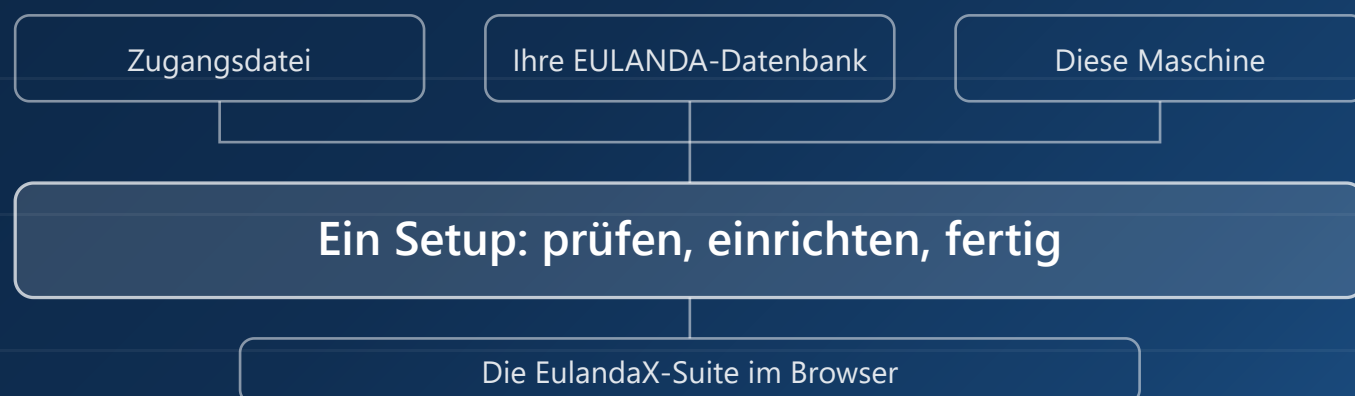


ADMINISTRATOR-HANDBUCH

EulandaX Setup



VERSION 1.0.18 · STAND 25.09.2026

Unbeaufsichtigt einrichten, Netz und Zertifikat, Wartung, Umzug, Störungen

Alles ohne Bildschirm

Jede Seite lässt sich über eine Antwortdatei beantworten - für die Fernwartung und für jede Wiederholung

Messen statt behaupten

Ob der Zugang von außen steht, sagt nur ein Anruf von draußen. Genau das tut die Prüfung

Ein Rückweg

Die Wartung nimmt zurück, was angelegt wurde - und lässt die Datenbank stehen

Inhalt

Über dieses Handbuch

- Was das Setup anlegt - die ganze Liste
- Die drei Aufgaben
- Das Dienstkonto und sein Kennwort
- Die Abschlussprüfung
- Alle Aufgaben auf einen Blick

Einrichtung ohne Rückfragen

- Die Antwortdatei
- Die Schalter
- Der Probelauf
- In der Konsole
- Ohne Internet, oder mit schlechtem

Netz, Zertifikat und Erreichbarkeit

- Die drei Stufen, technisch
- Der Weg zum Zertifikat
- Wenn der Dienst gerade nicht ausstellt
- Der Name gehört zur Lizenz
- Erneuerung
- Wenn es klemmt

Wartung

- Der Zustandsbericht
- Die Aktionen

Protokolle und Fehlerbilder

- Wo mitgeschrieben wird
- Das Protokoll lesen
- Fehlerbilder
- Wenn Sie uns schreiben

Die Prüfungen

- Die Maschine
- Netz
- Sicherheit
- Ausnahmen in Windows Defender
- Die Probe mit Dienstkonto und Aufgabe
- Mit Zugangsdatei
- Der Bericht

Über dieses Handbuch

Für den, der die Suite einrichtet, betreibt und im Störfall aufmacht. Es setzt voraus, dass Sie wissen, was eine Portweiterleitung ist und wo die Aufgabenplanung liegt; die Grundlagen stehen im Anwender-Handbuch.

Was das Setup anlegt - die ganze Liste

Wer eine fremde Maschine übernimmt, will zuerst wissen, was darauf eigentlich installiert wurde. Das ist die Antwort:

Was	Wo
PowerShell-Module	%ProgramFiles%\WindowsPowerShell\Modules
Stationsdatei	C:\ProgramData\Eulanda\XSuite\station.json
Startskript	C:\ProgramData\Eulanda\XSuite\Start-Xclient.ps1
Protokolle	C:\ProgramData\Eulanda\XSuite\logs
Aufgaben	\Eulanda\ in der Aufgabenplanung
Dienstkonto	Lokales Konto, Vorgabe EulandaXsvc
URL-Reservierung	netsh http show urlacl
Zertifikatsbindung	netsh http show sslcert
Firewall-Regel	Name beginnt mit EulandaX
Schema in der Datenbank	xrest und die Schemata der Plugins

Alles Eigene liegt unter \Eulanda - auch auf Ihrer Maschine. Das ist keine Kosmetik: in einer Aufgabenplanung mit hundert Einträgen in der Wurzel findet man fremde Software schlecht, und die Frage "was habt ihr hier eigentlich installiert" soll in drei Sekunden zu beantworten sein.

Die drei Aufgaben

Aufgabe	Wann	Wofür
\Eulanda\EulandaXclient	Beim Hochfahren, eine Minute verzögert	Der Server selbst. Die Verzögerung ist für den SQL Server
\Eulanda\EulandaXclient-Update	Vom Server angestoßen	Spielt neue Fassungen ein und nimmt zurück, wenn der neue Stand nicht antwortet
\Eulanda\EulandaXclient-Certificate	Täglich 03:30 plus Zufall	Erneuert das Zertifikat ab 30 Resttagen und meldet die aktuelle Adresse

Die dritte gibt es nur, wenn das Zertifikat von EULANDA stammt. Sie läuft **täglich**, obwohl ein Zertifikat 90 Tage hält - der Grund ist nicht das Zertifikat, sondern die Adresse: derselbe Lauf meldet, unter welcher Adresse die Maschine gerade zu erreichen ist. An einem Anschluss mit wechselnder Adresse ersetzt das DynDNS.

Hinweis. Der zufällige Versatz von bis zu einer Stunde ist Absicht. Tausend Installationen, die um Punkt 03:30 losliefen, wären für unseren Dienst eine Lastspitze mit Ansage.

Das Dienstkonto und sein Kennwort

Server und Zertifikatserneuerung laufen unter dem Dienstkonto `EulandaXsvc`, nicht unter dem Administrator, der eingerichtet hat. Das Konto gehört zu den Administratoren, weil der Update-Agent nach `C:\Program Files` schreibt und Aufgaben anlegt. Anmelden kann man sich damit weder am Bildschirm noch über Remotedesktop; erlaubt ist nur "Anmelden als Stapelverarbeitungsauftrag", also das Starten von Aufgaben.

