



**DS-900WN DS-800WN**

# **Administratorhandbuch**

---

**Empfohlene Einstellungen für spezielle Aufgaben**

---

**Netzwerkeinstellungen**

---

**Erforderliche Einstellungen für das Scannen**

---

**Einfache Sicherheitseinstellungen**

---

**Erweiterte Sicherheitseinstellungen**

---

**Verwenden von Epson Open Platform**

# Copyright

Kein Teil dieser Veröffentlichung darf ohne die schriftliche Erlaubnis von Seiko Epson Corporation auf irgendeine Weise, ob elektronisch, mechanisch, als Fotokopie, Aufzeichnung oder anderweitig reproduziert, in einem Datenabrufsystem gespeichert oder übertragen werden. Das Unternehmen übernimmt keine patentrechtliche Haftung bezüglich der hierin enthaltenen Informationen. Ebenfalls wird keine Haftung übernommen für Schäden, die sich aus der Verwendung der hierin enthaltenen Informationen ergeben. Die hierin enthaltenen Informationen sind nur zur Verwendung mit diesem Epson-Produkt beabsichtigt. Epson übernimmt keine Verantwortung für die Verwendung dieser Informationen im Zusammenhang mit anderen Produkten.

Weder Seiko Epson Corporation noch seine Partner haften gegenüber dem Käufer dieses Produkts oder gegenüber Dritten für Schäden, Verluste, Kosten oder Aufwendungen, die dem Käufer oder Dritten als Folge von Unfällen, falschem oder missbräuchlichem Gebrauch dieses Produkts, durch unautorisierte Modifikationen, Reparaturen oder Abänderungen dieses Produkts oder (ausgenommen USA) durch Nichtbefolgung der Bedienungs- und Wartungsanweisungen von Seiko Epson Corporation entstehen.

Seiko Epson Corporation und seine Partner haften für keine Schäden oder Probleme, die durch die Verwendung anderer Optionsprodukte oder Verbrauchsmaterialien entstehen, die nicht als Original Epson-Produkte oder von Seiko Epson Corporation genehmigte Epson-Produkte gekennzeichnet sind.

Seiko Epson Corporation haftet nicht für Schäden infolge elektromagnetischer Störungen, welche durch andere Schnittstellenkabel entstehen, die nicht als von Seiko Epson Corporation genehmigte Epson-Produkte gekennzeichnet sind.

© 2024 Seiko Epson Corporation

Der Inhalt dieses Handbuchs und die technischen Daten dieses Produkts können ohne Vorankündigung geändert werden.

# Markenhinweis

- ❑ Microsoft, Windows, Windows Server, Microsoft Edge, SharePoint, and Internet Explorer are trademarks of the Microsoft group of companies.
- ❑ Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- ❑ Chrome, Chromebook and Android are trademarks of Google LLC.
- ❑ Wi-Fi®, Wi-Fi Direct®, and Wi-Fi Protected Access® are registered trademarks of Wi-Fi Alliance®. Wi-Fi Protected Setup™, WPA2™, WPA3™ are trademarks of Wi-Fi Alliance®.
- ❑ The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- ❑ The Mopria™ word mark and the Mopria™ Logo are registered and/or unregistered trademarks of Mopria Alliance, Inc. in the United States and other countries. Unauthorized use is strictly prohibited.
- ❑ Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- ❑ Allgemeiner Hinweis: alle anderen Marken sind das Eigentum ihrer jeweiligen Besitzer und werden nur zu Identifikationszwecken verwendet.

---

# Inhalt

## Copyright

## Markenhinweis

## Einleitung

Der Inhalt dieses Dokuments. . . . .	8
Verwendung dieser Anleitung. . . . .	8
Marken und Symbole. . . . .	8
In dieser Anleitung verwendete Beschreibungen. . . . .	8
Betriebssysteme. . . . .	8

## Hinweise zum Administratorkennwort

Hinweise zum Administratorkennwort. . . . .	11
Anfängliches Administratorkennwort. . . . .	11
Vorgänge, die ein Administratorkennwort voraussetzen. . . . .	11
Andern des Administratorkennworts. . . . .	11
Zurücksetzen des Administratorkennworts. . . . .	11

## Empfohlene Einstellungen für spezielle Aufgaben

Empfohlene Einstellungen für spezielle Aufgaben. . .	14
--	----

## Netzwerkeinstellungen

Verbinden des Scanners mit dem Netzwerk. . . . .	17
Vor dem Einrichten einer Netzwerkverbindung. .	17
Verbindung zum Netzwerk über das Bedienfeld herstellen. . . . .	19
Hinzufügen oder Ersetzen von Computer oder Geräten. . . . .	24
Verbinden mit einem Scanner, der mit dem Netzwerk verbunden ist. . . . .	24
Direktes Verbinden eines Smart-Geräts mit dem Scanner (Wi-Fi Direct). . . . .	26
Erneutes Konfigurieren der Netzwerkverbindung. . . . .	28
Überprüfen des Netzwerkverbindungsstatus. . . . .	30
Überprüfen des Netzwerkverbindungsstatus über das Bedienfeld. . . . .	30
Technische Daten des Netzwerks. . . . .	32
WLAN-Spezifikationen. . . . .	32

Ethernet-Spezifikationen. . . . .	33
Netzwerkfunktionen und Unterstützung für IPv4/IPv6. . . . .	34
Sicherheitsprotokoll. . . . .	34
Verwendeter Scannerport. . . . .	34
Probleme lösen. . . . .	35
Netzwerkverbindung kann nicht hergestellt werden. . . . .	35

## Software für das Einrichten des Scanners

Anwendung für das Konfigurieren des Scannerbetriebs (Web Config). . . . .	40
Ausführen von Web Config in einem Webbrowser. . . . .	40
Epson Device Admin. . . . .	41
Konfigurationsvorlage. . . . .	42

## Erforderliche Einstellungen für das Scannen

Registrieren eines E-Mail-Servers. . . . .	47
Überprüfen einer Verbindung zum E-Mail- Server. . . . .	48
Erstellen eines Netzwerkordners. . . . .	50
Kontakte zur Verfügung stellen. . . . .	57
Vergleich der Kontaktkonfiguration. . . . .	58
Registrieren eines Ziels für Kontakte mit Web Config. . . . .	58
Registrieren von Zielen als Gruppe mit Web Config. . . . .	60
Sichern und Importieren von Kontakten. . . . .	61
Exportieren und Mengenregistrierung von Kontakten mithilfe eines Tools. . . . .	62
Kooperation zwischen LDAP-Server und Benutzern. . . . .	64
Einrichten von AirPrint. . . . .	67
Probleme bei der Vorbereitung von Netzwerk- Scans. . . . .	68
Hinweise zur Fehlerbehebung. . . . .	68
Zugriff auf Web Config nicht möglich. . . . .	68

## Anpassen der Bedienfeldanzeige

Registrieren von Voreinst. . . . .	71
Menüoptionen von Voreinst. . . . .	72
Editieren des Bedienfeld-Startbildschirms. . . . .	73

Ändern des Layout des Startbildschirms. . . . .	73
Symbol zufügen. . . . .	74
Symbol entfernen. . . . .	75
Symbol verschieben. . . . .	76

## **Einfache Sicherheitseinstellungen**

Einführung in die Sicherheitsfunktionen des Produkts. . . . .	78
Administratoreinstellungen. . . . .	78
Konfigurieren des Administratorkennworts. . . . .	78
Verwenden der Sperreinstellung für das Bedienfeld. . . . .	80
Anmelden als Administrator am Bedienfeld. . . . .	83
Einschränken der Verfügbarkeit von Funktionen (Zugangssteuerung). . . . .	84
Erstellen des Benutzerkontos. . . . .	84
Aktivieren der Zugangssteuerung. . . . .	85
Anmelden bei einem Scanner, auf dem Zugangssteuerung aktiviert ist. . . . .	85
Deaktivieren der externen Schnittstelle. . . . .	86
Aktivieren der Programmüberprüfung beim Start. . . . .	87
Deaktivieren des Netzwerk-Scannens auf dem Computer. . . . .	87
Aktivieren oder Deaktivieren des WSD Scanners. . . . .	87
Überwachen eines Remote-Scanners. . . . .	88
Überprüfen von Informationen für einen entfernten Scanner. . . . .	88
Empfang von E-Mail-Benachrichtigungen bei Ereignissen. . . . .	88
Verwenden von Web Config zur Steuerung der Stromversorgung des Scanners. . . . .	90
Wiederherstellen der-Standard-einstellungen. . . . .	90
Epson Remote Services-Information. . . . .	90
Probleme lösen. . . . .	90
Das Administratorkennwort wurde vergessen. . . . .	90

## **Erweiterte Sicherheitseinstellungen**

Sicherheitseinstellungen und Gefahrenvermeidung. . . . .	93
Sicherheitsfunktionseinstellungen. . . . .	94
Steuern anhand von Protokollen. . . . .	94
Protokolle kontrollieren. . . . .	94
Aktivierbare und Deaktivierbare Protokolle. . . . .	94
Protokoll-Einstellungen. . . . .	95
Verwenden eines digitalen Zertifikats. . . . .	97
Über digitale Zertifizierung. . . . .	97
Konfigurieren eines CA-signiertes Zertifikat. . . . .	98
Aktualisieren eines selbstsignierten Zertifikats. . . . .	101

Konfigurieren eines CA-Zertifikat. . . . .	102
SSL/TLS-Kommunikation mit dem Scanner. . . . .	103
Konfigurieren grundlegender SSL/TLS-Einstellungen. . . . .	103
Konfiguration eines Serverzertifikats für den Scanner. . . . .	104
Verschlüsselte Kommunikation mit IPsec/IP-Filterung. . . . .	104
Über IPsec/IP-Filterung. . . . .	104
Konfigurieren der Standardrichtlinie. . . . .	104
Konfigurieren der Gruppenrichtlinie. . . . .	108
Konfigurationsbeispiele für IPsec/IP-Filterung. . . . .	114
Konfigurieren eines Zertifikats für IPsec/IP-Filterung. . . . .	115
Verbinden des Scanners mit einem IEEE802.1X-Netzwerk. . . . .	116
Konfiguration eines IEEE 802.1X-Netzwerks. . . . .	116
Konfigurieren eines Zertifikats für IEEE 802.1X . . . . .	117
Beheben von Problemen für erweiterte Sicherheit. . . . .	118
Wiederherstellen der Sicherheitseinstellungen. . . . .	118
Probleme bei Verwendung der Netzwerksicherheitsfunktionen. . . . .	118
Probleme bei der Verwendung eines digitalen Zertifikats. . . . .	120

## **Verwenden von Epson Open Platform**

Epson Open Platform Übersicht. . . . .	125
Konfigurieren von Epson Open Platform. . . . .	125
Validierung von Epson Open Platform. . . . .	125

## **Mounting eines Authentifizierungsgeräts**

Verbinden des Authentifizierungsgeräts. . . . .	128
Funktionsprüfung des Authentifizierungsgeräts. . . . .	128
Überprüfen der Erkennung der Authentifizierungskarte. . . . .	128
Fehlerbehebung bei Problemen mit dem Authentifizierungsgerät. . . . .	129
Authentifizierungskarte kann nicht gelesen werden. . . . .	129

## **Wartung**

Äußerliches Reinigen des Scanners. . . . .	131
Reinigen der Innenbereiche des Scanners. . . . .	131
Austauschen des Roller-Assembly-Kits. . . . .	136
Codes für Roller-Assembly-Kit. . . . .	141

---

Zurücksetzen der Anzahl der Scans nach dem Austauschen der Rollen. . . . .	141
Energie sparen. . . . .	142
Transportieren des Scanners. . . . .	142
Sichern der Einstellungen. . . . .	143
Einstellungen exportieren. . . . .	143
Importieren der Einstellungen. . . . .	144
Werkseinstlg. wiederh.. . . .	144
Aktualisieren von Anwendungen und Firmware. . .	145
Aktualisieren der Scannerfirmware über das Bedienfeld. . . . .	146
Aktualisieren der Firmware mit Web Config. . .	146
Aktualisieren der Firmware ohne Internetverbindung. . . . .	147

---

# Einleitung

Der Inhalt dieses Dokuments. . . . .	8
Verwendung dieser Anleitung. . . . .	8

---

## Der Inhalt dieses Dokuments

Dieses Dokument enthält die folgenden Informationen für Scanner-Administratoren.

- Netzwerkeinstellungen
- Vorbereiten der Scanfunktion
- Aktivieren und Verwalten von Sicherheitseinstellungen
- Durchführen der täglichen Wartung

Die Standardmethoden zur Verwendung des Scanners finden Sie im *Benutzerhandbuch*.

---

## Verwendung dieser Anleitung

### Marken und Symbole



**Achtung:**

Anweisungen, die sorgfältig befolgt werden müssen, um Verletzungen zu vermeiden.



**Wichtig:**

Anweisungen, die befolgt werden müssen, um Geräteschäden zu vermeiden.

**Hinweis:**

Bietet zusätzliche Informationen als Referenz.

### Zugehörige Informationen

- ➔ Verweist auf zugehörige Abschnitte.

## In dieser Anleitung verwendete Beschreibungen

- Bildschirmabbildungen der Anwendungen wurden unter Windows 10 oder macOS High Sierra erstellt. Die Bildschirminhalte variieren je nach Modell und Situation.
- Sämtliche Illustrationen in dieser Anleitung dienen lediglich zur Orientierung. Obwohl die Darstellungen leicht vom tatsächlichen Aussehen des Produkts abweichen können, ändert sich nichts an der Bedienung.

## Betriebssysteme

### Windows

Im vorliegenden Handbuch beziehen sich Begriffe wie „Windows 11“, „Windows 10“, „Windows 8.1“, „Windows 8“, „Windows 7“, „Windows Server 2022“, „Windows Server 2019“, „Windows Server 2016“, „Windows Server 2012 R2“, „Windows Server 2012“, „Windows Server 2008 R2“ und „Windows Server 2008“ auf die folgenden Betriebssysteme. Darüber hinaus bezieht sich der Begriff „Windows“ auf alle Windows-Versionen.

- Betriebssystem Microsoft® Windows® 11
- Betriebssystem Microsoft® Windows® 10
- Betriebssystem Microsoft® Windows® 8.1
- Betriebssystem Microsoft® Windows® 8
- Betriebssystem Microsoft® Windows® 7
- Betriebssystem Microsoft® Windows Server® 2022
- Betriebssystem Microsoft® Windows Server® 2019
- Betriebssystem Microsoft® Windows Server® 2016
- Betriebssystem Microsoft® Windows Server® 2012 R2
- Betriebssystem Microsoft® Windows Server® 2012
- Betriebssystem Microsoft® Windows Server® 2008 R2
- Betriebssystem Microsoft® Windows Server® 2008

### **Mac OS**

In diesem Handbuch bezieht sich „Mac OS“ auf Mac OS X 10.9 oder höher sowie macOS 11 oder höher.

---

# Hinweise zum Administrator Kennwort

Hinweise zum Administrator Kennwort. . . . .	11
Anfängliches Administrator Kennwort. . . . .	11
Vorgänge, die ein Administrator Kennwort voraussetzen. . . . .	11
Ändern des Administrator Kennworts. . . . .	11
Zurücksetzen des Administrator Kennworts. . . . .	11

---

## Hinweise zum Administratorkennwort

Sie können für dieses Gerät ein Administratorkennwort festlegen, um zu verhindern, dass unbefugte Dritte auf die Geräteeinstellungen oder die im Gerät gespeicherten Netzwerkeinstellungen zugreifen oder sie ändern, wenn das Gerät mit einem Netzwerk verbunden ist.

Wenn Sie ein Administratorkennwort eingerichtet haben, müssen Sie dieses Kennwort eingeben, wenn Sie Einstellungen in der Konfigurationssoftware z. B. Web Config ändern.

Der Scanner hat ein anfängliches Administratorkennwort, Sie können es jedoch beliebig ändern.

---

## Anfängliches Administratorkennwort

Das anfängliche Administratorkennwort variiert und ist auf dem Etikett des Produkts angegeben. Wenn sich auf der Rückseite ein Etikett „PASSWORD“ befindet, geben Sie die achtstellige Zahl auf dem Etikett ein. Wenn kein Etikett „PASSWORD“ vorhanden ist, geben Sie die Seriennummer auf dem Etikett auf der Rückseite des Produkts als anfängliches Administratorkennwort ein.

Wir empfehlen das anfängliche Administratorkennwort in den Standardeinstellungen zu ändern.

**Hinweis:**

*Als Standard ist kein Benutzername festgelegt.*

---

## Vorgänge, die ein Administratorkennwort voraussetzen

Wenn Sie bei einem der folgenden Vorgänge aufgefordert werden, ein Administratorkennwort einzugeben, geben Sie das für das Produkt festgelegte Administratorkennwort ein.

- Anmeldung bei den erweiterten Einstellungen von Web Config
- Bedienung eines Menüs, das vom Administrator gesperrt wurde, auf dem Bedienfeld
- Ändern der Geräteeinstellungen in der Anwendung
- Aktualisierung der Firmware des Gerätes
- Ändern oder Zurücksetzen des Administratorkennworts

---

## Ändern des Administratorkennworts

Sie können es auf dem Bedienfeld des Produktes oder in Web Config ändern.

Das neue Kennwort muss zwischen 8 und 20 Zeichen lang sein und darf nur alphanumerische Zeichen und Symbole im Ein-Byte-Format enthalten.

---

## Zurücksetzen des Administratorkennworts

Sie können das Administratorkennworts auf dem Bedienfeld des Produkts oder in Web Config auf die anfängliche Einstellung zurücksetzen.

Wenn Sie das Kennwort vergessen haben und es nicht auf die Standardeinstellung zurücksetzen können, muss das Produkt repariert werden. Kontaktieren Sie Ihren Fachhändler.

---

# **Empfohlene Einstellungen für spezielle Aufgaben**

Empfohlene Einstellungen für spezielle Aufgaben. . . . . 14

## Empfohlene Einstellungen für spezielle Aufgaben

Im Folgenden finden Sie die notwendigen Einstellungen für Ihre Zwecke.

### Verbinden des Scanners mit dem Netzwerk

Zweck	Erforderliche Einstellungen
Ich möchte den Scanner an das Netzwerk anschließen.	Richten Sie Ihren Scanner für das Netzwerk-Scannen ein. „Verbinden des Scanners mit dem Netzwerk“ auf Seite 17
Ich möchte den Scanner an einen neuen Computer anschließen.	Nehmen Sie die Netzwerkeinstellungen für Ihren Scanner auf dem neuen Computer vor. „Hinzufügen oder Ersetzen von Computer oder Geräten“ auf Seite 24

### Einstellungen für das Scannen

Zweck	Erforderliche Einstellungen
Ich möchte gescannte Bilder per E-Mail versenden. (An eMail scannen)	1. Richten Sie den E-Mail-Server ein, den Sie verknüpfen möchten. „Registrieren eines E-Mail-Servers“ auf Seite 47  2. Registrieren Sie die E-Mail-Adresse des Empfängers in den <b>Kontakte</b> (optional). Durch die Registrierung der E-Mail-Adresse müssen Sie diese nicht jedes Mal eingeben, wenn Sie etwas senden möchten, sondern können sie einfach aus Ihren Kontakten auswählen. „Kontakte zur Verfügung stellen“ auf Seite 57
Ich möchte gescannte Bilder in einem Ordner im Netzwerk speichern. (In Netzwerkordner/FTP scannen)	1. Erstellen Sie einen Ordner im Netzwerk, in dem Sie die Bilder speichern möchten. „Erstellen eines Netzwerkordners“ auf Seite 50  2. Registrieren Sie den Pfad zu dem Ordner in <b>Kontakte</b> (optional). Durch die Registrierung des Ordnerpfads müssen Sie diese nicht jedes Mal eingeben, wenn Sie etwas senden möchten, sondern können ihn einfach aus Ihren Kontakten auswählen. „Kontakte zur Verfügung stellen“ auf Seite 57
Ich möchte gescannte Bilder in einem Cloud-Dienst ablegen. (In Cloud scannen)	Einrichten von Epson Connect. Weitere Informationen zur Einrichten finden Sie auf der Epson Connect-Portal-Website.  Bei der Einrichtung benötigen Sie ein Benutzerkonto für den Online-Speicherdienst, mit dem Sie eine Verbindung herstellen möchten. <a href="https://www.epsonconnect.com/">https://www.epsonconnect.com/</a> <a href="http://www.epsonconnect.eu">http://www.epsonconnect.eu</a> (nur Europa)

### Anpassen der Bedienfeldanzeige

Zweck	Erforderliche Einstellungen
Ich möchte die auf dem Bedienfeld des Scanners angezeigten Elemente ändern.	Legen <b>Voreinst.</b> oder <b>Startbild bearbeiten</b> fest. Sie können Ihre bevorzugten Scaneinstellungen auf dem Bedienfeld registrieren und die angezeigten Elemente bearbeiten. „Anpassen der Bedienfeldanzeige“ auf Seite 70

### Einstellen grundlegender Sicherheitsfunktionen

Zweck	Erforderliche Einstellungen
Ich möchte verhindern, dass jemand anderes als der Administrator die Scanner-Einstellungen ändert.	Legen Sie ein Administrator Kennwort für den Scanner fest. <a href="#">„Administratoreinstellungen“ auf Seite 78</a>
Ich möchte die Verwendung von Scannern bei USB-Anschluss deaktivieren.	Deaktivieren der externen Schnittstelle. <a href="#">„Deaktivieren der externen Schnittstelle“ auf Seite 86</a>

### Einstellen erweiterter Sicherheitsfunktionen

Zweck	Erforderliche Einstellungen
Ich möchte kontrollieren, welche Protokolle verwendet werden sollen.	Aktivieren oder Deaktivieren von Protokollen. <a href="#">„Steuern anhand von Protokollen“ auf Seite 94</a>
Ich möchte den Kommunikationspfad verschlüsseln.	1. Einrichten des digitalen Zertifikats. <a href="#">„Verwenden eines digitalen Zertifikats“ auf Seite 97</a> 2. Konfigurieren der SSL/TLS-Kommunikation. <a href="#">„SSL/TLS-Kommunikation mit dem Scanner“ auf Seite 103</a>
Ich möchte verschlüsselte Kommunikation (IPsec) verwenden. Ich möchte die Software nur von einem bestimmten Computer aus nutzen können (IP-Filterung).	Richtlinien zur Filterung des Datenverkehrs einrichten. <a href="#">„Verschlüsselte Kommunikation mit IPsec/IP-Filterung“ auf Seite 104</a>
Ich möchte einen Scanner in einem IEEE802.1X verwenden.	Einrichten von IEEE802.1X für den Scanner. <a href="#">„Verbinden des Scanners mit einem IEEE802.1X-Netzwerk“ auf Seite 116</a>

### Synchronisieren des Scanners mit einem Authentifizierungssystem

Beziehen Sie von der speziellen Website den Produktschlüssel und aktivieren Sie Epson Open Platform auf Ihrem Scanner.

[„Verwenden von Epson Open Platform“ auf Seite 124](#)

### Verwenden der Authentifizierungsoption (Epson Print Admin/Epson Print Admin Serverless)

Sie benötigen einen Lizenzschlüssel, um diese Option verwenden zu können.

Weitere Informationen erhalten Sie von Ihrem Händler.

**Hinweis:**

*Sie können Epson Print Admin Serverless nicht verwenden, wenn das System mit Epson Open Platform synchronisiert ist.*

---

# Netzwerkeinstellungen

Verbinden des Scanners mit dem Netzwerk. . . . .	17
Hinzufügen oder Ersetzen von Computer oder Geräten. . . . .	24
Überprüfen des Netzwerkverbindungsstatus. . . . .	30
Technische Daten des Netzwerks. . . . .	32
Probleme lösen. . . . .	35

## Verbinden des Scanners mit dem Netzwerk

In diesem Abschnitt wird die Vorgehensweise zum Anschluss des Scanners an das Netzwerk über das Bedienfeld des Scanners erläutert.

### Hinweis:

Wenn sich der Scanner und der Computer im selben Segment befinden, können Sie sie mit dem Installationsprogramm verbinden.

Rufen Sie folgende Website auf und geben Sie den Produktnamen ein, um das Installationsprogramm zu starten. Rufen Sie **Setup** auf, und beginnen Sie dann die Einrichtung.

<https://epson.sn>

Sie finden die Betriebsanweisungen in den Webfilmanleitungen. Rufen Sie sie unter der folgenden URL auf.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

## Vor dem Einrichten einer Netzwerkverbindung

Prüfen Sie für die Verbindung mit dem Netzwerk zuvor die Verbindungsmethode und die Verbindungseinstellungen.

## Sammeln von Informationen über die Verbindungseinstellung

Bereiten Sie die erforderlichen Einstellinformationen für die Verbindung vor. Überprüfen Sie vorab die folgenden Informationen.

Abschnitte	Optionen	Hinweis
Methode der Geräteverbindung	<input type="checkbox"/> Ethernet <input type="checkbox"/> Wi-Fi	Entscheiden Sie, wie der Scanner an das Netzwerk angeschlossen wird.  Bei verkabeltem LAN wird die Verbindung zum LAN-Switch hergestellt.  Bei WLAN wird die Verbindung mit dem Netzwerk (SSID) des Zugangspunktes hergestellt.
LAN-Verbindungsdaten	<input type="checkbox"/> IP-Adresse <input type="checkbox"/> Subnetzmaske <input type="checkbox"/> Standard-Gateway	Legen Sie die IP-Adresse fest, die dem Scanner zugewiesen werden soll.  Wenn Sie die IP-Adresse statisch zuweisen, werden alle Werte benötigt.  Wenn Sie die IP-Adresse über die DHCP-Funktion dynamisch zuweisen, ist diese Information nicht erforderlich, da sie automatisch eingestellt wird.
WLAN-Verbindungsdaten	<input type="checkbox"/> SSID <input type="checkbox"/> Passwort	Dies sind die SSID (Netzwerkname) und das Passwort des Zugangspunktes, mit dem sich der Scanner verbindet.  Wenn die MAC-Adressfilterung eingestellt ist, registrieren Sie die MAC-Adresse des Scanners im Voraus, um den Scanner zu registrieren.  Im Folgenden finden Sie die unterstützten Standards.  „Technische Daten des Netzwerks“ auf Seite 32

Abschnitte	Optionen	Hinweis
DNS-Serverdaten	<input type="checkbox"/> IP-Adresse des primären DNS-Servers <input type="checkbox"/> IP-Adresse des sekundären DNS-Servers	Diese werden bei der Angabe von DNS-Servern benötigt. Das sekundäre DNS wird eingestellt, wenn das System eine redundante Konfiguration hat und es einen sekundären DNS-Server gibt.  Wenn Sie in einer kleinen Organisation sind und den DNS-Server nicht einstellen, dann stellen Sie die IP-Adresse des Routers ein.
Daten des Proxyservers	<input type="checkbox"/> Name des Proxyservers	Stellen Sie dies ein, wenn Ihre Netzwerkumgebung den Proxy-Server für den Internetzugang aus dem Intranet verwendet, und Sie die Funktion verwenden, dass der Scanner direkt auf das Internet zugreift.  Für die folgenden Funktionen stellt der Scanner eine direkte Verbindung zum Internet her. <ul style="list-style-type: none"> <li><input type="checkbox"/> Epson-Connect-Dienste</li> <li><input type="checkbox"/> Cloud-Dienste anderer Unternehmen</li> <li><input type="checkbox"/> Firmware-Aktualisierung</li> <li><input type="checkbox"/> Senden von gescannten Bildern an SharePoint (WebDAV)</li> </ul>
Portnummer-Angaben	<input type="checkbox"/> Freizugebende Portnummer	Überprüfen Sie die Portnummer des Scanners und des Computers und geben Sie dann falls erforderlich den Port frei, der durch eine Firewall blockiert ist.  Im Folgenden finden Sie die Portnummer, die vom Scanner verwendet wird.  <a href="#">„Verwendeter Scannerport“ auf Seite 34</a>

## IP-Adresszuweisung

IP-Adressen können auf folgende Arten zugewiesen werden.

### Statische IP-Adresse:

Es wird eine manuell vergebene IP-Adresse an den Scanner (Host) vergeben.

Die für die Verbindung mit dem Netzwerk erforderlichen Angaben (Subnetzmaske, Standardgateway, DNS-Server usw.) müssen manuell eingestellt werden.

Die IP-Adresse ändert sich auch dann nicht, wenn das Gerät ausgeschaltet wird. Daher eignet sich diese Einstellung zur Verwaltung von Geräten in einer Umgebung, in denen die IP-Adresse nicht verändert werden kann bzw. Geräte anhand der IP-Adresse verwaltet werden sollen. Diese Einstellung empfiehlt sich für Scanner, Server usw., auf die von vielen Computern zugegriffen wird. Weisen Sie eine feste IP-Adresse auch dann zu, wenn Funktionen wie IPsec/IP-Filterung verwendet werden, damit sich die IP-Adresse nicht ändert.

### Automatisches Zuweisen mithilfe der DHCP-Funktion (dynamische IP-Adresse):

Die IP-Adresse wird dem Scanner (Host) automatisch über die DHCP-Funktion des DHCP-Servers oder Routers zugewiesen.

Die Angaben zur Verbindung mit dem Netzwerk (Subnetzmaske, Standardgateway, DNS-Server usw.) werden automatisch festgelegt, damit Sie das Gerät einfach mit dem Netzwerk verbinden können.

Falls das Gerät oder der Router ausgeschaltet wird, kann sich die IP-Adresse je nach den Einstellungen des DHCP-Servers ändern.

Es ist empfehlenswert, dass die Geräteverwaltung in diesem Fall nicht anhand der IP-Adresse erfolgt und Protokolle eingesetzt werden, die der IP-Adresse folgen können.

**Hinweis:**

*Durch Nutzung der DHCP-Funktion zur IP-Adressreservierung lässt sich den Geräten jederzeit dieselbe IP-Adresse zuweisen.*

## DNS-Server und Proxyserver

Der DNS-Server ermittelt aus Hostnamen, Domainnamen für E-Mail-Adressen usw. deren IP-Adresse.

Eine Kommunikation ist nicht möglich, wenn die Gegenstelle zwar über ihren Host- oder Domainnamen bekannt ist, der Computer oder Scanner jedoch nur über IP kommuniziert.

Daher findet eine Abfrage des DNS-Servers nach diesen Angaben statt, der die IP-Adresse der Gegenstelle übermittelt. Dieser Vorgang wird als Auflösung bezeichnet.

Auf diese Weise können Geräte wie Computer und Scanner anhand der IP-Adresse miteinander kommunizieren.

Die Namensauflösung ist auch für die Kommunikation des Scanners per E-Mails und für seine Internetverbindung erforderlich.

Konfigurieren Sie die DNS-Server-Einträge, wenn Sie diese Funktion nutzen.

Wenn Sie die IP-Adresse des Scanners mit Hilfe der DHCP-Funktion des DHCP-Servers oder Routers zuweisen, wird sie automatisch eingestellt.

Der Proxyserver wird am Gateway zwischen Netzwerk und Internet platziert und kommuniziert als Mittler zwischen Computer, Scanner und Internet (Gegenstelle). Der Server der Gegenstelle kommuniziert nur mit dem Proxyserver. Daher hat er keinen Zugriff auf Scannerinformationen wie IP-Adresse und Portnummer, wodurch die Sicherheit verbessert wird.

Konfigurieren Sie auf dem Scanner die Einstellung für den Proxyserver, wenn Sie sich über einen Proxyserver mit dem Internet verbinden.

## Verbindung zum Netzwerk über das Bedienfeld herstellen

Verbinden Sie den Scanner über das Bedienfeld des Scanners mit dem Netzwerk.

### Zuweisen der IP-Adresse

Richten Sie die grundlegenden Elemente wie Host-Adresse, Subnetzmaske und Standard-Gateway ein.

In diesem Abschnitt wird die Vorgehensweise zum Einstellen einer statischen IP-Adresse erläutert.

1. Schalten Sie den Scanner ein.
2. Wählen Sie im Startbildschirm auf dem Bedienfeld des Scanners **Einstellungen**.
3. Wählen Sie **Netzwerkeinstellungen** > **Erweitert** > **TCP/IP**.
4. Wählen Sie **Manuell** bei **IP-Adresse anfordern**.

Wenn Sie die IP-Adresse automatisch über die DHCP-Funktion des Routers einstellen, wählen Sie **Auto**. In diesem Fall werden **IP-Adresse**, **Subnetzmaske** und **Standard-Gateway** in Schritt 5 bis 6 ebenfalls automatisch eingestellt. Fahren Sie daher mit Schritt 7 fort.

5. Eingeben der IP-Adresse.

Der Fokus bewegt sich zum vorderen Segment oder zum hinteren Segment, das durch einen Punkt getrennt ist, wenn Sie ◀ oder ▶ wählen.

Bestätigen Sie den auf dem vorherigen Bildschirm angezeigten Wert.

6. Richten Sie **Subnetzmaske** und **Standard-Gateway** ein.

Bestätigen Sie den auf dem vorherigen Bildschirm angezeigten Wert.



**Wichtig:**

Wenn die Kombination aus IP-Adresse, Subnetzmaske und Standard-Gateway falsch ist, bleibt **Einrichtung starten** inaktiv und kann mit den Einstellungen nicht fortfahren. Bestätigen Sie, dass kein Fehler in der Eingabe vorliegt.

7. Geben Sie die IP-Adresse für den primären DNS-Server ein.

Bestätigen Sie den auf dem vorherigen Bildschirm angezeigten Wert.

**Hinweis:**

Bei Auswahl von **Auto** als Einstellung für die IP-Adresszuteilung lassen sich die DNS-Server-Einstellungen **Manuell** oder **Auto** auswählen. Wenn die DNS-Server-Adresse nicht automatisch abgerufen werden kann, wählen Sie **Manuell** aus, und geben Sie dann die Adresse des DNS-Servers ein. Geben Sie dann die Adresse des sekundären DNS-Servers direkt ein. Falls Sie **Auto** auswählen, wechseln Sie zu Schritt 9.

8. Geben Sie die IP-Adresse für den sekundären DNS-Server ein.

Bestätigen Sie den auf dem vorherigen Bildschirm angezeigten Wert.

9. Tippen Sie auf **Einrichtung starten**.

### **Einrichten des Proxy-Servers**

Richten Sie den Proxy-Server ein, wenn beide der folgenden Punkte erfüllt sind.

- Der Proxy-Server ist für die Internetverbindung ausgelegt.
- Bei Verwendung einer Funktion, bei der sich der Scanner direkt mit dem Internet verbindet, wie beispielsweise dem Epson Connect Service oder den Cloud Services eines anderen Unternehmens.

1. Wählen Sie auf dem Startbildschirm **Einstellungen**.

Wenn Sie Einstellungen nach der Einstellung der IP-Adresse vornehmen, wird der Bildschirm **Erweitert** angezeigt. Fahren Sie mit Schritt 3 fort.

2. Wählen Sie **Netzwerkeinstellungen** > **Erweitert**.

3. Wählen Sie **Proxy-Server**.

4. Wählen Sie **Verw.** bei **Proxy-Servereinst..**

5. Geben Sie die Adresse für den Proxy-Server im IPv4- oder FQDN-Format ein.

Bestätigen Sie den auf dem vorherigen Bildschirm angezeigten Wert.

6. Geben Sie die Portnummer für den Proxy-Server ein.

Bestätigen Sie den auf dem vorherigen Bildschirm angezeigten Wert.

7. Tippen Sie auf **Einrichtung starten**.

## **Anschließen an Ethernet**

So verbinden Sie den Scanner mithilfe eines LAN-Kabels mit dem Netzwerk und prüfen die Verbindung.

1. Verbinden Sie den Scanner mit einem Hub (LAN-Switch), indem Sie eine LAN-Kabel verwenden.
2. Wählen Sie auf dem Startbildschirm .
3. Wählen Sie **Router**.
4. Achten Sie darauf, dass Einstellungen für Verbindung und IP-Adresse korrekt sind.
5. Tippen Sie auf **Schließen**.

## **Verbindung zu einem drahtlosen Netzwerk (WLAN) herstellen**

Sie können den Scanner auf verschiedene Weise mit einem drahtlosen Netzwerk (WLAN) verbinden. Wählen Sie die Verbindungsmethode aus, die Ihrer Umgebung und den Nutzungsbedingungen am besten entspricht.

Falls Ihnen die Zugangsdaten des Wireless-Routers wie dessen SSID und das Kennwort bekannt sind, können Sie die Einstellungen manuell vornehmen.

Falls der Wireless-Router WPS unterstützt, können Sie die Einstellungen per Tastendruck-Setup vornehmen.

Verbinden Sie sich nach Anschluss des Scanners an das Netzwerk von dem gewünschten Gerät aus (Computer, Smartgerät, Tablet usw.) mit dem Scanner

### ***Hinweis bei Verwendung einer WLAN 5 GHz-Verbindung***

Dieses Produkt verwendet normalerweise W52 (36ch) als Kanal für die Verbindung mit Wi-Fi Direct (Simple AP). Da der Kanal für die drahtlose LAN-Verbindung (Wi-Fi) automatisch ausgewählt wird, kann der verwendete Kanal bei gleichzeitiger Verwendung mit einer Wi-Fi Direct-Verbindung abweichen. Wenn die Kanäle unterschiedlich sind, kann die Datenkommunikation mit dem Scanner langsam sein. Wenn die Nutzung nicht gestört wird, verbinden Sie sich mit der SSID im 2,4-GHz-Band. Im 2,4-GHz-Frequenzband werden die verwendeten Kanäle übereinstimmen.

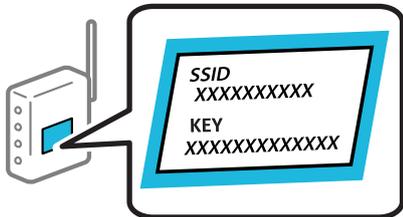
Wenn Sie das drahtlose LAN auf 5 GHz einstellen, empfehlen wir, Wi-Fi Direct zu deaktivieren.

### ***Vornehmen von Wi-Fi-Einstellungen durch Eingabe der SSID und des Kennworts***

Sie können ein Wi-Fi-Netzwerk einrichten, indem Sie die nötigen Informationen im Scannerbedienfeld eingeben, um sich mit einem Wireless-Router zu verbinden. Für die Einrichtung mit dieser Methode benötigen Sie die SSID und das Kennwort für einen Wireless-Router.

**Hinweis:**

Wenn Sie einen Wireless-Router mit seinen Standardeinstellungen verwenden, finden Sie die SSID und das Kennwort auf dem Aufkleber. Wenn Sie SSID und Passwort nicht wissen, wenden Sie sich an die Person, die den Wireless-Router eingerichtet hat oder sehen Sie in der mit dem Zugangspunkt gelieferten Dokumentation nach.



1. Tippen Sie auf dem Startbildschirm auf .
2. Wählen Sie **Router**.
3. Tippen Sie auf **Setup starten**.

Wenn die Netzwerkverbindung bereits eingerichtet ist, werden die Verbindungsdetails angezeigt. Tippen Sie auf **Zu Wi-Fi-Verbindung wechseln**, oder **Einstellungen ändern**, um die Einstellungen zu ändern.

4. Wählen Sie **WLAN-Einrichtungsassistent**.
5. Befolgen Sie die Anweisungen auf dem Bildschirm, um die SSID auszuwählen, das Passwort für den Wireless Router einzugeben und die Einrichtung zu starten.

Wenn Sie den Status der Netzwerkverbindung für den Scanner nach Abschluss der Installation überprüfen möchten, finden Sie weitere Informationen unter dem entsprechenden Link unten.

**Hinweis:**

- Falls Sie die SSID nicht kennen, sehen Sie bitte nach, ob sie sich auf dem Aufkleber am Wireless-Router befindet. Falls Sie den Wireless-Router mit seinen Standardeinstellungen verwenden, können Sie die auf dem Aufkleber aufgedruckte SSID verwenden. Wenn Sie keine Informationen finden, beziehen Sie sich auf die mit dem Wireless-Router mitgelieferte Dokumentation.
- Beachten Sie die Groß-/Kleinschreibung beim Kennwort.
- Falls Sie das Kennwort nicht kennen, sehen Sie bitte nach, ob es sich auf dem Aufkleber am Wireless-Router befindet. Auf dem Aufkleber kann das Kennwort als „Network Key“ oder „Wireless Password“ usw. angegeben sein. Falls Sie den Wireless-Router mit seinen Standardeinstellungen verwenden, können Sie das auf dem Aufkleber aufgedruckte Kennwort verwenden.
- Wenn Sie die SSID nicht sehen, mit der Sie sich verbinden möchten, richten Sie das WLAN auf Ihrem Computer oder Smartgerät, wie z. B. Smartphone oder Tablet, mit Software oder einer App ein. Um weitere Informationen zu erhalten, geben Sie in Ihren Browser „<https://epson.sn>“ und rufen die Website auf. Geben Sie Ihren Namen oder Ihr Produkt ein und gehen Sie zu **Setup**.

**Zugehörige Informationen**

➔ „Überprüfen des Netzwerkverbindungsstatus“ auf Seite 30

**Einrichten der WLAN-Einstellungen per Tastendruck (WPS)**

Ein Wi-Fi-Netzwerk kann durch Drücken einer Taste am Wireless-Router automatisch eingerichtet werden. Diese Methode ist dann geeignet, wenn folgende Bedingungen erfüllt sind.

- Der Wireless-Router ist mit WPS (Wi-Fi Protected Setup) kompatibel.

- Die aktuelle Wi-Fi-Verbindung wurde durch Drücken einer Taste am Wireless-Router hergestellt.

**Hinweis:**

Wenn Sie die Taste nicht finden können oder die Software zur Einrichtung verwenden, nehmen Sie die mit dem Wireless-Router gelieferte Dokumentation zur Hand.

1. Tippen Sie auf der Startseite auf .
2. Wählen Sie **Router**.
3. Tippen Sie auf **Setup starten**.

Wenn die Netzwerkverbindung bereits eingerichtet ist, werden die Verbindungsdetails angezeigt. Tippen Sie auf **Zu Wi-Fi-Verbindung wechseln**, oder **Einstellungen ändern**, um die Einstellungen zu ändern.

4. Wählen Sie **Tastendruck-Setup (WPS)**.
5. Lassen Sie sich von den Hinweisen auf dem Bildschirm durch die nötigen Schritte führen.

Wenn Sie den Status der Netzwerkverbindung für den Scanner nach Abschluss der Installation überprüfen möchten, finden Sie weitere Informationen unter dem entsprechenden Link unten.

