

Software Upgrade Tool Benutzerhandbuch

2024.10
Ver.1.0



Inhaltsverzeichnis

1. Einleitung	3
1.1 Über dieses Dokument	3
1.2 Rechts- und Sicherheitsinformationen	3
1.3 Über Handelsnamen	3
1.4 Über das Software Upgrade Tool	3
1.5 Systemanforderungen	4
2. Produkt-Firmware- und HyPAS-Anwendungsupdate	5
2.1 Voraussetzungen	5
2.2 Aktualisieren der Produktfirmware oder der HyPAS-Anwendung	5
3. Fehlerbehebung	15

1. Einleitung

1.1 Über dieses Dokument

Dieses Dokument enthält ein Aktualisierungsverfahren, das die Anwendungssoftware „Software Upgrade Tool“ verwendet, um Ihre Produkt-Firmware oder Anwendungen der Hybrid Platform for Advanced Solutions (HyPAS) zu aktualisieren.

1.2 Rechts- und Sicherheitsinformationen

- Die unerlaubte Vervielfältigung des Handbuchs oder eines Teils davon ist verboten.
- Informationen in diesem Handbuch können ohne vorherige Ankündigung geändert werden.
- Dieses Dokument beschreibt Verfahren, die beispielsweise in Windows 11 ausgeführt werden.
- Wir sind nicht für Ausfälle oder Schäden verantwortlich, die sich aus Bedingungen oder Nutzungsverfahren ergeben, die nicht in diesem Dokument enthalten sind.

1.3 Über Handelsnamen

- Microsoft, Windows und Windows Server sind eingetragene Warenzeichen oder Warenzeichen der Microsoft Corporation in den USA und/oder anderen Ländern.
- Mac und macOS sind eingetragene Warenzeichen von Apple Inc. in den USA und anderen Ländern.
- Linux ist das eingetragene Warenzeichen oder Warenzeichen von Linus Torvalds in den USA und anderen Ländern.
- Alle anderen Marken und Produktnamen sind eingetragene Warenzeichen oder Warenzeichen der jeweiligen Unternehmen. Die Bezeichnungen™ und ® werden in diesem Handbuch nicht verwendet.

1.4 Über das Software Upgrade Tool

Eine Firmware ist eine integrierte Software, die ein Produkt steuert. Eine HyPAS-Anwendung ist eine Software, die die Produktfunktionalität verbessert. Durch die Aktualisierung der Firmware oder der HyPAS-Anwendung können die Sicherheit des Produkts verbessert und der Betrieb stabilisiert werden. Wir empfehlen, diese Anwendung zu verwenden, um die Firmware des Produkts oder die HyPAS-Anwendung zu aktualisieren, damit Sie das Produkt weiterhin sicher verwenden können.

1.5 Systemanforderungen

Betriebssystem:	Windows	Windows 11 Windows 10 Windows Server 2022 Windows Server 2019 Windows Server 2016
	Mac	macOS 14 Sonoma macOS 13 Ventura macOS 12 Monterey
	Linux	Ubuntu 22.04 LTS CentOS Stream 9 OpenSUSE Leap 15.5
Speicherkapazität:	Mindestens 2 GB	
Ausführungsumgebung:	„Visual C++ Redistributable Package“ erforderlich (nur für Windows)	
Netzwerk:	Verkabelte Netzwerkverbindung empfohlen	

2. Produkt-Firmware- und HyPAS-Anwendungsupdate

Achtung

- Während der Aktualisierung ist eine Netzwerkverbindung erforderlich.
- Wenn die Produkt-Firmware aktualisiert wird, kann sie nicht auf eine frühere Version zurückgesetzt werden. Wenn HyPAS-Anwendungen aktualisiert werden, können diese auf eine frühere Version zurückgesetzt werden.
- Schalten Sie während der Aktualisierung das Gerät nicht aus und trennen Sie das Netzkabel nicht.
- Wenn Sie die Produkt-Firmware aktualisieren, stellen Sie sicher, dass die HTTP/HTTPS-Portnummer nicht durch eine Firewall oder einen Virens Scanner blockiert wird.

