

Netzwerkhandbuch



Inhaltsverzeichnis

1	Einleitung	1
	Netzwerkfunktionen	1
	Andere Funktionen	2
2	Ändern der Netzwerkeinstellungen	3
	Ändern der Netzwerkeinstellungen des Gerätes	3
	Bedienfeld des Gerätes verwenden (ADS-2800W / ADS-3600W)	3
	So prüfen Sie den Netzwerkstatus (ADS-2800W / ADS-3600W)	3
	BRAdmin Light verwenden (Windows®)	3
	Weitere Verwaltungsprogramme	6
	Web-based Management	6
	BRAdmin Professional 3 (Windows®)	6
3	Konfigurieren Ihres Gerätes für ein Wireless-Netzwerk (ADS-2800W / ADS-3600W)	8
	Übersicht	8
	Prüfen der Netzwerkkumgebung	9
	Verbunden mit einem Computer über einen WLAN-Access-Point/Router im Netzwerk (Infrastruktur-Modus)	9
	Verbunden mit einem Wireless-Computer ohne WLAN-Access Point/Router im Netzwerk (Ad-hoc-Modus)	10
	Konfiguration	11
	Wenn die SSID nicht sendet	11
	Verwenden von WPS (Wi-Fi Protected Setup™)	18
	Verwenden der PIN-Methode des Wi-Fi Protected Setup™ (WPS)	19
	Konfiguration im Ad-hoc-Modus	22
	Verwenden einer konfigurierten SSID	22
	Konfigurieren des Gerätes für ein Wireless-Netzwerk über den Setup-Assistenten des Geräte- Bedienfelds	29
	Wi-Fi Direct® verwenden	31
	Von Ihrem Mobilgerät scannen mit Wi-Fi Direct®	31
	Ihr Wi-Fi Direct®-Netzwerk konfigurieren	32
	Übersicht über die Wi-Fi Direct®-Netzwerkkonfiguration	32
	Ihr Wi-Fi Direct®-Netzwerk mittels Tastendruck-Methode konfigurieren	33
	Ihr Wi-Fi Direct®-Netzwerk über die Tastendruck-Methode von Wi-Fi Protected Setup™ (WPS) konfigurieren	34
	Ihr Wi-Fi Direct®-Netzwerk mittels PIN-Methode konfigurieren	34
	Ihr Wi-Fi Direct®-Netzwerk über die PIN-Methode von Wi-Fi Protected Setup™ (WPS) konfigurieren	35
	Ihr Wi-Fi Direct®-Netzwerk manuell konfigurieren	37

4 Web-based Management 38

Übersicht.....	38
Konfiguration der Geräteeinstellungen	39
Festlegen eines Anmeldekennworts.....	40
Verwenden der LDAP-Authentifizierung.....	41
Einführung in die LDAP-Authentifizierung	41
Konfigurieren der LDAP-Authentifizierung mittels Web-based Management.....	41
Anmelden, um die Geräteeinstellungen über das Bedienfeld des Gerätes zu ändern.....	42
Einschränken von Benutzern.....	43
Konfigurieren der Active Directory LDAP-Authentifizierung (ADS-2800W / ADS-3600W).....	43
LDAP-Funktion (ADS-2800W / ADS-3600W).....	44
Ändern der LDAP-Konfiguration	44
Ändern der LDAP-Konfiguration über das Gerätebedienfeld (ADS-2800W / ADS-3600W).....	45
Synchronisieren mit dem SNTTP-Server.....	47
Ändern der Konfiguration Scannen: FTP.....	49
Ändern der Konfiguration Scannen: SFTP	50
Ändern der Konfiguration von Scan to SMB (Windows®)	52
Ändern der Konfiguration von Scannen: SharePoint (Windows®)	54
Konfigurieren der erweiterten TCP/IP-Einstellungen	56
Adressbuch importieren/exportieren (ADS-2800W / ADS-3600W)	58
Adressbuch importieren.....	58
Adressbuch exportieren.....	58

5 Scan to E-Mail-Server (ADS-2800W / ADS-3600W) 59

Übersicht.....	59
Größenbeschränkungen bei Scan to E-Mail-Server.....	59
Konfiguration von Scan to E-Mail-Server.....	60
Vor dem Scannen an E-Mail-Server.....	60
Informationen zur Verwendung von Scan to E-Mail-Server	61
Scan to E-Mail-Server: Weitere Funktionen	62
Bestätigungs-E-Mail	62

6 Sicherheitsfunktionen 63

Übersicht.....	63
Sicheres Versenden von E-Mails (ADS-2800W / ADS-3600W)	64
Konfiguration mit Web-based Management	64
Versenden von E-Mails mit Benutzerauthentifizierung.....	64
Sicheres Senden von E-Mails mit SSL/TLS	65
Sicherheitseinstellungen für SFTP	66
Erstellen eines Client-Schlüsselpaars	66
Exportieren eines Client-Schlüsselpaars.....	67
Importieren eines öffentlichen Serverschlüssels	68
Verwalten mehrerer Zertifikate	69
Importieren eines CA-Zertifikates	69
Sicheres Verwalten Ihres Netzwerkgerätes mit IPsec	71
Einführung in IPsec.....	71
IPsec mittels Web-based Management konfigurieren	72
IPsec-Adressvorlage mittels Web-based Management konfigurieren.....	73
IPsec-Vorlage mittels Web-based Management konfigurieren	74
IKEv1-Einstellungen für eine IPsec-Vorlage.....	75

IKEv2-Einstellungen für eine IPsec-Vorlage.....	77
Manuelle Einstellungen für eine IPsec-Vorlage.....	80
Einschränken von Scanfunktionen von externen Geräten.....	84
Einschränken von Scanfunktionen von externen Geräten über Webbrowser-Einstellungen	84
Benutzersperre 3.0 (ADS-2800W / ADS-3600W).....	85
Bevor Sie Benutzersperre 3.0 verwenden.....	85
Benutzersperre ein- und ausschalten.....	86
Konfigurieren der Benutzersperre 3.0 mit Web-based Management	86
Firmware-Update	87
7 Problemlösung	88
Übersicht.....	88
Identifizieren des Problems	88
8 Weitere Netzwerkeinstellungen (für Windows®)	98
Einstellungstypen.....	98
Installieren von Treibern zum Scannen über Webdienste (Windows Vista®, Windows® 7, Windows® 8, Windows® 8.1, Windows® 10)	98
Installation von Netzwerk-Scannen für den Infrastruktur-Modus mit Vertical Pairing (Windows® 7, Windows® 8, Windows® 8.1, Windows® 10).....	100
A Anhang	102
Unterstützte Protokolle und Sicherheitsfunktionen	102
Web-based Management Funktionstabelle	103
B Stichwortverzeichnis	112

Netzwerkfunktionen

Sie können das Brother-Gerät durch den integrierten Netzwerk-Scanserver gemeinsam mit anderen Benutzern in einem drahtlosen IEEE 802.11b/g/n Ethernet-Netzwerk verwenden. Der Scanserver unterstützt je nach Betriebssystem und Netzwerkkonfiguration verschiedene Funktionen und Anschlussarten. Die folgende Tabelle zeigt, welche Netzwerkfunktionen und -verbindungen von den einzelnen Betriebssystemen unterstützt werden:

Betriebssysteme	Windows® XP 32 Bit (SP3) Windows Vista® Windows® 7 Windows® 8 Windows® 8.1 Windows® 10 Windows Server® 2003 R2 32 Bit (SP2) Windows Server® 2008 Windows Server® 2008 R2 Windows Server® 2012 Windows Server® 2012 R2 Server-Betriebssystem unterstützt ausschließlich Scanvorgänge	OS X v10.8.5, 10.9.x, 10.10.x, 10.11.x
Scannen Siehe <i>Benutzerhandbuch</i> .	✓	✓
BRAdmin Light ¹ Siehe <i>BRAdmin Light verwenden (Windows®)</i> auf Seite 3.	✓	
BRAdmin Professional 3 ² Siehe <i>BRAdmin Professional 3 (Windows®)</i> auf Seite 6.	✓	
Web-based Management (Webbrowser) Siehe <i>Web-based Management</i> auf Seite 38.	✓	✓
Remote Setup Siehe <i>Benutzerhandbuch</i> .	✓	✓
Status Monitor Siehe <i>Benutzerhandbuch</i> .	✓	
Vertical Pairing (Vertikales Pairing) Siehe <i>Installation von Netzwerk-Scannen für den Infrastruktur-Modus mit Vertical Pairing (Windows® 7, Windows® 8, Windows® 8.1, Windows® 10)</i> auf Seite 100.	✓	

¹ BRAdmin Light ist als Download verfügbar unter support.brother.com

² BRAdmin Professional 3 ist als Download verfügbar unter support.brother.com

Andere Funktionen

LDAP (ADS-2800W / ADS-3600W)

Das LDAP-Protokoll ermöglicht auf Ihrem Computer die Suche nach Informationen wie z. B. E-Mail-Adressen. Wenn Sie die Funktion Scan to E-Mail-Server verwenden, können Sie über die LDAP-Suche nach E-Mail-Adressen suchen. (Siehe *Ändern der LDAP-Konfiguration über das Gerätebedienfeld (ADS-2800W / ADS-3600W)* auf Seite 45.)

Scan to E-Mail-Server (ADS-2800W/ADS-3600W)

Mit der Funktion Scan to E-Mail-Server können Sie gescannte Dokumente über das Internet versenden. (Siehe *Scan to E-Mail-Server (ADS-2800W / ADS-3600W)* auf Seite 59.)

Bevor Sie diese Funktion verwenden können, müssen Sie zunächst die erforderlichen Geräteeinstellungen über das Bedienfeld des Gerätes, über BRAdmin Professional 3 oder Web-based Management konfigurieren.

Sicherheit

Das Brother-Gerät verwendet moderne Protokolle zur Netzwerksicherheit und Datenverschlüsselung. (Siehe *Sicherheitsfunktionen* auf Seite 63.)

Wi-Fi Direct[®] (ADS-2800W / ADS-3600W)

Wi-Fi Direct[®] ist eine der von der Wi-Fi Alliance[®] entwickelten Konfigurationsmethoden für Wireless-Netzwerke. Bei dieser Verbindungsart handelt es sich um einen WLAN-Standard, der ohne einen Wireless Access Point eine Verbindung zwischen Geräten über ein gesichertes Verfahren zulässt. (Siehe *Wi-Fi Direct[®] verwenden* auf Seite 31.)

Ändern der Netzwerkeinstellungen des Gerätes

Die Netzwerkeinstellungen des Gerätes können über das Bedienfeld, BRAdmin Light, Web-based Management oder BRAdmin Professional 3 geändert werden.

Bedienfeld des Gerätes verwenden (ADS-2800W / ADS-3600W)

Sie können das Gerät zur Verwendung im Netzwerk über das Netzwerk-Menü des Funktionstastenfeldes konfigurieren.

So prüfen Sie den Netzwerkstatus (ADS-2800W / ADS-3600W)

- 1 Drücken Sie im Display des Gerätes auf .
- 2 Drücken Sie `Netzwerk`.
- 3 Drücken Sie `LAN (Kabel)`.
- 4 Drücken Sie `Status (Kabel)`.
- 5 Drücken Sie `Status`.

BRAdmin Light verwenden (Windows®)

Das Dienstprogramm BRAdmin Light wurde für die Ersteinrichtung von netzwerkfähigen Brother-Geräten entwickelt. In einer TCP/IP-Umgebung können Sie damit auch nach Brother-Geräten suchen, deren Status anzeigen und grundlegende Netzwerkeinstellungen konfigurieren, wie z. B. die IP-Adresse.

Installieren von BRAdmin Light

- 1 Stellen Sie sicher, dass das Gerät eingeschaltet ist.
- 2 Schalten Sie den Computer ein. Schließen Sie alle geöffneten Anwendungen.
- 3 Legen Sie die Installations-DVD in Ihr DVD-Laufwerk ein.
- 4 Doppelklicken Sie auf `(DVD-Laufwerk):\Tools\BRAdminLight\xxx\disk1\setup.exe`.

Ändern von IP-Adresse, Subnetzmaske und Gateway über BRAdmin Light

HINWEIS

- Laden Sie die neueste Version von BRAdmin Light über den **Downloads**-Bereich im Brother Solutions Center unter support.brother.com herunter.
- Wenn Sie für die Geräteverwaltung erweiterte Funktionen benötigen, benutzen Sie die neueste Version des Dienstprogramms BRAdmin Professional 3. Laden Sie BRAdmin Professional 3 aus dem **Downloads**-Bereich des Brother Solutions Center unter support.brother.com herunter. Dieses Dienstprogramm steht ausschließlich Nutzern von Windows® zur Verfügung.
- Wenn Sie die Firewall-Funktion einer Anti-Spyware oder Antiviren-Anwendung verwenden, sollten Sie diese vorübergehend deaktivieren. Sobald Sie sicher sind, dass Sie scannen können, aktivieren Sie die Anwendung wieder.
- Knotenname: Der Knotenname wird im aktuellen BRAdmin Light-Fenster angezeigt. Der Standardknotenname des Scanservers im Gerät ist „BRWxxxxxxxxxx“ für ein Wireless-Netzwerk („xxxxxxxxxx“ steht für die MAC-/Ethernet-Adresse Ihres Gerätes).
- Standardmäßig ist kein Kennwort erforderlich. Geben Sie ein möglicherweise festgelegtes Kennwort ein und drücken Sie **OK**.

1 Starten Sie BRAdmin Light.

- Windows® XP, Windows Vista® und Windows® 7

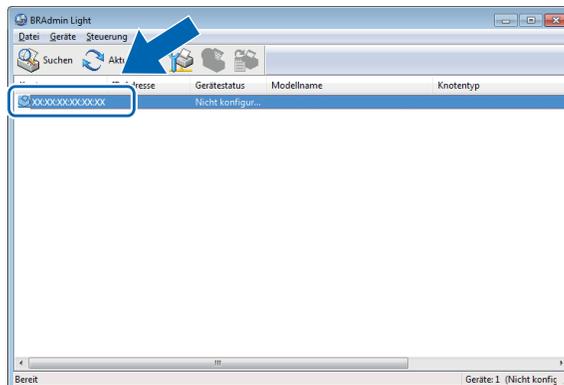
Klicken Sie auf  (**Start**) > **Alle Programme** > **Brother** > **BRAdmin Light** > **BRAdmin Light**.

- Windows® 8, Windows® 8.1 und Windows® 10

Klicken Sie in der Taskleiste auf  (**BRAdmin Light**).

2 BRAdmin Light sucht nun automatisch nach neuen Geräten.

- 3 Doppelklicken Sie auf Ihr Brother-Gerät.



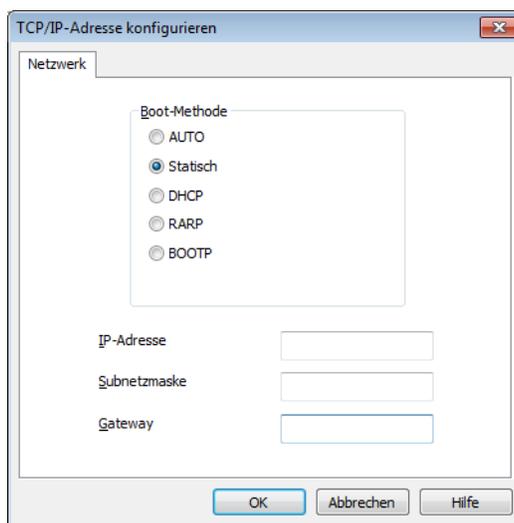
HINWEIS

- Wenn der Scanserver auf die werkseitigen Einstellungen eingestellt ist (und Sie keinen DHCP/BOOTP/RARP-Server verwenden), wird das Gerät unter BRAdmin Light als **Nicht konfiguriert** angezeigt.
- Sie können sich auf dem LCD-Display die MAC-Adresse (Ethernet-Adresse) und den Knotennamen Ihres Gerätes anzeigen lassen (ADS-2800W / ADS-3600W).

Um die MAC-Adresse zu ermitteln, drücken Sie  > Netzwerk > WLAN > MAC-Adresse.

Um den Knotennamen zu ermitteln, drücken Sie  > Netzwerk > WLAN > TCP/IP > Knotenname.

- 4 Wählen Sie **Statisch** aus der Liste Boot-Methode aus. Geben Sie die **IP-Adresse**, **Subnetzmaske** und, falls erforderlich, das **Gateway** Ihres Gerätes ein.



- 5 Klicken Sie auf **OK**.

- 6 Das Brother-Gerät erscheint in der Geräteliste. Sollte dies nicht der Fall sein, überprüfen Sie im Schritt 4 Ihre IP-Adresse.

Weitere Verwaltungsprogramme

Web-based Management

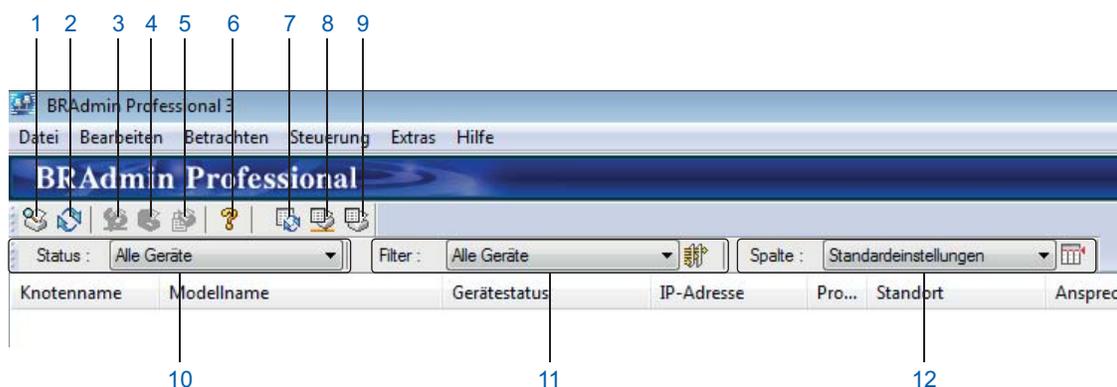
Sie können die Scanserver-Einstellungen über einen normalen Webbrowser und das HTTP-Protokoll (Hyper Text Transfer Protocol) oder HTTPS-Protokoll (Hyper Text Transfer Protocol Secure) ändern. (Siehe *Konfiguration der Geräteeinstellungen* auf Seite 39.)

BRAdmin Professional 3 (Windows®)

BRAdmin Professional 3 ist ein Dienstprogramm für die erweiterte Verwaltung von netzwerkfähigen Brother-Geräten. Dieses Dienstprogramm kann nach anderen Brother-Geräten in Ihrem Netzwerk suchen, die dann in einem übersichtlichen Fenster im Explorer-Stil angezeigt werden. Die Symbole ändern in Abhängigkeit vom Gerätestatus ihre Farbe. Außerdem können Sie über einen Windows®-Computer in Ihrem Netzwerk die Netzwerk- und Geräteeinstellungen ändern und die Firmware aktualisieren. BRAdmin Professional 3 kann auch die Aktivitäten von Brother-Geräten im Netzwerk protokollieren und die Protokolldaten in das HTML-, CSV-, TXT- oder SQL-Format exportieren.

HINWEIS

- Verwenden Sie die neueste Version des Dienstprogramms BRAdmin Professional 3. Laden Sie BRAdmin Professional 3 von Brother aus dem **Downloads**-Bereich des Brother Solutions Center unter support.brother.com herunter. Dieses Dienstprogramm steht ausschließlich Nutzern von Windows® zur Verfügung.
- Wenn Sie die Firewall-Funktion einer Anti-Spyware oder Antiviren-Anwendung verwenden, sollten Sie diese vorübergehend deaktivieren. Sobald Sie sicher sind, dass Sie scannen können, aktivieren Sie erneut die Anwendung.
- Knotenname: BRAdmin Professional 3 zeigt den Knotennamen für jedes im Netzwerk vorhandene Brother-Gerät an. Der Standardknotenname für ein Wireless-Netzwerk lautet „BRNxxxxxxxxxxxx“ (wobei „xxxxxxxxxxxx“ für die MAC-/Ethernet-Adresse Ihres Gerätes steht).



1 Netzwerk suchen

Führt in Ihrem Netzwerk eine Suche nach Geräten aus.

BRAdmin Professional ist so konfiguriert, dass alle unterstützten Netzwerkgeräte in Ihrem lokalen Netzwerk angezeigt werden, die mit einer gültigen IP-Adresse konfiguriert wurden.

2 Gerätestatus anzeigen (ALLE)

Aktualisiert den Status der Geräte, mit denen BRAdmin Professional kommuniziert.

3 Nicht konfigurierte Geräte einrichten

Wenn Ihr netzwerkfähiges Brother-Gerät nicht über eine gültige IP-Adresse verfügt, können Sie über BRAdmin Professional die IP-Adresse, Subnetzmaske, Gatewayadresse und Boot-Methode für Ihr Gerät einstellen.

4 Geräte-Homepage (Web-based Management)

Stellt eine Verbindung zum innerhalb des Gerätes eingebetteten Webserver her (bitte beachten Sie, dass nicht alle Geräte über einen eingebetteten Webserver verfügen).

5 Datei senden

Sendet eine Datei an ein Gerät.

6 Hilfethemen

Zeigt die Hilfedatei von BRAdmin Professional 3 an.

7 Protokoll aktualisieren

Aktualisiert die Protokoll-Chronik.

8 Netzwerkgeräte-Protokoll anzeigen

Zeigt die Protokollinfos aller im Netzwerk vorhandenen Geräte an.

9 Protokolle von lokalen Geräten anzeigen

Zeigt die Protokollinfos aller Geräte an, die mit den unter „Local Devices Log Settings“ (Protokolleinstellungen für lokale Geräte) registrierten Client-Computern verbunden sind.

10 Status

Wählen Sie einen Status aus der Dropdown-Liste aus.

11 Filter

Wählen Sie einen Filter aus der Dropdown-Liste aus.

Um einen Filter aus der Dropdown-Liste auszuwählen, müssen Sie vorher auf  klicken, um Menüs hinzuzufügen.

12 Spalte

Die Spalteneinstelloption ermöglicht Ihnen eine Auswahl der in der Hauptansicht von BRAdmin Professional anzuzeigenden Spalten.

HINWEIS

Für weitere Informationen zu BRAdmin Professional 3 klicken Sie auf  .

Konfigurieren Ihres Gerätes für ein Wireless-Netzwerk (ADS-2800W / ADS-3600W)

Übersicht

Zur Verbindung des Gerätes mit dem Wireless-Netzwerk empfehlen wir eine der folgenden Einrichtungsmethoden, die in der *Installationsanleitung* erläutert sind. Wählen Sie im Brother Solutions Center unter solutions.brother.com/manuals Ihr Gerät aus und laden Sie die *Installationsanleitung* herunter.

Weitere Informationen zu zusätzlichen Konfigurationsmethoden und Einstellungen für Wireless-Netzwerke finden Sie in diesem Kapitel. Informationen zu TCP/IP-Einstellungen finden Sie unter *Ändern der Netzwerkeinstellungen des Gerätes* auf Seite 3.

HINWEIS

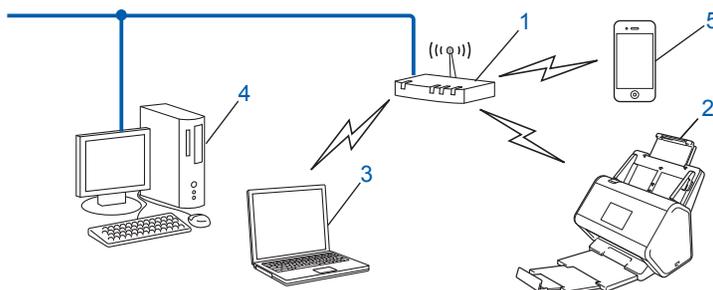
- Zur Erzielung optimaler Ergebnisse beim alltäglichen Scannen von Dokumenten sollten Sie das Brother-Gerät möglichst nah am WLAN-Access-Point/Router des Netzwerkes aufstellen und darauf achten, dass keine Hindernisse den Funkkontakt beeinträchtigen. Große Gegenstände und Wände zwischen den beiden Geräten sowie Funkstörungen durch andere elektronische Einrichtungen können die Geschwindigkeit der Datenübertragung beeinträchtigen.

Daher ist eine drahtlose Verbindung möglicherweise nicht die beste Verbindungsmethode zur Übertragung aller Arten von Dokumenten und Anwendungen. Wenn Sie große Dateien, z. B. mehrseitige Dokumente mit Text und großen Grafiken scannen, sollten Sie zum Erreichen einer höheren Übertragungsgeschwindigkeit eine USB-Verbindung wählen.

- Um die Wireless-Einstellungen konfigurieren zu können, müssen Sie Ihren Netzwerknamen (SSID) kennen und den Netzwerkschlüssel bereithalten.
-

Prüfen der Netzwerkumgebung

Verbunden mit einem Computer über einen WLAN-Access-Point/Router im Netzwerk (Infrastruktur-Modus)



1 WLAN-Access-Point/Router ¹

¹ Wenn Ihr Computer die My WiFi Technology (MWT) von Intel[®] unterstützt, können Sie Ihren Computer auch als Access-Point mit Wi-Fi Protected Setup™ (WPS) verwenden.

2 Wireless-Netzwerkgerät (Ihr Gerät)

3 Mit dem WLAN-Access-Point/Router verbundener, wireless-fähiger Computer

4 Verkabelter Computer (nicht wireless-fähig) über ein Netzwerkkabel mit dem WLAN-Access-Point/Router verbunden

5 Mit dem WLAN-Access-Point/Router verbundenes Mobilgerät

Konfigurationsmethode

Im Folgenden werden unterschiedliche Methoden zur Konfiguration des Brother-Gerätes in einer Wireless-Netzwerkumgebung beschrieben. Wählen Sie die für Ihre Umgebung bevorzugte Methode:

- Wireless-Konfiguration, vorübergehend (empfohlen). Siehe *Installationsanleitung*.
- Wireless-Konfiguration per Tastendruck mit WPS (Wi-Fi Protected Setup™). Siehe Seite 18.
- Wireless-Konfiguration mit PIN-Methode über WPS. Siehe Seite 19.
- Wireless-Netzwerk mit dem Setup-Assistenten konfigurieren. Siehe Seite 29.

So überprüfen Sie den WLAN-Status (ADS-2800W / ADS-3600W)

- 1 Drücken Sie im Display des Gerätes auf .
- 2 Drücken Sie Netzwerk.
- 3 Drücken Sie WLAN.
- 4 Drücken Sie ▲ oder ▼ und drücken Sie dann WLAN-Status.
- 5 Drücken Sie Status.

Verbunden mit einem Wireless-Computer ohne WLAN-Access Point/Router im Netzwerk (Ad-hoc-Modus)

Bei diesem Netzwerktyp gibt es keinen zentralen WLAN-Access-Point/Router. Jeder Wireless-Client kommuniziert direkt mit dem anderen. Wenn das Wireless-Gerät von Brother (Ihr Gerät) Teil dieses Netzwerkes ist, empfängt es alle Scanaufträge direkt von dem Computer, der die Scandaten sendet.



1 Wireless-Netzwerkgerät (Ihr Gerät)

2 Wireless-fähiger Computer

Wir garantieren nicht für eine Wireless-Netzwerkverbindung im Ad-hoc-Modus. Zum Einrichten Ihres Gerätes im Ad-hoc-Modus siehe *Konfiguration im Ad-hoc-Modus* auf Seite 22.

Konfiguration

Wenn die SSID nicht sendet

- 1 Vor der Konfiguration Ihres Gerätes sollten Sie sich die Wireless-Netzwerkeinstellungen notieren. Sie benötigen diese Informationen, um mit der Konfiguration fortfahren zu können. Überprüfen Sie die aktuellen Wireless-Netzwerkeinstellungen und notieren Sie sich diese.

Netzwerkname (SSID)

Kommunikationsmodus	Authentifizierungsmethode	Verschlüsselungsmodus	Netzwerkschlüssel
Infrastruktur	Offenes System	KEINE	—
		WEP	
	Shared key	WEP	
	WPA/WPA2-PSK	AES	
TKIP ¹			

¹ TKIP wird nur für WPA-PSK unterstützt.

Beispiel:

Netzwerkname (SSID)
HELLO

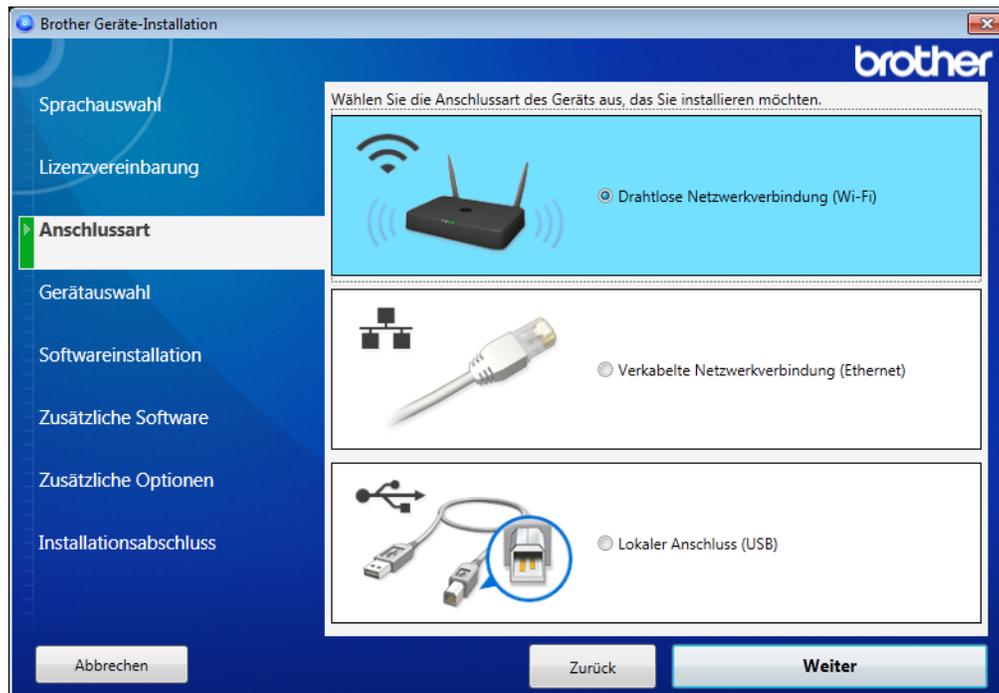
Kommunikationsmodus	Authentifizierungsmethode	Verschlüsselungsmodus	Netzwerkschlüssel
Infrastruktur	WPA2-PSK	AES	12345678

HINWEIS

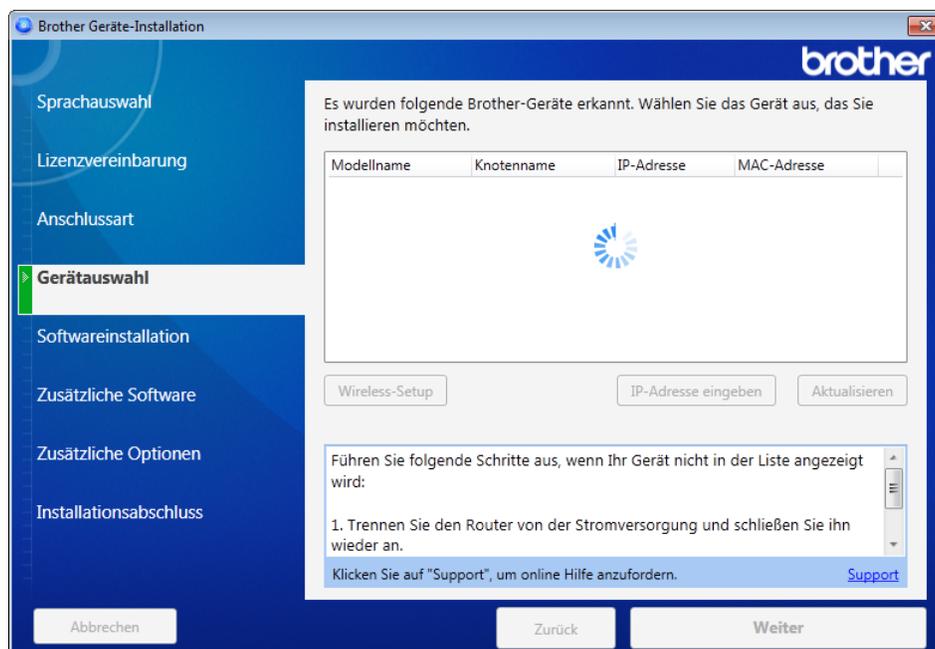
Wenn der Router die WEP-Verschlüsselung verwendet, geben Sie den als ersten WEP-Schlüssel benutzten Schlüssel ein. Das Brother-Gerät unterstützt nur die Verwendung des ersten WEP-Schlüssels.