**Hinweis:**

Wenn keine Verbindung hergestellt werden kann, starten Sie den Wireless-Router neu, verringern Sie den Abstand des Wireless-Routers zum Scanner und versuchen Sie es erneut.

**Zugehörige Informationen**

➔ [„Überprüfen des Netzwerkverbindungsstatus“ auf Seite 30](#)

**Einrichten der WLAN-Einstellungen per PIN-Code (WPS)**

Mit einem PIN-Code können Sie die Verbindung zu einem Wireless-Router automatisch herstellen. Sie können diese Setupmethode verwenden, wenn der Wireless-Router WPS-fähig (Wi-Fi Protected Setup) ist. Geben Sie über einen Computer einen PIN-Code in den Wireless-Router ein.

1. Tippen Sie auf der Startseite auf .
2. Wählen Sie **Router**.
3. Tippen Sie auf **Setup starten**.

Wenn die Netzwerkverbindung bereits eingerichtet ist, werden die Verbindungsdetails angezeigt. Tippen Sie auf **Zu Wi-Fi-Verbindung wechseln**, oder **Einstellungen ändern**, um die Einstellungen zu ändern.

4. Wählen Sie **Sonstiges > PIN-Code-Setup (WPS)**
5. Lassen Sie sich von den Hinweisen auf dem Bildschirm durch die nötigen Schritte führen.

Wenn Sie den Status der Netzwerkverbindung für den Scanner nach Abschluss der Installation überprüfen möchten, finden Sie weitere Informationen unter dem entsprechenden Link unten.

**Hinweis:**

Ausführliche Informationen zur Eingabe eines PIN-Codes finden Sie in der mit dem Wireless-Router gelieferten Dokumentation.

### Zugehörige Informationen

➔ „Überprüfen des Netzwerkverbindungsstatus“ auf Seite 30

---

## Hinzufügen oder Ersetzen von Computer oder Geräten

### Verbinden mit einem Scanner, der mit dem Netzwerk verbunden ist

Wenn der Scanner bereits mit dem Netzwerk verbunden ist, können Sie über das Netzwerk einen Computer oder ein Smart-Gerät mit dem Scanner verbinden.

### Verwenden eines Netzwerkscanners von einem zweiten Computer

Wir empfehlen die Verwendung eines Installationsprogramms, um den Scanner an den Computer anzuschließen.

Rufen Sie folgende Website auf und geben Sie den Produktnamen ein, um das Installationsprogramm zu starten.

Rufen Sie **Setup** auf, und beginnen Sie dann die Einrichtung.

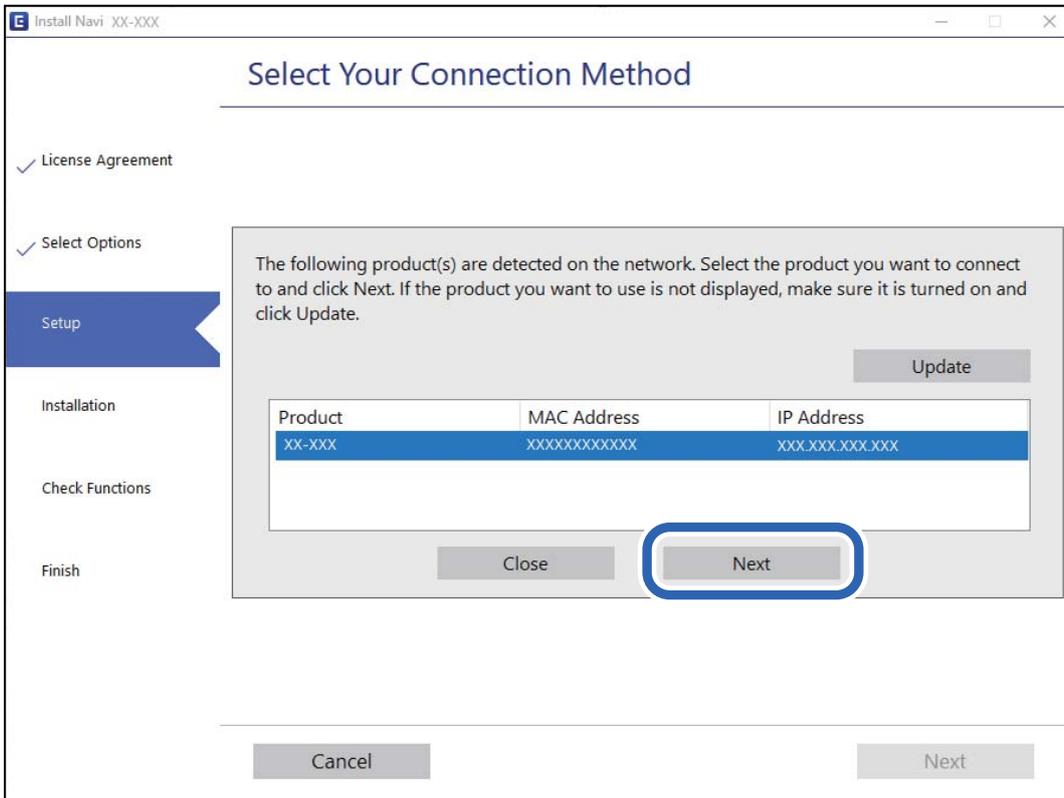
<https://epson.sn>

Sie finden die Betriebsanweisungen in den Webfilmanleitungen. Rufen Sie sie unter der folgenden URL auf.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

## Auswählen des Scanners

Folgen Sie der Bildschirmanleitung, bis der folgende Bildschirm angezeigt wird., wählen Sie den Namen des Scanners, den Sie verbinden möchten und klicken Sie dann auf **Weiter**.



Befolgen Sie die Anweisungen auf dem Bildschirm.

## Verwenden eines Netzwerkscanners von einem Smart-Gerät

Sie können den Scanner mit einer der folgenden Methoden mit einem Smart-Gerät verbinden.

### Verbinden über einen Drahtlos-Router

Verbinden Sie das Smart-Gerät mit demselben WLAN-Netzwerk (SSID), das der Scanner verwendet.

Ausführliche Informationen finden Sie im Folgenden.

[„Konfigurieren von Einstellungen für die Verbindung zum Smartgerät“ auf Seite 29](#)

### Verbinden über Wi-Fi Direct

Verbinden Sie das Smart-Gerät direkt mit dem Scanner ohne einen Drahtlos-Router.

Ausführliche Informationen finden Sie im Folgenden.

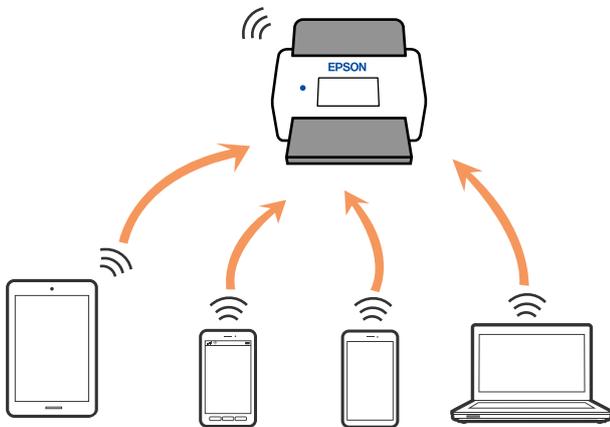
[„Direktes Verbinden eines Smart-Geräts mit dem Scanner \(Wi-Fi Direct\)“ auf Seite 26](#)

## Direktes Verbinden eines Smart-Geräts mit dem Scanner (Wi-Fi Direct)

Mit Wi-Fi Direct (Einfacher AP) können Sie ein Smart-Gerät ohne Drahtlos-Router direkt mit dem Scanner verbinden und vom Smart-Gerät aus scannen.

### Über Wi-Fi Direct

Verwenden Sie diese Verbindungsmethode, wenn zu Hause oder im Büro kein Wi-Fi vorhanden ist, oder wenn der Scanner direkt mit dem Computer oder Smartgerät verbunden werden soll. In diesem Modus fungiert der Scanner als Wireless-Router und Sie können die Geräte ohne einen herkömmlichen Wireless-Router mit dem Scanner verbinden. Die mit dem Scanner verbundenen Geräte können jedoch nicht untereinander über den Scanner kommunizieren.



Der Scanner kann gleichzeitig per Wi-Fi oder Ethernet und Wi-Fi Direct- (Einfacher AP) Verbindung verbunden werden. Falls Sie jedoch eine Netzwerkverbindung in der Wi-Fi Direct- (Einfacher AP) Verbindung starten, während der Scanner per Wi-Fi verbunden ist, wird Wi-Fi vorübergehend getrennt.

### Verbinden mit einem Smartgerät über Wi-Fi Direct

Mit dieser Methode können Sie den Scanner direkt ohne einen Wireless-Router mit anderen Smart-Geräten verbinden.

1. Wählen Sie auf dem Startbildschirm .
2. Wählen Sie **Wi-Fi Direct**.
3. Wählen Sie **Setup starten**.
4. Starten Sie Epson Smart Panel auf dem Smartgerät.
5. Folgen Sie den Anweisungen auf dem Epson Smart Panel, um sich mit dem Scanner zu verbinden.  
Wenn Ihr Smartgerät an den Scanner angeschlossen ist, fahren Sie mit dem nächsten Schritt fort.
6. Wählen Sie auf dem Bedienfeld des Scanners **Fertig**.

## Deaktivieren der Wi-Fi Direct-Verbindung (Einfacher AP)

Es stehen zwei Methoden zur Verfügung, um eine Wi-Fi Direct-Verbindung (Einfacher AP) zu deaktivieren; Sie können alle Verbindungen über das Bedienfeld des Scanners deaktivieren oder die einzelnen Verbindungen vom Computer oder Smart-Gerät aus deaktivieren.

Wenn alle Verbindungen deaktiviert werden sollen, wählen Sie  > **Wi-Fi Direct** > **Setup starten** > **Ändern** > **Wi-Fi Direct deaktivieren**.



### **Wichtig:**

Wenn Wi-Fi Direct (Einfacher AP) deaktiviert wird, werden alle Computer und Smart-Geräte, die über Wi-Fi Direct (Einfacher AP) mit dem Scanner verbunden sind, getrennt.

### **Hinweis:**

Wenn Sie nur ein bestimmtes Gerät trennen möchten, trennen Sie anstelle der Verbindung zum Scanner die Verbindung zum Gerät. Verwenden Sie eine der folgenden Methoden, um die Wi-Fi Direct-Verbindung (Einfacher AP) vom Gerät aus zu trennen.

- Deaktivieren Sie die Wi-Fi-Verbindung zum Netzwerknamen (SSID) des Scanners.
- Stellen Sie eine Verbindung zu einem anderen Netzwerknamen (SSID) her.

## Ändern der Einstellungen für Wi-Fi Direct (Einfacher AP) wie SSID

Wenn die Wi-Fi Direct (Einfacher AP)-Verbindung aktiviert ist, können Sie die Einstellungen über  > **Wi-Fi Direct** > **Setup starten** > **Ändern** ändern. Danach werden die folgenden Menüoptionen angezeigt:

### **Netzwerknamen ändern**

Ändert den Wi-Fi Direct (Einfacher AP)-Netzwerknamen (SSID), der zur Verbindung des Scanners verwendet wird, auf einen Namen Ihrer Wahl. Sie können den Netzwerknamen (SSID) mit ASCII-Zeichen eingeben, die auf der Software-Tastatur auf dem Bedienfeld angezeigt werden. Sie können bis zu 22 Zeichen eingeben.

Beim Ändern des Netzwerknamens (SSID) werden alle verbundenen Geräte getrennt. Verwenden Sie den neuen Netzwerknamen (SSID), wenn Sie die Geräteverbindung wiederherstellen möchten.

### **Kennwort ändern**

Ändert das Wi-Fi Direct (Einfacher AP)-Kennwort, das zur Verbindung des Scanners verwendet wird, in ein Kennwort Ihrer Wahl. Sie können das Kennwort mit ASCII-Zeichen eingeben, die auf der Software-Tastatur auf dem Bedienfeld angezeigt werden. Sie können zwischen 8 und 22 Zeichen eingeben.

Beim Ändern des Kennworts werden alle verbundenen Geräte getrennt. Verwenden Sie das neue Kennwort, wenn Sie die Geräteverbindung wiederherstellen möchten.

### **Frequenzbereich ändern**

Ändern Sie den Frequenzbereich von Wi-Fi Direct, der zur Verbindung des Scanners verwendet wird. Sie können 2,4 GHz oder 5 GHz wählen.

Beim Ändern des Frequenzbereichs werden alle verbundenen Geräte getrennt. Stellen Sie die Geräteverbindung wieder her.

Beachten Sie, dass Sie die Verbindung für Geräte, die den 5-GHz-Frequenzbereich nicht unterstützen, nicht wiederherstellen können, wenn Sie zum 5-GHz-Bereich wechseln.

Je nach Region wird diese Einstellung möglicherweise nicht angezeigt.

### **Wi-Fi Direct deaktivieren**

Deaktiviert die Wi-Fi Direct (Einfacher AP)-Einstellungen des Scanners. Bei der Deaktivierung werden alle Geräte, die mit einer Wi-Fi Direct (Einfacher AP)-Verbindung mit dem Scanner verbunden sind, getrennt.

### **Werkseinstlg. wiederh.**

Setzt alle Wi-Fi Direct (Einfacher AP)-Einstellungen auf die Standardwerte zurück.

Die Wi-Fi Direct (Einfacher AP)-Verbindungsinformationen des Smart-Geräts, die auf dem Scanner gespeichert sind, werden gelöscht.

#### **Hinweis:**

*Ebenfalls können Sie die Einrichtung für die folgenden Einstellungen über die Registerkarte **Netzwerk** > **Wi-Fi Direct** unter **Web Config** vornehmen.*

Aktivieren oder Deaktivieren von Wi-Fi Direct (Einfacher AP)

Ändern des Netzwerknamens (SSID)

Ändern des Kennworts

Ändern des Frequenzbereichs

*Je nach Region wird diese Einstellung möglicherweise nicht angezeigt.*

Wiederherstellen der Wi-Fi Direct (Einfacher AP)-Einstellungen

## **Erneutes Konfigurieren der Netzwerkverbindung**

In diesem Abschnitt wird erläutert, wie Sie die Netzwerkverbindungseinstellungen konfigurieren und die Verbindungsmethode ändern, wenn Sie den Drahtlos-Router oder den Computer austauschen.

### **Austauschen des Drahtlos-Routers**

Wenn Sie den Drahtlos-Router austauschen, konfigurieren Sie die Einstellungen für die Verbindung zwischen dem Computer oder Smart-Gerät und dem Scanner.

Sie müssen diese Änderungen vornehmen, wenn Sie Ihren Internetanbieter wechseln usw.

### **Konfigurieren von Einstellungen für die Verbindung zum Computer**

Wir empfehlen die Verwendung eines Installationsprogramms, um den Scanner an den Computer anzuschließen.

Rufen Sie folgende Website auf und geben Sie den Produktnamen ein, um das Installationsprogramm zu starten. Rufen Sie **Setup** auf, und beginnen Sie dann die Einrichtung.

<https://epson.sn>

Sie finden die Betriebsanweisungen in den Webfilmanleitungen. Rufen Sie sie unter der folgenden URL auf.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

### **Auswählen der Verbindungsmethode**

Befolgen Sie die Anweisungen auf dem Bildschirm. Wählen Sie auf dem Bildschirm **Installationsoption wählen** die Option **Drucker-Verbindung erneut einrichten (bei neuem Netzwerk-Router oder Wechsel von USB zu Netzwerk usw.)** aus und klicken Sie dann auf **Weiter**.

Folgen Sie den Anweisungen auf dem Bildschirm, um die Einrichtung abzuschließen.

Wenn Sie keine Verbindung herstellen können, lesen Sie Folgendes, um das Problem zu lösen.

„Netzwerkverbindung kann nicht hergestellt werden“ auf Seite 35

### **Konfigurieren von Einstellungen für die Verbindung zum Smartgerät**

Sie können den Scanner über ein Smartgerät verwenden, wenn Sie den Scanner mit dem gleichen WLAN-Netzwerk (SSID) wie das Smartgerät verbinden. Rufen Sie folgende Website auf und geben Sie den Produktnamen ein, um den Scanner mit einem Smartgerät zu verwenden. Rufen Sie **Setup** auf, und beginnen Sie dann die Einrichtung.

<https://epson.sn>

Greifen Sie über das Smartgerät auf die Website zu, mit dem Sie den Scanner verwenden möchten.

## **Austauschen des Computers**

Wenn Sie den Computer austauschen, konfigurieren Sie die Verbindungseinstellungen zwischen dem Computer und dem Scanner.

### **Konfigurieren von Einstellungen für die Verbindung zum Computer**

Wir empfehlen die Verwendung eines Installationsprogramms, um den Scanner an den Computer anzuschließen.

Rufen Sie folgende Website auf und geben Sie den Produktnamen ein, um das Installationsprogramm zu starten.

Rufen Sie **Setup** auf, und beginnen Sie dann die Einrichtung.

<https://epson.sn>

Sie finden die Betriebsanweisungen in den Webfilmanleitungen. Rufen Sie sie unter der folgenden URL auf.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

Befolgen Sie die Anweisungen auf dem Bildschirm.

## **Ändern der Verbindungsmethode zum Computer**

In diesem Abschnitt wird erläutert, wie Sie die Verbindungsmethode ändern können, wenn der Computer und der Scanner verbunden wurden.

### **Ändern der Netzwerkverbindung von Ethernet zu WLAN**

Wechseln Sie von einer Ethernetverbindung zu einer WLAN-Verbindung über das Bedienfeld des Scanners. Die Methode zum Ändern der Verbindung ist praktisch dieselbe wie bei den WLAN-Verbindungseinstellungen.

### **Zugehörige Informationen**

➔ „Verbindung zu einem drahtlosen Netzwerk (WLAN) herstellen“ auf Seite 21

### **Ändern der Netzwerkverbindung von WLAN zu Ethernet**

Führen Sie die nachstehenden Schritte aus, um von einer WLAN-Verbindung zu einer Ethernet-Verbindung zu wechseln.

1. Wählen Sie auf dem Startbildschirm **Einstellungen**.
2. Wählen Sie **Netzwerkeinstellungen** > **LAN-Einrichtung**.
3. Lassen Sie sich von den Hinweisen auf dem Bildschirm durch die nötigen Schritte führen.

### **Wechseln von einer USB- zu einer Netzwerkverbindung**

Einstellen einer neuen Verbindungsmethode mithilfe des Installationsprogramms.

Rufen Sie folgende Website auf und geben Sie den Produktnamen ein. Rufen Sie **Setup** auf, und beginnen Sie dann die Einrichtung.

<https://epson.sn>

### **Auswählen von Verbindungsmethode ändern**

Befolgen Sie die Anweisungen in jedem Fenster. Wählen Sie auf dem Bildschirm **Installationsoption wählen** die Option **Drucker-Verbindung erneut einrichten (bei neuem Netzwerk-Router oder Wechsel von USB zu Netzwerk usw.)** aus und klicken Sie dann auf **Weiter**.

Wählen Sie die Netzwerkverbindung, die verwenden möchten, **Über Drahtlosnetzwerk (WLAN) verbinden** oder **Über kabelgebundenes LAN (Ethernet) verbinden** und klicken Sie dann auf **Weiter**.

Folgen Sie den Anweisungen auf dem Bildschirm, um die Einrichtung abzuschließen.

---

## **Überprüfen des Netzwerkverbindungsstatus**

Der Netzwerkverbindungsstatus kann auf folgende Weise überprüft werden.

### **Überprüfen des Netzwerkverbindungsstatus über das Bedienfeld**

Sie können den Netzwerkverbindungsstatus anhand des Netzwerksymbols oder der Netzwerkinformationen auf dem Bedienfeld des Scanners überprüfen.

### **Überprüfen des Netzwerkverbindungsstatus anhand des Netzwerksymbols**

Anhand des Netzwerksymbols im Startbildschirm des Scanners können Sie den Netzwerkverbindungsstatus und die Stärke des Funksignals prüfen.



	<p>Zeigt den Netzwerkverbindungsstatus an.</p> <p>Wählen Sie das Symbol, um die aktuellen Einstellungen zu prüfen und zu ändern. Dies ist eine Verknüpfung für das folgende Menü.</p> <p><b>Einstellungen &gt; Netzwerkeinstellungen &gt; Wi-Fi-Setup</b></p>
	<p>Der Scanner ist nicht mit einem drahtlosen (Wi-Fi-) Netzwerk verbunden.</p>
	<p>Der Scanner sucht nach einer SSID, IP-Adresseinstellung wurde aufgehoben oder ein Problem mit einem Drahtlosnetzwerk (Wi-Fi) liegt vor.</p>
	<p>Der Scanner ist mit einem Drahtlosnetzwerk (Wi-Fi) verbunden.</p> <p>Die Balkenanzahl zeigt die Signalstärke der Verbindung an. Je mehr Balken vorhanden sind, desto stärker ist die Verbindung.</p>
	<p>Zeigt an, dass der Scanner nicht mit einem Drahtlosnetzwerk (Wi-Fi) im Wi-Fi Direct-Modus (Einfacher AP) verbunden ist.</p>
	<p>Zeigt an, dass der Scanner mit einem Drahtlosnetzwerk (Wi-Fi) im Wi-Fi Direct-Modus (Einfacher AP) verbunden ist.</p>
	<p>Der Scanner ist nicht mit einem drahtgebundenen (Ethernet-)Netzwerk verbunden; oder diese Einstellung aufheben.</p>
	<p>Der Scanner ist mit einem drahtgebundenen (Ethernet-)Netzwerk verbunden.</p>

## Anzeigen der Netzwerkdetails auf dem Bedienfeld

Wenn der Scanner mit dem Netzwerk verbunden ist, können Sie auch andere netzwerkbezogene Informationen durch Aufrufen der entsprechenden Netzwerkmenüs anzeigen.

1. Wählen Sie auf dem Startbildschirm **Einstellungen**.
2. Wählen Sie **Netzwerkeinstellungen > Netzwerkstatus**.
3. Um die Informationen zu prüfen, wählen Sie die entsprechenden Menüs.
  - Wired LAN/Wi-Fi-Status**  
Zeigt die Netzwerkdaten (Gerätename, Verbindung, Signalstärke, usw.) für Ethernet oder WLAN-Verbindungen an.
  - Wi-Fi Direct-Status**  
Zeigt an, ob Wi-Fi Direct aktiviert oder deaktiviert ist, sowie die SSID und das Kennwort usw. für Wi-Fi Direct-Verbindungen.
  - eMail-Serverstatus**  
Zeigt die Netzwerkdaten für E-Mail-Server an.

## Technische Daten des Netzwerks

### WLAN-Spezifikationen

In der folgenden Tabelle finden Sie die WLAN-Spezifikationen.

Länder oder Regionen mit Ausnahme der unten aufgeführten Länder oder Regionen	<b>Tabelle A</b>
Irland, Vereinigtes Königreich, Österreich, Deutschland, Liechtenstein, Schweiz, Frankreich, Belgien, Luxemburg, Niederlande, Italien, Portugal, Spanien, Dänemark, Finnland, Norwegen, Schweden, Island, Kroatien, Zypern, Griechenland, Nordmazedonien, Serbien, Slowenien, Malta, Bosnien und Herzegowina, Kosovo, Montenegro, Albanien, Bulgarien, Tschechische Republik, Estland, Ungarn, Lettland, Litauen, Polen, Rumänien, Slowakei, Israel, Australien, Neuseeland, Taiwan	<b>Tabelle B</b>
Türkei	DS-900WN: Seriennummern, die mit XDA8: <b>Tabelle A</b> beginnen Seriennummern, die mit XDA7: <b>Tabelle B</b> beginnen
	DS-800WN: Seriennummern, die mit XDA2: <b>Tabelle A</b> beginnen Seriennummern, die mit XD9Z: <b>Tabelle B</b> beginnen

#### Tabelle A

Standards	IEEE 802.11b/g/n <sup>*1</sup>
Frequenzbereich	2 400 – 2 483,5 MHz
Maximal übertragene Radiofrequenzleistung	20 dBm (EIRP)
Kanäle	1/2/3/4/5/6/7/8/9/10/11/12/13
Verbindungsmodi	Infrastruktur, Wi-Fi Direct (Einfacher AP) <sup>*2*3</sup>
Sicherheitsprotokolle <sup>*4</sup>	WEP (64/128bit), WPA2-PSK (AES) <sup>*5</sup> , WPA3-SAE (AES), WPA2/WPA3-Enterprise

\*1 Nur für den HT20 verfügbar.

\*2 Bei IEEE 802.11b nicht unterstützt.

\*3 Infrastruktur- und Wi-Fi Direct-Modus oder eine Ethernet-Verbindung können gleichzeitig genutzt werden.

\*4 Wi-Fi Direct unterstützt nur WPA2-PSK (AES).

\*5 Entspricht WPA2-Standards mit Unterstützung von WPA/WPA2 Personal.

#### Tabelle B

Standards	IEEE 802.11a/b/g/n <sup>*1</sup> /ac		
Frequenzbereiche	IEEE 802.11b/g/n: 2,4 GHz, IEEE 802.11a/n/ac: 5 GHz		
Kanäle	WLAN	2,4 GHz	1/2/3/4/5/6/7/8/9/10/11/12 <sup>*2</sup> /13 <sup>*2</sup>
		5 GHz <sup>*3</sup>	W52 (36/40/44/48), W53 (52/56/60/64), W56 (100/104/108/112/116/120/124/128/132/136/140/144), W58 (149/153/157/161/165)
	Wi-Fi Direct	2,4 GHz	1/2/3/4/5/6/7/8/9/10/11/12 <sup>*2</sup> /13 <sup>*2</sup>
		5 GHz <sup>*3</sup>	W52 (36/40/44/48) W58 (149/153/157/161/165)
Verbindungsmodi	Infrastruktur, Wi-Fi Direct (Simple AP) <sup>*4*5</sup>		
Sicherheitsprotokolle <sup>*6</sup>	WEP (64/128bit), WPA2-PSK (AES) <sup>*7</sup> , WPA3-SAE (AES), WPA2/WPA3-Enterprise		

\*1 Nur für den HT20 verfügbar.

\*2 Nicht in Taiwan verfügbar.

\*3 Die Verfügbarkeit dieser Kanäle und die Nutzung des Produkts im Freien über diese Kanäle variiert je nach Standort. Weitere Informationen unter <http://support.epson.net/wifi5ghz/>

\*4 Bei IEEE 802.11b nicht unterstützt.

\*5 Infrastruktur- und Wi-Fi Direct-Modus oder eine Ethernet-Verbindung können gleichzeitig genutzt werden.

\*6 Wi-Fi Direct unterstützt nur WPA2-PSK (AES).

\*7 Entspricht WPA2-Standards mit Unterstützung von WPA/WPA2 Personal.

## Ethernet-Spezifikationen

Standards	IEEE802.3i (10BASE-T) <sup>*1</sup> IEEE802.3u (100BASE-TX) <sup>*1</sup> IEEE802.3ab (1000BASE-T) <sup>*1</sup> IEEE802.3az (Energy Efficient Ethernet) <sup>*2</sup>
Kommunikationsmodus	Auto, 10 Mbit/s Full-duplex, 10 Mbit/s Half-duplex, 100 Mbit/s Full-duplex, 100 Mbit/s Half-duplex
Anschluss	RJ-45

\*1 Verwenden Sie ein abgeschirmtes Twisted-Pair-Kabel der Kategorie 5e oder höher, um Funkstörungen zu vermeiden.

\*2 Das verbundene Gerät sollte IEEE802.3az-Standards entsprechen.

## Netzwerkfunktionen und Unterstützung für IPv4/IPv6

Unterstützte	Funktionen
Epson Scan 2	IPv4, IPv6
Document Capture Pro/Document Capture	IPv4

## Sicherheitsprotokoll

IEEE802.1X*	
IPsec/IP-Filtering	
SSL/TLS	HTTPS Server/Client
SMTPS (STARTTLS, SSL/TLS)	
SNMPv3	

\* Sie müssen ein IEEE802.1X-konformes Verbindungsgerät verwenden.

## Verwendeter Scannerport

Der Scanner verwendet folgenden Port. Diese Ports sollten vom Netzwerkadministrator bei Bedarf zur Verfügung gestellt werden können.

### Wenn der Scanner der Absender (Client) ist

Aktivieren	Ziel (Server)	Protokoll	Portnummer	
Dateiübertragung (Wenn vom Scanner „Scannen an einen Netzwerkordner“ verwendet wird)	FTP/FTPS-Server	FTP/FTPS (TCP)	20	
			21	
	Dateiserver	SMB (TCP)	445	
			NetBIOS (UDP)	137
				138
	WebDAV-Server	NetBIOS (TCP)	139	
Protocol HTTP (TCP)			80	
		Protocol HTTPS (TCP)	443	
Versand per E-Mail (Wenn vom Scanner „Scannen an E-Mail“ verwendet wird)	SMTP-Server	SMTP (TCP)	25	
		SMTP SSL/TLS (TCP)	465	
		SMTP STARTTLS (TCP)	587	

Aktivieren	Ziel (Server)	Protokoll	Portnummer
POP-vor-SMTP-Verbindung (Wenn vom Scanner „Scannen an E-Mail“ verwendet wird)	POP-Server	POP3 (TCP)	110
Bei Verwendung von Epson Connect	Epson-Connect-Server	HTTPS	443
		XMPP	5222
Sammeln von Benutzerinformationen (Anhand der Kontakte aus dem Scanner)	LDAP-Server	LDAP (TCP)	389
		LDAP SSL/TLS (TCP)	636
		LDAP STARTTLS (TCP)	389
Benutzerauthentifizierung beim Sammeln von Benutzerinformationen (Bei Verwendung der Kontakte aus dem Scanner)  Benutzerauthentifizierung wenn der Scanner „Scannen an einen Netzwerkordner (SMB)“ verwendet	KDC-Server	Kerberos	88
Control WSD	Client-Computer	WSD (TCP)	5357
Durchsuchen des Computers beim Push-Scannen mit einer Anwendung	Client-Computer	Netzwerk-Push-Scan-Erkennung	2968

**Wenn der Client-Computer der Absender (Client) ist**

Aktivieren	Ziel (Server)	Protokoll	Portnummer
Ermitteln des Scanners von einer Anwendung wie EpsonNet Config oder dem Scannertreiber.	Scanner	ENPC (UDP)	3289
Ermitteln und Einrichten der MIB-Daten von einer Anwendung wie EpsonNet Config oder dem Scannertreiber.	Scanner	SNMP (UDP)	161
Suche nach WSD-Scanner	Scanner	WS-Discovery (UDP)	3702
Weiterleiten der Scandaten von einer Anwendung	Scanner	Netzwerk-Scan (TCP)	1865
Sammeln der Auftragsinformationen beim Push-Scannen von einer Anwendung	Scanner	Netzwerk-Push-Scan	2968
Web Config	Scanner	HTTP (TCP)	80
		HTTPS (TCP)	443

## Probleme lösen

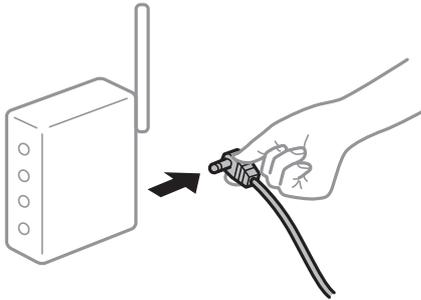
**Netzwerkverbindung kann nicht hergestellt werden**

Das Problem könnte mit einer der folgenden Ursachen zusammenhängen.

### Es gibt ein Problem mit den Netzwerkgeräten für die WLAN-Verbindung.

#### Lösungen

Schalten Sie alle Geräte aus, die mit dem Netzwerk verbunden werden sollen. Warten Sie etwa 10 Sekunden und schalten Sie die Geräte dann in folgender Reihenfolge ein: Drahtlos-Router, Computer oder Smart-Gerät und dann den Scanner. Positionieren Sie Scanner und Computer oder Smart-Gerät näher am Drahtlos-Router, um die Funkkommunikation zu erleichtern, und nehmen Sie die Netzwerkeinstellungen dann erneut vor.



### Geräte können wegen zu großem Abstand keine Signale vom Drahtlos-Router empfangen.

#### Lösungen

Nachdem Sie den Computer oder das Smart-Gerät und den Scanner näher am Drahtlos-Router platziert haben, schalten Sie den Drahtlos-Router aus und dann wieder ein.

### Nach dem Austausch des Drahtlos-Routers stimmen die Einstellungen nicht mit dem neuen Router überein.

#### Lösungen

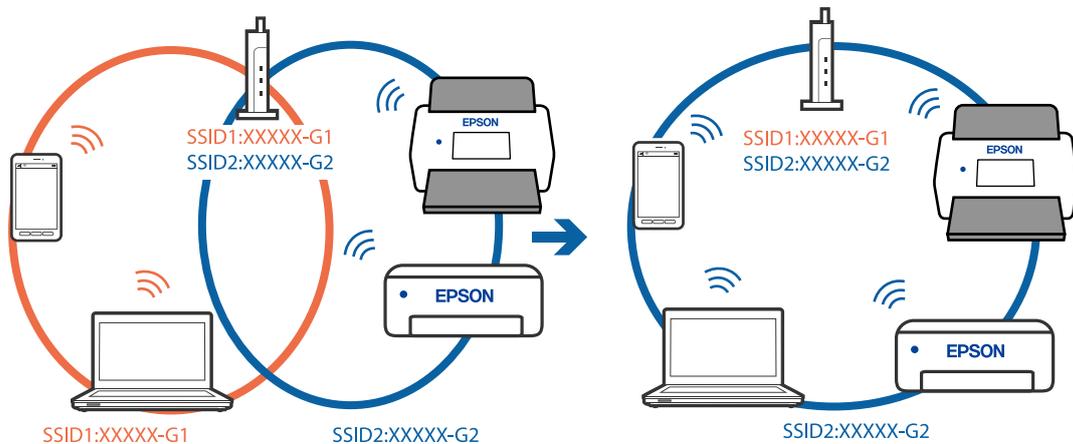
Konfigurieren Sie die Verbindungseinstellungen erneut, sodass sie mit dem neuen Drahtlos-Router übereinstimmen.

### Der Computer oder das Smart-Gerät und der Drucker sind mit unterschiedlichen SSIDs verbunden.

#### Lösungen

Wenn Sie mehrere Drahtlos-Router gleichzeitig verwenden oder wenn der Drahtlos-Router mehrere SSIDs hat und die Geräte mit unterschiedlichen SSIDs verbunden sind, können Sie keine Verbindung zum Drahtlos-Router herstellen.

Verbinden Sie den Computer oder das Smartgerät mit derselben SSID wie der Scanner.



### Der Drahtlos-Router verfügt über einen Privacy Separator.

#### Lösungen

Die meisten Drahtlos-Router verfügen über die Funktion „Privacy Separator“, mit der die Kommunikation zwischen verbundenen Geräten blockiert wird. Falls eine Kommunikation zwischen Scanner und Computer oder Smartgerät nicht möglich ist, obwohl sich beide in demselben Netzwerk befinden, deaktivieren Sie den Privacy-Separator am Drahtlos-Router. Einzelheiten dazu finden Sie in dem Handbuch, das mit dem Drahtlos-Router mitgeliefert wurde.

### Die IP-Adresse ist nicht richtig zugewiesen.

#### Lösungen

Falls die dem Scanner zugewiesene IP-Adresse 169.254.XXX.XXX ist und die Subnetzmaske 255.255.0.0, wurde die IP-Adresse möglicherweise nicht richtig zugewiesen.

Wählen Sie **Einstellungen > Netzwerkeinstellungen > Erweitert > TCP/IP-Einrichtung** auf dem Bedienfeld des Scanners, und überprüfen Sie dann die IP-Adresse und die Subnetzmaske, die dem Scanner zugewiesen wurden.

Starten Sie den Drahtlos-Router neu oder setzen Sie die Netzwerkeinstellungen für den Scanner zurück.

### Es liegt ein Problem mit den Netzwerkeinstellungen auf dem Computer vor.

#### Lösungen

Versuchen Sie über Ihren Computer auf Webseiten zuzugreifen, um sicherzustellen, dass die Netzwerkeinstellungen Ihres Computers korrekt sind. Wenn Sie nicht auf Webseiten zugreifen können, gibt es ein Problem mit dem Computer.

Überprüfen Sie die Netzwerkverbindung des Computers. Ausführliche Informationen dazu finden Sie in der mit dem Computer gelieferten Dokumentation.

### Der Scanner ist via Ethernet mithilfe von Geräten verbunden, die IEEE 802.3az (Energy Efficient Ethernet) unterstützen.

#### Lösungen

Wenn Sie den Scanner via Ethernet mithilfe von Geräten verbinden, die IEEE 802.3az (Energy Efficient Ethernet) unterstützen, können je nach verwendetem Hub oder Router die folgenden Probleme auftreten.

- Die Verbindung wird instabil; die Verbindung des Scanner wird ständig hergestellt und getrennt.

- Die Verbindung zum Scanner kann nicht hergestellt werden.
- Die Verbindungsgeschwindigkeit wird langsam.

Führen Sie die folgenden Schritte aus, um IEEE 802.3az für den Scanner zu deaktivieren und dann erneut eine Verbindung herzustellen.

1. Ziehen Sie das Ethernetkabel vom Computer und Scanner ab.
2. Wenn IEEE 802.3az für den Computer aktiviert ist, deaktivieren Sie es.  
Ausführliche Informationen dazu finden Sie in der mit dem Computer gelieferten Dokumentation.
3. Verbinden Sie Computer und Scanner direkt mit einem Ethernetkabel.
4. Überprüfen Sie auf dem Scanner die Netzwerkeinstellungen.  
Wählen Sie **Einstellungen > Netzwerkeinstellungen > Netzwerkstatus > Wired LAN/Wi-Fi-Status**.
5. Überprüfen Sie die IP-Adresse des Scanners.
6. Rufen Sie auf dem Computer Web Config auf.  
Starten Sie einen Webbrowser und geben Sie dann die IP-Adresse des Scanners ein.  
[„Ausführen von Web Config in einem Webbrowser“ auf Seite 40](#)
7. Wählen Sie die Registerkarte **Netzwerk > Kabelgebundenes LAN**.
8. Wählen Sie **Aus** bei **IEEE 802.3az**.
9. Klicken Sie auf **Weiter**.
10. Klicken Sie auf **OK**.
11. Ziehen Sie das Ethernetkabel vom Computer und Scanner ab.
12. Wenn Sie in Schritt 2 IEEE 802.3az für den Computer deaktiviert haben, aktivieren Sie es.
13. Schließen Sie die Ethernetkabel, die Sie in Schritt 1 entfernt haben, an den Computer und den Scanner an.

Wenn das Problem weiterhin besteht, wird es möglicherweise nicht durch den Scanner, sondern durch andere Geräte verursacht.

### ■ **Der Scanner ist ausgeschaltet.**

#### **Lösungen**

Vergewissern Sie sich, dass der Scanner eingeschaltet ist.

Warten Sie insbesondere, bis die Statusanzeige zu blinken aufhört und anzeigt, dass der Scanner betriebsbereit ist.

---

# Software für das Einrichten des Scanners

Anwendung für das Konfigurieren des Scannerbetriebs (Web Config) . . . . .	40
Epson Device Admin. . . . .	41

## Anwendung für das Konfigurieren des Scannerbetriebs (Web Config)

Die Anwendung Web Config wird auf einem Computer oder Smart-Gerät in einem Webbrowser, wie z. B. Microsoft Edge und Safari ausgeführt. Sie können den Scannerstatus kontrollieren oder die Netzwerkdienst- und Druckereinstellungen ändern. Zur Verwendung von Web Config müssen der Scanner und der Computer oder das Gerät mit demselben Netzwerk verbunden sein.

Die folgenden Browser werden unterstützt. Verwenden Sie die neueste Version.

Microsoft Edge, Windows Internet Explorer, Firefox, Chrome, Safari

### **Hinweis:**

Sie werden möglicherweise aufgefordert, Ihr Administrator Kennwort einzugeben. Siehe die folgenden Informationen zum Administrator Kennwort.

[„Hinweise zum Administrator Kennwort“ auf Seite 11](#)

### **Zugehörige Informationen**

➔ [„Zugriff auf Web Config nicht möglich“ auf Seite 68](#)

## Ausführen von Web Config in einem Webbrowser

Der Scanner wird mit der integrierten Software Web Config geliefert. (Das ist eine Website, auf der Sie die Einstellungen vornehmen können.) Geben Sie einfach die IP-Adresse des vernetzten Scanners ein, um Web Config aufzurufen.

1. Überprüfen Sie die IP-Adresse des Scanners.

Wählen Sie **Einstellungen** > **Netzwerkeinstellungen** > **Netzwerkstatus** auf dem Scannerbedienfeld aus.

Wählen Sie dann die aktive Verbindungsmethode aus (**Wired LAN/Wi-Fi-Status** oder **Wi-Fi Direct-Status**), um die IP-Adresse des Scanners zu bestätigen.

Beispiel für eine IP-Adresse: 192.168.100.201

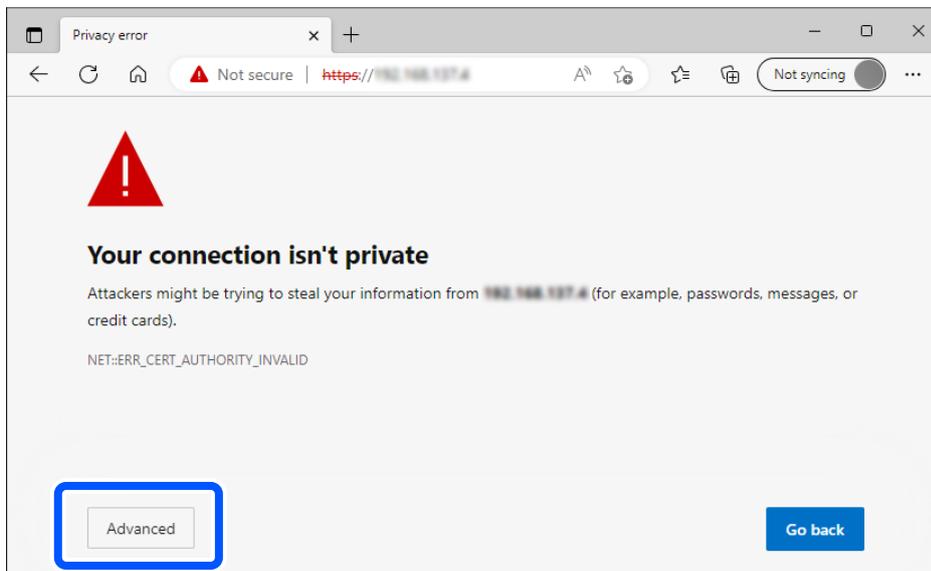
2. Starten Sie einen-Browser auf dem Computer oder Smartgerät und geben Sie dann die IP-Adresse in Adresse des Scanners in der Adressleiste ein.