2.1 Voraussetzungen

Stellen Sie vor der Verwendung dieses Tools Folgendes sicher:

- Rufen Sie die Support-Site für Ihre Region auf und laden Sie die Firmware-Datei oder das HyPAS-Anwendungspaket auf Ihren Computer herunter.
- Bestätigen Sie die SNMP-Einstellungen vor der Aktualisierung. Wenn Sie die Produkt-Firmware aktualisieren, vergewissern Sie sich, dass auch HTTP und HTTPS aktiviert sind.

Bestätigen Sie die Einstellungsdetails im Command Center RX. Weitere Einzelheiten finden Sie im Command Center RX User Guide.

- Bestätigen Sie den Benutzernamen und das Kennwort für den Administrator, der auf dem Produkt registriert ist und dessen Firmware oder HyPAS-Anwendung aktualisiert werden soll.

Hinweis

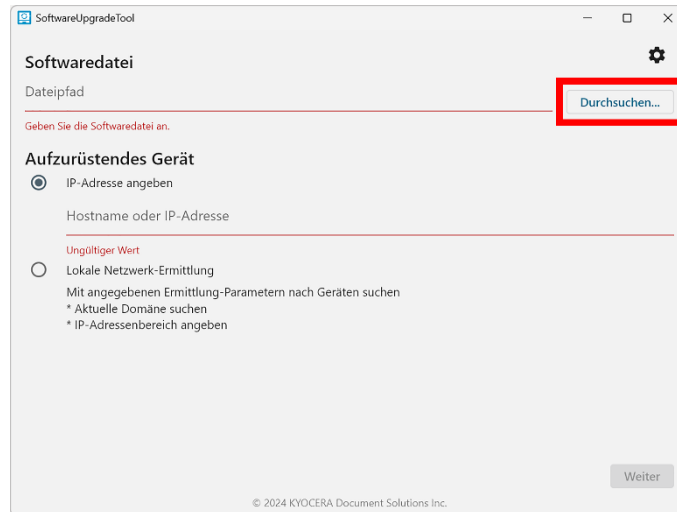
Bestätigen Sie den Benutzernamen und das Passwort für den Administrator, nicht den Geräte-Administrator. Beachten Sie die Bedienungsanleitung für Einzelheiten zum Benutzernamen und Passwort für den Administrator.

2.2 Aktualisieren der Produktfirmware oder der HyPAS-Anwendung

1. Starten Sie das Software Upgrade Tool.
2. Klicken Sie auf [Akzeptieren] im Bildschirm

„LIZENZVEREINBARUNG“.

3. Klicken Sie auf [Durchsuchen] und wählen Sie die Firmware-Datei oder das HyPAS-Anwendungspaket aus, das Sie auf Ihren Computer heruntergeladen haben.



Hinweis

Sie können Folgendes auswählen:

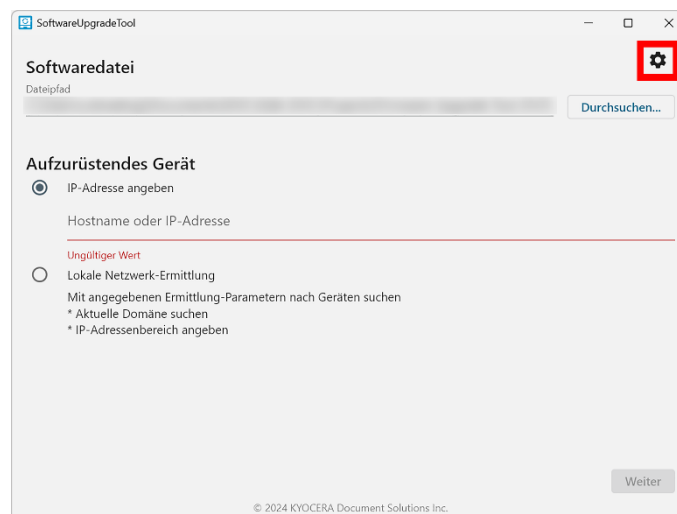
Produkt-Firmware-Datei

Firmware für Ihren Drucker

HyPAS-Anwendungspaket

Software für Ihre HyPAS-Anwendungen

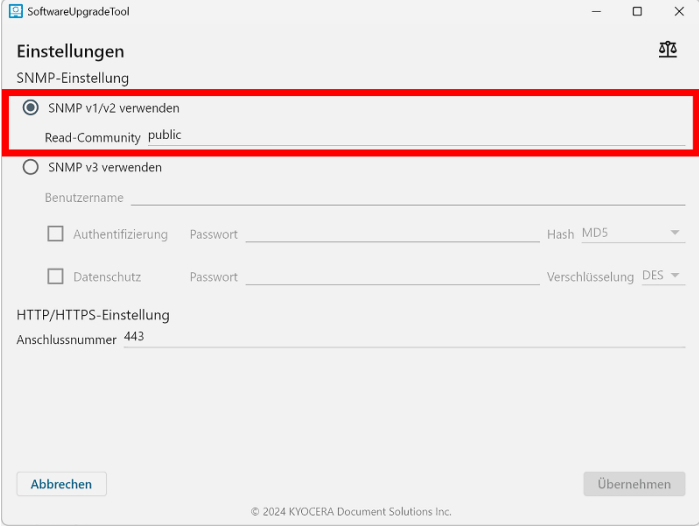
4. Klicken Sie auf .



5. Legen Sie die Protokollinformationen (SNMPv1/v2c, SNMPv3) für das Produkt fest, dessen Firmware oder HyPAS-Anwendung aktualisiert werden soll.

Wenn SNMPv1/v2c im Command Center RX aktiviert ist

1. Wählen Sie „SNMP v1/v2 verwenden“ aus.
2. Geben Sie unter „Read-Community“ SNMPv1/v2c als Community-Name ein.



The screenshot shows the 'Einstellungen' (Settings) window of the 'SoftwareUpgradeTool'. The 'SNMP-Einstellung' (SNMP Settings) section is highlighted with a red rectangle. It contains two radio buttons: 'SNMP v1/v2 verwenden' (selected) and 'SNMP v3 verwenden'. Below the selected option, the 'Read-Community' is set to 'public'. The 'SNMP v3 verwenden' section includes fields for 'Benutzername' (Username), 'Authentifizierung' (Authentication) with a 'Passwort' (Password) field and a 'Hash' dropdown set to 'MD5', and 'Datenschutz' (Data Protection) with a 'Passwort' (Password) field and a 'Verschlüsselung' (Encryption) dropdown set to 'DES'. The 'HTTP/HTTPS-Einstellung' (HTTP/HTTPS Settings) section shows the 'Anschlussnummer' (Port Number) set to '443'. At the bottom, there are 'Abbrechen' (Cancel) and 'Übernehmen' (Apply) buttons, and a copyright notice: '© 2024 KYOCERA Document Solutions Inc.'

Wenn SNMPv3 im Command Center RX aktiviert ist

1. Wählen Sie „SNMP v3 verwenden“ aus.
2. Geben Sie unter „Benutzername“ SNMPv3 als Benutzername ein.
3. Falls „Authentifizierung“ im Command Center RX aktiviert ist, wählen Sie „Authentifizierung“, geben Sie Ihr Passwort ein und wählen Sie dann den Authentifizierungsalgorithmus aus dem Drop-down-Menü „Hash“.
4. Falls „Datenschutz“ im Command Center RX aktiviert ist, wählen Sie „Datenschutz“, geben Sie Ihr Passwort ein und wählen Sie dann den Verschlüsselungsalgorithmus aus dem Drop-down-Menü „Verschlüsselung“.

The screenshot shows the 'Einstellungen' (Settings) window of the 'SoftwareUpgradeTool'. The 'SNMP-Einstellung' (SNMP Settings) section is active. The 'SNMP v3 verwenden' (Use SNMP v3) option is selected with a radio button. Below this, the 'Benutzername' (Username) field is filled with 'xxxxxxxxxx'. The 'Authentifizierung' (Authentication) checkbox is checked, and the 'Datenschutz' (Encryption) checkbox is also checked. The 'Hash' dropdown menu is set to 'MD5', and the 'Verschlüsselung' (Encryption) dropdown menu is set to 'DES'. The 'HTTP/HTTPS-Einstellung' (HTTP/HTTPS Settings) section below shows the 'Anschlussnummer' (Port number) as '443'. At the bottom, there are 'Abbrechen' (Cancel) and 'Übernehmen' (Apply) buttons. A red rectangle highlights the SNMPv3 configuration fields.