2 Sie haben die folgenden Möglichkeiten:

- Windows®
 - a Legen Sie die mitgelieferte DVD in das DVD-Laufwerk ein.
 - b Wählen Sie **Drahtlose Netzwerkverbindung (Wi-Fi)** und klicken Sie auf **Weiter**.



c Klicken Sie auf **Wireless-Setup**.

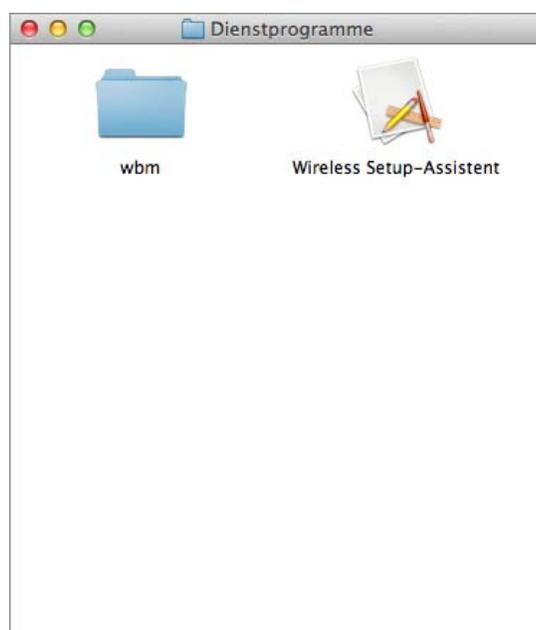


■ Macintosh

- a Laden Sie das gesamte Treiber- und Software-Paket von der Website des Brother Solutions Center (support.brother.com) herunter.
- b Doppelklicken Sie auf das **BROTHER**-Symbol auf dem Desktop.
- c Doppelklicken Sie auf **Dienstprogramme**.



- d Doppelklicken Sie auf **Wireless Setup-Assistent**.



- 3 Wählen Sie **Setup mit USB-Kabel (empfohlen)** und klicken Sie dann auf **Weiter**. Wir empfehlen die vorübergehende Verwendung eines USB-Kabels.



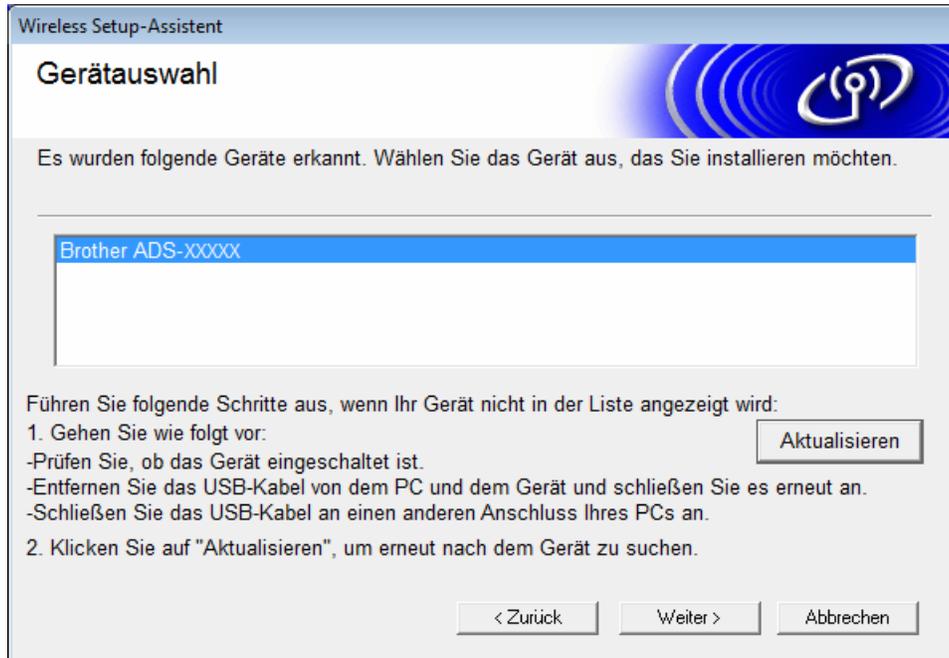
HINWEIS

Wenn diese Anzeige erscheint, müssen Sie den Text unter **Wichtiger Hinweis** lesen. Bestätigen Sie SSID und Netzwerkschlüssel, aktivieren Sie das Kontrollkästchen **Überprüft und bestätigt** und klicken Sie anschließend auf **Weiter**.



- 4 Schließen Sie vorübergehend das USB-Kabel direkt an den Computer und das Gerät an. Wenn der Bestätigungsbildschirm erscheint, klicken Sie auf **Weiter**.

5 Klicken Sie auf **Weiter**. (Nur Windows®)



6 Sie haben die folgenden Möglichkeiten:

- Wählen Sie die zu verwendende SSID und klicken Sie auf **Weiter**. Konfigurieren Sie anschließend den **Netzwerkschlüssel** und fahren Sie mit Schritt 10 fort.
- Wenn die von Ihnen zu verwendende SSID nicht sendet, klicken Sie auf **Erweitert** und fahren Sie mit Schritt 7 fort.



- 7 Geben Sie in das Feld **Name (SSID)** eine neue SSID ein und klicken Sie dann auf **Weiter**.

Wireless Setup-Assistent

Name des Wireless-Netzwerks

Geben Sie den Namen des Wireless-Netzwerks ein, mit dem das Gerät verbunden werden soll.

Name (SSID)

Dies ist ein Ad-hoc-Netzwerk und es gibt keinen Access Point.

Kanal

Hilfe < Zurück Weiter > Abbrechen

- 8 Wählen Sie **Authentifizierungsmethode** und **Verschlüsselungsmodus** aus den Dropdown-Listen aus, geben Sie in das Feld **Netzwerkschlüssel** einen Netzwerkschlüssel ein, klicken Sie auf **Weiter** und fahren Sie mit Schritt 10 fort.

Wireless Setup-Assistent

Authentifizierungs- und Verschlüsselungsmethoden

Geben Sie die gewünschte Authentifizierungsmethode und Verschlüsselungsart an.

Name (SSID):

Authentifizierungsmethode

Innere Authentifizierungsmethode

Verschlüsselungsmodus

Netzwerkschlüssel

Hilfe < Zurück Weiter > Abbrechen

- 9 Geben Sie in das Feld **Netzwerkschlüssel** einen neuen Netzwerkschlüssel ein und klicken Sie dann auf **Weiter**.

The screenshot shows the 'Wireless Setup-Assistent' window with the title 'Konfiguration des Netzwerkschlüssels'. It contains a text box for the network key and a button to find the key. Navigation buttons 'Hilfe', '< Zurück', 'Weiter >', and 'Abbrechen' are at the bottom.

Wireless Setup-Assistent

Konfiguration des Netzwerkschlüssels

Bitte geben Sie den zuvor ermittelten Netzwerksicherheitsschlüssel ein.

Wo finde ich meinen Netzwerkschlüssel?

Netzwerkschlüssel

Die in Ihrem Wireless-Netzwerk verwendete Authentifizierungs- und Verschlüsselungsmethode wird automatisch erkannt. Sie brauchen nur den Netzwerkschlüssel einzugeben.

Hilfe < Zurück Weiter > Abbrechen

- 10 Klicken Sie auf **Weiter**. Das Gerät empfängt nun die Einstellungen. (Die folgende Anzeige kann je nach Einstellungen anders aussehen.)

The screenshot shows the 'Wireless Setup-Assistent' window with the title 'Wireless-Netzwerkeinstellungen (WLAN) bestätigen'. It displays various network settings in a list format and a 'Weiter >' button highlighted in blue. Navigation buttons 'Hilfe', '< Zurück', 'Weiter >', and 'Abbrechen' are at the bottom.

Wireless Setup-Assistent

Wireless-Netzwerkeinstellungen (WLAN) bestätigen

Klicken Sie auf "Weiter", um die folgenden Einstellungen zum Gerät zu senden.

IP-Adresse	Auto	IP-Adresse ändern
Kommunikationsmodus	Infrastruktur	
Name (SSID)	XXXXXXXX	
Authentifizierungsmethode	Open System	
Verschlüsselungsmodus	Keiner	

Hilfe < Zurück Weiter > Abbrechen

HINWEIS

TRENNEN Sie die USB-Verbindung ERST, wenn auf dem Bildschirm bestätigt wird, dass die Konfiguration abgeschlossen ist und das Kabel sicher entfernt werden kann.

- 11 Trennen Sie das USB-Kabel vom Computer und vom Gerät.
- 12 Klicken Sie auf **Fertig stellen**.

Verwenden von WPS (Wi-Fi Protected Setup™)

- 1 Überprüfen Sie, ob Ihr Wireless Access Point/Router mit dem untenstehenden WPS-Symbol gekennzeichnet ist.

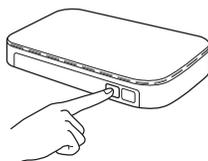


- 2 Platzieren Sie das Brother-Gerät in Reichweite des Wireless Access Points/-Routers. Die Reichweite kann je nach Umgebung unterschiedlich sein. Weitere Informationen erhalten Sie in der mit Ihrem Wireless Access Point/Router gelieferten Anleitung.
- 3 Drücken Sie im Display des Gerätes  > Netzwerk > WLAN > WPS.
Wenn WLAN aktivieren? angezeigt wird, drücken Sie zur Bestätigung Ja.

HINWEIS

- Starten Sie kurz nach Drücken der Taste WPS am Wireless Access Point/-Router am Gerätedisplay die Funktion WPS, da ansonsten der Verbindungsversuch möglicherweise scheitert.
- Falls der Wireless Access Point/Router WPS unterstützt, können Sie zur Konfiguration des Gerätes die PIN-Methode (Personal Identification Number) benutzen, siehe *Verwenden der PIN-Methode des Wi-Fi Protected Setup™ (WPS)* auf Seite 19.

- 4 Wenn das Display zu einem Start von WPS auffordert, müssen Sie am Wireless Access Point/-Router die Taste WPS drücken (weitere Informationen finden Sie in der mit dem Wireless Access Point/Router gelieferten Anleitung).



Drücken Sie OK auf dem Display des Brother-Gerätes.

- 5 Ihr Gerät erkennt automatisch, welchen Modus (WPS) Ihr Wireless Access Point/Router verwendet, und versucht, eine Verbindung mit Ihrem Wireless-Netzwerk herzustellen.
- 6 Wenn das Wireless-Gerät erfolgreich vernetzt wurde, erscheint im Display so lange die Nachricht *Verbunden*, bis Sie OK drücken.
Das Wireless-Setup ist jetzt abgeschlossen. Die Wi-Fi-LED  auf dem Bedienfeld leuchtet auf und signalisiert, dass die Netzwerkschnittstelle des Gerätes auf WLAN eingestellt ist.

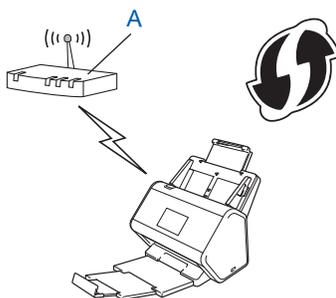
Verwenden der PIN-Methode des Wi-Fi Protected Setup™ (WPS)

Wenn der WLAN-Access-Point/Router das WPS (PIN-Methode) unterstützt, konfigurieren Sie das Gerät gemäß den Anweisungen.

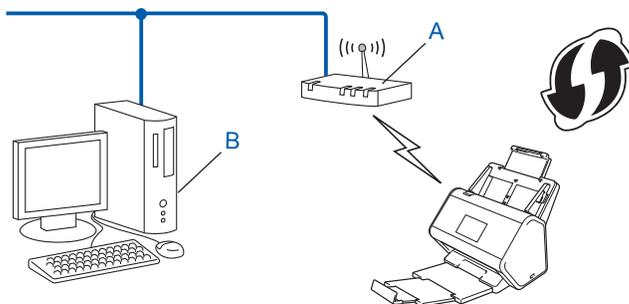
HINWEIS

Die PIN-Methode (Personal Identification Number) ist eine von der Wi-Fi Alliance® entwickelte Anschlussart. Das Wireless-Netzwerk und die Sicherheitseinstellungen können durch Übermittlung einer PIN, die von Ihrem Gerät (dem *Antragsteller*) erstellt wurde, an die *Registrierungsstelle* (das Gerät zum Verwalten des Wireless-LANs) eingerichtet werden. Informationen zum Zugriff auf den WPS-Modus finden Sie im *Benutzerhandbuch* des WLAN-Access-Points/Routers.

- Verbindung, wenn der WLAN-Access-Point/Router (A) auch als Registrierungsstelle fungiert ¹.



- Verbindung, wenn ein anderes Gerät (B), z. B. ein Computer, als Registrierungsstelle verwendet wird ¹.



¹ In der Regel ist der WLAN-Access-Point/Router die Registrierungsstelle.

HINWEIS

Router oder Access-Points, die WPS unterstützen, sind an folgendem Symbol zu erkennen:



- 1 Drücken Sie auf dem Gerätedisplay .
- 2 Drücken Sie **Netzwerk**.
- 3 Drücken Sie **WLAN**.
- 4 Drücken Sie **▲** oder **▼**, um **WPS + PIN-Code** anzuzeigen.
Drücken Sie **WPS + PIN-Code**.
- 5 Wenn **WLAN aktivieren?** angezeigt wird, drücken Sie zur Bestätigung **Ja**.
Der Wireless-Setup-Assistent wird gestartet.
Zum Abbrechen drücken Sie **Nein**.
- 6 Auf dem Display wird eine achtstellige PIN angezeigt und das Gerät beginnt mit der Suche nach einem Access-Point.
- 7 Geben Sie in der Adresszeile Ihres Browsers die IP-Adresse Ihres Access Points (Registrierungsstelle ¹) ein.
¹ In der Regel ist der WLAN-Access-Point/Router die Registrierungsstelle.
- 8 Gehen Sie zur WPS-Einstellungsseite, geben Sie die in Schritt 6 im Display angezeigte PIN für die Registrierungsstelle ein und folgen Sie dann den Anweisungen auf dem Bildschirm.

HINWEIS

- Die Einstellungsseite sieht je nach Modell des verwendeten Access-Points/Routers unterschiedlich aus. Siehe Benutzerhandbuch des Access-Points/Routers.
- Um einen Windows Vista[®]-, Windows[®] 7-, Windows[®] 8-, Windows[®] 8.1 oder Windows[®] 10-Computer als Registrierungsstelle verwenden zu können, müssen Sie diesen zunächst im Netzwerk registrieren. Siehe Benutzerhandbuch des WLAN-Access-Points/Routers.
- Wenn Sie einen Windows[®] 7-, Windows[®] 8-, Windows[®] 8.1 oder Windows[®] 10-Computer als Registrierungsstelle verwenden, können Sie nach der Wireless-Konfiguration den Scannertreiber mit Hilfe der folgenden Bildschirmanweisungen installieren. Wenn Sie das gesamte Treiber- und Softwarepaket installieren möchten, führen Sie die in der *Installationsanleitung* beschriebenen Schritte aus.

Windows Vista[®] / Windows[®] 7 / Windows[®] 8 / Windows[®] 8.1 / Windows[®] 10

Falls Sie den Computer als Registrierungsstelle verwenden, gehen Sie wie folgt vor:

a Windows Vista[®]

Klicken Sie auf  (**Start**) > **Netzwerk** > **Ein Drahtlosgerät hinzufügen**.

Windows[®] 7

Klicken Sie auf  (**Start**) > **Geräte und Drucker** > **Gerät hinzufügen**.

Windows[®] 8 und Windows[®] 8.1

Bewegen Sie die Maus in die untere rechte Ecke. Klicken Sie in der Menüleiste auf **Einstellungen** > **Systemsteuerung** > **Geräte und Drucker** > **Gerät hinzufügen**.

Windows[®] 10

Klicken Sie auf  (**Start**) > **Einstellungen** > **Geräte** > **Angeschlossene Geräte** > **Gerät hinzufügen**.

b Wählen Sie das Gerät aus und klicken Sie auf **Weiter**.

- c Geben Sie die im Schritt 6 im Display angezeigte PIN ein und klicken Sie dann auf **Weiter**.
- d Wählen Sie das Netzwerk aus, zu dem Sie eine Verbindung herstellen möchten, und klicken Sie auf **Weiter**.
- e Klicken Sie auf **Schließen**.

- 9 Wenn das Wireless-Gerät erfolgreich eine Verbindung aufgebaut hat, wird im Display *Verbunden* angezeigt.
Bei einer fehlgeschlagenen Verbindung wird im Display ein Fehlercode angezeigt. Notieren Sie den Fehlercode, siehe *WLAN-Fehlercodes (ADS-2800W / ADS-3600W)* auf Seite 90, und beheben Sie den Fehler.

 **Windows®**

Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Um mit der Installation der Treiber und der Software, die für den Betrieb des Gerätes erforderlich sind, fortzufahren, legen Sie die DVD-ROM in Ihr DVD-Laufwerk ein.

HINWEIS

Falls der Brother-Bildschirm nicht automatisch angezeigt wird, klicken Sie auf  **(Start) > Computer (Arbeitsplatz)**. (Bei Windows® 8, Windows® 8.1, Windows® 10 klicken Sie in der Taskleiste auf das Symbol  **(Explorer)** und wählen Sie dann **Dieser Computer / Dieser PC**.) Doppelklicken Sie auf das DVD-Symbol und anschließend auf **start.exe**.

Macintosh

Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Zum Fortfahren der Installation von Treiber und Software, die für den Gerätebetrieb erforderlich sind, wählen Sie aus dem Treibermenü **Start Here OSX** aus.

Konfiguration im Ad-hoc-Modus

Verwenden einer konfigurierten SSID

Wenn Sie versuchen, das Gerät mit einem Computer zu koppeln, der sich bereits im Ad-hoc-Modus mit einer konfigurierten SSID befindet, führen Sie die folgenden Schritte durch:

- 1 Vor der Konfiguration Ihres Gerätes sollten Sie sich die Wireless-Netzwerkeinstellungen notieren. Sie benötigen diese Informationen, um mit der Konfiguration fortfahren zu können. Überprüfen und notieren Sie die aktuellen Wireless-Netzwerkeinstellungen des Computers, zu dem Sie eine Verbindung herstellen möchten.

HINWEIS

Für die Wireless-Netzwerkeinstellungen des Computers, zu dem Sie eine Verbindung herstellen möchten, muss der Ad-hoc-Modus mit bereits konfigurierter SSID festgelegt sein. Weitere Informationen zur Konfiguration des Computers für den Ad-hoc-Modus finden Sie in der mit dem Computer mitgelieferten Dokumentation, oder wenden Sie sich an Ihren Netzwerkadministrator.

Netzwerkname (SSID)

Kommunikationsmodus	Verschlüsselungsmodus	Netzwerkschlüssel
Ad-hoc	KEINE	—
	WEP	

Beispiel:

Netzwerkname (SSID)
HELLO

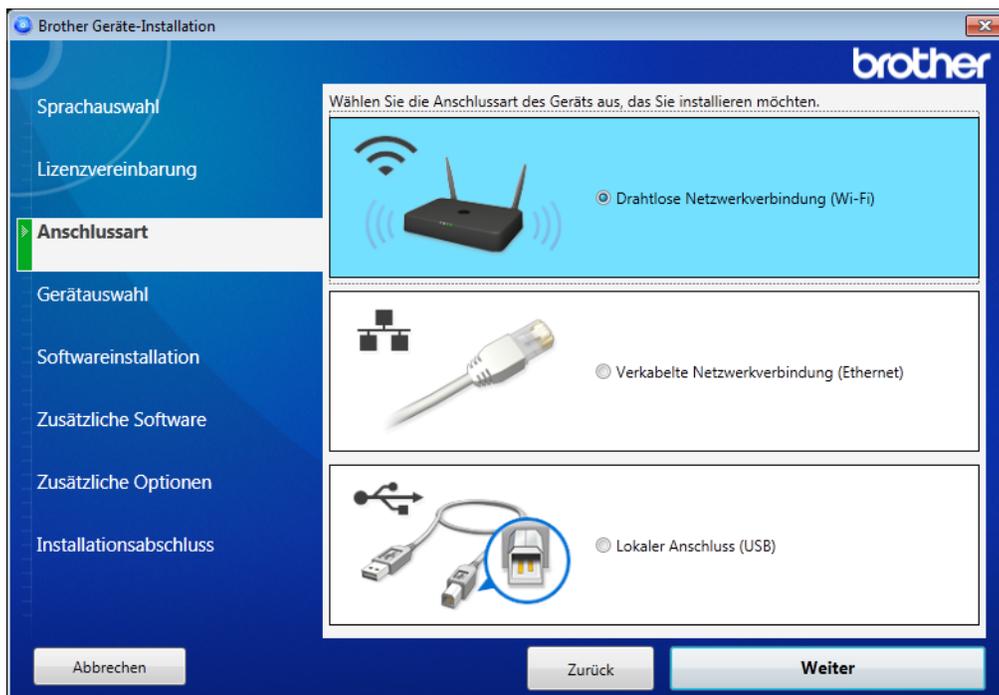
Kommunikationsmodus	Verschlüsselungsmodus	Netzwerkschlüssel
Ad-hoc	WEP	12345

HINWEIS

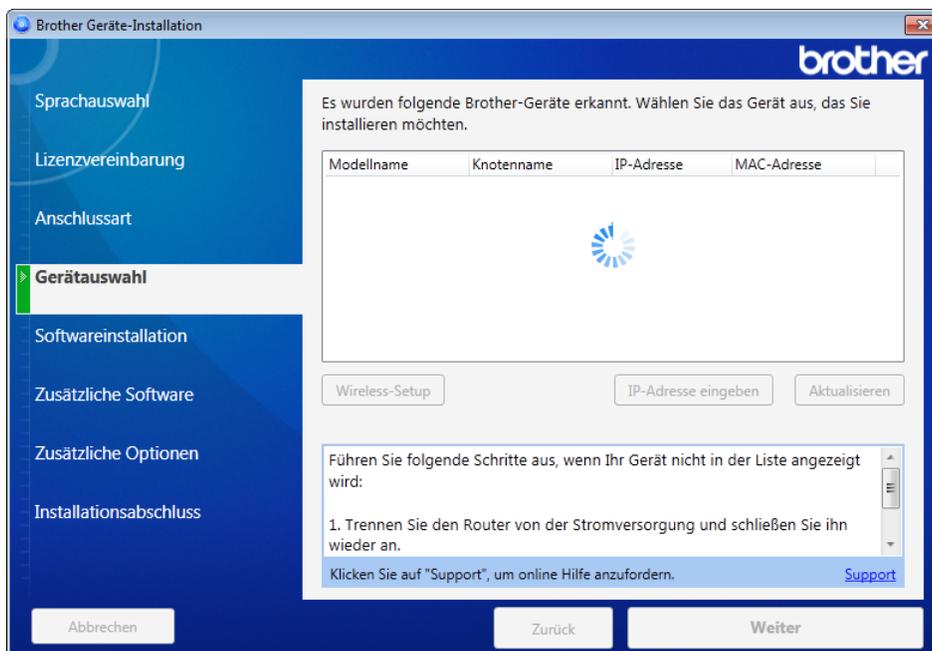
Das Brother-Gerät unterstützt nur die Verwendung des ersten WEP-Schlüssels.

2 Sie haben die folgenden Möglichkeiten:

- Windows®
 - a Legen Sie die mitgelieferte DVD in das DVD-Laufwerk ein.
 - b Wählen Sie **Drahtlose Netzwerkverbindung (Wi-Fi)** und klicken Sie auf **Weiter**.



c Klicken Sie auf **Wireless-Setup**.

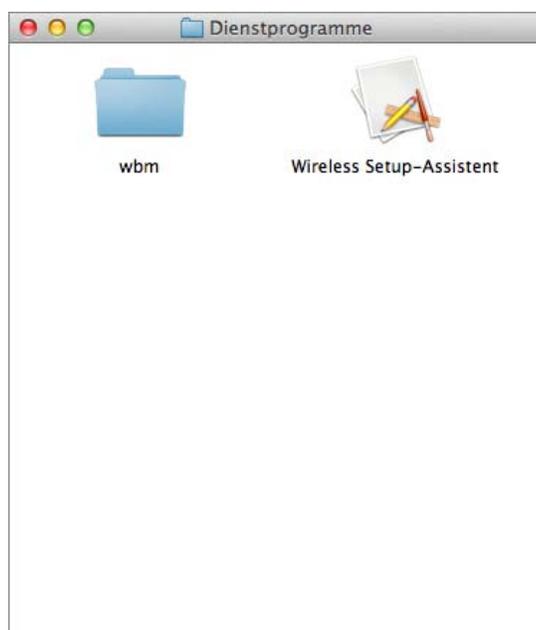


■ Macintosh

- a Laden Sie das gesamte Treiber- und Software-Paket von der Website des Brother Solutions Center (support.brother.com) herunter.
- b Doppelklicken Sie auf das **BROTHER**-Symbol auf dem Desktop.
- c Doppelklicken Sie auf **Dienstprogramme**.



- d Doppelklicken Sie auf **Wireless Setup-Assistent**.



- Wählen Sie **Setup mit USB-Kabel (empfohlen)** und klicken Sie dann auf **Weiter**. Wir empfehlen die vorübergehende Verwendung eines USB-Kabels.



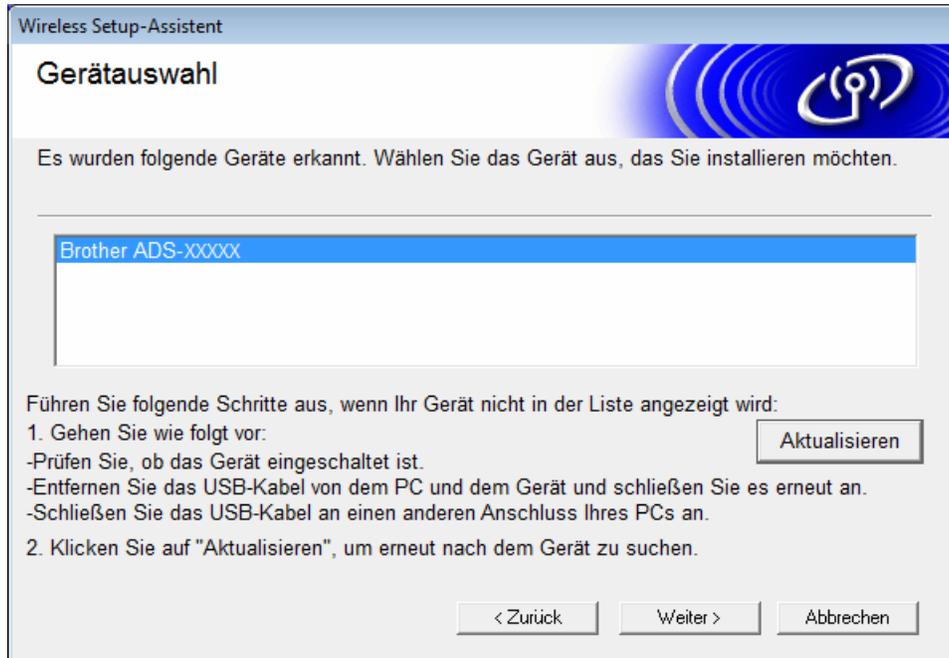
HINWEIS

Wenn diese Anzeige erscheint, müssen Sie den Text unter **Wichtiger Hinweis** lesen. Bestätigen Sie SSID und Netzwerkschlüssel, aktivieren Sie das Kontrollkästchen **Überprüft und bestätigt** und klicken Sie anschließend auf **Weiter**.



- Schließen Sie vorübergehend das USB-Kabel direkt an den Computer und das Gerät an. Wenn der Bestätigungsbildschirm erscheint, klicken Sie auf **Weiter**.

5 Klicken Sie auf **Weiter**. (Nur Windows®)



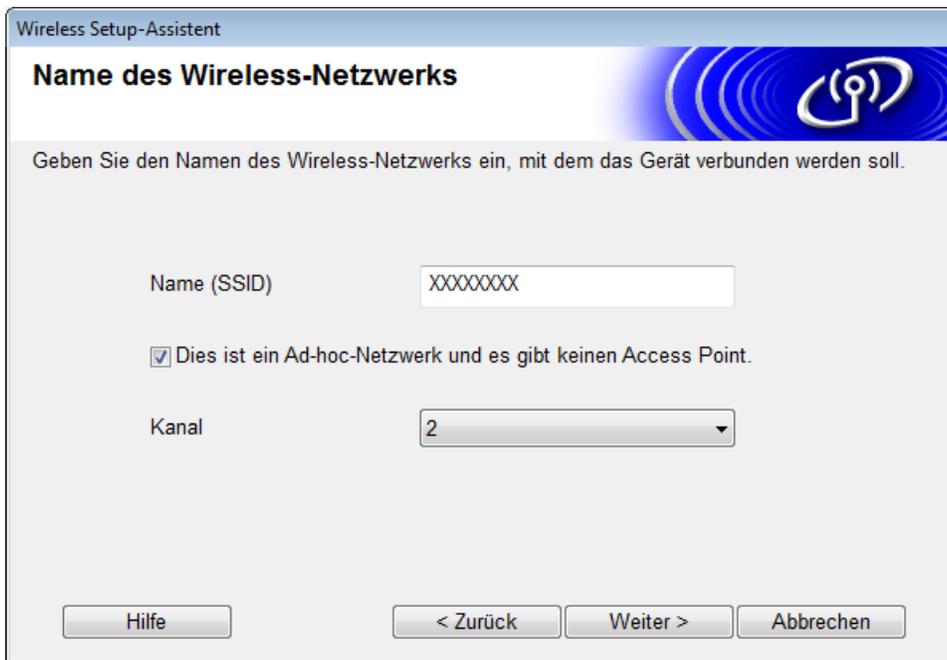
6 Klicken Sie auf **Erweitert**.