Aufgabe	Läuft als	Anmeldung
<code>\Eulanda\EulandaXclient</code>	<code>EulandaXsvc</code>	mit Kennwort
<code>\Eulanda\EulandaXclient-Certificate</code>	<code>EulandaXsvc</code>	mit Kennwort
<code>\Eulanda\EulandaXclient-Update</code>	<code>EulandaXsvc</code>	S4U, legt der Server selbst an

Das Kennwort kennt niemand. Das Setup erzeugt es zufällig, setzt es dem Konto und gibt es beim Eintragen der Aufgaben an die Aufgabenplanung; die hält es verschlüsselt. Es steht in keiner Datei, keinem Protokoll und nicht in der Station, und es läuft nie ab.

Warum mit Kennwort und nicht S4U. S4U kommt ohne Kennwort aus, aber Windows 11 lässt einen Administrator eine solche Aufgabe nur für sich selbst anlegen, für ein anderes Konto antwortet es "Zugriff verweigert". Die Aufgabe des Update-Agenten ist der Fall "für sich selbst": der Server legt sie unter seinem eigenen Konto an, deshalb geht dort S4U.

Bei einem Update

Passiert mit Konto und Kennwort nichts. Der Update-Agent hält die Serveraufgabe an, spielt die neuen Module ein und startet dieselbe Aufgabe wieder; er trägt sie nicht neu ein und braucht das Kennwort nicht. Auch ein neues `setup.exe` fasst die Aufgaben nicht an, solange Sie nicht die Wartung aufrufen.

Wann das Kennwort neu gesetzt werden muss

Nur, wenn eine der beiden Aufgaben mit Kennwort nicht mehr anläuft:

- jemand hat das Kennwort von `EulandaXsvc` geändert, von Hand oder über eine Richtlinie,
- eine der Aufgaben wurde gelöscht,
- die Suite ist auf eine andere Maschine umgezogen.

Dann `setup.exe /maintenance` und **"Reparieren"**. Die Reparatur setzt dem Konto ein neues Zufallskennwort und trägt **beide** Aufgaben zusammen neu ein. Beide zusammen, weil ein neues Kennwort die ältere Aufgabe ungültig macht - würde nur eine neu eingetragen, bliebe die andere mit dem alten Kennwort stehen und lief beim nächsten Termin nicht an.

Achtung. Ändern Sie das Kennwort von `EulandaXsvc` nicht von Hand. Die Aufgaben laufen danach bis zum nächsten Neustart weiter und scheitern dann mit `LastTaskResult 0x8007052E` (Anmeldung fehlgeschlagen). Wer das Konto per Richtlinie zu einem Kennwortwechsel zwingt, muss danach die Wartung laufen lassen.

Voraussetzung für die Anmeldung mit Kennwort: die Richtlinie "Netzwerkzugriff: Speicherung von Kennwörtern und Anmeldeinformationen für die Netzwerkauthentifizierung nicht erlauben" ist deaktiviert (die Vorgabe von Windows). Ist sie aktiv, kann die Aufgabenplanung kein Kennwort halten, und das Setup bricht beim Eintragen mit genau diesem Hinweis ab.

Die Abschlussprüfung

Am Ende jeder Einrichtung misst das Setup noch einmal alles einzeln, statt den Schritten zu glauben: Station, die Aufgaben, die Zertifikatsbindung, die URL-Reservierung, die Firewall-Regel, die Module, das Startskript, die Zugangsdatei zur Datenbank, ob die Serveraufgabe gerade läuft und ob der SQL-Dienst läuft, den das Setup installiert hat. Es ist dieselbe Messung wie der Zustandsbericht der Wartung. Erst wenn sie keinen Fehler findet, gilt die Einrichtung als gelungen; jede Zeile steht auf der letzten Seite und im Protokoll.

Die Aufgabe des Update-Agenten fehlt dort manchmal noch - der Server legt sie erst beim Start an. Das ist ein Hinweis, kein Fehler.

Alle Aufgaben auf einen Blick

```
Get-ScheduledTask -TaskPath '\Eulanda\*' |  
    ForEach-Object { $_ | Get-ScheduledTaskInfo } |  
    Format-Table TaskName, LastRunTime, LastTaskResult, NextRunTime
```

`LastTaskResult` ist `0`, wenn der Lauf sauber endete. **Alles andere ist ein Fehler**, auch wenn die Aufgabe danach wieder auf `Ready` steht - eine gescheiterte Terminaufgabe sieht in der Aufgabenplanung genauso aus wie eine erfolgreiche.

Einrichtung ohne Rückfragen

Alles, was der Assistent kann, geht auch ohne Bildschirm. Das ist nicht nur für die Fernwartung da, sondern auch der Weg für den Umzug und für jede Wiederholung.

Die Antwortdatei

Eine JSON-Datei, in der je Seite steht, was auf ihren Feldern stehen soll. Der Aufbau folgt der Seitenfolge, nicht irgendeinem eigenen Format:

```
{
  "access": { "cnregPath": "C:\\Setup\\kunde.cnreg" },
  "database": { "mode": "existing", "udlPath": "C:\\Eulanda\\EULANDA_1 Firma.udl" },
  "modules": { "plugins": [ "EulandaXedi" ] },
  "network": { "reach": "B", "hostName": "firma.x.eulanda.eu", "port": 443,
    "certificate": "managed" },
  "admin": { "login": "admin", "name": "Administrator" },
  "summary": { "confirm": true }
}
```

Der Aufruf:

```
setup.exe /answers C:\\Setup\\antwort.json
```

Eine Seite kann auch einen ihrer Knöpfe drücken, etwa **Erweitert** auf der Willkommenseite:

```
{
  "welcome": { "action": "expert" },
  "expert": { "mode": "offline", "offlineFolder": "D:\\eulandax" }
}
```

Die Aktion gilt nur beim ersten Zeigen der Seite - ein **retry** dreht sonst mit derselben Antwortdatei endlos. Ein Knopf, den die Seite nicht hat, bricht mit einer Meldung ab.

Kein Kennwort gehört in diese Datei. Was fehlt, fragt der Assistent nach; im stillen Betrieb bricht er ab und sagt, welches Feld fehlt. Ein Konventionstest im Repo prüft, dass die Beispieldatei keine Felder mit **password** oder **pin** enthält - das soll auch nicht versehentlich entstehen.

Die Schalter

Schalter	Wirkung
<code>/answers <datei></code>	Antworten aus der Datei
<code>/quiet</code>	Ohne Fenster. Nur mit vollständigen Antworten sinnvoll
<code>/dryrun</code>	Alles fragen und prüfen, nichts verändern
<code>/maintenance</code>	Wartung statt Einrichtung
<code>/download <ordner></code>	Alles in den Ordner holen, nichts einrichten
<code>/offline <ordner></code>	Nur aus diesem Ordner nehmen, nie ins Netz sehen
<code>/log <datei></code>	Protokoll woanders hin
<code>/lang de en</code>	Sprache erzwingen
<code>/noupdate</code>	Nicht nach einer neueren Fassung sehen

Der Rückgabewert sagt, wie es ausging: `0` gelungen, `1` gescheitert, `1602` abgebrochen.