Format: http://scanner's IP address/

Beispiel: http://192.168.100.201/

Wenn in Ihrem Browser ein Warnbildschirm angezeigt wird, ignorieren Sie die Warnung und erlauben das Anzeigen der Website (Web Config). Da der Scanner für den Zugriff auf HTTPS ein selbstsigniertes Zertifikat verwendet, wird im Browser beim Start von Web Config eine Warnung angezeigt; diese zeigt kein Problem an und kann ignoriert werden. Abhängig vom verwendeten Webbrowser müssen Sie möglicherweise auf **Advanced Settings** klicken, damit die Webseite angezeigt wird.

Beispiel: bei Microsoft Edge



**Hinweis:**

- Wenn kein Warnbildschirm angezeigt wird, fahren Sie mit dem nächsten Schritt fort.
- Verwenden Sie bei IPv6-Adressen das folgende Format.  
Format: `http://[IP-Adresse des Scanners]/`  
Beispiel: `http://[2001:db8::1000:1]/`

3. Melden Sie sich als Administrator bei Web Config an, um die Scanner-Einstellungen ändern zu können. Klicken Sie oben rechts am Bildschirm auf **anmelden**. Geben Sie **Benutzername** und **Aktuelles Kennwort** ein, und klicken Sie dann auf **OK**.

Im Folgenden finden Sie die anfänglichen Werte für die Web Config-Administratorinformationen.

·Benutzername: keiner (leer)

Kennwort: Auf dem Etikett des Produkts angegeben.

Wenn sich auf der Rückseite ein Etikett „PASSWORD“ befindet, geben Sie die achtstellige Zahl auf dem Etikett ein. Wenn kein Etikett „PASSWORD“ vorhanden ist, geben Sie die Seriennummer auf dem Etikett auf der Rückseite des Produkts als anfängliches Administratorkennwort ein.

**Hinweis:**

- Falls **abmelden** oben rechts auf dem Bildschirm angezeigt wird, sind Sie bereits als Administrator angemeldet.
- Sie werden nach zwanzig Minuten Inaktivität automatisch abgemeldet.

---

## Epson Device Admin

Epson Device Admin ist eine multifunktionale Anwendung, mit der Sie Geräte in einem Netzwerk verwalten können.

Mithilfe von Konfigurationsvorlagen können Sie einheitliche Einstellungen auf mehrere Scanner in einem Netzwerk anwenden, wodurch sich die Software für die Installation und Verwaltung mehrerer Scanner eignet.

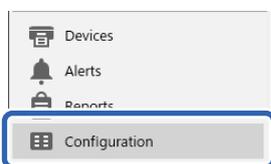
Epson Device Admin kann von der Epson-Support-Webseite heruntergeladen werden. Ausführliche Informationen zur Verwendung dieser Anwendung finden Sie in der Dokumentation oder Hilfe zu Epson Device Admin.

## Konfigurationsvorlage

### Erstellen der Konfigurationsvorlage

Erstellen Sie die Konfigurationsvorlage neu.

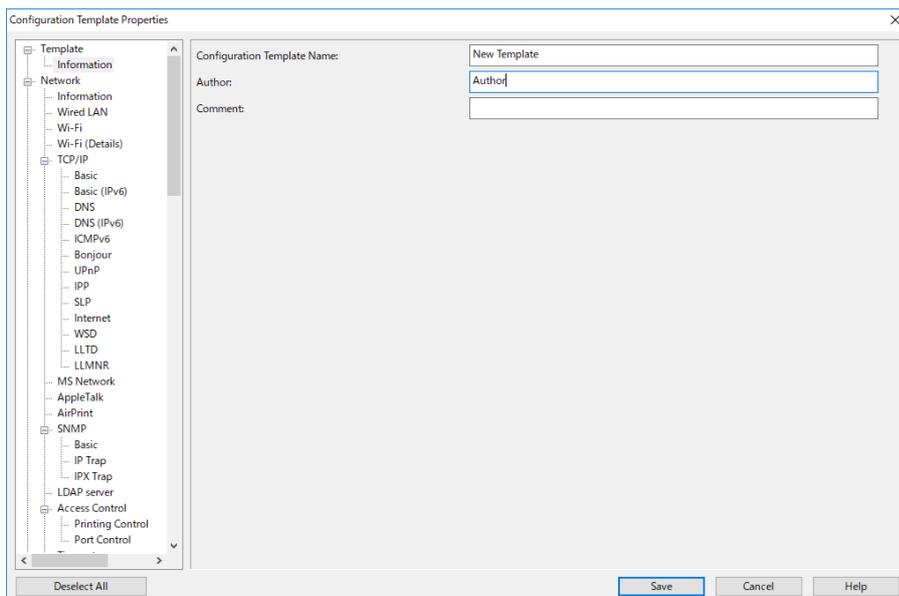
1. Starten Sie Epson Device Admin.
2. Wählen Sie im Aufgabenmenü der Seitenleiste **Konfiguration**.



3. Wählen Sie **Neu** im Ribbon-Menü.



4. Stellen Sie jeden Wert ein.



Element	Erklärung
Konfigurationvorlagenname	Name der Konfigurationsvorlage. Geben Sie bis zu 1024 Unicode-Zeichen (UTF-8) ein.
Urheber	Informationen zum Urheber der Vorlage. Geben Sie bis zu 1024 Unicode-Zeichen (UTF-8) ein.
Kommentar	Zur Eingabe optionaler Informationen. Geben Sie bis zu 1024 Unicode-Zeichen (UTF-8) ein.

5. Wählen Sie die Elemente, die Sie einstellen möchten, links aus.

**Hinweis:**

Klicken Sie auf die Menüelemente links, um zu jedem Bildschirm zu wechseln. Der eingestellte Wert wird beibehalten, wenn Sie den Bildschirm wechseln, aber nicht, wenn Sie abbrechen. Wenn Sie mit allen Einstellungen fertig sind, klicken Sie auf **Speichern**.

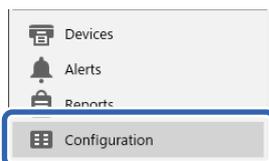
## Anwenden der Konfigurationsvorlage

Wenden Sie die gespeicherte Konfigurationsvorlage am Scanner an. Die auf der Vorlage ausgewählten Elemente werden angewendet. Besitzt der Zielscanner die betreffende Funktion nicht unterstützt, wird sie nicht angewandt.

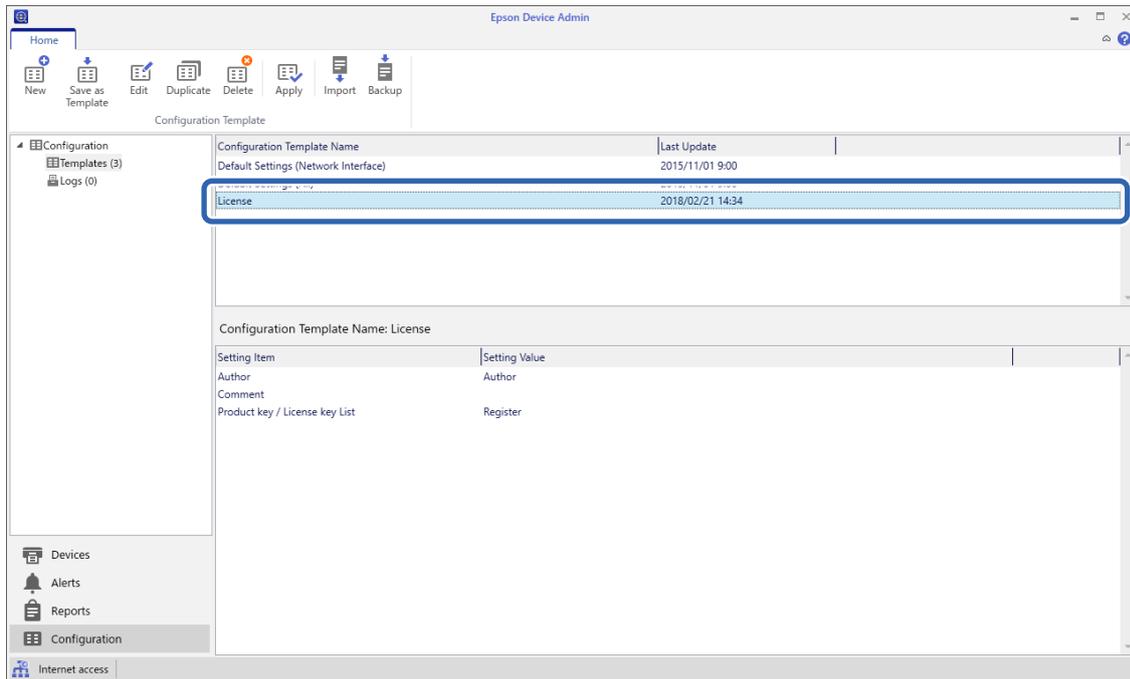
**Hinweis:**

Wenn ein Administratorkennwort am Scanner festgelegt ist, konfigurieren Sie das Kennwort im Voraus.

1. Wählen Sie im Ribbon-Menü des Bildschirms Geräte-Liste **Optionen** > **Kennwortverwaltung**.
  2. Wählen Sie **Automatische Kennwortverwaltung aktivieren** aus, und klicken Sie dann auf **Kennwortverwaltung**.
  3. Wählen Sie den betreffenden Scanner aus, und klicken Sie dann auf **Bearbeiten**.
  4. Legen Sie das Kennwort fest und klicken Sie dann auf **OK**.
1. Wählen Sie im Aufgabenmenü der Seitenleiste **Konfiguration**.



2. Wählen Sie die Konfigurationsvorlage, die Sie anwenden möchten, über **Konfigurationvorlagenname**.



3. Klicken Sie auf **Übernehmen** im Ribbon-Menü.  
Der Geräteauswahlbildschirm wird angezeigt.

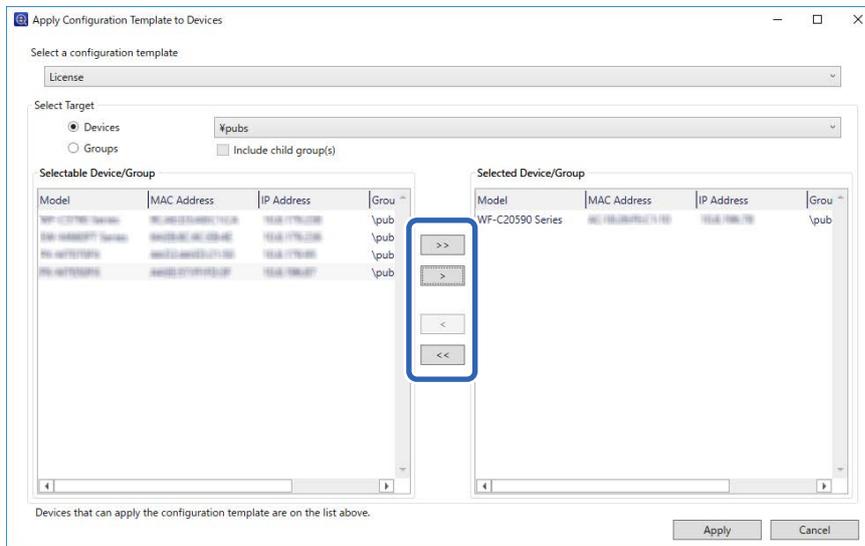


4. Wählen Sie die Konfigurationsvorlage aus, die Sie anwenden möchten.

**Hinweis:**

- Wenn Sie **Drucker** und Gruppen mit Geräten aus dem Auswahlmenü wählen, wird jedes einzelne Gerät angezeigt.
- Gruppen werden angezeigt, wenn Sie **Gruppen** wählen. Wählen Sie **Untergeordnete Gruppe(n) einschließen**, um automatisch untergeordnete Gruppen in der ausgewählten Gruppe auszuwählen.

5. Verschieben Sie die Scanner oder Gruppen, auf welche die Vorlage angewendet werden soll, nach **Ausgewählte(s) Gerät/Gruppe**.



6. Klicken Sie auf **Übernehmen**.  
Ein Bestätigungsbildschirm zur Anwendung der Konfigurationsvorlage wird angezeigt.
7. Klicken Sie auf **OK**, um die Konfigurationsvorlage anzuwenden.
8. Wenn eine Meldung angezeigt wird, die Sie darüber informiert, dass der Vorgang abgeschlossen ist, klicken Sie auf **OK**.
9. Klicken Sie auf **Details** und überprüfen Sie die Informationen.  
Wenn  bei den angewandten Elementen angezeigt wird, wurden diese erfolgreich übernommen.
10. Klicken Sie auf **Schließen**.

---

# **Erforderliche Einstellungen für das Scannen**

Registrieren eines E-Mail-Servers. . . . .	47
Erstellen eines Netzwerkordners. . . . .	50
Kontakte zur Verfügung stellen. . . . .	57
Einrichten von AirPrint. . . . .	67
Probleme bei der Vorbereitung von Netzwerk-Scans. . . . .	68

## Registrieren eines E-Mail-Servers

Prüfen Sie zuerst Folgendes, bevor Sie den E-Mail-Server konfigurieren.

- Der Scanner ist mit dem Netzwerk verbunden
- Einrichtungsinformationen des E-Mail-Servers
  - Wenn Sie einen internetbasierten E-Mail-Server verwenden, überprüfen Sie die Einstellungsinformationen beim Anbieter oder auf der Website.

### Vorgehensweise beim Registrieren

Rufen Sie Web Config auf, wählen Sie die Registerkarte **Netzwerk > eMail-Server > Grundlegend** aus.

[„Ausführen von Web Config in einem Webbrowser“](#) auf Seite 40

Sie können die Einstellungen auch auf dem Scannerbedienfeld vornehmen. Wählen Sie **Einstellungen > Netzwerkeinstellungen > Erweitert > eMail-Server > Servereinstellungen** aus.

### Einstellungsoptionen für E-Mail-Server

Option	Einstellungen und Erläuterung	
Authentisierungsmethode	Geben Sie die Authentifizierungsmethode für den Zugriff des Scanners auf den Mail-Server ein.	
	Aus	Die Authentifizierung ist bei der Kommunikation mit dem Mailserver deaktiviert.
	SMTP-Authentisierung	Der E-Mail-Server muss SMTP-Authentifizierung unterstützen.
	POP vor SMTP	Wenn Sie diese Option auswählen, richten Sie einen POP3-Server ein.
Authentisierungskonto	Wenn Sie <b>SMTP-Authentisierung</b> oder <b>POP vor SMTP</b> als <b>Authentisierungsmethode</b> auswählen, geben Sie den Namen des authentifizierten Kontos ein. Geben Sie 0 bis 255 Zeichen als ASCII (0x20–0x7E) ein.	
Authentisiertes Kennwort	Wenn Sie <b>SMTP-Authentisierung</b> oder <b>POP vor SMTP</b> als <b>Authentisierungsmethode</b> auswählen, geben Sie das authentifizierte Kennwort ein. Geben Sie zwischen 0 und 20 Zeichen in ASCII (0x20–0x7E) ein.	
Absender-eMail-Adresse	Legen Sie die E-Mail-Adresse fest, die verwendet wird, um E-Mails vom Scanner zu senden. Obwohl Sie auch eine vorhandene E-Mail-Adresse verwenden können, empfehlen wir, dass Sie eine spezielle E-Mail-Adresse beziehen und einrichten, damit sie von den E-Mails unterschieden werden kann, die vom Scanner gesendet werden.  Geben Sie zwischen 0 und 255 ASCII-Zeichen (0x20–0x7E) ein, außer: ( ) < > [ ] ; ¥. Das erste Zeichen darf kein Punkt „.“ sein.	
SMTP-Serveradresse	Geben Sie 0 bis 255 Zeichen ein: A–Z, a–z, 0–9, „ - ein. Sie können IPv4- oder FQDN-Format verwenden.	
SMTP-Serverportnummer	Geben Sie eine Nummer zwischen 1 und 65535 ein.	

Option	Einstellungen und Erläuterung	
Sichere Verbindung	Geben Sie die sichere Verbindungsmethode für den E-Mail-Server an.	
	Keine	Wenn Sie <b>POP vor SMTP</b> bei <b>Authentisierungsmethode</b> wählen, wird die Verbindungsmethode auf <b>Keine</b> eingestellt.
	SSL/TLS	Dies ist verfügbar, wenn <b>Authentisierungsmethode</b> auf <b>Aus</b> oder <b>SMTP-Authentisierung</b> eingestellt ist.
	STARTTLS	Dies ist verfügbar, wenn <b>Authentisierungsmethode</b> auf <b>Aus</b> oder <b>SMTP-Authentisierung</b> eingestellt ist.
Zertifikatsvalidierung (nur Web Config)	Das Zertifikat wird validiert, wenn diese Option aktiviert ist. Wir empfehlen diese Einstellung auf <b>Aktivieren</b> , wenn für <b>Sichere Verbindung</b> ein anderen Wert als <b>Keine</b> festgelegt ist.	
POP3-Serveradresse	Wenn Sie <b>POP vor SMTP</b> als <b>Authentisierungsmethode</b> auswählen, geben Sie die Serveradresse des POP3-Servers ein. Sie können 0 bis 255 Zeichen eingeben: A bis Z, a bis z, 0 bis 9. Sie können IPv4- oder FQDN-Format verwenden.	
POP3-Serverportnummer	Festzulegen, wenn Sie <b>POP vor SMTP</b> unter <b>Authentisierungsmethode</b> wählen. Geben Sie eine Nummer zwischen 1 und 65535 ein.	

### Zugehörige Informationen

➔ [„Ausführen von Web Config in einem Webbrowser“](#) auf Seite 40

## Überprüfen einer Verbindung zum E-Mail-Server

1. Wählen Sie das Menü „Verbindungstest“ aus.

**Einrichtung mit Web Config:**

Wählen Sie die Registerkarte **Netzwerk > eMail-Server > Verbindungstest > Start** aus.

**Wenn Sie die Einstellung auf dem Bedienfeld vornehmen:**

Wählen Sie **Einstellungen > Netzwerkeinstellungen > Erweitert > eMail-Server > Verbindungstest** aus.

Der Verbindungstest mit dem Mail-Server wird gestartet.

2. Überprüfen Sie die Testergebnisse.

Der Test war erfolgreich, wenn die Meldung **Verbindungstest war erfolgreich**. angezeigt wird.

Wenn ein Fehler angezeigt wird, beheben Sie den Fehler gemäß den Anweisungen in der Meldung.

[„Referenz zur Mailserver-Verbindungsprüfung“](#) auf Seite 49

## Referenz zur Mailserver-Verbindungsprüfung

Meldung	Ursache
SMTP-Server-Kommunikationsfehler. Folgendes prüfen. - Netzwerkeinstellungen	Diese Meldung erscheint, wenn <ul style="list-style-type: none"> <li><input type="checkbox"/> Der Scanner nicht mit einem Netzwerk verbunden ist</li> <li><input type="checkbox"/> Der SMTP-Server offline ist</li> <li><input type="checkbox"/> Die Netzwerkverbindung während der Kommunikation getrennt wird</li> <li><input type="checkbox"/> Unvollständige Daten empfangen werden</li> </ul>
POP3-Server-Kommunikationsfehler. Folgendes prüfen. - Netzwerkeinstellungen	Diese Meldung erscheint, wenn <ul style="list-style-type: none"> <li><input type="checkbox"/> Der Scanner nicht mit einem Netzwerk verbunden ist</li> <li><input type="checkbox"/> Der POP3-Server offline ist</li> <li><input type="checkbox"/> Die Netzwerkverbindung während der Kommunikation getrennt wird</li> <li><input type="checkbox"/> Unvollständige Daten empfangen werden</li> </ul>
Beim Verbinden mit dem SMTP-Server ist ein Fehler aufgetreten. Folgendes prüfen. - SMTP-Serveradresse - DNS-Server	Diese Meldung erscheint, wenn <ul style="list-style-type: none"> <li><input type="checkbox"/> Die Verbindung zu einem DNS-Server fehlschlägt</li> <li><input type="checkbox"/> Die Namensauflösung für einen SMTP-Server fehlschlägt</li> </ul>
Beim Verbinden mit dem POP3-Server ist ein Fehler aufgetreten. Folgendes prüfen. - POP3-Serveradresse - DNS-Server	Diese Meldung erscheint, wenn <ul style="list-style-type: none"> <li><input type="checkbox"/> Die Verbindung zu einem DNS-Server fehlschlägt</li> <li><input type="checkbox"/> Die Namensauflösung für einen POP3-Server fehlschlägt</li> </ul>
SMTP-Server-Authentifizierungs-fehler. Folgendes prüfen. - Authentisierungsmethode - Authentisierungskonto - Authentisiertes Kennwort	Diese Meldung erscheint, wenn die SMTP-Server fehlschlägt.
POP3-Server-Authentifizierungs-fehler. Folgendes prüfen. - Authentisierungsmethode - Authentisierungskonto - Authentisiertes Kennwort	Diese Meldung erscheint, wenn die POP3-Server fehlschlägt.
Nicht unterstützte Kommunikationsmethode. Folgendes prüfen. - SMTP-Serveradresse - SMTP-Serverportnummer	Diese Meldung erscheint, wenn Sie versuchen, mit nicht unterstützten Protokollen zu kommunizieren.
Verbindung zum SMTP-Server fehlgeschlagen. Sichere Verbindung in Keine ändern.	Diese Meldung erscheint, wenn eine SMTP-Fehlübereinstimmung zwischen einem Server und einem Client eintritt oder wenn der Server keine sicheren SMTP-Verbindungen (SSL-Verbindungen) unterstützt.
Verbindung zum SMTP-Server fehlgeschlagen. Sichere Verbindung in SSL/TLS ändern.	Diese Meldung erscheint, wenn eine SMTP-Fehlübereinstimmung zwischen einem Server und einem Client eintritt oder wenn der Server anfordert, eine SSL/TLS-Verbindung statt einer SMTP-Verbindung zu verwenden.
Verbindung zum SMTP-Server fehlgeschlagen. Sichere Verbindung in STARTTLS ändern.	Diese Meldung erscheint, wenn eine SMTP-Fehlübereinstimmung zwischen einem Server und einem Client eintritt oder wenn der Server anfordert, eine STARTTLS-Verbindung statt einer SMTP-Verbindung zu verwenden.
Die Verbindung ist nicht vertrauenswürdig. Folgendes prüfen. - Datum und Zeit	Diese Meldung erscheint, wenn die Datum- und Uhrzeiteinstellung des Scanners falsch ist oder das Zertifikat abgelaufen ist.

Meldung	Ursache
Die Verbindung ist nicht vertrauenswürdig. Folgendes prüfen. - CA-Zertifikat	Diese Meldung erscheint, wenn der Server nicht über ein Root-Zertifikat für den Server verfügt oder kein CA-Zertifikat importiert wurde.
Die Verbindung ist nicht vertrauenswürdig.	Diese Meldung erscheint, wenn das bezogene Zertifikat beschädigt ist.
SMTP-Serverauthentifizierung fehlgeschlagen. Authentifizierungsmethode in SMTP-Authentifizierung ändern.	Diese Meldung erscheint, wenn die Authentifizierungsmethode zwischen Server und Client nicht übereinstimmt. Der Server unterstützt SMTP-Authentifizierung.
SMTP-Serverauthentifizierung fehlgeschlagen. Authentifizierungsmethode in POP vor SMTP ändern.	Diese Meldung erscheint, wenn die Authentifizierungsmethode zwischen Server und Client nicht übereinstimmt. Der Server unterstützt SMTP-Authentifizierung nicht.
Absender-eMail-Adresse ist falsch. Zur eMail-Adresse für Ihren eMail-Dienst wechseln.	Diese Meldung erscheint, wenn die angegebene E-Mail-Adresse des Absenders falsch ist.
Zugriff auf das Produkt bis zum Abschluss des Vorgangs nicht möglich.	Diese Meldung erscheint, wenn der Scanner verwendet wird.

## Erstellen eines Netzwerkordners

Erstellen Sie einen Netzwerkordner auf Ihrem Computer. Der Computer muss mit demselben Netzwerk verbunden sein wie der Scanner.

Die Methode zur Einrichtung des Netzwerkordners variiert abhängig von der Umgebung. Das ist ein Beispiel für das Erstellen eines Netzwerkordners auf dem Desktop eines Computers in der folgenden Umgebung.

- Betriebssystem: Windows 10
- Ort für das Erstellen des Netzwerkordners: Desktop
- Ordnerpfad auf dem Desktop: C:\Users\xxxx\Desktop\scan\_folder (create a network folder called „scan\_folder“)

1. Melden Sie sich mit einem Benutzerkonto mit Administratorrechten an dem Computer an, auf dem Sie den Netzwerkordner erstellen möchten.

**Hinweis:**

Wenn Sie nicht wissen, welches Benutzerkonto Administratorrechte hat, wenden Sie sich an Ihren Computeradministrator.

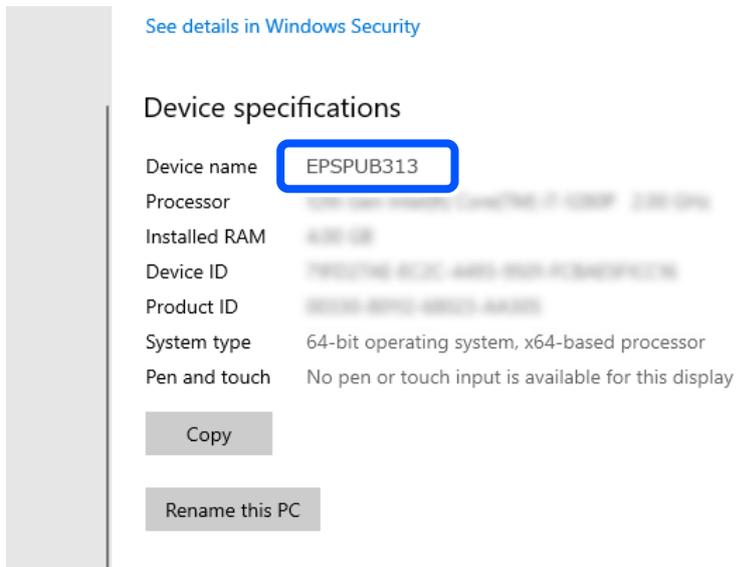
2. Achten Sie darauf, dass der Gerätename (Computername) keine Doppel-Byte-Zeichen enthält. Klicken Sie auf die Start-Schaltfläche von Windows und dann auf  **Einstellungen** > **System** > **Über**.

**Hinweis:**

Wenn der Gerätename ein Doppel-Byte-Zeichen enthält, kann die Datei möglicherweise nicht gespeichert werden.

3. Überprüfen Sie, ob die in **Gerätedaten** > **Gerätename** angezeigte Zeichenfolge Doppel-Byte-Zeichen enthält. Wenn der Gerätename nur Ein-Byte-Zeichen enthält, sollten keine Probleme auftreten. Schließen Sie den Bildschirm.

Beispiel: EPSPUB313



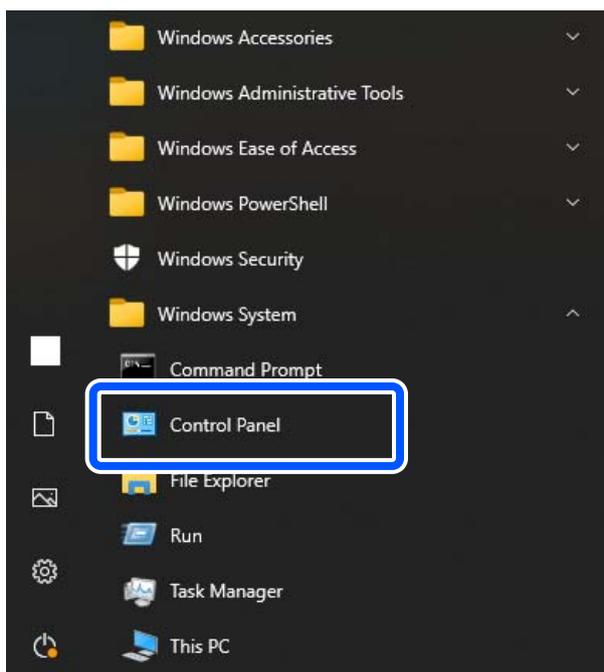
**Wichtig:**

Falls der Gerätename Doppel-Byte-Zeichen enthält, verwenden Sie einen Computer ohne Doppel-Byte-Zeichen oder benennen das Gerät um.

Wenn Sie den Gerätenamen ändern müssen, sollten Sie sich vorab an den Computeradministrator wenden, denn die Umbenennung hat möglicherweise Auswirkungen auf die Computerverwaltung und den Zugriff auf die Ressourcen.

Überprüfen Sie dann die Computereinstellungen.

4. Klicken Sie die Windows Start-Schaltfläche und wählen Sie dann **Windows System** > **Systemsteuerung** aus.



- Öffnen Sie die Systemsteuerung und klicken Sie auf **Netzwerk und Internet > Netzwerk- und Freigabecenter > Erweiterte Freigabeeinstellungen ändern**.

Der Netzwerkprofil wird angezeigt.

- Stellen Sie sicher, dass die Option **Datei- und Druckerfreigabe aktivieren** unter **Datei- und Druckerfreigabe** für das Netzwerkprofil (aktuelles Profil) aktiviert ist.

Falls bereits ausgewählt, klicken Sie auf **Abbrechen** und schließen Sie das Fenster.

Falls Einstellungen geändert werden, klicken Sie auf **Änderungen speichern**, und schließen Sie das Fenster.

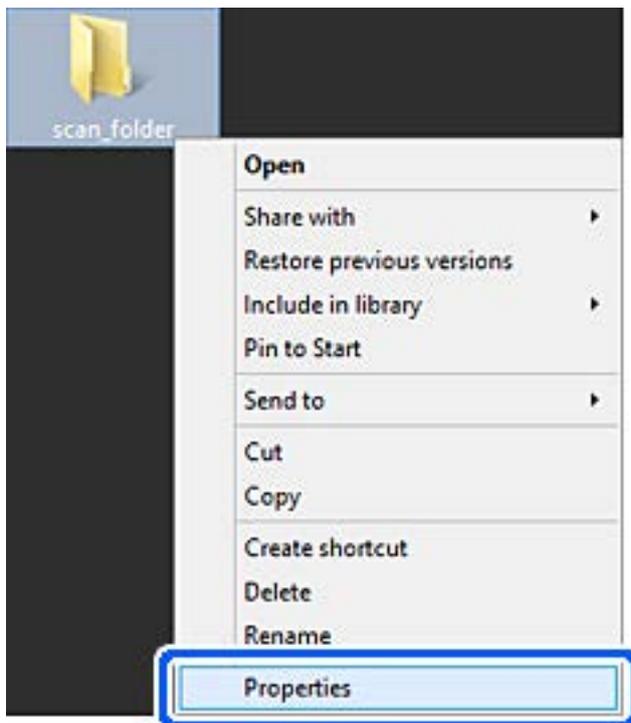
Erstellen Sie dann einen Netzwerkordner.

- Erstellen und benennen Sie einen Ordner auf Ihrem Desktop.

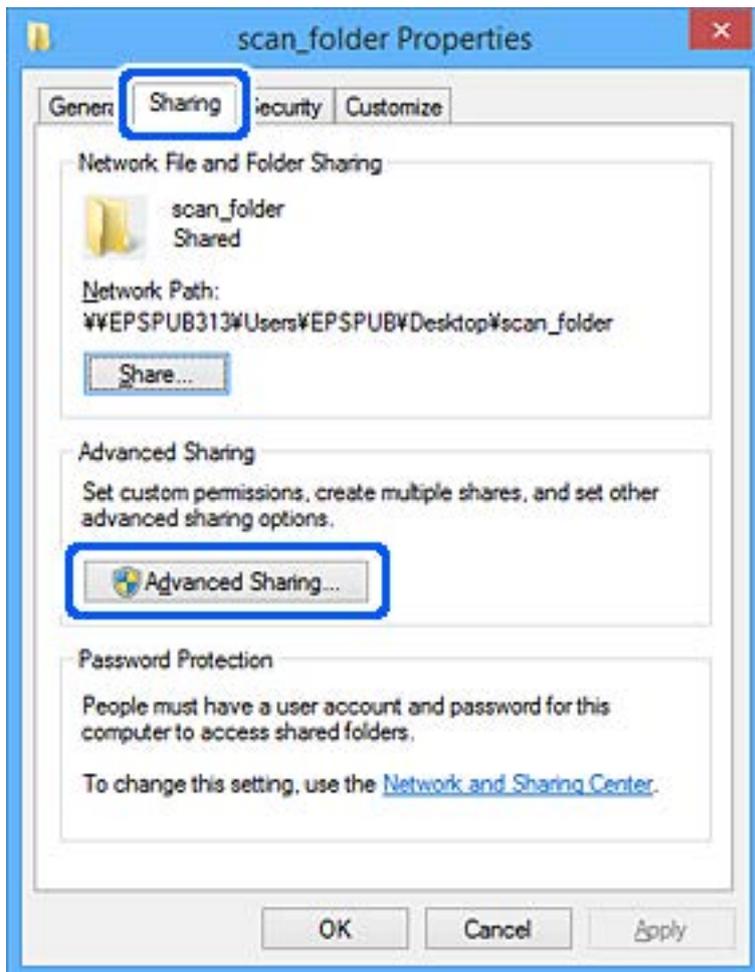
Geben Sie als Ordnernamen zwischen 1 und 12 alphanumerische Zeichen ein. Wenn der Ordnername länger als 12 Zeichen ist, können Sie abhängig von Ihrer Umgebung möglicherweise nicht darauf zugreifen.

Beispiel: scan\_folder

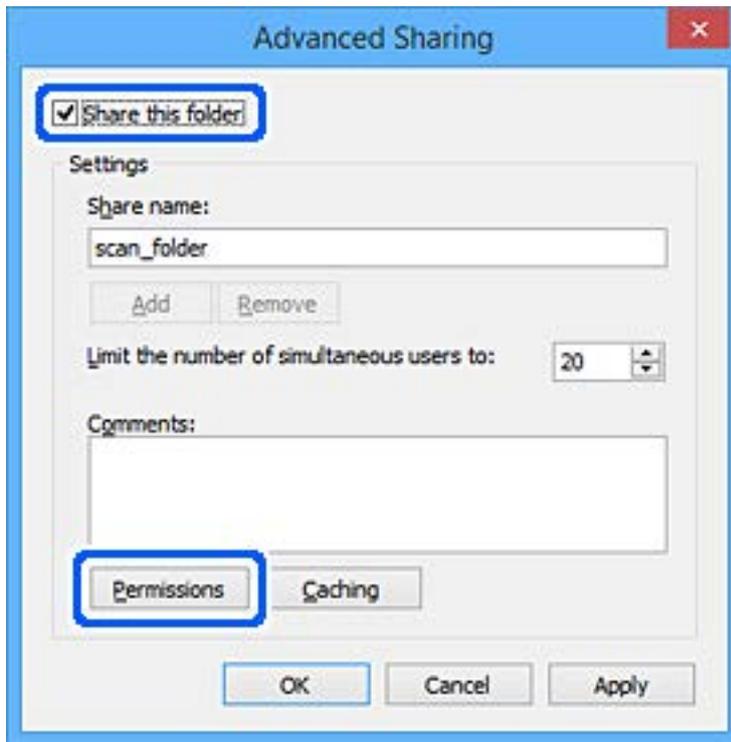
- Rechtsklicken Sie auf den Ordner und wählen Sie dann **Eigenschaften** aus.



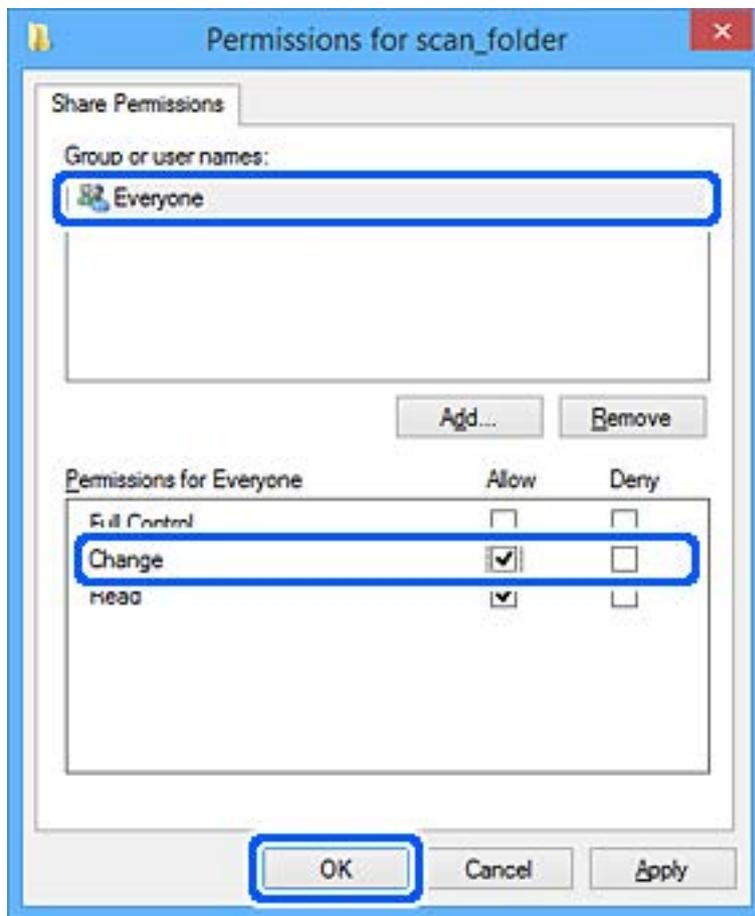
9. Klicken Sie auf **Erweiterte Freigabe** auf der Registerkarte **Freigabe**.



10. Wählen Sie **Diesen Ordner freigeben** und klicken Sie dann auf **Berechtigungen**.



11. Wählen Sie **Jeder** unter **Gruppen- oder Benutzernamen** aus, dann **Erlauben** unter **Ändern** und klicken Sie dann auf **OK**.

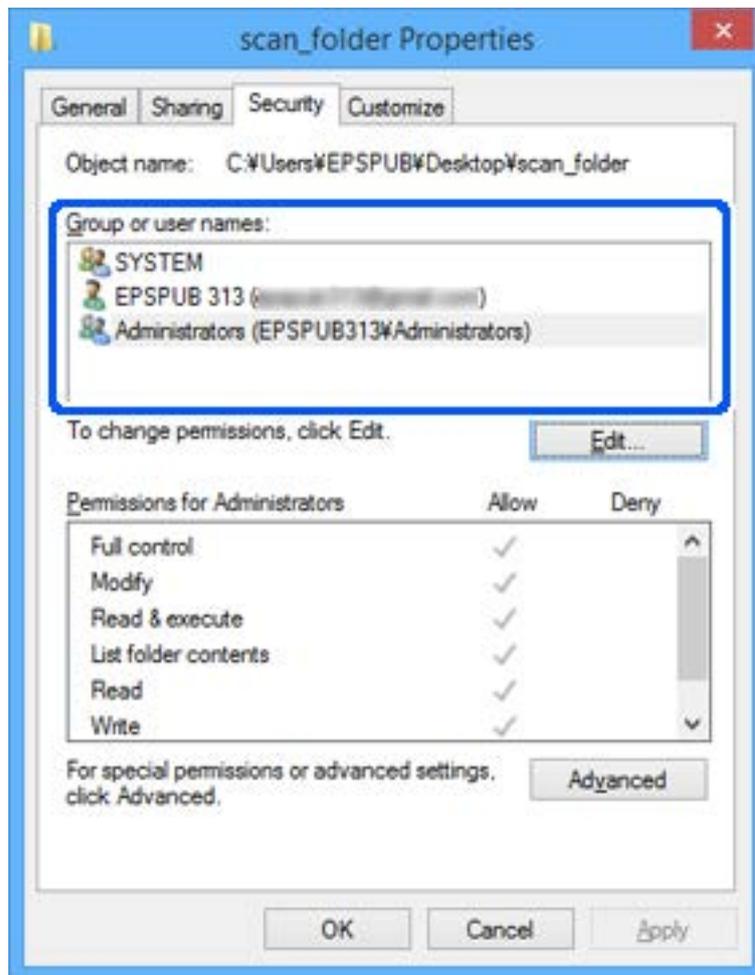


12. Klicken Sie auf **OK**, um den Bildschirm zu schließen und kehren Sie dann zum Fenster „Eigenschaften“ zurück.

**Hinweis:**

Sie können auf der Registerkarte **Sicherheit** > **Gruppen- oder Benutzername** überprüfen, welche Gruppen oder Benutzer Zugriff auf den Netzwerkordner haben.