HINWEIS

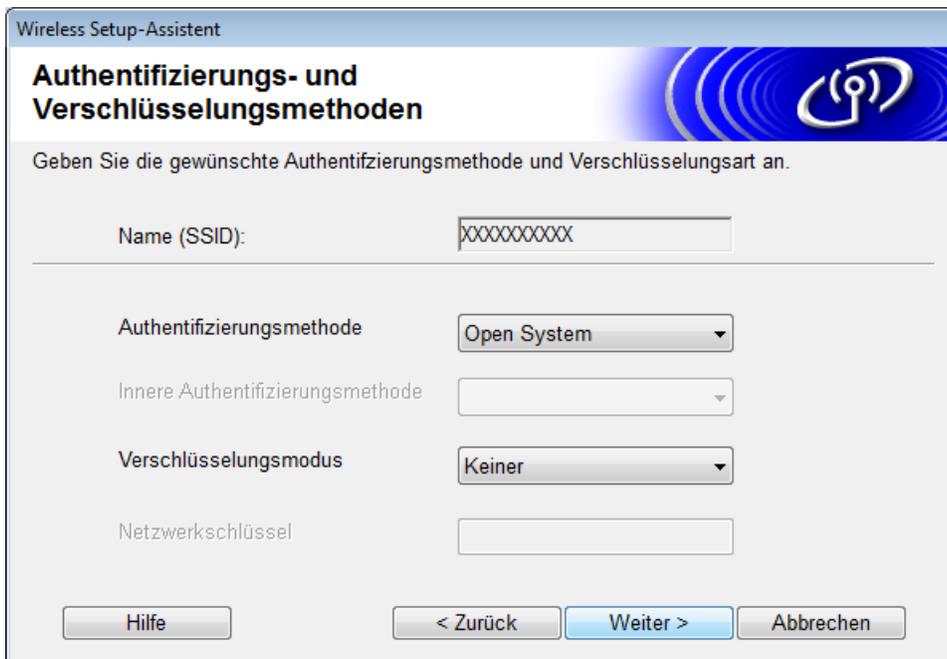
Sollte die Liste leer sein, überzeugen Sie sich, dass der Access-Point eingeschaltet ist und die SSID sendet. Prüfen Sie anschließend, ob sich das Gerät und der Computer in Reichweite für die drahtlose Kommunikation befinden. Klicken Sie anschließend auf **Aktualisieren**.

- 7 Aktivieren Sie das Kontrollkästchen **Dies ist ein Ad-hoc-Netzwerk und es gibt keinen Access Point** und klicken Sie anschließend auf **Weiter**.



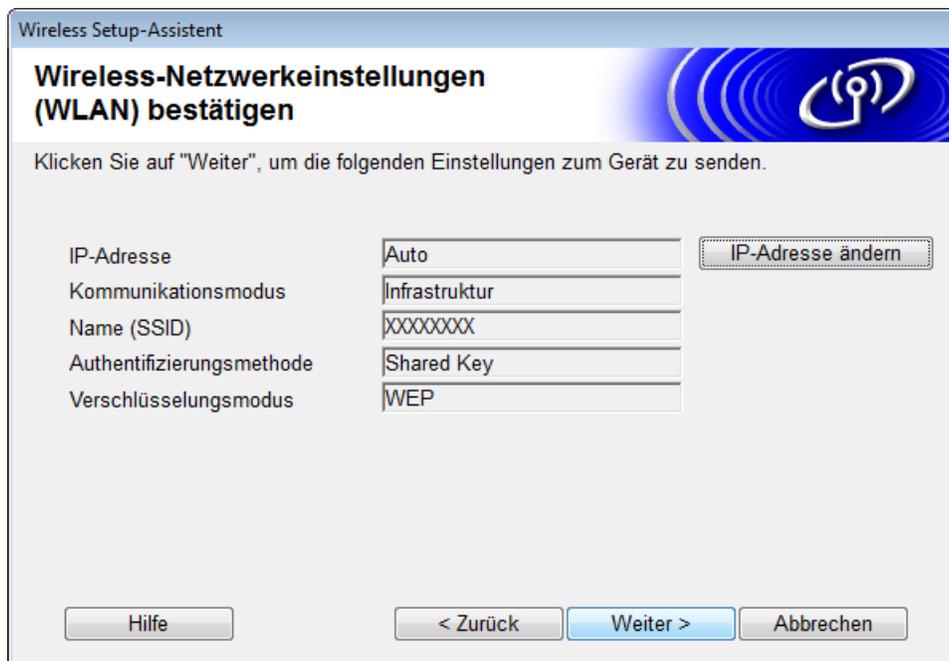
The screenshot shows the 'Wireless Setup-Assistent' window with the title 'Name des Wireless-Netzwerks'. Below the title is a blue decorative header with a wireless signal icon. The main text reads: 'Geben Sie den Namen des Wireless-Netzwerks ein, mit dem das Gerät verbunden werden soll.' There are three input fields: 'Name (SSID)' containing 'XXXXXXXX', a checked checkbox labeled 'Dies ist ein Ad-hoc-Netzwerk und es gibt keinen Access Point.', and 'Kanal' set to '2'. At the bottom are buttons for 'Hilfe', '< Zurück', 'Weiter >', and 'Abbrechen'.

- 8 Wählen Sie aus den Dropdown-Listen die **Authentifizierungsmethode** und den **Verschlüsselungsmodus** aus, geben Sie in das Feld **Netzwerkschlüssel** einen Netzwerkschlüssel ein und klicken Sie dann auf **Weiter**.



The screenshot shows the 'Wireless Setup-Assistent' window with the title 'Authentifizierungs- und Verschlüsselungsmethoden'. Below the title is a blue decorative header with a wireless signal icon. The main text reads: 'Geben Sie die gewünschte Authentifizierungsmethode und Verschlüsselungsart an.' There are four input fields: 'Name (SSID):' containing 'XXXXXXXXXX', 'Authentifizierungsmethode' set to 'Open System', 'Innere Authentifizierungsmethode' (empty), and 'Verschlüsselungsmodus' set to 'Keiner'. Below these is a 'Netzwerkschlüssel' field (empty). At the bottom are buttons for 'Hilfe', '< Zurück', 'Weiter >', and 'Abbrechen'.

- 9 Klicken Sie auf **Weiter**. Das Gerät empfängt nun die Einstellungen. (Der Verschlüsselungsmodus lautet im folgenden Beispiel WEP.)



The screenshot shows a window titled "Wireless Setup-Assistent" with a blue header. Below the header, the text "Wireless-Netzwerkeinstellungen (WLAN) bestätigen" is displayed in bold. A sub-header reads: "Klicken Sie auf 'Weiter', um die folgenden Einstellungen zum Gerät zu senden." The main area contains five rows of settings, each with a label on the left and a text input field on the right:

IP-Adresse	Auto	<input type="button" value="IP-Adresse ändern"/>
Kommunikationsmodus	Infrastruktur	
Name (SSID)	XXXXXXXX	
Authentifizierungsmethode	Shared Key	
Verschlüsselungsmodus	WEP	

At the bottom of the window, there are four buttons: "Hilfe", "< Zurück", "Weiter >" (highlighted in blue), and "Abbrechen".

- 10 Trennen Sie das USB-Kabel vom Computer und vom Gerät.
- 11 Klicken Sie auf **Fertig stellen**.

Konfigurieren des Gerätes für ein Wireless-Netzwerk über den Setup-Assistenten des Geräte-Bedienfelds

Vor der Konfiguration Ihres Gerätes sollten Sie sich die Wireless-Netzwerkeinstellungen notieren. Sie benötigen diese Informationen, um mit der Konfiguration fortfahren zu können.

- 1 Überprüfen Sie die aktuellen Wireless-Netzwerk-Einstellungen des Computers, mit dem Sie eine Verbindung herstellen möchten, und notieren Sie diese.

Netzwerkname (SSID)

Netzwerkschlüssel

Beispiel:

Netzwerkname (SSID)
HELLO

Netzwerkschlüssel
12345

HINWEIS

- Ihr Access Point/Router unterstützt möglicherweise die Verwendung mehrerer WEP-Schlüssel, wobei Ihr Brother-Gerät jedoch ausschließlich die Verwendung des ersten WEP-Schlüssels unterstützt.
- Wenn Sie beim Setup Hilfe benötigen und den Brother-Kundenservice kontaktieren möchten, halten Sie die SSID (Netzwerkname) und den Netzwerkschlüssel bereit. Diese Informationen können ausschließlich Sie ermitteln.
- Sie benötigen diese Informationen (SSID und Netzwerkschlüssel), um mit dem Wireless-Setup fortfahren zu können.

Wie kann ich diese Informationen ermitteln?

- a Lesen Sie die mit Ihrem Wireless Access Point/Router mitgelieferte Dokumentation.
- b Die standardmäßige SSID kann der Name des Herstellers oder die Modellbezeichnung sein.
- c Wenn Sie die Sicherheitsdaten nicht kennen, wenden Sie sich an den Hersteller des Routers, an Ihren Systemadministrator oder Ihren Internet-Provider.

- 2 Drücken Sie im Display des Brother-Gerätes  > Netzwerk > WLAN > Setup-Assist.
- 3 Das Gerät führt eine Netzwerksuche aus und zeigt anschließend eine Auflistung der verfügbaren SSIDs an. Drücken Sie nach Anzeige der SSIDs auf ▲ oder ▼, um die für die Verbindung gewünschte SSID anzuzeigen. Anschließend drücken Sie auf die SSID.
- 4 Drücken Sie OK.

5 Sie haben die folgenden Möglichkeiten:

- Wenn Sie eine Authentifizierungs- und Verschlüsselungsmethode verwenden, die einen Netzwerkschlüssel benötigt, dann geben Sie den im ersten Schritt notierten Netzwerkschlüssel ein. Nachdem Sie alle Zeichen eingegeben haben, drücken Sie **OK** und anschließend **Ja**, um Ihre Einstellungen anzuwenden.
- Lautet Ihre Authentifizierungsmethode „Offenes System“ und Ihr Verschlüsselungsmodus **Keine**, führen Sie den nächsten Schritt aus.
- Falls Ihr WLAN-Access-Point/Router WPS unterstützt, wird **Der ausgewählte Access Point/Router unterstützt WPS. WPS verwenden? angezeigt. Um Ihr Gerät über den automatischen Wireless-Modus zu verbinden, drücken Sie Ja. (Haben Sie Nein (manuell) gewählt, geben Sie den im ersten Schritt notierten Netzwerkschlüssel ein.) Wenn WPS auf Ihrem Wireless Access Point/Router starten, dann [Weiter] drücken. angezeigt wird, drücken Sie an Ihrem WLAN-Access-Point/Router die WPS-Taste und drücken Sie dann Weiter.**

6 Das Gerät versucht einen Verbindungsaufbau zu dem von Ihnen gewählten Wireless-Gerät.

Hat Ihr Wireless-Gerät erfolgreich eine Verbindung aufgebaut, zeigt das Gerätedisplay **Verbunden an**.

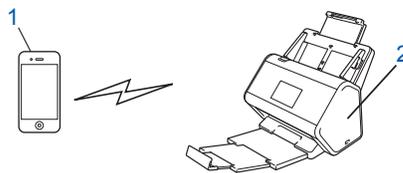
Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Für eine Installation von Treiber und Software, die für den Gerätebetrieb erforderlich sind, legen Sie die Installations-DVD in das DVD-Laufwerk Ihres Computers ein oder rufen Sie Ihr Modell unter **Downloads** im Brother Solutions Center unter support.brother.com auf.

Wi-Fi Direct[®] verwenden

- Von Ihrem Mobilgerät scannen mit Wi-Fi Direct[®]
- Ihr Wi-Fi Direct[®]-Netzwerk konfigurieren
- Ihre Wi-Fi Direct[®]-Netzwerkeinstellungen vom Bedienfeld Ihres Gerätes konfigurieren

Von Ihrem Mobilgerät scannen mit Wi-Fi Direct[®]

Wi-Fi Direct[®] ist eine der von der Wi-Fi Alliance[®] entwickelten Konfigurationsmethoden für Wireless-Netzwerke. Mithilfe von Wireless Direct können Sie ohne einen Access Point ein gesichertes drahtloses Netzwerk zwischen Ihrem Brother-Gerät und einem Mobilgerät wie etwa einem Android[™]-Gerät, Windows[®] Phone-Gerät, iPhone, iPod touch oder iPad herstellen. Wi-Fi Direct[®] unterstützt eine Wireless-Netzwerk-Konfiguration über die Tastendruck-Methode, die PIN-Methode oder das Wi-Fi Protected Setup[™] (WPS). Sie können ein Wireless-Netzwerk auch manuell über die Eingabe von SSID und Kennwort konfigurieren. Die Wi-Fi Direct[®]-Funktion Ihres Brother-Gerätes unterstützt den Sicherheitsstandard WPA2[™] mit AES-Verschlüsselung.



- 1 Mobilgerät
- 2 Ihr Brother-Gerät

HINWEIS

- Obwohl das Brother-Gerät sowohl in einem verkabelten als auch in einem Wireless-Netzwerk eingesetzt werden kann, ist immer nur eine der beiden Verbindungsarten möglich. Ein Anschluss über ein Wireless-Netzwerk und Wi-Fi Direct[®] oder ein Anschluss über ein verkabeltes Netzwerk und Wi-Fi Direct[®] können jedoch gleichzeitig verwendet werden.
- Das von Wi-Fi Direct[®] unterstützte Gerät kann als Gruppenbesitzer (G/B) fungieren. Bei der Konfiguration des Wi-Fi Direct[®]-Netzwerks dient der G/B als Access Point.
- Der Ad-hoc-Modus und Wi-Fi Direct[®] können nicht gleichzeitig verwendet werden. Deaktivieren Sie die eine Funktion, um die andere zu aktivieren. Um Wi-Fi Direct[®] während des Ad-hoc-Modus zu nutzen, müssen Sie Netzwerk I/F auf „LAN (Kabel)“ einstellen oder den Ad-hoc-Modus deaktivieren und Ihr Brother-Gerät an den Access Point anschließen.

Ihr Wi-Fi Direct®-Netzwerk konfigurieren

Konfigurieren Sie Ihre Wi-Fi Direct®-Netzwerkeinstellungen vom Bedienfeld Ihres Gerätes.

■ Übersicht über die Wi-Fi Direct®-Netzwerkconfiguration

Folgende Anweisungen beschreiben fünf Methoden zur Konfiguration Ihres Brother-Gerätes in einer Wireless-Netzwerkumgebung. Wählen Sie die für Ihre Umgebung bevorzugte Methode aus.

- Ihr Wi-Fi Direct®-Netzwerk mittels Tastendruck-Methode konfigurieren
- Ihr Wi-Fi Direct®-Netzwerk über die Tastendruck-Methode von Wi-Fi Protected Setup™ (WPS) konfigurieren
- Ihr Wi-Fi Direct®-Netzwerk mittels PIN-Methode konfigurieren
- Ihr Wi-Fi Direct®-Netzwerk über die PIN-Methode von Wi-Fi Protected Setup™ (WPS) konfigurieren
- Ihr Wi-Fi Direct®-Netzwerk manuell konfigurieren

Übersicht über die Wi-Fi Direct®-Netzwerkconfiguration

Folgende Anweisungen beschreiben fünf Methoden zur Konfiguration Ihres Brother-Gerätes in einer Wireless-Netzwerkumgebung. Wählen Sie die für Ihre Umgebung bevorzugte Methode aus.

Überprüfen Sie Ihr zu konfigurierendes Mobilgerät.

1 Unterstützt Ihr Mobilgerät Wi-Fi Direct®?

Option	Beschreibung
Ja	Gehen Sie zu Schritt 2.
Nein	Gehen Sie zu Schritt 3.

2 Unterstützt Ihr Mobilgerät die Tastendruck-Methode für Wi-Fi Direct®?

Option	Beschreibung
Ja	Siehe <i>Ihr Wi-Fi Direct®-Netzwerk mittels Tastendruck-Methode konfigurieren</i> auf Seite 33.
Nein	Siehe <i>Ihr Wi-Fi Direct®-Netzwerk mittels PIN-Methode konfigurieren</i> auf Seite 34.

3 Unterstützt Ihr Mobilgerät Wi-Fi Protected Setup™ (WPS)?

Option	Beschreibung
Ja	Gehen Sie zu Schritt 4.
Nein	Siehe <i>Ihr Wi-Fi Direct®-Netzwerk manuell konfigurieren</i> auf Seite 37.

4 Unterstützt Ihr Mobilgerät die Tastendruck-Methode für Wi-Fi Protected Setup™ (WPS)?

Option	Beschreibung
Ja	Siehe <i>Ihr Wi-Fi Direct®-Netzwerk über die Tastendruck-Methode von Wi-Fi Protected Setup™ (WPS) konfigurieren</i> auf Seite 34.
Nein	Siehe <i>Ihr Wi-Fi Direct®-Netzwerk über die PIN-Methode von Wi-Fi Protected Setup™ (WPS) konfigurieren</i> auf Seite 35.

Um die iPrint&Scan-Funktionalität von Brother in einem Wi-Fi Direct®-Netzwerk zu verwenden, das über die Tastendruck- oder PIN-Methode konfiguriert wurde, muss das zur Konfiguration von Wi-Fi Direct® verwendete Gerät unter Android™ 4.0 bzw. höher betrieben werden.

Ihr Wi-Fi Direct®-Netzwerk mittels Tastendruck-Methode konfigurieren

Wenn Ihr Mobilgerät Wi-Fi Direct® unterstützt, dann befolgen Sie zum Konfigurieren eines Wi-Fi Direct®-Netzwerks folgende Schritte.

HINWEIS

Erhält das Gerät von Ihrem Mobilgerät eine Wi-Fi Direct®-Anfrage, zeigt das Display die Meldung *Wi-Fi Direct Verbindungsanfrage empfangen*. Drücken Sie zum Verbinden [OK]. an. Drücken Sie für eine Verbindung OK.

- 1 Drücken Sie  > Netzwerk > Wi-Fi Direct > Taste drücken.
- 2 Aktivieren Sie Wi-Fi Direct® auf Ihrem Mobilgerät (weitere Anweisungen finden Sie im Benutzerhandbuch Ihres Mobilgerätes), wenn das Gerätedisplay *Wi-Fi Direct an anderem Gerät aktivieren*. Dann [OK] drücken. anzeigt. Drücken Sie auf Ihrem Gerät OK, um das Einrichten von Wi-Fi Direct® zu starten. Zum Abbrechen drücken Sie .
- 3 Sie haben die folgenden Möglichkeiten:
 - Handelt es sich bei Ihrem Brother-Gerät um den Gruppenbesitzer (G/B), verbinden Sie Ihr Mobilgerät direkt mit dem Gerät.
 - Handelt es sich bei Ihrem Brother-Gerät nicht um den G/B, werden die Bezeichnungen der Geräte angezeigt, mit denen Sie ein Wi-Fi Direct®-Netzwerk konfigurieren können. Wählen Sie das Mobilgerät aus, mit dem Sie eine Verbindung herstellen möchten, und drücken Sie OK. Führen Sie eine erneute Suche nach verfügbaren Geräten aus, indem Sie *Neuer Scan* drücken.
- 4 Hat Ihr Mobilgerät erfolgreich eine Verbindung aufgebaut, zeigt das Gerätedisplay *Verbunden an*. Sie haben jetzt die Einrichtung des Wi-Fi Direct®-Netzwerks abgeschlossen.

Ihr Wi-Fi Direct®-Netzwerk über die Tastendruck-Methode von Wi-Fi Protected Setup™ (WPS) konfigurieren

Wenn Ihr Mobilgerät WPS unterstützt (PBC: Push Button Configuration = Konfiguration per Tastendruck), befolgen Sie zum Konfigurieren eines Wi-Fi Direct®-Netzwerks folgende Schritte.

HINWEIS

Erhält das Gerät von Ihrem Mobilgerät eine Wi-Fi Direct®-Anfrage, zeigt das Display die Meldung **Wi-Fi Direct Verbindungsanfrage empfangen**. Drücken Sie zum Verbinden [OK]. **an**. Drücken Sie für eine Verbindung **OK**.

- 1 Drücken Sie  > Netzwerk > Wi-Fi Direct > Gruppeneigent.
- 2 Drücken Sie **Ein**.
- 3 Streichen Sie nach oben oder unten bzw. drücken Sie **▲** oder **▼**, um die Option **Taste drücken** auszuwählen. Drücken Sie **Taste drücken**.
- 4 Wenn **Wi-Fi Direct ein?** angezeigt wird, drücken Sie zur Bestätigung **Ein**. Zum Abbrechen drücken Sie **Aus**.
- 5 Aktivieren Sie für Ihr Mobilgerät das Konfigurationsverfahren auf Tastendruck mit WPS (weitere Anweisungen finden Sie im Benutzerhandbuch Ihres Mobilgerätes), wenn das Gerätedisplay **Wi-Fi Direct an anderem Gerät aktivieren**. Dann [OK] drücken. **anzeigt**. Drücken Sie **OK** auf Ihrem Brother-Gerät.
Sie starten damit das Einrichten von Wi-Fi Direct®. Zum Abbrechen drücken Sie .
- 6 Hat Ihr Mobilgerät erfolgreich eine Verbindung aufgebaut, zeigt das Gerätedisplay **Verbunden an**. Sie haben die Einrichtung des Wi-Fi Direct®-Netzwerks abgeschlossen.

Ihr Wi-Fi Direct®-Netzwerk mittels PIN-Methode konfigurieren

Wenn Ihr Mobilgerät die PIN-Methode oder Wi-Fi Direct® unterstützt, führen Sie zum Konfigurieren eines Wi-Fi Direct®-Netzwerks folgende Schritte aus:

HINWEIS

Erhält das Gerät von Ihrem Mobilgerät eine Wi-Fi Direct®-Anfrage, zeigt das Display die Meldung **Wi-Fi Direct Verbindungsanfrage empfangen**. Drücken Sie zum Verbinden [OK]. **an**. Drücken Sie für eine Verbindung **OK**.

- 1 Drücken Sie  > Netzwerk > Wi-Fi Direct > PIN-Code.
- 2 Wenn **Wi-Fi Direct ein?** angezeigt wird, drücken Sie zur Bestätigung **Ein**. Zum Abbrechen drücken Sie **Aus**.
- 3 Aktivieren Sie Wi-Fi Direct® auf Ihrem Mobilgerät (weitere Anweisungen finden Sie im Benutzerhandbuch Ihres Mobilgerätes), wenn das Gerätedisplay **Wi-Fi Direct an anderem Gerät aktivieren**. Dann [OK] drücken. **anzeigt**. Drücken Sie auf Ihrem Gerät **OK**, um das Einrichten von Wi-Fi Direct® zu starten. Zum Abbrechen drücken Sie .

- 4 Sie haben die folgenden Möglichkeiten:
 - Wenn es sich bei Ihrem Brother-Gerät um den Gruppenbesitzer (G/B) handelt, wartet das Gerät auf eine Verbindungsanfrage Ihres Mobilgerätes. Wenn PIN-Code angezeigt wird, müssen Sie die von Ihrem Mobilgerät angezeigte PIN im Gerät eingeben. Zum Beenden der Einrichtung drücken Sie **OK**. Wenn Ihr Brother-Gerät die PIN anzeigt, müssen Sie die PIN in Ihr Mobilgerät eingeben.
 - Handelt es sich bei Ihrem Brother-Gerät nicht um den G/B, werden die Bezeichnungen der Geräte angezeigt, mit denen Sie ein Wi-Fi Direct®-Netzwerk konfigurieren können. Wählen Sie das Mobilgerät aus, mit dem Sie eine Verbindung herstellen möchten, und drücken Sie **OK**.
Führen Sie eine erneute Suche nach verfügbaren Geräten aus, indem Sie **Neuer Scan** drücken.
- 5 Sie haben die folgenden Möglichkeiten:
 - Drücken Sie **PIN-Code anzeigen**, um die PIN auf Ihrem Mobilgerät anzuzeigen. Geben Sie die PIN in Ihr Mobilgerät ein. Fahren Sie mit dem nächsten Schritt fort.
 - Drücken Sie **PIN-Code eingeben**, um die von Ihrem Mobilgerät angezeigte PIN in das Gerät einzugeben, gefolgt von **OK**. Fahren Sie mit dem nächsten Schritt fort.
Wenn Ihr Mobilgerät keine PIN anzeigt, drücken Sie  auf Ihrem Brother-Gerät.
Gehen Sie zurück zum ersten Schritt und versuchen Sie es erneut.
- 6 Hat Ihr Mobilgerät erfolgreich eine Verbindung aufgebaut, zeigt das Gerätedisplay **Verbunden** an. Sie haben die Einrichtung des Wi-Fi Direct®-Netzwerks abgeschlossen.

Ihr Wi-Fi Direct®-Netzwerk über die PIN-Methode von Wi-Fi Protected Setup™ (WPS) konfigurieren

Wenn Ihr Mobilgerät die PIN-Methode oder Wi-Fi Protected Setup™ (WPS) unterstützt, befolgen Sie zum Konfigurieren eines Wi-Fi Direct®-Netzwerks folgende Schritte.

HINWEIS

Erhält das Gerät von Ihrem Mobilgerät eine Wi-Fi Direct®-Anfrage, zeigt das Display die Meldung **Wi-Fi Direct Verbindungsanfrage empfangen**. Drücken Sie zum Verbinden **[OK]**. an. Drücken Sie für eine Verbindung **OK**.

- 1 Drücken Sie  > **Netzwerk** > **Wi-Fi Direct** > **Gruppeneigent.**
- 2 Drücken Sie **Ein**.
- 3 Streichen Sie nach oben oder unten bzw. drücken Sie **▲** oder **▼**, um die Option **PIN-Code** auszuwählen. Drücken Sie **PIN-Code**.
- 4 Wenn **Wi-Fi Direct ein?** angezeigt wird, drücken Sie zur Bestätigung **Ein**. Zum Abbrechen drücken Sie **Aus**.
- 5 Wenn **Wi-Fi Direct an** anderem Gerät aktivieren. Dann **[OK]** drücken. angezeigt wird, aktivieren Sie die WPS PIN-Konfigurationsmethode Ihres Mobilgerätes (weitere Anweisungen finden Sie im Benutzerhandbuch Ihres Mobilgerätes) und drücken Sie anschließend auf Ihrem Brother-Gerät auf **OK**. Der Wi-Fi Direct®-Einrichtvorgang wird gestartet. Zum Abbrechen drücken Sie .

- 6 Das Gerät wartet auf eine Verbindungsanfrage von Ihrem Mobilgerät. Wenn PIN-Code angezeigt wird, müssen Sie die von Ihrem Mobilgerät angezeigte PIN im Gerät eingeben. Drücken Sie OK.
- 7 Hat Ihr Mobilgerät erfolgreich eine Verbindung aufgebaut, zeigt das Gerätedisplay Verbunden an. Sie haben jetzt die Einrichtung des Wi-Fi Direct[®]-Netzwerks abgeschlossen.

Ihr Wi-Fi Direct[®]-Netzwerk manuell konfigurieren

Wenn Ihr Mobilgerät kein Wi-Fi Direct[®] oder WPS unterstützt, müssen Sie das Wi-Fi Direct[®]-Netzwerk manuell konfigurieren.

HINWEIS

Erhält das Gerät von Ihrem Mobilgerät eine Wi-Fi Direct[®]-Anfrage, zeigt das Display die Meldung `Wi-Fi Direct Verbindungsanfrage empfangen`. Drücken Sie zum Verbinden `[OK]`. `an`. Drücken Sie für eine Verbindung `OK`.

- 1 Drücken Sie  > `Netzwerk` > `Wi-Fi Direct` > `Manuell`.
- 2 Wenn `Wi-Fi Direct ein?` angezeigt wird, drücken Sie zur Bestätigung `Ein`. Zum Abbrechen drücken Sie `Aus`.
- 3 Das Gerätedisplay zeigt zwei Minuten lang die SSID-Bezeichnung und das Kennwort an. Rufen Sie auf Ihrem Mobilgerät den Einstellungsbildschirm für das Wireless-Netzwerk auf und geben Sie die SSID-Bezeichnung und das Kennwort ein.
- 4 Hat Ihr Mobilgerät erfolgreich eine Verbindung aufgebaut, zeigt das Gerätedisplay `Verbunden an`. Sie haben die Einrichtung des Wi-Fi Direct[®]-Netzwerks abgeschlossen.

Übersicht

Sie können Ihr Gerät über einen in Ihrem Netzwerk befindlichen Computer mit einem standardmäßigen Webbrowser verwalten, der die Protokolle HTTP (Hyper Text Transfer Protocol) oder HTTPS (Hyper Text Transfer Protocol Secure) unterstützt.

- Sie benötigen die Statusinformationen, Wartungsinformationen und Informationen zur Softwareversion des Brother-Gerätes und Scanservers.
- Ändern Sie die Netzwerk- und Gerätekonfiguration (siehe *Konfiguration der Geräteeinstellungen* auf Seite 39).
- Konfiguration der Einstellungen zur Einschränkung des unberechtigten Zugriffs anderer.
 - Siehe *Festlegen eines Anmeldekennworts* auf Seite 40.
 - Siehe *Konfigurieren der Active Directory LDAP-Authentifizierung (ADS-2800W / ADS-3600W)* auf Seite 43.
- Netzwerkeinstellungen konfigurieren/anpassen.
 - Siehe *Ändern der Konfiguration Scannen: FTP* auf Seite 49.
 - Siehe *Ändern der Konfiguration Scannen: SFTP* auf Seite 50.
 - Siehe *Ändern der Konfiguration von Scan to SMB (Windows®)* auf Seite 52.
 - Siehe *Synchronisieren mit dem SNTTP-Server* auf Seite 47.
 - Siehe *LDAP-Funktion (ADS-2800W / ADS-3600W)* auf Seite 44.
 - Siehe *Konfigurieren der erweiterten TCP/IP-Einstellungen* auf Seite 56.
- Adressbuch importieren/exportieren. (Siehe *Adressbuch importieren/exportieren (ADS-2800W / ADS-3600W)* auf Seite 58.)

HINWEIS

Wir empfehlen Microsoft® Internet Explorer® 8.0/10.0/11.0 für Windows® und Safari 8.0 für Macintosh. Stellen Sie sicher, dass Ihr Webbrowser sowohl JavaScript verarbeiten kann und Cookies zugelassen sind. Wenn Sie einen anderen Webbrowser verwenden, müssen Sie darauf achten, dass diese mit HTTP 1.0 und HTTP 1.1 kompatibel sind.

In Ihrem Netzwerk muss das TCP/IP-Protokoll aktiviert und für den Scanserver und Ihren Computer jeweils eine gültige IP-Adresse registriert sein.

Konfiguration der Geräteeinstellungen

- 1 Starten Sie Web-based Management.
 - a Starten Sie den Webbrowser.
 - b Geben Sie in der Adresszeile Ihres Browsers die IP-Adresse Ihres Gerätes ein.
Beispiel: `http://192.168.1.2`.

HINWEIS

- Wenn Sie ein Domain Name System verwenden oder einen NetBIOS-Namen aktivieren, können Sie statt der IP-Adresse auch einen Namen eingeben, z. B. „GemeinsamerScanner“.

