



● KUNDENDOKUMENTATION

HANDBUCH FÜR IT-ADMINISTRATION

Administratorhandbuch

Systemvoraussetzungen, Installation und Softwareverteilung, Netzwerk und Firewall, Datenablage, Lizenzverwaltung, Datensicherung, Aktualisierung, Deinstallation und Fehlerbehebung

DOKUMENT-ID
NH-ADM-01

VERSION
1.6

STAND
29.09.2026

PROGRAMM
1.1.6

FÜR WEN IST DIESES HANDBUCH?

Für Administratorinnen und Administratoren, die NexHand RemoteManager im Unternehmen bereitstellen und betreuen. Die tägliche Bedienung beschreibt das Benutzerhandbuch NH-BH-01, die Schutzmaßnahmen die TOM NH-TOM-01.

Bezogen auf Programmversion 1.1.6.

DOKUMENTENKONTROLLE

Dokumentinformationen

Titel	Administratorhandbuch – Installation, Betrieb und Fehlerbehebung
Dokument-ID / Version	NH-ADM-01 / 1.6
Stand	29.09.2026 (Programmversion 1.1.6)
Hersteller	Michael Kappe
Klassifizierung	KUNDENDOKUMENTATION
Adressaten	IT-Administration, Softwareverteilung, Informationssicherheit
Bezug	NH-BH-01 (Benutzerhandbuch) · NH-TOM-01 (TOM) · NH-VF-01 (Verfahrensbeschreibungen)

Änderungshistorie

VERSION	DATUM	ÄNDERUNG
1.6	29.09.2026	Abschnitt 6 und Fehlerbehebung: Programmversion nach Ende der Wartung ist nicht lizenziert
1.5	29.09.2026	Abschnitt 6: Schaltfläche heißt jetzt „Lizenz entfernen“
1.4	28.09.2026	Abschnitt 3: Adresse des Lizenzservers für Firewall und Proxy
1.3	28.09.2026	Bezug auf Programmversion 1.1.1; Programmversion und Quellcodestand werden automatisch eingesetzt
1.2	28.09.2026	Abschnitt 11, Anhang A: RDP-Diagnoseprotokoll
1.1	28.09.2026	Abschnitt 6: Bezeichnung der Schaltfläche „Auf diesem Gerät freigeben“ korrigiert
1.0	28.09.2026	Erstfassung für Programmversion 1.1.0

ÜBERSICHT

Inhaltsverzeichnis

1	Systemvoraussetzungen	4
2	Installation	4
2.1	Installationspakete	5
2.2	Unbeaufsichtigte Installation und Softwareverteilung	5
2.3	Erster Start und Einrichtung	5
3	Netzwerk und Firewall	7
4	Datenablage	8
5	Bereitstellung eines Datenbestands für mehrere Techniker	9
6	Lizenzverwaltung	10
7	Datensicherung	10
8	Aktualisierung	11
9	Deinstallation und Außerbetriebnahme	11
10	Sicherheitsempfehlungen für den Betrieb	12
11	Fehlerbehebung	13
A	Anhang A – Pfade, Registry und Umgebungsvariablen	14
B	Anhang B – Checkliste Inbetriebnahme	15

ABSCHNITT 1

Systemvoraussetzungen

NexHand RemoteManager ist eine Einzelplatzanwendung für Windows. Es wird kein Server, keine Datenbankinstallation und kein Verzeichnisdienst benötigt.

KOMPONENTE	ANFORDERUNG
Betriebssystem	Windows 10 (ab 1809) oder Windows 11, jeweils 64 Bit
Microsoft Edge WebView2	Laufzeitumgebung für die Oberfläche; in Windows 11 und aktuellen Windows-10-Versionen enthalten. Fehlt sie, lädt der Installer sie von Microsoft nach (Internetzugang nötig) – oder sie wird vorab über die Softwareverteilung installiert.
Remotedesktop- Client	Das in Windows enthaltene Remotedesktop-Control (<code>mstscax.dll</code>). Keine zusätzliche Installation.
Arbeitsspeicher	ab 4 GB; je offene RDP- oder Web-Sitzung zusätzlich rund 100–300 MB
Festplatte	rund 30 MB für das Programm, wenige MB für Daten; Browserprofile der Web-Sitzungen wachsen mit der Nutzung
Bildschirm	ab 1280 × 720; hohe Skalierung (HiDPI) wird unterstützt
Rechte	Installation pro Benutzer ohne Administratorrechte möglich (Abschnitt 2.1). Für den Betrieb genügen Standardbenutzerrechte.