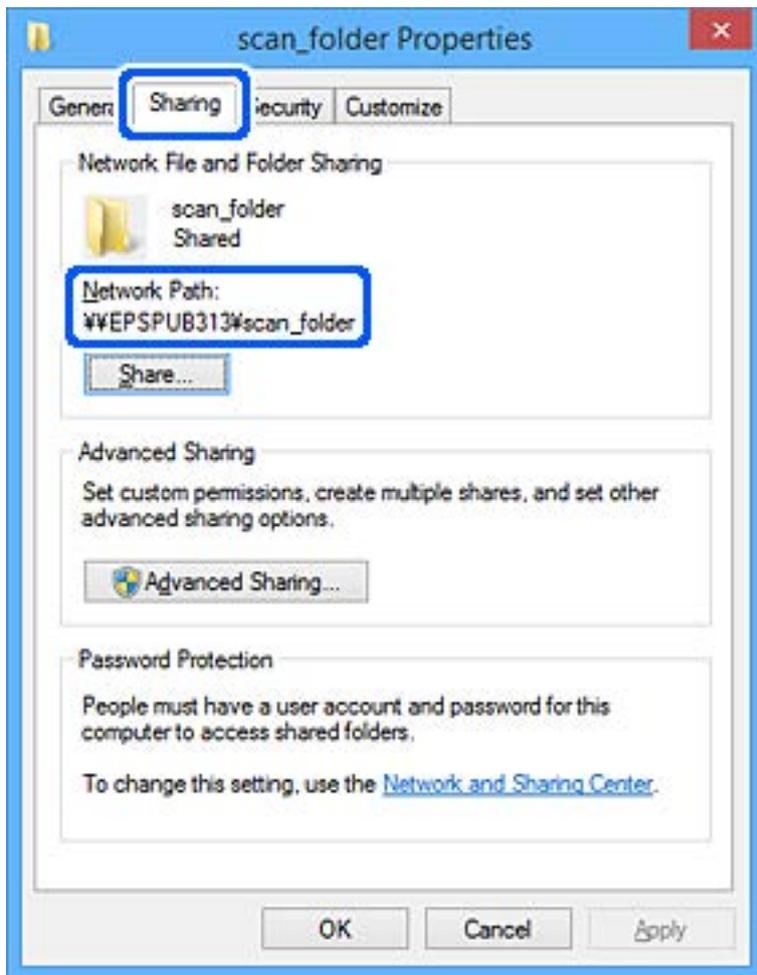
Beispiel: Sowohl der am Computer angemeldete Benutzer als auch die Administratoren können auf den Netzwerkordner zugreifen



13. Wählen Sie die Registerkarte **Freigabe** aus.

Der Netzwerkpfad für den Netzwerkordner wird angezeigt. Er wird beim Registrieren in den Kontakten des Scanners verwendet. Notieren Sie diesen Pfad.

Beispiel: \\EPSPUB313\scan\_folder



14. Klicken Sie auf **Schließen** oder **OK**, um das Fenster zu schließen.

Damit ist das Erstellen des Netzwerkordners abgeschlossen.

---

## Kontakte zur Verfügung stellen

Durch die Registrierung von Zielen in der Kontaktliste des Scanners können Sie das Ziel beim Scannen einfach eingeben.

Sie können die folgenden Arten von Zielen in der Kontaktliste registrieren. Sie können insgesamt bis zu 300 Einträge registrieren.

**Hinweis:**

Sie können auch den LDAP-Server (LDAP-Suche) zur Eingabe des Ziels verwenden.

E-Mail	Ziele für E-Mail. Sie müssen zuvor die E-Mail-Server-Einstellungen konfigurieren.
Netzwerk-Ordner	Ziel für Scandaten. Sie müssen den Netzwerkordner vorher vorbereiten.

## Zugehörige Informationen

➔ „Kooperation zwischen LDAP-Server und Benutzern“ auf Seite 64

## Vergleich der Kontaktkonfiguration

Zur Konfiguration der Kontakte des Scanners gibt es drei Tools: Web Config, Epson Device Admin und das Druckerbedienfeld. In der nachfolgenden Tabelle sind die Unterschiede zwischen den drei Tools aufgeführt.

Funktionen	Web Config*	Epson Device Admin	Scanner-Bedienfeld
Registrieren eines Ziels	✓	✓	✓
Bearbeiten eines Ziels	✓	✓	✓
Hinzufügen einer Gruppe	✓	✓	✓
Bearbeiten einer Gruppe	✓	✓	✓
Löschen eines Ziels oder von Gruppen	✓	✓	✓
Löschen aller Ziele	✓	✓	–
Importieren einer Datei	✓	✓	–
Exportieren in eine Datei	✓	✓	–

\* Melden Sie sich als Administrator an, um Einstellungen vorzunehmen.

## Registrieren eines Ziels für Kontakte mit Web Config

### Hinweis:

Sie können Kontakte auch über das Bedienfeld des Scanners registrieren.

1. Wechseln Sie zu Web Config und wählen Sie die Registerkarte **Scan > Kontakte**.
2. Wählen Sie die Nummer, die Sie registrieren möchten und klicken Sie dann auf **Bearbeiten**.
3. Geben Sie **Name** und **Indexwort** ein.
4. Wählen Sie den Zieltyp als Option für **Typ**.

### Hinweis:

Sie können die Option **Typ** nach der Registrierung nicht ändern. Wenn Sie den Typ ändern möchten, löschen Sie das Ziel und nehmen Sie die Registrierung erneut vor.

5. Geben Sie einen Wert für jedes Element ein und klicken Sie dann auf **Übernehmen**.

## Zugehörige Informationen

➔ „Ausführen von Web Config in einem Webbrowser“ auf Seite 40

## Zieleinstellungselemente

Optionen	Einstellungen und Erläuterung
Allgemeine Einstellungen	
Name	Geben Sie einen Namen zur Anzeige in den Kontakten in 30 Zeichen oder weniger in Unicode (UTF-16) ein. Wenn Sie es nicht angeben, lassen Sie es leer.
Indexwort	Geben Sie einen Namen mit maximal 30 Zeichen in Unicode (UTF-16) ein, um die Kontakte auf dem Bedienfeld des Scanners zu suchen. Wenn Sie es nicht angeben, lassen Sie es leer.
Typ	Wählen Sie die Art der Adresse, die Sie registrieren möchten.
Zu Häufig verwendet zuf.	Wählen Sie diese Option, um die registrierte Adresse als häufig genutzte Adresse zu markieren.  Beim Markieren als häufig genutzte Adresse wird diese auf dem oberen Bildschirm von Scannen angezeigt und Sie können das Ziel ohne Aufrufen der Kontakte angeben.
eMail	
eMail-Adresse	Geben Sie 1 bis 255 Zeichen aus A-Z a-z 0-9 ! # \$ % & ' * + - . / = ? ^ _ {   } ~ @ ein.
Netzwerkordner (SMB)	
Speichern unter	\\„Ordnerpfad“  Geben Sie den Ort an, an dem sich der Zielordner befindet, zwischen 1 und 253 Zeichen in Unicode (UTF-16), ohne „\\“.  Geben Sie den Netzwerkpfad ein, der auf dem Eigenschaftsbildschirm des Ordners angezeigt wird. Einzelheiten zum Einstellen des Netzwerkpfads finden Sie im Folgenden.  <a href="#">„Erstellen eines Netzwerkordners“ auf Seite 50</a>
Benutzername	Geben Sie den Benutzernamen zum Zugriff auf einen Netzwerkordner in 30 Zeichen oder weniger in Unicode (UTF-16) ein. Vermeiden Sie jedoch Steuerzeichen (0x00 bis 0x1f, 0x7f).
Kennwort	Geben Sie ein Kennwort bestehend auf 0 bis 20 Unicode-Zeichen (UTF-16) für den Zugriff auf einen Netzwerkordner ein. Vermeiden Sie jedoch Steuerzeichen (0x00 bis 0x1f, 0x7f).
FTP	
Sichere Verbindung	Wählen Sie gemäß dem Dateiübertragungsprotokoll, das der FTP-Server unterstützt, FTP oder FTPS. Wählen Sie <b>FTPS</b> , um dem Scanner zu erlauben, mit Sicherheitsmaßnahmen zu kommunizieren.
Speichern unter	Geben Sie einen Servernamen zwischen 1 und 253 Zeichen in Unicode (UTF-16) ein und lassen Sie "ftp://" oder "ftps://" weg.
Benutzername	Geben Sie den Benutzernamen zum Zugriff auf einen FTP-Server in 30 Zeichen oder weniger in Unicode (UTF-16) ein. Vermeiden Sie jedoch Steuerzeichen (0x00 bis 0x1f, 0x7f). Wenn der Server anonyme Verbindungen gestattet, geben Sie einen Benutzernamen wie „Anonym“ oder „FTP“ ein. Wenn Sie es nicht angeben, lassen Sie es leer.
Kennwort	Geben Sie ein Kennwort bestehend auf 0 bis 20 Unicode-Zeichen (UTF-16) zum Zugreifen auf einen FTP-Server ein. Vermeiden Sie jedoch Steuerzeichen (0x00 bis 0x1f, 0x7f). Wenn Sie es nicht angeben, lassen Sie es leer.

Optionen	Einstellungen und Erläuterung
Verbindungsmodus	Wählen Sie den Verbindungsmodus aus dem Menü. Ist eine Firewall zwischen Scanner und FTP-Server eingerichtet, wählen Sie <b>Passiver Modus</b> .
Anschlussnummer	Geben Sie eine FTP-Serverportnummer zwischen 1 und 65535 ein.
Zertifikatsvalidierung	Das Zertifikat des FTP-Servers wird validiert, wenn diese Option aktiviert ist. Diese Option ist verfügbar, wenn <b>FTPS</b> für <b>Sichere Verbindung</b> ausgewählt ist. Zum Einrichten müssen Sie das CA-Zertifikat in den Scanner importieren.
SharePoint(WebDAV)*	
Sichere Verbindung	Wählen Sie HTTP oder HTTPS gemäß dem Dateiübertragungsprotokoll, das der Server unterstützt. Wählen Sie <b>HTTPS</b> , um dem Scanner zu erlauben, mit Sicherheitsmaßnahmen zu kommunizieren.
Speichern unter	Geben Sie einen Servernamen zwischen 1 und 253 Zeichen in Unicode (UTF-16) ein und lassen Sie "http://" oder "https://" weg.
Benutzername	Geben Sie den Benutzernamen zum Zugriff auf einen Server in 30 Zeichen oder weniger in Unicode (UTF-16) ein. Vermeiden Sie jedoch Steuerzeichen (0x00 bis 0x1f, 0x7F). Wenn Sie es nicht angeben, lassen Sie es leer.
Kennwort	Geben Sie ein Kennwort bestehend auf 0 bis 20 Unicode-Zeichen (UTF-16) ein. Vermeiden Sie jedoch Steuerzeichen (0x00 bis 0x1f, 0x7F). Wenn Sie es nicht angeben, lassen Sie es leer.
Zertifikatsvalidierung	Das Zertifikat des Servers wird validiert, wenn diese Option aktiviert ist. Diese Option ist verfügbar, wenn <b>HTTPS</b> für <b>Sichere Verbindung</b> ausgewählt ist. Zum Einrichten müssen Sie das CA-Zertifikat in den Scanner importieren.
Proxy-Server	Wählen Sie, ob ein Proxyserver verwendet werden soll.

\* SharePoint Online wird nicht unterstützt, wenn Sie auf dem Scanner-Bedienfeld an einen Netzwerkordner scannen.

Um ein gescanntes Bild bei SharePoint Online zu speichern, verwenden Sie Document Capture Pro, nachdem Sie SharePoint Online Connector installiert haben. Ausführliche Informationen finden Sie im Document Capture Pro-Handbuch.

<https://support.epson.net/dcp/>

## Registrieren von Zielen als Gruppe mit Web Config

Wenn der Zieltyp auf **eMail** eingestellt wurde, können Sie die Ziele als Gruppe registrieren.

1. Wechseln Sie zu Web Config und wählen Sie die Registerkarte **Scan > Kontakte**.
2. Wählen Sie die Nummer, die Sie registrieren möchten und klicken Sie dann auf **Bearbeiten**.
3. Wählen Sie eine Gruppe aus **Typ**.
4. Klicken Sie auf **Wählen** für **Kontakt(e) für Gruppe**.  
Die verfügbaren Ziele werden angezeigt.
5. Wählen Sie das Ziel, das Sie in der Gruppe registrieren möchten und klicken Sie dann auf **Wählen**.

6. Geben Sie einen **Name** und ein **Indexwort** ein.
7. Wählen Sie, ob die registrierte Gruppe der häufig verwendeten Gruppe zugewiesen werden soll.

**Hinweis:**

*Ziele können in mehreren Gruppen registriert werden.*

8. Klicken Sie auf **Übernehmen**.

### **Zugehörige Informationen**

➔ [„Ausführen von Web Config in einem Webbrowser“ auf Seite 40](#)

## **Sichern und Importieren von Kontakten**

Mithilfe von Web Config oder anderen Tools lassen sich Kontakte sichern und importieren.

Für Web Config lassen sich Kontakte sichern, indem Sie die Scannereinstellungen mit den enthaltenen Kontakten exportieren. Die exportierte Datei kann nicht bearbeitet werden, da sie als Binärdatei exportiert wird.

Beim Importieren der Scannereinstellungen in den Scanner werden Kontakte überschrieben.

Für Epson Device Admin können vom Eigenschaftfenster des Geräts nur Kontakte exportiert werden. Zudem gilt, dass wenn sicherheitsbezogene Elemente nicht exportiert werden, die exportierten Kontakte bearbeitet und dann erneut importiert werden können, da diese als SYLK- oder CSV-Datei gespeichert werden.

### **Importieren von Kontakten mit Web Config**

Wenn Sie einen Scanner haben, der die Sicherung von Kontakten ermöglicht und mit diesem Scanner kompatibel ist, können Sie Kontakte einfach durch Importieren der Sicherungsdatei registrieren.

**Hinweis:**

*Anweisungen zum Sichern der Scannerkontakte finden Sie im Handbuch des Druckers.*

Befolgen Sie diese Schritte, um die Kontakte auf diesen Scanner zu importieren.

1. Rufen Sie Web Config auf, wählen Sie die Registerkarte **Geräteverwaltung > Einstellungswert exportieren und importieren > Importieren**.
2. Wählen Sie unter **Datei** die erstellte Sicherungsdatei, geben Sie das Kennwort ein und klicken Sie dann auf **Weiter**.
3. Wählen Sie das Kontrollkästchen **Kontakte** und klicken Sie dann auf **Weiter**.

### **Sichern von Kontakten mit Web Config**

Kontaktdaten können aufgrund einer Fehlfunktion des Scanners verlorengehen. Es wird empfohlen, nach der Aktualisierung Ihrer Daten ein Backup zu erstellen. Epson ist nicht haftbar für den Verlust von Daten, für das Sichern oder Wiederherstellen von Daten und/oder Einstellungen selbst innerhalb des Garantiezeitraums.

Mit Web Config können Sie die im Scanner gespeicherten Kontaktdaten auf einen Computer sichern.

1. Rufen Sie Web Config auf, und wählen Sie dann die Registerkarte **Geräteverwaltung > Einstellungswert exportieren und importieren > Exportieren**.

2. Aktivieren Sie das Kontrollkästchen **Kontakte** unter der Kategorie **Scan**.
3. Geben Sie ein Kennwort zur Verschlüsselung der exportierten Datei ein.  
Sie benötigen das Kennwort, um die Datei zu importieren. Lassen Sie dies leer, wenn Sie die Datei nicht verschlüsseln möchten.
4. Klicken Sie auf **Exportieren**.

## Exportieren und Mengenregistrierung von Kontakten mithilfe eines Tools

Mit Epson Device Admin lassen sich die Kontakte gesondert exportieren. Die exportierten Dateien können dann bearbeitet und in einem Schritt registriert werden.

Dies ist nützlich, wenn ausschließlich die Kontakte gesichert werden sollen oder der Scanner ausgetauscht wird und Sie die Kontakte vom alten Drucker auf den neuen übertragen möchten.

### Exportieren von Kontakten

Zum Speichern der Kontaktdaten in eine Datei.

Mithilfe einer Tabellenkalkulation oder einem Texteditor lassen sich Dateien im SYLK- oder CSV-Format bearbeiten. Nach dem Löschen bzw. Hinzufügen von Daten lassen sich die Kontakte in einem Durchgang registrieren.

Daten, die Sicherheitselemente wie Kennwörter oder persönliche Angaben enthalten, lassen sich in Binärform mit einem Kennwort speichern. Diese Dateien können nicht bearbeitet werden. Sie dienen zur Datensicherung einschließlich der Sicherheitselemente.

1. Starten Sie Epson Device Admin.
2. Wählen Sie im Aufgabenmenü der Seitenleiste **Drucker**.
3. Wählen Sie das zu konfigurierende Gerät aus der Geräteliste aus.
4. Klicken Sie auf **Gerätekonfiguration** auf der Registerkarte **Startseite** des Menübands.  
Falls ein Administratorkennwort eingerichtet wurde, geben Sie das Kennwort ein und klicken Sie auf **OK**.
5. Klicken Sie auf **Allgemein** > **Kontakte**.
6. Wählen Sie das Exportformat aus **Exportieren** > **Elemente exportieren**.
  - Alle Elemente  
Exportieren einer verschlüsselten Binärdatei. Wählen Sie diese Option, wenn auch Sicherheitselemente wie Kennwörter und persönliche Daten exportiert werden sollen. Diese Dateien können nicht bearbeitet werden. Bei dieser Auswahl muss ein Kennwort eingerichtet werden. Klicken Sie auf **Konfiguration** und legen Sie ein Kennwort zwischen 8 und 63 ASCII-Zeichen fest. Dieses Kennwort ist für das Importieren der Binärdatei erforderlich.
  - Elemente mit Ausnahme von Sicherheitsinformationen  
Exportieren einer Datei im Format SYLK oder CSV. Wählen Sie diese Option, wenn die exportierte Datei bearbeitet werden soll.

7. Klicken Sie auf **Exportieren**.
8. Wählen Sie einen Speicherort für die Datei aus sowie einen Dateityp, und klicken Sie dann auf **Speichern**.  
Eine Abschlussmeldung wird angezeigt.
9. Klicken Sie auf **OK**.  
Überprüfen Sie, ob die Datei am festgelegten Ort gespeichert wurde.

## Importieren von Kontakten

Zum Importieren der Kontaktdaten aus einer Datei.

Die Dateien lassen sich im SYLK- oder CSV-Format speichern, oder in einer Binärdatei zur Datensicherung inklusive der Sicherheitselemente.

1. Starten Sie Epson Device Admin.
2. Wählen Sie im Aufgabenmenü der Seitenleiste **Drucker**.
3. Wählen Sie das zu konfigurierende Gerät aus der Geräteliste aus.
4. Klicken Sie auf **Gerätekonfiguration** auf der Registerkarte **Startseite** des Menübands.  
Falls ein Administratorkennwort eingerichtet wurde, geben Sie das Kennwort ein und klicken Sie auf **OK**.
5. Klicken Sie auf **Allgemein > Kontakte**.
6. Klicken Sie auf **Durchsuchen** unter **Importieren**.
7. Wählen Sie die zu importierende Datei aus und klicken Sie dann auf **Öffnen**.  
Geben Sie beim Auswählen der Binärdatei unter **Passwort** das Kennwort für den Export ein.
8. Klicken Sie auf **Importieren**.  
Ein Bestätigungsbildschirm wird angezeigt.
9. Klicken Sie auf **OK**.  
Das Validierungsergebnis wird angezeigt.
  - Geladene Informationen bearbeiten  
Klicken, falls die Datensätze einzeln bearbeitet werden sollen.
  - Weitere Dateien laden  
Klicken, falls mehrere Dateien importiert werden sollen.
10. Klicken Sie auf **Importieren** und dann auf **OK** im Abschlussbildschirm des Importvorgangs.  
Sie befinden sich dann erneut auf der Seite mit den Geräteeigenschaften.
11. Klicken Sie auf **Senden**.
12. Klicken Sie in der Bestätigungsmeldung auf **OK**.  
Die Einstellungen werden an den Scanner gesendet.

13. Klicken Sie im Abschlussbildschirm des Versands auf **OK**.

Die Scannerdaten werden angezeigt.

Öffnen Sie die Kontakte in Web Config oder vom Scannerbedienfeld aus, und kontrollieren Sie dann, ob der Kontakt aktualisiert wurde.

## Kooperation zwischen LDAP-Server und Benutzern

Bei der Kooperation mit dem LDAP-Server können Sie die im LDAP-Server gespeicherten Adressdaten als Ziel für E-Mails verwenden.

### Konfigurieren des LDAP-Servers

Um die LDAP-Serverdaten zu verwenden, müssen diese im Scanner registriert werden.

1. Rufen Sie Web Config auf, und wählen Sie dann die Registerkarte **Netzwerk > LDAP-Server > Grundlegend**.
2. Geben Sie einen Wert für jedes Element ein.
3. Wählen Sie **OK**.

Die gewählten Einstellungen werden angezeigt.

### LDAP-Server-Einstellungselemente

Optionen	Einstellungen und Erläuterung
LDAP-Server nutzen	Wählen Sie <b>Verwenden</b> oder <b>Nicht verwenden</b> .
LDAP-Serveradresse	Geben Sie die Adresse des LDAP-Servers ein. Geben Sie 1 bis 255 Zeichen im IPv4-, IPv6- oder FQDN-Format ein. Für das FQDN-Format können Sie alphanumerische Zeichen in ASCII (0x20–0x7E) und „-“ verwenden, außer für Anfang und Ende der Adresse.
LDAP-Server-Portnummer	Geben Sie die LDAP-Serverportnr. zwischen 1 und 65535 ein.
Sichere Verbindung	Geben Sie die Authentifizierungsmethode für den Zugriff des Scanners auf den LDAP-Server an.
Zertifikatsvalidierung	Wenn diese Option aktiviert ist, wird das Zertifikat des LDAP-Servers validiert. Wir empfehlen, die Option auf <b>Aktivieren</b> zu setzen. Zum Vornehmen der Einstellung muss das <b>CA-Zertifikat</b> im Scanner importiert werden.
Suchzeitüberschreitung (Sek.)	Legen Sie die Länge der Suchzeit bis zur Zeitüberschreitung zwischen 5 und 300 fest.

Optionen	Einstellungen und Erläuterung
Authentisierungsmethode	<p>Wählen Sie eine der Methoden.</p> <p>Wenn Sie <b>Kerberos-Authentifizierung</b> wählen, wählen Sie <b>Kerberos-Einstellungen</b>, um Einstellungen für Kerberos vorzunehmen.</p> <p>Zum Durchführen der Kerberos-Authentifizierung ist die folgende Umgebung erforderlich.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Der Scanner und der DNS-Server können kommunizieren.</li> <li><input type="checkbox"/> Die Uhrzeiten des Scanners, des KDC-Servers und des Servers, der für die Authentifizierung erforderlich ist (LDAP-Server, SMTP-Server, Dateiserver), sind synchronisiert.</li> <li><input type="checkbox"/> Wenn der Service-Server als IP-Adresse zugewiesen ist, wird der FQDN des Service-Servers in der Reverse-Lookup-Zone des DNS-Servers registriert.</li> </ul>
Zu verwendender Kerberos-Realm	Wenn Sie <b>Kerberos-Authentifizierung</b> für <b>Authentisierungsmethode</b> wählen, wählen Sie den Kerberos-Realm, den Sie verwenden möchten.
Administrator-DN / Benutzername	Geben Sie den Benutzernamen für den LDAP-Server in 128 Zeichen oder weniger in Unicode (UTF-8) ein. Sie können keine Kontrollzeichen wie 0x00–0x1F und 0x7F verwenden. Diese Einstellung wird nicht verwendet, wenn <b>Anonyme Authentifizierung</b> als <b>Authentisierungsmethode</b> gewählt wird. Wenn Sie dies nicht angeben, lassen Sie es leer.
Kennwort	Geben Sie das Kennwort für den LDAP-Server in 128 Zeichen oder weniger in Unicode (UTF-8) ein. Sie können keine Kontrollzeichen wie 0x00–0x1F und 0x7F verwenden. Diese Einstellung wird nicht verwendet, wenn <b>Anonyme Authentifizierung</b> als <b>Authentisierungsmethode</b> gewählt wird. Wenn Sie dies nicht angeben, lassen Sie es leer.

### **Kerberos-Einstellungen**

Falls Sie **Kerberos-Authentifizierung** für **Authentisierungsmethode** in **LDAP-Server > Grundlegend** auswählen, nehmen Sie folgende Kerberos-Einstellungen auf der Registerkarte **Netzwerk > Kerberos-Einstellungen** vor. Sie können bis zu 10 Einstellungen in den Kerberos-Einstellungen registrieren.

Optionen	Einstellungen und Erläuterung
Realm (Domain)	Auf Kerberos-Authentifizierung in 255 Zeichen oder weniger in ASCII (0x20–0x7E) zugreifen. Falls dies nicht registriert wird, das Feld leer lassen.
KDC-Adresse	Geben Sie die Adresse des Kerberos-Authentifizierungsservers ein. Geben Sie 255 Zeichen oder weniger im IPv4-, IPv6- oder FQDN-Format ein. Falls dies nicht registriert wird, das Feld leer lassen.
Portnummer (Kerberos)	Geben Sie die Kerberos-Serverportnr. zwischen 1 und 65535 ein.

### **Konfigurieren der LDAP-Server-Sucheinstellungen**

Beim Einrichten der Sucheinstellungen können Sie die im LDAP-Server registrierte E-Mail-Adresse verwenden.

1. Wechseln Sie zu Web Config und wählen Sie die Registerkarte **Netzwerk > LDAP-Server > Sucheinstellungen**.
2. Geben Sie einen Wert für jedes Element ein.

3. Klicken Sie auf **OK**, um das Einstellungsergebnis anzuzeigen.  
Die gewählten Einstellungen werden angezeigt.

### **LDAP-Server-Sucheinstellungselemente**

<b>Optionen</b>	<b>Einstellungen und Erläuterung</b>
Suchbasis (distinguierter Name)	Wenn Sie nach einer bestimmten Domäne suchen, geben Sie den Domänennamen des LDAP-Servers an. Geben Sie zwischen 0 und 128 Zeichen in Unicode (UTF-8) ein. Wenn Sie nicht nach einem bestimmten Attribut suchen, lassen Sie dies leer.  Beispiel für das lokale Serververzeichnis: dc=server,dc=local
Anzahl Sucheinträge	Geben Sie die Anzahl der Sucheinträge zwischen 5 und 500 an. Die angegebene Zahl der Sucheinträge wird gespeichert und vorübergehend angezeigt. Selbst wenn die Anzahl der Sucheinträge die angegebene Zahl übersteigt und eine Fehlermeldung erscheint, kann die Suche abgeschlossen werden.
Benutzernamensattribut	Geben Sie den Attributnamen an, der bei der Suche nach Benutzernamen angezeigt werden soll. Geben Sie zwischen 1 und 255 Zeichen in Unicode (UTF-8) ein. Das erste Zeichen muss a-z oder A-Z sein.  Beispiel: cn, uid
Benutzernamensanzeigattribut	Geben Sie den Attributnamen an, der als Benutzername angezeigt werden soll. Geben Sie zwischen 0 und 255 Zeichen in Unicode (UTF-8) ein. Das erste Zeichen muss a-z oder A-Z sein.  Beispiel: cn, sn
eMail-Adressattribut	Geben Sie den Attributnamen an, der bei der Suche von E-Mail-Adressen angezeigt werden soll. Geben Sie eine Kombination zwischen 1 und 255 Zeichen aus A-Z, a-z, 0-9 und - ein. Das erste Zeichen muss a-z oder A-Z sein.  Beispiel: mail
Willkürliches Attribut 1 - Willkürliches Attribut 4	Sie können andere bestimmte Attribute angeben, nach denen gesucht werden soll. Geben Sie zwischen 0 und 255 Zeichen in Unicode (UTF-8) ein. Das erste Zeichen muss a-z oder A-Z sein. Wenn Sie nicht nach bestimmten Attributen suchen, lassen Sie dies leer.  Beispiel: o, ou

## **Überprüfen der LDAP-Serververbindung**

Zur Durchführung eines Verbindungstests zum LDAP-Server anhand des unter **LDAP-Server** > **Sucheinstellungen** eingestellten Parameters.

1. Wechseln Sie zu Web Config und wählen Sie die Registerkarte **Netzwerk** > **LDAP-Server** > **Verbindungstest**.
2. Wählen Sie **Start**.  
Der Verbindungstest wird gestartet. Nach dem Test wird der Prüfbericht angezeigt.

**Verbindungstestreferenzen für LDAP-Server**

Meldungen	Erklärung
Verbindungstest war erfolgreich.	Diese Meldung erscheint, wenn die Verbindung zum Server erfolgreich ist.
Verbindungstest fehlgeschlagen. Einstellungen prüfen.	Diese Meldung erscheint aus folgenden Gründen: <input type="checkbox"/> Die LDAP-Serveradresse oder die Portnummer ist falsch. <input type="checkbox"/> Eine Zeitüberschreitung ist erfolgt. <input type="checkbox"/> <b>Nicht verwenden</b> ist für <b>LDAP-Server nutzen</b> ausgewählt. <input type="checkbox"/> Falls <b>Kerberos-Authentifizierung</b> als Einstellung für <b>Authentisierungsmethode</b> ausgewählt wurde, sind Einstellungen wie <b>Realm (Domain)</b> , <b>KDC-Adresse</b> und <b>Portnummer (Kerberos)</b> ungültig.
Verbindungstest fehlgeschlagen. Prüfen Sie Datum und Zeit an Ihrem Produkt oder Server.	Diese Meldung erscheint, wenn die Verbindung fehlschlägt, weil die Zeiteinstellungen für Scanner und LDAP-Server nicht übereinstimmen.
Authentifizierung fehlgeschlagen. Einstellungen prüfen.	Diese Meldung erscheint aus folgenden Gründen: <input type="checkbox"/> <b>Benutzername</b> und/oder <b>Kenntwort</b> ist falsch. <input type="checkbox"/> Falls <b>Kerberos-Authentifizierung</b> als <b>Authentisierungsmethode</b> gewählt wurde, sind Datum/Uhrzeit möglicherweise nicht konfiguriert.
Zugriff auf das Produkt bis zum Abschluss des Vorgangs nicht möglich.	Diese Meldung erscheint, wenn der Scanner verwendet wird.

## Einrichten von AirPrint

Rufen Sie Web Config auf, wählen Sie die Registerkarte **Netzwerk** und wählen Sie dann **AirPrint-Einrichtung** aus.

Optionen	Erklärung
Bonjour-Dienstname	Geben Sie einen Bonjour-Dienst-Namen in ASCII-Textform (0x20–0x7E) mit bis zu 41 Zeichen ein.
Bonjour-Ort	Geben Sie eine Beschreibung des Scanner-Standorts in Unicode (UTF-8) mit bis zu 127 Bytes ein.
Wide-Area Bonjour	Legen Sie fest, ob Wide-Area Bonjour verwendet werden soll. Wenn Sie dieses Protokoll verwenden, muss der Scanner auf dem DNS-Server registriert sein, damit der Scanner über das Segment gesucht werden kann.
AirPrint aktivieren	Aktiviert Bonjour und AirPrint (Scandienst). Diese Schaltfläche ist nur verfügbar, wenn AirPrint deaktiviert ist.  <b>Hinweis:</b> Wenn AirPrint deaktiviert ist, ist auch das Scannen mit Mopria von Chromebooks, Windows und der App Mopria Scan aktiviert.

---

# Probleme bei der Vorbereitung von Netzwerk-Scans

## Hinweise zur Fehlerbehebung

Prüfen der Fehlermeldung

Prüfen Sie beim Auftreten eines Fehlers zunächst, ob am Bedienfeld des Scanners oder im Treiberfenster Meldungen angezeigt wurden. Falls beim Auftreten des Ereignisses Benachrichtigungs-E-Mails konfiguriert wurden, erhalten Sie anhand dieser umgehend eine Statusmeldung.

Prüfen des Kommunikationsstatus

Prüfen Sie den Kommunikationsstatus des Servercomputers oder Clientcomputers mit Befehlen wie ping und ipconfig.

Verbindungstest

Zum Überprüfen der Verbindung zwischen Scanner und E-Mail-Server über einen am Scanner durchgeführten Verbindungstest. Prüfen Sie auch die Verbindung vom Clientcomputer zum Server, um den Kommunikationsstatus zu prüfen.

Initialisieren der Einstellungen

Falls der Status von Einstellungen und Kommunikation in Ordnung ist, wird das Problem eventuell durch Deaktivieren oder Initialisieren der Netzwerkeinstellungen des Scanner und anschließende Neukonfiguration behoben.

## Zugriff auf Web Config nicht möglich

### ■ Dem Scanner wurde keine IP-Adresse zugewiesen.

#### Lösungen

Dem Scanner wurde möglicherweise keine gültige IP-Adresse zugewiesen. Konfigurieren Sie die IP-Adresse über das Bedienfeld des Scanners. Sie können die aktuellen Einstellungsinformationen über das Bedienfeld des Scanners bestätigen.

### ■ Der Webbrowser unterstützt die Verschlüsselungsstärke für SSL/TLS nicht.

#### Lösungen

SSL/TLS entspricht Verschlüsselungsstärke. Sie können Web Config mit einem Webbrowser öffnen, der Massenverschlüsselungen unterstützt, wie unten angegeben. Überprüfen Sie, ob Sie einen unterstützten Browser verwenden.

- 80 bit: AES256/AES128/3DES
- 112 bit: AES256/AES128/3DES
- 128 bit: AES256/AES128
- 192 bit: AES256
- 256 bit: AES256

## ■ CA-signiertes Zertifikat ist abgelaufen.

### Lösungen

Wenn es ein Problem mit dem Ablaufdatum des Zertifikats gibt, wird bei der Verbindung zu Web Config mit SSL/TLS-Kommunikation (https) „Das Zertifikat ist abgelaufen“ angezeigt. Wenn die Meldung vor dem Ablaufdatum erscheint, vergewissern Sie sich, dass das Datum des Scanners korrekt konfiguriert ist.

## ■ Der Common Name des Zertifikats und der des Scanners stimmen nicht überein.

### Lösungen

Wenn der Common Name des Zertifikats und des Scanners nicht übereinstimmen, wird beim Zugriff auf Web Config über SSL/TLS-Kommunikation (https) die Meldung „Der Name des Sicherheitszertifikats stimmt nicht überein...“ angezeigt. Dies geschieht, weil die folgenden IP-Adressen nicht übereinstimmen.

- Die Scanner-IP-Adresse, die als Common Name beim Erstellen eines Selbstsigniertes Zertifikat oder des CSR eingegeben wurde
- IP-Adresse, die beim Ausführen von Web Config in den Webbrowser eingegeben wurde

Aktualisieren Sie bei Selbstsigniertes Zertifikat das Zertifikat.

Verwenden Sie bei einem CA-signiertes Zertifikat ein neues, passendes Zertifikat für den Scanner.

## ■ Die Proxy-Server-Einstellung der lokalen Adresse ist nicht auf den Webbrowser eingestellt.

### Lösungen

Wenn der Scanner so eingestellt ist, dass er einen Proxy-Server verwendet, konfigurieren Sie den Webbrowser so, dass er sich nicht über den Proxy-Server mit der lokalen Adresse verbindet.

- Windows:

Wählen Sie **Systemsteuerung > Netzwerk und Internet > Internet-Optionen > Verbindungen > LAN-Einstellungen > Proxy-Server**, und konfigurieren Sie dann, dass der Proxy-Server für LAN (lokale Adressen) nicht verwendet wird.

- Mac OS:

Wählen Sie **Systemeinstellungen (oder Systempräferenzen) > Netzwerk > Erweitert > Proxies**, und registrieren Sie dann die lokale Adresse unter **Proxy-Einstellungen für folgende Hosts und Domains umgehen**.

Beispiel:

192.168.1.\*: Lokale Adresse 192.168.1.XXX, Subnetz-Maske 255.255.255.0

192.168.\*.\*: Lokale Adresse 192.168.XXX.XXX, Subnetz-Maske 255.255.0.0

## ■ DHCP ist in den Einstellungen des Computers deaktiviert.

### Lösungen

Solange DHCP zum automatischen Bezug einer IP-Adresse auf dem Computer deaktiviert ist, können Sie nicht auf Web Config zugreifen. DHCP aktivieren.

Beispiel Für Windows 10:

Öffnen Sie die Systemsteuerung und klicken Sie auf **Netzwerk und Internet > Netzwerk- und Freigabecenter > Adaptoreinstellungen ändern**. Öffnen Sie den Eigenschaften-Bildschirm der von Ihnen verwendeten Verbindung und dann den Eigenschaften-Bildschirm für **Internet Protocol Version 4 (TCP/IPv4)** oder **Internet Protocol Version 6 (TCP/IPv6)**. Achten Sie darauf, dass **IP-Adresse automatisch beziehen** auf dem angezeigten Bildschirm ausgewählt ist.

---

# Anpassen der Bedienfeldanzeige

Registrieren von Voreinst.. . . . .	71
Editieren des Bedienfeld-Startbildschirms. . . . .	73

## Registrieren von Voreinst.

Sie können häufig verwendete Scan-Einstellungen als **Voreinst.** registrieren. Es werden bis zu 48 Voreinstellungen unterstützt.

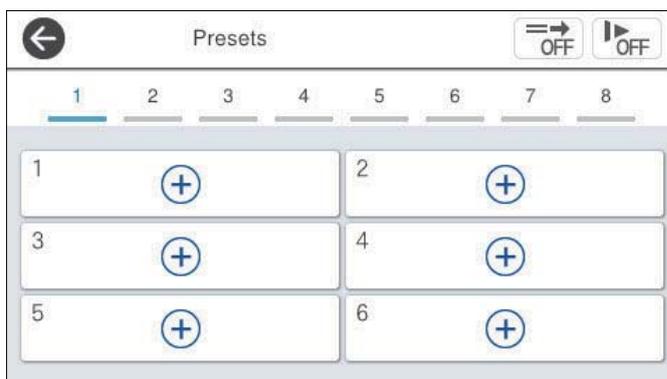
### Hinweis:

- Sie können die aktuellen Einstellungen registrieren, indem Sie auf dem Scanvorgang-Starten-Bildschirm  auswählen.
- Sie können **Voreinstellungen** auch in Web Config registrieren.  
Wählen Sie die Registerkarte **Scan > Voreinstellungen**.
- Wenn Sie bei der Registrierung die Option **An Computer scannen** wählen, können Sie den in Document Capture Pro erstellten Auftrag als **Voreinstellungen** registrieren. Dies ist nur für Computer verfügbar, die über ein Netzwerk verbunden sind. Registrieren Sie den Auftrag in Document Capture Pro im Voraus.
- Wenn die Authentifizierungsfunktion aktiviert ist, kann nur der Administrator **Voreinstellungen** registrieren.

1. Wählen Sie im Startbildschirm auf dem Bedienfeld des Scanners **Voreinst.**.



2. Wählen Sie .



3. Wählen Sie das Menü aus, das Sie zum Registrieren einer Voreinstellung verwenden möchten.



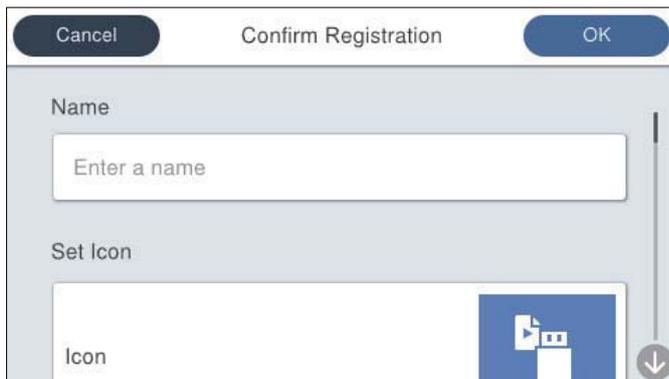
4. Konfigurieren Sie die einzelnen Elemente und klicken Sie dann auf .

**Hinweis:**

Wenn Sie **An Computer scannen** auswählen, wählen Sie den Computer aus, auf dem Document Capture Pro installiert ist, und wählen Sie dann einen registrierten Auftrag. Dies ist nur für Computer verfügbar, die über ein Netzwerk verbunden sind.

5. Anwenden der Voreinstellungen.

- Name:** Einrichten des Namens.
- Symbol einrichten:** Zum Einstellen von Bild und Farbe des darzustellenden Symbols.
- Schnellversand-Einstellung:** Beginnt nach Auswahl der Voreinstellung sofort ohne Abfrage mit dem Scannen.
- Inhalt:** Überprüfen der Scan-Einstellungen.



6. Wählen Sie OK.

## Menüoptionen von Voreinst.

Die Einstellungen einer Voreinstellung lassen sich jeweils durch Auswählen von  ändern.

Name ändern:

Ändert den Namen einer Voreinstellung.

Symbol ändern:

Ändert das Symbolbild und die Farbe einer Voreinstellung.

Schnellversand-Einstellung:

Beginnt nach Auswahl der Voreinstellung sofort ohne Abfrage mit dem Scannen.

Position ändern:

Ändert die Anzeigereihenfolge der Voreinstellungen.

Löschen:

Löscht eine Voreinstellung.

Symbol auf Startseite hinzufügen oder entfernen:

Fügt das Symbol der Voreinstellung dem Startbildschirm hinzu oder entfernt es.

Details bestätigen:

Zeigt die Daten einer Voreinstellung an. Sie können die Voreinstellung durch Auswahl von **Diese Einst. nutzen** laden.

---

## Editieren des Bedienfeld-Startbildschirms

Wählen Sie zum Anpassen des Startbildschirms **Einstellungen** > **Startbild bearbeiten** auf dem Bedienfeld des Scanners.

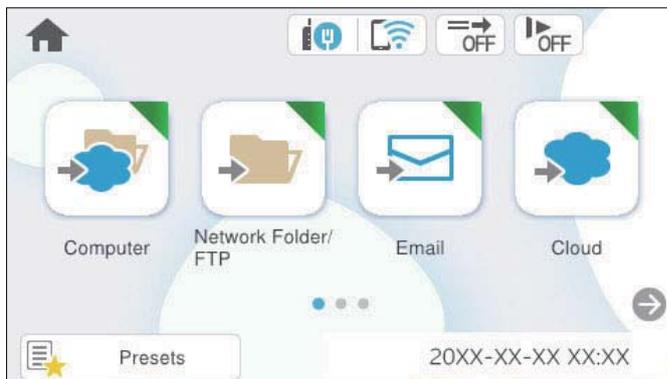
- Layout: Ändert die Anzeigemethode für Menusymbole.  
[„Ändern des Layout des Startbildschirms“ auf Seite 73](#)
- Symbol zufügen: Fügt den von Ihnen vorgenommenen **Voreinst.**-Einstellungen Symbole hinzu oder stellt vom Bildschirm entfernte Symbole wieder her.  
[„Symbol zufügen“ auf Seite 74](#)
- Symbol entfernen Entfernt Symbole vom Startbildschirm.  
[„Symbol entfernen“ auf Seite 75](#)
- Symbol verschieben: Ändert die Anzeigereihenfolge für Symbole.  
[„Symbol verschieben“ auf Seite 76](#)
- Standardsymbolanz. wiederherstellen: Stellt die Standard-Anzeigeeinstellungen für den Startbildschirm wieder her.