Der Probelauf

`/dryrun` ist der Schalter, den man am häufigsten braucht und am seltensten kennt. Er geht alle Seiten durch, **prüft alles** - die Systemvoraussetzungen, die Zugangsdatei, die Datenbank, ihre Fassung, die Rechte - und hört vor der Installation auf.

Bei einer fremden Maschine ist das der erste Aufruf, nicht der letzte: er beantwortet die Frage, ob eine Einrichtung überhaupt durchlaufen würde, ohne etwas anzufassen.

In der Konsole

Ohne `setup.exe` geht es auch. Im entpackten Paket liegt `setup.ps1` :

```
.\setup.ps1 -AnswerFile C:\Setup\antwort.json
.\setup.ps1 -Interactive           # fehlende Werte als Konsolenfrage
```

Das braucht eine **erhöhte Windows PowerShell 5.1**. Der Weg ist für die Fernwartung gedacht, bei der kein Fenster durchkommt.

Ohne Internet, oder mit schlechtem

Auf einer Leitung, die alle paar Minuten abreißt, ist ein Lauf, der zwischendurch vierzig Dateien holt, ein Glücksspiel. Ein Lauf, der nur noch aus einem Ordner liest, nicht.

Beides geht ohne Befehlszeile: der Knopf **Erweitert** auf der Willkommenseite führt zu *Nur herunterladen* und *Ohne Internet einrichten* (Anwender-Handbuch, Kapitel Starten). Startet `setup.exe` aus einem Download-Ordner, schlägt die Seite *Ohne Internet* schon vor. Die Schalter unten tun dasselbe und bleiben für Skripte und die Fernwartung.

Einmal alles holen

Auf einer Maschine **mit** Internet:

```
setup.exe /download D:\eulandax
```

Das ändert an dieser Maschine **nichts** - es lädt nur. Danach liegt im Ordner:

D:\eulandax\setup.exe	das Programm selbst
D:\eulandax\xsuite.zip	sein Paket
D:\eulandax\modules\<Modul>\<Fassung>\<Modul>.zip	alle Module
D:\eulandax\offline.json	was drin ist, von wann
D:\eulandax\access\cneulreg.txt	Lizenz der Klassik (mit Zugangsdatei)
D:\eulandax\access\catalog.json	Download-Schlüssel (mit Zugangsdatei)
D:\eulandax\access\<Kunde>-<Nr>.eullic	EulandaX-Lizenzblock (mit Zugangsdatei)

Den Unterordner `access` füllt die Zugangsdatei: der Lauf holt über sie über HTTPS vom Lizenzserver, was die Einrichtung später braucht. Ohne Internet erreicht die Zielmaschine den Lizenzserver nicht; mit dem Ordner ist die Seite *Zugang* dort schon ausgefüllt. **Der Ordner trägt damit Lizenz und Download-Schlüssel des Kunden** - nicht aus der Hand geben.

Geholt werden **alle** Plugins des Katalogs, nicht nur die voreingestellten: ein Stick, auf dem ausgerechnet das eine Modul fehlt, das der Kunde dazugekauft hat, ist die Reise nicht wert.

Ohne Zugangsdatei bleiben die geschützten Module außen vor. Der Lauf sagt das und lädt den offenen Teil trotzdem.

Auf der Zielmaschine

Den Ordner mitnehmen und `setup.exe` **aus diesem Ordner** starten. Mehr ist nicht zu tun: das Setup sucht neben sich selbst, bevor es ins Netz sieht.

Lage	Was passiert
Modul liegt lokal, gleiche Fassung	Es wird genommen, nichts geladen
Modul liegt lokal, online ist eine neuere	Die neuere wird geladen
Netz klemmt, Modul liegt lokal	Die lokale wird genommen, mit einem Hinweis im Protokoll
Netz klemmt, Modul fehlt lokal	Abbruch mit klarer Meldung

Der Vorrat ist also **kein Ersatz für den aktuellen Stand**, sondern ein Rückfall. Wer das nicht will - etwa auf einer Maschine ganz ohne Internet, wo jeder Versuch nur die Zeitgrenze kostet - sagt es ausdrücklich:

```
setup.exe /offline D:\eulandax
```

Dann wird gar nicht erst ins Netz gesehen - oder eben **Erweitert**, *Ohne Internet einrichten*. Die Systemprüfung zeigt dann statt des roten Punkts "files.eulanda.eu nicht erreichbar" eine Hinweiszeile: ohne Internet ist das fehlende Netz kein Befund. Auf dem normalen Weg bleibt es rot, und der Hinweis nennt diesen Ausweg.

Achtung. Ein Paket vom Stick ist kein vertrauenswürdiges Paket. Signatur und Herausgeber werden genauso geprüft; ein Paket, dessen Signatur nicht stimmt, wird auch offline abgewiesen.

Praxis. Der Ordner `modules` hat **dieselbe Form wie der Zwischenspeicher** des Setups. Das ist kein Zufall: es gibt kein zweites Format, keinen Umpackschritt und keine Stelle, an der beides auseinanderlaufen kann.