ABSCHNITT 2

Installation

2.1 Installationspakete

PAKET	ART	EINSATZ
NexHand RemoteManager_1.1.6_x64-setup.exe	NSIS-Installer, Installation pro Benutzer nach %LOCALAPPDATA%\NexHand RemoteManager	Einzelplätze, Techniker ohne Administratorrechte
NexHand RemoteManager_1.1.6_x64_en-US.msi	Windows-Installer, Installation für alle Benutzer nach C:\Program Files\NexHand RemoteManager	Softwareverteilung (Intune, SCCM, Gruppenrichtlinie)

Beide Pakete installieren dasselbe Programm. Die Daten liegen in jedem Fall im Profil des jeweiligen Benutzers ([Abschnitt 4](#)), nicht im Installationsverzeichnis.

SMARTSCREEN

Die Pakete der Version 1.1.6 sind noch nicht digital signiert. Windows SmartScreen zeigt deshalb beim ersten Start „Der Computer wurde durch Windows geschützt“. Prüfen Sie vor dem Freigeben die Herkunft des Pakets (Bezug nur vom Hersteller) und die Prüfsumme (SHA-256), die der Hersteller mitliefert.

2.2 Unbeaufsichtigte Installation und Softwareverteilung

MSI, für alle Benutzer, ohne Oberfläche:

```
msiexec /i "NexHand RemoteManager_1.1.6_x64_en-US.msi" /qn /norestart /l*v "%TEMP%\nexhand-install.log"
```

NSIS-Installer, für den angemeldeten Benutzer, ohne Oberfläche:

```
"NexHand RemoteManager_1.1.6_x64-setup.exe" /S
```

Die Deinstallation erfolgt entsprechend mit `msiexec /x ... /qn` bzw. mit `uninstall.exe /S` im Installationsverzeichnis.

- Für die Erkennung in der Softwareverteilung eignet sich der Uninstall-Eintrag „NexHand RemoteManager“ mit Version `1.1.6`.
- Fehlt WebView2 auf den Zielrechnern, verteilen Sie vorab den „Evergreen Standalone Installer“ von Microsoft.
- Programmeinstellungen müssen nicht verteilt werden. Autostart und Windows-Kopplung legt jeder Benutzer selbst fest.

2.3 Erster Start und Einrichtung

- Beim ersten Start legt der Benutzer sein Master-Passwort fest oder übernimmt eine Datensicherung („Stattdessen Daten aus einer Sicherung übernehmen...“).

- 2 Optional: Windows-Kopplung (Tresor mit Windows-Anmeldung entsperren) – Empfehlung in [Abschnitt 10](#).
- 3 Optional: Lizenz aktivieren (Extras → „Lizenz...“), sonst Free-Version mit 10 Verbindungen.
- 4 Optional: Autostart über das Menü des Symbols im Infobereich („Mit Windows starten“).

ABSCHNITT 3

Netzwerk und Firewall

NexHand baut nur ausgehende Verbindungen auf. Es öffnet keine Ports auf dem Arbeitsplatz und benötigt keine eingehenden Firewall-Regeln.

ZIEL	PORT / PROTOKOLL	HINWEIS
SSH, SFTP	22/TCP	Standard; je Verbindung änderbar
Remotedesktop	3389/TCP (+UDP)	über RD-Gateway: 443/TCP zum Gateway
VNC	5900/TCP	unverschlüsselt
Telnet	23/TCP	unverschlüsselt
Web	80, 443/TCP	laut URL der Verbindung
Lizenzserver	443/TCP (HTTPS)	nur bei aktivierter Lizenz: <code>lizenz.beuzelrecords.de</code>

- **Proxy:** Die Lizenzprüfung nutzt eine direkte HTTPS-Verbindung. Verlangt Ihr Netz einen Proxy, geben Sie die Adresse des Lizenzservers in der Proxy-Konfiguration frei.
- **TLS-Aufbrechen:** Die Lizenzprüfung vertraut nur öffentlichen Zertifizierungsstellen. Bei Proxys, die TLS aufbrechen, nehmen Sie den Lizenzserver von der Inspektion aus.
- **Offline:** Eine aktivierte Lizenz bleibt ohne Serverkontakt bis zum Ende ihrer Kulanzzzeit gültig. Die Free-Version benötigt nie eine Verbindung.

ABSCHNITT 4

Datenablage

Alle Daten liegen im Roaming-Profil des Benutzers unter `%APPDATA%\com.techtool.app`. Der Ordnername ist die interne Kennung der Anwendung und bleibt über Versionen hinweg gleich.