## Ändern des Layout des Startbildschirms

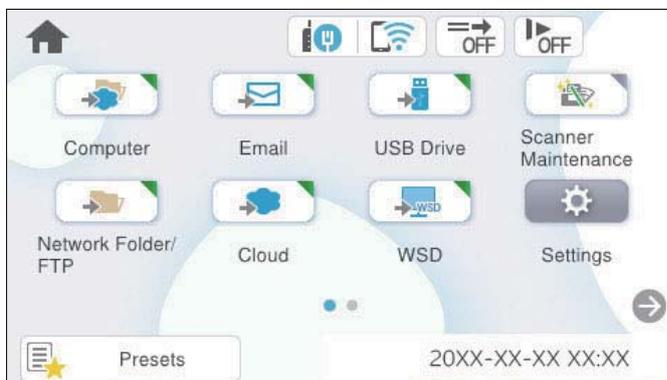
1. Wählen Sie **Einstellungen** > **Startbild bearbeiten** > **Layout** auf dem Scannerbedienfeld.

2. Wählen Sie **Zeile** oder **Matrix**.

**Zeile:**



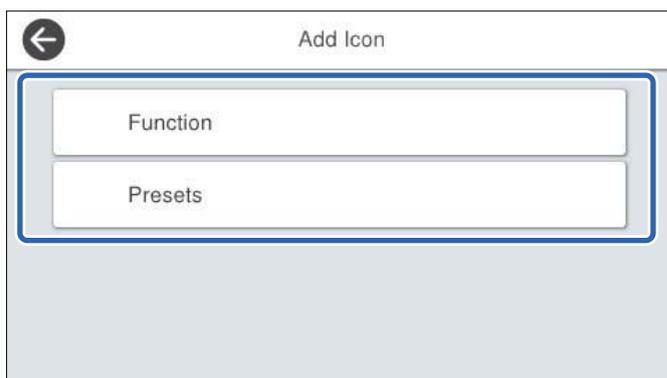
**Matrix:**



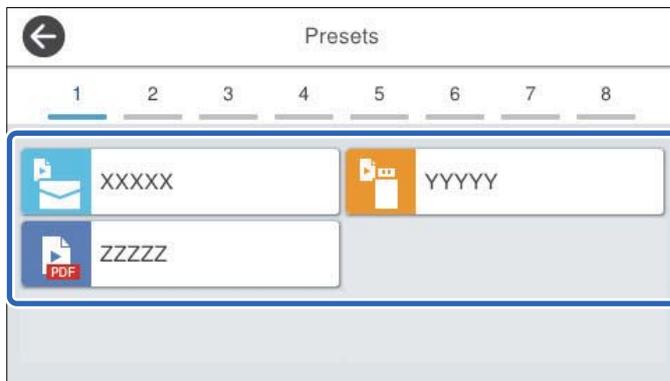
3. Wählen Sie , um zum Startbildschirm zurückzukehren und diesen zu kontrollieren.

## Symbol zufügen

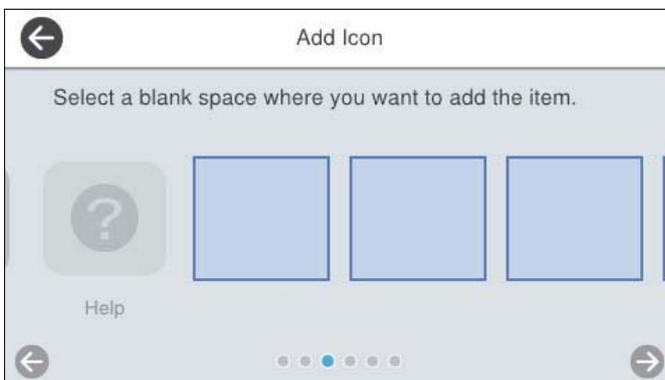
1. Wählen Sie **Einstellungen** > **Startbild bearbeiten** > **Symbol zufügen** auf dem Scannerbedienfeld.
2. Wählen Sie **Funktion** oder **Voreinst.**.
  - Funktion: Zeigt die auf dem Startbildschirm angezeigten Standardfunktionen an.
  - Voreinst.: Zeigt registrierte Voreinstellungen an.



3. Wählen Sie das Element aus, das Sie zur Startansicht hinzufügen möchten.



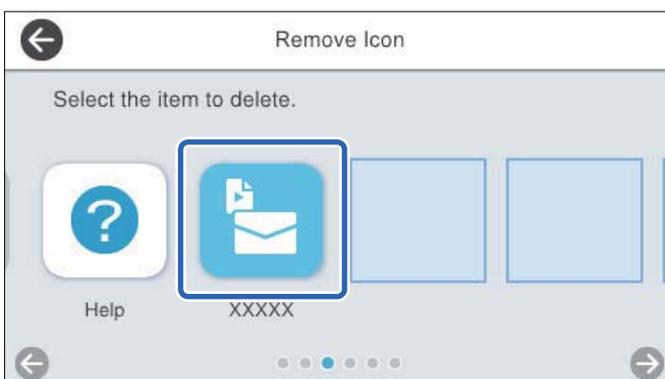
4. Wählen Sie den leeren Bereich aus, in dem Sie das Element hinzufügen möchten.  
Wenn Sie mehrere Symbole hinzufügen möchten, wiederholen Sie die Schritte 3 bis 4.



5. Wählen Sie , um zum Startbildschirm zurückzukehren und diesen zu kontrollieren.

## Symbol entfernen

1. Wählen Sie **Einstellungen** > **Startbild bearbeiten** > **Symbol entfernen** auf dem Scannerbedienfeld.
2. Wählen Sie das Symbol aus, das Sie entfernen möchten.



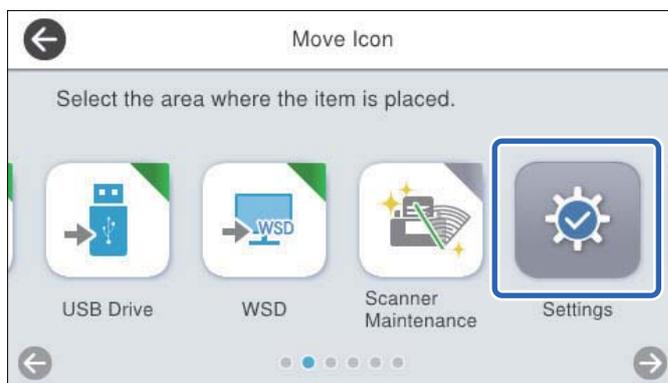
3. Wählen Sie zum Fertigstellen **Ja**.

Wenn Sie mehrere Symbole entfernen möchten, wiederholen Sie die Schritte 2 bis 3.

4. Wählen Sie , um zum Startbildschirm zurückzukehren und diesen zu kontrollieren.

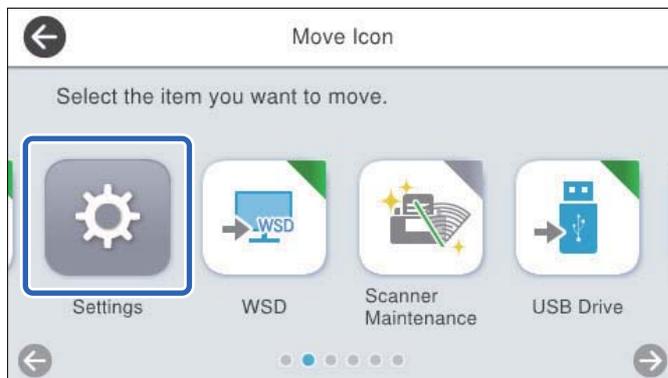
## Symbol verschieben

1. Wählen Sie **Einstellungen** > **Startbild bearbeiten** > **Symbol verschieben** auf dem Scannerbedienfeld.
2. Wählen Sie das Symbol aus, das Sie verschieben möchten.



3. Wählen Sie den Zielrahmen aus.

Wenn im Zielrahmen bereits ein anderes Symbol eingesetzt ist, wird dieses ersetzt.



4. Wählen Sie , um zum Startbildschirm zurückzukehren und diesen zu kontrollieren.

# Einfache Sicherheitseinstellungen

Einführung in die Sicherheitsfunktionen des Produkts. . . . .	78
Administratoreinstellungen. . . . .	78
Einschränken der Verfügbarkeit von Funktionen (Zugangssteuerung). . . . .	84
Deaktivieren der externen Schnittstelle. . . . .	86
Aktivieren der Programmüberprüfung beim Start. . . . .	87
Deaktivieren des Netzwerk-Scannens auf dem Computer. . . . .	87
Aktivieren oder Deaktivieren des WSD Scanners. . . . .	87
Überwachen eines Remote-Scanners. . . . .	88
Wiederherstellen der-StandardEinstellungen. . . . .	90
Epson Remote Services-Information. . . . .	90
Probleme lösen. . . . .	90

## Einführung in die Sicherheitsfunktionen des Produkts

Dieser Abschnitt beschreibt die Sicherheitsfunktionen der Epson-Geräte.

Name der Funktion	Funktionstyp	Einstellen	Vermeiden
Konfigurieren des Administratorkennworts	Sperrt die Systemeinstellungen, wie z. B. den Verbindungsaufbau für Netzwerk oder USB.	Ein Administrator legt ein Kennwort für das Gerät fest.  Eine Änderung ist sowohl über Web Config als auch über das Scannerbedienfeld möglich.	Verhindern Sie das unbefugte Lesen und Ändern der auf dem Gerät gespeicherten Informationen wie ID, Kennwort, Netzwerkeinstellungen usw. Verringern Sie zudem ein breites Spektrum von Sicherheitsrisiken, wie z. B. den Verlust von Daten über die Netzwerkkumgebung oder die Sicherheitsrichtlinie.
Zugangsteuerungseinstellungen	Wenn Sie sich mit einem zuvor registrierten Benutzerkonto anmelden, können Sie das Gerät nutzen.	Registrieren Sie ein Benutzerkonto.  Sie können bis zu 10 Benutzerkonten registrieren.	Die Einrichtung von Beschränkungen für Benutzer verhindert die unbefugte Nutzung des Geräts.
Einrichtung der externen Schnittstelle	Kontrolliert die Schnittstelle, die mit dem Gerät verbunden ist.	Aktivieren oder deaktivieren Sie die USB-Verbindung mit dem Computer.	USB-Anschluss des Computers: Verhindert die unbefugte Nutzung des Geräts, indem Scanvorgänge verhindert werden, sofern diese nicht über das Netzwerk erfolgen.

### Zugehörige Informationen

- ➔ [„Konfigurieren des Administratorkennworts“ auf Seite 78](#)
- ➔ [„Deaktivieren der externen Schnittstelle“ auf Seite 86](#)

## Administratoreinstellungen

### Konfigurieren des Administratorkennworts

Wenn Sie ein Administratorkennwort festlegen, verhindern Sie, dass die Benutzer die Einstellungen der Systemverwaltung ändern. Die Standardwerte werden zum Kaufzeitpunkt festgelegt. Ändern Sie es nach Bedarf.

#### **Hinweis:**

Im Folgenden finden Sie die Standardwerte der Administratorinformationen.

- Benutzername (nur Web Config): keiner (leer)*
- Kennwort: Auf dem Etikett des Produkts angegeben.*

*Wenn sich auf der Rückseite ein Etikett „PASSWORD“ befindet, geben Sie die achtstellige Zahl auf dem Etikett ein. Wenn kein Etikett „PASSWORD“ vorhanden ist, geben Sie die Seriennummer auf dem Etikett auf der Rückseite des Produkts als anfängliches Administratorkennwort ein.*

Sie können das Administratorkennwort entweder in Web Config, auf dem Scannerbedienfeld oder in Epson Device Admin ändern. Eine Anleitung oder Hilfestellung zur Verwendung von Epson Device Admin finden Sie in der Dokumentation zu Epson Device Admin.

## Ändern des Administratorkennworts mit Web Config

Ändern Sie das Administratorkennwort in Web Config.

1. Wechseln Sie zu Web Config und wählen Sie die Registerkarte **Produktsicherheit > Administratorkennwort ändern** aus.
2. Geben Sie die erforderlichen Informationen in **Aktuelles Kennwort**, **Benutzername**, **Neues Kennwort** und **Neues Kennwort bestätigen** ein.

Das neue Kennwort muss zwischen 8 und 20 Zeichen lang sein und darf nur alphanumerische Zeichen und Symbole im Ein-Byte-Format enthalten.

**Hinweis:**

*Im Folgenden finden Sie die Standardwerte der Administratorinformationen.*

*Benutzername: keiner (leer)*

*Kennwort: Auf dem Etikett des Produkts angegeben.*

*Wenn sich auf der Rückseite ein Etikett „PASSWORD“ befindet, geben Sie die achtstellige Zahl auf dem Etikett ein. Wenn kein Etikett „PASSWORD“ vorhanden ist, geben Sie die Seriennummer auf dem Etikett auf der Rückseite des Produkts als anfängliches Administratorkennwort ein.*



**Wichtig:**

*Bitte merken Sie sich das festgelegte Administratorkennwort. Falls Sie das Kennwort vergessen, können Sie es nicht zurücksetzen und müssen sich an das Service-Personal wenden.*

3. Wählen Sie **OK** aus.

### Zugehörige Informationen

➔ [„Ausführen von Web Config in einem Webbrowser“](#) auf Seite 40

## Ändern des Administratorkennworts auf dem Scannerbedienfeld

Sie können das Administratorkennwort auf dem Scannerbedienfeld ändern.

1. Wählen Sie **Einstellungen** auf dem Scannerbedienfeld aus.
2. Wählen Sie **Systemadministration > Admin-Einstellungen**.
3. Wählen Sie **Admin-Kennwort > Ändern**.
4. Geben Sie Ihr aktuelles Kennwort ein.

**Hinweis:**

*Das anfängliche Administratorkennwort (Standard) kann variieren, je nachdem, was auf dem Etikett auf des Produkts angegeben ist. Wenn sich auf der Rückseite ein Etikett „PASSWORD“ befindet, geben Sie die achtstellige Zahl auf dem Etikett ein. Wenn kein Etikett „PASSWORD“ vorhanden ist, geben Sie die Seriennummer auf dem Etikett auf der Rückseite des Produkts als anfängliches Administratorkennwort ein.*

5. Geben Sie Ihr neues Kennwort ein.

Das neue Kennwort muss zwischen 8 und 20 Zeichen lang sein und darf nur alphanumerische Zeichen und Symbole im Ein-Byte-Format enthalten.



**Wichtig:**

Bitte merken Sie sich das festgelegte Administratorkennwort. Falls Sie das Kennwort vergessen, können Sie es nicht zurücksetzen und müssen sich an das Service-Personal wenden.

6. Geben Sie das neue Kennwort zur Bestätigung erneut ein.

Eine Abschlussmeldung wird angezeigt.

## Verwenden der Sperreinstellung für das Bedienfeld

Mit der Option Sperreinstellung können Sie das Bedienfeld sperren, um zu verhindern, dass Benutzer Elemente im Zusammenhang mit den Systemeinstellungen ändern.

### Konfigurieren der Sperreinstellung über das Bedienfeld

1. Falls Sie die **Sperreinstellung** aufheben möchten, nachdem sie aktiviert wurde, tippen Sie oben rechts auf dem Startbildschirm auf , um sich als Administrator anzumelden.



wird nicht angezeigt, wenn **Sperreinstellung** deaktiviert ist. Falls Sie diese Einstellung aktivieren möchten, fahren Sie mit dem nächsten Schritt fort.

2. Wählen Sie **Einstellungen**.
3. Wählen Sie **Systemadministration > Admin-Einstellungen**.
4. Wählen Sie die Option **Ein** oder **Aus** als **Sperreinstellung**.

### Einstellen von Sperreinstellung über Web Config

1. Wählen Sie die Registerkarte **Geräteverwaltung > Bedienfeld**.
2. Wählen Sie **Ein** oder **Aus** als **Bedienfeldsperre**.
3. Klicken Sie auf **OK**.

#### Zugehörige Informationen

➔ „Ausführen von Web Config in einem Webbrowser“ auf Seite 40

### Optionen von Sperreinstellung im Menü Einstellungen

Dies ist eine Liste der Optionen, die im Menü **Einstellungen** des Bedienfelds durch Sperreinstellung gesperrt sind.

✓: Soll gesperrt werden.

- : Soll nicht gesperrt werden.

Menü Einstellungen		Sperreinstellung
Grundeinstellungen		-
	LCD-Helligkeit	-
	Töne	-
	Schlaf-Timer	✓
	Abschalttimer	✓
	Direkt Einschalten	✓
	Datum/Zeit-Einstellung	✓
	Sprache/Language	✓/-*
	Tastatur (Diese Funktion ist je nach Region bei Ihnen möglicherweise nicht verfügbar.)	-
	Betriebszeitüberschr.	✓
	PC-Verbindung via USB	✓
Scannereinst.		-
	Langsam	-
	Doppeleinzug-Stopptiming	✓
	DFDS-Funktion	-
	Papierschutz	✓
	Glasverschmutzungserkennung	✓
	Ultraschall-Doppeleinzugerk.	✓
	Zeitüberschreitung Automatischer Transportmodus	✓
	Empfänger bestätigen	✓
Startbild bearbeiten		✓
	Layout	✓
	Symbol zufügen	✓
	Symbol entfernen	✓
	Symbol verschieben	✓
	Standardsymbolanz. wiederherstellen	✓
Nutzereinstellungen		✓

Menü Einstellungen		Sperreinstellung
	Netz-ordner/FTP	✓
	eMail	✓
	Cloud	✓
	USB-Stick	✓
Netzwerkeinstellungen		✓
	Wi-Fi-Setup	✓
	LAN-Einrichtung	✓
	Netzwerkstatus	✓
	Erweitert	✓
Webdiensteinstellungen		✓
	Epson Connect-Services	✓
Document Capture Pro		-
	Einstellungen ändern	✓
Kontakte-Manager		-
	Registrieren/Löschen	✓/-*
	Regelmäßig	-
	Optionen anzeigen	-
	Suchoptionen	-
Systemadministration		✓
	Kontakte-Manager	✓
	Admin-Einstellungen	✓
	Beschränkungen	✓
	Zugangssteuerung	✓
	Kennwortverschlüsselung	✓
	Kundenforschung	✓
	WSD-Einstellungen	✓
	Werkseinstlg. wiederh.	✓
	Firmware-Aktualisierung	✓
Geräteinformationen		-

Menü Einstellungen		Sperreinstellung
	Seriennummer	–
	Aktuelle Version	–
	Gesamtanzahl Scans	–
	Anzahl 1-seitiger Scans	–
	Anzahl 2-seitiger Scans	–
	Anzahl Transporthülle-Scans	–
	Anz. Scans n. Walzenwechsel	–
	Anz. Scans nach Reg. Reinigung	–
	Status Authentifizierungsgerät	–
	Informationen zu Epson Open Platform	–
	 (Anzahl Scans rücksetzen)	✓
Wartung Scanner		–
	Walzenreinigung	–
	Walzenwechsel	–
	Anzahl Scans rücksetzen	✓
	Anleitung zu Auswechslung	–
	Reg. Reinigung	–
	Anzahl Scans rücksetzen	✓
	Reinig.-anleitung	–
	Glasreinigung	–
Walzenwechsel-Alarmeinrichtung		✓
	Zählalarmeinst.	✓
Alarmeinstellungen regelmäßige Reinigung		✓
	Alarmeinstellung Warnung	✓
	Zählalarmeinst.	✓

\* Sie können einstellen, ob Änderungen in **Systemadministration > Beschränkungen** erlaubt sein sollen oder nicht.

## Anmelden als Administrator am Bedienfeld

Wenn **Sperreinstellung** aktiviert ist, können Sie sich mit einer der folgenden Methoden auf dem Bedienfeld des Scanners anmelden.

1. Tippen Sie oben rechts am Bildschirm auf .

2. Wenn der Bildschirm **Benutzer wählen** angezeigt wird, wählen Sie **Administrator** aus.

3. Geben Sie das Kennwort ein, um sich anzumelden.

Es erscheint eine Meldung, dass die Anmeldung abgeschlossen ist, und dann wird der Startbildschirm auf dem Bedienfeld angezeigt.

Zum Abmelden tippen Sie auf  oben rechts auf dem Bildschirm oder drücken Sie die Schaltfläche .

---

## Einschränken der Verfügbarkeit von Funktionen (Zugangssteuerung)

Sie können Benutzer einschränken, indem Sie Benutzerkonten auf dem Scanner registrieren.

Wenn Zugangssteuerung aktiviert ist, kann der Benutzer die Scanfunktionen verwenden, nachdem er ein Kennwort auf dem Bedienfeld des Scanners eingegeben und sich angemeldet hat. Sie können nicht scannen, wenn Sie nicht angemeldet sind.

Sie können von einem Computer scannen, indem Sie Ihren Benutzernamen und Kennwort im Scannertreiber (Epson Scan 2) registrieren. Weitere Informationen zur Vornahme der Einstellungen finden Sie in der Hilfe von Epson Scan 2 oder im *Benutzerhandbuch* des Produkts.

### Erstellen des Benutzerkontos

Sie können ein Zugangssteuerung-Konto erstellen.

1. Rufen Sie Web Config auf und wählen Sie dann die Registerkarte **Produktsicherheit** > **Zugangssteuerungseinstellungen** > **Benutzereinstellungen** aus.

2. Klicken Sie auf **Hinzufügen** neben der zu registrierenden Nummer.



**Wichtig:**

*Wenn Sie den Scanner mit einem Authentifizierungssystem von Epson oder eines anderen Unternehmens verwenden, registrieren Sie den Benutzernamen in Zugangssteuerungseinstellungen in Steckplatznummer 2 bis 10.*

*Anwendungssoftware wie das Authentifizierungssystem verwendet den Steckplatz Nummer 1 und der Benutzernamen wird nicht auf dem Bedienfeld des Scanner angezeigt.*

3. Legen Sie jede Option fest.

Benutzername:

Geben Sie den in der Benutzernamenliste angezeigten Namen zwischen 1 und 14 Zeichen mit alphanumerischen Zeichen ein.

Kennwort:

Geben Sie ein Kennwort mit bis zu 20 Zeichen in ASCII (0x20–0x7E) ein. Wenn Sie das Kennwort initialisieren, lassen Sie es leer.

Wählen Sie das Kontrollkästchen zum De-/Aktivieren der jeweiligen Funktion.

Wählen Sie **Scan** aus, wenn Sie die Scanfunktionen erlauben möchten.

4. Klicken Sie auf **Übernehmen**.

## Bearbeiten des Benutzerkontos

Sie können das registrierte Zugangssteuerung-Konto bearbeiten.

1. Rufen Sie Web Config auf und wählen Sie dann die Registerkarte **Produktsicherheit** > **Zugangssteuerungseinstellungen** > **Benutzereinstellungen** aus.
2. Klicken Sie auf **Bearbeiten** neben der zu bearbeitenden Nummer.
3. Ändern Sie jede Option.
4. Klicken Sie auf **Übernehmen**.

## Löschen des Benutzerkontos

Sie können das registrierte Zugangssteuerung-Konto löschen.

1. Rufen Sie Web Config auf und wählen Sie dann die Registerkarte **Produktsicherheit** > **Zugangssteuerungseinstellungen** > **Benutzereinstellungen** aus.
2. Klicken Sie auf **Bearbeiten** neben der zu löschenden Nummer.
3. Klicken Sie auf **Löschen**.



**Wichtig:**

Wenn Sie auf **Löschen** klicken, wird das Benutzerkonto ohne Bestätigungsmeldung gelöscht. Vorsicht beim Löschen des Kontos.

## Aktivieren der Zugangssteuerung

Wenn Zugangssteuerung aktiviert wird, können nur registrierte Benutzer den Scanner verwenden.

**Hinweis:**

Wenn Zugangssteuerungseinstellungen aktiviert ist, müssen Sie die Benutzer über ihre Kontoinformationen benachrichtigen.

1. Rufen Sie Web Config auf und wählen Sie dann die Registerkarte **Produktsicherheit** > **Zugangssteuerungseinstellungen** > **Grundlegend** aus.
2. Wählen Sie **Aktiviert die Zugangssteuerung** aus.

Wenn Sie Zugangssteuerungseinstellungen aktivieren und von einem Computer scannen, der keine Authentifizierungsfunktionen hat, wählen Sie **Druck und Scan ohne Authentifizierungsinformationen von einem Computer erlauben** aus.

3. Klicken Sie auf **OK**.

## Anmelden bei einem Scanner, auf dem Zugangssteuerung aktiviert ist.

Wenn **Zugangssteuerung** aktiviert ist, können Sie sich mit einer der folgenden Methoden auf dem Bedienfeld des Scanners anmelden.

1. Tippen Sie oben rechts am Bildschirm auf .
2. Wenn der Bildschirm **Benutzer wählen** angezeigt wird, wählen Sie den Benutzer aus.
3. Geben Sie das Kennwort ein, um sich anzumelden.

Es erscheint eine Meldung, dass die Anmeldung abgeschlossen ist, und dann wird der Startbildschirm auf dem Bedienfeld angezeigt.

Zum Abmelden tippen Sie auf  oben rechts auf dem Bildschirm oder drücken Sie die Schaltfläche .

---

## Deaktivieren der externen Schnittstelle

Sie können die Schnittstelle deaktivieren, über die das Gerät mit dem Scanner verbunden wird. Nehmen Sie Einstellungen zur Beschränkung vor, um das Scannen auf andere Weise als über das Netzwerk einzuschränken.

### **Hinweis:**

Sie können die Einschränkungen auch über das Bedienfeld des Scanners vornehmen.

PC-Verbindung via USB: **Einstellungen > Grundeinstellungen > PC-Verbindung via USB**

1. Wechseln Sie zu Web Config und wählen Sie die Registerkarte **Produktsicherheit > Externe Schnittstelle**.

2. Wählen Sie **Deaktivieren** bei den Funktionen, die Sie einstellen möchten.

Wählen Sie **Aktivieren**, wenn Sie die Steuerung abbrechen möchten.

PC-Verbindung via USB

Sie können die Verwendung der USB-Verbindung vom Computer aus einschränken. Wählen Sie hierfür **Deaktivieren**.

3. Klicken Sie auf **OK**.

4. Versichern Sie sich, dass der deaktivierte Port nicht verwendet werden kann.

PC-Verbindung via USB

Der Treiber wurde auf dem Computer installiert

Schließen Sie den Scanner über ein USB-Kabel an den Computer an und bestätigen Sie dann, dass der Scanner nicht scannt.

Der Treiber wurde nicht auf dem Computer installiert

Windows:

Öffnen Sie den Geräte manager und lassen Sie ihn geöffnet. Schließen Sie dann den Scanner über ein USB-Kabel an den Computer an und überzeugen Sie sich, dass der Anzeigehalt des Geräte managers unverändert bleibt.

Mac OS:

Schließen Sie den Scanner mit einem USB-Kabel an den Computer an, und bestätigen Sie dann, dass Sie den Scanner nicht über **Drucker & Scanner** hinzufügen können.

### Zugehörige Informationen

➔ „Ausführen von Web Config in einem Webbrowser“ auf Seite 40

---

## Aktivieren der Programmüberprüfung beim Start

Wenn Sie die Funktion Programmüberprüfung aktivieren, führt der Scanner beim Start eine Überprüfung durch, um festzustellen, ob nicht autorisierte Dritte das Programm manipuliert haben. Wenn Probleme erkannt werden, startet der Scanner nicht.

**Hinweis:**

*Die Aktivierung dieser Funktion erhöht die Startzeit des Scanners.*

1. Rufen Sie Web Config auf und wählen Sie die Registerkarte **Produktsicherheit** > **Programmverifizierung beim Start** aus.

**Hinweis:**

*Sie können die Einstellungen auch auf dem Scannerbedienfeld vornehmen.*

**Einstellungen** > **Systemadministration** > **Programmverifizierung beim Start**

2. Wählen Sie **Ein** aus, um die **Programmverifizierung beim Start** zu aktivieren.
3. Klicken Sie auf **OK**.

---

## Deaktivieren des Netzwerk-Scannens auf dem Computer

Sie können das Netzwerk-Scannen in Web Config mithilfe von Epson Scan 2 auf dem Computer deaktivieren.

1. Rufen Sie Web Config auf und wählen Sie die Registerkarte **Scan** > **Netzwerkscan** aus.
2. Deaktivieren Sie in **Epson Scan 2** das Kontrollkästchen **Scannen aktivieren**.
3. Klicken Sie auf **Weiter**.  
Der Einstellungsbestätigungsbildschirm wird angezeigt.
4. Klicken Sie auf **OK**.

---

## Aktivieren oder Deaktivieren des WSD Scanners

**Hinweis:**

*Sie können die Einstellungen auch auf dem Scannerbedienfeld vornehmen. Wählen Sie **Einstellungen** > **Systemadministration** > **WSD-Einstellungen** aus.*

Sie können WSD-Scannen aktivieren oder deaktivieren.

Wenn der Computer den Scanner nicht als WSD-Scangerät konfigurieren soll, deaktivieren Sie die WSD-Einstellungen.

1. Rufen Sie Web Config auf und wählen Sie die Registerkarte **Netzwerksicherheit** > **Protokoll** aus.
2. Ändern Sie in **WSD-Einstellungen** das Kontrollkästchen **WSD aktivieren**.

3. Klicken Sie auf **Weiter**.

Der Einstellungsbestätigungsbildschirm wird angezeigt.

4. Klicken Sie auf **OK**.

**Hinweis:**

Wenn Ihr Computer den Scanner weiterhin als WSD-Scanner konfiguriert, wählen Sie die Registerkarte **Scan** > **Netzwerkscan** aus und deaktivieren Sie dann das Kontrollkästchen **Scannen aktivieren in AirPrint**.

Wenn AirPrint deaktiviert ist, ist auch das Scannen mit Mopria von Chromebooks, Windows und der App Mopria Scan aktiviert.

---

## Überwachen eines Remote-Scanners

### Überprüfen von Informationen für einen entfernten Scanner

Sie können die folgenden Informationen über den laufenden Scanner unter **Status** in Web Config überprüfen.

- Produktstatus

Überprüfen Sie Status, Cloud-Service, Produktnummer, MAC-Adresse, usw.

- Netzwerkstatus

Überprüfen Sie die Informationen über den Status der Netzwerkverbindung, die IP-Adresse, den DNS-Server usw.

- Nutzungsstatus

Überprüfen Sie den ersten Tag der Scans, die Anzahl der Scans, usw.

- Hardwarestatus

Überprüfen Sie den Status der einzelnen Scannerfunktionen.

- Panel-Schnappschuss

Zeigt einen Schnappschuss des auf dem Scannerbedienfeld angezeigten Bildschirms an.

## Empfang von E-Mail-Benachrichtigungen bei Ereignissen

### Infos zur E-Mail-Benachrichtigung

Mit dieser Funktion lassen sich bei Ereignissen wie abgeschlossenen Scanvorgängen oder Scannerfehlern E-Mail-Benachrichtigungen an die festgelegte Adresse senden.

Es können bis zu fünf Ziele festgelegt werden, für die individuelle Benachrichtigungseinstellungen gewählt werden können.

Um diese Funktion nutzen zu können, muss vor dem Einstellen der Benachrichtigungen der E-Mail-Server eingerichtet werden.

### Zugehörige Informationen

➔ [„Registrieren eines E-Mail-Servers“ auf Seite 47](#)

## Konfigurieren einer E-Mail-Benachrichtigung

Konfigurieren Sie E-Mail-Benachrichtigung in Web Config.

1. Wechseln Sie zu Web Config und wählen Sie die Registerkarte **Geräteverwaltung** > **eMail-Benachrichtigung**.

2. Legen Sie die Betreffzeile der E-Mail-Benachrichtigung fest.

Wählen Sie aus den beiden Pulldown-Menüs die im Betreff angezeigten Inhalte aus.

- Die ausgewählten Inhalte werden neben dem **Betreff** angezeigt.
- Der gleiche Inhalt kann nicht zugleich links und rechts eingestellt werden.
- Wenn die Anzahl der Zeichen in **Ort** 32 Bytes überschreitet, werden Zeichen nach dem 32. Byte nicht dargestellt.

3. Geben Sie die E-Mail-Adresse für den Versand der Benachrichtigungs-E-Mail ein.

Verwenden Sie A-Z a-z 0-9 ! # \$ % & ' \* + - . / = ? ^ \_ { | } ~ @, und geben Sie zwischen 1 und 255 Zeichen ein.

4. Wählen Sie die Sprache für die E-Mail-Benachrichtigungen aus.

5. Aktivieren Sie das Kontrollkästchen für das Ereignis, für das Sie eine Benachrichtigung erhalten möchten.

Die Anzahl der **Benachrichtigungseinstellungen** wird mit der Zielnummer der **eMail-Adresseinstellungen** verknüpft.

Beispiel:

Falls Sie eine Benachrichtigung an die E-Mail-Adresse senden möchten, die für Nr. 1 in **eMail-Adresseinstellungen** festgelegt wurde, wenn das Administrator Kennwort geändert wird, aktivieren Sie das Kontrollkästchen für Spalte **1** in der Zeile **Administrator Kennwort geändert**.

6. Klicken Sie auf **OK**.

Bestätigen Sie, dass eine E-Mail-Benachrichtigung gesendet wird, indem Sie ein Ereignis auslösen.

Beispiel: Das Administrator Kennwort wurde geändert.

### Zugehörige Informationen

➔ „Ausführen von Web Config in einem Webbrowser“ auf Seite 40

### Elemente für die E-Mail-Benachrichtigung

Optionen	Einstellungen und Erläuterung
Administrator Kennwort geändert	Benachrichtigung bei Änderung des Administrator Kennworts.
Scannerfehler	Benachrichtigung bei Auftreten eines Scannerfehlers.
Wi-Fi-Ausfall	Benachrichtigung bei Auftreten eines Fehlers im WLAN.

## Verwenden von Web Config zur Steuerung der Stromversorgung des Scanners

Auch wenn sich der Computer nicht in der Nähe des Scanners befindet, können Sie den Scanner mit Web Config ausschalten und starten.

1. Rufen Sie Web Config auf und wählen Sie die Registerkarte **Geräteverwaltung > Leistung** aus.
2. Wählen Sie **Abschalten** oder **Neu starten** aus.
3. Klicken Sie auf **Ausführen**.

---

## Wiederherstellen der-Standard Einstellungen

Sie können die Netzwerkeinstellungen oder andere auf dem Scanner gespeicherte Einstellungen auswählen, um sie als Standardwerte wiederherzustellen.

1. Rufen Sie Web Config auf und wählen Sie die Registerkarte **Geräteverwaltung > Werkseinstellungen wiederherstellen** aus.

**Hinweis:**

*Sie können die Einstellungen auch auf dem Scannerbedienfeld vornehmen.*

*Einstellungen > Systemadministration > Werkseinstlg. wiederh.*

2. Wählen Sie das Element aus, das Sie wiederherstellen möchten.
3. Klicken Sie auf **Ausführen**.  
Folgen Sie schließlich der Bildschirmanleitung.

---

## Epson Remote Services-Information

Epson Remote Services ist ein Dienst, der periodisch Scannerinformationen über das Internet sammelt. Auf diese Weise lässt sich vorhersagen, wann Verbrauchsmaterialien und Ersatzteile ersetzt oder nachgefüllt werden müssen, und etwaige Fehler oder Probleme können schnell behoben werden.

Weitere Informationen zum Epson Remote Services erhalten Sie von Ihrem Händler.

---

## Probleme lösen

### Das Administratorkennwort wurde vergessen

Bitte wenden Sie sich an das Service-Personal. Kontaktieren Sie Ihren Händler vor Ort.

**Hinweis:**

*Im Folgenden finden Sie die anfänglichen Werte für den Administrator Web Config.*

*Benutzername: keiner (leer)*

*Kennwort: Auf dem Etikett des Produkts angegeben.*

*Wenn sich auf der Rückseite ein Etikett „PASSWORD“ befindet, geben Sie die achtstellige Zahl auf dem Etikett ein.*

*Wenn kein Etikett „PASSWORD“ vorhanden ist, geben Sie die Seriennummer auf dem Etikett auf der Rückseite des Produkts als anfängliches Administratorkennwort ein.*

*Wenn Sie das Kennwort wiederherstellen, wird es auf den anfänglichen Wert zum Zeitpunkt des Kaufs zurückgesetzt.*

# Erweiterte Sicherheitseinstellungen

Sicherheitseinstellungen und Gefahrenvermeidung. . . . .	93
Steuern anhand von Protokollen. . . . .	94
Verwenden eines digitalen Zertifikats. . . . .	97
SSL/TLS-Kommunikation mit dem Scanner. . . . .	103
Verschlüsselte Kommunikation mit IPsec/IP-Filterung. . . . .	104
Verbinden des Scanners mit einem IEEE802.1X-Netzwerk. . . . .	116
Beheben von Problemen für erweiterte Sicherheit. . . . .	118

## Sicherheitseinstellungen und Gefahrenvermeidung

Wenn ein Scanner mit einem Netzwerk verbunden ist, können Sie von einem entfernten Ort aus darauf zugreifen. Zudem können mehrere Personen den Scanner gemeinsam nutzen, was positive Auswirkungen auf die Effizienz der Abläufe und den Komfort hat. Allerdings erhöht sich dadurch auch das Risiko von unbefugtem Zugriff, Missbrauch und Datenfälschung. Wenn Sie den Scanner in einer Umgebung nutzen, in der Sie auf das Internet zugreifen können, ist das Risiko sogar noch höher.

Bei Scannern, die über keinen Zugriffsschutz für externen Zugriff verfügen, können die im Scanner gespeicherten Druckauftragsprotokolle über das Internet abgerufen werden.

Um dieses Risiko zu vermeiden, sind Scanner von Epson mit einer Reihe von Sicherheitstechnologien ausgestattet.

Richten Sie den Scanner gemäß den Anforderungen der Betriebsumgebung ein, die anhand der Umgebungsinformationen des Kunden erstellt wurde.

Name	Merkmalstyp	Einstellen	Vermeiden
Protokollsteuerung	Steuert die Protokolle und Dienste für die Kommunikation zwischen Scannern und Computer und aktiviert und deaktiviert Funktionen.	Ein Protokoll oder Dienst, der auf Funktionen angewendet wird, die separat erlaubt oder verboten sind.	Reduziert Sicherheitsrisiken, die durch unbeabsichtigte Nutzung entstehen könnten, indem Benutzer daran gehindert werden, nicht benötigte Funktionen zu verwenden.
SSL/TLS-Kommunikation	Der Kommunikationsinhalt wird mit SSL/TLS-Kommunikation verschlüsselt, wenn vom Scanner aus auf den Epson-Server im Internet zugegriffen wird, z. B. bei der Kommunikation mit dem Computer über den Webbrowser mit Epson Connect und beim Aktualisieren der Firmware.	Stellen Sie ein CA-signiertes Zertifikat bereit, und importieren Sie es in den Scanner.	Durch die Identifizierung des Scanners mit dem CA-signierten Zertifikat werden Identitätsdiebstahl und unbefugter Zugriff verhindert. Zudem werden die SSL/TLS-Kommunikationsinhalte geschützt und das Offenlegen von Inhalten für Scandaten und Einrichtungsinformationen wird verhindert.
IPsec/IP-Filter	Sie können für Daten von einem bestimmten Client oder eines bestimmten Typs festlegen, die Verbindung zu trennen. Da IPsec die Daten auf Ebene von IP-Paketen (Verschlüsselung und Authentifizierung) schützt, können Sie sicher über ungesicherte Scanprotokolle kommunizieren.	Erstellen Sie eine Basisrichtlinie und eine individuelle Richtlinie, um den Client oder die Art von Daten festzulegen, die auf den Scanner zugreifen dürfen.	Schützen Sie den Scanner vor unbefugtem Zugriff sowie der Fälschung und Ausleitung von Kommunikationsdaten.
IEEE 802.1X	Erlaubt nur authentifizierten Benutzern, eine Verbindung zum Netzwerk herzustellen. Erlaubt nur einem berechtigten Benutzer, den Scanner zu verwenden.	Authentifizierungseinstellung für den RADIUS-Server (Authentifizierungsserver).	Schützen Sie den Scanner vor unbefugtem Zugriff und unberechtigter Nutzung.

### Zugehörige Informationen

- ➔ „Steuern anhand von Protokollen“ auf Seite 94
- ➔ „SSL/TLS-Kommunikation mit dem Scanner“ auf Seite 103
- ➔ „Verschlüsselte Kommunikation mit IPsec/IP-Filterung“ auf Seite 104
- ➔ „Verbinden des Scanners mit einem IEEE802.1X-Netzwerk“ auf Seite 116

## Sicherheitsfunktionseinstellungen

Bei Einstellung von IPsec/IP-Filterung oder IEEE802.1X sollten Sie über SSL/TLS auf Web Config zugreifen, um zur Reduzierung von Sicherheitsrisiken, wie Manipulation oder Abhörangriffen, Einstellungsinformationen zu kommunizieren.

Achten Sie darauf, vor Einstellung von IPsec/IP-Filterung oder IEEE802.1X das Administratorkennwort zu konfigurieren.

---

## Steuern anhand von Protokollen

Sie können mit einer Vielzahl von Pfaden und Protokollen scannen. Sie können auch das Netzwerk-Scannen von beliebig vielen Netzwerk-Computern verwenden.

Sie können unbeabsichtigte Sicherheitsrisiken verringern, indem Sie das Scannen von spezifischen Pfaden beschränken oder die verfügbaren Funktionen kontrollieren.

### Protokolle kontrollieren

Konfigurieren Sie die vom Scanner unterstützten Protokolleinstellungen.

1. Rufen Sie hierzu Web Config auf und öffnen Sie dann die Registerkarte **Netzwerksicherheit** tab > **Protokoll**.
2. Konfigurieren Sie die entsprechenden Elemente.
3. Klicken Sie auf **Weiter**.
4. Klicken Sie auf **OK**.

Die Einstellungen werden auf den Scanner angewendet.

### Zugehörige Informationen

- ➔ „Ausführen von Web Config in einem Webbrowser“ auf Seite 40

## Aktivierbare und Deaktivierbare Protokolle

Protokoll	Beschreibung
Bonjour-Einstellungen	Sie können festlegen, ob Bonjour verwendet wird. Bonjour dient zur Suche nach Geräten, zum Scannen und so weiter.