Netz, Zertifikat und Erreichbarkeit

Die drei Stufen, technisch

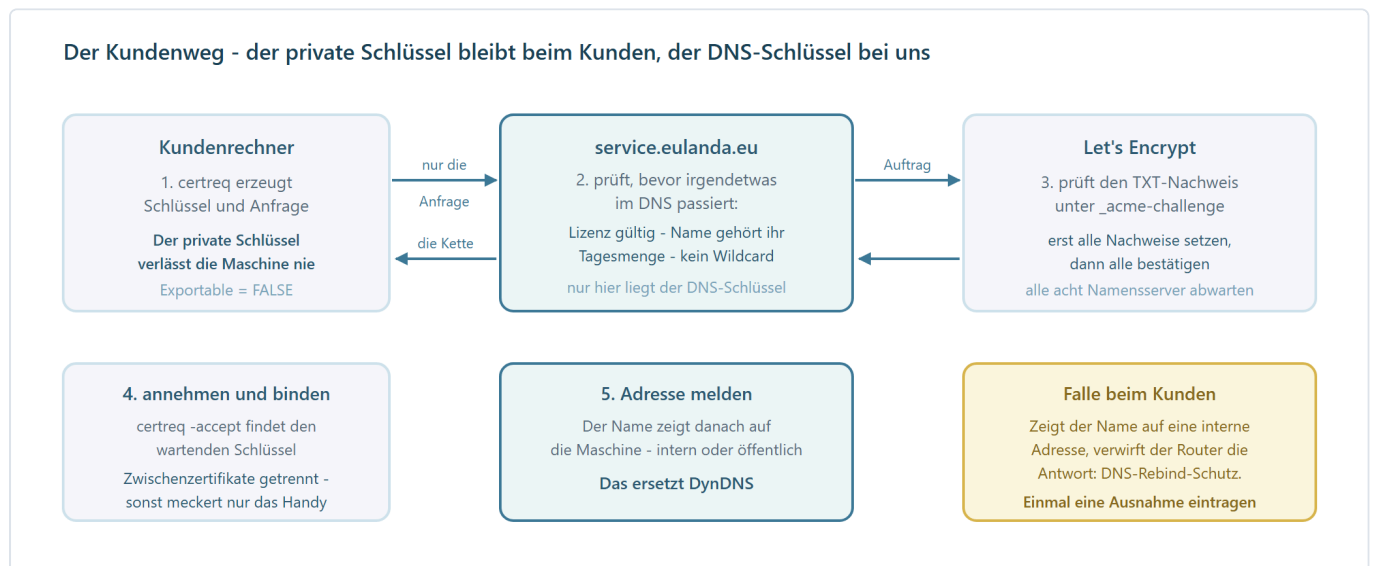
Stufe	Bindung	Firewall	Zertifikat
A - nur diese Maschine	localhost , HTTP	keine Regel	keines
B - Hausnetz	Hostname:443, HTTPS	Regel für Domäne und Privat	nötig
C - auch von außen	dito	dito, dazu Weiterleitung am Router	nötig

Die Firewall-Regel wird **port- und profilgenau** gesetzt, nie pauschal für alle Profile und nie als Programmfreigabe. Der SQL-Port bleibt zu.

Achtung. Bei Stufe B und C wird das Profil "Öffentlich" **nicht** geöffnet. Wer die Suite in einem Netz betreibt, das Windows als öffentlich einstuft, hat ein Netzproblem, kein Firewall-Problem.

Der Weg zum Zertifikat

Das Zertifikat von EULANDA entsteht so - und es lohnt sich, den Weg einmal gesehen zu haben, weil sich daraus alle Fehlerbilder erklären:



Vom Antrag zum gebundenen Zertifikat

1. **Schlüssel und Anfrage entstehen auf Ihrer Maschine** (certreq). Der private Schlüssel verlässt sie nie und ist als nicht exportierbar angelegt.
2. Nur die **Anfrage** geht an service.eulanda.eu .
3. Der Dienst prüft: Gibt es die Lizenz? Gehört der Name dieser Lizenz? Ist die Tagesmenge eingehalten?
4. Erst dann setzt **er** den Nachweis im DNS und lässt ausstellen.
5. Die Kette kommt zurück, wird angenommen und gebunden.

6. Zum Schluss meldet Ihre Maschine ihre Adresse - der Name zeigt danach auf sie.

Der Punkt, auf den es ankommt: **der Schlüssel, mit dem im DNS geschrieben wird, liegt nicht bei Ihnen.** Er gilt für unser ganzes Konto, und deshalb kommt er auf keine Kundenmaschine. Ihre Maschine bittet, sie schreibt nicht selbst.

Wenn der Dienst gerade nicht ausstellt

Das kommt vor: der Dienst antwortet "Service busy; retry later", oder er ist im Moment der Einrichtung nicht erreichbar. Die Einrichtung bleibt deswegen nicht stehen. Sie bindet ein **selbstsigniertes Zertifikat als Notbehelf**, damit der Server läuft, und merkt sich in der Station, dass das echte noch aussteht. Auf der letzten Seite steht dazu eine Warnzeile.

Was dann von allein passiert:

- Die tägliche Aufgabe `\Eulanda\EulandaXclient-Certificate` wird angelegt wie sonst auch.
- Sie erkennt beim nächsten Lauf, dass nur der Notbehelf gebunden ist - ein selbstsigniertes Zertifikat stellt sich selbst aus - und holt das echte nach, ohne auf Restlaufzeiten zu warten.
- Mit dem echten Zertifikat kommt auch die Meldung der Adresse, und damit steht der Name im DNS.

Warten müssen Sie darauf nicht: **Wartung, "Zertifikat erneuern"** versucht es sofort noch einmal.

Woran Sie den Notbehelf erkennen: Aussteller und Inhaber sind derselbe Name, und die Laufzeit beträgt fünf Jahre statt 90 Tagen.

```
Get-ChildItem Cert:\LocalMachine\My |  
  Where-Object { $_.Subject -eq $_.Issuer } |  
  Select-Object Subject, NotAfter
```

Solange er gebunden ist, zeigt jeder Browser eine Warnung, und der Name zeigt noch auf nichts.

Der Name gehört zur Lizenz

Vergeben wird er von uns, wenn die Lizenz entsteht. Er steht im Lizenzbuch, und der Dienst gibt nur für ihn ein Zertifikat aus. Wollen Sie einen anderen, ändern wir ihn - das ist ein Handgriff bei uns, kein Einstellwert auf Ihrer Maschine.

Erneuerung

Täglich, ab 30 Resttagen. Bei 90 Tagen Laufzeit bleibt damit ein Monat Luft für Störungen. Die eine Ausnahme ist der Notbehelf von oben: ein selbstsigniertes Zertifikat wird sofort ersetzt, egal wie lange es noch gälte.

Nachsehen lässt sich das so:

```
Get-ChildItem Cert:\LocalMachine\My |  
Where-Object { $_.Subject -like '*ihrefirma*' } |  
Select-Object Subject, NotAfter, Thumbprint
```

Und was wirklich ausgeliefert wird - das ist die Frage, auf die es ankommt:

```
netsh http show sslcert
```

Praxis. Nicht das Zertifikat im Speicher zählt, sondern die **Bindung**. Ein abgelaufenes Zertifikat im Speicher schadet nie; eine Bindung darauf schon. Wer prüft, prüft die Bindung.

Wenn es klemmt

Symptom	Ursache
Von außen geht es, von innen nicht	DNS-Rebind-Schutz im Router
Handy meldet "nicht vertrauenswürdig", PC nicht	Zwischenzertifikate fehlen
"Es antwortet niemand"	Keine Weiterleitung, Pakete werden verworfen
"Es antwortet jemand, aber nichts horcht"	Weiterleitung steht, Server läuft nicht
Fingerabdruck stimmt nicht	Die Weiterleitung zeigt auf ein anderes Gerät
Browser warnt, Name zeigt auf nichts	Der Dienst konnte bei der Einrichtung nicht ausstellen; der Notbehelf ist gebunden (siehe oben)
Prüfung endet sofort mit CGNAT	Geteilter Anschluss. Keine Weiterleitung möglich

Der vorletzte Fall ist der, den man ohne Prüfung sehr lange sucht: die Weiterleitung steht, aber auf dem falschen Gerät im Haus. Von außen antwortet dann etwas - nur nicht die Suite.

