

Netzwerkhandbuch

Multi-Protokoll On-Board Ethernet- Multifunktions-PrintServer und Wireless- Multifunktions-PrintServer



Dieses Netzwerkhandbuch enthält nützliche Informationen zu den LAN- und WLAN-Einstellungen, Sicherheitseinstellungen sowie zu Einstellungen für die Internet-Faxfunktion, die von Ihrem Brother-Gerät verwendet werden. Sie finden hier auch Informationen zu den unterstützten Protokollen und ausführliche Hinweise zur Problemlösung.

Das neueste Handbuch können Sie vom Brother Solutions Center unter <http://solutions.brother.com/> herunterladen. Sie können im Brother Solutions Center auch die neuesten Treiber und Dienstprogramme für Ihr Gerät herunterladen, Antworten auf häufig gestellte Fragen (FAQs) und Tipps zur Problemlösung finden oder sich über besondere Lösungen rund um das Drucken informieren.

Anwendbar für diese Modelle

Dieses Handbuch gilt für die folgenden Modelle.

HL-3180CDW/DCP-9015CDW/9017CDW/9020CDN/9020CDW/9022CDW/
MFC-9130CW/9140CDN/9142CDN/9330CDW/9332CDW/9340CDW/9342CDW

Hinweisdefinitionen

In diesem Handbuch werden die folgenden Symbole verwendet.

WICHTIG	<u>WICHTIG</u> weist auf eine potentiell gefährliche Situation hin, die zu Sachschäden oder zu Funktionsausfall des Gerätes führen kann.
HINWEIS	Hinweise informieren Sie, wie auf eine bestimmte Situation reagiert werden sollte, oder geben Ihnen hilfreiche Tipps zur beschriebenen Funktion.

WICHTIGER HINWEIS

- Verwenden Sie dieses Produkt daher nur in dem Land, in dem Sie es gekauft haben, da es in anderen Ländern eventuell gegen die Telekommunikationsbestimmungen und Anschlussvorschriften verstößt.
- Windows® XP steht in diesem Dokument für Windows® XP Professional, Windows® XP Professional x64 Edition und Windows® XP Home Edition.
- Windows Server® 2003 steht in diesem Dokument für Windows Server® 2003 und Windows Server® 2003 x64 Edition.
- Windows Server® 2008 steht in diesem Dokument für Windows Server® 2008 und Windows Server® 2008 R2.
- Windows Server® 2012 steht in diesem Handbuch für alle Ausgaben von Windows Server® 2012.
- Windows Vista® steht in diesem Handbuch für alle Ausgaben von Windows Vista®.
- Windows® 7 steht in diesem Handbuch für alle Ausgaben von Windows® 7.
- Windows® 8 steht in diesem Handbuch für alle Ausgaben von Windows® 8.
- Bitte besuchen Sie das Brother Solutions Center unter <http://solutions.brother.com/> und klicken Sie auf der Seite für Ihr Modell auf Handbücher, um die anderen Handbücher herunterzuladen.
- Nicht alle Modelle sind in allen Ländern verfügbar.

Inhaltsverzeichnis

Teil I Netzwerkbetrieb

1	Einleitung	2
	Netzwerkfunktionen	2
	Andere Netzwerkfunktionen	4
2	Netzwerkeinstellungen Ihres Gerätes ändern	5
	So ändern Sie die Netzwerkeinstellungen Ihres Gerätes (IP-Adresse, Subnetzmaske und Gateway)	5
	Mit Hilfe des Funktionstastenfelds	5
	Mit Hilfe des Dienstprogramms BRAdmin Light	5
	Andere Verwaltungsprogramme	8
	Web Based Management (Webbrowser)	8
	Dienstprogramm BRAdmin Professional 3 (Windows®)	8
	BRPrint Auditor (Windows®)	9
3	Konfigurieren Ihres Gerätes für ein Wireless-Netzwerk (Für HL-3180CDW, DCP-9015CDW, DCP-9017CDW, DCP-9020CDW, DCP-9022CDW, MFC-9130CW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW)	10
	Übersicht	10
	Überprüfen der Netzwerkumgebung	11
	Verbunden mit einem Computer mit WLAN-Zugriffspunkt/Router im Netzwerk (Infrastruktur-Modus)	11
	Verbunden mit einem wireless-fähigen Computer ohne WLAN-Access Point/Router im Netzwerk (Ad-hoc-Modus)	12
	Vorübergehende Wireless-Konfiguration über ein USB-Kabel (empfohlen)	13
	Konfiguration mit dem Setup-Assistenten über das Funktionstastenfeld des Gerätes	18
	Manuelle Konfiguration über das Funktionstastenfeld	19
	Konfigurieren Ihres Geräts, wenn keine SSID gesendet wird	21
	Konfigurieren Ihres Geräts für ein Wireless-Unternehmensnetzwerk	23
	Konfiguration mit WPS (Wi-Fi Protected Setup) oder AOSS™ per Tastendruck	27
	Konfiguration mit der PIN-Methode des WPS (Wi-Fi Protected Setup)	29
	Konfiguration im Ad-hoc-Modus	32
	Verwenden der konfigurierten SSID	32
	Verwenden einer neuen SSID	34
4	Aufbau des Funktionstastenfelds	36
	Netzwerk-Menü	36
	TCP/IP	36
	Ethernet (nur verkabeltes Netzwerk)	39
	LAN-Status (Für HL-3180CDW, DCP-9015CDW, DCP-9020CDN, DCP-9020CDW, DCP-9022CDW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW)	39
	Setup-Assistent (nur Wireless-Netzwerk)	39
	WPS (Wi-Fi Protected Setup)/AOSS™ (nur Wireless-Netzwerk)	39

