erhoben wurde (`erhoben_ueber` = `WinRM` oder `SNMP`) und, wenn ein Weg nicht ging, warum: `deep_scan` , `snmp_scan` und `winrm_fehler.<Abfrage>` für eine einzelne gescheiterte Teilabfrage. Ein Rechner ohne Tiefendaten ist damit nie ein Rätsel.

Welche Software erfasst wird. Die beiden Deinstallationszweige der Maschine (64 und 32 Bit), ohne Systemkomponenten. Programme, die nur für einen Benutzer installiert sind, erscheinen nicht.

Grenzen eines Laufs:

- je Netzbereich höchstens 65 534 Adressen – darüber wird ohne Meldung abgeschnitten;
- je Bericht höchstens 5000 antwortende Rechner und 20 MB – sonst weist die Zentrale den ganzen Bericht ab;
- Netz- und Broadcast-Adresse werden übersprungen; ein IPv6-Bereich bedeutet nur die angegebene Adresse;
- die Startadresse wird nicht auf die Netzadresse ausgerichtet: `10.20.0.5/24` durchsucht 10.20.0.6 bis 10.20.1.3. Richtig ist deshalb immer die Netzadresse, also `10.20.0.0/24` .

Wenn die Zentrale nicht erreichbar ist, holt der Collector keinen Auftrag – es läuft dann **kein** neuer Scan. Scheitert nur das Senden eines fertigen Berichts, legt er ihn in eine Warteschlange und reicht ihn nach dem nächsten erfolgreichen Kontakt nach – in der Reihenfolge, in der die Berichte entstanden sind. Die Zentrale erkennt Nachzügler an ihrer Kennung und verbucht sie nicht doppelt; ein älterer Fund überschreibt einen neueren nicht. Dasselbe gilt, wenn die Zentrale den **Zugang** abweist (gesperrt oder neuer Anmeldeschein): Der Bericht wartet, bis der Collector wieder angemeldet ist. Weist die Zentrale dagegen den **Bericht** selbst ab (etwa wegen zu vieler Rechner), wird er nicht aufbewahrt.

8 Das Client-Inventar: Funde prüfen und übernehmen

Alles, was Collector melden, landet unter *Erfassung & Abgleich* ▶ *Client-Inventar* – als **Fund**, nicht als CI.

Ein Fund ist kein Configuration Item. Was im Netz gefunden wurde, ist eine Beobachtung. Ein CI ist eine Aussage der Organisation über ihren Bestand. Erst die Bestätigung durch einen Menschen macht aus dem einen das andere – genau wie bei den unbestätigten Adressen der IP-Verwaltung.

Oben wählen Sie den *Standort* (alle oder ein bestimmter Collector) und den *Prüfstand* (*Offen* – Vorgabe –, *Übernommen*, *Verworfen*, *Alle*). Zwei Registerkarten:

- **Clients** – eine Zeile je Rechner mit IP, Bezeichnung, MAC, Betriebssystem, *Sammler* (der Name des Collectors), Zahl der Anwendungen, *Zuletzt gesehen* und *Prüfstand*.
- **Anwendungen** – eine Zeile je Anwendung und Version mit Hersteller und Zahl der Clients. Das ist die Frage, die im Betrieb tatsächlich gestellt wird: „Wo läuft das überall?“ **Gruppieren** ▶ **Anwendung** stapelt alle Versionen einer Anwendung unter einem Eintrag.

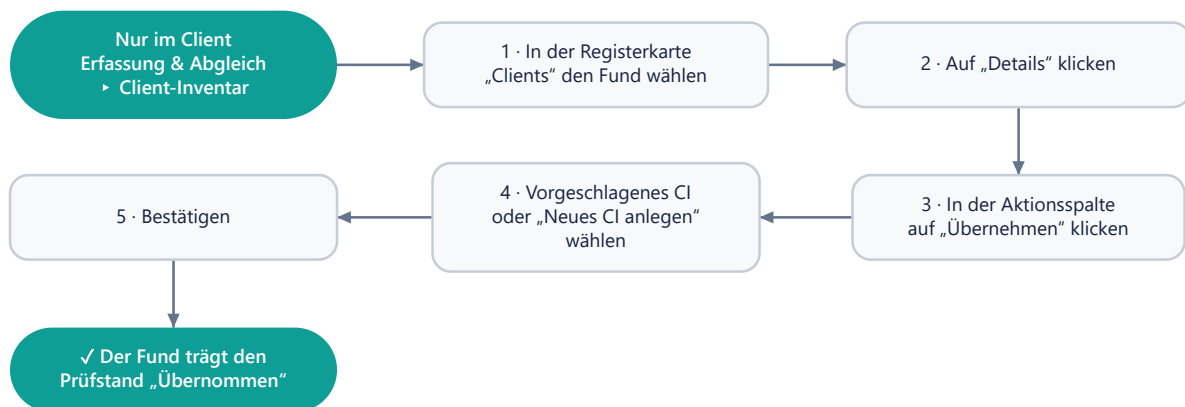
Beide sind Standardtabellen mit Suche, Spaltenfiltern, Sortierung, Spaltenauswahl und Export als CSV oder PDF. Geladen werden bis zu 2000 Funde und 5000 Anwendungen; liegt mehr vor, nennt die Fußzeile „... von ... Funden“ – grenzen Sie dann über den Standort ein.

Hinweis: Die Seite lädt neue Funde nicht von selbst nach. Klicken Sie nach einem Lauf auf *Aktualisieren*.

8.1 Übernehmen

 **Nur im Client:** *Erfassung & Abgleich* ▶ *Client-Inventar* ·  `discovery.result.review` — Das Portal zeigt das Client-Inventar nicht.

 **Pflichtreihenfolge** — der Dublettenabgleich läuft **vor** der Entscheidung. Wer ihn übergeht und blind anlegt, hat denselben Rechner zweimal in der CMDB.



Klickweg – Übernehmen

1. Wählen Sie in der Registerkarte *Clients* den Fund.
2. Klicken Sie auf *Details* (oder doppelt auf die Zeile), um alle gemeldeten Merkmale und Anwendungen zu sehen.
3. Klicken Sie in der Aktionsspalte auf *Übernehmen*.
4. Wählen Sie im Fenster *Als CI übernehmen* entweder ein vorgeschlagenes CI (gleiche MAC-Adresse oder gleicher Hostname) oder *Neues CI anlegen*.
5. Bestätigen Sie.

 **Ergebnis:** Der Fund trägt den Prüfstand *Übernommen*. Das CI hat die gemeldeten Merkmale, die Anwendungen hängen als Software-Installationen daran – die Grundlage der Lizenzzählung (ID-23). Jede weitere Meldung des Collectors schreibt dieses CI fort.