Protokoll	Beschreibung
SLP-Einstellungen	Sie können die Funktion SLP aktivieren oder deaktivieren. SLP wird für das Push-Scannen und zur Netzwerksuche in EpsonNet Config verwendet.
WSD-Einstellungen	Sie können die Funktion WSD aktivieren oder deaktivieren. Wenn dies aktiviert ist, können WSD-Geräte hinzugefügt werden, und es kann über den WSD-Anschluss gescannt werden.
LLTD-Einstellungen	Sie können die Funktion LLTD aktivieren oder deaktivieren. Falls dies aktiviert ist, erscheint ein Hinweis in der Windows-Netzwerkkarte.
LLMNR-Einstellungen	Sie können die Funktion LLMNR aktivieren oder deaktivieren. Wenn aktiviert, ist eine Namensauflösung ohne NetBIOS auch möglich ohne DNS.
SNMPv1/v2c-Einstellungen	Sie können festlegen, ob SNMPv1/v2c aktiviert sein soll oder nicht. Dies wird verwendet, um Geräte einzurichten, zu überwachen usw.
SNMPv3-Einstellungen	Sie können festlegen, ob SNMPv3 aktiviert sein soll oder nicht. Dies wird verwendet, um verschlüsselte Geräte und Monitoring usw. einzurichten.

## Protokoll-Einstellungen

### Bonjour-Einstellungen

Optionen	Einstellwert und Beschreibung
Bonjour nutzen	Wählen Sie diese Option, um über Bonjour nach Geräten zu suchen oder diese zu verwenden.
Bonjour-Name	Zeigt den Bonjour-Namen an.
Bonjour-Dienstname	Zeigt den Bonjour-Dienstnamen an.
Ort	Zeigt den Bonjour-Standortnamen an.
Wide-Area Bonjour	Stellen Sie ein, ob Sie Wide-Area Bonjour verwenden möchten.

### SLP-Einstellungen

Optionen	Einstellwert und Beschreibung
SLP aktivieren	Wählen Sie diese Option, um die SLP-Funktion zu aktivieren. Dies wird z. B. bei der Netzwerksuche in EpsonNet Config verwendet.

### WSD-Einstellungen

Optionen	Einstellwert und Beschreibung
WSD aktivieren	Wählen Sie diese Option, um das Hinzufügen von Geräten über WSD sowie das Scannen über den WSD-Port zu aktivieren.
Scanzeitüberschreitung (Sek.)	Geben Sie den Kommunikations-Timeout-Wert für das WSD-Scannen zwischen 3 und 3.600 Sekunden ein.

Optionen	Einstellwert und Beschreibung
Gerätename	Zeigt den WSD-Gerätenamen an.
Ort	Zeigt den WSD-Standortnamen an.

#### LLTD-Einstellungen

Optionen	Einstellwert und Beschreibung
LLTD aktivieren	Wählen Sie diese Option, um LLTD zu aktivieren. Der Scanner wird in der Windows-Netzwerkübersicht angezeigt.
Gerätename	Zeigt den LLTD-Gerätenamen an.

#### LLMNR-Einstellungen

Optionen	Einstellwert und Beschreibung
LLMNR aktivieren	Wählen Sie diese Option, um LLMNR zu aktivieren. Sie können die Namensauflösung ohne NetBIOS verwenden, auch wenn Sie DNS nicht verwenden können.

#### SNMPv1/v2c-Einstellungen

Optionen	Einstellwert und Beschreibung
SNMPv1/v2c aktivieren	Wählen Sie diese Option, um SNMPv1/v2c zu aktivieren.
Zugangsautorität	Legen Sie die Zugriffsrechte fest, wenn SNMPv1/v2c aktiviert ist. Wählen Sie <b>Nur Lesen</b> oder <b>Lesen/Schreiben</b> .
Community-Name (nur Lesen)	Geben Sie 0 bis 32 ASCII-Zeichen (0x20 bis 0x7E) ein.
Community-Name (Lesen/Schreiben)	Geben Sie 0 bis 32 ASCII-Zeichen (0x20 bis 0x7E) ein.

#### SNMPv3-Einstellungen

Optionen	Einstellwert und Beschreibung
SNMPv3 aktivieren	SNMPv3 ist aktiviert, wenn das Kontrollkästchen aktiviert ist.
Benutzername	Geben Sie zwischen 1 und 32 Zeichen mit 1 Byte Zeichen ein.
Authentifizierungseinstellungen	
Algorithmus	Wählen Sie einen Algorithmus für eine Authentifizierung für SNMPv3 aus.
Kennwort	Geben Sie das Passwort für eine Authentifizierung für SNMPv3 ein. Geben Sie zwischen 8 und 32 Zeichen in ASCII (0x20–0x7E) ein. Wenn Sie dies nicht angeben, lassen Sie es leer.
Kennwort bestätigen	Geben Sie das Passwort ein, das Sie zur Bestätigung konfiguriert haben.

Optionen		Einstellwert und Beschreibung
Verschlüsselungseinstellungen		
	Algorithmus	Wählen Sie einen Algorithmus für eine Verschlüsselung für SNMPv3 aus.
	Kennwort	Geben Sie das Passwort für eine Verschlüsselung für SNMPv3 ein. Geben Sie zwischen 8 und 32 Zeichen in ASCII (0x20–0x7E) ein. Wenn Sie dies nicht angeben, lassen Sie es leer.
	Kennwort bestätigen	Geben Sie das Passwort ein, das Sie zur Bestätigung konfiguriert haben.
Kontextname		Geben Sie innerhalb von 32 Zeichen oder weniger in Unicode (UTF-8) ein. Wenn Sie dies nicht angeben, lassen Sie es leer. Die Anzahl der eingebbaren Zeichen variiert je nach Sprache.

## Verwenden eines digitalen Zertifikats

### Über digitale Zertifizierung

CA-signiertes Zertifikat

Das ist ein von einer Zertifizierungsstelle (Certification Authority, CA) signiertes Zertifikat. Sie können es von einer Zertifizierungsstelle beziehen. Dieses Zertifikat bescheinigt, dass der Scanner für SSL/TLS-Kommunikation verwendet wird. So können Sie die Sicherheit der Datenkommunikation gewährleisten.

Wenn es für SSL/TLS-Kommunikation verwendet wird, wird es als Serverzertifikat verwendet.

Bei der Nutzung während der IPsec/IP-Filterung oder der IEEE 802.1X-Kommunikation wird es als Client-Zertifikat verwendet.

CA-Zertifikat

Das ist ein Zertifikat, das in der Kette des CA-signiertes Zertifikat steht. Es wird auch als Zwischen-CA-Zertifikat bezeichnet. Es wird vom Webbrowser verwendet, um beim Zugriff auf den Server der Gegenstelle oder Web Config den Pfad des Scannerzertifikats zu validieren.

Legen Sie für das CA-Zertifikat fest, wann der Pfad des Serverzertifikats, auf das vom Scanner aus zugegriffen wird, validiert werden soll. Legen Sie für den Scanner fest, dass der Pfad für das CA-signiertes Zertifikat für die SSL/TLS-Verbindung zertifiziert werden soll.

Sie können das CA-Zertifikat des Scanners von der Zertifizierungsstelle beziehen, die das CA-Zertifikat ausstellt.

Sie können das CA-Zertifikat, das zur Validierung des Servers der Gegenstelle verwendet wird, auch von der Zertifizierungsstelle beziehen, die das CA-signiertes Zertifikat des anderen Servers ausgestellt hat.

#### Selbstsigniertes Zertifikat

Das ist ein Zertifikat, das der Scanner selbst signiert und ausstellt. Es wird auch als Stammzertifikat bezeichnet. Da es vom Aussteller selbst signiert wird, ist es nicht zuverlässig und kann keinen Identitätsdiebstahl verhindern.

Verwenden Sie es, wenn Sie die Sicherheitseinstellung vornehmen und einfache SSL/TLS-Kommunikation ohne das CA-signiertes Zertifikat durchführen.

Wenn Sie dieses Zertifikat für eine SSL/TLS-Kommunikation einsetzen, wird möglicherweise eine Sicherheitswarnung im Webbrowser angezeigt, da das Zertifikat nicht bei einem Webbrowser registriert ist. Sie können das Selbstsigniertes Zertifikat nur für die SSL/TLS-Kommunikation einsetzen.

#### **Zugehörige Informationen**

- ➔ [„Konfigurieren eines CA-signiertes Zertifikat“ auf Seite 98](#)
- ➔ [„Aktualisieren eines selbstsignierten Zertifikats“ auf Seite 101](#)
- ➔ [„Konfigurieren eines CA-Zertifikat“ auf Seite 102](#)

## **Konfigurieren eines CA-signiertes Zertifikat**

### **Erhalten eines CA-signierten Zertifikats**

Um ein CA-signiertes Zertifikat zu erhalten, erstellen Sie einen Zertifikatsantrag (CSR, Certificate Signing Request) und senden ihn an die Zertifizierungsbehörde. Sie können einen CSR mit Web Config und einem Computer erstellen.

Führen Sie zur Erstellung eines CSR und zum Erhalten eines CA-signierten Zertifikats mit Web Config die folgenden Schritte aus. Wenn Sie einen CSR mit Web Config erstellen, erhält das Zertifikat das PEM/DER-Format.

1. Rufen Sie hierzu Web Config auf und öffnen Sie dann die Registerkarte **Netzwerksicherheit**. Wählen Sie als nächstes **SSL/TLS > Zertifikat** oder **IPsec/IP-Filterung > Client-Zertifikat** oder **IEEE802.1X > Client-Zertifikat**.

Ungeachtet Ihrer Auswahl können Sie dasselbe Zertifikat abrufen und gemeinsam nutzen.

2. Klicken Sie auf **Generieren** von **CSR**.

Eine Seite zur CSR-Erstellung wird angezeigt.

3. Geben Sie einen Wert für jedes Element ein.

**Hinweis:**

*Verfügbare Schlüssellänge und Abkürzungen variieren je nach Zertifizierungsbehörde. Erstellen Sie einen Antrag entsprechend den Regeln der jeweiligen Zertifizierungsbehörde.*

4. Klicken Sie auf **OK**.

Eine Abschlussmeldung wird angezeigt.

5. Wählen Sie die Registerkarte **Netzwerksicherheit**. Wählen Sie als nächstes **SSL/TLS > Zertifikat** oder **IPsec/IP-Filterung > Client-Zertifikat** oder **IEEE802.1X > Client-Zertifikat** aus.

- Klicken Sie entsprechend dem Ausstellungsformat der jeweiligen Zertifizierungsbehörde auf eine der **CSR-Download-Schaltflächen**, um einen CSR auf einen Computer herunterzuladen.



**Wichtig:**

*Generieren einen CSR nicht erneut. Andernfalls können Sie ein ausgestelltes CA-signiertes Zertifikat möglicherweise nicht importieren.*

- Senden Sie den CSR an eine Zertifizierungsbehörde und beziehen Sie ein CA-signiertes Zertifikat. Folgen Sie für Sendemethode und -form den Regeln der jeweiligen Zertifizierungsbehörde.
- Speichern Sie das ausgestellte CA-signiertes Zertifikat auf einem mit dem Scanner verbundenen Computer. Der Bezug eines CA-signiertes Zertifikat ist abgeschlossen, wenn Sie das Zertifikat auf einem Ziel speichern.

**Zugehörige Informationen**

➔ [„Ausführen von Web Config in einem Webbrowser“ auf Seite 40](#)

**CSR-Einstellungen**

Optionen	Einstellungen und Erläuterung
Schlüssellänge	Wählen Sie eine Schlüssellänge für CSR.
Allgemeiner Name	Sie können zwischen 1 und 128 Zeichen eingeben. Falls dies eine IP-Adresse ist, sollte es eine statische IP-Adresse sein. Sie können 1 bis 5 IPv4-Adressen, IPv6-Adressen, Hostnamen, FQDNs eingeben, indem Sie sie durch Kommas trennen.  Das erste Element wird unter dem Common Name und andere Elemente unter dem Alias-Feld des Zertifikatsbetriffs gespeichert.  Beispiel:  IP-Adresse des Scanners: 192.0.2.123, Scannername: EPSONA1B2C3  Allgemeiner Name: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
Organisation/ Organisationseinheit/ Ort/ Staat/Bundesland	Sie können zwischen 0 und 64 Zeichen in ASCII (0x20–0x7E) eingeben. Sie können unterschiedene Namen durch Kommas trennen.
Land	Geben Sie einen zweistelligen Ländercode nach ISO-3166 ein.
Absender-eMail-Adresse	Sie können die E-Mail-Adresse des Absenders als Mailserver-Einstellung eingeben. Geben Sie dieselbe E-Mail-Adresse ein wie <b>Absender-eMail-Adresse</b> auf der Registerkarte <b>Netzwerk</b> > <b>eMail-Server</b> > <b>Grundlegend</b> .

**Importieren eines CA-signierten Zertifikats**

Importieren Sie das bezogene CA-signiertes Zertifikat auf dem Scanner.



**Wichtig:**

- Achten Sie darauf, dass Datum und Uhrzeit des Scanners richtig eingestellt sind. Das Zertifikat könnte ungültig sein.
- Wenn Sie ein Zertifikat beziehen, das mit einem in Web Config erstellten CSR beantragt worden ist, können Sie ein Zertifikat einmal importieren.

1. Rufen Sie Web Config auf, und wählen Sie dann die Registerkarte **Netzwerksicherheit**. Wählen Sie als nächstes **SSL/TLS > Zertifikat** oder **IPsec/IP-Filterung > Client-Zertifikat** oder **IEEE802.1X > Client-Zertifikat** aus.

2. Klicken Sie auf **Importieren**

Die Seite für den Import des Zertifikats wird geöffnet.

3. Geben Sie einen Wert für jedes Element ein. Legen Sie **CA-Zertifikat 1** und **CA-Zertifikat 2** fest, wenn Sie den Pfad des Zertifikats in dem Webbrowser verifizieren, der auf den Scanner zugreift.

Je nachdem, wo Sie einen CSR erstellt haben und welches Dateiformat das Zertifikat hat, können sich die erforderlichen Einstellungen unterscheiden. Geben Sie wie folgt Werte für erforderliche Optionen ein.

- Ein Zertifikat im PEM/DER-Format erhalten von Web Config
  - Privater Schlüssel:** Nicht konfigurieren, da der Scanner einen privaten Schlüssel enthält.
  - Kennwort:** Nicht konfigurieren.
  - CA-Zertifikat 1/CA-Zertifikat 2:** Optional

- Ein Zertifikat im PEM/DER-Format erhalten von einem Computer
  - Privater Schlüssel:** Muss eingestellt werden.
  - Kennwort:** Nicht konfigurieren.
  - CA-Zertifikat 1/CA-Zertifikat 2:** Optional

- Ein Zertifikat im PKCS#12-Format erhalten von einem Computer
  - Privater Schlüssel:** Nicht konfigurieren.
  - Kennwort:** Optional
  - CA-Zertifikat 1/CA-Zertifikat 2:** Nicht konfigurieren.

4. Klicken Sie auf **OK**.

Eine Abschlussmeldung wird angezeigt.

**Hinweis:**

Klicken Sie auf **Bestätigen**, um die Zertifikatsinformationen zu verifizieren.

**Zugehörige Informationen**

➔ „Ausführen von Web Config in einem Webbrowser“ auf Seite 40

### Einstellungen für den Import von CA-signierten Zertifikaten

Optionen	Einstellungen und Erläuterung
Serverzertifikat oder Client-Zertifikat	Wählen Sie ein Zertifikatformat aus. Für SSL/TLS-Verbindungen wird Serverzertifikat angezeigt. Für IPsec/IP-Filterung oder IEEE 802.1X wird Client-Zertifikat angezeigt.
Privater Schlüssel	Falls Sie ein Zertifikat im PEM/DER-Format unter Verwendung eines von einem Computer erstellten CSR erhalten, geben Sie eine private Schlüsseldatei an, die einem Zertifikat entspricht.
Kennwort	Wenn das Dateiformat <b>Zertifikat mit privatem Schlüssel (PKCS#12)</b> lautet, geben Sie das Kennwort zur Verschlüsselung des privaten Schlüssels ein, das beim Erhalt des Zertifikats festgelegt wird.
CA-Zertifikat 1	Wenn das Format Ihres Zertifikats <b>Zertifikat (PEM/DER)</b> ist, importieren Sie ein Zertifikat einer Zertifizierungsstelle, die ein CA-signiertes Zertifikat ausstellt, das als Serverzertifikat verwendet wird. Geben Sie falls erforderlich eine Datei an.
CA-Zertifikat 2	Wenn das Format Ihres Zertifikats <b>Zertifikat (PEM/DER)</b> ist, importieren Sie ein Zertifikat einer Zertifizierungsstelle, die ein CA-Zertifikat 1 ausstellt. Geben Sie falls erforderlich eine Datei an.

### Löschen eines CA-signierten Zertifikats

Sie können ein importiertes Zertifikat löschen, wenn es abgelaufen ist oder eine verschlüsselte Verbindung nicht mehr erforderlich ist.



**Wichtig:**

Wenn Sie ein Zertifikat beziehen, das mit einem in Web Config erstellten CSR beantragt worden ist, können Sie ein gelöscht Zertifikat nicht noch einmal importieren. Erstellen Sie in diesem Fall einen CSR und beziehen Sie das Zertifikat erneut.

1. Rufen Sie Web Config auf und öffnen Sie die Registerkarte **Netzwerksicherheit**. Wählen Sie als nächstes **SSL/TLS > Zertifikat** oder **IPsec/IP-Filterung > Client-Zertifikat** oder **IEEE802.1X > Client-Zertifikat**.
2. Klicken Sie auf **Löschen**.
3. Bestätigen Sie, dass Sie das in der Meldung angezeigte Zertifikat löschen möchten.

#### Zugehörige Informationen

➔ „Ausführen von Web Config in einem Webbrowser“ auf Seite 40

### Aktualisieren eines selbstsignierten Zertifikats

Da das Selbstsigniertes Zertifikat vom Scanner selbst ausgestellt wird, kann es nach Ablauf oder bei Änderung der Inhaltsbeschreibung aktualisiert werden.

1. Rufen Sie hierzu Web Config auf und öffnen Sie dann die Registerkarte **Netzwerksicherheit** tab > **SSL/TLS > Zertifikat**.

2. Klicken Sie auf **Aktualisieren**.

3. Geben Sie **Allgemeiner Name** ein.

Es können jeweils durch Kommas getrennt bis zu 5 IPv4-Adressen, IPv6-Adressen, Hostnamen, FQDNs zwischen 1 und 128 Zeichen eingegeben werden. Der erste Parameter wird im Common Name gespeichert, die anderen werden im Aliasfeld als Betreff des Zertifikats gespeichert.

Beispiel:

IP-Adresse des Scanners: 192.0.2.123, Scannernamen: EPSONA1B2C3

Gemeinsamer Name: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123

4. Geben Sie eine Gültigkeitsdauer für das Zertifikat ein.

5. Klicken Sie auf **Weiter**.

Eine Bestätigungsmeldung wird angezeigt.

6. Klicken Sie auf **OK**.

Der Scanner ist aktualisiert.

**Hinweis:**

Die Zertifikatsdaten lassen sich auf der Registerkarte **Netzwerksicherheit** > **SSL/TLS** > **Zertifikat** > **Selbstsigniertes Zertifikat** überprüfen. Klicken Sie anschließend auf **Bestätigen**.

### Zugehörige Informationen

➔ [„Ausführen von Web Config in einem Webbrowser“](#) auf Seite 40

## Konfigurieren eines CA-Zertifikat

Beim Festlegen eines CA-Zertifikat, können Sie den Pfad zum CA-Zertifikat des Servers, auf den der Scanner zugreift, überprüfen. Dies kann den Zugriff auf einen gefälschten Server verhindern.

Sie können das CA-Zertifikat bei der Zertifizierungsstelle erhalten, bei der das CA-signiertes Zertifikat ausgestellt wird.

## Importieren eines CA-Zertifikat

Importiert das CA-Zertifikat in den Scanner.

1. Rufen Sie Web Config auf, und wählen Sie dann die Registerkarte **Netzwerksicherheit** > **CA-Zertifikat**.

2. Klicken Sie auf **Importieren**.

3. Geben Sie das CA-Zertifikat an, das Sie importieren möchten.

4. Klicken Sie auf **OK**.

Wenn der Import abgeschlossen ist, kehren Sie zum Bildschirm **CA-Zertifikat** zurück, und das importierte CA-Zertifikat wird angezeigt.

### Zugehörige Informationen

➔ „Ausführen von Web Config in einem Webbrowser“ auf Seite 40

## Löschen eines CA-Zertifikat

Sie können das importierte CA-Zertifikat löschen.

1. Rufen Sie Web Config auf, und wählen Sie dann die Registerkarte **Netzwerksicherheit** > **CA-Zertifikat**.
2. Klicken Sie auf **Löschen** neben dem zu löschenden CA-Zertifikat.
3. Bestätigen Sie, dass Sie das Zertifikat in der angezeigten Meldung löschen möchten.
4. Klicken Sie auf **Netzwerk neu starten** und vergewissern Sie sich, dass das gelöschte CA-Zertifikat auf dem aktualisierten Bildschirm nicht aufgeführt ist.

### Zugehörige Informationen

➔ „Ausführen von Web Config in einem Webbrowser“ auf Seite 40

---

## SSL/TLS-Kommunikation mit dem Scanner

Wenn das Server-Zertifikat für die Kommunikation mit dem Scanner mit SSL/TLS (Secure Sockets Layer/Transport Layer Security) verwendet wird, lässt sich der Kommunikationsweg zwischen Computern verschlüsseln. Verwenden Sie diese Funktion, um einen insbesondere unbefugten Fernzugriff zu verhindern.

## Konfigurieren grundlegender SSL/TLS-Einstellungen

Wenn der Scanner die HTTPS-Serverfunktion unterstützt, können Sie eine SSL/TLS-Kommunikation zur Verschlüsselung der Kommunikation verwenden. Sie können den Scanner über Web Config konfigurieren und verwalten und gleichzeitig die Sicherheit gewährleisten.

Konfigurieren Sie die Verschlüsselungsstärke und die Umleitungsfunktion.

1. Wechseln Sie zu Web Config und wählen Sie die Registerkarte **Netzwerksicherheit** > **SSL/TLS** > **Grundlegend**.
2. Wählen Sie einen Wert für jedes Element.
  - Verschlüsselungsstärke  
Wählen Sie das Verschlüsselungsniveau.
  - HTTP auf HTTPS umleiten  
Umleitung auf HTTPS bei Zugriff auf HTTP.
3. Klicken Sie auf **Weiter**.  
Eine Bestätigungsmeldung wird angezeigt.
4. Klicken Sie auf **OK**.  
Der Scanner ist aktualisiert.

### Zugehörige Informationen

➔ „Ausführen von Web Config in einem Webbrowser“ auf Seite 40

## Konfiguration eines Serverzertifikats für den Scanner

1. Wechseln Sie zu Web Config und wählen Sie die Registerkarte **Netzwerksicherheit** > **SSL/TLS** > **Zertifikat**.
2. Legen Sie ein Serverzertifikat zur Verwendung als **Serverzertifikat** fest.
  - Selbstsigniertes Zertifikat  
Vom Scanner wurde ein selbstsigniertes Zertifikat erzeugt. Falls Sie kein CA-signiertes Zertifikat erhalten haben, wählen Sie das selbstsignierte aus.
  - CA-signiertes Zertifikat  
Falls Sie jedoch ein CA-signiertes Zertifikat im Voraus bezogen und importiert haben, können Sie auch dieses auswählen.
3. Klicken Sie auf **Weiter**.  
Eine Bestätigungsmeldung wird angezeigt.
4. Klicken Sie auf **OK**.  
Der Scanner ist aktualisiert.

### Zugehörige Informationen

➔ „Ausführen von Web Config in einem Webbrowser“ auf Seite 40

➔ „Konfigurieren eines CA-signiertes Zertifikat“ auf Seite 98

➔ „Konfigurieren eines CA-Zertifikat“ auf Seite 102

---

## Verschlüsselte Kommunikation mit IPsec/IP-Filterung

### Über IPsec/IP-Filterung

Der Datenverkehr lässt sich mithilfe der Funktion IPsec/IP-Filterung nach IP-Adressen, Diensten oder Ports filtern. Durch Filterkombinationen können Sie den Scanner so konfigurieren, dass bestimmte Clients oder Daten blockiert oder zugelassen werden. Darüber hinaus können Sie die Sicherheitsstufe durch Verwenden einer IPsec noch weiter erhöhen.

**Hinweis:**

*Computer mit Windows Vista oder späteren Versionen oder Windows Server 2008 oder späteren Versionen unterstützen IPsec.*

### Konfigurieren der Standardrichtlinie

Konfigurieren Sie die Standardrichtlinie, um Datenverkehr zu filtern. Die Standardrichtlinie gilt für jeden Benutzer oder jede Gruppe, die eine Verbindung mit dem Scanner herstellt. Für eine detaillierte Kontrolle von Benutzern oder Benutzergruppen konfigurieren Sie Gruppenrichtlinien.

1. Rufen Sie hierzu Web Config auf und öffnen Sie dann die Registerkarte **Netzwerksicherheit > IPsec/IP-Filterung > Grundlegend**.
2. Geben Sie einen Wert für jedes Element ein.
3. Klicken Sie auf **Weiter**.  
Eine Bestätigungsmeldung wird angezeigt.
4. Klicken Sie auf **OK**.  
Der Scanner ist aktualisiert.

### Zugehörige Informationen

➔ [„Ausführen von Web Config in einem Webbrowser“](#) auf Seite 40

## Einstellungselemente für Standardrichtlinie

### Standardrichtlinie

Optionen	Einstellungen und Erläuterung
IPsec/IP-Filterung	Sie können eine IPsec/IP-Filterfunktion aktivieren oder deaktivieren.

### Zugangssteuerung

Konfigurieren Sie eine Kontrollmethode für den Verkehr von IP-Paketen.

Optionen	Einstellungen und Erläuterung
Zugang erlauben	Wählen Sie diesen Punkt, um konfigurierte IP-Pakete zuzulassen.
Zugang verweigern	Wählen Sie diesen Punkt, um konfigurierte IP-Pakete zu sperren.
IPsec	Wählen Sie diesen Punkt, um konfigurierte IPsec-Pakete zuzulassen.

**IKE-Version**

Wählen Sie **IKEv1** oder **IKEv2** als **IKE-Version**. Wählen Sie eine der beiden Optionen anhand des Geräts aus, an das der Scanner angeschlossen ist.

**IKEv1**

Die folgenden Elemente werden angezeigt, wenn Sie **IKEv1** als **IKE-Version** auswählen.

Optionen	Einstellungen und Erläuterung
Authentisierungsmethode	Um <b>Zertifikat</b> wählen zu können, müssen Sie vorher ein CA-signiertes Zertifikat erhalten und importieren.
Vorinstallierter Schlüssel	Falls <b>Vorinstallierter Schlüssel</b> für <b>Authentisierungsmethode</b> ausgewählt wird, geben Sie einen PSA-Schlüssel zwischen 1 und 127 Zeichen ein.
Vorinstallierter Schlüssel bestätigen	Geben Sie zur Bestätigung den konfigurierten Schlüssel ein.

**IKEv2**

Die folgenden Elemente werden angezeigt, wenn Sie **IKEv2** als **IKE-Version** auswählen.

Optionen	Einstellungen und Erläuterung	
Lokal	Authentisierungsmethode	Um <b>Zertifikat</b> wählen zu können, müssen Sie vorher ein CA-signiertes Zertifikat erhalten und importieren.
	ID-Typ	Bei Auswahl von <b>Vorinstallierter Schlüssel</b> für <b>Authentisierungsmethode</b> , wählen Sie den ID-Typ für den Scanner aus.
	ID	Geben Sie die ID des Scanners ein, die dem ID-Typ entspricht. Die Zeichen „@“, „#“ und „=“ dürfen nicht als erstes Zeichen vorkommen. <b>Eindeutiger Name:</b> Geben Sie 1 bis 255 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein. Das Zeichen „=“ muss enthalten sein. <b>IP-Adresse:</b> Geben Sie diese im IPv4 oder IPv6-Format ein. <b>FQDN:</b> Geben Sie eine Kombination aus 1 bis 255 Zeichen ein: A–Z, a–z, 0–9, „-“ und Punkt „.“. <b>eMail-Adresse:</b> Geben Sie 1 bis 255 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein. Das Zeichen „@“ muss enthalten sein. <b>Schlüssel-ID:</b> Geben Sie 1 bis 255 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein.
	Vorinstallierter Schlüssel	Falls <b>Vorinstallierter Schlüssel</b> für <b>Authentisierungsmethode</b> ausgewählt wird, geben Sie einen PSA-Schlüssel zwischen 1 und 127 Zeichen ein.
	Vorinstallierter Schlüssel bestätigen	Geben Sie zur Bestätigung den konfigurierten Schlüssel ein.

Optionen		Einstellungen und Erläuterung
Extern	Authentisierungsmethode	Um <b>Zertifikat</b> wählen zu können, müssen Sie vorher ein CA-signiertes Zertifikat erhalten und importieren.
	ID-Typ	Falls Sie <b>Vorinstallierter Schlüssel</b> für <b>Authentisierungsmethode</b> auswählen, wählen Sie den ID-Typ des Geräts aus, das Sie authentifizieren möchten.
	ID	Geben Sie die ID des Scanners ein, die dem ID-Typ entspricht. Die Zeichen „@“, „#“ und „=“ dürfen nicht als erstes Zeichen vorkommen. <b>Eindeutiger Name:</b> Geben Sie 1 bis 255 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein. Das Zeichen „=“ muss enthalten sein. <b>IP-Adresse:</b> Geben Sie diese im IPv4 oder IPv6-Format ein. <b>FQDN:</b> Geben Sie eine Kombination aus 1 bis 255 Zeichen ein: A–Z, a–z, 0–9, „-“ und Punkt „.“. <b>eMail-Adresse:</b> Geben Sie 1 bis 255 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein. Das Zeichen „@“ muss enthalten sein. <b>Schlüssel-ID:</b> Geben Sie 1 bis 255 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein.
	Vorinstallierter Schlüssel	Falls <b>Vorinstallierter Schlüssel</b> für <b>Authentisierungsmethode</b> ausgewählt wird, geben Sie einen PSA-Schlüssel zwischen 1 und 127 Zeichen ein.
	Vorinstallierter Schlüssel bestätigen	Geben Sie zur Bestätigung den konfigurierten Schlüssel ein.

**Kapselung**

Wenn Sie **IPsec** für **Zugangssteuerung** wählen, müssen Sie einen Encapsulation-Modus konfigurieren.

Optionen	Einstellungen und Erläuterung
Transportmodus	Falls Sie den Scanner nur im selben LAN verwenden, wählen Sie diese Option. IP-Pakete der Schicht 4 oder höher werden verschlüsselt.
Tunnelmodus	Falls Sie den Scanner über ein internetfähiges Netzwerk wie IPsec-VPN verwenden, wählen Sie diese Option aus. Header und Daten der IP-Pakete werden verschlüsselt. <b>Remote-Gateway-Adresse:</b> Falls Sie <b>Tunnelmodus</b> als <b>Kapselung</b> ausgewählt haben, geben Sie eine Gateway-Adresse zwischen 1 und 39 Zeichen ein.

**Sicherheitsprotokoll**

Wenn Sie **IPsec** für **Zugangssteuerung** wählen, wählen Sie eine Option.

Optionen	Einstellungen und Erläuterung
ESP	Wählen Sie diese Option, um die Integrität einer Authentifizierung und der Daten sicherzustellen und die Daten zu verschlüsseln.
AH	Wählen Sie diese Option, um die Integrität einer Authentifizierung und der Daten sicherzustellen. Selbst wenn die Verschlüsselung von Daten nicht erlaubt ist, können Sie IPsec verwenden.

**❑ Algorithmeinstellungen**

Es wird empfohlen, dass Sie für alle Einstellungen **Beliebig** auswählen, oder für jeden Punkt eine Einstellung außer **Beliebig** auswählen. Falls **Beliebig** für einige Einstellungen ausgewählt wird, und eine andere Option als **Beliebig** für eine andere Einstellung, kommuniziert das Gerät möglicherweise je nach dem Gerät, das authentifiziert werden soll, nicht.

Optionen		Einstellungen und Erläuterung
IKE	Verschlüsselung	Wählen Sie den Verschlüsselungsalgorithmus für IKE aus. Die Punkte hängen von der verwendeten IKE-Version ab.
	Authentifizierung	Wählen Sie den Authentifizierungsalgorithmus für IKE aus.
	Schlüsselaustausch	Wählen Sie den Algorithmus zum Schlüsseltausch für IKE aus. Die Punkte hängen von der verwendeten IKE-Version ab.
ESP	Verschlüsselung	Wählen Sie den Verschlüsselungsalgorithmus für ESP aus. Diese Option ist verfügbar, wenn <b>ESP</b> für <b>Sicherheitsprotokoll</b> ausgewählt ist.
	Authentifizierung	Wählen Sie den Authentifizierungsalgorithmus für ESP aus. Diese Option ist verfügbar, wenn <b>ESP</b> für <b>Sicherheitsprotokoll</b> ausgewählt ist.
AH	Authentifizierung	Wählen Sie den Verschlüsselungsalgorithmus für AH aus. Diese Option ist verfügbar, wenn <b>AH</b> für <b>Sicherheitsprotokoll</b> ausgewählt ist.

## Konfigurieren der Gruppenrichtlinie

Eine Gruppenrichtlinie vereint eine oder mehrere Regeln, die auf einen Benutzer oder eine Benutzergruppe angewendet werden. Der Scanner kontrolliert IP-Pakete, die auf konfigurierte Richtlinien passen. IP-Pakete werden in der Reihenfolge nach entsprechend der Gruppenrichtlinie 1 bis 10 und dann der Standardrichtlinie authentifiziert.

1. Rufen Sie hierzu Web Config auf und öffnen Sie dann die Registerkarte **Netzwerksicherheit > IPsec/IP-Filterung > Grundlegend**.
2. Klicken Sie auf ein nummeriertes Register, um es zu konfigurieren.
3. Geben Sie einen Wert für jedes Element ein.
4. Klicken Sie auf **Weiter**.  
Eine Bestätigungsmeldung wird angezeigt.
5. Klicken Sie auf **OK**.  
Der Scanner ist aktualisiert.

## Einstellungselemente für Gruppenrichtlinie

Optionen	Einstellungen und Erläuterung
Diese Gruppenrichtlinie aktivieren	Sie können eine Gruppenrichtlinie aktivieren oder deaktivieren.

### Zugangssteuerung

Konfigurieren Sie eine Kontrollmethode für den Verkehr von IP-Paketen.

Optionen	Einstellungen und Erläuterung
Zugang erlauben	Wählen Sie diesen Punkt, um konfigurierte IP-Pakete zuzulassen.
Zugang verweigern	Wählen Sie diesen Punkt, um konfigurierte IP-Pakete zu sperren.
IPsec	Wählen Sie diesen Punkt, um konfigurierte IPsec-Pakete zuzulassen.

### Lokale Adresse (Scanner)

Wählen Sie eine IPv4- oder IPv6-Adresse aus, die Ihrer Netzwerkumgebung entspricht. Falls automatisch eine IP-Adresse zugewiesen ist, können Sie **Automatisch bezogene IPv4-Adresse verwenden** auswählen.

#### Hinweis:

Wenn eine IPv6-Adresse automatisch zugewiesen wird, ist die Verbindung ggf. nicht verfügbar. Konfigurieren Sie eine statische IPv6-Adresse.

### Remote-Adresse(Host)

Geben Sie zur Zugriffskontrolle die IP-Adresse eines Gerätes ein. Die IP-Adresse darf höchstens 43 Zeichen lang sein. Falls keine IP-Adresse eingegeben wird, werden alle Adressen kontrolliert.

#### Hinweis:

Wenn eine IP-Adresse automatisch zugewiesen wird (z. B. durch DHCP), ist die Verbindung ggf. nicht verfügbar. Konfigurieren Sie eine statische IP-Adresse.

### Methode zur Anschlussauswahl

Wählen Sie eine Methode zur Festlegung von Anschlüssen.

Servicename

Wenn Sie **Servicename** für **Methode zur Anschlussauswahl** wählen, wählen Sie eine Option.

Transportprotokoll

Wenn Sie **Anschlussnummer** für **Methode zur Anschlussauswahl** wählen, müssen Sie einen Encapsulation-Modus konfigurieren.

Optionen	Einstellungen und Erläuterung
Beliebiges Protokoll	Wählen Sie diese Option zur Datenkontrolle aller Protokolltypen.
TCP	Wählen Sie diese Option zur Datenkontrolle bei Unicast-Verbindungen.
UDP	Wählen Sie diese Option zur Datenkontrolle bei Broadcast- und Multicast-Verbindungen.
ICMPv4	Wählen Sie diese Option zur Kontrolle des Ping-Befehls.

Lokaler Anschluss

Falls **Anschlussnummer** für **Methode zur Anschlussauswahl** ausgewählt wird, sowie **TCP** oder **UDP** für **Transportprotokoll** geben Sie durch Kommas getrennte Anschlussnummern ein, um empfangene Pakete zu kontrollieren. Sie können maximal 10 Anschlussnummern eingeben.

Beispiel: 20,80,119,5220

Wenn Sie keine Anschlussnummer eingeben, werden alle Anschlüsse kontrolliert.

Remote-Anschluss

Falls **Anschlussnummer** für **Methode zur Anschlussauswahl** ausgewählt wird, sowie **TCP** oder **UDP** für **Transportprotokoll** geben Sie durch Kommas getrennte Anschlussnummern ein, um gesendete Pakete zu kontrollieren. Sie können maximal 10 Anschlussnummern eingeben.

Beispiel: 25,80,143,5220

Wenn Sie keine Anschlussnummer eingeben, werden alle Anschlüsse kontrolliert.

**IKE-Version**

Wählen Sie **IKEv1** oder **IKEv2** als **IKE-Version**. Wählen Sie eine der beiden Optionen anhand des Geräts aus, an das der Scanner angeschlossen ist.

IKEv1

Die folgenden Elemente werden angezeigt, wenn Sie **IKEv1** als **IKE-Version** auswählen.

Optionen	Einstellungen und Erläuterung
Authentisierungsmethode	Wenn Sie <b>IPsec</b> für <b>Zugangssteuerung</b> wählen, wählen Sie eine Option. Verwendetes Zertifikat gemeinsam mit einer Standardrichtlinie.
Vorinstallierter Schlüssel	Falls <b>Vorinstallierter Schlüssel</b> für <b>Authentisierungsmethode</b> ausgewählt wird, geben Sie einen PSA-Schlüssel zwischen 1 und 127 Zeichen ein.
Vorinstallierter Schlüssel bestätigen	Geben Sie zur Bestätigung den konfigurierten Schlüssel ein.

IKEv2

Die folgenden Elemente werden angezeigt, wenn Sie **IKEv2** als **IKE-Version** auswählen.

Optionen		Einstellungen und Erläuterung
Lokal	Authentisierungsmethode	Wenn Sie <b>IPsec</b> für <b>Zugangssteuerung</b> wählen, wählen Sie eine Option. Verwendetes Zertifikat gemeinsam mit einer Standardrichtlinie.
	ID-Typ	Bei Auswahl von <b>Vorinstallierter Schlüssel</b> für <b>Authentisierungsmethode</b> , wählen Sie den ID-Typ für den Scanner aus.
	ID	Geben Sie die ID des Scanners ein, die dem ID-Typ entspricht. Die Zeichen „@“, „#“ und „=“ dürfen nicht als erstes Zeichen vorkommen. <b>Eindeutiger Name:</b> Geben Sie 1 bis 255 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein. Das Zeichen „=“ muss enthalten sein. <b>IP-Adresse:</b> Geben Sie diese im IPv4 oder IPv6-Format ein. <b>FQDN:</b> Geben Sie eine Kombination aus 1 bis 255 Zeichen ein: A–Z, a–z, 0–9, „-“ und Punkt „.“. <b>eMail-Adresse:</b> Geben Sie 1 bis 255 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein. Das Zeichen „@“ muss enthalten sein. <b>Schlüssel-ID:</b> Geben Sie 1 bis 255 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein.
	Vorinstallierter Schlüssel	Falls <b>Vorinstallierter Schlüssel</b> für <b>Authentisierungsmethode</b> ausgewählt wird, geben Sie einen PSA-Schlüssel zwischen 1 und 127 Zeichen ein.
	Vorinstallierter Schlüssel bestätigen	Geben Sie zur Bestätigung den konfigurierten Schlüssel ein.
Extern	Authentisierungsmethode	Wenn Sie <b>IPsec</b> für <b>Zugangssteuerung</b> wählen, wählen Sie eine Option. Verwendetes Zertifikat gemeinsam mit einer Standardrichtlinie.
	ID-Typ	Falls Sie <b>Vorinstallierter Schlüssel</b> für <b>Authentisierungsmethode</b> auswählen, wählen Sie den ID-Typ des Geräts aus, das Sie authentifizieren möchten.
	ID	Geben Sie die ID des Scanners ein, die dem ID-Typ entspricht. Die Zeichen „@“, „#“ und „=“ dürfen nicht als erstes Zeichen vorkommen. <b>Eindeutiger Name:</b> Geben Sie 1 bis 255 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein. Das Zeichen „=“ muss enthalten sein. <b>IP-Adresse:</b> Geben Sie diese im IPv4 oder IPv6-Format ein. <b>FQDN:</b> Geben Sie eine Kombination aus 1 bis 255 Zeichen ein: A–Z, a–z, 0–9, „-“ und Punkt „.“. <b>eMail-Adresse:</b> Geben Sie 1 bis 255 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein. Das Zeichen „@“ muss enthalten sein. <b>Schlüssel-ID:</b> Geben Sie 1 bis 255 1-Byte-ASCII-Zeichen (0x20 bis 0x7E) ein.
	Vorinstallierter Schlüssel	Falls <b>Vorinstallierter Schlüssel</b> für <b>Authentisierungsmethode</b> ausgewählt wird, geben Sie einen PSA-Schlüssel zwischen 1 und 127 Zeichen ein.
	Vorinstallierter Schlüssel bestätigen	Geben Sie zur Bestätigung den konfigurierten Schlüssel ein.

**Kapselung**

Wenn Sie **IPsec** für **Zugangssteuerung** wählen, müssen Sie einen Encapsulation-Modus konfigurieren.

Optionen	Einstellungen und Erläuterung
Transportmodus	Falls Sie den Scanner nur im selben LAN verwenden, wählen Sie diese Option. IP-Pakete der Schicht 4 oder höher werden verschlüsselt.
Tunnelmodus	Falls Sie den Scanner über ein internetfähiges Netzwerk wie IPsec-VPN verwenden, wählen Sie diese Option aus. Header und Daten der IP-Pakete werden verschlüsselt.  <b>Remote-Gateway-Adresse:</b> Falls Sie <b>Tunnelmodus</b> als <b>Kapselung</b> ausgewählt haben, geben Sie eine Gateway-Adresse zwischen 1 und 39 Zeichen ein.