WPS (Wi-Fi Protected Setup) mit PIN-Code (nur Wireless-Netzwerk).....	39
WLAN-Status (Für HL-3180CDW, DCP-9015CDW, DCP-9017CDW, DCP-9020CDW, DCP-9022CDW, MFC-9130CW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW).....	39
MAC-Adresse	40
Standardwert einstellen	40
LAN aktivieren (Für DCP-9020CDW, DCP-9022CDW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW).....	40
WLAN aktivieren	40
E-Mail/IFAX (MFC-9130CW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW: als Download verfügbar)	41
Fax-to-Server (MFC-9130CW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW: als Download verfügbar).....	45
So richten Sie eine neue Standardeinstellung für die Scan-to-FTP-Funktion ein	47
So richten Sie eine neue Standardeinstellung für die Scan-to-Netzwerk-Funktion (Windows®) ein.....	47
Zurücksetzen der Netzwerkeinstellungen auf die werkseitigen Standardeinstellungen	48
Drucken des Netzwerk-Konfigurationsberichts.....	49
Drucken des WLAN-Bericht (Für HL-3180CDW, DCP-9015CDW, DCP-9017CDW, DCP-9020CDW, DCP-9022CDW, MFC-9130CW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW)	49
Funktionstabelle und werkseitige Standardeinstellungen.....	50

5 Web Based Management 57

Übersicht.....	57
So konfigurieren Sie die Geräteeinstellungen über Web Based Management (Webbrowser)	58
Kennwort festlegen	59
Secure Function Lock 2.0	60
So konfigurieren Sie die Einstellungen von Secure Function Lock 2.0 mit Web Based Management (Webbrowser).....	61
Synchronisieren mit SNTP-Server.....	64
Druckprotokoll im Netzwerk speichern	66
So konfigurieren Sie die Einstellungen der Funktion „Druckprotokoll im Netzwerk speichern“ mit Web Based Management (Webbrowser)	67
Einstellung Fehlererkennung.....	69
Fehlermeldungen verstehen.....	70
Verwenden der Funktion „Druckprotokoll im Netzwerk speichern“ mit Secure Function Lock 2.0	71
Ändern der Konfiguration für Scan-to-FTP mit einem Webbrowser	71
Ändern der Konfiguration für Scan-to-Netzwerk mit einem Webbrowser (Windows®)	73

6 Internet-Faxfunktion (MFC-9130CW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW: als Download verfügbar) 75

Übersicht über die Internet-Faxfunktion.....	75
Wichtige Informationen zur Internet-Faxfunktion.....	76
So verwenden Sie die Internet-Faxfunktion.....	77
Versenden eines Internet-Faxdokuments.....	77
Empfangen einer E-Mail oder eines Internet-Faxdokuments	78

Zusätzliche Optionen für die Internetfax-Funktion	80
Empfangene E-Mail- und Faxnachrichten weiterleiten	80
Kettenrundsenden	80
Sendebestätigungs-E-Mail	84
Fehler-Mail	85

7 Sicherheitsfunktionen 86

Übersicht	86
Verwenden von Zertifikaten zur Gerätesicherheit	87
Konfigurieren eines Zertifikats mit Web Based Management	89
Erstellen und Installieren eines Zertifikats	90
Auswählen des Zertifikats	93
So installieren Sie das selbstsignierte Zertifikat auf Ihrem Computer	93
Importieren und Exportieren des Zertifikats und des privaten Schlüssels (Private Key)	98
Importieren und Exportieren eines CA-Zertifikats	99
Mehrere Zertifikate verwalten	99
Netzwerkgerät mit SSL/TLS sicher verwalten	100
Sichere Verwaltung mit Web Based Management (Webbrowser)	100
Sichere Verwaltung mit BRAdmin Professional 3 (Windows®)	103
Um das Dienstprogramm BRAdmin Professional 3 sicher nutzen zu können, müssen Sie die folgenden Punkte beachten	103
Sicherer Druck von Dokumenten mit SSL/TLS	104
Sicheres Versenden oder Empfangen einer E-Mail	105
Konfiguration mit Web Based Management (Webbrowser)	105
Versenden einer E-Mail mit Benutzerauthentifizierung	106
Sicheres Versenden oder Empfangen einer E-Mail mit SSL/TLS	107
Verwenden der IEEE 802.1x-Authentifizierung	108
Konfigurieren der IEEE 802.1x-Authentifizierung mit Web Based Management (Webbrowser)	108