DATEI / ORDNER	INHALT
<code>techtool.db</code>	SQLite-Datenbank mit Projekten, Verbindungen, Credentials (Geheimnisse verschlüsselt), Hostschlüsseln und Lizenzdaten. Dazu während des Betriebs <code>-wal</code> und <code>-shm</code> .
<code>vault.dpapi</code>	nur bei aktivierter Windows-Kopplung; an Benutzerkonto und Rechner gebunden
<code>web\</code> , <code>web-insecure\</code>	Browserprofile der Web-Sitzungen
<code>techtool-vor-wiederherstellung-*.db</code>	automatische Sicherung vor einer Wiederherstellung; kann nach Prüfung gelöscht werden

SERVERGESPEICHERTE PROFILE

Bei Roaming-Profilen wandert `techtool.db` mit dem Profil. Die Windows-Kopplung (`vault.dpapi`) funktioniert nur, solange DPAPI das Profil auf dem jeweiligen Rechner entschlüsseln kann. NexHand darf nicht gleichzeitig auf zwei Rechnern mit demselben Profil laufen, sonst überschreibt die Profilsynchronisation Änderungen. Die Web-Profile (`web\`) können groß werden; schließen Sie sie bei Bedarf von der Synchronisation aus.

Getrennter Datenordner

Mit der Umgebungsvariable `TECHTOOL_DATA_DIR` nutzt NexHand einen anderen Datenordner, z. B. für Schulungs- und Testbestände oder einen verschlüsselten Wechseldatenträger:

```
set TECHTOOL_DATA_DIR=D:\NexHand-Schulung
"%LOCALAPPDATA%\NexHand RemoteManager\techtool.exe"
```

ABSCHNITT 5

Bereitstellung eines Datenbestands für mehrere Techniker

Version 1.1 arbeitet als Einzelplatz; ein gemeinsamer Bestand mit laufendem Abgleich ist für eine spätere Version geplant. Bis dahin verteilen Sie einen vorbereiteten Bestand über die Datensicherung.

- 1 Auf einem Referenzrechner Projekte, Ordner, Verbindungen und die gemeinsam genutzten Credentials pflegen, z. B. per Import aus Royal TS.
- 2 Einstellungen → „Datensicherung & Übertragung“ → Sicherung erstellen.
- 3 Sicherungsdatei über einen geschützten Weg bereitstellen (Netzlaufwerk mit Berechtigungen nur für die Technikgruppe).
- 4 Master-Passwort der Sicherung getrennt übermitteln (persönlich oder über den Passwortmanager der Firma).
- 5 Techniker übernehmen die Sicherung beim ersten Start und ändern anschließend ihr Master-Passwort (Einstellungen → „Master-Passwort ändern“).

HINWEIS

Nach der Übernahme sind die Bestände unabhängig. Spätere Änderungen am Referenzbestand erreichen die Techniker nur durch eine erneute Übernahme, die deren lokale Änderungen ersetzt (der vorherige Stand wird automatisch gesichert).

ABSCHNITT 6

Lizenzverwaltung

ZUSTAND	BEDEUTUNG
Free-Version	ohne Lizenz; bis zu 10 Verbindungen, alle Funktionen, keine Serververbindung
Lizenziert	Grenzen und freigeschaltete Protokolle laut Plan; Anzeige im Lizenzdialog
Test-Lizenz	zeitlich begrenzte Lizenz zum Ausprobieren
Lizenz ungültig	Aktivierung gesperrt, widerrufen, abgelaufen, Kulanzzeit ohne Serverkontakt überschritten oder Programmversion nach dem Ende der Wartung erschienen („Diese Version ist nicht durch Ihre Wartung abgedeckt“); es gelten die Grenzen der Free-Version

- **Zählung:** je Gerät. Eine Lizenz mit n Plätzen kann auf n Rechnern gleichzeitig aktiviert sein.
- **Gerätewechsel:** auf dem alten Rechner im Lizenzdialog „Lizenz entfernen“, dann auf dem neuen aktivieren. Ist der alte Rechner nicht mehr verfügbar (Defekt, Verlust), kann der Platz über die Lizenzverwaltung des Herstellers freigegeben werden; das Gerät ist dort am Rechnernamen erkennbar.
- **Neuinstallation von Windows:** ändert die Geräteerkennung; das Gerät zählt dann als neues Gerät.
- **Grenzen:** Beim Überschreiten der Verbindungsgrenze lassen sich keine neuen Verbindungen anlegen; vorhandene bleiben nutzbar. Gesperrte Protokolle lassen sich nicht öffnen.