- Beispiel:

`http://GemeinsamerScanner/`

Wenn Sie einen NetBIOS-Namen aktivieren, können Sie auch den Knotennamen verwenden.

- Beispiel:

`http://brwxxxxxxxxxxxxx/`

Der NetBIOS-Name wird im Bedienfeld des Gerätes unter *Knotenname* angezeigt.

- Um zur Konfiguration der Einstellungen mit Web-based Management das sichere HTTPS-Protokoll zu verwenden, müssen Sie das CA-Zertifikat vor dem Start des Web-based Management konfigurieren. Siehe *Verwalten mehrerer Zertifikate* auf Seite 69.

- 2 Standardmäßig ist kein Kennwort erforderlich. Geben Sie ein Kennwort ein, wenn Sie eins eingerichtet haben, und klicken Sie auf .
- 3 Jetzt können Sie Ihre Computereinstellungen konfigurieren.

HINWEIS

Wenn Sie die Protokolleinstellungen geändert haben, klicken Sie auf **Senden** und starten Sie Ihr Brother-Gerät neu, um die Konfiguration zu aktivieren.

Festlegen eines Anmeldekennworts

Es wird empfohlen, ein Anmeldekennwort festzulegen, um den unberechtigten Zugriff auf das Web-based Management zu verhindern.

- 1 Starten Sie Web-based Management und greifen Sie auf das Brother-Gerät zu (siehe Schritt 1 unter Seite 39).
- 2 Wenn der Web-based Management-Bildschirm erscheint, klicken Sie auf die Registerkarte **Administrator** und dann in der linken Navigationsleiste auf **Anmeldekennwort**.
- 3 Geben Sie das gewünschte Kennwort ein (bis zu 32 Zeichen).
- 4 Geben Sie das Kennwort erneut im Kästchen **Neues Kennwort bestätigen** ein.
- 5 Klicken Sie auf **Senden**.
Wenn Sie das nächste Mal auf Web-based Management zugreifen, geben Sie im Feld **Anmelden** das Kennwort ein und klicken Sie auf .
Melden Sie sich anschließend durch Klicken auf  ab.

HINWEIS

Sie können auch ein Anmeldekennwort einstellen, indem Sie unter Web-based Management auf **Bitte konfigurieren Sie das Kennwort** klicken.

Verwenden der LDAP-Authentifizierung

Einführung in die LDAP-Authentifizierung

Die LDAP-Authentifizierung schränkt die Nutzung Ihres Brother-Gerätes ein. Bei aktivierter LDAP-Authentifizierung ist das Bedienfeld des Gerätes gesperrt. Sie können die Geräteeinstellungen erst ändern, wenn Sie einen Benutzernamen und ein Kennwort eingegeben haben.

- Erhält je nach Benutzer-ID E-Mail-Adresse von LDAP-Server, wenn gescannte Daten an einen E-Mail-Server versandt werden.
Um diese Funktion zu nutzen, wählen Sie die Option **E-Mail-Adresse abrufen** aus. Ihre E-Mail-Adresse wird entweder als Sender (wenn das Gerät gescannte Daten an einen E-Mail-Server sendet) oder als Empfänger (wenn Sie die gescannten Daten an Ihre E-Mail-Adresse senden möchten) eingestellt.

Sie können die Einstellung für die LDAP-Authentifizierung über Web-based Management oder BRAdmin Professional 3 (Windows®) ändern.

Konfigurieren der LDAP-Authentifizierung mittels Web-based Management

- 1 Starten Sie den Webbrowser.
- 2 Geben Sie in die Adresszeile Ihres Browsers „http://Geräte-IP-Adresse“ ein (wobei „Geräte-IP-Adresse“ der IP-Adresse Ihres Gerätes entspricht).
Beispiel: http://192.168.1.2
- 3 Klicken Sie auf die Registerkarte **Administrator**.
- 4 Klicken Sie in der linken Navigationsleiste auf das Menü **Funktion zur Nutzungseinschränkung**.
- 5 Wählen Sie **LDAP-Authentifizierung** aus.
- 6 Klicken Sie auf **Senden**.
- 7 Wählen Sie in der linken Navigationsleiste **LDAP-Authentifizierung** aus.

8 Konfigurieren Sie die folgenden Einstellungen:

Option	Beschreibung
Benutzer-ID speichern	Wählen Sie zum Speichern Ihrer Benutzer-ID diese Option aus.
LDAP-Server-Adresse	Geben Sie die IP-Adresse oder den Servernamen des LDAP-Servers ein (Beispiel: ad.beispiel.com).
E-Mail-Adresse abrufen	Wählen Sie diese Option, um vom LDAP-Server die E-Mail-Adresse Ihres Gerätes zu erhalten.
LDAP-Serverport	Geben Sie die Port-Nr. des LDAP-Servers ein.
LDAP-Suchverzeichnis	Geben Sie das LDAP-Suchverzeichnis ein.
Namensattribut (Suchschlüssel)	Geben Sie das Attribut ein, das Sie als Suchschlüssel verwenden möchten.

9 Klicken Sie auf **Senden**.

Anmelden, um die Geräteeinstellungen über das Bedienfeld des Gerätes zu ändern

HINWEIS

Wenn LDAP-Authentifizierung aktiv ist, ist das Bedienfeld des Gerätes gesperrt, bis Sie über das Bedienfeld des Gerätes Ihre Benutzer-ID und das Kennwort eingeben.

- 1 Geben Sie über den Touchscreen des Bedienfelds Ihre Benutzer-ID und das Kennwort ein.
- 2 Drücken Sie **OK**.
- 3 Bei erfolgreicher Authentifizierung wird das Bedienfeld des Gerätes freigegeben.

Einschränken von Benutzern

Konfigurieren der Active Directory LDAP-Authentifizierung (ADS-2800W / ADS-3600W)

Die Active Directory-Authentifizierung schränkt die Nutzung des Brother-Gerätes ein. Wenn die Active Directory-Authentifizierung aktiviert ist, ist das Bedienfeld des Gerätes gesperrt. Sie können die Scanfunktionen erst nach dem Eingeben einer Benutzer-ID, eines Domännennamens und des Kennworts nutzen.

HINWEIS

- Die Active Directory-Authentifizierung unterstützt die Kerberos-Authentifizierung.
- Sie müssen zuerst das Simple Network Time Protocol (SNTP) (Netzwerk-Zeitserver) konfigurieren.

- 1 Starten Sie Web-based Management und greifen Sie auf das Brother-Gerät zu (siehe Schritt 1 unter Seite 39).
- 2 Klicken Sie auf die Registerkarte **Administrator**.
- 3 Klicken Sie in der linken Navigationsleiste auf das Menü **Funktion zur Nutzungseinschränkung**.
- 4 Wählen Sie **Active Directory-Authentifizierung** aus.
- 5 Klicken Sie auf **Senden**.
- 6 Wählen Sie in der linken Navigationsleiste **Active Directory-Authentifizierung** aus.
- 7 Konfigurieren Sie die folgenden Einstellungen:
 - **Benutzer-ID speichern**
Wählen Sie zum Speichern Ihrer Benutzer-ID diese Option aus.
 - **Active Directory-Serveradresse**
Geben Sie die IP-Adresse oder den Servernamen des Active Directory-Servers ein (Beispiel: „ad.beispiel.com“).
 - **Active Directory-Domänenname**
Geben Sie den Active Directory-Domännennamen ein.
 - **Protokoll und Authentifizierungsmethode**
Wählen Sie die Protokoll- und Authentifizierungsmethode aus.
 - **E-Mail-Adresse abrufen**
Wählen Sie diese Option aus, um vom LDAP-Server die E-Mail-Adresse Ihres Gerätes zu erhalten (ausschließlich für die Authentifizierungsmethode LDAP + kerberos verfügbar).
 - **Auf Basisverzeichnis für Benutzer zugreifen**
Wählen Sie diese Option aus, um Ihr Basisverzeichnis zu erhalten und um dieses als Scan to SMB-Ziel festzulegen.

■ LDAP-Serverport

Geben Sie die Port-Nr. des LDAP-Servers ein (ausschließlich für die Authentifizierungsmethode LDAP + kerberos verfügbar).

■ LDAP-Suchverzeichnis

Geben Sie das LDAP-Suchverzeichnis ein (ausschließlich für die Authentifizierungsmethode LDAP + kerberos verfügbar).

■ DNs abrufen

Folgen Sie den Anweisungen auf dem Bildschirm.

■ SNTP

Weitere Informationen zum SNTP-Protokoll finden Sie unter Seite 47.

8 Klicken Sie auf **Senden**.

Schalten Sie das Gerät frei, wenn die Active Directory-Authentifizierung aktiviert ist

- 1 Geben Sie über den Touchscreen Ihre `Benutzer-ID` und Ihr `Kennwort` ein.
- 2 Drücken Sie `OK`.
- 3 Nach Authentifizierung Ihrer Daten wird das Bedienfeld freigegeben und Sie können die Scanfunktionen nutzen.

HINWEIS

Sie können keine Einstellungen verändern, wenn die **Active Directory-Authentifizierung** aktiviert ist.

LDAP-Funktion (ADS-2800W / ADS-3600W)

Mit dem LDAP-Protokoll können Sie vom Server mit den Server-Funktionen von Scan to E-Mail-Server nach E-Mail-Adressen suchen.

Ändern der LDAP-Konfiguration

- 1 Starten Sie Web-based Management und greifen Sie auf das Brother-Gerät zu (siehe Schritt 1 unter Seite 39).
- 2 Klicken Sie auf der Geräte-Webseite auf **Netzwerk**.
- 3 Klicken Sie in der linken Navigationsleiste auf **Protokoll**.
- 4 Aktivieren Sie das Kontrollkästchen **LDAP** und klicken Sie anschließend auf **Senden**.
- 5 Führen Sie zum Aktivieren der Konfiguration einen Neustart Ihres Brother-Gerätes aus.
- 6 Wählen Sie über Ihren Computer in der Web-based Management-Registerkarte **Adressbuch** in der linken Navigationsleiste **LDAP** aus.

7 Konfigurieren Sie die folgenden LDAP-Einstellungen:

- **LDAP-Server-Adresse**
- **Port** (Die Standard-Portnummer ist 389.)
- **Stammverzeichnis**
- **Authentifizierung**
- **Benutzername**
Die Verfügbarkeit dieser Auswahl hängt von der verwendeten Authentifizierungsmethode ab.
- **Kennwort**
Die Verfügbarkeit dieser Auswahl hängt von der verwendeten Authentifizierungsmethode ab.
- **Kerberos-Serveradresse**
Die Verfügbarkeit dieser Auswahl hängt von der verwendeten Authentifizierungsmethode ab.
- **SNTP**
- **LDAP-Zeitüberschreitung**
- **Namensattribut (Suchschlüssel)**
- **E-Mail-Attribut**

8 Klicken Sie abschließend auf **Senden**. Achten Sie darauf, dass für **Status** auf der Seite der Testergebnisse **OK** angegeben ist.

HINWEIS

- Vereinfachtes Chinesisch, Traditionelles Chinesisch und Koreanisch werden vom LDAP-Protokoll nicht unterstützt.
- Wenn der LDAP-Server die Kerberos-Authentifizierung unterstützt, empfehlen wir, als Einstellung für die **Authentifizierung** Kerberos zu verwenden. Dadurch wird eine strenge Authentifizierung zwischen dem LDAP-Server und dem Gerät durchgeführt. Zur Kerberos-Authentifizierung müssen Sie das SNTP-Protokoll (Netzwerk-Zeitserver) konfigurieren oder das Datum, die Uhrzeit und die Zeitzone im Bedienfeld des Gerätes korrekt einstellen. (Informationen zur SNTP-Konfiguration finden Sie unter *Synchronisieren mit dem SNTP-Server* auf Seite 47.)

Ändern der LDAP-Konfiguration über das Gerätebedienfeld (ADS-2800W / ADS-3600W)

Nach der Konfiguration der LDAP-Einstellungen können Sie mit der LDAP-Suche des Gerätes nach E-Mail-Adressen suchen.

- 1 Legen Sie das zu scannende und per E-Mail zu verschickende Dokument in das Gerät ein.
- 2 Drücken Sie auf dem Gerätedisplay an **E-Mail-Server**.
- 3 Drücken Sie **Adressbuch**.
- 4 Drücken Sie  zur Suche.

- 5 Geben Sie die ersten Zeichen für die Suche über die Tasten auf dem Display ein.

HINWEIS

- Sie können bis zu 15 Zeichen eingeben.
 - Weitere Informationen zur Eingabe von Text finden Sie in *Text eingeben (ADS-2800W / ADS-3600W)* im *Benutzerhandbuch*.
-

- 6 Drücken Sie OK.
Die LDAP-Suchergebnisse werden im Display mit  vor den Ergebnissen aus dem lokalen Adressbuch angezeigt. Wenn auf dem Server und im lokalen Adressbuch kein Treffer für die Suche gefunden wird, zeigt das Display *Kein Ergebnis gefunden.* an.
- 7 Drücken Sie zum Scrollen ▲ oder ▼, bis Sie den gewünschten Namen gefunden haben.
- 8 Wenn das Ergebnis mehr als eine E-Mail-Adresse enthält, drücken Sie auf die gewünschte E-Mail-Adresse.
- 9 Drücken Sie Übernehmen.
- 10 Drücken Sie OK.

HINWEIS

Drücken Sie *Optionen*, um die Scaneinstellungen vor dem Scannen des Dokumentes einzustellen.

- 11 Drücken Sie Start.

HINWEIS

- Die LDAP-Funktion dieses Gerätes unterstützt LDAPv3.
 - Weitere Informationen erhalten Sie, wenn Sie rechts von der LDAP-Einstellungsansicht auf  klicken.
-

Synchronisieren mit dem SNTP-Server

Das Simple Network Time Protocol (SNTP) ist ein Protokoll zum Synchronisieren der Gerätezeit für eine Authentifizierung mit dem SNTP-Zeitserver (diese ist nicht identisch mit der im Gerätedisplay angezeigten Zeit). Sie können die Gerätezeit in regelmäßigen Abständen mit der vom SNTP-Zeitserver zur Verfügung gestellten UTC-Zeit (Coordinated Universal Time) synchronisieren.

HINWEIS

- Diese Funktion steht nicht in allen Ländern zur Verfügung.
- Mit Ausnahme von „Datum/Uhrzeit“ muss für die SNTP-Funktionalität keine der ursprünglichen Einstellungen geändert werden.

1 Starten Sie Web-based Management und greifen Sie auf das Brother-Gerät zu (siehe Schritt 1 unter Seite 39).

2 Wenn der Web-based Management-Bildschirm erscheint, klicken Sie auf **Netzwerk** und anschließend in der linken Navigationsleiste auf **Protokoll**.

3 Aktivieren Sie das Kontrollkästchen **SNTP**.

4 Klicken Sie auf **Erweiterte Einstellung**.

■ Status

Zeigt an, ob die Einstellungen des SNTP-Servers aktiviert oder deaktiviert sind.

■ Synchronisationsstatus

Überprüfen Sie den letzten Synchronisationsstatus.

■ SNTP-Server-Methode

Wählen Sie **AUTO** oder **STATISCH**.

• AUTO

Wenn in Ihrem Netzwerk ein DHCP-Server vorhanden ist, erhält der SNTP-Server seine Adresse automatisch von diesem Server.

• STATISCH

Geben Sie die gewünschte Adresse ein.

■ Adresse des primären SNTP-Servers, Adresse des sekundären SNTP-Servers

Geben Sie die Serveradresse ein (bis zu 64 Zeichen).

Die sekundäre SNTP-Serveradresse wird als Ersatz für die primäre SNTP-Serveradresse verwendet. Falls der primäre Server nicht erreichbar ist, verwendet das Gerät den sekundären SNTP-Server.

■ Port des primären SNTP-Servers, Port des sekundären SNTP-Servers

Geben Sie die Portnummer ein (zwischen 1 und 65535).

Der Port des sekundären SNTP-Servers wird als Ersatz für den Port des primären SNTP-Servers verwendet. Falls der primäre Port nicht erreichbar ist, verwendet das Gerät den sekundären SNTP-Port.

■ Synchronisationsintervall

Geben Sie die Anzahl der Stunden ein, die zwischen den Versuchen zur Serversynchronisierung (1 bis 168 Stunden) verstreichen.

HINWEIS

- Sie müssen **Datum/Uhrzeit** konfigurieren, um die vom Gerät verwendete Zeit mit dem SNTP-Zeitserver zu synchronisieren. Klicken Sie auf **Datum/Uhrzeit** und konfigurieren Sie **Datum/Uhrzeit** im Bildschirm **Allgemein**.

Datum/Uhrzeit

Datum / /

Uhrtyp 12-Std.-Format 24-Std.-Format

Uhrzeit : AM

Zeitzone

Zeitumstellung Aus Ein

Mit SNTP-Server synchron.

Zur Synchronisation von "Datum/Uhrzeit" mit dem SNTP-Server, die Einstellungen des SNTP-Servers konfigurieren.

[SNTP>>](#)

- Aktivieren Sie das Kontrollkästchen **Mit SNTP-Server synchron**. Überprüfen Sie die Zeitzoneneinstellungen und wählen Sie aus der Dropdown-Liste **Zeitzone** den Zeitunterschied zwischen Ihrem Standort und UTC aus. Beispiel: Für Eastern Time (USA und Kanada) gilt Zeitzone UTC -5, während Großbritannien UTC entspricht und CET (Central European Time) UTC +1.

- 5 Klicken Sie auf **Senden**.

Ändern der Konfiguration Scannen: FTP

Mit der Funktion Scannen: FTP können Sie ein Dokument einscannen und direkt auf einem FTP-Server im lokalen Netzwerk oder im Internet speichern. Weitere Informationen zu Scannen: FTP siehe den Abschnitt *Scannen von Dokumenten auf einen FTP-Server* im *Benutzerhandbuch*.

- 1 Starten Sie Web-based Management und greifen Sie auf das Brother-Gerät zu (siehe Schritt 1 unter Seite 39).
- 2 Wenn der Web-based Management-Bildschirm erscheint, klicken Sie auf die Registerkarte **Scannen** und anschließend in der linken Navigationsleiste auf **Scannen: FTP/SFTP/Netzwerk/SharePoint**.
- 3 Aktivieren Sie das Kontrollkästchen **FTP** in den Profilnummern (1 bis 25).
- 4 Klicken Sie auf **Senden**.
- 5 Klicken Sie in der linken Navigationsleiste auf **Scannen: FTP/SFTP/Netzwerk/SharePoint-Profil**.
- 6 Klicken Sie bei der Profilnummer, die Sie in Schritt 3 gewählt haben, auf **FTP**. Sie können die folgenden Einstellungen für Scannen: FTP konfigurieren:
 - **Profilname** (max. 15 Zeichen)
 - **Host-Adresse**
 - **Benutzername**
 - **Kennwort**
 - **Zielordner**
 - **Dateiname**
 - **Qualität**
 - **Auto. Farberkennung anpassen**
 - **Dateityp**
 - **Kennwort für sicheres PDF** (ADS-2400N / ADS-3000N)
 - **Dokumentengröße**
 - **Einstellungen Rand**
 - **Dateigröße**
 - **Auto Ausrichtung**
 - **Leerseite überspringen**
 - **Leere Seite Empfindlichkeit überspr.**
 - **2-seitiger Scan**
 - **Helligkeit**
 - **Kontrast**
 - **Fortlaufender Scan** (ADS-2800W / ADS-3600W)
 - **Passiv-Modus**
 - **Port-Nummer**

Stellen Sie den **Passiv-Modus** in Abhängigkeit von der Konfiguration Ihres FTP-Servers und Ihrer Netzwerkfirewall auf **Aus** oder auf **Ein**. Die Standardeinstellung ist **Ein**. Sie können auch die Portnummer, über die auf den FTP-Server zugegriffen wird, ändern. Die Standardeinstellung hierfür ist Port 21. In den meisten Fällen können diese beiden Standardeinstellungen beibehalten werden.

- 7 Klicken Sie auf **Senden**.

Ändern der Konfiguration Scannen: SFTP

Mit der Funktion Scannen: SFTP können Sie ein Dokument einscannen und direkt auf einem SFTP-Server im lokalen Netzwerk oder im Internet speichern. Weitere Informationen zu Scannen: SFTP siehe den Abschnitt *Scannen von Dokumenten auf einen SFTP-Server* im *Benutzerhandbuch*.

- 1 Starten Sie Web-based Management und greifen Sie auf das Brother-Gerät zu (siehe Schritt 1 unter Seite 39).
- 2 Wenn der Web-based Management-Bildschirm erscheint, klicken Sie auf die Registerkarte **Scannen** und anschließend in der linken Navigationsleiste auf **Scannen: FTP/SFTP/Netzwerk/SharePoint**.
- 3 Aktivieren Sie das Kontrollkästchen **SFTP** in den Profilnummern (1 bis 25).
- 4 Klicken Sie auf **Senden**.
- 5 Klicken Sie in der linken Navigationsleiste auf **Scannen: FTP/SFTP/Netzwerk/SharePoint-Profil**.
- 6 Klicken Sie bei der Profilnummer, die Sie in Schritt 3 gewählt haben, auf **SFTP**. Sie können die folgenden Einstellungen für Scannen: SFTP konfigurieren:
 - **Profilname** (max. 15 Zeichen)
 - **Host-Adresse**
 - **Benutzername**
 - **Authentifizierungsmethode**
 - **Kennwort**
 - **Client-Schlüsselpaar**
 - **Öffentlicher Serverschlüssel**
 - **Zielordner**
 - **Dateiname**
 - **Qualität**
 - **Auto. Farberkennung anpassen**
 - **Dateityp**
 - **Kennwort für sicheres PDF** (ADS-2400N / ADS-3000N)
 - **Dokumentengröße**
 - **Einstellungen Rand**
 - **Dateigröße**
 - **Auto Ausrichtung**
 - **Leerseite überspringen**
 - **Leere Seite Empfindlichkeit überspr.**
 - **2-seitiger Scan**
 - **Helligkeit**

- **Kontrast**
- **Fortlaufender Scan** (ADS-2800W / ADS-3600W)
- **Port-Nummer**

Sie können die Portnummer für den Zugriff auf den SFTP-Server ändern. Die Standardeinstellung hierfür ist Port 21. In den meisten Fällen kann die Standardeinstellung beibehalten werden.

- 7 Klicken Sie auf **Senden**.

Ändern der Konfiguration von Scan to SMB (Windows®)

Mit der Funktion „Scan to SMB“ können Sie Dokumente einscannen und direkt in einem freigegebenen Ordner im lokalen Netzwerk oder im Internet speichern. Weitere Informationen zu Scannen: Netzwerk siehe *Scannen von Dokumenten und direktes Ablegen auf einem freigegebenen Ordner / Netzwerk (Windows®)* im *Benutzerhandbuch*.

HINWEIS

Scan to SMB unterstützt die NTLMv2-Authentifizierung.

Zur Authentifizierung müssen Sie das SNTP-Protokoll (Netzwerk-Zeitserver) konfigurieren oder das Datum, die Uhrzeit und die Zeitzone im Bedienfeld des Gerätes korrekt einstellen. (Informationen zur SNTP-Konfiguration finden Sie unter *Synchronisieren mit dem SNTP-Server* auf Seite 47. Informationen zum Einstellen von Datum, Uhrzeit und Zeitzone siehe das *Benutzerhandbuch*.)

- 1 Starten Sie Web-based Management und greifen Sie auf das Brother-Gerät zu (siehe Schritt 1 unter Seite 39).
- 2 Wenn der Web-based Management-Bildschirm erscheint, klicken Sie auf die Registerkarte **Scannen** und anschließend in der linken Navigationsleiste auf Scannen: FTP/SFTP/Netzwerk/SharePoint.
- 3 Aktivieren Sie das Kontrollkästchen **Netzwerk** in den Profilnummern (1 bis 25).
- 4 Klicken Sie auf **Senden**.
- 5 Klicken Sie in der linken Navigationsleiste auf **Scannen: FTP/SFTP/Netzwerk/SharePoint-Profil**.
- 6 Klicken Sie bei der Profilnummer, die Sie in Schritt 3 gewählt haben, auf **Netzwerk**. Sie können die folgenden Einstellungen für Scan to SMB konfigurieren:
 - **Profilname** (max. 15 Zeichen)
 - **Netzwerkordnerpfad**
 - **Dateiname**
 - **Qualität**
 - **Auto. Farberkennung anpassen**
 - **Dateityp**
 - **Kennwort für sicheres PDF** (ADS-2400N / ADS-3000N)
 - **Dokumentengröße**
 - **Einstellungen Rand**
 - **Dateigröße**
 - **Auto Ausrichtung**
 - **Leerseite überspringen**
 - **Leere Seite Empfindlichkeit überspr.**
 - **2-seitiger Scan**
 - **Helligkeit**

- **Kontrast**
- **Fortlaufender Scan** (ADS-2800W / ADS-3600W)
- **PIN zur Authentifizierung verwenden**
- **PIN-Code**
- **Authentifizierungsmethode**
- **Benutzername**
- **Kennwort**
- **Datum/Uhrzeit**

7 Klicken Sie auf **Senden**.

Ändern der Konfiguration von Scannen: SharePoint (Windows®)

SharePoint

Sie können Dokumente scannen und direkt zu einem SharePoint-Server übertragen, wenn Sie das gescannte Dokument freigeben möchten. Konfigurieren Sie unterschiedliche Profile, um Ihre favorisierten Scannen: SharePoint-Ziele zu speichern. Weitere Informationen zu Scannen: SharePoint siehe den Abschnitt *Scannen von Dokumenten auf einen SharePoint* im *Benutzerhandbuch*.

HINWEIS

Scannen: SharePoint unterstützt die NTLMv2-Authentifizierung.

Zur Authentifizierung müssen Sie das SNTP-Protokoll (Netzwerk-Zeitserver) konfigurieren oder das Datum, die Uhrzeit und die Zeitzone im Bedienfeld des Gerätes korrekt einstellen. (Informationen zur SNTP-Konfiguration finden Sie unter *Synchronisieren mit dem SNTP-Server* auf Seite 47. Informationen zum Einstellen von Datum, Uhrzeit und Zeitzone siehe das *Benutzerhandbuch*.)

- 1 Starten Sie Web-based Management und greifen Sie auf das Brother-Gerät zu (siehe Schritt 1 unter Seite 39).
- 2 Wenn der Web-based Management-Bildschirm erscheint, klicken Sie auf die Registerkarte **Scannen** und anschließend in der linken Navigationsleiste auf Scannen: FTP/SFTP/Netzwerk/SharePoint.
- 3 Aktivieren Sie das Kontrollkästchen **SharePoint** in den Profilnummern (1 bis 25).
- 4 Klicken Sie auf **Senden**.
- 5 Klicken Sie in der linken Navigationsleiste auf **Scannen: FTP/SFTP/Netzwerk/SharePoint-Profil**.
- 6 Klicken Sie bei der Profilnummer, die Sie in Schritt 3 gewählt haben, auf **SharePoint**. Sie können die folgenden Einstellungen für Scannen: SharePoint konfigurieren:
 - **Profilname** (max. 15 Zeichen)
 - **SharePoint-Siteadresse**
 - **SSL/TLS**

HINWEIS

SSL/TLS wird nur angezeigt, wenn Sie **HTTPS** unter **SharePoint-Siteadresse** gewählt haben.

- **Dateiname**
- **Qualität**
- **Auto. Farberkennung anpassen**
- **Dateityp**
- **Kennwort für sicheres PDF** (ADS-2400N / ADS-3000N)
- **Dokumentengröße**
- **Einstellungen Rand**

- **Dateigröße**
- **Auto Ausrichtung**
- **Leerseite überspringen**
- **Leere Seite Empfindlichkeit überspr.**
- **2-seitiger Scan**
- **Helligkeit**
- **Kontrast**
- **Fortlaufender Scan (ADS-2800W / ADS-3600W)**
- **PIN zur Authentifizierung verwenden**
- **PIN-Code**
- **Authentifizierungsmethode**
- **Benutzername**
- **Kennwort**
- **Datum/Uhrzeit**

7 Klicken Sie auf **Senden**.

Konfigurieren der erweiterten TCP/IP-Einstellungen

- 1 Starten Sie Web-based Management und greifen Sie auf das Brother-Gerät zu (siehe Schritt 1 unter Seite 39).
- 2 Klicken Sie auf die Registerkarte **Netzwerk** und wählen Sie dann den Verbindungstyp aus (**Verkabelt** oder **Wireless**).
- 3 Wählen Sie im linken Navigationsmenü **TCP/IP** aus.
- 4 Klicken Sie auf **Erweiterte Einstellungen**. Konfigurieren Sie die folgenden Einstellungen: (Im unten dargestellten Beispiel wird **TCP/IP Erweiterte Einstellungen (Verkabelt)** verwendet).

TCP/IP Erweiterte Einstellungen (Verkabelt) ?

Boot-Versuche

RARP Boot-Einstellungen Keine Subnet Mask
 Kein Gateway

TCP-Zeitlimit Minute(n)

DNS-Servermethode

Primäre DNS-Server-IP-Adresse

Sekundäre DNS-Server-IP-Adresse

Gateway-Timeout Sekunde(n)

■ Boot-Versuche

Geben Sie die Anzahl der Startversuche mit der Boot-Methode ein (zwischen 0 und 32767).

■ RARP Boot-Einstellungen

Wählen Sie **Keine Subnet Mask** oder **Kein Gateway** aus.

- **Keine Subnet Mask**

Die Subnetzmaske wird nicht automatisch verändert.

- **Kein Gateway**

Die Gateway-Adresse wird nicht automatisch verändert.

■ TCP-Zeitlimit

Geben Sie die Anzahl der Minuten vor einer TCP-Zeitüberschreitung ein (zwischen 0 und 32767).

■ DNS-Servermethode

Wählen Sie **AUTO** oder **STATIC**.

■ **Primäre DNS-Server-IP-Adresse, Sekundäre DNS-Server-IP-Adresse**

Geben Sie die IP-Adresse des Servers ein.

Die sekundäre IP-Adresse des DNS-Servers wird als Ersatz für die primäre IP-Adresse des DNS-Servers verwendet.

Falls der primäre DNS-Server nicht erreichbar ist, verwendet das Gerät den sekundären DNS-Server.

■ **Gateway-Timeout**

Geben Sie die Anzahl der Sekunden vor einer Router-Zeitüberschreitung ein (zwischen 1 und 32767).

5 Klicken Sie auf **Senden**.

Adressbuch importieren/exportieren (ADS-2800W / ADS-3600W)

Adressbuch importieren

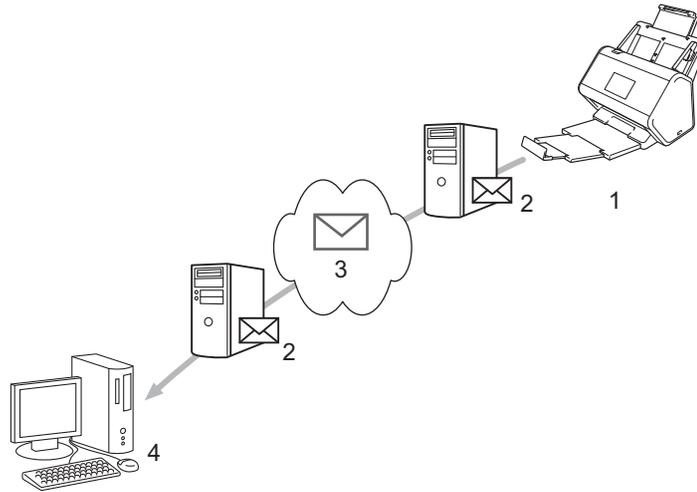
- 1 Starten Sie Web-based Management und greifen Sie auf das Brother-Gerät zu (siehe Schritt 1 unter Seite 39).
- 2 Klicken Sie auf die Registerkarte **Adressbuch**.
- 3 Wählen Sie im linken Navigationsmenü **Importieren** aus.
- 4 Geben Sie **Datendatei „Adressbuch“** oder **Datendatei „Gruppe“** ein.
- 5 Klicken Sie auf **Senden**.