8 Problemlösung 111

Übersicht	111
Problemerkennung	111

Teil II Netzwerkbegriffe

9 Netzwerkverbindungsarten und Protokolle 120

Netzwerkverbindungsarten	120
Beispiel für eine verkabelte Netzwerkverbindung	120
Protokolle	122
TCP/IP-Protokolle und -Funktionen	122

10 Konfigurieren Ihres Geräts für ein Netzwerk 126

IP-Adressen, Subnetzmasken und Gateways	126
IP-Adresse	126
Subnetzmaske	127
Gateway (und Router)	127
IEEE 802.1x-Authentifizierung	128

11	Bedingungen und Konzepte für WLAN-Netzwerke (Für HL-3180CDW, DCP-9015CDW, DCP-9017CDW, DCP-9020CDW, DCP-9022CDW, MFC-9130CW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW)	130
	Festlegen Ihres Netzwerks	130
	SSID (Service Set Identifier) und Kanäle	130
	Sicherheitsbegriffe	130
	Authentifizierung und Verschlüsselung	130
	Authentifizierungs- und Verschlüsselungsmethoden für ein privates kabelloses Netzwerk	131
	Authentifizierungs- und Verschlüsselungsmethoden für Wireless-Unternehmensnetzwerke	132
12	Zusätzliche Netzwerkeinstellungen von Windows®	134
	Arten von zusätzlichen Netzwerkeinstellungen	134
	Installieren von Treibern zum Drucken und Scannen über Web Services (Windows Vista®, Windows® 7 und Windows® 8)	134
	Deinstallieren von Treibern zum Drucken und Scannen über Web Services (Windows Vista®, Windows® 7 und Windows® 8)	136
	Netzwerkdruck- und -Scan-Installation für den Infrastruktur-Modus bei der Nutzung von Vertical Pairing (Windows® 7 und Windows® 8)	137
13	Sicherheitsbegriffe und -konzepte	139
	Sicherheitsfunktionen	139
	Sicherheitsbegriffe	139
	Sicherheitsprotokolle	140
	Sicherheitsmethoden für das Senden und Empfangen von E-Mails	141

Teil III Anhänge

A	Anhang A	143
	Unterstützte Protokolle und Sicherheitsfunktionen	143
B	Anhang B	144
	Dienste verwenden	144
	Weitere Möglichkeiten, die IP-Adresse einzustellen (für fortgeschrittene Benutzer und Administratoren)	144
	Konfigurieren der IP-Adresse mit DHCP	144
	Konfigurieren der IP-Adresse mit RARP	145
	Konfigurieren der IP-Adresse mit BOOTP	146
	Konfigurieren der IP-Adresse mit APIPA	146
	Konfigurieren der IP-Adresse mit ARP	147
	Konfigurieren der IP-Adresse über die TELNET-Konsole	148
C	Stichwortverzeichnis	149



Netzwerkbetrieb

Einleitung	2
Netzwerkeinstellungen Ihres Gerätes ändern	5
Konfigurieren Ihres Gerätes für ein Wireless-Netzwerk (Für HL-3180CDW, DCP-9015CDW, DCP-9017CDW, DCP-9020CDW, DCP-9022CDW, MFC-9130CW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW)	10
Aufbau des Funktionstastenfelds	36
Web Based Management	57
Internet-Faxfunktion (MFC-9130CW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW: als Download verfügbar)	75
Sicherheitsfunktionen	86
Problemlösung	111

Netzwerkfunktionen

Ihr Brother-Gerät kann mit Hilfe des internen Netzwerkdruckservers über ein verkabeltes Ethernet-Netzwerk mit 10/100 MB¹ oder ein IEEE 802.11b/g/n Wireless-Ethernet-Netzwerk (für Wireless-Modelle) freigegeben werden. Der MFC/DCP-Server bietet vielfältige Funktionen und unterstützt verschiedene Verbindungsverfahren, je nachdem mit welchem Betriebssystem Sie in Ihrem TCP/IP-fähigen Netzwerk arbeiten. Die folgende Tabelle zeigt, welche Netzwerkfunktionen und -verbindungen von den einzelnen Betriebssystemen unterstützt werden.

HINWEIS

- Obwohl das Brother-Gerät sowohl in einem Wireless-Netzwerk als auch in einem verkabelten Netzwerk¹ verwendet werden kann, können nicht beide Verbindungsmethoden gleichzeitig genutzt werden. Allerdings können eine Wireless-Netzwerkverbindung und eine Wi-Fi Direct™-Verbindung oder eine verkabelte Netzwerkverbindung und eine Wi-Fi Direct-Verbindung gleichzeitig verwendet werden.
- Einzelheiten dazu finden Sie im Wi-Fi Direct™ Anleitung auf der Handbücher-Downloadseite für Ihr Modell im Brother Solutions Center (<http://solutions.brother.com/>).