ABSCHNITT 7

Datensicherung

NexHand sichert nicht automatisch. Zwei Wege sind möglich:

WEG	VORGEHEN	HINWEIS
In der Anwendung	Einstellungen → „Datensicherung & Übertragung“	konsistente Kopie im laufenden Betrieb; empfohlen
Dateisicherung	Ordner %APPDATA%\com.techtool.app sichern	nur bei beendetem Programm konsistent; vault.dpapi ist auf anderen Rechnern wertlos

Sicherungen enthalten die Geheimnisse verschlüsselt. Zum Wiederherstellen wird das Master-Passwort benötigt, das zum Zeitpunkt der Sicherung galt. Verfahren und Aufbewahrung: [NH-VF-01](#).

ABSCHNITT 8

Aktualisierung

- 1 NexHand auf dem Rechner beenden (Symbol im Infobereich → „Beenden“).
- 2 Neues Paket über das bestehende installieren (gleiche Paketart wie bisher). Die Daten bleiben erhalten.
- 3 Beim ersten Start passt NexHand die Datenbank bei Bedarf automatisch an. Eine Rückkehr zur älteren Version ist danach nur mit einer vorher angelegten Sicherung möglich.

Eine automatische Aktualisierung ist in Version 1.1 nicht enthalten. Vor dem Verteilen einer neuen Version empfiehlt sich ein Test auf einem Referenzrechner mit Kopie eines echten Bestands (`TECHTOOL_DATA_DIR`).

ABSCHNITT 9

Deinstallation und Außerbetriebnahme

- 1 Lizenz im Lizenzdialog freigeben, damit der Platz wieder verfügbar ist.
- 2 Programm über „Apps & Features“ oder die Softwareverteilung deinstallieren. Der NSIS-Deinstaller bietet an, die Anwendungsdaten zu löschen.
- 3 Bei Außerbetriebnahme eines Rechners: Ordner `%APPDATA%\com.techtool.app` löschen, Sicherungen unter `Dokumente\NexHand-Sicherungen` prüfen und löschen, Datenträger nach den Vorgaben des Unternehmens löschen.
- 4 Autostart vor der Deinstallation im Infobereich abschalten („Mit Windows starten“). Sonst bleibt der Eintrag unter `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` zurück und ist von Hand zu entfernen.

ABSCHNITT 10

Sicherheitsempfehlungen für den Betrieb

THEMA	EMPFEHLUNG
Festplattenverschlüsselung	BitLocker auf allen Rechnern mit NexHand, besonders auf Notebooks. Projektnamen, Hosts und Notizen liegen unverschlüsselt in der Datenbank.
Windows-Kopplung	nur auf persönlichen, verschlüsselten Rechnern mit Bildschirmsperre. Auf gemeinsam genutzten Rechnern und Terminalservern nicht verwenden.
Master-Passwort	mindestens 12 Zeichen; Hinterlegung nach NH-VF-01
Bildschirmsperre	per Gruppenrichtlinie nach wenigen Minuten Inaktivität
Protokolle	Telnet und VNC nur in abgeschotteten Netzen; nach Möglichkeit SSH und RDP mit NLA
RDP-Weiterleitungen	Laufwerksweiterleitung nur im Einzelfall; ggf. zusätzlich serverseitig per Richtlinie einschränken
Jump-Host	Zugriffe auf Kundennetze über einen zentralen SSH-Sprungserver bündeln; dort protokollieren
Sicherungen	nur auf verschlüsselten Laufwerken oder Freigaben mit eingeschränkten Rechten
Offboarding	bei Ausscheiden Rechner zurücknehmen, Daten löschen, gemeinsam genutzte Zugangsdaten auf den Zielsystemen ändern (NH-VF-01)