SoftwareUpgradeTool

Einstellungen

SNMP-Einstellung

☐ SNMP v1/v2 verwenden

Read-Community public

☒ SNMP v3 verwenden

Benutzername xxxxxxxxxxxx

☒ Authentifizierung Passwort Hash MD5

☒ Datenschutz Passwort Verschlüsselung DES

HTTP/HTTPS-Einstellung

Anschlussnummer 443

Abbrechen Übernehmen

© 2024 KYOCERA Document Solutions Inc.

6. Wenn Sie die Produkt-Firmware aktualisieren, bestätigen Sie die HTTP/HTTPS-Portnummer. Wenn Sie die HyPAS-Anwendung aktualisieren, fahren Sie mit Schritt 7 fort.

SoftwareUpgradeTool

Einstellungen

SNMP-Einstellung

☒ SNMP v1/v2 verwenden

Read-Community public

☐ SNMP v3 verwenden

Benutzername

☐ Authentifizierung Passwort Hash MD5

☐ Datenschutz Passwort Verschlüsselung DES

HTTP/HTTPS-Einstellung

Anschlussnummer 443

Abbrechen Übernehmen

© 2024 KYOCERA Document Solutions Inc.

Hinweis

- Normalerweise ist es nicht notwendig, die Portnummer zu ändern.
- Wenn die folgenden HTTP/HTTPS-Portnummern bereits verwendet werden, geben Sie eine neue Portnummer an:

Für Windows oder Mac

Anschluss 443

Unter Linux

Anschluss 10443

7. Klicken Sie auf [Übernehmen].

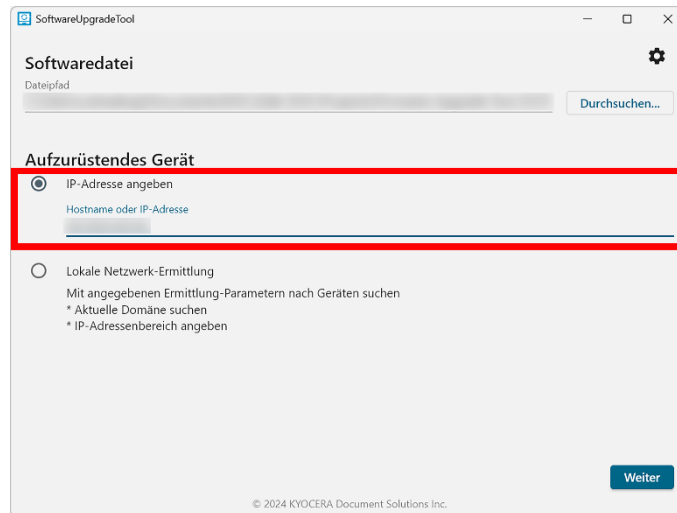
Hinweis

Klicken Sie auf [Abbrechen], wenn Sie die Änderung an den Einstellungen abbrechen möchten.