¹ Eine verkabelte Netzwerkschnittstelle steht bei den Modellen DCP-9020CDW, DCP-9022CDW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW zur Verfügung.

Betriebssysteme	Windows® XP	Windows Server® 2003/2008/2012	Mac OS X v10.6.8, 10.7.x, 10.8.x
	Windows Vista®		
	Windows® 7		
	Windows® 8		
Drucken	✓	✓	✓
Scannen ➤➤ Software-Handbuch	✓		✓
PC-Fax senden ¹ ➤➤ Software-Handbuch	✓		✓
PC-Fax empfangen ¹ ➤➤ Software-Handbuch	✓		
BRAdmin Light ² Siehe Seite 5.	✓	✓	✓
BRAdmin Professional 3 ³ Siehe Seite 8.	✓	✓	
Web Based Management (Webbrowser) Siehe Seite 57.	✓	✓	✓
Remote Setup ¹ ➤➤ Software-Handbuch	✓		✓
Status Monitor ➤➤ Software-Handbuch	✓		✓
Treiberinstallations-Assistent	✓	✓	
Vertical Pairing Siehe Seite 137.	✓ ⁴		

¹ Nicht verfügbar für DCP-Modelle.

² BRAdmin Light für Macintosh ist als Download verfügbar unter <http://solutions.brother.com/>.

³ BRAdmin Professional 3 ist als Download verfügbar unter <http://solutions.brother.com/>.

⁴ Nur Windows® 7 und Windows® 8.

Andere Netzwerkfunktionen

Internet-Fax (MFC-9130CW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW: als Download verfügbar)

Mit der Internet-Faxfunktion (IFax) können Sie Faxe über das Internet versenden und empfangen. (Siehe *Internet-Faxfunktion (MFC-9130CW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW: als Download verfügbar)* >> Seite 75.)

Zur Verwendung dieser Funktion laden Sie bitte die erforderliche Firmware von der Seite „Downloads“ für Ihr Modell vom Brother Solutions Center herunter unter <http://solutions.brother.com/>. Bevor Sie diese Funktion verwenden können, müssen Sie zunächst die erforderlichen Geräteeinstellungen über das Funktionstastenfeld des Geräts, BRAdmin Professional 3 oder Web Based Management konfigurieren. Weitere Informationen finden Sie im Benutzerhandbuch für Internet-Faxfunktionen auf der oben angegebenen Website.

Sicherheit

Ihr Brother-Gerät verwendet moderne Protokolle zur Netzwerksicherheit und Datenverschlüsselung. (Siehe *Sicherheitsfunktionen* >> Seite 86.)

Fax-to-Server (MFC-9130CW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW: als Download verfügbar)

Mit der Fax-to-Server-Funktion kann ein Dokument eingescannt und über das Netzwerk an einen separaten Faxserver gesendet werden. (Siehe *Fax-to-Server (MFC-9130CW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW: als Download verfügbar)* >> Seite 45.)

Zur Verwendung dieser Funktion laden Sie bitte die erforderliche Firmware von der Seite „Downloads“ für Ihr Modell vom Brother Solutions Center herunter unter <http://solutions.brother.com/>. Bevor Sie diese Funktion verwenden können, müssen Sie zunächst die erforderlichen Geräteeinstellungen über das Funktionstastenfeld des Geräts, BRAdmin Professional 3 oder Web Based Management konfigurieren. Weitere Informationen finden Sie im Benutzerhandbuch für Internet-Faxfunktionen auf der oben angegebenen Website.

Secure Function Lock 2.0

Secure Function Lock 2.0 erhöht die Sicherheit durch die Möglichkeit, die Verwendung von Funktionen zu sperren. (Siehe *Secure Function Lock 2.0* >> Seite 60.)

Druckprotokoll im Netzwerk speichern

Die Funktion Druckprotokoll im Netzwerk speichern ermöglicht das Speichern der Druckprotokoll-Datei Ihres Brother-Gerätes auf einem Netzwerkserver unter Verwendung von CIFS. (Siehe *Druckprotokoll im Netzwerk speichern* >> Seite 66.)

Brother Web Connect

Mit Brother Web Connect können Sie Bilder herunterladen und drucken sowie Dateien hochladen, indem Sie im Internet verfügbare Dienste direkt über Ihr Gerät nutzen. Einzelheiten dazu finden Sie im Web Connect Anleitung auf der Handbücher-Downloadseite für Ihr Modell im Brother Solutions Center (<http://solutions.brother.com/>).

So ändern Sie die Netzwerkeinstellungen Ihres Gerätes (IP-Adresse, Subnetzmaske und Gateway)

Die Netzwerkeinstellungen des Gerätes können über das Funktionstastenfeld, BRAdmin Light, Web Based Management und BRAdmin Professional 3 geändert werden. Einzelheiten dazu finden Sie in diesem Kapitel.