Der letzte ist der ärgerlichste, weil kein Herumstellen hilft: bei einem Anschluss hinter CGNAT teilt sich Ihr Anschluss die öffentliche Adresse mit anderen Kunden. Da geht nur Stufe B - oder ein Tarif mit eigener Adresse.

Wartung

```
setup.exe /maintenance
```

Dasselbe Programm auf einer Maschine, auf der die Suite schon läuft. Der Ablauf ist eine **Schleife**: messen, wählen, tun, wieder messen. Nach einer Reparatur will man sehen, ob sie gewirkt hat, und das sagt nur eine neue Messung.

Der Zustandsbericht

Steht immer oben, vor jeder Wahl. Er vergleicht die Stationsdatei - was eingerichtet **wurde** - mit dem, was heute **da ist**. Dazwischen liegen Monate, ein Update, vielleicht ein Virens Scanner und jemand, der in der Aufgabenplanung aufgeräumt hat.

Gemessen wird jedes Stück einzeln, weil jedes einzeln fehlen kann: Aufgaben, Bindung, URL-Reservierung, Firewall, Module, Startskript, Zugangsdatei.

Die Aktionen

Aktion	Was sie tut
Reparieren	Legt wieder an, was fehlt - und fasst nichts an, was steht
Zertifikat erneuern	Holt ein frisches, bindet und startet den Server neu
Erreichbarkeit prüfen	Lässt von außen anrufen, dazu die Anleitung zur Weiterleitung
Plugin nachinstallieren	Holt ein dazugekauftes Modul, registriert es, startet neu
Umzug vorbereiten	Schreibt eine Antwortdatei für die neue Maschine
Deinstallieren	Nimmt zurück, was der Setup angelegt hat

Reparieren

Arbeitet genau die Befunde ab, die der Bericht meldet. Es ist **kein zweiter Einrichtungslauf**: Datenbank, Schema, Mandant, Lizenz und Benutzer werden nicht angefasst.

Zwei Dinge tut es bewusst nicht:

- **Ein fremdes Zertifikat wird nicht ersetzt.** Ein gekauftes Zertifikat durch unseres zu tauschen ist eine Entscheidung, kein Reparaturfall.
- **Die Agent-Aufgabe wird nicht nachgebaut.** Die legt der Server beim nächsten Start selbst an; sonst gäbe es zwei Stellen, die dasselbe tun.

Fehlt die Serveraufgabe oder die Zertifikatsaufgabe, bekommt das Dienstkonto ein neues Zufallskennwort, und die Reparatur trägt **beide** Aufgaben damit neu ein (Kapitel 1, "Das Dienstkonto und sein Kennwort"). Das

ist der Weg nach einem geänderten Kennwort, einer gelöschten Aufgabe oder einem Umzug.

Praxis. Eine Reparatur, die vorsichtshalber alles neu macht, ist gefährlicher als der Schaden: sie wirft eine funktionierende Bindung weg und hofft, dass die neue klappt.

Zertifikat erneuern

Erneuert **ohne Rücksicht auf die Restlaufzeit** - wer hier drückt, hat einen Grund. Startet den Server danach neu, weil http.sys sonst das alte Zertifikat weiter ausliefert.

Umzug

Es gibt keine eigene Einlesemaschinerie, und das ist Absicht: umziehen heißt dieselbe Datenbank, dieselbe Lizenz, derselbe Name auf einem anderen Rechner - also eine ganz normale Einrichtung mit feststehenden Antworten. Die Aktion schreibt deshalb eine **Antwortdatei**, und auf der neuen Maschine läuft der gewöhnliche Weg.

Kein Geheimnis geht mit, und das ist keine Vorsicht, sondern Physik: die Station schützt Schlüssel und PIN über DPAPI, und das ist an die Maschine gebunden. Auf dem Zielrechner wären die Werte ohnehin nicht zu entschlüsseln.

Geheimnis	Was auf der neuen Maschine passiert
ApiKey des App-Servers	Wird beim Einrichten erneuert
Pairing-PIN	Wird neu vergeben - die Geräte koppeln sich einmal neu

Wollen Sie das vermeiden, tragen Sie auf der neuen Maschine dieselbe PIN ein. Sie steht absichtlich nicht in der Datei.

Achtung. Die alte Maschine erst abschalten, wenn die neue läuft. Beide gleichzeitig am selben Mandanten sind kein Unglück, aber zwei Server unter demselben Namen sind einer zu viel - der DNS-Eintrag zeigt nur auf einen.

Deinstallieren

Der Rückweg. Entfernt wird in dieser Reihenfolge, und sie ist nicht beliebig: zuerst die Aufgaben (sonst startet der Server mitten im Abräumen neu), dann Bindung und Reservierung, dann die Firewall-Regeln, dann Startskript und Station.

Was stehen bleibt, und warum:

Bleibt	Grund
Das Schema in der Datenbank	Dort liegen die Daten. Eine Deinstallation, die eine Datenbank leert, ist keine Deinstallation
Das Dienstkonto	Kann anderswo Rechte haben; ein gelöschttes Konto ist nicht zurückzuholen
Das Zertifikat im Speicher	Läuft von selbst ab. Gefährlich ist nie das Zertifikat, sondern die Bindung
Die Module	Nur auf ausdrücklichen Wunsch. Eine zweite Installation braucht sie vielleicht

Die Seite zeigt erst, was wegginge, und fragt dann. Ein Fehlschlag hält die übrigen Schritte nicht auf: wer deinstalliert, will am Ende wenig Rest, nicht einen Abbruch in der Mitte.

Protokolle und Fehlerbilder

Wo mitgeschrieben wird

Datei	Was drinsteht
C:\ProgramData\Eulanda\XSuite\logs\setup-*.log	Jeder Schritt der Einrichtung mit Zeitstempel
C:\ProgramData\Eulanda\XSuite\logs\host-*.log	Was setup.exe selbst tat: Paket, Signatur, Selbstaktualisierung
%ProgramData%\Eulanda\EulandaXclient\log\	Der laufende Server
C:\ProgramData\Eulanda\cert\renewal.log	Nur auf unseren eigenen Servern

Kein Geheimnis steht in einem Protokoll. Schlüssel, PIN und Kennwörter werden vor dem Schreiben ersetzt. Sie können die Datei deshalb bedenkenlos mitschicken - und genau dafür ist sie da.

Das Protokoll lesen

Jede Zeile beginnt mit Zeitstempel und Stufe. Für den Anfang reicht:

```
Get-Content C:\ProgramData\Eulanda\XSuite\logs\setup-*.log |  
Select-String -Pattern 'ERROR|WARN' | Select-Object -Last 20
```

Wenn ein Schritt gescheitert ist, steht die Ursache **in der Zeile darüber**, nicht in der Fehlermeldung selbst: die sagt, was nicht ging, die Zeile davor sagt, was gerade versucht wurde.