### Sicherheitsprotokoll

Wenn Sie IPsec für **Zugangssteuerung** wählen, wählen Sie eine Option.

Optionen	Einstellungen und Erläuterung
ESP	Wählen Sie diese Option, um die Integrität einer Authentifizierung und der Daten sicherzustellen und die Daten zu verschlüsseln.
AH	Wählen Sie diese Option, um die Integrität einer Authentifizierung und der Daten sicherzustellen. Selbst wenn die Verschlüsselung von Daten nicht erlaubt ist, können Sie IPsec verwenden.

### Algorithmeinstellungen

Es wird empfohlen, dass Sie für alle Einstellungen **Beliebig** auswählen, oder für jeden Punkt eine Einstellung außer **Beliebig** auswählen. Falls **Beliebig** für einige Einstellungen ausgewählt wird, und eine andere Option als **Beliebig** für eine andere Einstellung, kommuniziert das Gerät möglicherweise je nach dem Gerät, das authentifiziert werden soll, nicht.

Optionen	Einstellungen und Erläuterung	
IKE	Verschlüsselung	Wählen Sie den Verschlüsselungsalgorithmus für IKE aus. Die Punkte hängen von der verwendeten IKE-Version ab.
	Authentifizierung	Wählen Sie den Authentifizierungsalgorithmus für IKE aus.
	Schlüsselaustausch	Wählen Sie den Algorithmus zum Schlüsseltausch für IKE aus. Die Punkte hängen von der verwendeten IKE-Version ab.
ESP	Verschlüsselung	Wählen Sie den Verschlüsselungsalgorithmus für ESP aus. Diese Option ist verfügbar, wenn <b>ESP</b> für <b>Sicherheitsprotokoll</b> ausgewählt ist.
	Authentifizierung	Wählen Sie den Authentifizierungsalgorithmus für ESP aus. Diese Option ist verfügbar, wenn <b>ESP</b> für <b>Sicherheitsprotokoll</b> ausgewählt ist.
AH	Authentifizierung	Wählen Sie den Verschlüsselungsalgorithmus für AH aus. Diese Option ist verfügbar, wenn <b>AH</b> für <b>Sicherheitsprotokoll</b> ausgewählt ist.

## Kombination aus Lokale Adresse (Scanner) und Remote-Adresse(Host) in Gruppenrichtlinie

		Einstellung Lokale Adresse (Scanner)		
		IPv4	IPv6* <sup>2</sup>	Beliebige Adressen* <sup>3</sup>
<b>Einstellung Remote-Adresse(Host)</b>	IPv4* <sup>1</sup>	✓	–	✓
	IPv6* <sup>1</sup> , * <sup>2</sup>	–	✓	✓
	Leer	✓	✓	✓

\*1 Falls **IPsec** ausgewählt ist für **Zugangssteuerung**, kann keine Präfixlänge ausgewählt werden.

\*2 Falls **IPsec** ausgewählt ist für **Zugangssteuerung**, kann eine Link-Local-Adresse (fe80::) ausgewählt werden, aber die Gruppenrichtlinie wird deaktiviert sein.

\*3 Außer IPv6-Link-Local-Adressen.

### Zugehörige Informationen

➔ „Ausführen von Web Config in einem Webbrowser“ auf Seite 40

## Verweise auf Servicename in Gruppenrichtlinie

### Hinweis:

Nicht verfügbare Dienste werden angezeigt, können jedoch nicht ausgewählt werden.

Servicename	Protokolltyp	Lokale Portnummer	Remote-Portnummer	Kontrollierte Funktionen
Beliebig	–	–	–	Alle Services
ENPC	UDP	3289	Beliebiger Port	Scannersuche über Anwendungen wie Epson Device Admin und einem Scannertreiber
SNMP	UDP	161	Beliebiger Port	MIB-Erfassung und -Konfiguration über Anwendungen wie Epson Device Admin und dem Epson-Scannertreiber
WSD	TCP	Beliebiger Port	5357	WSD-Kontrolle
WS-Discovery	UDP	3702	Beliebiger Port	Suche nach WSD-Scannern
Network Scan	TCP	1865	Beliebiger Port	Weiterleitung von Scandaten über Document Capture Pro
Network Push Scan	TCP	Beliebiger Port	2968	Erfassung von Auftragsinformationen für Push-Scan über Document Capture Pro
Network Push Scan Discovery	UDP	2968	Beliebiger Port	Suche nach einem Computer vom Scanner aus

Servicename	Protokolltyp	Lokale Portnummer	Remote-Portnummer	Kontrollierte Funktionen
FTP-Daten (Remote)	TCP	Beliebiger Port	20	FTP-Client (Weiterleitung von Scandaten)  So kann jedoch nur ein FTP-Server mit Remote-Portnummer 20 kontrolliert werden.
FTP-Steuerung (Remote)	TCP	Beliebiger Port	21	FTP-Client (Kontrolle der Weiterleitung von Scandaten)
CIFS (Remote)	TCP	Beliebiger Port	445	CIFS-Client (Weiterleitung von Scandaten an einen Ordner)
NetBIOS Name Service (Remote)	UDP	Beliebiger Port	137	CIFS-Client (Weiterleitung von Scandaten an einen Ordner)
NetBIOS Datagram Service (Remote)	UDP	Beliebiger Port	138	
NetBIOS Session Service (Remote)	TCP	Beliebiger Port	139	
HTTP (Lokal)	TCP	80	Beliebiger Port	HTTP(S)-Server (Weiterleitung von Web Config- und WSD-Daten)
HTTPS (Lokal)	TCP	443	Beliebiger Port	
HTTP (Remote)	TCP	Beliebiger Port	80	HTTP(S)-Client (Aktualisieren der Firmware und des Stammzertifikats)
HTTPS (Remote)	TCP	Beliebiger Port	443	

## Konfigurationsbeispiele für IPsec/IP-Filterung

### Ausschließliches Empfangen von IPsec-Paketen

In diesem Beispiel wird nur eine Standardrichtlinie konfiguriert.

#### Standardrichtlinie:

- IPsec/IP-Filterung: Aktivieren**
- Zugangssteuerung: IPsec**
- Authentisierungsmethode: Vorinstallierter Schlüssel**
- Vorinstallierter Schlüssel:** Geben Sie bis zu 127 Zeichen ein.

**Gruppenrichtlinie:** Nicht konfigurieren.

### Empfangen von Scandaten und Druckereinstellungen

Dieses Beispiel ermöglicht die Kommunikation von Scandaten und Scannerkonfiguration aus bestimmten Diensten.

#### Standardrichtlinie:

- IPsec/IP-Filterung: Aktivieren**
- Zugangssteuerung: Zugang verweigern**

#### Gruppenrichtlinie:

- Diese Gruppenrichtlinie aktivieren:** Aktivieren Sie das Kontrollkästchen.
- Zugangssteuerung: Zugang erlauben**
- Remote-Adresse(Host):** IP-Adresse des Clients
- Methode zur Anschlussauswahl: Servicename**
- Servicename:** Aktivieren Sie das Kontrollkästchen für ENPC, SNMP, HTTP (Lokal), HTTPS (Lokal) und Network Scan.

#### Empfangen des Zugriffs nur von einer bestimmten IP-Adresse aus

In diesem Beispiel kann eine bestimmte IP-Adresse auf den Scanner zugreifen.

#### Standardrichtlinie:

- IPsec/IP-Filterung: Aktivieren**
- Zugangssteuerung: Zugang verweigern**

#### Gruppenrichtlinie:

- Diese Gruppenrichtlinie aktivieren:** Aktivieren Sie das Kontrollkästchen.
- Zugangssteuerung: Zugang erlauben**
- Remote-Adresse(Host):** IP-Adresse eines Administratorclients

#### **Hinweis:**

*Unabhängig von der Richtlinienkonfiguration kann der Client auf den Scanner zugreifen und ihn konfigurieren.*

## Konfigurieren eines Zertifikats für IPsec/IP-Filterung

So konfigurieren Sie ein Client-Zertifikat für die IPsec/IP-Filterung. Sobald dieses festgelegt wurde, können Sie das Zertifikat als Authentifizierungsmethode für die IPsec/IP-Filterung verwenden. Wenn Sie die Zertifizierungsstelle konfigurieren möchten, wechseln Sie zu **CA-Zertifikat**.

1. Navigieren Sie zu Web Config und wählen Sie dann die Registerkarte **Netzwerksicherheit > IPsec/IP-Filterung > Client-Zertifikat**.
2. Importieren Sie das Zertifikat unter **Client-Zertifikat**.

Wenn Sie bereits ein von einer Zertifizierungsstelle veröffentlichtes Zertifikat importiert haben, können Sie das Zertifikat kopieren und in IPsec/IP-Filterung verwenden. Zum Kopieren wählen Sie das Zertifikat unter **Kopieren von** aus, und klicken dann auf **Kopie**.

#### Zugehörige Informationen

- ➔ [„Ausführen von Web Config in einem Webbrowser“](#) auf Seite 40
- ➔ [„Konfigurieren eines CA-signiertes Zertifikat“](#) auf Seite 98
- ➔ [„Konfigurieren eines CA-Zertifikat“](#) auf Seite 102

# Verbinden des Scanners mit einem IEEE802.1X-Netzwerk

## Konfiguration eines IEEE 802.1X-Netzwerks

Wenn im Scanner IEEE 802.1X eingestellt ist, kann dieses Protokoll in einem Netzwerk mit RADIUS-Server, einem LAN-Switch mit Authentifizierungsfunktion oder einem Zugangspunkt verwendet werden.

1. Rufen Sie hierzu Web Config auf und öffnen Sie dann die Registerkarte **Netzwerksicherheit > IEEE802.1X > Grundlegend**.

2. Geben Sie einen Wert für jedes Element ein.

Falls Sie den Scanner in einem WLAN-Netzwerk nutzen möchten, klicken Sie auf **Wi-Fi-Setup** und wählen Sie eine SSID aus bzw. geben Sie eine ein.

**Hinweis:**

*Die Einstellungen zwischen Ethernet und WLAN lassen sich gemeinsam nutzen.*

3. Klicken Sie auf **Weiter**.

Eine Bestätigungsmeldung wird angezeigt.

4. Klicken Sie auf **OK**.

Der Scanner ist aktualisiert.

### Zugehörige Informationen

➔ „Ausführen von Web Config in einem Webbrowser“ auf Seite 40

## Optionen für die IEEE802.1X-Netzwerkeinstellung

Optionen	Einstellungen und Erläuterung	
IEEE802.1X (Kabel-LAN)	Sie können die Einstellungen der Seite ( <b>IEEE802.1X &gt; Grundlegend</b> ) für IEEE802.1X (Wired LAN) aktivieren oder deaktivieren.	
IEEE802.1X (Wi-Fi)	Es wird der Verbindungsstatus von IEEE802.1X (Wi-Fi) angezeigt.	
Verbindungsmethode	Es wird die Verbindungsmethode eines aktuellen Netzwerks angezeigt.	
EAP-Typ	Wählen Sie eine Option für eine Authentifizierungsmethode zwischen dem Scanner und einem RADIUS Server aus.	
	EAP-TLS	Sie müssen ein CA-signiertes Zertifikat erhalten und importieren.
	PEAP-TLS	
	PEAP/MSCHAPv2	Sie müssen ein Kennwort konfigurieren.
EAP-TTLS		
Benutzer-ID	Konfigurieren Sie eine ID für die Authentifizierung eines RADIUS-Servers. Geben Sie 1 bis 128 1-Byte ASCII-Zeichen (0x20 bis 0x7E) ein.	

Optionen	Einstellungen und Erläuterung	
Kennwort	Konfigurieren Sie ein Kennwort zur Authentifizierung des Scanners. Geben Sie 1 bis 128 1-Byte ASCII-Zeichen (0x20 bis 0x7E) ein. Wenn Sie einen Windows Server als RADIUS Server verwenden können Sie bis zu 127 Zeichen eingeben.	
Kennwort bestätigen	Geben Sie das zur Bestätigung konfigurierte Kennwort ein.	
Server-ID	Sie können eine Server-ID für die Authentifizierung bei einem bestimmten RADIUS Server konfigurieren. Authenticator prüft, ob eine Server-ID im Feld subject/subjectAltName eines Serverzertifikats enthalten ist, das von einem RADIUS gesendet wird oder nicht. Geben Sie 0 bis 128 1-Byte ASCII-Zeichen (0x20 bis 0x7E) ein.	
Zertifikatsvalidierung (WLAN)	Wenn Sie die <b>Zertifikatsvalidierung</b> mit <b>IEEE802.1X (Kabel-LAN)</b> durchführen möchten, wählen Sie <b>Aktivieren</b> . Wenn Sie „Aktivieren“ ausgewählt haben, lesen Sie die entsprechenden Informationen und importieren das <b>CA-Zertifikat</b> . Beachten Sie, dass Zertifikatsvalidierung in IEEE802.1X (Wi-Fi) immer aktiviert ist. Importieren Sie das CA-Zertifikat.	
Anonymer Name	Wenn Sie <b>PEAP-TLS</b> oder <b>PEAP/MSCHAPv2</b> für <b>EAP-Typ</b> auswählen, können Sie einen anonymen Namen anstelle einer Benutzer-ID für die Phase 1 einer PEAP-Authentifizierung konfigurieren. Geben Sie 0 bis 128 1-Byte ASCII-Zeichen (0x20 bis 0x7E) ein.	
Verschlüsselungsstärke	Sie können eine der Folgenden auswählen.	
	Hoch	AES256/3DES
	Mittel	AES256/3DES/AES128/RC4

### Zugehörige Informationen

➔ „Konfigurieren eines CA-Zertifikat“ auf Seite 102

## Konfigurieren eines Zertifikats für IEEE 802.1X

So konfigurieren Sie das Client-Zertifikat für IEEE802.1X. Beim Einrichten können Sie sowohl **EAP-TLS** als auch **PEAP-TLS** als Authentifizierungsmethode für IEEE 802.1X verwenden. Wenn Sie das Zertifikat der Zertifizierungsstelle konfigurieren möchten, wechseln Sie zu **CA-Zertifikat**.

1. Navigieren Sie zu Web Config und wählen Sie dann die Registerkarte **Netzwerksicherheit > IEEE802.1X > Client-Zertifikat**.
2. Geben Sie ein Zertifikat ein unter **Client-Zertifikat**.

Wenn Sie bereits ein von einer Zertifizierungsstelle veröffentlichtes Zertifikat importiert haben, können Sie das Zertifikat kopieren und in IEEE802.1X verwenden. Zum Kopieren wählen Sie das Zertifikat unter **Kopieren von** aus, und klicken dann auf **Kopie**.

### Zugehörige Informationen

➔ „Ausführen von Web Config in einem Webbrowser“ auf Seite 40

## Beheben von Problemen für erweiterte Sicherheit

### Wiederherstellen der Sicherheitseinstellungen

Beim Einsatz äußerst sicherer Verfahren wie IPsec/IP-Filterung kann es vorkommen, dass Sie aufgrund falscher Einstellungen oder Problemen auf dem Gerät oder Server nicht mehr mit den Geräten kommunizieren können. Stellen Sie in einem solchen Fall die Sicherheitseinstellungen wieder her, um die richtigen Geräteeinstellungen erneut vorzunehmen oder temporären Zugriff zu gewähren.

### Deaktivieren der Sicherheitsfunktion mit Web Config

Sie können IPsec/IP-Filterung mit Web Config deaktivieren.

1. Wechseln Sie zu Web Config und wählen Sie die Registerkarte **Netzwerksicherheit > IPsec/IP-Filterung > Grundlegend**.
2. Deaktivieren Sie den **IPsec/IP-Filterung**.

## Probleme bei Verwendung der Netzwerksicherheitsfunktionen

### Ein PSA-Schlüssel wurde vergessen

#### Einen PSA-Schlüssel neu konfigurieren.

Um den Zugriffsschlüssel zu ändern, rufen Sie Web Config auf und öffnen Sie die Registerkarte **Netzwerksicherheit > IPsec/IP-Filterung > Grundlegend > Standardrichtlinie** oder **Gruppenrichtlinie**.

Ändern Sie nach dem Wechsel des PSA-Schlüssels auch die auf den Computern hinterlegten PSA-Schlüssel.

#### Zugehörige Informationen

- ➔ [„Ausführen von Web Config in einem Webbrowser“](#) auf Seite 40
- ➔ [„Verschlüsselte Kommunikation mit IPsec/IP-Filterung“](#) auf Seite 104

### Keine IPsec-Kommunikation

#### Festlegen eines Algorithmus, den der Computer oder der Drucker nicht unterstützt.

Der Scanner unterstützt die folgenden Algorithmen. Überprüfen Sie die Einstellungen des Computers.

Sicherheitsverfahren	Algorithmen
IKE-Verschlüsselungsalgorithmus	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
IKE-Authentifizierungsalgorithmus	SHA-1, SHA-256, SHA-384, SHA-512, MD5

Sicherheitsverfahren	Algorithmen
IKE-Schlüsseltauschalgorithmus	DH Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27*, DH Group28*, DH Group29*, DH Group30*
ESP-Verschlüsselungsalgorithmus	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP-Authentifizierungsalgorithmus	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH-Authentifizierungsalgorithmus	SHA-1, SHA-256, SHA-384, SHA-512, MD5

\* Nur für IKEv2

### Zugehörige Informationen

➔ [„Verschlüsselte Kommunikation mit IPsec/IP-Filterung“](#) auf Seite 104

## Plötzlich ausfallende Kommunikation

### Die IP-Adresse des Scanners wurde geändert oder kann nicht verwendet werden.

Wenn die als lokale Adresse in der Gruppenrichtlinie verwendete IP-Adresse geändert wurde oder nicht verwendet werden kann, ist eine Kommunikation über IPsec nicht möglich. Deaktivieren Sie IPsec im Scannerbedienfeld.

Falls der DHCP-Server veraltet ist, neu startet oder die IPv6-Adresse veraltet oder nicht abgerufen wurde, kann die auf der Registerkarte Web Config (**Netzwerksicherheit > IPsec/IP-Filterung > Grundlegend > Gruppenrichtlinie > Lokale Adresse (Scanner)**) des Scanners registrierte IP-Adresse vielleicht nicht gefunden werden.

Verwenden Sie eine statische IP-Adresse.

### Die IP-Adresse des Computers wurde geändert oder kann nicht verwendet werden.

Wenn die als Remote-Adresse in der Gruppenrichtlinie verwendete IP-Adresse geändert wurde oder nicht verwendet werden kann, ist eine Kommunikation über IPsec nicht möglich.

Deaktivieren Sie IPsec im Scannerbedienfeld.

Falls der DHCP-Server veraltet ist, neu startet oder die IPv6-Adresse veraltet oder nicht abgerufen wurde, kann die auf der Registerkarte Web Config (**Netzwerksicherheit > IPsec/IP-Filterung > Grundlegend > Gruppenrichtlinie > Remote-Adresse(Host)**) des Scanners registrierte IP-Adresse vielleicht nicht gefunden werden.

Verwenden Sie eine statische IP-Adresse.

### Zugehörige Informationen

➔ [„Ausführen von Web Config in einem Webbrowser“](#) auf Seite 40

➔ [„Verschlüsselte Kommunikation mit IPsec/IP-Filterung“](#) auf Seite 104

## **Verbindung nach Konfiguration von IPsec/IP-Filterung nicht möglich**

### **Die Einstellungen der IPsec/IP-Filterung sind falsch.**

Deaktivieren Sie IPsec/IP-Filterung im Scannerbedienfeld. Verbinden Sie Scanner und Computer und nehmen Sie die Einstellungen von IPsec/IP-Filterung erneut vor.

### **Zugehörige Informationen**

➔ [„Verschlüsselte Kommunikation mit IPsec/IP-Filterung“ auf Seite 104](#)

## **Zugriff auf das Gerät nach Konfiguration von IEEE 802.1X nicht möglich**

### **Die Einstellungen für IEEE 802.1X sind falsch.**

Deaktivieren Sie IEEE 802.1X und WLAN auf dem Scannerbedienfeld. Verbinden Sie den Scanner mit einem Computer, und konfigurieren Sie dann IEEE 802.1X erneut.

### **Zugehörige Informationen**

➔ [„Konfiguration eines IEEE 802.1X-Netzwerks“ auf Seite 116](#)

## **Probleme bei der Verwendung eines digitalen Zertifikats**

### **Ein CA-signiertes Zertifikat kann nicht importiert werden**

#### **Das CA-signierte Zertifikat stimmt nicht mit dem CSR überein.**

Wenn das CA-signierte Zertifikat andere Daten als der CSR enthält, kann das Zertifikat nicht importiert werden. Prüfen Sie Folgendes:

- Versuchen Sie, das Zertifikat auf ein Gerät zu importieren, das nicht dieselben Informationen enthält?  
Prüfen Sie die Informationen auf dem CSR und importieren Sie dann das Zertifikat auf ein Gerät, das dieselben Informationen enthält.
- Haben Sie den im Scanner gespeicherten CSR nach dem Senden an eine Zertifizierungsbehörde überschrieben?  
Beziehen Sie mit dem CSR erneut ein CA-signiertes Zertifikat.

#### **CA-signiertes Zertifikat ist größer als 5KB.**

Ein CA-signiertes Zertifikat, das größer als 5 KB ist, kann nicht importiert werden.

#### **Das Kennwort zum Importieren des Zertifikats ist ungültig.**

Geben Sie das richtige Passwort ein. Wenn Sie das Kennwort vergessen haben, können Sie das Zertifikat nicht importieren. Rufen Sie das CA-signierte Zertifikat erneut ab.

### **Zugehörige Informationen**

➔ [„Importieren eines CA-signierten Zertifikats“ auf Seite 99](#)

## Aktualisieren eines selbstsignierten Zertifikats nicht möglich

### Es wurde kein Allgemeiner Name eingegeben.

Allgemeiner Name muss eingegeben werden.

### Es wurden nicht unterstützte Zeichen in Allgemeiner Name eingegeben.

Geben Sie 1 bis 128 ASCII-Zeichen (0x20–0x7E) im IPv4-, IPv6-, Hostnamen- oder FQDN-Format ein.

### Der „Common Name“ enthält ein Komma oder Leerzeichen.

Enthält der **Allgemeiner Name** ein Komma, wird er an dieser Stelle geteilt. Wenn vor oder nach einem Komma nur ein Leerzeichen steht, tritt ein Fehler auf.

### Zugehörige Informationen

➔ [„Aktualisieren eines selbstsignierten Zertifikats“ auf Seite 101](#)

## Ein CSR kann nicht erstellt werden

### Es wurde kein Allgemeiner Name eingegeben.

Der **Allgemeiner Name** muss eingegeben werden.

### Es wurden nicht unterstützte Zeichen in Allgemeiner Name, Organisation, Organisationseinheit, Ort und Staat/Bundesland eingegeben.

Geben Sie ASCII-Zeichen (0x20–0x7E) im IPv4-, IPv6-, Hostnamen- oder FQDN-Format ein.

### Der Allgemeiner Name enthält ein Komma oder Leerzeichen.

Enthält der **Allgemeiner Name** ein Komma, wird er an dieser Stelle geteilt. Wenn vor oder nach einem Komma nur ein Leerzeichen steht, tritt ein Fehler auf.

### Zugehörige Informationen

➔ [„Erhalten eines CA-signierten Zertifikats“ auf Seite 98](#)

## Warnmeldung für ein digitales Zertifikat wird angezeigt

Meldungen	Ursache/Lösung
Ein Serverzertifikat eingeben.	<b>Ursache:</b> Es ist keine Datei für den Import ausgewählt. <b>Lösung:</b> Wählen Sie eine Datei und klicken Sie auf <b>Importieren</b> .

Meldungen	Ursache/Lösung
CA-Zertifikat 1 nicht eingegeben.	<p><b>Ursache:</b> CA-Zertifikat 1 ist nicht eingegeben und nur CA-Zertifikat 2 ist eingegeben.</p> <p><b>Lösung:</b> Importieren Sie CA-Zertifikat 1 zuerst.</p>
Der nachfolgende Wert ist ungültig.	<p><b>Ursache:</b> Der Dateipfad und/oder das Kennwort enthalten nicht unterstützte Zeichen.</p> <p><b>Lösung:</b> Stellen Sie sicher, dass die Zeichen für das Element richtig eingegeben werden.</p>
Datum und Zeit ungültig.	<p><b>Ursache:</b> Datum und Uhrzeit sind für den Scanner nicht eingestellt.</p> <p><b>Lösung:</b> Stellen Sie Datum und Uhrzeit mit Web Config oder EpsonNet Config ein.</p>
Kennwort ungültig.	<p><b>Ursache:</b> Das für das CA-Zertifikat festgelegte Kennwort und das eingegebene Kennwort stimmen nicht überein.</p> <p><b>Lösung:</b> Geben Sie das richtige Kennwort ein.</p>
Datei ungültig.	<p><b>Ursache:</b> Sie importieren keine Zertifikatsdatei im X509-Format.</p> <p><b>Lösung:</b> Stellen Sie sicher, dass Sie das richtige, von einer vertrauenswürdigen Zertifizierungsbehörde gesendete Zertifikat gewählt haben.</p>
	<p><b>Ursache:</b> Die importierte Datei ist zu groß. Die maximale Dateigröße beträgt 5 KB.</p> <p><b>Lösung:</b> Wenn Sie die richtige Datei gewählt haben, ist das Zertifikat ggf. beschädigt oder fabriziert.</p>
	<p><b>Ursache:</b> Die im Zertifikat enthaltene Kette ist ungültig.</p> <p><b>Lösung:</b> Weitere Informationen zum Zertifikat finden Sie auf der Website der Zertifizierungsbehörde.</p>
Kann Serverzertifikate nicht nutzen, die mehr als drei CA-Zertifikate beinhalten.	<p><b>Ursache:</b> Die Zertifikatsdatei im PKCS#12-Format enthält mehr als 3 CA-Zertifikate.</p> <p><b>Lösung:</b> Importieren Sie jedes Zertifikat durch Konvertieren vom PKCS#12- ins PEM-Format oder importieren Sie die Zertifikatsdatei im PKCS#12-Format, die bis zu 2 CA-Zertifikate enthält.</p>

Meldungen	Ursache/Lösung
Das Zertifikat ist abgelaufen. Prüfen Sie, ob das Zertifikat gültig ist, oder prüfen Sie Datum und Zeit auf dem Produkt.	<p><b>Ursache:</b></p> <p>Das Zertifikat ist abgelaufen.</p> <p><b>Lösung:</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Wenn das Zertifikat abgelaufen ist, beziehen und importieren Sie ein neues Zertifikat.</li> <li><input type="checkbox"/> Wenn das Zertifikat nicht abgelaufen ist, stellen Sie sicher, dass Datum und Uhrzeit im Scanner richtig eingestellt sind.</li> </ul>
Privater Schlüssel erforderlich.	<p><b>Ursache:</b></p> <p>Mit dem Zertifikat ist kein privater Schlüssel verknüpft.</p> <p><b>Lösung:</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Bei einem Zertifikat im PEM/DER-Format, das über einen Computer mit einem CSR bezogen worden ist, geben Sie den privaten Schlüssel ein.</li> <li><input type="checkbox"/> Bei einem Zertifikat im PKCS#12-Format, das über einen Computer mit einem CSR bezogen worden ist, erstellen Sie eine Datei, die den privaten Schlüssel enthält.</li> </ul>
	<p><b>Ursache:</b></p> <p>Sie haben ein PEM/DER-Zertifikat, das über einen CSR mit Web Config bezogen worden ist, erneut importiert.</p> <p><b>Lösung:</b></p> <p>Ein Zertifikat im PEM/DER-Format, das mit Web Config und einem CSR bezogen worden ist, kann nur einmal importiert werden.</p>
Einrichtung ist fehlgeschlagen.	<p><b>Ursache:</b></p> <p>Die Konfiguration kann nicht abgeschlossen werden, weil die Kommunikation zwischen Scanner und Computer fehlgeschlagen ist oder die Datei wegen einiger Fehler nicht gelesen werden kann.</p> <p><b>Lösung:</b></p> <p>Prüfen Sie die angegebene Datei und Kommunikation und importieren Sie die Datei erneut.</p>

### Zugehörige Informationen

➔ [„Über digitale Zertifizierung“ auf Seite 97](#)

## CA-signiertes Zertifikat versehentlich gelöscht

### Für das CA-signierte Zertifikat ist keine Sicherungsdatei vorhanden.

Wenn Sie eine Sicherungsdatei haben, importieren Sie das Zertifikat erneut.

Wenn Sie ein Zertifikat beziehen, das mit einem in Web Config erstellten CSR beantragt worden ist, können Sie ein gelöscht Zertifikat nicht noch einmal importieren. Erstellen Sie einen CSR und beziehen Sie ein neues Zertifikat.

### Zugehörige Informationen

➔ [„Importieren eines CA-signierten Zertifikats“ auf Seite 99](#)

➔ [„Löschen eines CA-signierten Zertifikats“ auf Seite 101](#)

---

# Verwenden von Epson Open Platform

Epson Open Platform Übersicht. . . . .	125
Konfigurieren von Epson Open Platform. . . . .	125
Validierung von Epson Open Platform. . . . .	125

---

## Epson Open Platform Übersicht

Epson Open Platform ist eine Plattform, die Ihnen die Verwendung des Authentifizierungssystems mit diesem Scanner ermöglicht.

Die Plattform lässt sich mit Epson Print Admin (Epson Authentifizierungssystem) oder einem Authentifizierungssystem von Dritten verwenden. Sie können Protokolle nach Gerät und Benutzer abrufen, Geräte für die Benutzer und Gruppen konfigurieren, Schwellenwerte für Funktionen festlegen usw.

Bei Anschluss eines Authentifizierungsgeräts kann die Benutzerauthentifizierung auch über eine ID-Karte erfolgen.

---

## Konfigurieren von Epson Open Platform

Aktivieren Sie Epson Open Platform, um das Gerät über das Authentifizierungssystem verwenden zu können.

1. Beziehen Sie einen Produktschlüssel von der angegebenen Website.  
Im Handbuch zu Epson Open Platform finden Sie u. a. Einzelheiten zum Beziehen des Produktschlüssels.
2. Rufen Sie Web Config auf und wählen Sie die Registerkarte **Epson Open Platform > Produktschlüssel oder Lizenzschlüssel** aus.
3. Überprüfen und legen Sie jede Option fest.
  - Seriennummer  
Die Seriennummer des Geräts wird angezeigt.
  - Epson Open Platform-Version  
Wählen Sie die Version von Epson Open Platform. Die entsprechende Version kann je nach Authentifizierungssystem unterschiedlich sein.
  - Produktschlüssel oder Lizenzschlüssel  
Geben Sie den zu beziehenden Produktschlüssel ein.
4. Klicken Sie auf **Weiter**.  
Der Einstellungsbestätigungsbildschirm wird angezeigt.
5. Klicken Sie auf **OK**.  
Die Einstellungen werden auf den Scanner angewendet.

**Hinweis:**

*Sie können Epson Print Admin Serverless nicht verwenden, wenn das System mit Epson Open Platform synchronisiert ist.*

---

## Validierung von Epson Open Platform

Sie können die Gültigkeit der Epson Open Platform mit einer der folgenden Methoden validieren.

Web Config

Es wurde ein Produktschlüssel auf der Registerkarte **Epson Open Platform > Produktschlüssel oder Lizenzschlüssel > Produktschlüssel oder Lizenzschlüssel** eingegeben und die Registerkarte **Epson Open Platform > Authentifizierungssystem** wird links im Menüverzeichnis angezeigt.

Bedienfeld des Scanners

Überprüfen Sie, ob der Produktschlüssel in **Einstellungen > Geräteinformationen > Informationen zu Epson Open Platform** angezeigt wird.

---

# Mounting eines Authentifizierungsgeräts

Verbinden des Authentifizierungsgeräts. . . . .	128
Funktionsprüfung des Authentifizierungsgeräts. . . . .	128
Überprüfen der Erkennung der Authentifizierungskarte. . . . .	128
Fehlerbehebung bei Problemen mit dem Authentifizierungsgerät. . . . .	129

## Verbinden des Authentifizierungsgeräts

**Hinweis:**

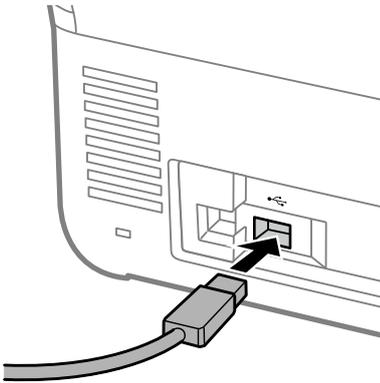
Ein Authentifizierungssystem verwendet ein Authentifizierungsgerät.



**Wichtig:**

Wenn Sie das Authentifizierungsgerät mit mehreren Scannern verbinden, verwenden Sie ein Produkt mit derselben Modellnummer.

Schließen Sie das USB-Kabel des Kartenlesers an den externen Schnittstellen-USB-Port des Scanners an.



---

## Funktionsprüfung des Authentifizierungsgeräts

Sie können den Verbindungsstatus und die Erkennung der Authentifizierungskarte für das Authentifizierungsgerät über das Bedienfeld des Scanners prüfen.

Informationen werden angezeigt, wenn Sie **Einstellungen > Geräteinformationen > Status Authentifizierungsgerät** wählen.

---

## Überprüfen der Erkennung der Authentifizierungskarte

Sie können mit Web Config.überprüfen, ob die Authentifizierungskarten erkannt werden kann.

1. Rufen Sie Web Config auf und wählen Sie die Registerkarte **Geräteverwaltung > Kartenleser** aus.
2. Halten Sie die Authentifizierungskarte über den Authentifizierungskartenleser.
3. Klicken Sie auf **Prüfen**.  
Das Ergebnis wird angezeigt.

## **Fehlerbehebung bei Problemen mit dem Authentifizierungsgerät**

### **Authentifizierungskarte kann nicht gelesen werden**

Überprüfen Sie Folgendes.

- Überprüfen Sie, ob das Authentifizierungsgerät richtig am Scanner angeschlossen ist.  
Schließen Sie das Authentifizierungsgerät an den externen Schnittstellen-USB-Port auf der Rückseite des Scanners an.
- Überprüfen Sie, ob Authentifizierungsgerät und Authentifizierungskarte zertifiziert sind.  
Wenden Sie sich an Ihren Händler, um Informationen über unterstützte Authentifizierungsgeräte und -karten zu erhalten.

---

# Wartung

Äußerliches Reinigen des Scanners. . . . .	131
Reinigen der Innenbereiche des Scanners. . . . .	131
Austauschen des Roller-Assembly-Kits. . . . .	136
Zurücksetzen der Anzahl der Scans nach dem Austauschen der Rollen. . . . .	141
Energie sparen. . . . .	142
Transportieren des Scanners. . . . .	142
Sichern der Einstellungen. . . . .	143
Werkseinstlg. wiederh.. . . .	144
Aktualisieren von Anwendungen und Firmware. . . . .	145

---

## Äußerliches Reinigen des Scanners

Wischen Sie Verschmutzungen am Außengehäuse mit einem trockenen oder mit mildem Reinigungsmittel und Wasser befeuchteten Tuch ab.



**Wichtig:**

- Verwenden Sie niemals Alkohol, Verdünner oder ätzende Lösungsmittel zum Reinigen des Scanners. Andernfalls können Verformungen oder Verfärbungen auftreten.
- Kein Wasser in das Innere des Geräts gelangen lassen. Andernfalls kann eine Fehlfunktion auftreten.
- Öffnen Sie niemals das Scannergehäuse.

1. Drücken Sie zum Ausschalten des Scanners die Taste .
2. Trennen Sie das Netzkabel vom Scanner.
3. Reinigen Sie die Außenflächen des Gehäuses mit einem leicht mit mildem Reinigungsmittel und etwas Wasser angefeuchteten Tuch.

**Hinweis:**

Wischen Sie den Touchscreen mit einem weichen, trockenen Tuch ab.

---

## Reinigen der Innenbereiche des Scanners

Wenn der Scanner eine bestimmte Zeit in Benutzung war, können Papier- und Hausstaub auf dem Roller oder den Glasflächen im Inneren des Scanners Probleme beim Einzug oder bei der Bildqualität hervorrufen. Reinigen Sie das Innere des Scanners etwa alle 5,000 Scanvorgänge.

Die aktuelle Anzahl durchgeführter Scans lässt sich auf dem Bedienfeld oder in Epson Scan 2 Utility überprüfen.

Ist eine Oberfläche mit einem schwer entfernbaren Material beschmutzt, verwenden Sie ein originales Epson-ReinigungsKit zum Entfernen der Beschmutzung. Tragen Sie eine geringe Menge des Reinigers auf ein Reinigungstuch auf, um die Verschmutzungen zu entfernen.

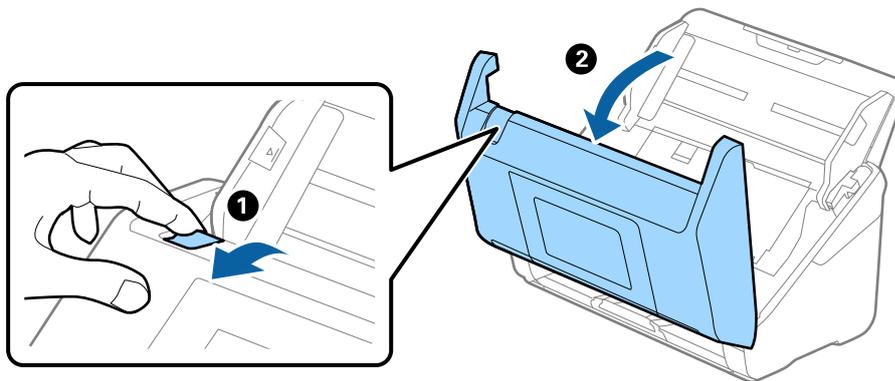


**Wichtig:**

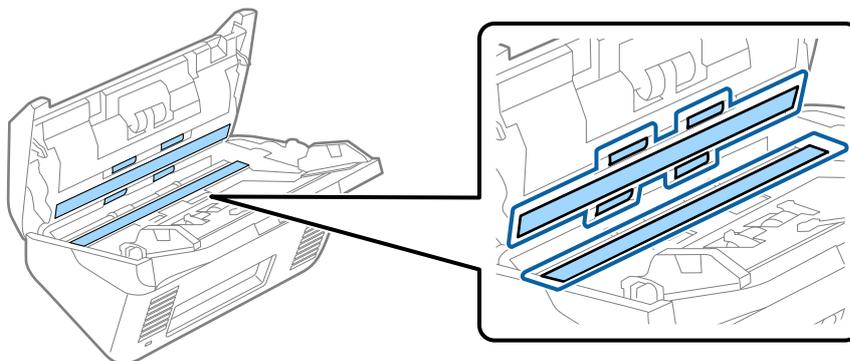
- Verwenden Sie niemals Alkohol, Verdünner oder ätzende Lösungsmittel zum Reinigen des Scanners. Andernfalls können Verformungen oder Verfärbungen auftreten.
- Sprühen Sie keinesfalls Flüssigkeiten oder Schmiermittel auf den Scanner. Eine Beschädigung des Geräts oder der Schaltkreise kann zu Fehlfunktionen führen.
- Öffnen Sie niemals das Scannergehäuse.

1. Drücken Sie zum Ausschalten des Scanners die -Taste.
2. Trennen Sie das Netzkabel vom Scanner.

3. Ziehen Sie den Hebel und öffnen Sie die Scannerabdeckung.



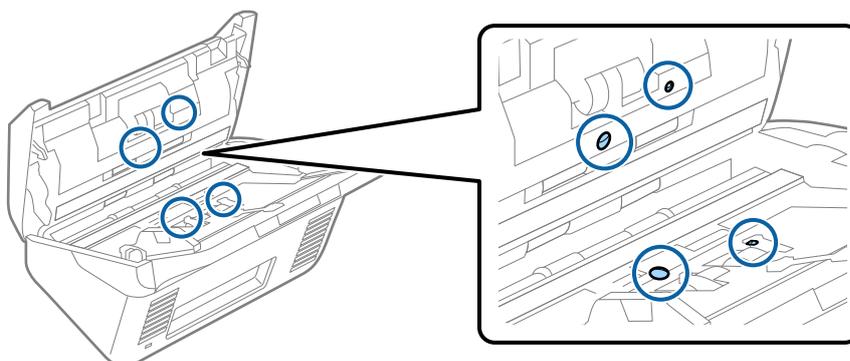
4. Wischen Sie eventuelle Verschmutzungen auf dem Kunststoffroller (vier Stellen) und auf der Glasfläche in der Scannerabdeckung ab. Wischen Sie sie mit einem weichen, fusselfreien Tuch ab und feuchten Sie das Tuch mit einem speziellen Reinigungsmittel oder Wasser an.



**! Wichtig:**

- Die Glasfläche nicht zu stark belasten.
- Keine Bürsten oder harte Werkzeuge verwenden. Jegliche Kratzer auf dem Glas können die Scanqualität beeinträchtigen.
- Sprühen Sie Reiniger nicht direkt auf die Glasfläche.