Mit Hilfe des Funktionstastenfelds

Sie können das Gerät zur Verwendung im Netzwerk über das Netzwerk-Menü des Funktionstastenfeldes konfigurieren. (Siehe *Aufbau des Funktionstastenfelds* ►► Seite 36.)

Mit Hilfe des Dienstprogramms BRAdmin Light

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, wie die IP-Adresse, vornehmen.

BRAdmin Light for Windows® installieren

- 1 Vergewissern Sie sich, dass das Gerät eingeschaltet ist.
- 2 Schalten Sie den Computer ein. Schließen Sie alle Anwendungen, bevor Sie mit der Konfiguration beginnen.
- 3 Legen Sie die Installations-CD-ROM in das CD-ROM-Laufwerk ein. Der Startbildschirm wird automatisch angezeigt. Wenn der Bildschirm zur Auswahl des Modells erscheint, wählen Sie Ihr Modell. Wenn der Bildschirm zur Auswahl der Sprache erscheint, wählen Sie Ihre Sprache.
- 4 Das Hauptmenü der CD-ROM wird angezeigt. Klicken Sie auf **Benutzerdefinierte Installation** und dann auf **Netzwerk-Utilities**.
- 5 Klicken Sie auf **BRAdmin Light** und folgen Sie den Anweisungen auf dem Bildschirm.

BRAdmin Light for Macintosh installieren

Sie können die neueste Version von Brother BRAdmin Light von <http://solutions.brother.com/> herunterladen.

Konfigurieren der IP-Adresse, Subnetzmaske und Gateway mit BRAdmin Light

HINWEIS

- Sie können die neueste Version von Brother BRAdmin Light von <http://solutions.brother.com/> herunterladen.
- Wenn Sie ein erweitertes Geräteverwaltungsprogramm benötigen, sollten Sie die neueste Version von BRAdmin Professional 3 verwenden, die von <http://solutions.brother.com/> heruntergeladen werden kann. Dieses Dienstprogramm ist nur für Windows® verfügbar.
- Wenn Sie die Firewall-Funktion einer Anti-Spyware oder Antiviren-Anwendung verwenden, deaktivieren Sie diese vorübergehend. Sobald Sie sicher sind, dass Sie drucken können, aktivieren Sie die Anwendung wieder.
- Knotenname: Der Knotenname erscheint im aktuellen BRAdmin Light-Fenster. Der Standardknotenname des PrintServers im Gerät ist „BRNxxxxxxxxxxxx“ für ein verkabeltes Netzwerk und „BRWxxxxxxxxxxxx“ für ein Wireless-Netzwerk. („xxxxxxxxxxxx“ steht für die MAC-Adresse / Ethernet-Adresse Ihres Gerätes.)
- Standardmäßig ist kein Kennwort erforderlich. Geben Sie ein Kennwort ein, wenn Sie eines eingerichtet haben, und drücken Sie **OK**.

1 Starten Sie BRAdmin Light.

■ Windows®

(Windows® XP/Windows® Vista/Windows® 7/Windows Server® 2003/Windows Server® 2008)

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

(Windows® 8/Windows Server® 2012)

Klicken Sie auf  (**BRAdmin Light**).

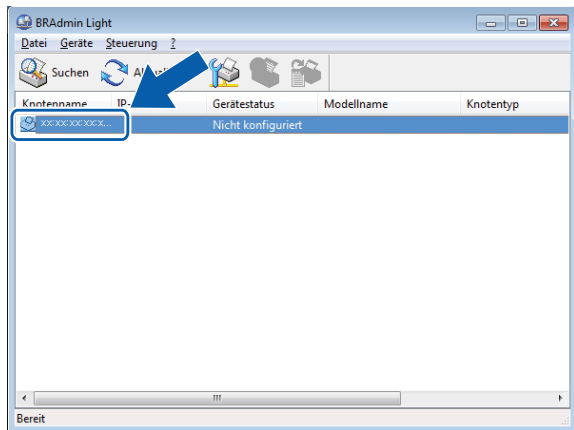
■ Macintosh

Doppelklicken Sie nach dem Herunterladen auf die Datei **BRAdmin Light.jar**, um das Dienstprogramm BRAdmin Light zu starten.

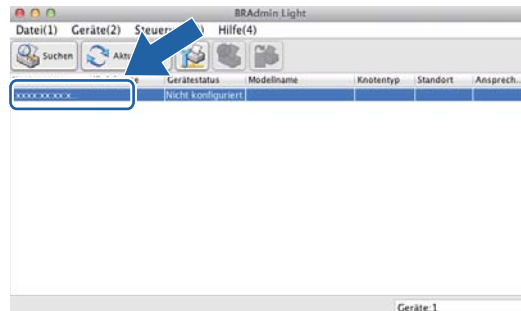
2 BRAdmin Light sucht nun automatisch nach neuen Geräten.