8. Wählen Sie das Produkt aus, dessen Firmware oder HyPAS-Anwendung aktualisiert werden soll.

Wenn Sie das Produkt mit einer IP-Adresse oder einem Hostnamen angeben

1. Wählen Sie „IP-Adresse angeben“ aus.
2. Geben Sie die IP-Adresse oder den Hostnamen des Produkts ein.

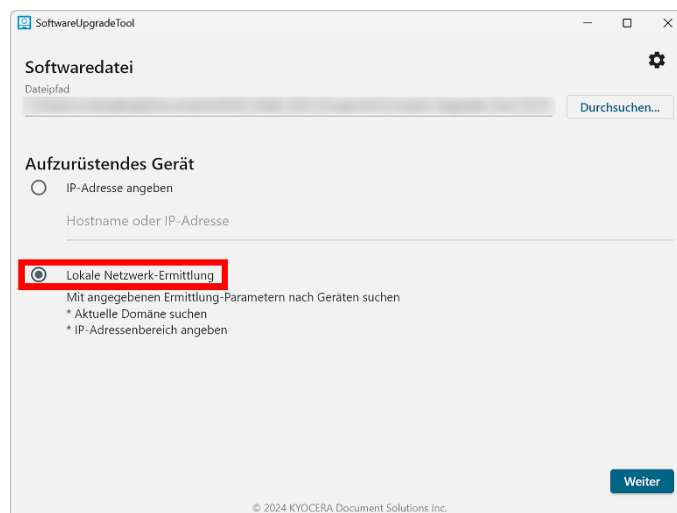


The screenshot shows the 'SoftwareUpgradeTool' window. At the top, there is a 'Softwaredatei' section with a 'Dateipfad' input field and a 'Durchsuchen...' button. Below this is the 'Aufzurüstendes Gerät' section. It contains two radio button options: 'IP-Adresse angeben' (which is selected and highlighted with a red rectangle) and 'Lokale Netzwerk-Ermittlung'. The 'IP-Adresse angeben' option has a text input field labeled 'Hostname oder IP-Adresse' next to it. Below the second option, there is explanatory text: 'Mit angegebenen Ermittlung-Parametern nach Geräten suchen', '* Aktuelle Domäne suchen', and '* IP-Adressenbereich angeben'. At the bottom right of the window is a 'Weiter' button. The footer contains the copyright notice '© 2024 KYOCERA Document Solutions Inc.'.

3. Klicken Sie auf [Weiter] und gehen Sie zum nächsten Schritt 9.

Wenn Sie das Produkt über eine Suche im Netzwerk angeben

1. Wählen Sie „Lokale Netzwerk-Ermittlung“ aus.

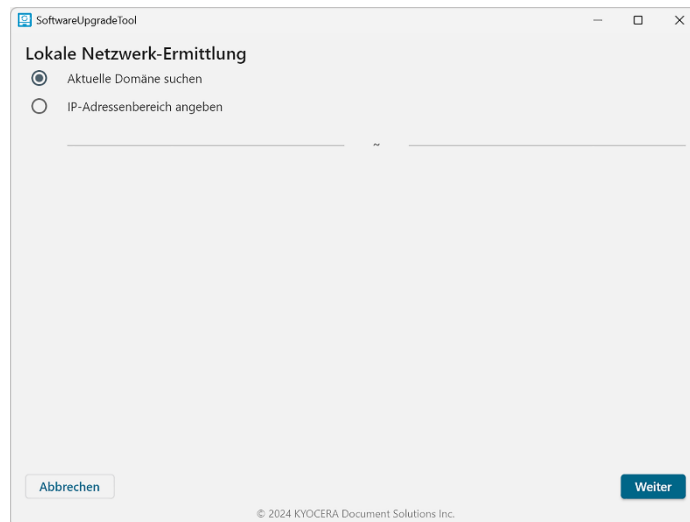


This screenshot shows the same 'SoftwareUpgradeTool' window as the previous one, but with the 'Lokale Netzwerk-Ermittlung' radio button selected and highlighted with a red rectangle. The 'IP-Adresse angeben' option is now unselected. The text input field 'Hostname oder IP-Adresse' remains empty. The explanatory text for the selected option is still visible. The 'Weiter' button and the footer copyright notice are also present.

2. Klicken Sie auf [Weiter].

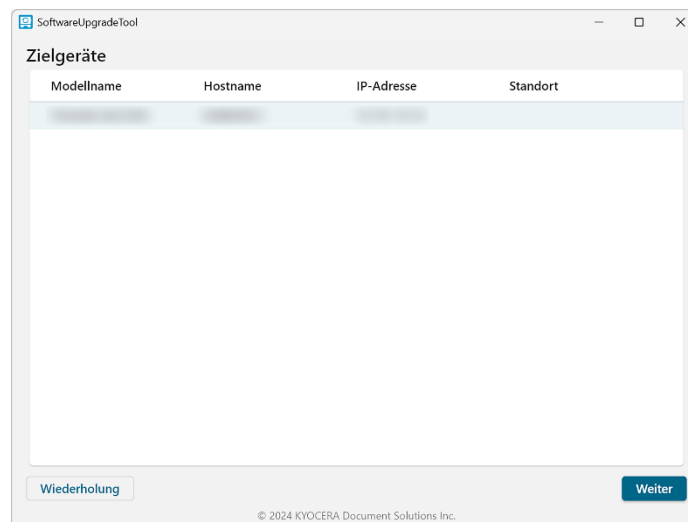
3. Führen Sie eine der folgenden Aktionen aus:

- Wenn Sie aus allen Produkten im Netzwerk auswählen, wählen Sie „Aktuelle Domäne suchen“ aus.
- Wenn Sie aus einer gefilterten Liste aller Produkte im Netzwerk auswählen, wählen Sie „IP-Adressenbereich angeben“ aus und geben Sie die IP-Adressen ein.