Adressbuch exportieren

- 1 Starten Sie Web-based Management und greifen Sie auf das Brother-Gerät zu (siehe Schritt 1 unter Seite 39).
- 2 Klicken Sie auf die Registerkarte **Adressbuch**.
- 3 Wählen Sie im linken Navigationsmenü **Exportieren** aus.
- 4 Klicken Sie auf die Schaltfläche **Export in Datei**.

Übersicht

Mit „Scan to E-Mail-Server“ können Sie gescannte Dokumente per E-Mail versenden.



- 1 Sender
- 2 E-Mail-Server
- 3 Internet
- 4 Empfänger

Größenbeschränkungen bei Scan to E-Mail-Server

Wenn die Bilddaten des Dokuments zu groß sind, schlägt die Übertragung möglicherweise fehl.

Konfiguration von Scan to E-Mail-Server

Vor dem Verwenden der Scan to E-Mail-Server-Funktion müssen Sie das Brother-Gerät für die Kommunikation mit dem Netzwerk und E-Mail-Server konfigurieren. Sie können diese Informationen über Web-based Management, Remote Setup oder BRAdmin Professional 3 eingeben. Folgende Elemente müssen im Gerät konfiguriert sein:

- IP-Adresse (Wenn Sie das Gerät bereits im Netzwerk verwenden, wurde die IP-Adresse des Gerätes korrekt konfiguriert.)
- E-Mail-Adresse
- SMTP-Serveradresse/Port/Authentifizierungsmethode/ Verschlüsselungsmethode/Server-Zertifikat-Verifizierung
- Name für SMTP-AUTH-Konto und Kennwort

Wenn Sie sich bezüglich dieser Informationen nicht sicher sind, wenden Sie sich an Ihren Netzwerkadministrator.

HINWEIS

Obwohl eine E-Mail-Adresse im Gerät angegeben werden muss, empfängt das Gerät keine E-Mails. Antwortet der Empfänger auf die vom Gerät gesendete E-Mail, kann das Gerät die E-Mail deshalb nicht empfangen.

Vor dem Scannen an E-Mail-Server

Sie müssen ggf. Folgendes konfigurieren (mit Web-based Management oder Remote Setup):

- Absender Betreff
- Größenbegrenzung
- Benachrichtigung (Weitere Informationen finden Sie unter *Bestätigungs-E-Mail* auf Seite 62.)

Informationen zur Verwendung von Scan to E-Mail-Server

- 1 Legen Sie das Dokument ein.
- 2 Streichen Sie nach links oder rechts bzw. drücken Sie ◀ oder ▶, um an E-Mail-Server anzuzeigen.
- 3 Wählen Sie die E-Mail-Adresse, an die Sie schicken möchten, und drücken Sie dann OK.
- 4 Drücken Sie Start.

Weitere Informationen zu den E-Mail-Einstellungen finden Sie in *Senden gescannter Dokumente direkt an eine E-Mail-Adresse (ADS-2800W / ADS-3600W)* im *Benutzerhandbuch*.

Nach dem Scannen des Dokuments wird es automatisch über den SMTP-Server an die angegebene E-Mail-Adresse gesendet.

Abschließend zeigt das Gerätedisplay den Startbildschirm an.

HINWEIS

Einige E-Mail-Server gestatten keinen Versand von umfangreichen E-Mails (Systemadministratoren legen oftmals eine Obergrenze für die E-Mail-Größe fest). Wenn die Scan to E-Mail-Server-Funktion aktiviert ist, zeigt das Gerät `Speicher voll` an, wenn versucht wird, E-Mail-Dokumente einer Größe von über 1 MB zu versenden. Das Dokument wird nicht versendet. Teilen Sie dann Ihr Dokument in kleinere Dokumente auf, die vom E-Mail-Server akzeptiert werden.

Scan to E-Mail-Server: Weitere Funktionen

Bestätigungs-E-Mail

Fordern Sie mit der Bestätigungs-E-Mail-Funktion vom Zielcomputer eine Benachrichtigung an, dass die E-Mail empfangen und verarbeitet wurde.

Mail (Senden)

Aktivieren Sie die Bestätigungsfunktion am Bedienfeld des Gerätes. Wenn für **Mail (Senden)** **Ein** festgelegt wurde, enthält Ihre E-Mail ein zusätzliches Feld, in das automatisch das Eingangsdatum und die Eingangszeit der E-Mail eingetragen werden.

- 1 Drücken Sie im Display des Gerätes auf .
- 2 Drücken Sie **Netzwerk**.
- 3 Drücken Sie **E-Mail**.
- 4 Drücken Sie **Mail (Senden)**.
- 5 Drücken Sie **Bestätigung**.
- 6 Drücken Sie **Ein (oder Aus)**.

HINWEIS

- **Message Disposition Notification (MDN)**
Dieses Feld fragt den Status der E-Mail-Nachricht ab, nachdem diese durch das SMTP-Übertragungsprotokoll (Simple Mail Transfer Protocol) gesendet worden ist. Sobald die Nachricht den Empfänger erreicht hat, werden diese Daten verwendet, wenn das Gerät oder der Benutzer die empfangene E-Mail liest. Wenn z. B. die Nachricht geöffnet und gelesen wurde, sendet der Empfänger eine Benachrichtigung an das Gerät oder den Benutzer, von dem die Nachricht ursprünglich stammt.
Der Empfänger muss das MDN-Feld aktivieren, um einen Empfangsbericht senden zu können, andernfalls wird die Anforderung ignoriert.
 - Dieses Brother-Gerät kann keine E-Mails empfangen. Wenn die Bestätigungsfunktion verwendet werden soll, müssen Sie die Benachrichtigung an eine andere E-Mail-Adresse umleiten. Konfigurieren Sie die E-Mail-Adresse im Display des Gerätes. Drücken Sie **Netzwerk > E-Mail > Mail-Adresse** und geben Sie dann die E-Mail-Adresse ein, an die Benachrichtigung geschickt werden soll.
-

Übersicht

Das Brother-Gerät verwendet moderne Protokolle zur Netzwerksicherheit und Datenverschlüsselung. Diese Netzwerkfunktionen können in Ihr Gesamtsicherheitskonzept eingebunden werden, um Ihre Daten zu schützen und den Zugriff von unberechtigten Personen auf Ihr Gerät zu verhindern.

Sie können die folgenden Sicherheitsfunktionen konfigurieren:

- E-Mails sicher versenden (siehe *Sicheres Versenden von E-Mails (ADS-2800W / ADS-3600W)* auf Seite 64)
- Mehrere Zertifikate verwalten (siehe *Verwalten mehrerer Zertifikate* auf Seite 69)
- Client-Schlüsselpaar erstellen (siehe *Erstellen eines Client-Schlüsselpaares* auf Seite 66)
- Client-Schlüsselpaar exportieren (siehe *Exportieren eines Client-Schlüsselpaares* auf Seite 67)
- Öffentlichen Serverschlüssel importieren (siehe *Importieren eines öffentlichen Serverschlüssels* auf Seite 68)
- Netzwerkgeräte mit IPsec sicher verwalten (siehe *Sicheres Verwalten Ihres Netzwerkgerätes mit IPsec* auf Seite 71)
- Scanfunktion von externen Geräten einschränken (siehe *Einschränken von Scanfunktionen von externen Geräten* auf Seite 84)
- Benutzersperre 3.0 (siehe *Benutzersperre 3.0 (ADS-2800W / ADS-3600W)* auf Seite 85)

HINWEIS

Es wird empfohlen, das FTP- und das TFTP-Protokoll zu deaktivieren. Der Zugriff auf das Gerät mit diesen Protokollen ist nicht sicher. Wenn Sie FTP deaktivieren, wird jedoch auch die Funktion „Scannen to FTP“ deaktiviert. (Nähere Informationen zum Konfigurieren der Protokolleinstellungen finden Sie unter *Konfiguration der Geräteeinstellungen* auf Seite 39.)

Sicheres Versenden von E-Mails (ADS-2800W / ADS-3600W)

Konfiguration mit Web-based Management

Konfigurieren Sie das sichere Versenden von E-Mails mit Benutzerauthentifizierung oder E-Mail-Versand und -Empfang per SSL/TLS.

- 1 Starten Sie den Webbrowser.
- 2 Geben Sie in der Adresszeile Ihres Browsers die IP-Adresse Ihres Gerätes ein. Beispiel: http://192.168.1.2.
- 3 Standardmäßig ist kein Kennwort erforderlich. Geben Sie ein Kennwort ein, wenn Sie eins eingerichtet haben, und klicken Sie auf .
- 4 Klicken Sie auf **Netzwerk**.
- 5 Klicken Sie auf **Protokoll**.
- 6 Klicken Sie auf **Erweiterte Einstellung** unter **SMTP** und stellen Sie sicher, dass der **SMTP-Status Aktiviert** lautet.
- 7 Konfigurieren Sie auf dieser Seite die Einstellungen für **SMTP**.

HINWEIS

- Bestätigen Sie die Korrektheit der E-Mail-Einstellungen, indem Sie nach dem Abschluss der Konfiguration probeweise eine Test-E-Mail senden.
 - Wenn Sie keinen Zugriff auf die SMTP-Servereinstellungen besitzen, wenden Sie sich an Ihren Systemadministrator oder Internetanbieter (ISP).
- 8 Klicken Sie abschließend auf **Senden**. Das Dialogfeld **Konfiguration des E-Mail-Versands testen** wird angezeigt.
 - 9 Befolgen Sie für eine Überprüfung der aktuellen Einstellungen die Anweisungen auf dem Bildschirm.

Versenden von E-Mails mit Benutzerauthentifizierung

Dieses Gerät bevorzugt zum Senden von E-Mails über einen E-Mail-Server, der eine Benutzerauthentifizierung verlangt, das „SMTP-AUTH“-Verfahren. Diese Methode verhindert einen Zugriff auf den E-Mail-Server durch unbefugte Benutzer. Sie können diese Einstellungen mit Web-based Management oder BRAdmin Professional 3 konfigurieren. Das SMTP-AUTH-Verfahren können Sie für E-Mail-Benachrichtigungen, E-Mail-Berichte und Scan to E-Mail-Server verwenden.

E-Mail-Client-Einstellungen

- Die Einstellungen der SMTP-Authentifizierungsmethode müssen mit der Methode der E-Mail-Anwendung übereinstimmen.
- Wenden Sie sich zur Konfiguration des E-Mail-Clients an Ihren Netzwerkadministrator oder Internetanbieter.
- Um die SMTP-Serverauthentifizierung zu aktivieren, müssen Sie das Kontrollkästchen **SMTP-AUTH** unter **Serverauthentifizierungsmethode** aktivieren.

SMTP-Einstellungen

- Sie können die SMTP-Portnummer mit dem Web-based Management ändern. Dies ist besonders dann hilfreich, wenn Ihr Internetanbieter den OP25B-Dienst zur Blockierung von Port 25 („Outbound Port 25 Blocking“) implementiert hat.
- Durch Ändern der SMTP-Portnummer in eine bestimmte Portnummer, die Ihr Internetanbieter für den SMTP-Server verwendet (zum Beispiel Port 587), können Sie dann über den SMTP-Server E-Mails versenden.

Sicheres Senden von E-Mails mit SSL/TLS

Dieses Gerät unterstützt SSL/TLS zum Senden von E-Mails über einen E-Mail-Server, der eine sichere SSL/TLS-Kommunikation erfordert. Um E-Mails über einen E-Mail-Server zu senden, der die SSL/TLS-Kommunikation verwendet, muss SSL/TLS richtig konfiguriert sein.

Server-Zertifikat verifizieren

- Wenn Sie SSL oder TLS für SSL/TLS wählen, wird zur Überprüfung des Serverzertifikats automatisch das Kontrollkästchen Server-Zertifikat verifizieren aktiviert.
 - Das Serverzertifikat wird beim Versand der E-Mail während des Verbindungsversuchs mit dem Server automatisch überprüft.
 - Wenn Sie das Server-Zertifikat nicht überprüfen müssen, deaktivieren Sie **Server-Zertifikat verifizieren**.

Portnummer

- Wenn Sie SSL oder TLS wählen, werden die Einstellungen für den Port an das Protokoll angepasst. Um die Portnummer manuell zu ändern, müssen Sie SSL/TLS wählen und anschließend die Portnummer eingeben.
- Sie müssen die SMTP-Kommunikationsmethode konfigurieren, um sie an den E-Mail-Server anzupassen. Ausführliche Informationen zu den Einstellungen des E-Mail-Servers erhalten Sie von Ihrem Netzwerkadministrator oder ISP (Internetanbieter).

In den meisten Fällen erfordern die sicheren Webmail-Dienste die folgenden Einstellungen:

SMTP

Port: 587

Serverauthentifizierungsmethode: SMTP-AUTH

SSL/TLS: TLS

Sicherheitseinstellungen für SFTP

Für eine SFTP-Verbindung können Sie Sicherheitsschlüssel konfigurieren.

Erstellen eines Client-Schlüsselpaars

Ein Client-Schlüsselpaar wurde erstellt, um eine SFTP-Verbindung herzustellen.

- 1 Starten Sie den Webbrowser.
- 2 Geben Sie in der Adresszeile Ihres Browsers die IP-Adresse Ihres Gerätes ein. Beispiel: `http://192.168.1.2`.

HINWEIS

- Wenn Sie ein Domain Name System verwenden oder einen NetBIOS-Namen aktivieren, können Sie statt der IP-Adresse auch einen Namen eingeben, z. B. „GemeinsamerScanner“.

- Beispiel:

`http://GemeinsamerScanner/`

Wenn Sie einen NetBIOS-Namen aktiviert haben, können Sie auch den Knotennamen verwenden.

- Beispiel:

`http://brnxxxxxxxxxxxxx/`

Der NetBIOS-Name befindet sich im Netzwerkkonfigurationsbericht.

- 3 Standardmäßig ist kein Kennwort erforderlich. Geben Sie ein möglicherweise festgelegtes Kennwort ein und drücken Sie .
- 4 Klicken Sie auf die Registerkarte **Netzwerk**.
- 5 Klicken Sie auf die Registerkarte **Sicherheit**.
- 6 Klicken Sie in der linken Navigationsleiste auf **Client-Schlüsselpaar**.
- 7 Klicken Sie auf **Neues Client-Schlüsselpaar erstellen**.
- 8 Geben Sie im Feld **Name des Client-Schlüsselpaars** eine (aus bis zu 20 Zeichen bestehende) beliebige Bezeichnung ein.
- 9 Klicken Sie auf die Dropdown-Liste **Algorithmus des öffentlichen Schlüssels** und wählen Sie den gewünschten Algorithmus aus.
- 10 Klicken Sie auf **Senden**.
Das Client-Schlüsselpaar wurde erstellt und im Gerätespeicher gespeichert. Der Name des öffentlichen Schlüsselpaars und der Algorithmus des öffentlichen Schlüssels erscheinen in der **Liste der Client-Schlüsselpaare**.

Exportieren eines Client-Schlüsselpaars

Das Client-Schlüsselpaar kommt beim Erstellen einer SFTP-Verbindung zum Einsatz, wenn als Authentifizierungsprotokoll „Öffentlicher Schlüssel“ gewählt wurde.

- 1 Starten Sie den Webbrowser.
- 2 Geben Sie in der Adresszeile Ihres Browsers die IP-Adresse Ihres Gerätes ein. Beispiel: `http://192.168.1.2`.

HINWEIS

- Wenn Sie ein Domain Name System verwenden oder einen NetBIOS-Namen aktivieren, können Sie statt der IP-Adresse auch einen Namen eingeben, z. B. „GemeinsamerScanner“.

- Beispiel:

`http://GemeinsamerScanner/`

Wenn Sie einen NetBIOS-Namen aktivieren, können Sie auch den Knotennamen verwenden.

- Beispiel:

`http://brnxxxxxxxxxxxxx/`

Der NetBIOS-Name befindet sich im Netzwerkkonfigurationsbericht.

- 3 Standardmäßig ist kein Kennwort erforderlich. Geben Sie ein möglicherweise festgelegtes Kennwort ein und drücken Sie .
- 4 Klicken Sie auf die Registerkarte **Netzwerk**.
- 5 Klicken Sie auf die Registerkarte **Sicherheit**.
- 6 Klicken Sie in der linken Navigationsleiste auf **Client-Schlüsselpaar**.
- 7 Klicken Sie in der **Liste der Client-Schlüsselpaare** auf **Öffentlichen Schlüssel exportieren**.
- 8 Klicken Sie auf **Senden**.
- 9 Legen Sie den Ort fest, wo Sie die Datei speichern möchten.

Das Client-Schlüsselpaar wird zu Ihrem Computer exportiert.

Importieren eines öffentlichen Serverschlüssels

Der öffentliche Serverschlüssel kommt beim Verwenden der Funktion Scan to SFTP zum Einsatz, um eine SFTP-Verbindung herzustellen.

- 1 Starten Sie den Webbrowser.
- 2 Geben Sie in der Adresszeile Ihres Browsers die IP-Adresse Ihres Gerätes ein. Beispiel: `http://192.168.1.2`.

HINWEIS

- Wenn Sie ein Domain Name System verwenden oder einen NetBIOS-Namen aktivieren, können Sie statt der IP-Adresse auch einen Namen eingeben, z. B. „GemeinsamerScanner“.

- Beispiel:

`http://GemeinsamerScanner/`

Wenn Sie einen NetBIOS-Namen aktivieren, können Sie auch den Knotennamen verwenden.

- Beispiel:

`http://brnxxxxxxxxxxxxx/`

Der NetBIOS-Name befindet sich im Netzwerkkonfigurationsbericht.

- 3 Standardmäßig ist kein Kennwort erforderlich. Geben Sie ein möglicherweise festgelegtes Kennwort ein und drücken Sie .
- 4 Klicken Sie auf die Registerkarte **Netzwerk**.
- 5 Klicken Sie auf die Registerkarte **Sicherheit**.
- 6 Klicken Sie in der linken Navigationsleiste auf **Öffentlicher Serverschlüssel**.
- 7 Klicken Sie in der **Liste der öffentlichen Serverschlüssel** auf **Öffentlichen Serverschlüssel importieren**.
- 8 Legen Sie die zu importierende Datei fest.
- 9 Klicken Sie auf **Senden**.

Der öffentliche Serverschlüssel wird auf Ihr Gerät importiert.

Verwalten mehrerer Zertifikate

Die Funktion für mehrere Zertifikate gestattet Ihnen die Verwaltung aller installierten Zertifikaten über das Web-based Management Ihres Gerätes. Gehen Sie in Web-based Management zum Bildschirm **CA-Zertifikat**, um den Inhalt der einzelnen Zertifikate anzuzeigen, die Zertifikate zu löschen oder zu exportieren.

Sie können bis zu drei CA-Zertifikate speichern, um SSL zu verwenden.

Wir empfehlen, ein Zertifikat weniger als erlaubt zu speichern, um dadurch einen freien Speicherplatz für den Fall freizuhalten, dass ein Zertifikat abläuft. Wenn ein Zertifikat abgelaufen ist, importieren Sie ein neues Zertifikat in den freigehaltenen Speicherplatz und löschen das abgelaufene Zertifikat. So werden Konfigurationsfehler sicher vermieden.

HINWEIS

Wenn Sie SSL für die SMTP-Kommunikation verwenden, brauchen Sie kein Zertifikat auszuwählen. Das nötige Zertifikat wird automatisch gewählt.

6

Importieren eines CA-Zertifikates

- 1 Starten Sie den Webbrowser.
- 2 Geben Sie in der Adresszeile Ihres Browsers die IP-Adresse Ihres Gerätes ein. Beispiel: `http://192.168.1.2`.

HINWEIS

- Wenn Sie ein Domain Name System verwenden oder einen NetBIOS-Namen aktivieren, können Sie statt der IP-Adresse auch einen Namen eingeben, z. B. „GemeinsamerScanner“.

- Beispiel:

`http://GemeinsamerScanner/`

Wenn Sie einen NetBIOS-Namen aktivieren, können Sie auch den Knotennamen verwenden.

- Beispiel:

`http://brwxxxxxxxxxxxxx/`

Der NetBIOS-Name wird im Bedienfeld des Gerätes unter `Knotenname` angezeigt.

- 3 Standardmäßig ist kein Kennwort erforderlich. Geben Sie ein Kennwort ein, wenn Sie eins eingerichtet haben, und klicken Sie auf .
- 4 Klicken Sie auf die Registerkarte **Netzwerk** und dann auf **Sicherheit**.
- 5 Klicken Sie auf **CA-Zertifikat**.
- 6 Klicken Sie auf **CA-Zertifikat importieren** und wählen Sie ein Zertifikat.
- 7 Klicken Sie auf **Senden**.

Exportieren eines CA-Zertifikates

- 1 Starten Sie den Webbrowser.
- 2 Geben Sie in der Adresszeile Ihres Browsers die IP-Adresse Ihres Gerätes ein. Beispiel: `http://192.168.1.2`.

HINWEIS

- Wenn Sie ein Domain Name System verwenden oder einen NetBIOS-Namen aktivieren, können Sie statt der IP-Adresse auch einen Namen eingeben, z. B. „GemeinsamerScanner“.

- Beispiel:

`http://GemeinsamerScanner/`

Wenn Sie einen NetBIOS-Namen aktivieren, können Sie auch den Knotennamen verwenden.

- Beispiel:

`http://brwxxxxxxxxxxxxx/`

Der NetBIOS-Name wird im Bedienfeld des Gerätes unter `Knotenname` angezeigt.

- 3 Standardmäßig ist kein Kennwort erforderlich. Geben Sie ein möglicherweise festgelegtes Kennwort ein und klicken Sie auf .
- 4 Klicken Sie auf die Registerkarte **Netzwerk** und dann auf **Sicherheit**.
- 5 Klicken Sie auf **CA-Zertifikat**.
- 6 Wählen Sie das Zertifikat, das Sie exportieren möchten, und klicken Sie auf **Exportieren**.
- 7 Klicken Sie auf **Senden**.

Sicheres Verwalten Ihres Netzwerkgerätes mit IPsec

■ Einführung in IPsec

Bei IPsec (Internet Protocol Security = Internetprotokollsicherheit) handelt es sich um ein Sicherheitsprotokoll, das auf eine optionale Internetprotokollfunktion zurückgreift, um Datenmanipulationen zu verhindern und die Vertraulichkeit der als IP-Paket übertragenen Daten sicherzustellen. IPsec verschlüsselt die über das Netzwerk übertragenen Daten. Da die Daten auf der Vermittlungsschicht verschlüsselt werden, können Anwendungen mit einem auf höherer Ebene ausgeführten Protokoll auf IPsec zurückgreifen, ohne dass sich der Benutzer dessen bewusst ist.

■ IPsec mittels Web-based Management konfigurieren

Die IPsec-Anschlussbedingungen umfassen zwei **Vorlage**-Typen: **Adresse** und **IPsec**.

Sie können bis zu 10 Anschlussbedingungen konfigurieren.

■ IPsec-Adressvorlage mittels Web-based Management konfigurieren

■ IPsec-Vorlage mittels Web-based Management konfigurieren

Einführung in IPsec

IPsec unterstützt die folgenden Funktionen:

■ IPsec-Datenübertragungen

Gemäß den IPsec-Einstellungsbedingungen findet zwischen dem netzwerkfähigen Computer und dem Gerät eine Datenübertragung mittels IPsec statt. Wenn die Geräte eine Kommunikation mittels IPsec starten, dann werden zuerst über Internet Key Exchange (IKE) die Schlüssel miteinander ausgetauscht, über die anschließend die verschlüsselten Daten übertragen werden.

Darüber hinaus verfügt IPsec über die zwei Betriebsmodi, den Transportmodus und den Tunnelmodus. Der Transportmodus wird hauptsächlich für die Kommunikation zwischen Geräten verwendet, während der Tunnelmodus in Umgebungen wie etwa einem Virtual Private Network (VPN) eingesetzt wird.

HINWEIS

Für IPsec-Datenübertragungen sind folgende Bedingungen notwendig:

- Am Netzwerk ist ein Computer angeschlossen, der über IPsec kommunizieren kann.
- Ihr Brother-Gerät ist für eine Kommunikation mittels IPsec konfiguriert.
- Der an Ihr Brother-Gerät angeschlossene Computer ist für IPsec-Verbindungen konfiguriert.

■ IPsec-Einstellungen

Diese Einstellungen sind für Verbindungen notwendig, die auf IPsec zurückgreifen. Sie lassen sich über Web-based Management konfigurieren.

HINWEIS

Für die Konfiguration der IPsec-Einstellungen müssen Sie einen am Netzwerk angeschlossenen Browser benutzen.

IPSec mittels Web-based Management konfigurieren

Die IPSec-Anschlussbedingungen umfassen zwei **Vorlage**-Typen: **Adresse** und **IPSec**. Sie können bis zu 10 Anschlussbedingungen konfigurieren.

- 1 Starten Sie den Webbrowser.
- 2 Geben Sie in der Adresszeile Ihres Browsers die IP-Adresse Ihres Gerätes ein. Beispiel: http://192.168.1.2.
- 3 Standardmäßig ist kein Kennwort erforderlich. Geben Sie ein Kennwort ein, wenn Sie eins eingerichtet haben, und klicken Sie auf .
- 4 Klicken Sie auf die Registerkarte **Netzwerk**.
- 5 Klicken Sie auf die Registerkarte **Sicherheit**.
- 6 Klicken Sie in der linken Navigationsleiste auf das Menü **IPSec**.
- 7 Aktivieren oder deaktivieren Sie IPSec im **Status**-Feld.
- 8 Wählen Sie **Aushandlungsmodus** für IKE-Phase 1 aus.
IKE ist ein Protokoll zum Austausch von Verschlüsselungsschlüsseln, die für eine verschlüsselte Kommunikation mittels IPSec verwendet werden.
Im Modus **Normal** liegt eine zwar niedrige Verarbeitungsgeschwindigkeit, dafür aber eine hohe Sicherheit vor. Im Modus **Aggressiv** hingegen ist die Verarbeitungsgeschwindigkeit zwar höher als im Modus **Normal**, doch dafür ist eine nur geringere Sicherheit gegeben.
- 9 Wählen Sie im Feld **Jeglicher Nicht-IPsec-Verkehr** die Aktion aus, wenn keine IPSec-Pakete vorliegen. Bei der Verwendung von Webdiensten müssen Sie für **Jeglicher Nicht-IPsec-Verkehr** die Option **Zulassen** wählen. Wenn Sie **Blockieren** wählen, können Webdienste nicht verwendet werden.
- 10 Wählen Sie im Feld **Broadcast/Multicast-Bypass** die Option **Aktiviert** oder **Deaktiviert** aus.
- 11 Wählen Sie im Feld **Protokoll-Bypass** das von Ihnen gewünschte Kontrollkästchen bzw. die gewünschte Option / Optionen aus.
- 12 Markieren Sie zum Aktivieren der Vorlage in der Tabelle **Richtlinien** das Kontrollkästchen **Aktiviert**. Wenn Sie mehrere Kontrollkästchen auswählen, dann haben bei einem Einstellungskonflikt der gewählten Kontrollkästchen die Kontrollkästchen mit der niedrigsten Nummer Priorität.
- 13 Klicken Sie auf die entsprechende Dropdown-Liste, um die für die IPSec-Anschlussbedingungen verwendete **Adressvorlage** auszuwählen.
Klicken Sie zum Hinzufügen einer **Adressvorlage** auf **Vorlage hinzufügen**.
- 14 Klicken Sie auf die entsprechende Dropdown-Liste, um die für die IPSec-Anschlussbedingungen verwendete **IPsec-Vorlage** auszuwählen.
Klicken Sie zum Hinzufügen einer **IPsec-Vorlage** auf **Vorlage hinzufügen**.
- 15 Klicken Sie auf **Senden**.
Wenn der Computer für die Registrierung der neuen Einstellungen neu gestartet werden muss, erscheint der Neustart-Bestätigungsbildschirm. Wenn Sie in der von Ihnen in der Tabelle **Richtlinien** aktivierten Vorlage ein Element nicht ausgefüllt haben, erscheint eine Fehlermeldung.
Bestätigen Sie Ihre Auswahl und versenden Sie diese erneut.

IPsec-Adressvorlage mittels Web-based Management konfigurieren

- 1 Starten Sie den Webbrowser.
- 2 Geben Sie in der Adresszeile Ihres Browsers die IP-Adresse Ihres Gerätes ein. Beispiel: http://192.168.1.2.
- 3 Standardmäßig ist kein Kennwort erforderlich. Geben Sie ein Kennwort ein, wenn Sie eins eingerichtet haben, und klicken Sie auf .
- 4 Klicken Sie auf die Registerkarte **Netzwerk**.
- 5 Klicken Sie auf die Registerkarte **Sicherheit**.
- 6 Klicken Sie in der linken Navigationsleiste auf das Menü **IPsec-Adressvorlage**.
Es wird die Vorlagenliste mit 10 Adressvorlagen geöffnet.
Klicken Sie zum Löschen einer **Adressvorlage** auf die Schaltfläche **Löschen**. Sie können eine in Gebrauch befindliche **Adressvorlage** nicht löschen.
- 7 Klicken Sie auf die zu erstellende **Adressvorlage**. Die **IPsec-Adressvorlage** wird geöffnet.
- 8 Weisen Sie der Vorlage im Feld **Vorlagenname** eine (aus bis zu 16 Zeichen bestehende) Bezeichnung zu.
- 9 Wählen Sie die Option **Lokale IP-Adresse** aus, um die IP-Adressenbedingungen für das zu sendende Gerät festzulegen:
 - **IP-Adresse**
Legen Sie die IP-Adresse fest. Wählen Sie aus der Dropdown-Liste entweder **ALLE IPv4-Adressen**, **ALLE IPv6-Adressen**, **ALLE Link Local IPv6** oder **Benutzerdefiniert** aus.
Wenn Sie **Benutzerdefiniert** aus der Dropdown-Liste ausgewählt haben, dann müssen Sie im Textfeld die IP-Adresse (IPv4 bzw. IPv6) eingeben.
 - **IP-Adressbereich**
Geben Sie in den Textfeldern die Anfangs- und End-IP-Adressen des IP-Adressbereichs ein. Wenn die Anfangs- und End-IP-Adressen nicht gemäß dem IPv4- oder IPv6-Format standardisiert sind oder wenn die End-IP-Adresse kürzer als die Anfangs-IP-Adresse ist, erscheint eine Fehlermeldung.
 - **IP-Adresse / Präfix**
Spezifizieren Sie die IP-Adresse anhand der CIDR-Schreibweise.
Beispiel: 192.168.1.1/24
Da das Präfix in Form einer 24-Bit-Subnetzmaske (255.255.255.0) für 192.168.1.1 spezifiziert ist, ergibt sich ein gültiger Adressbereich von 192.168.1.xxx.
- 10 Wählen Sie die Option **Remote-IP-Adresse** aus, um die IP-Adressenbedingungen für das zu empfangende Gerät festzulegen:
 - **Beliebig**
Aktiviert alle IP-Adressen.
 - **IP-Adresse**
Ermöglicht eine Eingabe der spezifizierten IP-Adresse (IPv4 bzw. IPv6) in das Textfeld.