3 Doppelklicken Sie auf das nicht konfigurierte Gerät.

Windows®



Macintosh



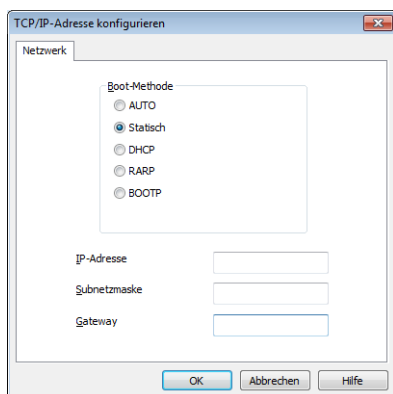
2

HINWEIS

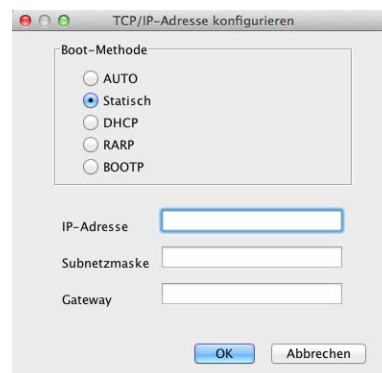
- Sind für den MFC/DCP-Server die werkseitigen Standardeinstellungen eingestellt (wenn Sie keinen DHCP/BOOTP/RARP-Server verwenden) wird das Gerät in BRAdmin Light als **Nicht konfiguriert** angezeigt.
- Sie finden den Knotennamen und die MAC-Adresse (Ethernet-Adresse), indem Sie den Netzwerk-Konfigurationsbericht ausdrucken (siehe *Drucken des Netzwerk-Konfigurationsberichts* ►► Seite 49). Den Knotennamen und die MAC-Adresse können Sie auch dem Funktionstastenfeld entnehmen. (Siehe *Kapitel 4: Aufbau des Funktionstastenfelds*.)

4 Wählen Sie **Statisch** für **Boot-Methode**. Geben Sie **IP-Adresse**, **Subnetzmaske** und **Gateway** (soweit erforderlich) für Ihr Gerät ein.

Windows®



Macintosh



5 Klicken Sie auf **OK**.

6 Wenn die IP-Adresse korrekt ist, wird das Brother-Gerät in der Geräteliste angezeigt.

Andere Verwaltungsprogramme

Für Ihr Brother-Gerät stehen neben dem Dienstprogramm BRAdmin Light noch die folgenden Verwaltungsprogramme zur Verfügung. Mit diesen Programmen können Sie Ihre Netzwerkeinstellungen ändern.

Web Based Management (Webbrowser)

Sie können die PrintServer-Einstellungen über einen normalen Webbrowser und das HTTP-Protokoll (Hyper Text Transfer Protocol) oder HTTPS-Protokoll (Hyper Text Transfer Protocol over Secure Socket Layer) ändern. (Siehe *So konfigurieren Sie die Geräteeinstellungen über Web Based Management (Webbrowser)* >> Seite 58.)

Dienstprogramm BRAdmin Professional 3 (Windows®)

BRAdmin Professional 3 ist ein Dienstprogramm für die erweiterte Verwaltung von netzwerkfähigen Brother-Geräten. Sie können mit diesem Dienstprogramm nach Brother-Geräten im Netzwerk suchen und den Gerätestatus in einem leicht lesbaren explorer-artigen Fenster ansehen, das die Farbe ändert, um den Status der einzelnen Geräte anzuzeigen. Daneben können Sie mit einem Windows®-Computer in Ihrem LAN 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.

Nutzer, die lokal angeschlossene Geräte überwachen möchten, sollten die Print Auditor Client-Software auf ihrem Client-PC installieren. Dieses Dienstprogramm ermöglicht es, auch solche Geräte mit BRAdmin Professional 3 zu überwachen, die über die USB- oder die parallele Schnittstelle an den Client-PC angeschlossen sind.

Besuchen Sie uns unter <http://solutions.brother.com/>, um weitere Informationen zu erhalten und die Software herunterzuladen.

HINWEIS

- Sie sollten die neueste Version von BRAdmin Professional 3 verwenden, die Sie von <http://solutions.brother.com/> herunterladen können. Dieses Dienstprogramm ist nur für Windows® verfügbar.
 - Wenn Sie die Firewall-Funktion einer Anti-Spyware oder Antiviren-Anwendung verwenden, deaktivieren Sie diese vorübergehend. Sobald Sie sicher sind, dass Sie drucken können, konfigurieren Sie die Software-Einstellungen entsprechend den Anweisungen erneut.
 - Knotenname: Der Knotenname der einzelnen Brother-Geräte im Netzwerk wird in BRAdmin Professional 3 angezeigt. Der Standardknotenname ist „BRNxxxxxxxxxxxx“ für ein verkabeltes Netzwerk und „BRWxxxxxxxxxxxx“ für ein Wireless-Netzwerk. („xxxxxxxxxxxx“ steht für die MAC-Adresse / Ethernet-Adresse Ihres Gerätes.)
-