8.2 Verwerfen und wieder öffnen

Verwerfen nimmt einen Fund vom Tisch, ohne ein CI anzulegen – für Geräte, die nicht in die CMDB gehören (Gastgeräte, Fremdtechnik, Testaufbauten). Die Entscheidung hält: Beim nächsten Lauf kommt derselbe Fund nicht wieder hoch. **Wieder öffnen** holt ihn zurück. Beide Aktionen stehen in der Aktionsspalte – *Übernehmen* und *Verwerfen* bei offenen Funden, *Wieder öffnen* bei verworfenen.

Wiedererkannt wird ein Fund je Collector zuerst an der MAC-Adresse, dann am Hostnamen, zuletzt an der IP-Adresse (diese nur ohne MAC). Funde, die nicht mehr gemeldet werden, bleiben mit ihrem alten *Zuletzt gesehen* stehen; entfernt wird nichts von selbst.

9 Betrieb und Überwachung

Die Liste *Discovery-Collector* zeigt je Collector *Bezeichnung*, *Standort*, *Netzbereiche*, *Zustand*, *Zuletzt gesehen*, *Letzter Lauf* und *Offene Funde*. Ist ein Lauf gescheitert, steht der Fehler rot unter der Zeile. Melden sich Collector nicht mehr, nennt ein gelber Hinweis ihre Zahl.

Zustand	Bedeutung
Anmeldung ausstehend	angelegt oder entsperrt; der Anmeldeschein ist noch nicht eingelöst
Aktiv	angemeldet, meldet sich regelmäßig
Aktiv (Läufe aus)	meldet Lebenszeichen, scannt aber nicht (<i>Geplante Läufe aktiv aus</i>)
Überfällig	hat sich zu lange nicht gemeldet: länger als der doppelte <i>Abstand der Läufe</i> , mindestens eine Stunde – bei der Vorgabe 1440 also nach 48 Stunden
Gesperrt	gesperrt; der Zugang ist widerrufen

Tipp: Verlassen Sie sich für die Überwachung auf *Zuletzt gesehen*: Ein laufender Collector erneuert es alle fünf Minuten. *Überfällig* schlägt bei täglichen Läufen erst nach zwei Tagen an.

Die Aktionen in der Zeile (mit `discovery.collector.manage`):

Aktion	Wirkung
Bearbeiten	Bezeichnung, Standort, Bereiche, Abstand und Schalter ändern; wirkt beim nächsten Anruf.
Anmeldeschein	fragt nach („Neuen Anmeldeschein ausstellen?“), stellt dann einen neuen Schein aus und widerruft den laufenden Zugang sofort. Der Collector braucht danach den neuen Schein (Abschnitt 10).
Sperren	fragt nach und widerruft den Zugang; der Collector ist ab dem nächsten Anruf draußen. Zurück kommt er erst mit <i>Entsperren</i> und einem neuen Anmeldeschein.
Entsperren	setzt den Zustand auf <i>Anmeldung ausstehend</i> . Danach ist immer ein neuer Anmeldeschein nötig.
Löschen	fragt nach und entfernt den Collector, seinen Zugang und alle seine Funde. CIs in der CMDB bleiben.

Hinweis: In der Liste können auch Einträge „Ordavis Toolbox (...)“ erscheinen. Das sind angebundene Agenten, keine Collector; *Anmeldeschein*, *Sperren* und *Löschen* wirken dort auf den Zugang des Agenten. Sie stehen schon nach 60 Minuten ohne Meldung auf *Überfällig*.

10 Die Konfigurationsdatei `appsettings.json`

Die Datei liegt in `C:\Program Files\Ordavis Collector\collector\appsettings.json`. Der Dienst liest sie **nur beim Start** – nach jeder Änderung `Restart-Service InfraDesk.Discovery.Collector`. Eine Aktualisierung lässt sie unangetastet.

Abschnitt `Collector`:

Schlüssel	Vorgabe	Bedeutung
<code>ServerUrl</code>	leer	Adresse der Ordavis-Schnittstelle. Leer = der Dienst tut nichts.

Schlüssel	Vorgabe	Bedeutung
EnrollmentToken	leer	Anmeldeschein aus der Zentrale; einmal einlösbar, sieben Tage gültig. Er bleibt nach der Anmeldung in der Datei stehen, ist dann aber verbraucht.
CertificateFingerprint	leer	SHA-256-Fingerabdruck eines eigenen Serverzertifikats (64 Hex-Zeichen). Dann gilt genau dieses Zertifikat.
HeartbeatSeconds	300	Abstand der Anrufe in der Zentrale in Sekunden (mindestens 30).
MaxConcurrency	128	gleichzeitige Pings; WinRM nutzt ein Achtel, SNMP ein Viertel davon.
MaxHostsPerRange	65534	Adressen je Netzbereich; darüber wird ohne Meldung abgeschnitten.
DeepScanWindows	true	WinRM-Erhebung an diesem Rechner erlauben (zusätzlich zum Schalter in der Zentrale).
WindowsUsername	leer	Scan-Konto <code>DOMAENE\benutzer</code> .
WindowsPassword	leer	Kennwort, nur verschlüsselt (<code>DPAPI:...</code> , Abschnitt 6.2).
SnmpBenutzer	(nicht ausgeliefert)	SNMPv3-Benutzer; bei v2c leer.
SnmpGeheimnis	(nicht ausgeliefert)	verschlüsselte Gemeinschaft oder SNMPv3-Material (Abschnitt 6.3); leer = <code>public</code> .

Das frühere `AllowInvalidCertificate` wird nicht mehr ausgeliefert. Ein Collector, der es noch gesetzt hat, merkt sich beim ersten Kontakt das Zertifikat der Zentrale und nimmt danach nur noch dieses an (Meldung „CMP-27: Die Zertifikatsprüfung war abgeschaltet ...“). Wechselt das Zertifikat, tragen Sie den neuen Fingerabdruck ein.

Abschnitt **Logging**: `Logging:LogLevel:Default` und `Logging:LogLevel:Microsoft.Hosting.Lifetime` sind die üblichen .NET-Stufen; maßgeblich für die Protokolldatei sind die Schlüssel unter `Logging:File` (`Enabled` , `Directory` , `Level` , `RetainedDays` , `FileSizeLimitMb` usw.), die ID-50 in Kapitel 10 erklärt. Läuft der Collector auf dem Server, gelten zusätzlich die zentralen Protokoll-Einstellungen aus `operations.json`.

Jeder Schlüssel lässt sich auch als Umgebungsvariable setzen, zum Beispiel `Collector_HeartbeatSeconds`.