■ IP-Adressbereich

Ermöglicht die Eingabe der Anfangs- und End-IP-Adressen des IP-Adressbereichs. Wenn die Anfangs- und End-IP-Adressen nicht gemäß dem IPv4- oder IPv6-Format standardisiert sind oder wenn die End-IP-Adresse kürzer als die Anfangs-IP-Adresse ist, erscheint eine Fehlermeldung.

■ IP-Adresse / Präfix

Spezifizieren Sie die IP-Adresse anhand der CIDR-Schreibweise.

Beispiel: 192.168.1.1/24

Da das Präfix in Form einer 24-Bit-Subnetzmaske (255.255.255.0) für 192.168.1.1 spezifiziert ist, ergibt sich ein gültiger Adressbereich von 192.168.1.xxx.

- 11 Klicken Sie auf **Senden**.

HINWEIS

Wenn Sie die Einstellungen für die in Gebrauch befindliche Vorlage ändern, wird der IPSec-Bildschirm im Web-based Management geschlossen und sogleich wieder geöffnet.

6

IPsec-Vorlage mittels Web-based Management konfigurieren

- 1 Starten Sie den Webbrowser.
- 2 Geben Sie in der Adresszeile Ihres Browsers die IP-Adresse Ihres Gerätes ein. Beispiel: http://192.168.1.2.
- 3 Standardmäßig ist kein Kennwort erforderlich. Geben Sie ein Kennwort ein, wenn Sie eins eingerichtet haben, und klicken Sie auf .
- 4 Klicken Sie auf die Registerkarte **Netzwerk**.
- 5 Klicken Sie auf die Registerkarte **Sicherheit**.
- 6 Klicken Sie in der linken Navigationsleiste auf das Menü **IPSec-Vorlage**.
Es wird die Vorlagenliste mit 10 IPSec-Vorlagen geöffnet.
Klicken Sie zum Löschen einer **IPSec-Vorlage** auf die Schaltfläche **Löschen**. Sie können eine in Gebrauch befindliche **IPSec-Vorlage** nicht löschen.
- 7 Klicken Sie auf die zu erstellende **IPsec-Vorlage**. Es wird der Bildschirm **IPsec-Vorlage** geöffnet.
Die Konfigurationsfelder unterscheiden sich auf Grundlage der von Ihnen gewählten Optionen **Vorgegebene Vorlage verwenden** und **Internet Key Exchange (IKE)**.
- 8 Weisen Sie der Vorlage im Feld **Vorlagenname** eine (aus bis zu 16 Zeichen bestehende) Bezeichnung zu.
- 9 Wählen Sie die Optionen für **Internet Key Exchange (IKE)**.
- 10 Klicken Sie auf **Senden**.

IKEv1-Einstellungen für eine IPsec-Vorlage

Vorlagename

Geben Sie eine (aus bis zu 16 Zeichen bestehende) Bezeichnung für die Vorlage ein.

Vorgegebene Vorlage verwenden

Wählen Sie **Benutzerdefiniert**, **IKEv1 Hohe Sicherheit**, **IKEv1 Mittlere Sicherheit**, **IKEv2 Hohe Sicherheit** oder **IKEv2 Mittlere Sicherheit**. Die einstellbaren Elemente fallen je nach ausgewählter Vorlage unterschiedlich aus.

HINWEIS

Die Standardvorlage kann je nach Auswahl von **Normal** oder **Aggressiv** für **Aushandlungsmodus** im **IPsec**-Konfigurationsanzeige unterschiedlich ausfallen.

Internet Key Exchange (IKE)

IKE ist ein Kommunikationsprotokoll zum Austausch von Verschlüsselungsschlüsseln, um eine verschlüsselte Kommunikation mittels IPsec auszuführen. Für die einmalig ausgeführte verschlüsselte Kommunikation wird der für IPsec erforderliche Verschlüsselungsalgorithmus bestimmt und die Verschlüsselungsschlüssel gemeinsam verwendet. Der Austausch der Verschlüsselungsschlüssel unter IKE greift auf das Diffie-Hellman Schlüsselaustauschverfahren zurück und es findet eine verschlüsselte und auf IKE limitierte Kommunikation statt.

Haben Sie unter **Vorgegebene Vorlage verwenden Benutzerdefiniert** gewählt, dann haben Sie die Wahl zwischen **IKEv1**, **IKEv2** oder **Manuell**. Haben Sie sich für eine andere Einstellung als **Benutzerdefiniert** entschieden, dann werden IKE, Authentifizierungstyp und die in **Vorgegebene Vorlage verwenden** gewählte Encapsulating Security angezeigt.

Authentifizierungstyp

Konfigurieren Sie die IKE-Authentifizierung und -Verschlüsselung.

■ Diffie-Hellman-Gruppe

Dieses Schlüsselaustauschverfahren ermöglicht einen gesicherten Austausch von geheimen Schlüsseln über ein ungesichertes Netzwerk. Das Diffie-Hellman-Schlüsselaustauschverfahren verwendet anstelle von geheimen Schlüsseln diskrete Logarithmen zum Versenden und Empfangen offener Informationen, die mittels einer Zufallszahl und dem geheimen Schlüssel generiert wurden.

Wählen Sie **Gruppe1**, **Gruppe2**, **Gruppe5** oder **Gruppe14**.

■ Verschlüsselung

Wählen Sie **DES**, **3DES**, **AES-CBC 128** oder **AES-CBC 256**.

■ Hash

Wählen Sie **MD5**, **SHA1**, **SHA256**, **SHA384** oder **SHA512**.

■ SA-Lebensdauer

Legen Sie die IKE SA-Lebensdauer fest.

Geben Sie die Zeit (Sekunden) und Anzahl der Kilobytes (KByte) ein.

Encapsulating Security

■ Protokoll

Wählen Sie **ESP**, **AH+ESP** oder **AH**.

HINWEIS

- ESP ist ein Protokoll zur Ausführung von verschlüsselter Kommunikation mittels IPSec. ESP verschlüsselt die Nutzdaten (die kommunizierten Inhalte) und fügt zusätzliche Informationen hinzu. Das IP-Paket umfasst die Kopfzeile und die sich an die Kopfzeile anschließenden verschlüsselten Nutzdaten. Das IP-Paket enthält zusätzlich zu den verschlüsselten Daten Informationen zur Verschlüsselungsmethode und zum Verschlüsselungsschlüssel, die Authentifizierungsdaten usw.
- AH (Authentication Header) ist Bestandteil des IPSec-Protokolls zur Authentifizierung des Senders. Hierüber wird eine Manipulation der Daten verhindert und deren Vollständigkeit sichergestellt. Im IP-Paket sind die Daten unmittelbar hinter der Kopfzeile angeordnet. Die Pakete enthalten darüber hinaus Hash-Werte, die sich aus einer Berechnung der kommunizierten Inhalte mittels einer Gleichung ergeben, sowie den geheimen Schlüssel etc., um eine Falsifizierung des Senders und eine Manipulation der Daten zu verhindern. Die kommunizierten Inhalte sind im Gegensatz zu ESP nicht verschlüsselt: Der Versand und Empfang der Daten erfolgt im Nur-Text-Format.

■ Verschlüsselung

Wählen Sie **DES**, **3DES**, **AES-CBC 128** oder **AES-CBC 256**. Verschlüsselung steht ausschließlich dann zur Verfügung, wenn unter **Protokoll** die Option **ESP** gewählt wurde.

■ Hash

Wählen Sie **Keine**, **MD5**, **SHA1**, **SHA256**, **SHA384** oder **SHA512**.

Keine steht ausschließlich dann zur Verfügung, wenn unter **Protokoll** die Option **ESP** gewählt wurde.

Wenn unter **Protokoll** die Option **ESP** gewählt wurde, müssen Sie das jeweilige Protokoll für **Hash(AH)** und **Hash(ESP)** auswählen.

■ SA-Lebensdauer

Legen Sie die IPSec SA-Lebensdauer fest.

Geben Sie die Zeit (Sekunden) und Anzahl der Kilobytes (KByte) ein.

■ Encapsulation-Modus

Wählen Sie **Transport** oder **Tunnel** aus.

■ IP-Adresse des Remote-Routers

Legen Sie die IP-Adresse (IPv4 bzw. IPv6) für den Remote-Router fest. Geben Sie diese Informationen nur bei der Auswahl des **Tunnel**modus ein.

HINWEIS

Die SA-Verschlüsselungsmethode (Security Association) greift auf IPSec bzw. IPv6 zurück, tauscht Informationen über die Verschlüsselungsmethode und den Verschlüsselungsschlüssel aus bzw. stellt diese für einen gemeinsamen Zugriff zur Verfügung, um vor der Kommunikation einen sicheren Kommunikationskanal zu schaffen. SA kann sich auch auf einen bereits erstellten virtuellen, verschlüsselten Kommunikationskanal beziehen. Die für IPSec verwendete SA-Verschlüsselungsmethode legt die Verschlüsselungsmethode fest, sorgt für einen Austausch der Verschlüsselungsschlüssel und stellt gemäß der IKE-Standardprozedur (Internet Key Exchange) eine gegenseitige Authentifizierung sicher. Die Verschlüsselungsmethode-SA wird darüber hinaus regelmäßig aktualisiert.

Perfect Forward Secrecy (PFS)

PFS verzichtet auf eine Ableitung von Verschlüsselungsschlüsseln aus vorherigen Verschlüsselungsschlüsseln, die für die Verschlüsselung von Nachrichten verwendet wurden. Darüber hinaus werden übergeordnete Schlüssel, mit denen Verschlüsselungsschlüssel für die Verschlüsselung von Nachrichten abgeleitet werden, nicht für die Ableitung anderer Schlüssel verwendet. Aus diesem Grund beschränkt sich bei einem kompromittierten Schlüssel der Schaden ausschließlich auf Nachrichten, die mit diesem Schlüssel verschlüsselt wurden.

Wählen Sie **Aktiviert** oder **Deaktiviert**.

Authentifizierungsmethode

Wählen Sie die Authentifizierungsmethode. Wählen Sie **Pre-Shared Key** oder **Zertifikate**.

Pre-Shared Key

Bei der Verschlüsselung von Kommunikationsvorgängen wird der Verschlüsselungsschlüssel vor der Nutzung eines anderen Kanals ausgetauscht und gemeinsam verwendet.

Wenn Sie **Pre-Shared Key** als **Authentifizierungsmethode** gewählt haben, dann geben Sie den **Pre-Shared Key** ein (bis zu 32 Zeichen).

■ Lokal ID-Typ/ID

Wählen Sie den ID-Typ des Senders aus und geben Sie anschließend die ID ein.

Wählen Sie für den Typ **IPv4-Adresse**, **IPv6-Adresse**, **FQDN**, **E-Mail-Adresse** oder **Zertifikat** aus. Haben Sie **Zertifikat** ausgewählt, dann geben Sie in das **ID**-Feld den allgemeinen Namen ein.

■ Remote ID-Typ/ID

Wählen Sie den ID-Typ des Empfängers aus und geben Sie anschließend die ID ein.

Wählen Sie für den Typ **IPv4-Adresse**, **IPv6-Adresse**, **FQDN**, **E-Mail-Adresse** oder **Zertifikat** aus. Haben Sie **Zertifikat** ausgewählt, dann geben Sie in das **ID**-Feld den allgemeinen Namen ein.

Zertifikat

Haben Sie als **Authentifizierungsmethode Zertifikate** ausgewählt, müssen Sie nun das Zertifikat auswählen.

HINWEIS

Sie können ausschließlich die Zertifikate auswählen, die über die **Zertifikat**-Seite im Sicherheitskonfigurationsmenü des Web-based Managements erstellt wurden.

IKEv2-Einstellungen für eine IPsec-Vorlage

Vorlagename

Geben Sie eine (aus bis zu 16 Zeichen bestehende) Bezeichnung für die Vorlage ein.

Vorgegebene Vorlage verwenden

Wählen Sie **Benutzerdefiniert**, **IKEv1 Hohe Sicherheit**, **IKEv1 Mittlere Sicherheit**, **IKEv2 Hohe Sicherheit** oder **IKEv2 Mittlere Sicherheit**. Die einstellbaren Elemente fallen je nach ausgewählter Vorlage unterschiedlich aus.

HINWEIS

Die Standardvorlage kann je nach Auswahl von **Normal** oder **Aggressiv** für **Aushandlungsmodus** im **IPsec**-Konfigurationsanzeige unterschiedlich ausfallen.

Internet Key Exchange (IKE)

IKE ist ein Kommunikationsprotokoll zum Austausch von Verschlüsselungsschlüsseln, um eine verschlüsselte Kommunikation mittels IPSec auszuführen. Für die einmalig ausgeführte verschlüsselte Kommunikation wird der für IPSec erforderliche Verschlüsselungsalgorithmus bestimmt und die Verschlüsselungsschlüssel gemeinsam verwendet. Der Austausch der Verschlüsselungsschlüssel unter IKE greift auf das Diffie-Hellman Schlüsselaustauschverfahren zurück und es findet eine verschlüsselte und auf IKE limitierte Kommunikation statt.

Haben Sie unter **Vorgegebene Vorlage verwenden Benutzerdefiniert** gewählt, dann haben Sie die Wahl zwischen **IKEv1**, **IKEv2** oder **Manuell**.

Haben Sie sich für eine andere Einstellung als **Benutzerdefiniert** entschieden, dann werden IKE, Authentifizierungstyp und die in **Vorgegebene Vorlage verwenden** gewählte Encapsulating Security angezeigt.

Authentifizierungstyp

Konfigurieren Sie die IKE-Authentifizierung und -Verschlüsselung.

■ Diffie-Hellman-Gruppe

Dieses Schlüsselaustauschverfahren ermöglicht einen gesicherten Austausch von geheimen Schlüsseln über ein ungesichertes Netzwerk. Das Diffie-Hellman-Schlüsselaustauschverfahren verwendet anstelle von geheimen Schlüsseln diskrete Logarithmen zum Versenden und Empfangen offener Informationen, die mittels einer Zufallszahl und dem geheimen Schlüssel generiert wurden.

Wählen Sie **Gruppe1**, **Gruppe2**, **Gruppe5** oder **Gruppe14**.

■ Verschlüsselung

Wählen Sie **DES**, **3DES**, **AES-CBC 128** oder **AES-CBC 256**.

■ Hash

Wählen Sie **MD5**, **SHA1**, **SHA256**, **SHA384** oder **SHA512**.

■ SA-Lebensdauer

Legen Sie die IKE SA-Lebensdauer fest.

Geben Sie die Zeit (Sekunden) und Anzahl der Kilobytes (KByte) ein.

Encapsulating Security

■ Protokoll

Wählen Sie **ESP**.

HINWEIS

ESP ist ein Protokoll zur Ausführung von verschlüsselter Kommunikation mittels IPSec. ESP verschlüsselt die Nutzdaten (die kommunizierten Inhalte) und fügt zusätzliche Informationen hinzu. Das IP-Paket umfasst die Kopfzeile und die sich an die Kopfzeile anschließenden verschlüsselten Nutzdaten. Das IP-Paket enthält zusätzlich zu den verschlüsselten Daten Informationen zur Verschlüsselungsmethode und zum Verschlüsselungsschlüssel, die Authentifizierungsdaten usw.

■ Verschlüsselung

Wählen Sie **DES**, **3DES**, **AES-CBC 128** oder **AES-CBC 256**.

■ Hash

Wählen Sie **MD5**, **SHA1**, **SHA256**, **SHA384** oder **SHA512**.

■ SA-Lebensdauer

Legen Sie die IPSec SA-Lebensdauer fest.

Geben Sie die Zeit (Sekunden) und Anzahl der Kilobytes (KByte) ein.

■ Encapsulation-Modus

Wählen Sie **Transport** oder **Tunnel** aus.

■ IP-Adresse des Remote-Routers

Legen Sie die IP-Adresse (IPv4 bzw. IPv6) für den Remote-Router fest. Geben Sie diese Informationen nur bei der Auswahl des **Tunnel**modus ein.

HINWEIS

Die SA-Verschlüsselungsmethode (Security Association) greift auf IPSec bzw. IPv6 zurück, tauscht Informationen über die Verschlüsselungsmethode und den Verschlüsselungsschlüssel aus bzw. stellt diese für einen gemeinsamen Zugriff zur Verfügung, um vor der Kommunikation einen sicheren Kommunikationskanal zu schaffen. SA kann sich auch auf einen virtuell verschlüsselten Kommunikationskanal beziehen, der hergestellt wurde. Die für IPSec verwendete SA-Verschlüsselungsmethode legt die Verschlüsselungsmethode fest, sorgt für einen Austausch der Verschlüsselungsschlüssel und stellt gemäß der IKE-Standardprozedur (Internet Key Exchange) eine gegenseitige Authentifizierung sicher. Die Verschlüsselungsmethode-SA wird darüber hinaus regelmäßig aktualisiert.

Perfect Forward Secrecy (PFS)

PFS verzichtet auf eine Ableitung von Verschlüsselungsschlüsseln aus vorherigen Verschlüsselungsschlüsseln, die für die Verschlüsselung von Nachrichten verwendet wurden. Darüber hinaus werden übergeordnete Schlüssel, mit denen Verschlüsselungsschlüssel für die Verschlüsselung von Nachrichten abgeleitet werden, nicht für die Ableitung anderer Schlüssel verwendet. Aus diesem Grund beschränkt sich bei einem kompromittierten Schlüssel der Schaden ausschließlich auf Nachrichten, die mit diesem Schlüssel verschlüsselt wurden.

Wählen Sie **Aktiviert** oder **Deaktiviert**.

Authentifizierungsmethode

Wählen Sie die Authentifizierungsmethode. Wählen Sie **Pre-Shared Key**, **Zertifikate**, **EAP - MD5** oder **EAP - MS-CHAPv2**.

Pre-Shared Key

Bei der Verschlüsselung von Kommunikationsvorgängen wird der Verschlüsselungsschlüssel vor der Nutzung eines anderen Kanals ausgetauscht und gemeinsam verwendet.

Wenn Sie für die **Authentifizierungsmethode Pre-Shared Key** gewählt haben, dann geben Sie den **Pre-Shared Key** ein (bis zu 32 Zeichen).

■ Lokal ID-Typ/ID

Wählen Sie den ID-Typ des Senders aus und geben Sie anschließend die ID ein.

Wählen Sie für den Typ **IPv4-Adresse**, **IPv6-Adresse**, **FQDN**, **E-Mail-Adresse** oder **Zertifikat** aus.

Haben Sie **Zertifikat** ausgewählt, dann geben Sie in das **ID**-Feld den allgemeinen Namen ein.

■ Remote ID-Typ/ID

Wählen Sie den ID-Typ des Empfängers aus und geben Sie anschließend die ID ein.

Wählen Sie für den Typ **IPv4-Adresse**, **IPv6-Adresse**, **FQDN**, **E-Mail-Adresse** oder **Zertifikat** aus.

Haben Sie **Zertifikat** ausgewählt, dann geben Sie in das **ID**-Feld den allgemeinen Namen ein.

Zertifikat

Haben Sie als **Authentifizierungsmethode Zertifikate** ausgewählt, müssen Sie nun das Zertifikat auswählen.

HINWEIS

Sie können ausschließlich die Zertifikate auswählen, die über die **Zertifikat**-Seite im Sicherheitskonfigurationsmenü des Web-based Managements erstellt wurden.

EAP

EAP ist ein Authentifizierungsprotokoll, bei dem es sich um eine Erweiterung von PPP handelt. Bei der Verwendung von EAP mit IEEE 802.1x wird während jeder Sitzung ein unterschiedlicher Schlüssel für die Benutzerauthentifizierung eingesetzt.

Die folgenden Einstellungen sind nur dann erforderlich, wenn **EAP - MD5** oder **EAP - MS-CHAPv2** unter **Authentifizierungsmethode** gewählt wurden:

■ Modus

Wählen Sie **Server-Modus** oder **Client-Modus**.

■ Zertifikat

Wählen Sie das Zertifikat aus.

■ Benutzername

Geben Sie den Benutzernamen ein (bis zu 32 Zeichen).

■ Kennwort

Geben Sie das Kennwort ein (bis zu 32 Zeichen). Das Kennwort muss zwei Mal eingegeben werden, um bestätigt zu werden.

■ Zertifikat

Klicken Sie auf diese Schaltfläche, um zur **Zertifikat**-Konfigurationsanzeige zu gelangen.

Manuelle Einstellungen für eine IPsec-Vorlage

Vorlagename

Geben Sie eine (aus bis zu 16 Zeichen bestehende) Bezeichnung für die Vorlage ein.

Vorgegebene Vorlage verwenden

Wählen Sie **Benutzerdefiniert**, **IKEv1 Hohe Sicherheit**, **IKEv1 Mittlere Sicherheit**, **IKEv2 Hohe Sicherheit** oder **IKEv2 Mittlere Sicherheit**. Die Einstellungen fallen je nach ausgewählter Vorlage unterschiedlich aus.

HINWEIS

Die Standardvorlage kann je nach Auswahl von **Normal** oder **Aggressiv** für **Aushandlungsmodus** im **IPsec**-Konfigurationsanzeige unterschiedlich ausfallen.

Internet Key Exchange (IKE)

IKE ist ein Kommunikationsprotokoll zum Austausch von Verschlüsselungsschlüsseln, um eine verschlüsselte Kommunikation mittels IPsec auszuführen. Für die einmalig ausgeführte verschlüsselte Kommunikation wird der für IPsec erforderliche Verschlüsselungsalgorithmus bestimmt und die Verschlüsselungsschlüssel gemeinsam verwendet. Der Austausch der Verschlüsselungsschlüssel unter IKE greift auf das Diffie-Hellman Schlüsselaustauschverfahren zurück und es findet eine verschlüsselte und auf IKE limitierte Kommunikation statt.

Haben Sie unter **Vorgegebene Vorlage verwenden Benutzerdefiniert** gewählt, dann haben Sie die Wahl zwischen **IKEv1**, **IKEv2** oder **Manuell**.

Haben Sie sich für eine andere Einstellung als **Benutzerdefiniert** entschieden, dann werden IKE, Authentifizierungstyp und die in **Vorgegebene Vorlage verwenden** gewählte Encapsulating Security angezeigt.

Authentifizierungsschlüssel (ESP, AH)

Legen Sie den für eine Authentifizierung zu verwendenden Schlüssel fest. Geben Sie die Werte für **Eingehend/Ausgehend** ein.

Diese Einstellungen sind erforderlich, wenn **Benutzerdefiniert** für **Vorgegebene Vorlage verwenden** ausgewählt wurde, **Manuell** für **IKE** und eine andere Einstellung als **Keine** für **Hash** unter **Encapsulating Security** ausgewählt wurde.

HINWEIS

Die Anzahl der Zeichen, die von Ihnen eingegeben werden können, kann je nach gewählter Einstellung für **Hash** unter **Encapsulating Security** unterschiedlich sein.

Ist die Länge des spezifizierten Authentifizierungsschlüssels unterschiedlich zum gewählten Hashalgorithmus, dann erscheint eine Fehlermeldung.

- **MD5**: 128 Bit (16 Byte)
- **SHA1**: 160 Bit (20 Byte)
- **SHA256**: 256 Bit (32 Byte)
- **SHA384**: 384 Bit (48 Byte)
- **SHA512**: 512 Bit (64 Byte)

Wenn Sie den Schlüssel als ASCII-Code spezifizieren, müssen Sie die Zeichen in doppelten Anführungszeichen (") einschließen.

Codeschlüssel (ESP)

Legen Sie den für eine Verschlüsselung zu verwendenden Schlüssel fest. Geben Sie die Werte für **Eingehend/Ausgehend** ein.

Diese Einstellungen sind erforderlich, wenn **Benutzerdefiniert** für **Vorgegebene Vorlage verwenden**, **Manuell** für **IKE** und **ESP** für **Protokoll** unter **Encapsulating Security** gewählt wurde.

HINWEIS

Die Anzahl der Zeichen, die von Ihnen eingegeben werden können, kann je nach gewählter Einstellung für **Verschlüsselung** unter **Encapsulating Security** unterschiedlich sein.

Ist die Länge des spezifizierten Codes unterschiedlich zum gewählten Verschlüsselungsalgorithmus, dann erscheint eine Fehlermeldung.

- **DES**: 64 Bit (8 Byte)
- **3DES**: 192 Bit (24 Byte)
- **AES-CBC 128**: 128 Bit (16 Byte)
- **AES-CBC 256**: 256 Bit (32 Byte)

Wenn Sie den Schlüssel als ASCII-Code spezifizieren, müssen Sie die Zeichen in doppelten Anführungszeichen (") einschließen.

SPI

Diese Parameter dienen der Identifizierung von Sicherheitsinformationen. Ein Host besitzt allgemein mehrere Security Associations (SAs), die für mehrere Typen an IPSec-Kommunikationsvorgängen zutreffen. Aus diesem Grund ist beim Empfang eines IPSec-Pakets die Identifizierung der entsprechenden SA notwendig. Der für die SA-Identifizierung zuständige SPI-Parameter ist im Authentication Header (AH) und im Encapsulating Security Payload (ESP)-Header enthalten.

Diese Einstellungen sind erforderlich, wenn **Benutzerdefiniert** für **Vorgegebene Vorlage verwenden** und **Manuell** für **IKE** gewählt wurde.

Geben Sie die Werte für **Eingehend/Ausgehend** (3 bis 10 Zeichen) ein.

Encapsulating Security

■ Protokoll

Wählen Sie **ESP** oder **AH**.

HINWEIS

- ESP ist ein Protokoll zur Ausführung von verschlüsselter Kommunikation mittels IPSec. ESP verschlüsselt die Nutzdaten (die kommunizierten Inhalte) und fügt zusätzliche Informationen hinzu. Das IP-Paket umfasst die Kopfzeile und die sich an die Kopfzeile anschließenden verschlüsselten Nutzdaten. Das IP-Paket enthält zusätzlich zu den verschlüsselten Daten Informationen zur Verschlüsselungsmethode und zum Verschlüsselungsschlüssel, die Authentifizierungsdaten usw.
- AH ist Bestandteil des IPSec-Protokolls zur Authentifizierung des Senders. Hierüber wird eine Manipulation der Daten verhindert und deren Vollständigkeit sichergestellt. Im IP-Paket sind die Daten unmittelbar hinter der Kopfzeile angeordnet. Die Pakete enthalten darüber hinaus Hash-Werte, die sich aus einer Berechnung der kommunizierten Inhalte mittels einer Gleichung ergeben, sowie den geheimen Schlüssel etc., um eine Falsifizierung des Senders und eine Manipulation der Daten zu verhindern. Die kommunizierten Inhalte sind im Gegensatz zu ESP nicht verschlüsselt: Der Versand und Empfang der Daten erfolgt im Nur-Text-Format.

■ Verschlüsselung

Wählen Sie **DES**, **3DES**, **AES-CBC 128** oder **AES-CBC 256**. Verschlüsselung steht ausschließlich dann zur Verfügung, wenn unter **Protokoll** die Option **ESP** gewählt wurde.

■ Hash

Wählen Sie **Keine**, **MD5**, **SHA1**, **SHA256**, **SHA384** oder **SHA512**.

Keine steht ausschließlich dann zur Verfügung, wenn unter **Protokoll** die Option **ESP** gewählt wurde.

■ SA-Lebensdauer

Legen Sie die IKE SA-Lebensdauer fest.

Geben Sie die Zeit (Sekunden) und Anzahl der Kilobytes (KByte) ein.

■ Encapsulation-Modus

Wählen Sie **Transport** oder **Tunnel** aus.

■ IP-Adresse des Remote-Routers

Legen Sie die IP-Adresse (IPv4 bzw. IPv6) des Verbindungsziels fest. Geben Sie diese Informationen nur bei der Auswahl des **Tunnelmodus** ein.

HINWEIS

Die SA-Verschlüsselungsmethode (Security Association) greift auf IPSec bzw. IPv6 zurück, tauscht Informationen über die Verschlüsselungsmethode und den Verschlüsselungsschlüssel aus bzw. stellt diese für einen gemeinsamen Zugriff zur Verfügung, um vor der Kommunikation einen sicheren Kommunikationskanal zu schaffen. SA kann sich auch auf einen virtuell verschlüsselten Kommunikationskanal beziehen, der hergestellt wurde. Die für IPSec verwendete SA-Verschlüsselungsmethode legt die Verschlüsselungsmethode fest, sorgt für einen Austausch der Verschlüsselungsschlüssel und stellt gemäß der IKE-Standardprozedur (Internet Key Exchange) eine gegenseitige Authentifizierung sicher. Die Verschlüsselungsmethode-SA wird darüber hinaus regelmäßig aktualisiert.

Senden

Klicken Sie auf diese Schaltfläche, um die Einstellungen zu registrieren.

HINWEIS

Wenn Sie die Einstellungen für die in Gebrauch befindliche Vorlage ändern, wird der IPSec-Bildschirm im Web-based Management geschlossen und sogleich wieder geöffnet.

Einschränken von Scanfunktionen von externen Geräten

Diese Funktion ermöglicht Ihnen, die von externen Geräten ausgehenden Scanfunktionen einzuschränken. Wenn Sie die Scanfunktionen externer Geräte einschränken, erscheint auf dem Gerät eine Fehlermeldung und die Anwender können diese Scanfunktionen nicht verwenden.

Einschränken von Scanfunktionen von externen Geräten über Webbrowser-Einstellungen

- 1 Starten Sie den Webbrowser.
- 2 Geben Sie in der Adresszeile Ihres Browsers die IP-Adresse Ihres Gerätes ein. Beispiel: `http://192.168.1.2`.
- 3 Standardmäßig ist kein Kennwort erforderlich. Geben Sie ein möglicherweise festgelegtes Kennwort ein und drücken Sie .
- 4 Klicken Sie auf die Registerkarte **Scannen**.
- 5 Klicken Sie in der Navigationsleiste auf das Menü **Scan von PC**.
- 6 Deaktivieren Sie **Scan ziehen**.
- 7 Klicken Sie auf **Senden**.

Benutzersperre 3.0 (ADS-2800W / ADS-3600W)

Mit der Benutzersperre können Sie den öffentlichen Zugriff auf folgende Funktionen des Gerätes einschränken:

- Scannen:PC
- Scannen:FTP/SFTP
- Scan-to-SMB
- Scan to USB
- Scannen:Web
- Scan to E-Mail-Server
- Scan-to-SharePoint
- Scan to WSS (Web Service-Scan)
- Anwendungen

Die Benutzersperre schränkt auch den Zugriff auf die Geräteeinstellungen ein und verhindert dadurch, dass Benutzer die Standardeinstellungen des Gerätes ändern können.