BRPrint Auditor (Windows®)

Die BRPrint Auditor-Software ermöglicht es, die Überwachungsfunktionen der Brother Netzwerkverwaltungsprogramme auch für lokal angeschlossene Geräte zu verwenden. Mit Hilfe dieses Dienstprogramms kann ein Client-Computer Nutzungs- und Statusinformationen von einem Brother-Gerät abrufen, das über eine Parallel- oder USB-Schnittstelle angeschlossen ist. Der BRPrint Auditor kann diese Informationen dann zu einem anderen Computer im Netzwerk weiterleiten, auf dem BRAdmin Professional 3 ausgeführt wird. Dadurch kann der Administrator verschiedene Informationen wie den Seitenzähler, den Toner- und Trommelstatus und die Firmware-Version abrufen und prüfen. Dieses Dienstprogramm kann die Nutzungs- und Statusinformationen aber nicht nur an die Brother-Netzwerkverwaltungsanwendungen weiterleiten, sondern auch per E-Mail im CSV- oder XML-Dateiformat direkt an eine voreingestellte E-Mail-Adresse senden (SMTP-Mailunterstützung ist erforderlich). Das BRPrint Auditor-Dienstprogramm unterstützt darüber hinaus auch die E-Mail-Benachrichtigungsfunktion zum Anzeigen von Warnmeldungen und Fehlerbedingungen.

Konfigurieren Ihres Gerätes für ein Wireless-Netzwerk (Für HL-3180CDW, DCP-9015CDW, DCP-9017CDW, DCP-9020CDW, DCP-9022CDW, MFC-9130CW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW)

Übersicht

Zur Verbindung Ihres Gerätes mit Ihrem Wireless-Netzwerk wird eine der folgenden Einrichtungsmethoden empfohlen, die in der Installationsanleitung erläutert sind.

Die einfachste Einrichtungsmethode für die Wireless-Einrichtung erfolgt über die Installations-CD-ROM und ein USB-Kabel.

Weitere Konfigurationsmethoden für Wireless-Netzwerke finden Sie in diesem Kapitel, in dem weitere Verfahren zur Konfiguration der Wireless-Netzwerkeinstellungen beschrieben werden. Informationen zu TCP/IP-Einstellungen finden Sie unter *So ändern Sie die Netzwerkeinstellungen Ihres Gerätes (IP-Adresse, Subnetzmaske und Gateway)* >> Seite 5.

HINWEIS

- Zur Erzielung optimaler Ergebnisse beim alltäglichen Drucken 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.

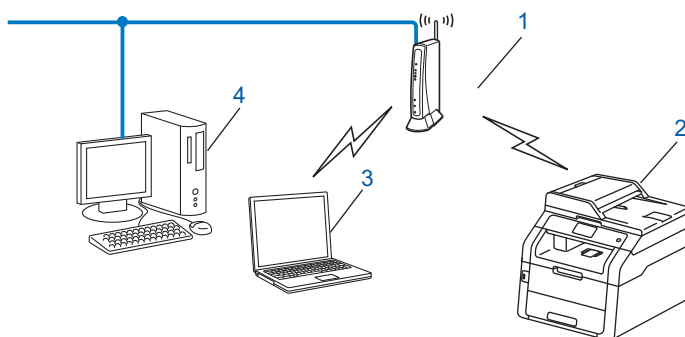
Daher ist eine drahtlose Verbindung möglicherweise nicht die beste Verbindungsmethode zur Übertragung aller Dokumentenarten und Anwendungen. Wenn Sie große Dateien wie mehrseitige Dokumente mit Text und großen Grafiken drucken, sollten Sie ein verkabeltes Ethernet-Netzwerk für einen schnelleren Datentransfer ¹ oder eine USB-Verbindung zum Erreichen der höchsten Übertragungsgeschwindigkeit wählen.

- Obwohl das Brother-Gerät sowohl in einem Wireless-Netzwerk als auch in einem verkabelten Netzwerk ¹ verwendet werden kann, können nicht beide Verbindungsmethoden gleichzeitig genutzt werden. Allerdings können eine Wireless-Netzwerkverbindung und eine Wi-Fi Direct-Verbindung oder eine verkabelte Netzwerkverbindung und eine Wi-Fi Direct-Verbindung gleichzeitig verwendet werden.
- Einzelheiten dazu finden Sie im Wi-Fi Direct™ Anleitung auf der Handbücher-Downloadseite für Ihr Modell im Brother Solutions Center (<http://solutions.brother.com/>).
- Bevor Sie die Wireless-Einstellungen konfigurieren, müssen Sie Ihren Netzwerknamen (SSID) und Ihren Netzwerkschlüssel kennen. Wenn Sie ein Wireless-Firmennetzwerk verwenden, müssen Sie auch die Benutzer-ID und das Kennwort wissen.

¹ Eine verkabelte Netzwerkschnittstelle steht bei den Modellen DCP-9020CDW, DCP-9022CDW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW zur Verfügung.