Fehlerbilder

Die Einrichtung bricht bei der Systemprüfung ab

Fast immer ein **ausstehender Neustart**. Windows hat ein Update halb eingespielt; der SQL Server lässt sich in diesem Zustand nicht installieren. Neu starten, Setup wieder aufrufen.

"Der Zugang ließ sich nicht lesen"

Die `.cnreg` gehört zu einer anderen Lizenz, oder sie ist beim Übertragen beschädigt worden. Prüfen Sie die Dateigröße gegen das, was wir geschickt haben - eine per Mail durchgereichte Datei ist gelegentlich umkodiert worden.

Die Migration scheitert

Dann wurde **nicht migriert**. Vor der ersten Änderung legt das Setup eine Sicherung an; scheitert die Sicherung, hört es auf. Das ist Absicht - lieber keine Suite als ein halb geändertes Schema ohne Rückweg.

Häufigste Ursache: kein Platz auf dem Laufwerk, auf dem der SQL Server seine Sicherungen ablegt.

"Die Platte meldet ... Byte je Sektor"

Manche NVMe-Platten melden unter Windows 11 mehr als 4 KB je Sektor. SQL Server kommt damit nicht zurecht: die Installation hängt lange oder der Dienst startet nicht. Richtet das Setup einen eigenen SQL Server ein, prüft es das vorher. Bei einer zu großen Sektorgröße setzt es den Registry-Eintrag, den Microsoft dafür vorsieht (`HKLM\SYSTEM\CurrentControlSet\Services\storndvme\Parameters\Device , ForcedPhysicalSectorSizeInBytes = * 4095`), und hält an: der Eintrag wirkt erst nach einem **Neustart**. Danach das Setup noch einmal aufrufen, es macht dort weiter.

Meldet die Platte auch nach dem Neustart zu große Sektoren, hängt sie an einem Treiber des Herstellers statt am NVMe-Treiber von Windows; dann wirkt der Eintrag nicht. Abhilfe: den Treiber von Windows verwenden, den SQL Server auf einer anderen Platte einrichten oder eine vorhandene Instanz wählen.

Die Systemprüfung zeigt den Befund vorab als Hinweiszeile. Mit einer vorhandenen Datenbank auf einem anderen Server betrifft er die Einrichtung nicht.

Der Server startet nicht

```
Get-ScheduledTask -TaskPath '\Eulanda\' -TaskName 'EulandaXclient' | Get-ScheduledTaskInfo
```

`LastTaskResult` ungleich `0` ist der Hinweis. Die häufigsten Gründe:

Grund	Woran man es sieht
Port belegt	<code>netsh http show servicestate</code> zeigt einen fremden Belegten
URL-Reservierung fehlt	Der Server meldet "Zugriff verweigert" beim Binden
Zertifikat weg	Die Bindung zeigt auf einen Fingerabdruck, den es nicht mehr gibt
Datenbank nicht erreichbar	Der SQL Server war beim Start noch nicht oben
Kennwort des Dienstkontos geändert	<code>LastTaskResult</code> <code>0x8007052E</code> ; Wartung, "Reparieren" setzt ein neues und trägt beide Aufgaben neu ein

Der letzte Fall erklärt die Minute Verzögerung in der Aufgabe. Startet Ihr SQL Server langsamer, erhöhen Sie sie.

Ein Update hat etwas kaputtgemacht

Hat es vermutlich nicht: der Agent prüft nach dem Neustart, ob der Server wieder antwortet, und **nimmt zurück**, wenn nicht. Im Protokoll des Agenten steht, was er getan hat.

Was wirklich vorkommt: der Agent wartet auf die Warteseite und die dauert länger als sonst, weil der Mandant gewachsen ist. Das ist kein Fehler, sondern eine Frist, die knapp wird.

Der Virens Scanner schlägt an

Kommt vor, und wir haben die Ursache 2026 ausgeräumt. Der Vollständigkeit halber, damit Sie wissen, wonach Sie suchen.

PowerShell konnte bis dahin bei bestimmten Aufrufen den C#-Compiler des Systems starten. Der legt eine unsignierte Programmbibliothek im Temp-Ordner ab und lädt sie sofort - von außen sieht das aus wie ein Schadprogramm, das sich nachlädt. Manche Scanner haben daraufhin Prozesse blockiert oder ganze Dateien in Quarantäne genommen. Bei Windows PowerShell 5.1 trat das auf, bei PowerShell 7 nicht.

Seit September 2026 tut die X-Suite das nicht mehr: beim Laden der Module startet kein Compiler, und die wenigen verbliebenen Stellen laufen erst, wenn man die betreffende Funktion wirklich benutzt.

Wenn Ihr Scanner trotzdem anschlägt:

1. Sehen Sie in seiner Quarantäne nach, **welche Datei** er genommen hat. Ist es eine Datei aus dem Modulordner oder das `setup.exe`, schicken Sie uns den Namen - alles, was wir ausliefern, ist mit einem EV-Zertifikat auf die EULANDA Software GmbH signiert, und einen Fehlalarm auf eine signierte Datei melden wir dem Hersteller.
2. Ist es eine Datei im Temp-Ordner, sagen Sie uns bitte trotzdem Bescheid. Dann haben wir eine Stelle übersehen.
3. **Nehmen Sie den Virens Scanner nicht herunter.** Eine Ausnahme für den Modulordner ist das mildere Mittel und reicht in allen Fällen, die wir gesehen haben.

Prüfen, ob die Signatur intakt ist, können Sie selbst - Rechtsklick auf die Datei, `Eigenschaften`, `Reiter Digitale Signaturen`. Steht dort EULANDA Software GmbH und meldet Windows die Signatur als gültig, ist die Datei die, die wir gebaut haben.

Microsoft Defender meldet `Trojan:PowerShell/DownloadObfus.A!MTB`

Ein Fehlalarm beim **ersten** Laden von EulandaXrest auf einer Maschine, gesehen im September 2026 auf einem frischen Windows 11 in etwa jedem zweiten Lauf. Defender bewertet eine unbekannte Datei beim ersten Kontakt über seine Cloud ("Block at first sight") und blockiert so lange; nach gut 20 Sekunden steht das Urteil fest, und dieselbe signierte Datei lädt ohne Beanstandung. In der Quarantäne steht sie als `amsi:...\\EulandaXrest.psm1`, sie wird nicht gelöscht.