Bevor Sie die Sicherheitsfunktionen nutzen können, müssen Sie zunächst ein Administratorkennwort eingeben.

Der Administrator kann mithilfe von Benutzerkennwörtern Einschränkungen für einzelne Benutzer einrichten.

Notieren Sie sich sorgfältig das Kennwort. Wenn Sie es vergessen, müssen Sie das im Gerät gespeicherte Kennwort zurücksetzen. Wenn Sie Informationen zum Zurücksetzen des Kennworts benötigen, wenden Sie sich an den Brother Kundenservice.

HINWEIS

- Sie können die Benutzersperre über Web-based Management oder BRAdmin Professional 3 (nur Windows®) einrichten.
- Nur Administratoren können Einschränkungen und Änderungen für jeden Benutzer festlegen.
- (Für ADS-3600W)
Verwenden Sie Karten-Authentifizierung, um zu einem anderen Benutzer zu wechseln und um Zugriff auf Scanfunktionen wie Scannen:PC, Scannen:FTP oder Scan to SMB zu erhalten.

Bevor Sie Benutzersperre 3.0 verwenden

Sie können die Einstellungen für die Benutzersperre mit einem Webbrowser konfigurieren. Führen Sie zuerst folgende Schritte aus:

- 1 Starten Sie den Webbrowser.
- 2 Geben Sie in der Adresszeile Ihres Browsers die IP-Adresse Ihres Gerätes ein. Beispiel: <http://192.168.1.2>.
- 3 Geben Sie im Feld **Anmelden** ein Administratorkennwort ein. (Dies ist das Kennwort für die Anmeldung auf der Geräte-Webseite.) Klicken Sie auf .

Benutzersperre ein- und ausschalten

- 1 Klicken Sie auf **Administrator**.
- 2 Klicken Sie auf **Funktion zur Nutzungseinschränkung**.
- 3 Wählen Sie **Benutzersperre** oder **Aus**.
- 4 Klicken Sie auf **Senden**.

Konfigurieren der Benutzersperre 3.0 mit Web-based Management

Richten Sie Gruppen mit Einschränkungen und Benutzer mit Kennwörtern und Karten-ID (NFC-ID) ¹ ein. Sie können bis zu 100 eingeschränkte Gruppen und 100 Benutzer einrichten. Konfigurieren Sie diese Einstellungen mit einem Webbrowser. Informationen zum Einrichten der Webseite finden Sie unter *Bevor Sie Benutzersperre 3.0 verwenden* auf Seite 85. Führen Sie anschließend folgende Schritte aus:

¹ Für ADS-3600W

- 1 Klicken Sie auf **Administrator**.
- 2 Klicken Sie auf **Funktion zur Nutzungseinschränkung**.
- 3 Wählen Sie **Benutzersperre**.
- 4 Klicken Sie auf **Senden**.
- 5 Klicken Sie auf **Benutzerliste xx-xx**.
- 6 Geben Sie im Feld **Benutzerliste** mit den Benutzernamen ein, der max. 20 Zeichen lang sein darf.
- 7 Geben Sie im Feld **PIN-Nummer** ein Kennwort aus vier Ziffern ein.
- 8 (Für ADS-3600W)
Geben Sie im Feld **Karten-ID** die Kartenummer (max. 16 Zeichen) ein. ¹
¹ Sie können die Ziffern 0–9 und die Buchstaben A–F verwenden (Groß-/Kleinschreibung wird nicht berücksichtigt).
- 9 Wählen Sie aus der Dropdown-Liste für jeden Nutzer **Benutzerliste/ingeschränkte Funktionen** aus.
- 10 Klicken Sie auf **Senden**.

Firmware-Update

Sie können die Firmware über ein Update von der Brother-Website aktualisieren.

HINWEIS

Falls Sie für die Internetkommunikation einen Proxyserver verwenden, müssen Sie unter „Proxy“ die entsprechenden Angaben machen.

- 1 Starten Sie den Webbrowser.
- 2 Geben Sie in der Adresszeile Ihres Browsers die IP-Adresse Ihres Gerätes ein. Beispiel: `http://192.168.1.2`.
- 3 Standardmäßig ist kein Kennwort erforderlich. Geben Sie ein möglicherweise festgelegtes Kennwort ein und drücken Sie .
- 4 Klicken Sie auf die Registerkarte **Administrator**.
- 5 Klicken Sie in der Navigationsleiste auf das Menü **Firmware-Update**.
- 6 Klicken Sie auf **Nach neuer Firmware suchen**.

Übersicht

In diesem Kapitel wird beschrieben, wie Sie Netzwerkprobleme lösen können, die bei der Verwendung des Brother-Gerätes möglicherweise auftreten.

Um weitere Handbücher für Ihr Gerät herunterzuladen, wählen Sie im Brother Solutions Center Ihr Modell aus unter solutions.brother.com/manuals

Identifizieren des Problems

Stellen Sie sicher, dass die folgenden Punkte erfüllt sind, bevor Sie die Problemlösungen lesen.

Vergewissern Sie sich, dass Sie Folgendes überprüft haben:

Der Netzadapter ist richtig angeschlossen und das Brother-Gerät ist eingeschaltet.
Der Access Point, Router oder Hub ist eingeschaltet und die Verbindungstaste blinkt.
Alle Transportschutzteile wurden vom Gerät entfernt.
Die vordere Abdeckung, die Abdeckung des Papiertrenners und die Abdeckung der Einzugsrolle sind vollständig geschlossen.

Gehen Sie auf die Seite für Ihr Produkt:

- *Ich kann die Konfiguration des Wireless-Netzwerks nicht abschließen.* auf Seite 89.
- *WLAN-Fehlercodes (ADS-2800W / ADS-3600W)* auf Seite 90.
- *Das Brother-Gerät wird während der Brother-Geräteinstallation nicht im Netzwerk gefunden.* auf Seite 92.
- *Das Brother-Gerät kann nicht über das Netzwerk scannen. Das Brother-Gerät wird auch nach erfolgreicher Installation nicht im Netzwerk gefunden.* auf Seite 93.
- *Ich verwende Sicherheitssoftware.* auf Seite 95.
- *Ich möchte überprüfen, ob meine Netzwerkgeräte ordnungsgemäß funktionieren.* auf Seite 96.

Ich kann die Konfiguration des Wireless-Netzwerks nicht abschließen.

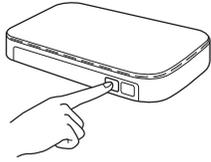
Problem	Schnittstelle	Lösung
Konnte das Gerät während der Einrichtung des Wireless-Netzwerks keine Verbindung zum Netzwerk herstellen?	Wireless	Schalten Sie Ihren Wireless-Router aus und wieder ein, versuchen Sie es erneut oder konfigurieren Sie erneut die Wireless-Einstellungen.
Sind die Sicherheitseinstellungen (SSID/Netzwerkschlüssel) korrekt?	Wireless	Vergewissern Sie sich, dass Ihre Sicherheitseinstellungen korrekt sind. <ul style="list-style-type: none"> ■ Als Standard-Sicherheitseinstellungen können der Herstellername oder die Modellnummer des WLAN-Access-Points/-Routers verwendet werden. ■ Lesen Sie die Anleitung des WLAN-Access-Points/Routers, um die Sicherheitseinstellungen zu erfahren. ■ Wenden Sie sich an den Hersteller des WLAN-Access-Points/Routers, Ihren Internetanbieter oder Netzwerkadministrator.
Verwenden Sie MAC-Adressenfilterung?	Wireless	Vergewissern Sie sich, dass die MAC-Adresse des Brother-Gerätes im Filter zugelassen ist. Sie können die MAC-Adresse des Brother-Gerätes im Gerätebedienfeld ermitteln.
Befindet sich der WLAN-Access-Point/-Router im Stealth-Modus (SSID wird nicht gesendet)?	Wireless	<ul style="list-style-type: none"> ■ Geben Sie den SSID-Namen manuell ein. ■ Überprüfen Sie den SSID-Namen bzw. den Netzwerkschlüssel anhand der mit dem WLAN-Access-Point/Router gelieferten Anleitung und konfigurieren Sie die Wireless-Netzwerkeinstellungen erneut. (Weitere Informationen finden Sie unter <i>Wenn die SSID nicht sendet</i> auf Seite 11.)
Ich habe alle oben genannten Punkte überprüft und ausgeführt, kann jedoch die Konfiguration des Wireless-Netzwerkes noch immer nicht abschließen. Was kann ich sonst noch tun?	Wireless	Verwenden Sie das Dienstprogramm zum Reparieren der Netzwerkverbindung. Siehe <i>Das Brother-Gerät kann nicht über das Netzwerk scannen. Das Brother-Gerät wird auch nach erfolgreicher Installation nicht im Netzwerk gefunden.</i> auf Seite 93.
Ihre Sicherheitseinstellungen (SSID/Kennwort) sind nicht korrekt.	Wi-Fi Direct®	Bestätigen Sie die SSID und das Kennwort. Wenn Sie das Netzwerk manuell konfigurieren, zeigt Ihr Brother-Gerät die SSID und das Kennwort an. Wenn Ihr Mobilgerät eine manuelle Konfiguration unterstützt, dann werden SSID und Kennwort auf dem Display Ihres Mobilgerätes angezeigt.
Sie benutzen Android™ 4.0.	Wi-Fi Direct®	Wenn Ihr Mobilgerät die Verbindung trennt (ca. sechs Minuten nach Aktivierung von Wi-Fi Direct®), probieren Sie die Tastendruck-Methode über WPS (empfohlen) und stellen Sie G/B für das Brother-Gerät ein.
Ihr Brother-Gerät ist zu weit vom Mobilgerät entfernt.	Wi-Fi Direct®	Stellen Sie Ihr Brother-Gerät max. 1 Meter entfernt vom Mobilgerät auf, wenn Sie die Wi-Fi Direct®-Netzwerkeinstellungen konfigurieren.
Zwischen Ihrem Gerät und dem Mobilgerät befinden sich Hindernisse (z. B. Wände oder Möbel).	Wi-Fi Direct®	Stellen Sie Ihr Brother-Gerät an einer Stelle ohne Hindernisse auf.

Problem	Schnittstelle	Lösung
In der Nähe des Brother-Gerätes oder Mobilgerätes befindet sich ein Wireless-Computer, ein Gerät mit Bluetooth-Unterstützung, ein Mikrowellengerät oder ein digitales schnurloses Telefon.	Wi-Fi Direct®	Stellen Sie andere Geräte etwas weiter entfernt vom Brother-Gerät oder Mobilgerät auf.
Wenn Sie alle obigen Punkte überprüft und ausgeführt haben, Wi-Fi Direct® jedoch noch immer nicht abschließend konfigurieren konnten:	Wi-Fi Direct®	<ul style="list-style-type: none"> ■ Schalten Sie Ihr Brother-Gerät aus und wieder ein. Versuchen Sie dann erneut, eine Konfiguration der Wi-Fi Direct®-Einstellungen auszuführen. ■ Wenn Sie Ihr Brother-Gerät als Client betreiben, überprüfen Sie, wie viele Geräte das aktuelle Wi-Fi Direct®-Netzwerk zulässt. Überprüfen Sie anschließend, wie viele Geräte tatsächlich verbunden sind.

WLAN-Fehlercodes (ADS-2800W / ADS-3600W)

Zeigt das Display einen Fehlercode an, ermitteln Sie anhand der untenstehenden Tabelle den Fehlercode und beheben Sie den Fehler mithilfe der empfohlenen Lösung.

Fehlercode	Empfohlene Lösungen
TS-01	<p>Die Wireless-Einstellung ist nicht aktiviert. Schalten Sie die Wireless-Einstellung ein:</p> <ol style="list-style-type: none"> 1 Drücken Sie an Ihrem Gerät  > Netzwerk > WLAN > Setup-Assist. 2 Wenn WLAN aktivieren? angezeigt wird, drücken Sie zum Start des Wireless-Setup-Assistenten auf Ja.
TS-02	<p>Der Wireless Access Point/Router kann nicht gefunden werden.</p> <ol style="list-style-type: none"> 1 Überprüfen Sie Folgendes: <ul style="list-style-type: none"> ■ Vergewissern Sie sich, dass der Wireless Access Point/Router eingeschaltet ist. ■ Stellen Sie Ihr Gerät in einem Bereich ohne Hindernisse oder näher am Wireless Access Point/Router auf. ■ Stellen Sie für die Konfiguration der Wireless-Einstellungen das Gerät vorübergehend in einem Abstand von ca. 1 Meter vom Wireless Access Point/Router auf. ■ Greift Ihr Wireless Access Point/Router auf MAC-Adressenfilterung zurück, überprüfen Sie, ob die MAC-Adresse des Brother-Gerätes vom Filter zugelassen ist. 2 Wenn Sie die SSID- und Sicherheitsinformationen (SSID / Authentifizierungsmethode / Verschlüsselungsmethode / Netzwerkschlüssel) manuell eingegeben haben, sind diese Informationen möglicherweise fehlerhaft. Überprüfen Sie die SSID- und Sicherheitsinformationen und geben Sie bei Bedarf die richtigen Informationen ein. Ihr Gerät unterstützt keine 5-GHz-SSID/ESSID und Sie müssen eine 2,4-GHz-SSID/ESSID auswählen. Stellen Sie sicher, dass der Access Point/Router auf 2,4 GHz bzw. 2,4 GHz/5 GHz gemischter Modus eingestellt ist.
TS-03	<p>Die eingegebenen Wireless-Netzwerkeinstellungen und Sicherheitseinstellungen sind möglicherweise nicht korrekt. Überprüfen Sie die Wireless-Netzwerkeinstellungen. Überprüfen Sie, ob die eingegebenen oder gewählten SSID- und Sicherheitsinformationen (SSID / Authentifizierungsmethode / Verschlüsselungsmethode / Benutzer-ID / Benutzerkennwort) korrekt sind.</p>

Fehlercode	Empfohlene Lösungen														
<p>TS-04</p>	<p>Die vom gewählten Wireless Access Point/Router verwendeten Authentifizierungs-/Verschlüsselungsmethoden werden von Ihrem Gerät nicht unterstützt. Ändern Sie für den Infrastruktur-Modus die Authentifizierungs- und Verschlüsselungsmethoden des Wireless Access Points/Routers. Ihr Gerät unterstützt die folgenden Authentifizierungsmethoden:</p> <table border="1" data-bbox="443 464 1198 762"> <thead> <tr> <th data-bbox="443 464 821 506">Authentifizierungsmethode</th> <th data-bbox="821 464 1198 506">Verschlüsselungsmethode</th> </tr> </thead> <tbody> <tr> <td data-bbox="443 506 821 590">WPA-Personal</td> <td data-bbox="821 506 1198 548">TKIP</td> </tr> <tr> <td data-bbox="443 590 821 590"></td> <td data-bbox="821 548 1198 590">AES</td> </tr> <tr> <td data-bbox="443 590 821 632">WPA2-Personal</td> <td data-bbox="821 590 1198 632">AES</td> </tr> <tr> <td data-bbox="443 632 821 716">Offen</td> <td data-bbox="821 632 1198 674">WEP</td> </tr> <tr> <td data-bbox="443 716 821 716"></td> <td data-bbox="821 674 1198 716">Keine (unverschlüsselt)</td> </tr> <tr> <td data-bbox="443 716 821 762">Shared key</td> <td data-bbox="821 716 1198 762">WEP</td> </tr> </tbody> </table> <p>Wenn das Problem weiterhin auftritt, sind eventuell die eingegebenen SSID- oder Netzwerkeinstellungen falsch. Überprüfen Sie die Wireless-Netzwerkeinstellungen. Ad-hoc-Modus: Ändern Sie die Authentifizierungs- und Verschlüsselungsmethoden des Computers für die Wireless-Einstellungen. Ihr Gerät unterstützt ausschließlich die Authentifizierungsmethode „Open“ mit optionaler WEP-Verschlüsselung.</p>	Authentifizierungsmethode	Verschlüsselungsmethode	WPA-Personal	TKIP		AES	WPA2-Personal	AES	Offen	WEP		Keine (unverschlüsselt)	Shared key	WEP
Authentifizierungsmethode	Verschlüsselungsmethode														
WPA-Personal	TKIP														
	AES														
WPA2-Personal	AES														
Offen	WEP														
	Keine (unverschlüsselt)														
Shared key	WEP														
<p>TS-05</p>	<p>Die Sicherheitsinformationen (SSID/Netzwerkschlüssel) sind inkorrekt. Überprüfen Sie die SSID- und Sicherheitsinformationen (Netzwerkschlüssel). Wenn der Router die WEP-Verschlüsselung verwendet, geben Sie den als ersten WEP-Schlüssel benutzten Schlüssel ein. Das Brother-Gerät unterstützt nur die Verwendung des ersten WEP-Schlüssels.</p>														
<p>TS-06</p>	<p>Die Wireless-Sicherheitsinformationen (Authentifizierungsmethode / Verschlüsselungsmethode / Netzwerkschlüssel) sind inkorrekt. Überprüfen Sie anhand der Authentifizierungsmethodentabelle für Fehlercode TS-04 die Wireless-Sicherheitsinformationen (Authentifizierungsmethode / Verschlüsselungsmethode / Netzwerkschlüssel). Wenn der Router die WEP-Verschlüsselung verwendet, geben Sie den als ersten WEP-Schlüssel benutzten Schlüssel ein. Das Brother-Gerät unterstützt nur die Verwendung des ersten WEP-Schlüssels.</p>														
<p>TS-07</p>	<p>Das Gerät kann einen Wireless Access Point/Router, an dem WPS aktiviert ist, nicht erkennen. Wenn Sie Ihre Wireless-Einstellungen mit WPS konfigurieren möchten, müssen sowohl Ihr Gerät als auch der Wireless Access Point/Router entsprechend arbeiten.</p> <p>Falls Sie nicht wissen, wie Sie den Wireless Access Point/Router mit WPS zu betreiben haben, sehen Sie in der Dokumentation nach, die mit Ihrem Wireless Access Point/Router mitgeliefert wurde, oder wenden Sie sich an den Hersteller Ihres Wireless Access Points/Routers bzw. an Ihren Netzwerkadministrator.</p> 														
<p>TS-08</p>	<p>Es wurden zwei oder mehr Wireless Access Points gefunden, an denen WPS aktiviert ist. Stellen Sie sicher, dass innerhalb der Reichweite nur an einem Wireless Access Point/Router WPS aktiviert ist, und versuchen Sie es noch einmal.</p>														
<p>TS-20</p>	<p>Das Gerät versucht weiterhin, eine Verbindung zu Ihrem Wireless-Netzwerk herzustellen. Warten Sie einige Minuten und überprüfen Sie dann den WLAN-Status.</p>														

Das Brother-Gerät wird während der Brother-Geräteinstallation nicht im Netzwerk gefunden.

Frage	Schnittstelle	Lösung
Ist der Computer mit dem Netzwerk verbunden?	Verkabelt / Wireless	Vergewissern Sie sich, dass der Computer an ein Netzwerk (beispielsweise eine LAN-Umgebung oder an Internet-Dienste) angeschlossen ist. Für weiteren Support wenden Sie sich an Ihren Netzwerkadministrator.
Ist das Gerät mit dem Netzwerk verbunden und hat es eine gültige IP-Adresse?	Verkabelt / Wireless	(Verkabeltes Netzwerk) Überprüfen Sie, ob der Status in Status (Kabel) auf Aktiv XXXX-XX gesetzt ist. (Wobei XXXX-XX Ihre gewählte Ethernet-Schnittstelle ist.) Siehe <i>So prüfen Sie den Netzwerkstatus (ADS-2800W / ADS-3600W)</i> auf Seite 3. Zeigt das Display Inaktiv oder Kabelgebunden AUS an, fragen Sie Ihren Netzwerkadministrator, ob Ihre IP-Adresse gültig ist. (Wireless-Netzwerk) Stellen Sie sicher, dass Status unter WLAN-Status nicht Keine Verbindung ist. Siehe <i>So überprüfen Sie den WLAN-Status (ADS-2800W / ADS-3600W)</i> auf Seite 9. Zeigt das Display Keine Verbindung an, dann fragen Sie Ihren Netzwerkadministrator, ob die IP-Adresse gültig ist.
Verwenden Sie Sicherheitssoftware?	Verkabelt / Wireless	<ul style="list-style-type: none"> ■ Suchen Sie im Dialogfeld des Installationsprogramms erneut nach dem Brother-Gerät. ■ Wenn während der Installation des Brother-Gerätes die Warnmeldung der Sicherheitssoftware angezeigt wird, erlauben Sie den Zugriff. ■ Weitere Informationen zur Sicherheitssoftware finden Sie unter <i>Ich verwende Sicherheitssoftware.</i> auf Seite 95.
Verwenden Sie einen WLAN-Router?	Wireless	Möglicherweise ist der Privacy Separator Ihres WLAN-Routers aktiviert. Deaktivieren Sie den Privacy Separator.
Ist das Brother-Gerät zu weit entfernt vom WLAN-Access-Point/Router aufgestellt?	Wireless	Stellen Sie das Brother-Gerät für eine Konfiguration der Wireless-Netzwerkeinstellungen innerhalb eines Abstandes von ca. 1 Meter vom WLAN-Access-Point/Router auf.
Befinden sich Hindernisse (zum Beispiel Wände oder Möbel) zwischen dem Gerät und dem WLAN-Access-Point/Router?	Wireless	Stellen Sie Ihr Brother-Gerät in einem Bereich ohne Hindernisse oder näher am Wireless Access Point/Router auf.
Befindet sich in der Nähe des Brother-Gerätes oder des WLAN-Access-Points/Routers ein Wireless-Computer, ein Gerät, das Bluetooth unterstützt, ein Mikrowellengerät oder ein digitales schnurloses Telefon?	Wireless	Stellen Sie alle Geräte in größerer Entfernung vom Brother-Gerät bzw. vom WLAN-Access-Point/Router auf.

**Das Brother-Gerät kann nicht über das Netzwerk scannen.
Das Brother-Gerät wird auch nach erfolgreicher Installation nicht im Netzwerk gefunden.**

Frage	Schnittstelle	Lösung
Verwenden Sie Sicherheitssoftware?	Verkabelt / Wireless	Siehe <i>Ich verwende Sicherheitssoftware.</i> auf Seite 95.
Wurde dem Brother-Gerät eine verfügbare IP-Adresse zugewiesen?	Verkabelt / Wireless	<p>■ Überprüfen Sie die IP-Adresse und die Subnetzmaske.</p> <p>Prüfen Sie, dass die IP-Adresse und die Subnetzmaske sowohl des Computers als auch des Brother-Gerätes korrekt zugeordnet sind und dass sie sich im selben Netzwerk befinden. Weitere Informationen zur Prüfung von IP-Adresse und Subnetzmaske erhalten Sie von Ihrem Netzwerkadministrator.</p> <p>■ (Windows®)</p> <p>Prüfen Sie IP-Adresse und Subnetzmaske mit dem Dienstprogramm zum Reparieren der Netzwerkverbindung.</p> <p>Verwenden Sie das Reparaturprogramm für Netzwerkverbindungen, um die Netzwerkeinstellungen des Brother-Gerätes zu reparieren (es weist die korrekte IP-Adresse und Subnetzmaske zu).</p> <p>Um das Reparaturprogramm für Netzwerkverbindungen anzuwenden, bitten Sie Ihren Netzwerkadministrator um die nötigen Informationen und gehen Sie dann wie folgt vor:</p> <p>HINWEIS</p> <ul style="list-style-type: none"> • (Windows® XP) Sie müssen sich mit Administratorrechten anmelden. • Achten Sie darauf, dass das Brother-Gerät eingeschaltet und mit demselben Netzwerk wie der Computer verbunden ist.

Frage	Schnittstelle	Lösung
<p>Wurde dem Brother-Gerät eine verfügbare IP-Adresse zugewiesen? (Fortsetzung)</p>	<p>Verkabelt / Wireless</p>	<p>1 Legen Sie die mitgelieferte DVD in das DVD-Laufwerk ein. Wenn das Hauptmenü der DVD angezeigt wird, müssen Sie dies schließen.</p> <p>2 Öffnen Sie im jeweiligen Betriebssystem Ihres Computers das Hauptverzeichnis:</p> <ul style="list-style-type: none"> ■ Windows® XP Klicken Sie auf Start > Alle Programme > Zubehör > Windows-Explorer > Arbeitsplatz. ■ Windows Vista®/Windows® 7 Klicken Sie auf  (Start) > Computer. ■ Windows® 8/Windows® 8.1 Klicken Sie auf das Symbol  (Explorer) in der Taskleiste und klicken Sie auf Dieser Computer. ■ Windows® 10 Klicken Sie in der Taskleiste auf das Symbol  (Explorer) und wählen Sie Dieser PC. <p>3 Doppelklicken Sie auf DVD-Laufwerk, doppelklicken Sie auf Werkzeuge, doppelklicken Sie auf NetTool und doppelklicken Sie dann auf BrotherNetTool.exe, um das Programm zu starten.</p> <p>HINWEIS</p> <p>Wenn der Bildschirm Benutzerkontensteuerung erscheint: (Windows Vista®) Klicken Sie auf Fortsetzen (Zulassen). (Windows® 7/Windows® 8/Windows® 8.1/Windows® 10) Klicken Sie auf Ja.</p> <p>4 Folgen Sie den Bildschirmanweisungen.</p> <p>Wenn auch nach der Verwendung des Dienstprogramms zum Reparieren der Netzwerkverbindung die IP-Adresse und Subnetzmaske nicht richtig zugewiesen sind, wenden Sie sich an Ihren Netzwerkadministrator.</p>
<p>Verbinden Sie das Brother-Gerät drahtlos mit dem Netzwerk?</p>	<p>Wireless</p>	<ul style="list-style-type: none"> ■ Prüfen Sie den Status unter WLAN-Status. Siehe <i>So überprüfen Sie den WLAN-Status (ADS-2800W / ADS-3600W)</i> auf Seite 9. Zeigt das Display <i>Keine Verbindung an</i>, dann fragen Sie Ihren Netzwerkadministrator, ob die IP-Adresse gültig ist. ■ Siehe <i>Das Brother-Gerät wird während der Brother-Geräteinstallation nicht im Netzwerk gefunden.</i> auf Seite 92.
<p>Ich habe alle obigen Punkte überprüft und ausgeführt, aber das Brother-Gerät scannt nicht. Was kann ich sonst noch tun?</p>	<p>Verkabelt / Wireless</p>	<p>Deinstallieren Sie das Brother-Gerät und installieren Sie es erneut.</p>

Ich verwende Sicherheitssoftware.

Frage	Schnittstelle	Lösung
<p>Haben Sie während der Installation des Brother-Gerätes, beim Starten der Anwendung oder beim Verwenden der Scanfunktionen die Sicherheitswarnung im Dialogfeld Akzeptiert?</p>	<p>Verkabelt / Wireless</p>	<p>Wenn Sie bei der Sicherheitswarnung im Dialogfeld nicht Akzeptiert gewählt haben, verweigert die Firewall-Funktion Ihrer Sicherheitssoftware möglicherweise den Zugriff. Einige Sicherheitsprogramme blockieren ggf. den Zugriff, ohne ein Dialogfeld zur Sicherheitswarnung anzuzeigen. Lesen Sie die Anleitung der Sicherheitssoftware oder wenden Sie sich an den Hersteller, um den Zugriff freizugeben.</p>
<p>Ich möchte die notwendigen Portnummern für die Sicherheitssoftware-Einstellungen wissen.</p>	<p>Verkabelt / Wireless</p>	<p>Die folgenden Portnummern werden von den Brother-Netzwerkfunktionen verwendet:</p> <ul style="list-style-type: none"> ■ Scannen im Netzwerk → Portnummer 54925/Protokoll UDP ■ Scannen im Netzwerk, Remote Setup¹ → Portnummer 161 und 137/Protokoll UDP ■ BRAdmin Light¹ → Portnummer 161/Protokoll UDP <p>¹ Nur Windows®.</p> <p>Siehe die Anleitung der Sicherheitssoftware oder wenden Sie sich an den Hersteller, um Informationen zum Öffnen der Ports zu erhalten.</p>

Ich möchte überprüfen, ob meine Netzwerkgeräte ordnungsgemäß funktionieren.