Kommandozeile von `InfraDesk.Worker.Discovery.exe`:

Aufruf	Wirkung
<code>--protect [Wert]</code>	verschlüsselt einen Wert mit dem Maschinenschlüssel und gibt <code>DPAPI:...</code> aus; ohne Wert fragt er verdeckt <i>Kennwort</i> :. Gilt nur auf diesem Rechner. Ein Wert auf der Kommandozeile ist für andere Prozesse sichtbar; ohne Wert bleibt er verdeckt.
<code>--protect-stdin</code>	wie <code>--protect</code> , liest den Wert aber aus der Standardeingabe (UTF-8). So ruft das Setup auf; für Skripte geeignet.
<code>--protokollordner</code>	gibt den Ordner aus, in den der Dienst sein Protokoll schreibt, und öffnet ihn im Explorer (der Startmenüeintrag <i>Ordivis Collector — Protokoll</i>).
<code>--protect-snmpv3 <Benutzer> <Hash> <Verschlüsselung></code>	fragt die SNMPv3-Kennwörter verdeckt ab und gibt die Zeilen <code>SnmpBenutzer</code> und <code>SnmpGeheimnis</code> aus.
ohne Schalter	startet den Collector; in einer Konsole läuft er im Vordergrund und schreibt sein Protokoll sichtbar mit – nützlich zur Fehlersuche (vorher den Dienst beenden).

11 Dateien, Dienste und Protokolle

Was	Wo
Programm	C:\Program Files\Ordivis Collector\collector\
Einstellungen	...\collector\appsettings.json
Anmeldung und Zugang	%ProgramData%\InfraDesk\collector\state.json (Zugang DPAPI-geschützt)
Warteschlange	%ProgramData%\InfraDesk\collector\outbox\ (dauerhaft abgewiesene Berichte als .rejected)
Gemerakter Fingerabdruck	%ProgramData%\InfraDesk\collector\server-zertifikat.txt
Protokoll	<Datenlaufwerk>\Ordivis\Logs\worker\ , ohne Datenlaufwerk %ProgramData%\InfraDesk\Logs\worker\ ; die Meldungen des Collectors stehen in wartung-JJJJMMTT.log
Ereignisprotokoll	Windows-Protokoll <i>Anwendung</i> , ab Warnungen
Setup-Protokolle	%ProgramData%\InfraDesk\setup-logs\collector.log , collectorupdate.log
Dienste	InfraDesk.Discovery.Collector (Ordivis Discovery-Collector), InfraDesk.CollectorUpdate (Ordivis Aktualisierungsdienst (Collector))

Tipp: Welcher Ordner es auf diesem Rechner ist, zeigt der Startmenüeintrag *Ordivis Collector — Protokoll*: Er öffnet genau den Ordner, in den der Dienst schreibt. In PowerShell nennt ihn

```
.\InfraDesk.Worker.Discovery.exe --protokollordner .
```

12 Aktualisieren und entfernen

Aktualisieren geschieht von selbst. Der Dienst `InfraDesk.CollectorUpdate` fragt alle 240 Minuten denselben Server, an den der Collector meldet, nach dessen Fassung – über denselben ausgehenden Weg. Liegt der Collector zurück, lädt er die Aktualisierung geprüft herunter und tauscht sie **ohne Rückfrage**: Dienst anhalten, Dateien tauschen, Dienst starten. Startet der Collector danach nicht, wird die vorige Fassung wiederhergestellt. Ist der Server nicht erreichbar, weicht der Dienst auf die Aktualisierungsquelle des Herstellers aus. Sein Protokoll liegt unter `<Protokollordner>\collectorupdate\`. Einzelheiten zum Aktualisierungssystem stehen in ID-50a.

Der Aktualisierungsdienst hat eine eigene Datei `C:\Program Files\Ordivis Collector\clientupdate\appsettings.json`:

Schlüssel	Vorgabe	Bedeutung
<code>ClientUpdate:ServerUrl</code>	leer	Server, der gefragt wird; leer = derselbe wie <code>Collector:ServerUrl</code> .
<code>ClientUpdate:FallbackUrl</code>	<code>https://update.ordivis.eu/v1/platform</code>	Aktualisierungsquelle des Herstellers, wenn der Server nicht antwortet.

Schlüssel	Vorgabe	Bedeutung
<code>ClientUpdate:CheckIntervalMinutes</code>	240	Prüfabstand in Minuten (15 bis 1440).

Nach einer Änderung: `Restart-Service InfraDesk.CollectorUpdate`. Hat der Standort keinen Weg ins Internet, scheitert nur dieser Rückfall; solange der eigene Server antwortet, wird er nicht gebraucht.

Wichtig: Ein Collector, der vor dem Aktualisierungsdienst eingerichtet wurde, braucht **genau einmal** das aktuelle Collector-Setup. Es erkennt die bestehende Anmeldung: Adresse und Fingerabdruck sind vorbelegt, ein leeres Feld behält seinen Wert, ein neuer Anmeldeschein ist nicht nötig.

Der Collector meldet bei jedem Dienststart seinen Rechnernamen und seine Version an die Zentrale. Nach einer Aktualisierung steht in der Collector-Liste deshalb binnen fünf Minuten die neue Version.

Entfernen geschieht an zwei Stellen: am Standort und in der Zentrale.

 **Am Standort-Rechner:** Windows-Einstellungen *Apps* oder Startmenü *Ordivis Collector deinstallieren* · 
lokaler Administrator

1. Deinstallieren Sie *Ordivis Discovery-Collector*.

✓ **Ergebnis:** Beide Dienste sind entfernt, ebenso `%ProgramData%\InfraDesk\collector` (Anmeldung, Warteschlange, Fingerabdruck) und die Aktualisierungsdaten. Die Protokolle bleiben.

In der Zentrale bleibt der Zugang gültig, bis Sie ihn sperren oder löschen – er hat kein Ablaufdatum.

 **Nur im Client:** *Erfassung & Abgleich* ▶ *Discovery-Collector* ·  `discovery.collector.manage` — Das Portal bietet keine Collector-Verwaltung.



Klickweg – Aktualisieren und entfernen

- Klicken Sie in der Zeile des Collectors auf *Löschen* – oder auf *Sperren*, wenn seine Funde erhalten bleiben sollen.
- Bestätigen Sie die Rückfrage.

✓ **Ergebnis:** Der Zugang ist widerrufen. *Löschen* entfernt zusätzlich alle Funde des Collectors; die CIs in der CMDB bleiben in beiden Fällen.