Das Setup fängt das selbst ab: im Protokoll steht "Microsoft Defender prüft EulandaXrest noch ... neuer Versuch in 30 Sekunden", und nach bis zu sechs Versuchen geht es weiter. Bricht es trotzdem ab, starten Sie es in einigen Minuten noch einmal. Einen einzelnen Auslöser im Code gibt es nicht; das Modell zählt viele unscheinbare Merkmale zusammen. Melden Sie uns den Fall, wir reichen die signierte Datei bei Microsoft als Fehlalarm ein.

Nichts von alledem

Dann `setup.exe /maintenance`. Der Zustandsbericht sagt in zwanzig Zeilen, was da ist und was fehlt - und das ist meist schneller als jede Suche im Protokoll.

Wenn Sie uns schreiben

Drei Dinge, und wir können sofort antworten:

1. Das Protokoll aus `logs\` .
2. Die Ausgabe des Zustandsberichts aus der Wartung.
3. Was Sie erwartet haben und was stattdessen passiert ist.

Der dritte Punkt ist der wichtigste und wird am häufigsten vergessen.

Die Prüfungen

Das Setup prüft eine Maschine, bevor es etwas anfasst. Dieselben Prüfungen laufen im Modus **Nur prüfen** (Erweitert auf der ersten Seite): dann ohne Installation und mit einem Bericht auf dem Desktop. Es gibt also nur eine Wahrheit, und die Checkliste im Anwender-Handbuch lässt sich damit vor dem Termin belegen.

Die Liste unten sagt zu jeder Zeile, was sie prüft, warum, und was bei Gelb oder Rot zu tun ist. Rot verhindert die Einrichtung, Gelb ist ein Hinweis.

Die Maschine

Zeile	Prüft	Warum	Bei Rot oder Gelb
Windows	Build ab 14393 (Windows 10, Server 2016)	Ältere Fassungen können TLS 1.2 und die nötigen PowerShell-Befehle nicht zuverlässig	Nur eine neuere Maschine hilft
Administratorrechte	Läuft das Setup erhöht	Es legt Konto, Aufgaben, Firewall-Regel und Zertifikatsbindung an	Rechtsklick, Als Administrator ausführen
PowerShell	Windows PowerShell 5.1, 64 Bit	Der Server der Suite läuft später genau darin	64-Bit- <code>powershell.exe</code> nehmen
.NET	Release 461808 (4.7.2) oder höher	TLS 1.2 und die Kryptografie der Suite	.NET 4.8 über Windows Update
Ausführungsrichtlinie	Keine Gruppenrichtlinie <code>Restricted</code>	Die Module sind Skripte; signiert, aber Skripte	Richtlinie auf <code>AllSigned</code> oder <code>RemoteSigned</code> ; bei <code>AllSigned</code> den Herausgeber EULANDA Software GmbH vertrauen
Platz	Freier Platz auf dem Laufwerk der Programme	Module, Zwischenspeicher, Sicherung vor jeder Migration	Mindestens 2 GB, besser 5 GB freigeben
Neustart	Wartet Windows auf einen Neustart	Die Installation eines SQL Servers scheitert sonst	Vorher neu starten
Browser	Gibt es Edge, Chrome oder Firefox	Die Suite läuft im Browser, aber nicht im Internet Explorer, der auf Servern oft noch Standard ist. Den Prüfbericht öffnet das Setup deshalb ausdrücklich mit einem dieser Browser	Gelb: Edge oder Chrome installieren, wenn die Suite am Server bedient wird

Zeile	Prüft	Warum	Bei Rot oder Gelb
files.eulanda.eu	HTTPS mit TLS 1.2	Von dort kommen die Module	Ausgehendes HTTPS auf 443 freigeben, oder über Erweitert ohne Internet einrichten
Aktivierungsdienst	service.eulanda.eu auf 443	Lizenz, Zugangsdateien, Zertifikat und DNS-Eintrag kommen von dort; ohne ihn gibt es nur ein selbstsigniertes Zertifikat	Ausgehendes HTTPS zu service.eulanda.eu freigeben
Port 443	Lauscht ein anderes Programm auf 443	Die Suite braucht einen Port; lauscht nur http.sys (etwa ein IIS), geht es nebeneinander	Gelb: auf der Seite Netz einen anderen Port wählen, etwa 8443
hosts-Datei	Lässt sie sich zum Schreiben öffnen (ohne dass etwas geändert wird)	Sie ist der Rückweg, wenn der DNS im Haus unsere Antwort verwirft	Meist sperrt ein Virenschutz sie; im Notfall den Eintrag von Hand setzen
Rebind-Schutz	Ein fester Prüfname unserer Zone mit privater Adresse: kennt ihn der öffentliche DNS (1.1.1.1), der örtliche aber nicht?	Der Name der Suite zeigt auf eine interne Adresse. Viele Router und DNS-Weiterleiter verwerfen genau solche Antworten - dann ist die Suite im Haus nicht erreichbar, obwohl alles stimmt	Bedingte Weiterleitung für x.eulanda.eu am Domänencontroller, Ausnahme im Router, oder am Server ein Eintrag in der hosts-Datei. Ist der Router eine Fritz!Box (erkannt über http://<Gateway>:49000/tr64desc.xml oder fritz.box), nennt der Hinweis den genauen Weg zu den Hostnamen-Ausnahmen

Von Hand prüft das jeder Admin mit einer Zeile, ohne Setup, ohne Lizenz und lange vor dem Termin:

```
if ((Resolve-DnsName rebind-probe.x.eulanda.eu -Type A -DnsOnly -ErrorAction SilentlyContinue).IPAddress -contains '10.99.99.99') { 'OK: kein Rebind-Schutz' } else { 'GESPERRT: der DNS im Haus verwirft private Adressen' }
```

-DnsOnly lässt die hosts-Datei aus, gefragt wird wirklich der DNS im Haus. Ist nach einer Abhilfe per hosts-Eintrag nur der Server selbst versorgt, zeigt die Zeile weiter GESPERRT - die Arbeitsplätze brauchen dann die bedingte Weiterleitung oder die Ausnahme im Router.