4. Klicken Sie auf [Weiter].

5. Wählen Sie das Produkt aus, dessen Firmware oder HyPAS-Anwendung aktualisiert werden soll.



6. Klicken Sie auf [Weiter].

Hinweis

Klicken Sie auf [Wiederholung], um die Suche zu wiederholen.

9. Klicken Sie auf [OK].

Wenn die Produktfirmware aktualisiert wird

SoftwareUpgradeTool

Geräteinformation

Eigenschaft	Wert
Modellname	
Seriennummer	
Hostname	

Firmware-Informationen

Firmware-Typ	Firmware-Version	Neue Version
CPKG		

Warnung
Die folgenden Informationen sorgfältig durchlesen.
Wenn das Gerät ausgeschaltet oder die Stromversorgung während des Upgrades unterbrochen wird, kann es sein, dass der Vorgang nicht abgeschlossen wird oder das Gerät nicht mehr funktionsfähig ist.
Detaillierte Informationen erhalten Sie im Benutzerhandbuch.

Möchten Sie fortfahren?

© 2024 KYOCERA Document Solutions Inc.

Wenn eine der HyPAS-Anwendungen aktualisiert wird

SoftwareUpgradeTool

Geräteinformation

Eigenschaft	Wert
Modellname	
Seriennummer	
Hostname	

HyPAS-Anwendungsdetails

HyPAS-Anwendungsname	HyPAS-Anwendungsversion	Neue Version
Test Application 1		

Warnung
Die folgenden Informationen sorgfältig durchlesen.
Wenn das Gerät ausgeschaltet oder die Stromversorgung während des Upgrades unterbrochen wird, kann es sein, dass der Vorgang nicht abgeschlossen wird oder das Gerät nicht mehr funktionsfähig ist.
Detaillierte Informationen erhalten Sie im Benutzerhandbuch.

Möchten Sie fortfahren?

© 2024 KYOCERA Document Solutions Inc.

Achtung

Schalten Sie während der Aktualisierung das Gerät nicht aus und trennen Sie das Netzkabel nicht.

Hinweis

- Wenn Sie die Produkt-Firmware mit einer früheren oder ähnlichen Version aktualisieren, wird „WARNUNG: Auf dem Gerät ist bereits eine neuere Version installiert.“ angezeigt. Die Aktualisierung ist nicht erforderlich, da auf dem Produkt bereits eine neuere Version der Firmware ausgeführt wird. Klicken Sie auf [Abbrechen] und beenden Sie den Vorgang.

- Wenn Sie die HyPAS-Anwendung mit einer früheren Version aktualisieren, wird ein Downgrade der HyPAS-Anwendung durchgeführt.

10. Geben Sie den Benutzernamen und das Passwort des Administrators ein, der für das Produkt registriert ist.

The screenshot shows a window titled "SoftwareUpgradeTool". Inside, there is a section "Geräteinformation" with a table:

Eigenschaft	Wert
Modellname	
Seriennummer	
Hostname	

Below this is the "Authentifizierung" section. It contains the text: "Sie benötigen Administrator-Rechte, um die Geräte-Einstellungen zu ändern. Geben Sie den Admin-Login und das Admin-Passwort ein." There are input fields for "Benutzername" and "Passwort" (masked with dots). Below these fields are buttons "Abbrechen" and "Anmelden".

At the bottom, there is a warning: "Die folgenden Informationen sorgfältig durchlesen. Wenn das Gerät ausgeschaltet oder die Stromversorgung während des Upgrades unterbrochen wird, kann es sein, dass der Vorgang nicht abgeschlossen wird oder das Gerät nicht mehr funktionsfähig ist. Detaillierte Informationen erhalten Sie im Benutzerhandbuch." Below this is a question "Möchten Sie fortfahren?" with buttons "Abbrechen" and "OK".