13 Fehlerbehebung

Meldung im Protokoll oder Bild	Ursache	Abhilfe
„DDS-02: Keine Serveradresse konfiguriert (Collector:ServerUrl). Der Dienst tut nichts.“	<code>ServerUrl</code> leer	Adresse eintragen, Dienst neu starten.
„DDS-02: Nicht angemeldet und kein Anmeldeschein hinterlegt (Collector:EnrollmentToken). ...“	kein Schein in der Datei	In der Zentrale <i>Anmeldeschein</i> , Schein in <code>EnrollmentToken</code> eintragen, Dienst neu starten.
„DDS-02: Anmeldung fehlgeschlagen: Anmeldeschein ungültig, abgelaufen oder bereits eingelöst.“	Schein vertippt, älter als sieben Tage, schon eingelöst oder Collector gesperrt	Bei <i>Gesperrt</i> erst <i>Entsperren</i> ; dann <i>Anmeldeschein</i> und neuen Schein eintragen.
„... Zentrale nicht erreichbar: ...“	DNS, Firewall, Zertifikat nicht vertrauenswürdig oder falscher Fingerabdruck	Erreichbarkeit vom Standort prüfen; bei eigenem Zertifikat Fingerabdruck prüfen.
„... Abgewiesen (429): ...“	mehr als 30 Anfragen je Minute von einer Adresse	Kurz warten.
„DDS-02: Zugang abgewiesen — Anmeldung wird verworfen. Neuer Anmeldeschein nötig.“	gesperrt, gelöscht oder neuer Schein ausgestellt	Neuen Schein eintragen, Dienst neu starten.
„DDS-02: Läufe sind in der Zentrale abgeschaltet — nur Lebenszeichen.“	<i>Geplante Läufe aktiv</i> aus	Schalter setzen (Abschnitt 6.1).
„DDS-02: Kein Netzbereich zugewiesen.“	keine Bereiche eingetragen	Bereiche ergänzen.
„DDS-02: Collector:WindowsPassword ist nicht DPAPI-geschuetzt ...“	Kennwort im Klartext	Mit <code>--protect</code> verschlüsseln (Abschnitt 6.2).
„DDS-02: Scan-Kennwort nicht entschlüsselbar — der Tiefen-Scan bleibt aus.“	auf einem anderen Rechner verschlüsselt	Auf diesem Rechner neu mit <code>--protect</code> verschlüsseln.
„DDS-25: ... SnmpGeheimnis ist nicht DPAPI-geschuetzt ...“ / „DDS-25: SNMP-Geheimnis nicht entschlüsselbar — SNMP fragt nur mit "public".“	Klartext oder fremder Rechner	Mit <code>--protect</code> bzw. <code>--protect-snmppv3</code> neu erzeugen.
„DDS-02: Zugangstoken nicht entschlüsselbar (anderes Konto/Rechner?).“	<code>state.json</code> kopiert oder Rechner getauscht	Der Collector meldet sich neu an – dafür ist ein gültiger Schein nötig.
„DDS-02: ARP-Tabelle nicht lesbar — Funde bleiben ohne MAC-Adresse.“	<code>arp -a</code> gescheitert	Rechner prüfen; Funde kommen weiterhin, nur ohne MAC.
„DDS-03: Bericht ... abgewiesen: (413) ... Zu viele Hosts (... > 5000) — bitte aufteilen.“	mehr als 5000 Rechner oder 20 MB in einem Bericht	Bereiche auf mehrere Collector aufteilen oder verkleinern; dieser Bericht ist verloren.

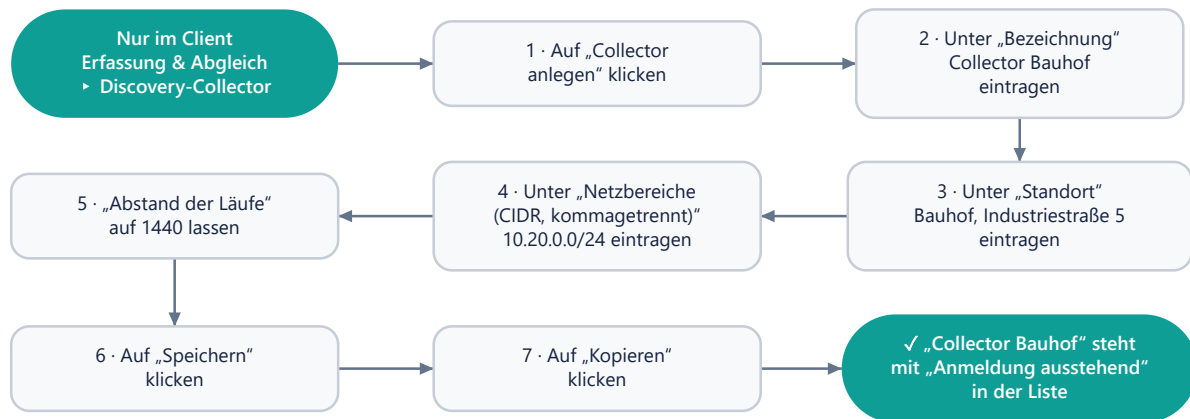
Meldung im Protokoll oder Bild	Ursache	Abhilfe
„DDS-03: ... — Bericht ... zwischengespeichert.“	Zentrale beim Senden nicht erreichbar oder Zugang abgewiesen	Bei „nicht erreichbar“ nichts zu tun; bei „Zugang abgewiesen“ einen neuen Anmeldeschein eintragen. Danach wird er nachgereicht.
„DDS-03: Zwischengespeicherter Bericht dauerhaft abgewiesen: ...“	ein nachgereichter Bericht wurde von der Zentrale abgelehnt	Die Datei liegt als <code>.rejected</code> in der Warteschlange; Ursache aus der Meldung beheben, die Datei danach löschen.
„DDS-02: Lauf abgebrochen.“	Fehler während des Laufs	Der Fehlertext steht rot unter der Zeile des Collectors und im Protokoll.
„CMP-27: Die Zertifikatsprüfung war abgeschaltet. Ab jetzt gilt nur noch das Zertifikat mit dem Fingerabdruck ...“	alter Schalter <code>AllowInvalidCertificate</code> ; der Fingerabdruck wurde gemerkt	Fingerabdruck mit dem Serverzertifikat abgleichen (Abschnitt 10).
Fund mit <code>deep_scan</code> = „nicht möglich: ...“ oder „keine Antwort vom Ziel“	WinRM aus, fehlende Rechte, IP ohne <code>TrustedHosts</code> , kein Windows	Zielrechner nach Abschnitt 6.4 prüfen.
Fund mit <code>winrm_fehler.<Abfrage></code>	eine einzelne Teilabfrage scheiterte	Übrige Daten sind gültig; Rechte am Ziel prüfen.
Fund mit <code>snmp_scan</code> = „keine Antwort: Das Gerät lehnt die SNMPv3-Anmeldung ab ...“	falsche v3-Daten oder Uhrzeit außerhalb des Fensters	Zugang neu erzeugen, Uhrzeit prüfen.
„So nicht verwendbar: KennwortZuKurz ...“	<code>--protect-snmpv3</code> mit weniger als 8 Zeichen	Längeres Kennwort.
Setup: „Der Dienst „Ordavis Discovery-Collector“ konnte NICHT eingerichtet werden. ...“	siehe <code>setup-logs\collector.log</code>	Ursache dort lesen, Setup erneut.
Setup: „... ist eingerichtet, läuft aber NICHT (Zustand: ...)“	der Dienst startet nicht	<code>setup-logs\collector.log</code> und das Protokoll des Dienstes lesen.
Setup: „... ist eingerichtet, aber NICHT gestartet: Es ist keine Adresse der Ordavis-API hinterlegt.“	keine Serveradresse	<code>ServerUrl</code> eintragen, Dienst starten (Abschnitt 10).
Setup: „Der Fingerabdruck muss aus 64 Hex-Zeichen bestehen ...“	ein SHA-1-Wert (40 Zeichen) oder unvollständig eingefügt	Den SHA-256-Wert vollständig einfügen (Abschnitt 15, Frage zum Fingerabdruck).
Collector bleibt auf <i>Anmeldung ausstehend</i>	Schein ungültig, keine Verbindung oder Dienst ohne Adresse	Collector-Protokoll lesen; bei fehlender Adresse steht im Setup-Protokoll „Keine Serveradresse angegeben — Dienst angelegt, aber nicht gestartet.“
Funde fehlen	kein Ping-Echo, Bereich zu groß oder nicht an der Netzadresse ausgerichtet, mehr als 5000 Rechner	Abschnitt 7 <i>Grenzen</i> prüfen.