Sicherheit

Zeile	Prüft	Warum	Bei Gelb
Virenschutz für PowerShell	Welche Programme sich als AMSI-Anbieter in PowerShell einhängen	Jedes Skript geht vor dem Ausführen an alle Anbieter. Ein EDR wie CrowdStrike Falcon kann Module der Suite sperren und sogar löschen, ohne dass Windows Defender etwas zeigt	Beim Betreuer dieses Virenschutzes vorab eine Ausnahme einrichten: <code>C:\ProgramData\Eulanda**</code> und <code>C:\Program Files\WindowsPowerShell\Modules\Eulanda**</code> , oder für den Signaturgeber EULANDA Software GmbH. Keine Freigabe einzelner Hashes, die Module ändern sich mit jedem Update

Bei CrowdStrike Falcon (schon erlebt: die Ausnahme stand, das Modul wurde trotzdem gelöscht) zwei Dinge klären: in der Falcon-Konsole die Erkennung zur Datei suchen - dort steht, welcher Mechanismus greift (Machine Learning, IOA, Script-Based Execution Monitoring), und die Ausnahme muss für genau diesen gelten. Und Pfadmuster schreibt Falcon nach unserem Kenntnisstand **ohne Laufwerksbuchstaben**:

`\ProgramData\Eulanda\**` und `\Program Files\WindowsPowerShell\Modules\Eulanda\**`. Die Zeile sagt nur, **wer** sich einhängt. Ob er unsere Module wirklich sperrt, misst in *Nur prüfen* die **Ladeprobe**: sie holt EulandaXtools und EulandaXcrypt in den Zwischenspeicher, lädt sie in einem eigenen PowerShell-Prozess und sieht danach nach, ob die Dateien noch da sind. Rot heißt: gesperrt oder gelöscht, mit dem Namen des Anbieters. So lässt sich auch prüfen, ob eine Ausnahme wirkt, ohne eine Installation anzufangen.

Sperrt ein Virenschutz trotzdem ein Modul, bricht das Setup mit einer Meldung ab, die den Anbieter beim Namen nennt. Wartet es, dann nur bei Windows Defender: dessen erstes Urteil über eine neue Datei kann eine halbe Minute dauern und fällt danach oft anders aus. Ein anderer Wächter sperrt jedes Mal gleich, dort wäre Warten verlorene Zeit.

Ausnahmen in Windows Defender

Auf der Seite *Umfang* steht der Haken **Ausnahmen in Windows Defender für die Module der Suite einrichten**, vorgegeben ein. Als Schritt gleich nach der Probe mit Dienstkonto und Aufgabe setzt das Setup dann genau diese Ausnahmen, nicht mehr:

Pfad	Warum
<code>C:\Program Files\WindowsPowerShell\Modules\Eulanda*</code>	dort laufen die Module, der Update-Agent spielt dorthin ein
<code>C:\ProgramData\Eulanda\Xsetup\cache\modules\Eulanda*</code>	Zwischenspeicher des Setups
<code>C:\ProgramData\Eulanda\EulandaXclient\update</code>	Zustand und Pakete des Update-Agenten
<code>C:\ProgramData\Eulanda\XSuite\Start-Xclient.ps1</code>	Startskript des Servers

Der Platzhalter `Eulanda*` trifft nur Ordner, die so beginnen - andere Module im selben Ordner bleiben geprüft. Dass eine Pfadausnahme auch beim Laden eines Moduls über AMSI wirkt und der Platzhalter so eng

greift, ist in der Test-VM mit dem AMSI-Testtext von Microsoft geprüft (24.09.2026).

- Ist Defender nicht der aktive Virenschutz, setzt das Setup nichts und sagt es.
- Verbietet eine Gruppenrichtlinie lokale Ausnahmen, meldet der Schritt das gelb, und die Einrichtung läuft weiter.
- Die Wartung nimmt die Ausnahmen zusammen mit den Modulen wieder heraus; solange die Module liegen, bleiben auch die Ausnahmen.
- Nachsehen: `(Get-MpPreference).ExclusionPath`.

Die Probe mit Dienstkonto und Aufgabe

Die Suite läuft als Aufgabe unter einem lokalen Konto (`EuLandaXsvc`) mit Kennwort und höchsten Rechten. In einer Domäne kann eine Gruppenrichtlinie genau das verbieten: lokale Konten, die Aufnahme in die Administratoren oder das Recht **Anmelden als Batchauftrag** (Ergebnis `0x80070569`). Ohne Probe zeigte sich das erst mitten in der Installation.

Die Probe legt das Konto `XsetupProbe` an, nimmt es in die Administratoren auf, registriert unter `\EuLandaProbe\` eine Aufgabe mit seinem Kennwort und höchsten Rechten, führt sie einmal aus und entfernt danach Aufgabe, Ordner und Konto - auch wenn ein Schritt scheitert.

- **Bei der Einrichtung** ist sie der erste Schritt nach **Installieren**, noch vor der Datenbank. Scheitert sie, bricht das Setup ab, ohne etwas verändert zu haben.
- **Bei Nur prüfen** läuft sie mit, sofern das Setup erhöht läuft. Das ist die einzige Stelle, an der *Nur prüfen* etwas anlegt; deshalb steht der Satz "installiert wird nichts" im Anwender-Handbuch mit Sternchen.

Mit Zugangsdatei

Unter *Nur prüfen* lässt sich die Zugangsdatei angeben (freiwillig). Dann holt das Setup beim Aktivierungsdienst, was die Einrichtung später holt, legt aber nichts ab:

Zeile	Prüft
Zugang: Lizenz der Klassik	liegt <code>cneulreg.txt</code> bereit
Zugang: Download-Schlüssel	liegt die Katalog-Erweiterung bereit (ohne sie keine geschützten Module)
Zugang: Lizenzblock	liegt eine <code>.eullic</code> bereit (ohne sie 30 Tage Probe)
Name Ihrer Suite	der vergebene Name, etwa <code>firma.x.eulanda.eu</code> (Lizenzmanager, Reiter X-Suite)
Name löst auf	löst dieser Name auf der Maschine auf, samt <code>hosts</code> -Datei - wie ein Browser

Mit dem Namen nennt auch der Hinweis zur Fritz!Box genau den Eintrag, der dort als Ausnahme hineingehört. Lehnt der Dienst die Datei ab, steht das als Fehler im Bericht, und der Rest der Prüfung läuft trotzdem.

Der Bericht

Nur prüfen schreibt den Bericht als eine HTML-Datei ohne externe Teile, in den Temp-Ordner und als Kopie auf den Desktop: `EULANDA-Setup-Check-<Maschine>-<yyyy-MM-dd>.html` . Ein neuer Lauf am selben Tag überschreibt die Kopie. Danach öffnet er sich im Browser.

Oben stehen das Urteil und alle Prüfzeilen, darunter der Steckbrief der Maschine - was man braucht, wenn etwas klemmt:

Teil	Inhalt
Maschine	Name, Domäne oder Arbeitsgruppe, Hersteller und Modell, Prozessor
Windows	Ausgabe, Build mit Update-Stand, Fassung, Sprache, letzter Start, PowerShell, .NET-Release
Arbeitsspeicher	Gesamt und frei
Laufwerke	Größe und freier Platz je Festplatte
SQL Server	Je Instanz: Fassung mit Build, Service-Pack-Stand, Ausgabe, zugeteilter Speicher (<code>max server memory</code>), ob das angemeldete Konto sysadmin ist, Zustand des Dienstes

Die SQL-Werte kommen aus der Registry und, wenn das Konto sich mit Windows-Anmeldung an der Instanz anmelden darf, aus der Instanz selbst. Kennwörter stehen nicht im Bericht.