5. Wischen Sie Verschmutzungen auf den Sensoren mit einem Wattestäbchen ab.

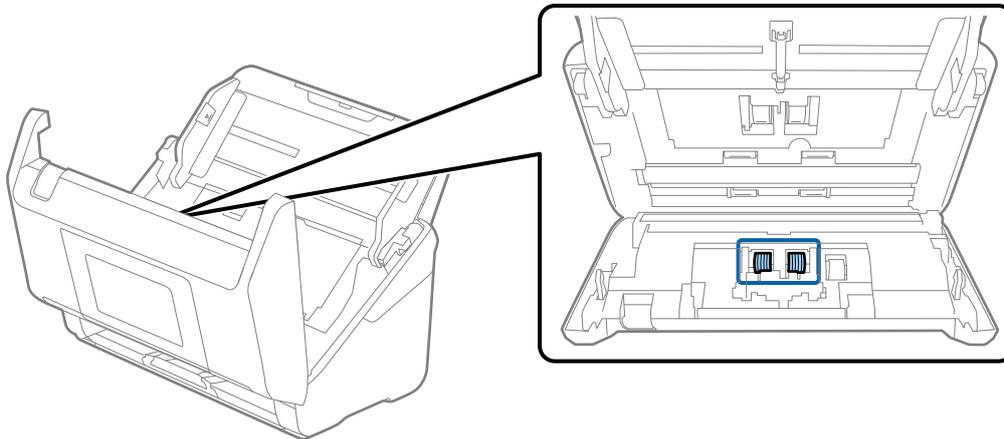




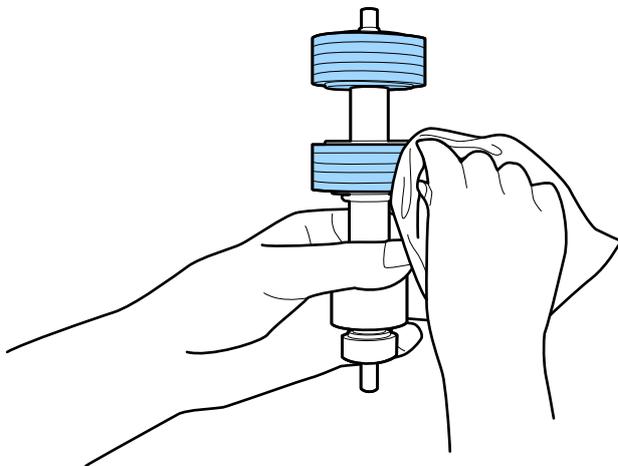
**Wichtig:**

*Keine Flüssigkeiten wie Reinigungsmittel auf das Wattestäbchen auftragen.*

6. Öffnen Sie die Abdeckung und entfernen Sie die Trennwalze.  
Einzelheiten hierzu finden Sie unter „Austauschen des Roller-Assembly-Kits“.



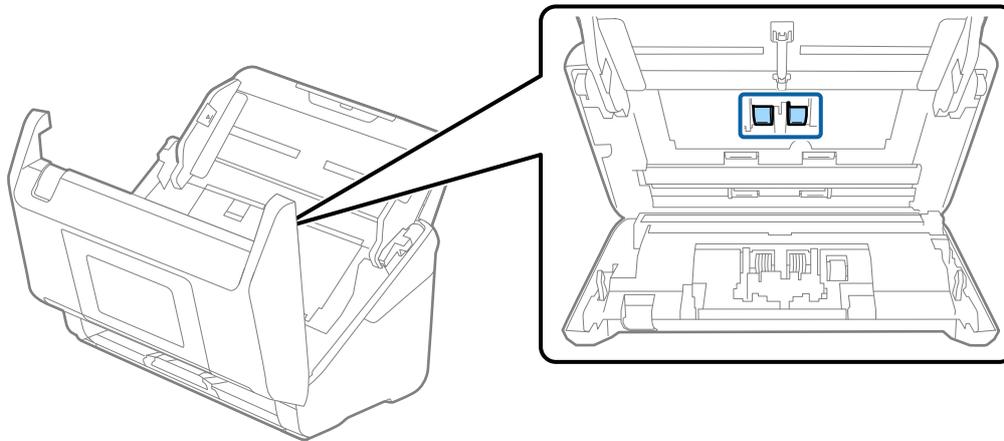
7. Wischen Sie die Trennwalze ab. Wischen Sie sie mit einem weichen, fusselfreien Tuch ab und feuchten Sie das Tuch mit einem speziellen Reinigungsmittel oder Wasser an.



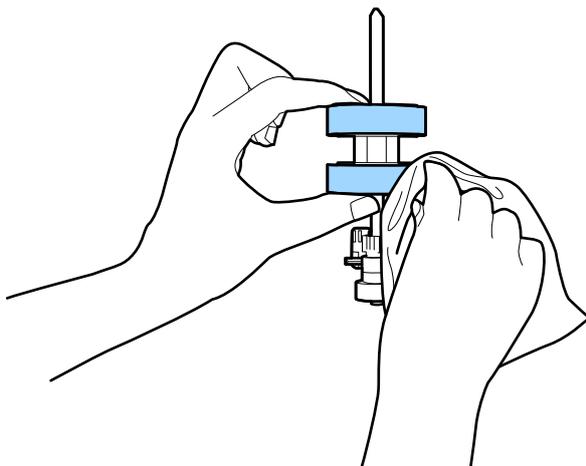
**Wichtig:**

*Verwenden Sie zum Reinigen des Rollers nur ein originales Epson-ReinigungsKit oder ein weiches, feuchtes Tuch. Ein trockenes Tuch kann die Walzenoberfläche beschädigen.*

- Öffnen Sie die Abdeckung und entfernen Sie die Aufnahmewalze.  
Einzelheiten hierzu finden Sie unter „Austauschen des Roller-Assembly-Kits“.



- Wischen Sie die Aufnahmewalze ab. Wischen Sie sie mit einem weichen, fusselfreien Tuch ab und feuchten Sie das Tuch mit einem speziellen Reinigungsmittel oder Wasser an.

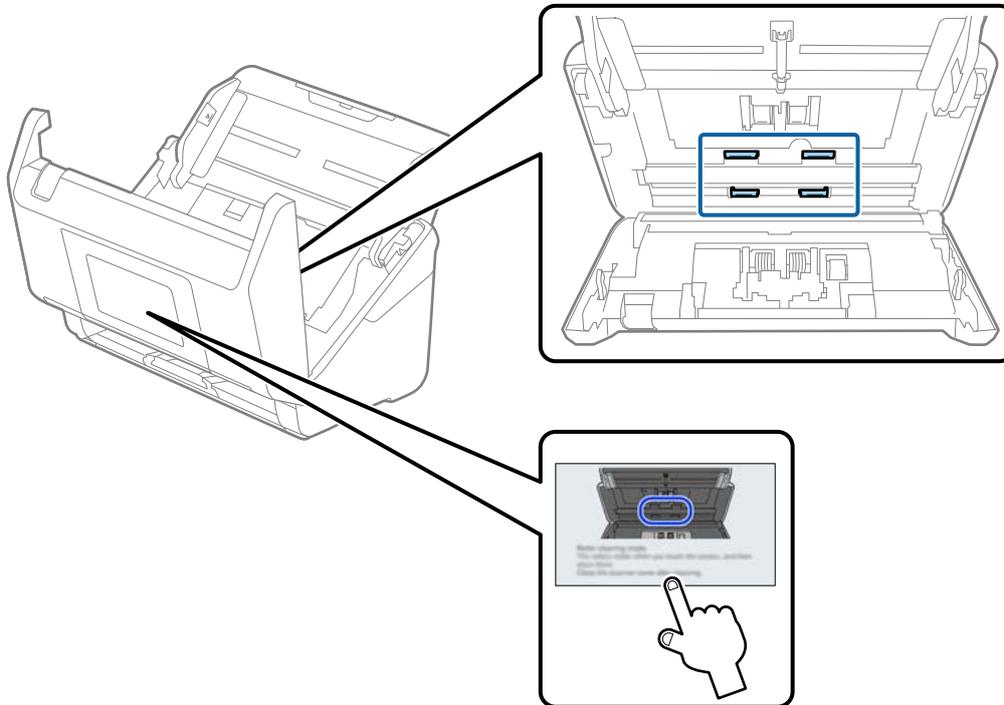


**Wichtig:**

Verwenden Sie zum Reinigen des Rollers nur ein originales Epson-Reinigungsset oder ein weiches, feuchtes Tuch. Ein trockenes Tuch kann die Walzenoberfläche beschädigen.

- Schließen Sie die Scannerabdeckung.
- Schließen Sie das Netzteil an und schalten Sie den Scanner ein.
- Wählen Sie **Wartung Scanner** auf dem Startbildschirm.
- Wählen Sie auf dem Bildschirm **Wartung Scanner** die Option **Walzenreinigung** aus.
- Ziehen Sie den Hebel, um die Scannerabdeckung zu öffnen.  
Der Scanner wechselt in den Walzenreinigungsmodus.

15. Drehen Sie die Walzen unten langsam, indem Sie auf den LCD-Bildschirm tippen. Wischen Sie die Oberfläche der Roller mit einem originalen Epson-Reinigungsset oder einem weichen, feuchten Tuch ab. Wiederholen Sie diesen Vorgang, bis die Walzen sauber sind.



**⚠ Achtung:**

*Achten Sie darauf, dass Ihre Hände oder Haare beim Betrieb der Walze nicht von der Mechanik eingezogen werden. Dies könnte zu Verletzungen führen.*

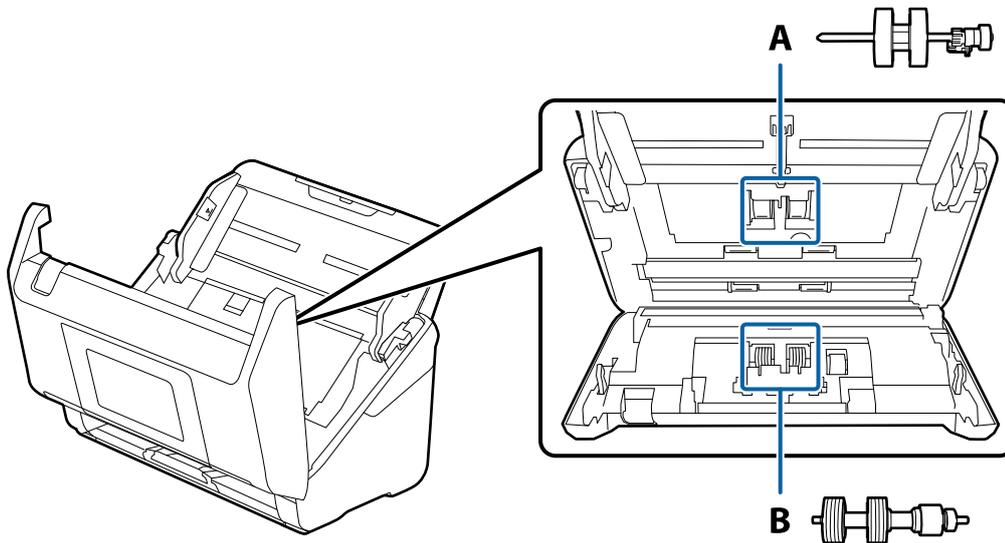
16. Schließen Sie die Scannerabdeckung.  
Der Scanner verlässt den Walzenreinigungsmodus.

**Zugehörige Informationen**

➔ „Austauschen des Roller-Assembly-Kits“ auf Seite 136

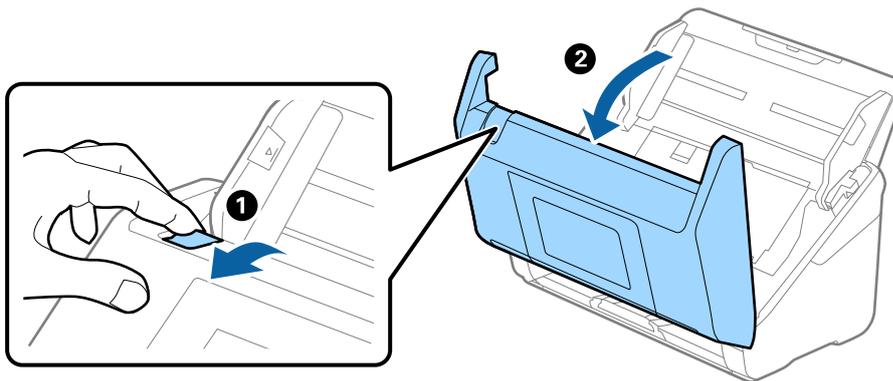
## Austauschen des Roller-Assembly-Kits

Das Roller-Assembly-Kit (Aufnahmewalze und Trennwalze) muss ausgetauscht werden, wenn die Anzahl der Scanvorgänge die Lebensdauer der Walzen überschreitet. Wenn die Meldung zum Austausch auf dem Bedienfeld angezeigt wird, befolgen Sie die folgenden Schritte, um das Kit auszutauschen.

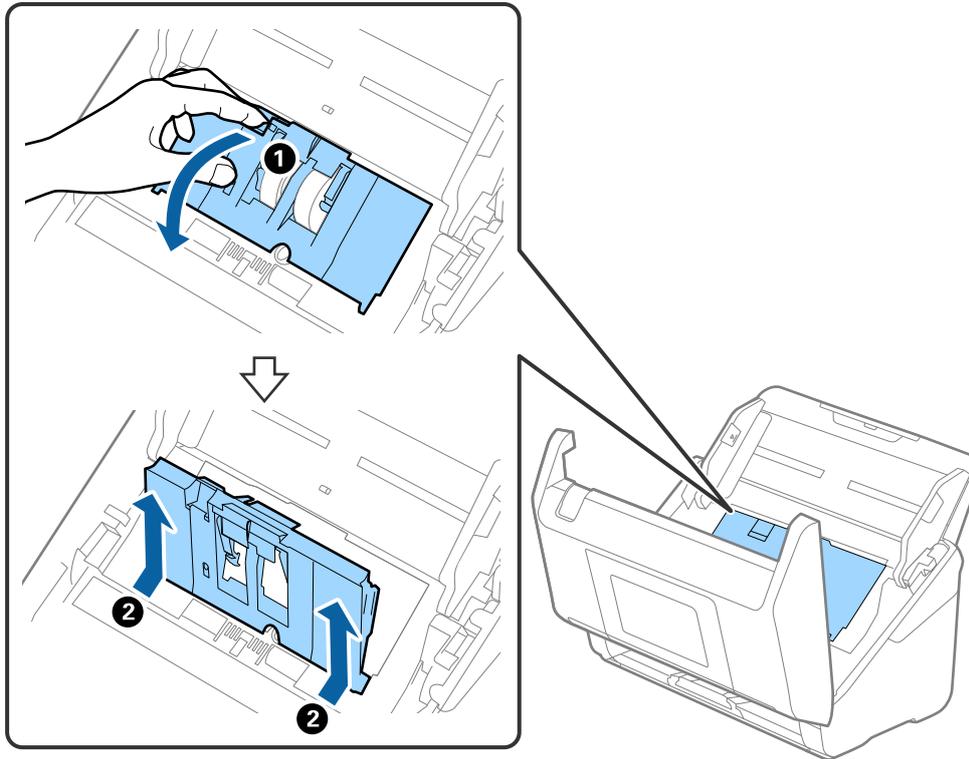


A: Aufnameroller, B: Trennroller

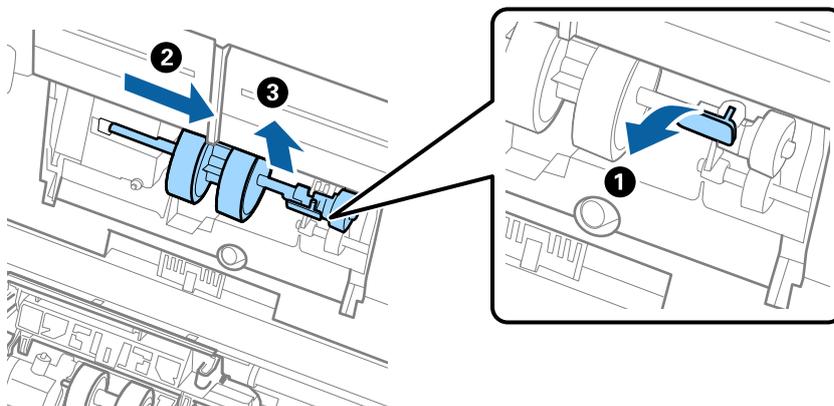
1. Drücken Sie zum Ausschalten des Scanners die Taste .
2. Trennen Sie das Netzkabel vom Scanner.
3. Ziehen Sie den Hebel und öffnen Sie die Scannerabdeckung.



4. Öffnen Sie die Abdeckung der Aufnahmelwalze, schieben Sie sie zur Zeit und entnehmen Sie die Walze.



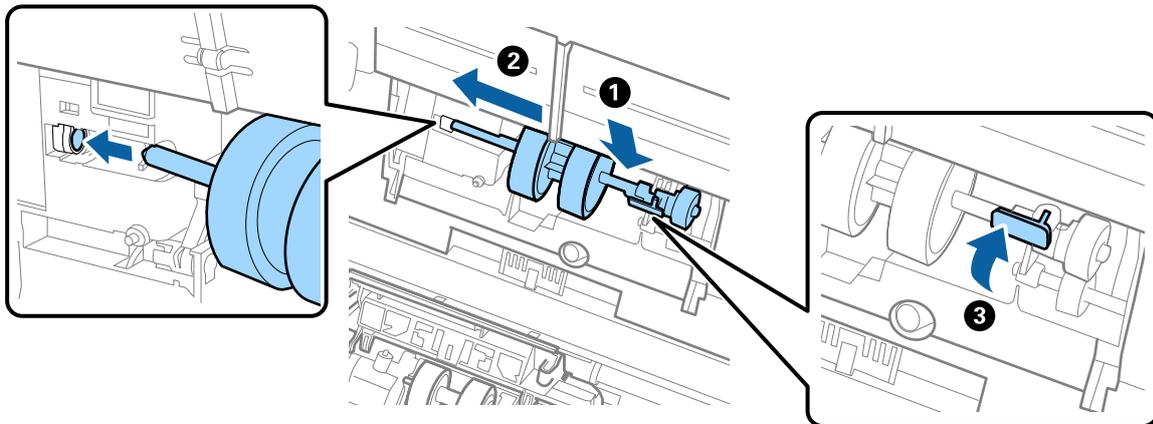
5. Ziehen Sie die Befestigung der Walzenachse herunter, schieben Sie sie zur Seite und entnehmen Sie die eingebaute Aufnahmelwalze.



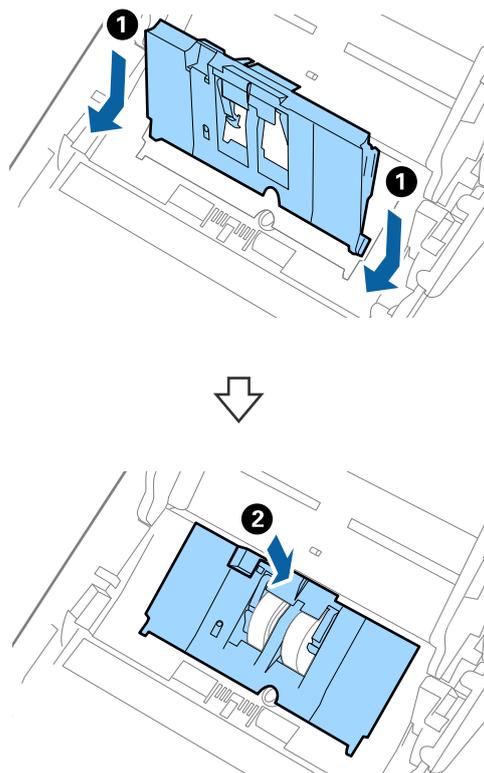
**Wichtig:**

Ziehen Sie die Aufnahmelwalze nicht fest heraus. Dadurch könnte das Innere des Scanners beschädigt werden.

6. Schieben Sie die neue Aufnahmewalze nach links, während Sie die Befestigung herunterhalten, und setzen Sie sie in die Öffnung im Scanner ein. Sichern Sie die Walze durch Verschließen der Befestigung.

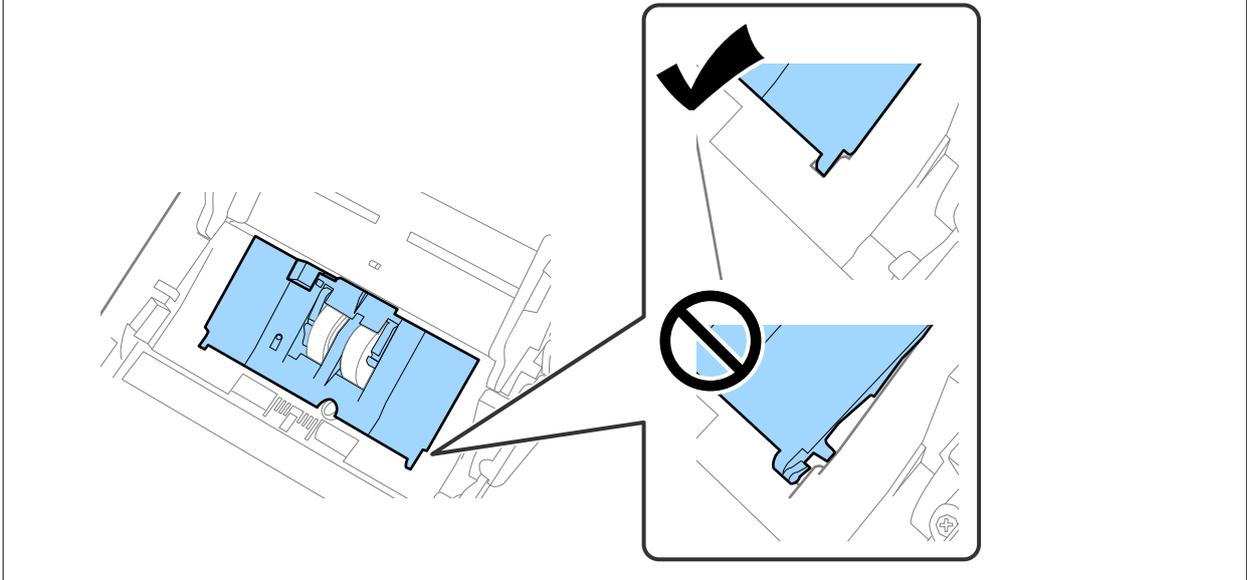


7. Setzen Sie den Rand der Abdeckung der Aufnahmewalze in die Rille und verschieben Sie ihn. Schließen Sie die Abdeckung fest.

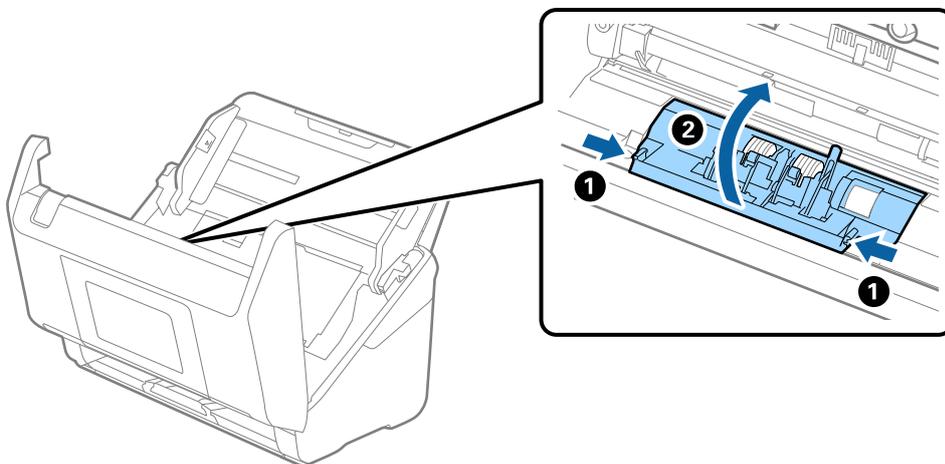


**!** Wichtig:

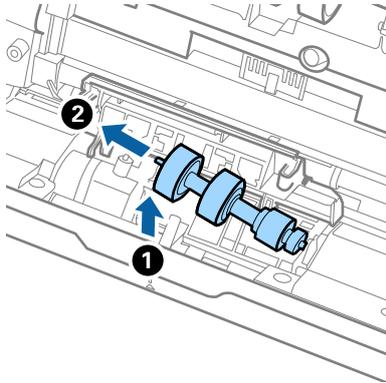
- Achten Sie darauf, dass die Abdeckung der Aufnahmewalze richtig geschlossen ist.
- Achten Sie darauf, dass die Aufnahmewalze richtig installiert ist, wenn die Abdeckung schwer zu schließen ist.
- Installieren Sie die Abdeckung nicht in aufgestellter Position.



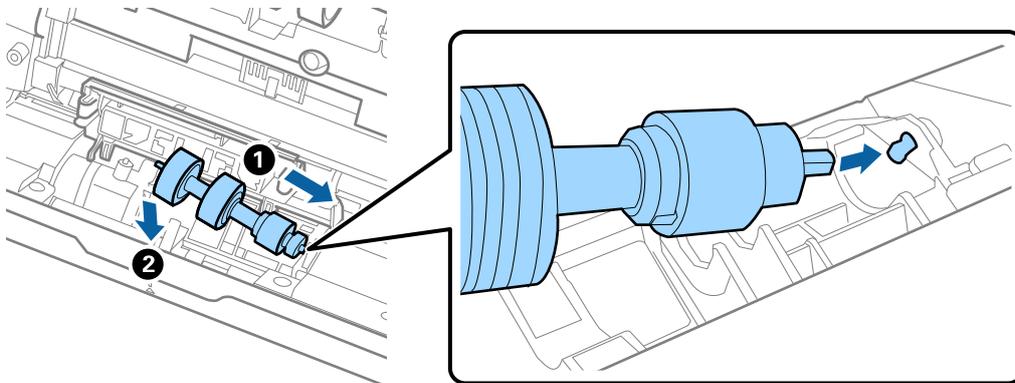
8. Drücken Sie die Haken an beiden Enden der Trennwälzenabdeckung, um die Abdeckung zu öffnen.



9. Heben Sie die linke Seite der Trennwalze an, verschieben Sie dann die eingebaute Trennwalze und entnehmen Sie sie.



10. Setzen Sie die neue Trennwalze in die Öffnung an der rechten Seite ein und senken Sie die Walze ab.



11. Schließen Sie die Trennwalzenabdeckung.



**Wichtig:**

*Wenn sich die Abdeckung nur schwer schließen lässt, stellen Sie sicher, dass die Trennwalzen korrekt montiert sind.*

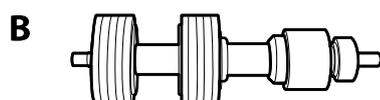
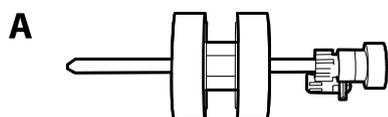
12. Schließen Sie die Scannerabdeckung.
13. Schließen Sie den Netzadapter an und schalten Sie den Scanner ein.
14. Setzen Sie die Anzahl der Scans auf dem Bedienfeld zurück.

**Hinweis:**

*Entsorgen Sie die Aufnahmewalze und die Trennwalze unter Beachtung der Regeln und Vorschriften der lokalen Behörden. Versuchen Sie nicht, Komponenten zu zerlegen.*

## Codes für Roller-Assembly-Kit

Die Teile (Aufnahmewalze und Trennwalze) sollten ausgetauscht werden, wenn die Anzahl der Scans die Serviceanzahl überschritten hat. Die aktuelle Anzahl durchgeführter Scans lässt sich auf dem Bedienfeld oder in Epson Scan 2 Utility überprüfen.



A: Aufnahmewalze, B: Trennwalze

Teilebez.	Codes	Lebensdauer in Zyklen
Roller-Assembly-Kit 2	B12B819711 B12B819721 (nur Indien)	200,000*

\* Diese Zahl wurde durch fortlaufendes Scannen von Epson-Testseiten ermittelt, und dient als Anhaltspunkt für den Austauschzeitpunkt. Der Austauschzyklus kann von den verschiedenen Papiersorten abhängen, beispielsweise bei Papier, das viel Abrieb erzeugt, oder durch raue Oberflächenstruktur die Nutzungsdauer herabsetzt.

---

## Zurücksetzen der Anzahl der Scans nach dem Austauschen der Rollen

Sie können die Anzahl der Scanvorgänge mit dem Bedienfeld oder mit Epson Scan 2 Utility zurücksetzen, nachdem das Roller-Assembly-Kit ausgetauscht wurde.

Dieser Abschnitt erklärt die Vorgehensweise beim Zurücksetzen mit dem Bedienfeld.

1. Tippen Sie auf dem Startbildschirm auf **Wartung Scanner**.
2. Tippen Sie auf **Walzenwechsel**.
3. Tippen Sie auf **Anzahl Scans rücksetzen**.
4. Wählen Sie **Anz. Scans n. Walzenwechsel** und tippen Sie dann auf **Ja**.

**Hinweis:**

Zum Zurücksetzen mit Epson Scan 2 Utility, starten Sie Epson Scan 2 Utility. Klicken Sie auf die Registerkarte **Zähler** und klicken Sie dann auf **Zurücksetzen in Rollenmontagekit**.

### Zugehörige Informationen

➔ [„Austauschen des Roller-Assembly-Kits“ auf Seite 136](#)

## Energie sparen

Sie können Energie sparen, indem Sie den Ruhemodus oder die automatische Abschaltfunktion nutzen, wenn keine Scanvorgänge durchgeführt werden. Die Zeitspanne, bevor der Scanner in den Ruhemodus wechselt oder sich automatisch abschaltet, lässt sich einstellen. Eine Erhöhung beeinträchtigt die Energieeffizienz des Produkts. Bitte denken Sie an die Auswirkungen auf die Umwelt, bevor Sie Änderungen vornehmen.

1. Wählen Sie auf dem Startbildschirm **Einstellungen**.
2. Wählen Sie **Grundeinstellungen** aus.
3. Wählen Sie **Schlaf-Timer** oder **AbschaltEinst.** und nehmen Sie die gewünschten Einstellungen vor.

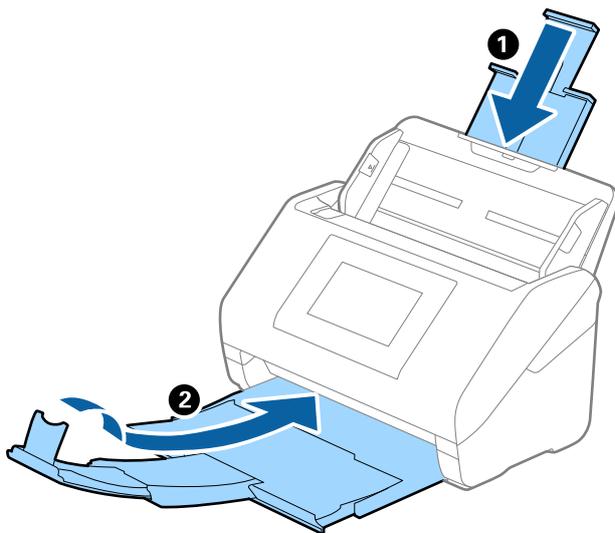
**Hinweis:**

*Die verfügbaren Funktionen können je nach dem Ort des Kaufs variieren.*

## Transportieren des Scanners

Wenn der Scanner am Standort oder für die Reparatur transportiert werden muss, verpacken Sie das Gerät wie folgt.

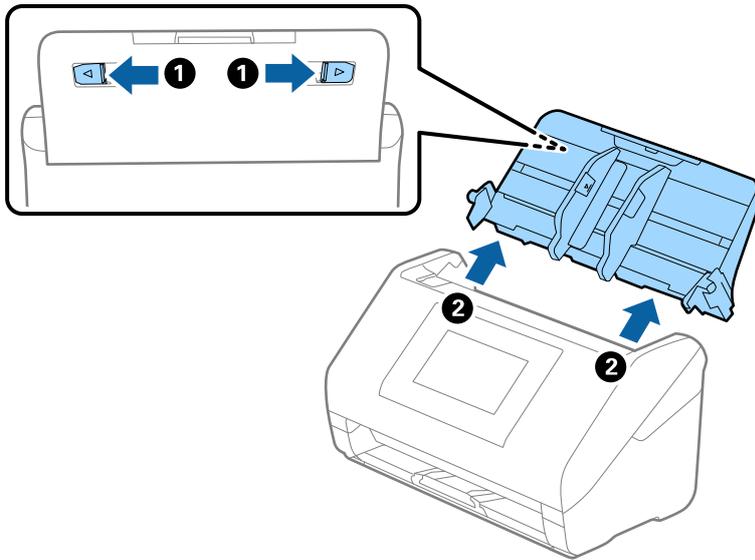
1. Drücken Sie zum Ausschalten des Scanners die -Taste.
2. Ziehen Sie den Netzadapter ab.
3. Entfernen Sie die Kabel und Geräte.  
Entfernen Sie ggf. die optionale oder im Lieferumfang enthaltene Paper Alignment Plate.
4. Schließen Sie die Eingabefachverlängerung und das Ausgabefach.



**Wichtig:**

Achten Sie darauf, das Ausgabefach sicher zu verschließen; andernfalls kann es beim Transport beschädigt werden.

5. Entfernen Sie das Eingabefach.



6. Sichern Sie den Scanner mit dem mitgelieferten Verpackungsmaterial und verpacken Sie ihn dann in seinem Original- oder einem robusten Karton.

---

## Sichern der Einstellungen

Die Einstellungen aus Web Config lassen sich in eine Datei exportieren. Diese Datei dient der Datensicherung von Kontakten, Einstellungen usw. und kann z. B. beim Auswechseln des Scanners wiederhergestellt werden.

Die exportierte Datei kann nicht bearbeitet werden, da sie als Binärdatei exportiert wird.

### Einstellungen exportieren

Exportieren Sie die Einstellung des Scanners.

1. Rufen Sie hierzu Web Config auf und öffnen Sie dann die Registerkarte **Geräteverwaltung > Einstellungswert exportieren und importieren > Exportieren**.

2. Wählen Sie die Einstellungen, die Sie exportieren möchten.

Wählen Sie die Einstellungen, die Sie exportieren möchten. Wenn Sie die übergeordnete Kategorie wählen, werden auch die Unterkategorien ausgewählt. Unterkategorien, die durch Duplikation innerhalb desselben Netzwerks Fehler verursachen (wie IP-Adressen usw.), können jedoch nicht ausgewählt werden.

3. Geben Sie ein Kennwort zur Verschlüsselung der exportierten Datei ein.

Sie benötigen das Kennwort, um die Datei zu importieren. Lassen Sie dies leer, wenn Sie die Datei nicht verschlüsseln möchten.

4. Klicken Sie auf **Exportieren**.



**Wichtig:**

*Wenn Sie die Netzwerkeinstellungen des Scanners, wie den Gerätenamen und die IPv6-Adresse, exportieren möchten, wählen Sie **Zur Auswahl der individuellen Geräteeinstellungen aktivieren** und dann weitere Elemente. Verwenden Sie nur die ausgewählten Werte für den Scanner.*

### Zugehörige Informationen

➔ „Ausführen von Web Config in einem Webbrowser“ auf Seite 40

## Importieren der Einstellungen

Importiert die exportierte Web Config-Datei in den Scanner.



**Wichtig:**

*Wenn Sie Werte importieren, die individuelle Informationen wie z. B. einen Scannernamen oder eine IP-Adresse enthalten, stellen Sie sicher, dass diese IP-Adresse nicht bereits im gleichen Netzwerk vorhanden ist.*

1. Navigieren Sie zu Web Config und wählen Sie dann die Registerkarte **Geräteverwaltung > Einstellungswert exportieren und importieren > Importieren**.
2. Wählen Sie die exportierte Datei und geben Sie dann das verschlüsselte Kennwort ein.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie die Einstellungen, die Sie importieren möchten und klicken Sie dann auf **Weiter**.
5. Klicken Sie auf **OK**.

Die Einstellungen werden auf den Scanner angewendet.

### Zugehörige Informationen

➔ „Ausführen von Web Config in einem Webbrowser“ auf Seite 40

---

## Werkseinstlg. wiederh.

Wählen Sie auf dem Bedienfeld **Einstellungen > Systemadministration > Werkseinstlg. wiederh.** aus, und wählen Sie dann die Elemente aus, die Sie auf die Standardwerte zurücksetzen möchten.

- Netzwerkeinstellungen: Setzen Sie netzwerkbezogene Einstellungen wieder in den Werkszustand zurück.
- Alles außer Netzwerkeinstellungen: Setzen Sie alle anderen Einstellungen außer netzwerkbezogene Einstellungen wieder in den Werkszustand zurück.
- Alle Einstellungen: Setzen Sie alle Einstellungen wieder in den Werkszustand zurück.



**Wichtig:**

Wenn Sie **Alle Einstellungen** auswählen und ausführen, werden alle im Scanner registrierten Einstellungsdaten, einschließlich der Kontakte, gelöscht. Gelöschte Einstellungen können nicht wiederhergestellt werden.

**Hinweis:**

Sie können die Einstellungen auch in Web Config vornehmen.

Registerkarte **Geräteverwaltung** > **Werkseinstellungen wiederherstellen**

---

## Aktualisieren von Anwendungen und Firmware

Durch Aktualisieren von Anwendungen und der Firmware lassen sich bestimmte Probleme beheben, Funktionen hinzufügen oder verbessern. Verwenden Sie stets die neuesten Versionen der Anwendungen und der Firmware.



**Wichtig:**

Schalten Sie Computer und Scanner nicht ab, solange die Aktualisierung läuft.

**Hinweis:**

Wenn der Scanner eine Internetverbindung herstellen kann, lässt sich die Firmware über Web Config aktualisieren. Wählen Sie die Registerkarte **Geräteverwaltung** > **Firmware-Update**, überprüfen Sie die angezeigte Meldung und klicken Sie dann auf **Start**.

1. Sorgen Sie dafür, dass Scanner und Computer miteinander verbunden sind und der Computer mit dem Internet verbunden ist.
2. Starten Sie EPSON Software Updater und aktualisieren Sie Anwendungen oder Firmware.

**Hinweis:**

Windows Server-Betriebssysteme werden nicht unterstützt.

Windows 11

Klicken Sie auf die Start-Schaltfläche und wählen Sie dann **Alle Apps** > **Epson Software** > **EPSON Software Updater**.

Windows 10

Klicken Sie auf die Start-Schaltfläche und wählen Sie **Epson Software** > **EPSON Software Updater**.

Windows 8.1/Windows 8

Geben Sie den Anwendungsnamen in den Charm „Suche“ ein und wählen Sie das angezeigte Symbol aus.

Windows 7

Klicken Sie auf die Start-Schaltfläche und wählen Sie dann **Alle Programme** oder **Programme** > **Epson Software** > **EPSON Software Updater**.

Mac OS

Wählen Sie **Finder** > **Gehe zu** > **Programme** > **Epson Software** > **EPSON Software Updater**.

**Hinweis:**

Wenn Sie die zu aktualisierende Anwendung nicht in der Liste finden, können Sie sie mit EPSON Software Updater nicht aktualisieren. Suchen Sie auf Ihrer lokalen Epson-Website nach den neuesten Versionen der Anwendungen.

<http://www.epson.com>

## Aktualisieren der Scannerfirmware über das Bedienfeld

Wenn der Scanner eine Internetverbindung hat, können Sie die Scannerfirmware über das Bedienfeld aktualisieren. Sie können auch einstellen, dass der Scanner regelmäßig nach Firmwareaktualisierungen sucht und Sie bei Verfügbarkeit benachrichtigt.

1. Wählen Sie auf dem Startbildschirm **Einstellungen**.
2. Wählen Sie **Systemadministration > Firmware-Aktualisierung > Aktualisierung**.

**Hinweis:**

Wählen Sie **Benachrichtigung > Ein**, um den Scanner auf regelmäßiges Prüfen auf verfügbare Firmwareaktualisierungen einzustellen.

3. Prüfen Sie die am Bildschirm angezeigten Meldungen und beginnen Sie mit der Suche nach verfügbaren Aktualisierungen.
4. Wenn auf dem LCD-Bildschirm die Meldung erscheint, dass eine Firmwareaktualisierung verfügbar ist, folgen Sie den Hinweisen auf dem Bildschirm, um die Aktualisierung zu starten.



**Wichtig:**

- Den Scanner nicht ausschalten oder trennen, bis die Aktualisierung abgeschlossen ist, andernfalls können Scannerfehlfunktionen auftreten.
- Wenn die Firmwareaktualisierung nicht abgeschlossen wird oder fehlschlägt, startet der Scanner nicht mehr normal und beim nächsten Einschalten erscheint „Recovery Mode“ auf dem LCD-Bildschirm. In diesem Fall muss die Firmware erneut mit einem Computer aktualisiert werden. Verbinden Sie den Scanner über ein USB-Kabel mit dem Computer. Solange „Recovery Mode“ am Scanner angezeigt wird, können Sie die Firmware nicht über eine Netzwerkverbindung aktualisieren. Rufen Sie vom Computer aus die lokale Epson-Website auf und laden Sie die neueste Scannerfirmware herunter. Informationen zu den weiteren Schritten finden Sie in der Anleitung auf der Website.

## Aktualisieren der Firmware mit Web Config

Wenn der Scanner eine Internetverbindung herstellen kann, lässt sich die Firmware über Web Config aktualisieren.

1. Wechseln Sie zu Web Config und wählen Sie die Registerkarte **Geräteverwaltung > Firmware-Update**.
2. Klicken Sie auf **Start** und folgen Sie dann den Anweisungen auf dem Bildschirm.

Die Firmware-Überprüfung beginnt, und die Firmware-Angaben werden angezeigt, falls eine aktualisierte Firmware vorhanden ist.

**Hinweis:**

Sie können die Firmware auch mithilfe von Epson Device Admin aktualisieren. In der Geräteliste lassen sich die Firmware-Angaben ablesen. Dies ist nützlich, wenn die Firmware mehrerer Geräte aktualisiert werden soll. Weitere Informationen finden Sie im Epson Device Admin-Handbuch oder in der Hilfe.

### Zugehörige Informationen

➔ [„Ausführen von Web Config in einem Webbrowser“](#) auf Seite 40

## Aktualisieren der Firmware ohne Internetverbindung

Sie können die Firmware für das Gerät von der Epson-Website auf den Computer herunterladen und über eine USB-Verbindung zwischen dem Computer und dem Gerät aktualisieren. If you cannot update over the network, try this method.

**Hinweis:**

*Stellen Sie vor der Aktualisierung sicher, dass der Scannertreiber Epson Scan 2 auf dem Computer installiert ist. Wenn Epson Scan 2 nicht installiert ist, installieren Sie es erneut.*

1. Suchen Sie auf der Epson-Website nach den Versionshinweisen zu den neuesten Firmware-Aktualisierungen.  
<http://www.epson.com>
  - Wenn Sie Firmware für den Scanner finden, laden Sie sie herunter und fahren mit dem nächsten Schritt fort.
  - Wenn Sie keine Firmware-Hinweise finden, ist auf dem Computer die neueste Firmware installiert.
2. Verbinden Sie den Computer, auf dem die Firmware gespeichert ist, über ein USB-Kabel mit dem Scanner.
3. Doppelklicken Sie auf die heruntergeladene EXE-Datei.  
Der Epson Firmware Updater wird gestartet.
4. Befolgen Sie die Anweisungen auf dem Bildschirm.