14 Beispiele aus der Praxis

14.1 Beispiel: Den Bauhof einbinden

Ausgangslage: Der Bauhof der Gemeinde Musterstadt hat ein eigenes Netz `10.20.0.0/24`, das vom Rathaus nur über eine VPN-Verbindung erreichbar ist. Dort steht der Server `BAUHOF-SRV01`. Die Windows-Rechner sollen mit dem Konto `MUSTERSTADT\svc-ordvis-scan` inventarisiert werden.

 **Nur im Client:** *Erfassung & Abgleich* ▶ *Discovery-Collector* ·  `discovery.collector.manage` — Das Portal bietet keine Collector-Verwaltung.



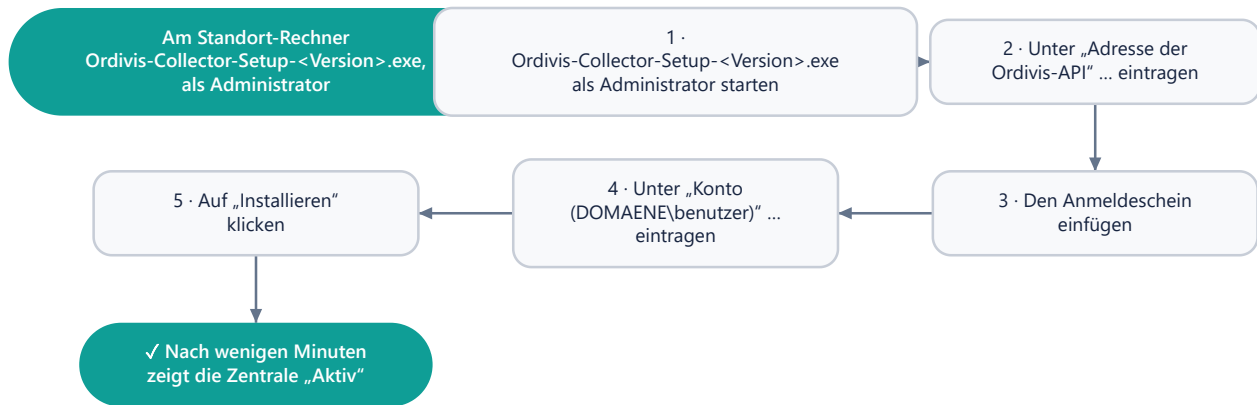
Klickweg – Beispiel: Den Bauhof einbinden

1. Klicken Sie auf *Collector anlegen*.
2. Tragen Sie unter *Bezeichnung* `Collector Bauhof` ein.
3. Tragen Sie unter *Standort* `Bauhof, Industriestraße 5` ein.
4. Tragen Sie unter *Netzbereiche (CIDR, kommasetrennt)* `10.20.0.0/24` ein.
5. Lassen Sie *Abstand der Läufe* auf `1440`.
6. Klicken Sie auf *Speichern*.
7. Klicken Sie auf *Kopieren* und übertragen Sie den Schein sicher zum Bauhof.

✓ **Ergebnis:** *Collector Bauhof* steht mit *Anmeldung ausstehend* in der Liste.

Am Server `BAUHOF-SRV01`:

 **Am Standort-Rechner:** `Ordvis-Collector-Setup-<Version>.exe`, als Administrator ·  lokaler Administrator



Klickweg – Beispiel: Den Bauhof einbinden

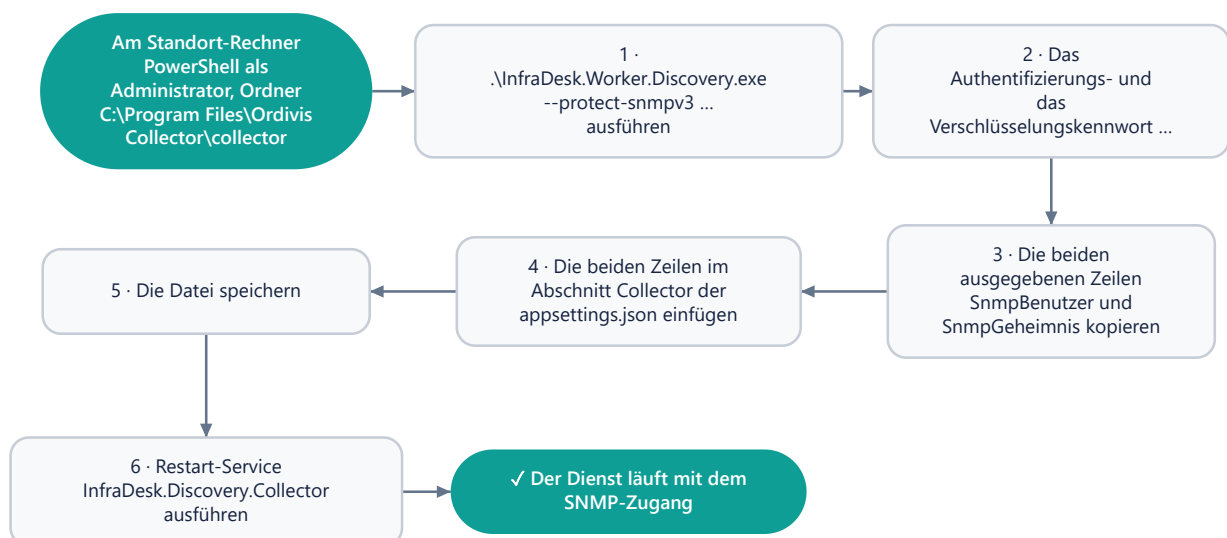
1. Starten Sie `Ordvis-Collector-Setup-<Version>.exe` als Administrator.
2. Tragen Sie unter *Adresse der Ordvis-API* `https://ordvis.musterstadt.local:5001` ein.
3. Fügen Sie unter *Anmeldeschein* (einmalig, aus der Collector-Verwaltung) den Schein ein.
4. Tragen Sie unter *Konto* (DOMAENE\benutzer) `MUSTERSTADT\svc-ordvis-scan` und darunter das *Kennwort* ein.
5. Klicken Sie auf *Installieren*.