Frage	Schnittstelle	Lösung
Ist das Brother-Gerät, der Access Point/Router oder der Netzwerk-Hub eingeschaltet?	Verkabelt / Wireless	Stellen Sie sicher, dass Sie alle Punkte unter <i>Vergewissern Sie sich, dass Sie Folgendes überprüft haben:</i> auf Seite 88 überprüft haben.
Wo kann ich die Netzwerkeinstellungen meines Brother-Gerätes, z. B. die IP-Adresse, finden?	Verkabelt / Wireless	<ul style="list-style-type: none"> ■ Web-based Management 1 Starten Sie Web-based Management und greifen Sie auf das Brother-Gerät zu (siehe Schritt ❶ unter Seite 39). 2 Wenn der Web-based Management-Bildschirm erscheint, klicken Sie auf die Registerkarte Netzwerk und dann in der linken Navigationsleiste auf Netzwerkstatus. ■ Bedienfeld (ADS-2800W / ADS-3600W) <p>Prüfen Sie die Einstellungen unter <i>Netzwerk</i> im Gerätebedienfeld.</p>
Wie kann ich den Verbindungsstatus meines Brother-Gerätes prüfen?	Verkabelt / Wireless	<ul style="list-style-type: none"> ■ Web-based Management 1 Starten Sie Web-based Management und greifen Sie auf das Brother-Gerät zu (siehe Schritt ❶ unter Seite 39). 2 Wenn der Web-based Management-Bildschirm erscheint, klicken Sie auf die Registerkarte Netzwerk und dann in der linken Navigationsleiste auf Netzwerkstatus. ■ Bedienfeld (ADS-2800W / ADS-3600W) <p>(Verkabeltes Netzwerk) Überprüfen Sie, ob <i>Status in Status (Kabel)</i> auf <i>Aktiv XXXX-XX</i> eingestellt ist (wobei <i>XXXX-XX</i> Ihre gewählte Ethernet-Schnittstelle ist). So überprüfen Sie den Netzwerkstatus: Drücken Sie  > <i>Netzwerk</i> > <i>LAN (Kabel)</i> > <i>Status (Kabel)</i> > <i>Status</i>. Zeigt das Display <i>Inaktiv</i> oder <i>Kabelgebunden AUS</i> an, fragen Sie Ihren Netzwerkadministrator, ob Ihre IP-Adresse gültig ist.</p> <p>(Wireless-Netzwerk) Stellen Sie sicher, dass <i>Status</i> unter <i>WLAN-Status</i> nicht <i>Keine Verbindung</i> ist. Siehe <i>So überprüfen Sie den WLAN-Status (ADS-2800W / ADS-3600W)</i> auf Seite 9. Wenn das Display <i>Keine Verbindung</i> anzeigt, fragen Sie Ihren Netzwerkadministrator, ob Ihre IP-Adresse gültig ist.</p>

Frage	Schnittstelle	Lösung
<p>Können Sie das Brother-Gerät vom Computer aus mit dem „Ping“-Befehl ansprechen?</p>	<p>Verkabelt / Wireless</p>	<p>Geben Sie folgenden „Ping“-Befehl mit der IP-Adresse oder dem Knotennamen des Brother-Gerätes von Ihrem Computer über die Windows®-Eingabeaufforderung ein: <code>ping <IP-Adresse> oder <Knotenname></code>.</p> <ul style="list-style-type: none"> ■ Erfolgreich > Das Brother-Gerät arbeitet korrekt und ist mit demselben Netzwerk wie der Computer verbunden. ■ Nicht erfolgreich > Das Brother-Gerät ist nicht mit demselben Netzwerk wie der Computer verbunden. <p>(Windows®) Wenden Sie sich an Ihren Netzwerkadministrator und verwenden Sie das Dienstprogramm zum Reparieren der Netzwerkverbindung, um die IP-Adresse und die Subnetzmaske automatisch zuzuweisen. Ausführliche Informationen zum Dienstprogramm für eine Reparatur der Netzwerkverbindung finden Sie unter <i>Wurde dem Brother-Gerät eine verfügbare IP-Adresse zugewiesen? unter Das Brother-Gerät kann nicht über das Netzwerk scannen. Das Brother-Gerät wird auch nach erfolgreicher Installation nicht im Netzwerk gefunden.</i> auf Seite 93.</p> <p>(Macintosh) Vergewissern Sie sich, dass IP-Adresse und Subnetzmaske korrekt eingestellt sind. Siehe <i>Überprüfen Sie die IP-Adresse und die Subnetzmaske</i> unter <i>Das Brother-Gerät kann nicht über das Netzwerk scannen. Das Brother-Gerät wird auch nach erfolgreicher Installation nicht im Netzwerk gefunden.</i> auf Seite 93.</p>
<p>Verbindet sich das Brother-Gerät mit dem Wireless-Netzwerk?</p>	<p>Wireless</p>	<p>Prüfen Sie den Status unter WLAN-Status. Siehe <i>So überprüfen Sie den WLAN-Status (ADS-2800W / ADS-3600W)</i> auf Seite 9. Zeigt das Display <i>Keine Verbindung</i> an, dann fragen Sie Ihren Netzwerkadministrator, ob die IP-Adresse gültig ist.</p>
<p>Ich habe alle oben genannten Punkte überprüft und ausgeführt, aber das Problem tritt weiter auf. Was kann ich sonst noch tun?</p>	<p>Wireless</p>	<p>Lesen Sie die Anleitung, die Sie mit dem WLAN-Access-Point/Router erhalten haben, um die SSID- und Netzwerkschlüssel-Informationen zu ermitteln und sie richtig einzustellen. Ausführliche Informationen zu SSID und Netzwerkschlüssel finden Sie unter <i>Sind die Sicherheitseinstellungen (SSID/Netzwerkschlüssel) korrekt?</i> unter <i>Ich kann die Konfiguration des Wireless-Netzwerks nicht abschließen.</i> auf Seite 89.</p>

Einstellungstypen

Außerdem sind die folgenden, optionalen Netzwerkfunktionen verfügbar:

- Webdienste zum Scannen (Windows Vista®, Windows® 7, Windows® 8, Windows® 8.1 und Windows® 10)
- Vertical Pairing (Windows® 7, Windows® 8, Windows® 8.1 und Windows® 10)

HINWEIS

Vergewissern Sie sich, dass sich der Hostcomputer und das Gerät entweder im selben Subnetzwerk befinden oder dass der Router für die Datenübertragung zwischen den beiden Geräten richtig konfiguriert ist.

Installieren von Treibern zum Scannen über Webdienste (Windows Vista®, Windows® 7, Windows® 8, Windows® 8.1, Windows® 10)

Mit der Webdienste-Funktion können Sie Geräte im Netzwerk überwachen und so den Installationsprozess der Treiber vereinfachen. Die zum Scannen über Webdienste verwendeten Treiber können installiert werden, indem Sie mit der rechten Maustaste auf das Scannersymbol auf dem Computer klicken. Daraufhin wird der Webdienste-Port (WSD-Port) automatisch erstellt. (Weitere Informationen zum Scannen über Webdienste finden Sie in *Scannen über Webdienste (Windows Vista®, Windows® 7, Windows® 8, Windows® 8.1 und Windows® 10)* im *Benutzerhandbuch*.)

HINWEIS

Bevor Sie diese Einstellung konfigurieren, müssen Sie die IP-Adresse Ihres Gerätes konfigurieren.

1 Öffnen Sie im jeweiligen Betriebssystem Ihres Computers die Netzwerkeinstellungen:

- Windows Vista®

Klicken Sie auf  (Start) > **Netzwerk**.

- Windows® 7

Klicken Sie auf  (Start) > **Systemsteuerung** > **Netzwerk und Internet** > **Netzwerkcomputer und-geräte anzeigen**.

- Windows® 8/Windows® 8.1

Bewegen Sie die Maus in die untere rechte Desктоpecke. Die Menüleiste erscheint. Klicken Sie auf **Einstellungen** > **PC-Einstellungen ändern** > **Geräte** > **Gerät hinzufügen**.

- Windows® 10

Klicken Sie auf  (Start) > **Einstellungen** > **Geräte** > **Drucker & Scanner**.

- 2 Der Webdienst-Name des Gerätes wird mit dem Scannersymbol angezeigt.
 - Windows Vista®/Windows® 7/Windows® 8/Windows® 8.1
Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie installieren möchten.
 - Windows® 10
Klicken Sie auf das Gerät, das Sie installieren möc.

HINWEIS

Der Webdienst-Name des Brother-Gerätes besteht aus dem Namen des Modells und der MAC-Adresse (Ethernet-Adresse) (z. B. Brother ADS-XXXXX (Modellname) [XXXXXXXXXXXXX] (MAC-Adresse/Ethernet-Adresse)).

- 3 Starten Sie die Geräteinstallation:
 - Windows Vista®/Windows® 7
Klicken Sie im Dropdown-Menü des Gerätes auf **Installieren**.
 - Windows® 8/Windows® 8.1
Wählen Sie das Gerät, das Sie installieren möchten.
 - Windows® 10
Klicken Sie auf **Geräte hinzufügen**.

Installation von Netzwerk-Scannen für den Infrastruktur-Modus mit Vertical Pairing (Windows® 7, Windows® 8, Windows® 8.1, Windows® 10)

Windows® Vertical Pairing ist eine Technologie, mit der sich das Wireless-Gerät, das diese Funktion unterstützt, mit dem Infrastruktur-Netzwerk über die WPS-PIN-Methode und die Webdienste-Funktion verbinden kann. Außerdem ermöglicht diese Funktion die Scannertreiber-Installation über das Scannersymbol im Bildschirm **Gerät hinzufügen**.

Sie können im Infrastruktur-Modus das Gerät mit dem Wireless-Netzwerk verbinden und dann mit dieser Funktion den Scannertreiber installieren. Gehen Sie dazu wie folgt vor:

HINWEIS

- Wenn Sie die Webdienste-Funktion des Gerätes ausgeschaltet haben, müssen Sie sie wieder einschalten. Die Standardeinstellung für die Webdienste des Brother-Gerätes ist „Ein“. Sie können die Webdienste-Einstellung über Web-based Management (Webbrowser) oder mit BRAdmin Professional 3 ändern.
- Vergewissern Sie sich, dass Ihr WLAN-Access Point/Router mit dem Kompatibilitätslogo für Windows® 7, Windows® 8, Windows® 8.1 oder Windows® 10 gekennzeichnet ist. Wenn Sie sich in Bezug auf das Kompatibilitätslogo nicht sicher sind, wenden Sie sich an den Hersteller des Access Points/Routers.
- Vergewissern Sie sich, dass Ihr Computer mit dem Kompatibilitätslogo für Windows® 7, Windows® 8, Windows® 8.1 oder Windows® 10 gekennzeichnet ist. Wenn Sie sich in Bezug auf das Kompatibilitätslogo nicht sicher sind, wenden Sie sich an den Hersteller des Computers.
- Wenn Sie das Wireless-Netzwerk mit Hilfe einer externen Wireless-Netzwerkkarte (NIC; Network Interface Card) konfigurieren, stellen Sie sicher, dass diese Netzwerkkarte mit dem Kompatibilitätslogo für Windows® 7, Windows® 8, Windows® 8.1 oder Windows® 10 gekennzeichnet ist. Weitere Informationen erhalten Sie beim Hersteller der Wireless-Netzwerkkarte.
- Um einen Windows® 7, Windows® 8, Windows® 8.1 oder Windows® 10-Computer als Registrierungsstelle verwenden zu können, müssen Sie diesen zunächst im Netzwerk registrieren. Lesen Sie die mit dem WLAN-Access-Point/Router gelieferte Anleitung.

- 1 Schalten Sie das Gerät ein.
- 2 Stellen Sie am Gerät den WPS-Modus ein (siehe *Verwenden der PIN-Methode des Wi-Fi Protected Setup™ (WPS)* auf Seite 19).
- 3 Funktion Gerät hinzufügen für Ihr Betriebssystem ausführen:
 - Windows® 7
Klicken Sie auf  (**Start**) > **Geräte und Drucker** > **Gerät hinzufügen**.
 - Windows® 8/Windows® 8.1
Bewegen Sie die Maus in die untere rechte Desктоpecke. Klicken Sie in der Menüleiste auf **Einstellungen** > **Systemsteuerung** > **Hardware und Sound** > **Geräte und Drucker** > **Gerät hinzufügen**.
 - Windows® 10
Klicken Sie auf  (**Start**) > **Einstellungen** > **Geräte > Drucker & Scanner** > **Drucker oder Scanner hinzufügen**.
- 4 Wählen Sie das Gerät aus und geben Sie die von dem Gerät angezeigte PIN ein.

- 5 Wählen Sie das Infrastruktur-Netzwerk aus, zu dem Sie eine Verbindung herstellen möchten, und klicken Sie auf **Weiter**.
- 6 Wenn das Gerät im Dialogfeld **Geräte und Drucker** angezeigt wird, ist die Wireless-Konfiguration und die Scannertreiber-Installation erfolgreich abgeschlossen.

Unterstützte Protokolle und Sicherheitsfunktionen

Schnittstelle	Ethernet	10BASE-T, 100BASE-TX
	Wireless (ADS-2800W / ADS-3600W)	IEEE 802.11b/g/n (Infrastruktur-Modus/Ad-hoc-Modus) IEEE 802.11g/n (Wi-Fi Direct®)
Netzwerk (allgemein)	Protokoll (IPv4)	ARP, RARP, BOOTP, DHCP, APIPA (Auto IP), WINS/NetBIOS-Namensauflösung, DNS Resolver, mDNS, LLNMR Responder, Custom Raw Port/Port9100, SMTP Client, FTP Client und Server, LDAP Client (nur ADS-2800W / ADS-3600W), CIFS Client, WebDAV-Client, SNMPv1/v2c/v3 (MD5/SHA1), HTTP/HTTPS-Server, TFTP-Client und -Server, ICMP, Web Services (Scan), SNTP-Client
	Protokoll (IPv6)	NDP, RA, DNS Resolver, mDNS, LLNMR Responder, Custom Raw, Port/Port9100, SMTP Client, FTP Client und Server, LDAP Client, CIFS Client, TELNET-Server, SNMPv1/v2c/v3, HTTP/HTTPS-Server, TFTP Client und Server, ICMPv6, Web Services (Scan), SNTP Client, WebDav Client
Netzwerk (Sicherheit)	Verkabelt	SMTP-AUTH, SSL/TLS (HTTPS, SMTP), SSH, SNMP v3, 802.1x (EAP-MD5, EAP-FAST, PEAP, EAP-TLS, EAP-TTLS), Kerberos, IPsec
	Wireless (ADS-2800W / ADS-3600W)	SMTP-AUTH, SSL/TLS (HTTPS, SMTP), SSH, SNMP v3, 802.1x (LEAP, EAP-FAST, PEAP, EAP-TLS, EAP-TTLS), Kerberos, Ipsec
E-Mail (Sicherheit) (ADS-2800W / ADS-3600W)	Verkabelt und Wireless	SMTP-AUTH, SSL/TLS (SMTP)
Netzwerk (Wireless) (ADS-2800W / ADS-3600W)	Wireless- Zertifizierung	Wi-Fi Certification Mark-Lizenz (WPA™/WPA2™ - Enterprise, Personal), Wi-Fi Protected Setup™ (WPS) Identifier Mark-Lizenz, Wi-Fi CERTIFIED Wi-Fi Direct®

Web-based Management Funktionstabelle

HINWEIS

Sie erhalten weitere Informationen, wenn Sie in der Schnittstelle für das Web-based Management rechts auf jeder Seite auf  klicken.

Haupt-kategorie	Unter-kategorie	Funktionsmenü	Funktionsoptionen	Beschreibung / optionale Einstellungen
Allgemein	-	Status	Gerätestatus / Automatische Aktualisierung / WebSprache / Gerätestandort	Gerätestatus, Kontakt und Ort anzeigen. Sie können die Sprache der Schnittstelle für das Web-based Management ändern.
	-	Automatische Aktualisierung	Aktualisierungsintervall	Aktualisierungsintervall konfigurieren (zwischen 15 Sekunden und 60 Minuten).
	-	Wartungs- informationen	Knoteninformation / Verbleibende Lebensdauer / Gescannte Seiten (insgesamt) / Bisher ausgetauscht / Reset-Anzahl / Fehlerzahl / Fehler-Chronik (letzte 10 Fehler)	Zeigt die Wartungsinformationen zum Brother-Gerät an, einschließlich Modell, Angaben zu Verbrauchsmaterialien, Seitenzähler und Fehler. Klicken Sie auf Senden , um die Seite mit den Wartungsinformationen in eine CSV-Datei umzuwandeln.
	-	Gerät suchen	Knotenname / Modellname / Gerätestatus / IP-Adresse	Zeigen Sie alle mit dem Netzwerk verbundenen Geräte an.
	-	Ansprechpartner & Standort	Ansprechpartner / Standort	Nach der Konfiguration von Kontakt und Ort können die Informationen unter Allgemein > Status > Gerätestandort angezeigt werden.
	-	Energiesparmodus	Energiesparmodus	Energiesparmodus konfigurieren (bis zu 90 Minuten).
	-	Automatische Abschaltung	Automatische Abschaltung	
	-	Lautstärke	Toneffekte	Konfigurieren Sie die Lautstärke (Aus / Leise / Normal / Laut).
	-	Bedienfeld (ADS-2800W / ADS-3600W)	Beleuchtung / Dimmer	
-	Geplante Wartungsmeldung	Geplante Wartungsmeldung		

Haupt-kategorie	Unter-kategorie	Funktionsmenü	Funktionsoptionen	Beschreibung / optionale Einstellungen
Adressbuch (ADS-2800W/ ADS-3600W)	-	Adresse	Adresse / E-Mail-Adresse / Name	E-Mail-Adresse und Namen registrieren (bis zu 300).
	-	Rundsende-Gruppen	Gruppe / Adresse / Name / Mitglieder	Kontaktgruppen registrieren (bis zu 20). Wählen Sie Adressnr. aus und klicken Sie auf Wählen , um die Gruppenmitglieder zu konfigurieren.
	-	LDAP	LDAP-Suche / Schnelleinstellungen / Erweiterte Einstellungen	LDAP-Einstellungen konfigurieren.
	-	Importieren	Datendatei „Adressbuch“ / Datendatei „Gruppe“	
	-	Exportieren		
E-Mail (ADS-2800W/ ADS-3600W)	-	E-Mail (Senden)	E-Mail (Betreff) / E-Mail (Text) / Max. Größe / Sendebestätigung senden / SMTP	Konfiguriert die Einstellungen zum Versenden von E-Mails, wie Betreff, Nachricht, Begrenzung der E-Mail-Größe und Sendebestätigung. Klicken Sie auf SMTP , um zu Netzwerk > Netzwerk > Protokoll > SMTP > Erweiterte Einstellungen zu gelangen.
Scannen	-	Scannen	Erkenn. Mehrfacheinz / Korrektur Scan-Offset / Startseite Offset X / Startseite Offset Y / Rückseite Offset X / Rückseite Offset Y / Scan-Ergebnis anzeigen	
	-	Scan-Auftrag E-Mail-Bericht (ADS-2800W / ADS-3600W)	SMTP-Serveradresse / Administratoradresse / SMTP / Scan to E-Mail-Server / Scannen: FTP / Scannen: SFTP / Scan to SMB / Scannen: SharePoint	
	-	Dateiname Scan	Stil Dateiname / Datum und Uhrzeit hinzufügen / Zähler / Scan to USB 1–5 / Scan to E-Mail-Server 1–10 / Scannen: FTP/SFTP 1–15 / Scannen: Netzwerk/SharePoint 1–15	

Haupt-kategorie	Unter-kategorie	Funktionsmenü	Funktionsoptionen	Beschreibung / optionale Einstellungen
Scannen (Fortsetzung)	-	Scan to USB	Dateiname / Qualität / Auto. Farberkennung anpassen / Dateityp / Kennwort für sicheres PDF (ADS-2400N / ADS-3000N) / Dokumentengröße / Einstellungen Rand / Dateigröße / Auto Ausrichtung / Leerseite überspringen / Leere Seite Empfindlichkeit überspr. / 2-seitiger Scan / Helligkeit / Kontrast / Fortlaufender Scan (ADS-2800W / ADS-3600W)	Konfigurieren der Scan-to-USB-Einstellungen.
	-	Scan to E-Mail-Server (ADS-2800W / ADS-3600W)	Dateiname / Qualität / Auto. Farberkennung anpassen / Farbe / Schwarz-weiß/Grau / Dateityp / Dokumentengröße / Einstellungen Rand / Dateigröße / Auto Ausrichtung / Leerseite überspringen / Leere Seite Empfindlichkeit überspr. / 2-seitiger Scan / Helligkeit / Kontrast / Fortlaufender Scan (ADS-2800W / ADS-3600W) / An meine E-Mail-Adresse senden	Konfiguration der Scan-to-E-Mail-Server-Einstellungen.
	-	Scannen:PC (ADS-2400N / ADS-3000N)	Scannen auf	
	-	Scannen: FTP/ FTP/Netzwerk/ SharePoint	Profil 1–25 / An meinen Ordner senden (ADS-2800W / ADS-3600W)	Konfiguration der Einstellungen von Scannen: FTP/SFTP/Netzwerk/SharePoint
	-	Scannen: FTP/ SFTP/Netzwerk/ SharePoint- Profile	Profil 1–25	Konfiguration der Profileinstellungen.
	-	Profil (FTP)	Profilname / Host-Adresse / Benutzername / Kennwort / Zielordner / Dateiname / Qualität / Auto. Farberkennung anpassen / Dateityp / Kennwort für sicheres PDF (ADS-2400N / ADS-3000N) / Dokumentengröße / Einstellungen Rand / Dateigröße / Auto Ausrichtung / Leerseite überspringen / Leere Seite Empfindlichkeit überspr. / 2-seitiger Scan / Helligkeit / Kontrast / Fortlaufender Scan (ADS-2800W / ADS-3600W) / Passiv-Modus / Port-Nummer	Konfiguration der Profileinstellungen. Weitere Informationen siehe <i>Ändern der Konfiguration Scannen: FTP</i> auf Seite 49.

Haupt-kategorie	Unter-kategorie	Funktionsmenü	Funktionsoptionen	Beschreibung / optionale Einstellungen
Scannen (Fortsetzung)	-	Profil (SFTP)	Profilname / Host-Adresse / Benutzername / Authentifizierungsmethode / Client-Schlüsselpaar / Öffentlicher Serverschlüssel / Zielordner / Dateiname / Qualität / Auto. Farberkennung anpassen / Dateityp / Kennwort für sicheres PDF (ADS-2400N / ADS-3000N) / Dokumentengröße / Einstellungen Rand / Dateigröße / Auto Ausrichtung / Leerseite überspringen / Leere Seite Empfindlichkeit überspr. / 2-seitiger Scan / Helligkeit / Kontrast / Fortlaufender Scan (ADS-2800W / ADS-3600W) / Port-Nummer	Konfiguration der Profileinstellungen. Weitere Informationen siehe <i>Ändern der Konfiguration Scannen: SFTP</i> auf Seite 50.
	-	Profil (Netzwerk)	Profilname / Netzwerkordnerpfad / Dateiname / Qualität / Auto. Farberkennung anpassen / Dateityp / Kennwort für sicheres PDF (ADS-2400N / ADS-3000N) / Dokumentengröße / Einstellungen Rand / Dateigröße / Auto Ausrichtung / Leerseite überspringen / Leere Seite Empfindlichkeit überspr. / 2-seitiger Scan / Helligkeit / Kontrast / Fortlaufender Scan (ADS-2800W / ADS-3600W) / PIN zur Authentifizierung verwenden / PIN-Code / Authentifizierungsmethode / Benutzername / Kennwort / Datum/Uhrzeit	Konfiguration der Profileinstellungen. Weitere Informationen siehe <i>Ändern der Konfiguration von Scan to SMB (Windows®)</i> auf Seite 52.

Haupt-kategorie	Unter-kategorie	Funktionsmenü	Funktionsoptionen	Beschreibung / optionale Einstellungen
Scannen (Fortsetzung)	-	Profil (SharePoint)	Profilname / SharePoint- Siteadresse / SSL/TLS / Dateiname / Qualität / Auto. Farberkennung anpassen / Dateityp / Kennwort für sicheres PDF (ADS-2400N / ADS-3000N) / Dokumentengröße / Einstellungen Rand / Dateigröße / Auto Ausrichtung / Leerseite überspringen / Leere Seite Empfindlichkeit überspr. / 2-seitiger Scan / Helligkeit / Kontrast / Fortlaufender Scan (ADS-2800W / ADS-3600W) / PIN zur Authentifizierung verwenden / PIN-Code / Authentifizierungsmethode / Benutzername / Kennwort / Datum/Uhrzeit	Konfiguration der Profileinstellungen. Weitere Informationen siehe <i>Ändern der Konfiguration von Scannen: SharePoint (Windows®)</i> auf Seite 54.
	-	Scannen auf Netzwerkgerät (ADS-2400N / ADS-3000N)	Netzwerkgerät1 / Typ / Ziel / Netzwerkgerät2 / Typ / Ziel / Netzwerkgerät3 / Typ / Ziel	
	-	Scan von PC	Scan ziehen	

Haupt-kategorie	Unter-kategorie	Funktionsmenü	Funktionsoptionen	Beschreibung / optionale Einstellungen
Administrator	-	Anmeldekennwort	Kennwort	Konfigurieren Sie das Kennwort für eine Anmeldung zum Web-based Management. Diese Einstellungen können Sie ohne Anmeldung nur auf der Registerkarte Allgemein verändern.
	-	Funktion zur Nutzungseinschränkung (ADS-2800W / ADS-3600W)		
	-	Benutzersperre (ADS-2800W / ADS-3600W)	Web / PC / Netzwerk / FTP/SFTP / E-Mail Server / Share Point / WS Scan / USB	Die Benutzersperre sperrt benutzerabhängig bestimmte Scan- und Web Connect-Funktionen. Weitere Informationen siehe <i>Benutzersperre 3.0</i> (ADS-2800W / ADS-3600W) auf Seite 85.
	-	Active Directory-Authentifizierung (ADS-2800W / ADS-3600W)	Benutzer-ID speichern / Active Directory-Serveradresse / Active Directory-Domänenname / Auf Basisverzeichnis für Benutzer zugreifen / Protokoll und Authentifizierungsmethode / E-Mail-Adresse abrufen / LDAP-Serverport / LDAP-Suchverzeichnis / SNTP	Die Active Directory-Authentifizierung schränkt die Nutzung des Brother-Gerätes ein. Weitere Informationen siehe <i>Konfigurieren der Active Directory LDAP-Authentifizierung</i> (ADS-2800W / ADS-3600W) auf Seite 43.
	-	LDAP-Authentifizierung (ADS-2800W / ADS-3600W)	Benutzer-ID speichern / LDAP-Server-Adresse / E-Mail-Adresse abrufen / LDAP-Serverport / LDAP-Suchverzeichnis / Namensattribut (Suchschlüssel) / SNTP	Die LDAP-Authentifizierung schränkt die Nutzung Ihres Brother-Gerätes ein. Weitere Informationen siehe <i>Ändern der LDAP-Konfiguration</i> auf Seite 44.
	-	Einstellsperre (ADS-2800W / ADS-3600W)	Einstellsperre / Kennwort	Konfigurieren Sie das Kennwort zur Änderung von Geräteeinstellungen am Display des Brother-Gerätes.
	-	Signierte PDF	Wählen Sie das Zertifikat / Zertifikat	Konfigurieren Sie die Zertifikateinstellungen für Signierte PDF.
	-	Datum/Uhrzeit	Datum / Uhrtyp / Uhrzeit / Zeitzone / Zeitumstellung / Mit SNTP-Server synchron. / SNTP	
	-	Reset-Menü	Reset-Einstellungen / Netzwerk / Adressbuch / Alle Einstell. / Werkseitige Einstellungen	
	-	Firmware-Update	Modellname / Seriennummer / Firmware-Version / MAIN / Firmware-Update / Proxy	Siehe <i>Firmware-Update</i> auf Seite 87

Haupt-kategorie	Unter-kategorie	Funktionsmenü	Funktionsoptionen	Beschreibung / optionale Einstellungen
Netzwerk	Netzwerk	Netzwerkstatus	Verkabelt / Wireless	Anzeigen des Netzwerkstatus.
		Schnittstelle (ADS-2800W / ADS-3600W)	Schnittstelle / Wi-Fi Direct	Ändern Sie die Schnittstelle.
		Protokoll	Web-based Management (Webserver) / Telnet / SNMP / Remote Setup / Raw-Port / Webdienst / Proxy / Netzwerk-Scan / SMTP / FTP-Server / FTP-Client / SFTP / TFTP / WebDAV / CIFS / LDAP / mDNS / LLNMR / SNMP	Konfigurieren Sie die Protokolleinstellungen des Brother-Gerätes. Aktivieren Sie das Kontrollkästchen für die Protokolle, die Sie ändern möchten.
		Benachrichtigung	SMTP-Serveradresse / E-Mail-Adresse des Geräts / SMTP / Administratoradresse	Konfigurieren der Einstellungen der Fehlerbenachrichtigungen.
		E-Mail-Bericht (ADS-2800W / ADS-3600W)	SMTP-Serveradresse / E-Mail-Adresse / SMTP / Datum/Uhrzeit / Administratoradresse	
	Verkabelt	TCP/IP (Verkabelt)	Ethernet 10/100/1000 BASE-T / IP-Adresse / Subnet Mask / Gateway / Boot-Methode / Erweitere Einstellungen / Schnittstelle	Konfigurieren Sie die TCP/IP (Verkabelt)-Einstellungen.
		Knotenname (Verkabelt)	Knotenname	
		NetBIOS (Verkabelt)	NETBIOS/IP / Computername / WINS-Servermethode / Primäre WINS-Server-IP-Adresse / Sekundäre WINS-Server-IP-Adresse	
		IPv6 (Verkabelt)	IPv6 / Statische IPv6-Adresse / Primäre DNS-Server-IP-Adresse / Sekundäre DNS-Server-IP-Adresse / IPv6-Adressenliste	
		Ethernet	Ethernet-Modus	
		802.1x-Authentifizierungs	802.1x-Status (verkabelt) / Authentifizierungsmethode / Innere Authentifizierungsmethode / Benutzer-ID / Kennwort / Client-Zertifikat / Server-Zertifikat-Verifizierung / Server-ID / Zertifikat	



Haupt-kategorie	Unter-kategorie	Funktionsmenü	Funktionsoptionen	Beschreibung / optionale Einstellungen
Netzwerk (Fortsetzung)	Wireless (ADS-2800W/ ADS-3600W)	TCP/IP (Wireless)	IEEE 802.11b/g/n / IP-Adresse / Subnet Mask / Gateway / Boot-Methode / Erweiterte Einstellungen / Schnittstelle	Konfigurieren Sie die TCP/IP- (Wireless-)Einstellungen.
		Knotenname (Wireless)	Knotenname	
		NetBIOS (Wireless)	NETBIOS/IP / Computername / WINS-Servermethode / Primäre WINS-Server-IP-Adresse / Sekundäre WINS-Server-IP-Adresse	
		IPv6 (Wireless)	IPv6 / Statische IPv6-Adresse / Primäre DNS-Server-IP-Adresse / Sekundäre DNS-Server-IP-Adresse / IPv6-Adressenliste	
		Wireless (Setup-Assistent)		Klicken Sie auf Assistent starten , um den Setup-Assistenten für Ihr Wireless-Netzwerk zu starten.
		Wireless (Privatbereich)	Aktueller Status / Kommunikationsmodus / Wireless Netzwerkname (SSID) / Kanal / Authentifizierungsmethode / Verschlüsselungsmodus / Netzwerkschlüssel	
		Wireless (Firmenbereich)	Aktueller Status / Kommunikationsmodus / Wireless Netzwerkname (SSID) / Kanal / Authentifizierungsmethode / Innere Authentifizierungsmethode / Verschlüsselungsmodus / Benutzer-ID / Kennwort Client-Zertifikat / Server-Zertifikat-Verifizierung / Server-ID / Zertifikat	

Haupt-kategorie	Unter-kategorie	Funktionsmenü	Funktionsoptionen	Beschreibung / optionale Einstellungen
Netzwerk (Fortsetzung)	Sicherheit	IPv4-Filter	IP-Filter verwenden / Administrator-IP-Adresse / Zugriffseinstellung	Konfigurieren Sie die Zugriffseinstellungen durch Filtern der IP-Adresse.
		Zertifikat	Zertifikatliste / Privates Zertifikat erstellen / Zertifikatsignieranforderung (CSR) erstellen / Zertifikat installieren / Zertifikat und Private Key importieren	Konfigurieren Sie die Zertifikateinstellungen.
		CA-Zertifikat	CA-Zertifikatliste / CA-Zertifikat importieren	Konfigurieren Sie die CA-Zertifikateinstellungen.
		Client-Schlüsselpaar	Liste der Client-Schlüsselpaare / Neues Client-Schlüsselpaar erstellen	Konfigurieren Sie die Client-Schlüsselpaareinstellungen.
		Öffentlicher Serverschlüssel	Liste der öffentlichen Serverschlüssel / Öffentlichen Serverschlüssel importieren	Konfigurieren Sie die Einstellungen für Öffentliche Serverschlüssel.
		IPsec	Status / Aushandlungsmodus / Jeglicher Nicht-IPsec-Verkehr / Broadcast/Multicast-Bypass / Protokoll-Bypass / Richtlinien	Konfigurieren Sie die IPsec-Einstellungen.
		IPsec-Adressvorlage	Vorlagenliste	
		IPsec-Vorlage	Vorlagenliste	

B

Stichwortverzeichnis

A

Ad-hoc-Modus 10, 22

B

BRAdmin Light 1, 3

BRAdmin Professional 3 1, 6

F

FTP 49, 50

H

HTTP 38

I

Infrastruktur-Modus 9

L

LDAP 44

M

MAC-Adresse 4, 5, 6, 99

P

PIN-Methode 19

R

Remote Setup 1

Reparaturprogramm für Netzwerkverbindung 93

S

SMTP-AUTH 64

Status Monitor 1

U

Unterstützte Protokolle und
Sicherheitsfunktionen 102

V

Vertical Pairing 1, 98

W

Web-based Management (Webbrowser) 1, 6

Webdienste 98

Wireless-Netzwerk 8

WPS (Wi-Fi Protected Setup™) 19