At the very bottom, the copyright notice "© 2024 KYOCERA Document Solutions Inc." is visible.

11. Klicken Sie auf [Anmelden].

Es startet die Aktualisierung.

Wenn die Aktualisierung beendet ist, wird das Ergebnis angezeigt.

Hinweis
Wenn „Authentifizierung fehlgeschlagen. Benutzernamen und Passwort überprüfen und erneut versuchen.“ nach dem Klicken von [Anmelden] angezeigt wird, dann liegt ein Fehler mit dem in Schritt 10 eingegebenen Benutzernamen oder Passwort vor. Bestätigen Sie den richtigen Benutzernamen und das richtige Passwort.

12. Klicken Sie auf [Beenden].

3. Fehlerbehebung

Mitteilung	Korrekturmaßnahme
Warnung Zugriff auf diesen Host verweigert. Überprüfen Sie Ihre Einstellungen, und versuchen Sie es erneut.	• Prüfen Sie, ob Sie den korrekten Hostnamen bzw. die richtige IP-Adresse eingegeben haben. • Prüfen Sie, ob die SNMP-Einstellungen am Bildschirm [Einstellungen] den Protokolleinstellungen (SNMPv1/v2c, SNMPv3) für das Produkt entsprechen. Im Command Center RX können Sie die Protokolleinstellungen überprüfen. Weitere Informationen finden Sie im Benutzerhandbuch des Command Center RX. • Überprüfen Sie, ob die angegebene Firmware-Datei oder das HyPAS-Anwendungspaket mit Ihrem Produkt kompatibel ist. • Prüfen Sie das Systemmenü des Produkts oder Command Center RX, um zu bestätigen, ob dieses Tool verwendet werden kann. In einigen Produkten werden die Berechtigungseinstellungen möglicherweise nicht unterstützt. Weitere Informationen finden Sie in der Bedienungsanleitung oder im Command Center RX User Guide.
Warnung Geräte nicht gefunden. Auf dem lokalen Netzwerk nach Geräten suchen	
Fehler Upgrade fehlgeschlagen. Grund: Versionsprüfung fehlgeschlagen.	• Überprüfen Sie, ob die Firmware-Version oder die HyPAS-Anwendungsversion des Produkts aktualisiert wurde. (Informationen zum Überprüfen der Firmware-Version oder der HyPAS-Anwendungsversion des Produkts finden Sie in der Bedienungsanleitung.) Ignorieren Sie diesen Fehler und klicken Sie auf [Beenden], sofern die Firmware aktualisiert ist. Wenn keine Aktualisierung erfolgt ist, überprüfen Sie die folgenden Punkte und aktualisieren Sie die Produkt-Firmware oder die HyPAS-Anwendung erneut. • Das Netzwerk ist verbunden • Das Produkt ist eingeschaltet • Wenn Sie die Produktfirmware aktualisieren möchten, darf diese Anwendung nicht durch eine Firewall blockiert werden • Wenden Sie sich an Ihren Kundendienstmitarbeiter, falls das Problem fortbesteht.
Fehler Upgrade fehlgeschlagen. Grund: Master-Dateiversionsfehler	
Fehler Upgrade fehlgeschlagen. Grund: Firmware-Datei kann nicht auf Gerät geschrieben werden.	
Fehler Upgrade fehlgeschlagen. Grund: Dieses HTTP/HTTPS-Port-Nummer (#) wurde benutzt. Bitte ein anderes angeben HTTP/HTTPS-Port-Nummer in einstellungen und erneut versuchen.	Die auf dem Einstellungsbildschirm angegebene HTTP/HTTPS-Port-Nummer wird bereits verwendet. Geben Sie eine freie Anschlussnummer an. Unter Windows Freie Anschlussnummern finden Sie in der Eingabeaufforderung mit dem Befehl „netstat“. Unter Mac Freie Anschlussnummern finden Sie in Terminal mit dem Befehl „netstat“ oder „lsof“.

Mitteilung	Korrekturmaßnahme
	Unter Linux Freie Anschlussnummern finden Sie im Terminal mit dem Befehl „ss“ oder „lsof“.