✓ **Ergebnis:** Nach wenigen Minuten zeigt die Zentrale *Aktiv*; nach dem ersten Lauf stehen unter *Offene Funde* die Rechner des Bauhofs.

14.2 Beispiel: Switches per SNMPv3 erfassen

Ausgangslage: Im Bauhof stehen zwei verwaltete Switches. Sie sind für SNMPv3 mit dem Benutzer `ordvis-ro`, SHA-256 und AES-128 eingerichtet.

⚙️ **Am Standort-Rechner:** PowerShell als Administrator, Ordner `C:\Program Files\Ordvis Collector\collector` · 🔑 lokaler Administrator

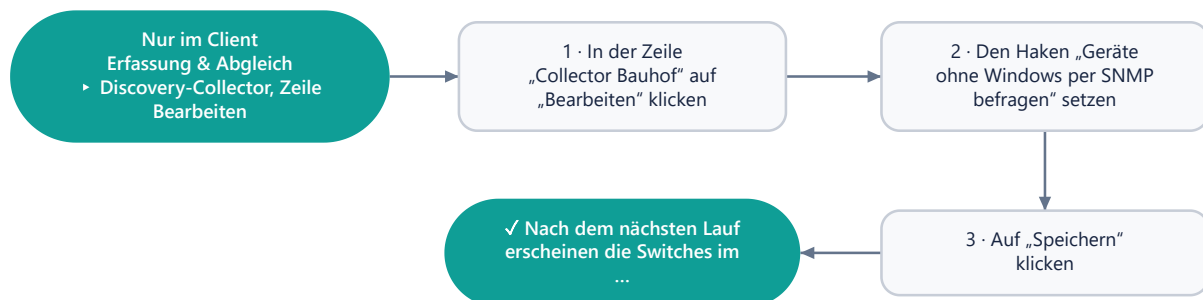


Klickweg – Beispiel: Switches per SNMPv3 erfassen

1. Führen Sie `.\InfraDesk.Worker.Discovery.exe --protect-snmpv3 ordivis-ro Sha256 Aes128` aus.
2. Geben Sie das Authentifizierungs- und das Verschlüsselungskennwort ein.
3. Kopieren Sie die beiden ausgegebenen Zeilen `SnmpBenutzer` und `SnmpGeheimnis`.
4. Fügen Sie die beiden Zeilen im Abschnitt `Collector` der `appsettings.json` ein.
5. Speichern Sie die Datei.
6. Führen Sie `Restart-Service InfraDesk.Discovery.Collector` aus.

✓ **Ergebnis:** Der Dienst läuft mit dem SNMP-Zugang. Jetzt fehlt nur noch der Schalter in der Zentrale.

 **Nur im Client:** *Erfassung & Abgleich* ▶ *Discovery-Collector, Zeile Bearbeiten* ·  `discovery.collector.manage` — Das Portal bietet keine Collector-Verwaltung.



Klickweg – Beispiel: Switches per SNMPv3 erfassen

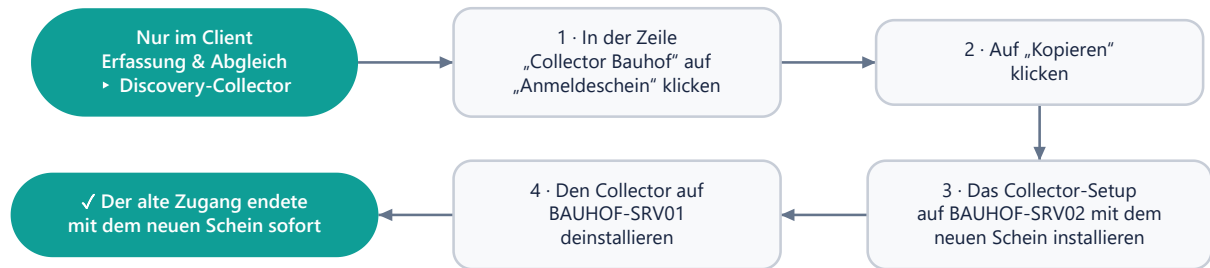
1. Klicken Sie in der Zeile *Collector Bauhof* auf *Bearbeiten*.
2. Setzen Sie den Haken *Geräte ohne Windows per SNMP befragen*.
3. Klicken Sie auf *Speichern*.

✓ **Ergebnis:** Nach dem nächsten Lauf erscheinen die Switches im Client-Inventar mit `sysName` und `sysDescr`; am Fund steht `erhoben_ueber` = `SNMP`.

14.3 Beispiel: Den Standort-Rechner austauschen

Ausgangslage: `BAUHOF-SRV01` wird durch `BAUHOF-SRV02` ersetzt. Der Collector soll auf dem neuen Rechner mit derselben Bezeichnung weiterlaufen.

 **Nur im Client:** *Erfassung & Abgleich* ▶ *Discovery-Collector* ·  `discovery.collector.manage` — Das Portal bietet keine Collector-Verwaltung.



Klickweg – Beispiel: Den Standort-Rechner austauschen

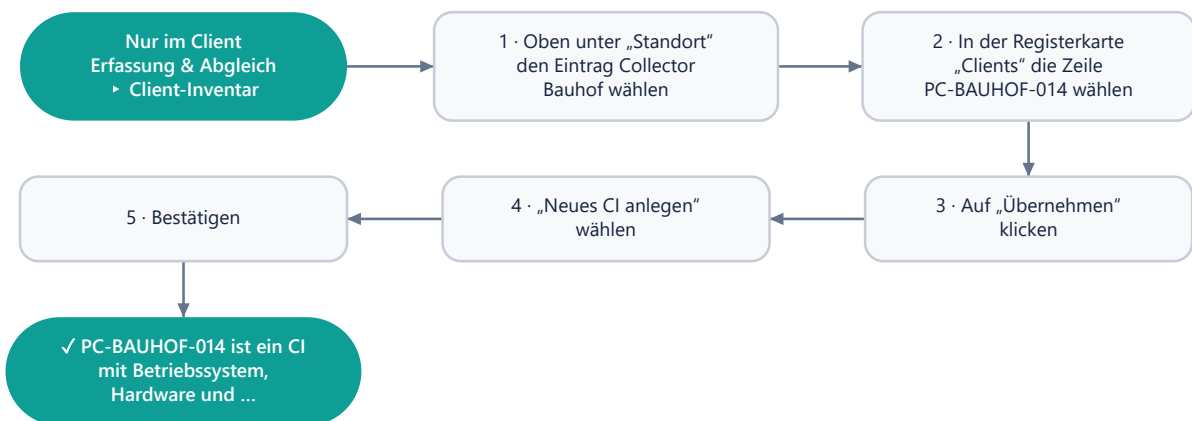
1. Klicken Sie in der Zeile *Collector Bauhof* auf *Anmeldeschein*.
2. Klicken Sie auf *Kopieren*.
3. Installieren Sie das Collector-Setup auf **BAUHOF-SRV02** mit dem neuen Schein (Abschnitt 4).
4. Deinstallieren Sie den Collector auf **BAUHOF-SRV01**.