ABSCHNITT 11

Fehlerbehebung

SYMPTOM	URSACHE UND LÖSUNG
Programm startet nicht, kein Fenster	WebView2 fehlt oder ist beschädigt. WebView2-Laufzeit von Microsoft installieren bzw. reparieren. Prüfen, ob NexHand bereits im Infobereich läuft.
Nach Kennwort-Rücksetzung durch einen Administrator verlangt NexHand das Master-Passwort	Durch das Zurücksetzen (nicht Ändern) des Windows-Kennworts verliert DPAPI den Zugriff auf seine Schlüssel. <code>vault.dpapi</code> ist dann wertlos. Mit dem Master-Passwort entsperren und die Windows-Kopplung neu einschalten.
Windows-Kopplung wirkt nach Übertragung nicht	Erwartet: Die Kopplung gilt nur für Rechner und Konto, auf denen sie eingerichtet wurde. Neu einschalten.
„RDP-Control konnte nicht gestartet werden“	Remotedesktop-Komponente fehlt oder ist per Richtlinie deaktiviert (z. B. Windows-Editionen ohne RDP-Client, gehärtete Images). <code>mstsc.exe</code> testweise starten; Richtlinien prüfen.
RDP-Verbindung scheitert oder bleibt schwarz	Die Ereignisse des Remotedesktop-Controls stehen in <code>logs\rdp.log</code> im Datenordner (Zeit, Ereignis, Code – ohne Hosts und Zugangsdaten). Datei nach einem Fehlversuch an den Hersteller senden; der Code nach „OnDisconnected“ nennt meist die Ursache.
RDP: Anmeldung schlägt mit NLA fehl	Zielsystem oder Konto unterstützt NLA nicht, oder das Passwort ist abgelaufen. Passwort prüfen; NLA nur für Altsysteme in der Verbindung abschalten.
SSH: „Hostschlüssel hat sich geändert!“	Server neu installiert, Adresse neu vergeben – oder Angriff. Fingerabdruck beim Serverbetreiber prüfen, erst dann vertrauen.
Web-Sitzung zeigt Zertifikatsfehler	Gerät mit selbstsigniertem Zertifikat. Besser: Zertifikat einer internen Zertifizierungsstelle auf dem Gerät einsetzen. Sonst „Zertifikatsfehler ignorieren“ nur für diese Verbindung.
Lizenz lässt sich nicht aktivieren	Keine HTTPS-Verbindung zum Lizenzserver (Proxy, Firewall, TLS-Inspektion; Abschnitt 3), Schlüssel falsch eingegeben oder alle Plätze belegt. Die Meldung im Lizenzdialog nennt den Grund.
„Diese Version ist nicht durch Ihre Wartung abgedeckt“	Die installierte Version ist nach dem Ende der Wartung („Updates bis“) erschienen. Die zuletzt abgedeckte Version installieren oder die Wartung verlängern; das Erscheinungsdatum steht im Lizenzdialog neben „Updates bis“.
„Lizenz ungültig“ nach längerer Offline-Zeit	Kulanzzeit überschritten. Internetverbindung herstellen; die Erneuerung erfolgt automatisch oder über „Jetzt prüfen“ im Lizenzdialog.
Serielle Schnittstelle lässt sich nicht öffnen	In einem anderen Programm geöffnet, Treiber des USB-Seriell-Adapters fehlt oder falsche COM-Nummer. Geräte-Manager prüfen.
Master-Passwort verloren, keine Windows-Kopplung	Die Geheimnisse sind nicht wiederherstellbar. Datenbestand aus einer Sicherung mit bekanntem Passwort übernehmen oder neu beginnen (NH-VF-01).

ANHANG A

Pfade, Registry und Umgebungsvariablen

EINTRAG	WERT
Programm (NSIS)	%LOCALAPPDATA%\NexHand RemoteManager\
Programm (MSI)	%ProgramFiles%\NexHand RemoteManager\
Daten	%APPDATA%\com.techtool.app\
Sicherungen (Standard)	%USERPROFILE%\Documents\NexHand-Sicherungen\
RDP-Diagnoseprotokoll	%APPDATA%\com.techtool.app\logs\rdp.log
Zwischendateien SFTP	%TEMP%\NexHand RemoteManager\
WebView2-Daten der Oberfläche	%LOCALAPPDATA%\com.techtool.app\
Autostart	HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Geräteerkennung (nur gelesen)	HKLM\SOFTWARE\Microsoft\Cryptography\MachineGuid
TECHTOOL_DATA_DIR	abweichender Datenordner

ANHANG B

Checkliste Inbetriebnahme

✓	PUNKT
☐	Herkunft und Prüfsumme des Installationspakets geprüft
☐	WebView2 auf den Zielrechnern vorhanden
☐	BitLocker und Bildschirmsperre auf den Zielrechnern aktiv
☐	Firewall/Proxy: ausgehende Ports nach Abschnitt 3 , Lizenzserver freigegeben
☐	Regel zur Windows-Kopplung festgelegt und den Technikern mitgeteilt
☐	Hinterlegung der Master-Passwörter geregelt (NH-VF-01)
☐	Referenzbestand erstellt und verteilt (Abschnitt 5)
☐	Lizenzen aktiviert, Geräte in der Lizenzverwaltung erkennbar
☐	Sicherungsrhythmus und Ablageort festgelegt
☐	TOM NH-TOM-01 in die eigene Dokumentation übernommen