✓ **Ergebnis:** Der alte Zugang endete mit dem neuen Schein sofort; **BAUHOF-SRV02** meldet sich an, der Zustand wird wieder *Aktiv*. Bisherige Funde bleiben erhalten.

14.4 Beispiel: Einen Rechner aus dem Bauhof übernehmen

Ausgangslage: Im Client-Inventar steht der Fund **PC-BAUHOF-014**. In der CMDB gibt es diesen Rechner noch nicht.

🖥️ **Nur im Client: Erfassung & Abgleich** ► *Client-Inventar* · 🔑 **discovery.result.review** — Das Portal zeigt das Client-Inventar nicht.



Klickweg – Beispiel: Einen Rechner aus dem Bauhof übernehmen

1. Wählen Sie oben unter *Standort* den Eintrag **Collector Bauhof**.
2. Wählen Sie in der Registerkarte *Clients* die Zeile **PC-BAUHOF-014**.
3. Klicken Sie auf *Übernehmen*.
4. Wählen Sie *Neues CI anlegen*.
5. Bestätigen Sie.

✓ **Ergebnis:** PC-BAUH0F-014 ist ein CI mit Betriebssystem, Hardware und Software-Installationen; der Fund trägt *Übernommen*. Die nächste Meldung des Collectors hält das CI aktuell.

14.5 Beispiel: Einen gesperrten Collector wieder zulassen

Ausgangslage: *Collector Bauhof* wurde während eines Netzbauwerks gesperrt. Der Dienst am Standort läuft weiter, kommt aber nicht mehr durch. Jetzt soll er wieder melden.

 **Nur im Client:** *Erfassung & Abgleich* ▶ *Discovery-Collector* ·  `discovery.collector.manage` — Das Portal bietet keine Collector-Verwaltung.

 **Pflichtreihenfolge** — ein gesperrter Collector kann keinen Schein einlösen; erst entsperren, dann den Schein ausstellen.



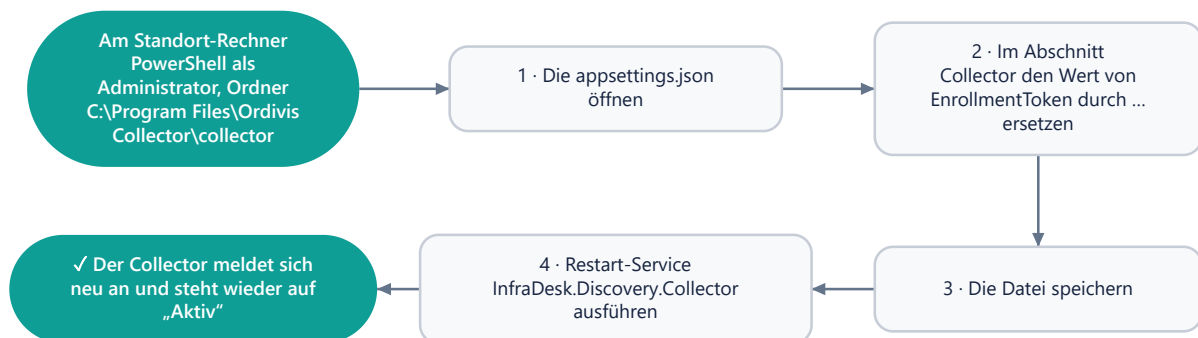
Klickweg – Beispiel: Einen gesperrten Collector wieder zulassen

1. Klicken Sie in der Zeile *Collector Bauhof* auf *Entsperren*.
2. Klicken Sie in derselben Zeile auf *Anmeldeschein*.
3. Klicken Sie auf *Kopieren*.

✓ **Ergebnis:** Der Zustand ist *Anmeldung ausstehend*, der neue Schein liegt bereit.

Am Server BAUH0F-SRV01 :

 **Am Standort-Rechner:** PowerShell als Administrator, Ordner `C:\Program Files\Ordivis Collector\collector` ·  lokaler Administrator



Klickweg – Beispiel: Einen gesperrten Collector wieder zulassen

1. Öffnen Sie die `appsettings.json` (Startmenü *Ordivis Collector* — *Einstellungen*).

2. Ersetzen Sie im Abschnitt `Collector` den Wert von `EnrollmentToken` durch den neuen Schein.
3. Speichern Sie die Datei.
4. Führen Sie `Restart-Service InfraDesk.Discovery.Collector` aus.

✓ **Ergebnis:** Der Collector meldet sich neu an und steht wieder auf *Aktiv*. Seine bisherigen Funde sind unverändert da.

15 Häufige Fragen

Ich sehe den Menüpunkt *Discovery-Collector* nicht. Sie brauchen das Recht `discovery.read`, und das Modul Discovery muss für den Mandanten eingeschaltet sein (Abschnitt 2.1). Im Portal gibt es die Seite nicht.

Kann ich einen Token aus *Integrations-Token* als Anmeldeschein nehmen? Nein. Der Collector nimmt nur den Anmeldeschein aus der Collector-Verwaltung an (Abschnitt 3).

Wie ermittle ich den SHA-256-Fingerabdruck des Serverzertifikats? Am einfachsten zeigt ihn der Verbindungsdialog des Windows-Clients: *Verbindung testen* nennt ihn bei einem Zertifikat ohne Zertifizierungsstelle (ID-50, Abschnitt 7.2). Am Server liefert PowerShell ihn für jedes Zertifikat des Rechners: `Get-ChildItem Cert:\LocalMachine\My | ForEach-Object { $_.Subject; [BitConverter]::ToString([Security.Cryptography.SHA256]::Create().ComputeHash($_.RawData)) -replace '-'` } . Gleichen Sie den Wert über einen zweiten Weg ab, bevor Sie ihn eintragen.

Wie lange dauert ein Lauf? Der Ping-Durchlauf ist schnell: 128 Adressen gleichzeitig, je Adresse höchstens 800 Millisekunden Wartezeit. Die meiste Zeit braucht WinRM mit bis zu 16 Rechnern gleichzeitig: Ein Rechner, der die Verbindung nicht annimmt, hält höchstens 15 Sekunden auf, eine Abfrage darf bis zu zwei Minuten dauern. SNMP fragt bis zu 32 Geräte gleichzeitig mit drei Sekunden Wartezeit. Die Gleichzeitigkeit wächst und schrumpft mit `MaxConcurrency` (Abschnitt 10).

Braucht der Standort eine eingehende Firewall-Freigabe? Nein. Nötig ist nur ausgehendes HTTPS zur Zentrale, dazu Ping, WinRM und SNMP ins eigene Netz (Abschnitt 2).

Ich habe den Anmeldeschein nicht kopiert – muss ich den Collector neu anlegen? Nein. Die Schaltfläche *Anmeldeschein* stellt einen neuen aus (Abschnitt 9).

Wie lange gilt ein Anmeldeschein? Sieben Tage, und er lässt sich genau einmal einlösen.

Wann läuft der erste Scan? Sofort nach der Anmeldung. Danach prüft der Collector alle fünf Minuten, ob der nächste fällig ist (Abschnitt 7).

Was bedeutet *Abstand der Läufe* = 0? Dann läuft kein Scan; einen Anstoß von Hand gibt es nicht. Für einen einmaligen Lauf stellen Sie den Abstand vorübergehend klein ein, zum Beispiel `5`, und danach zurück.

Ich habe die `appsettings.json` geändert, aber nichts passiert. Der Dienst liest sie nur beim Start: `Restart-Service InfraDesk.Discovery.Collector`.

Erfährt die Zentrale das Scan-Kennwort oder die SNMP-Gemeinschaft? Nein. Beides bleibt verschlüsselt am Standort; die Zentrale schaltet nur die Wege (Abschnitt 6.1).

Kann ich die `appsettings.json` auf einen anderen Rechner kopieren? Die `DPAPI:`-Werte sind an den Rechner gebunden und dort unlesbar. Verschlüsseln Sie sie auf dem Zielrechner neu und nehmen Sie die `state.json` nicht mit.

Warum fehlen Geräte? Meist antworten sie nicht auf Ping. Weitere Gründe: IPv6, ein Bereich über 65 534 Adressen, ein Bereich, der nicht an seiner Netzadresse beginnt, oder mehr als 5000 Rechner in einem Bericht (Abschnitt 7).

Warum fehlt die MAC-Adresse? Das Gerät steht hinter einem Router. Die MAC kommt nur aus dem eigenen Segment des Collectors.

Ein Windows-Rechner hat kein Betriebssystem und keine Software – warum? Sehen Sie in *Details* nach `deep_scan` und `winrm_fehler.*`. Häufige Ursachen: kein Scan-Konto, Schalter aus, Kennwort im Klartext, WinRM am Ziel aus, fehlende Remoting-Rechte oder ein Ziel ohne passenden PTR-Eintrag, das nicht in *TrustedHosts* steht (Abschnitt 6.4).

Welche Software wird erfasst? Die maschinenweit installierten Programme (64 und 32 Bit) ohne Systemkomponenten. Nur für einen Benutzer installierte Programme fehlen.

Wird deinstallierte Software entfernt? Nein. Einträge bleiben mit ihrem alten *Zuletzt gesehen* stehen.

Was passiert, wenn die Zentrale ausfällt? Es laufen keine neuen Scans. Ein Bericht, der beim Senden scheiterte, wird nach dem nächsten Kontakt nachgereicht – auch mehrere, in ihrer zeitlichen Folge.

Woran sehe ich, dass ein Collector lebt? An *Zuletzt gesehen* – alle fünf Minuten erneuert. *Überfällig* erscheint erst nach dem doppelten Laufabstand (Abschnitt 9).

Welche Version hat ein Collector? Die Collector-Liste zeigt sie; der Collector meldet sie bei jedem Dienststart neu. Am Standort zeigt sie zusätzlich die Dateiversion der Programmdatei.

Kann ein Rechner mehrere Collector oder Mandanten bedienen? Nein. Ein Rechner, ein Collector, ein Mandant.

Geht es über einen Proxy? Einen eigenen Proxy-Schalter gibt es nicht.

Was ist der Unterschied zum Discovery-Scan und zur Netzsonde? Diese laufen im Serverdienst mit Zugängen aus dem Tresor und füllen den *Scan-Abgleich*. Der Collector läuft am Standort mit eigenen Zugängen und füllt das *Client-Inventar* (Abschnitt 1).

Wird ein Fund von selbst zum CI? Nein, erst durch *Übernehmen*. Danach hält jede Meldung das CI aktuell (Abschnitt 8).

Neue Funde erscheinen nicht. Das Client-Inventar lädt nach, sobald ein Collector-Bericht eintrifft. Erscheint trotzdem nichts, prüfen Sie *Letzter Lauf* in der Collector-Liste und das Collector-Protokoll.

Zwei Collector im selben Netz – was passiert? Jeder führt eigene Funde; dasselbe Gerät erscheint dann zweimal. Teilen Sie die Bereiche so auf, dass sie sich nicht überschneiden.

Läuft SNMP auch ohne Scan-Konto? Ja, wenn der Schalter an ist – ohne hinterlegtes Geheimnis mit der Gemeinschaft `public`.

Gilt der Zugang nach der Deinstallation weiter? Ja, bis Sie den Collector in der Zentrale sperren oder löschen (Abschnitt 12).

Ich habe versehentlich einen neuen Anmeldeschein ausgestellt – was nun? Der alte Zugang ist sofort widerrufen; der Collector meldet nichts mehr. Tragen Sie den neuen Schein in die `appsettings.json` ein (`EnrollmentToken`) und starten Sie den Dienst neu. Berichte, die in der Zwischenzeit entstanden sind, reicht er danach nach.

Ich finde die Protokolldatei nicht. Startmenü *Ordavis Collector — Protokoll* öffnet den richtigen Ordner (Abschnitt 11). Die Meldungen des Collectors stehen in `wartung-JJJJMMTT.log`.

Verwandte Themen

- ID-24 – Modul Discovery – Scans der Zentrale, Anmeldedaten-Tresor, Scan-Abgleich
- ID-50a – Update-System – wie Collector und alle anderen Komponenten aktualisiert werden

- ID-21 – Modul CMDB – was aus einem übernommenen Fund wird
- ID-23 – Modul Asset- & Vertragsmanagement – Lizenzzählung aus den erkannten Anwendungen
- ID-50 – Betriebshandbuch – Protokollablage und Zertifikate
- ID-54 – Kryptokonzept – Anmeldeschein, Zugang und DPAPI