Überprüfen der Netzwerkkumgebung

Verbunden mit einem Computer mit WLAN-Zugriffspunkt/Router im Netzwerk (Infrastruktur-Modus)



1 WLAN Access Point/Router ¹

¹ Wenn Ihr Computer Intel® MWT (My WiFi Technology) unterstützt, können Sie Ihren Computer wie einen WPS (Wi-Fi Protected Setup) unterstützenden Access Point 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 Ethernetkabel mit dem WLAN Access Point verbunden

Konfigurationsmethode

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

■ Vorübergehende Wireless-Konfiguration über ein USB-Kabel (empfohlen)

Siehe *Vorübergehende Wireless-Konfiguration über ein USB-Kabel (empfohlen)* >> Seite 13.

■ Wireless-Konfiguration mit dem Setup-Assistenten über das Funktionstastenfeld

Siehe *Konfiguration mit dem Setup-Assistenten über das Funktionstastenfeld des Gerätes* >> Seite 18.

■ Wireless-Konfiguration mit WPS (Wi-Fi Protected Setup™) oder AOSS™ per Tastendruck

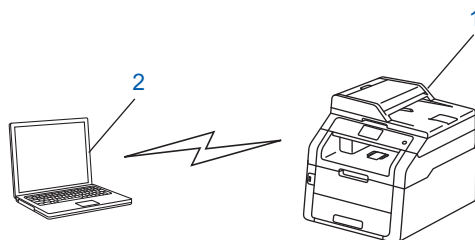
Siehe *Konfiguration mit WPS (Wi-Fi Protected Setup) oder AOSS™ per Tastendruck* >> Seite 27.

■ Wireless-Konfiguration mit PIN-Verfahren über WPS

Siehe *Konfiguration mit der PIN-Methode des WPS (Wi-Fi Protected Setup)* >> Seite 29.

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

Bei diesem Netzwerktyp gibt es keinen zentralen Zugriffspunkt (WLAN Access Point). Alle Wireless-Geräte kommunizieren direkt miteinander. Wenn das Brother Wireless-Gerät (Ihr Gerät) Teil dieses Netzwerkes ist, erhält es alle Druckaufträge direkt von dem Computer, der die Druckdaten sendet.



1 Wireless-Netzwerkgerät (Ihr Gerät)

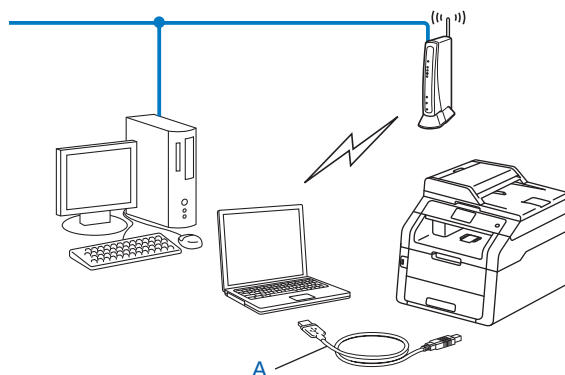
2 Wireless-fähiger Computer

Wir garantieren nicht für eine Wireless-Netzwerkverbindung mit Windows Server®-Produkten im Ad-hoc-Modus. Informationen zur Einrichtung Ihres Gerätes im Ad-hoc-Modus finden Sie unter *Konfiguration im Ad-hoc-Modus* ►► Seite 32.

Vorübergehende Wireless-Konfiguration über ein USB-Kabel (empfohlen)

Für diese Methode wird die Verwendung eines Computers mit Wireless-Verbindung zu Ihrem Netzwerk empfohlen.

Sie können das Gerät remote vom Computer im Netzwerk aus über ein USB-Kabel konfigurieren (A) ¹.



¹ Sie können die Wireless-Einstellungen des Gerätes konfigurieren, indem Sie das Gerät vorübergehend mit einem USB-Kabel an einen verkabelten oder Wireless-Computer anschließen.

WICHTIG

- Mit der folgenden Anleitung können Sie Ihr Brother-Gerät mit dem Brother-Installationsprogramm in einer Netzwerkumgebung installieren. Dieses Programm finden Sie auf der CD-ROM, die mit Ihrem Gerät geliefert wurde.
- Falls Sie die Wireless-Einstellungen des Gerätes zuvor schon einmal konfiguriert haben, müssen Sie erst die LAN-Einstellungen zurücksetzen, bevor Sie die Wireless-Einstellungen erneut konfigurieren können. Informationen zum Zurücksetzen der LAN-Einstellungen finden Sie unter *Zurücksetzen der Netzwerkeinstellungen auf die werkseitigen Standardeinstellungen* ►► Seite 48.
- Wenn Sie die Windows®-Firewall oder die Firewall-Funktion einer Anti-Spyware oder Antivirus-Anwendung verwenden, deaktivieren Sie diese vorübergehend. Sobald Sie sicher sind, dass Sie drucken können, aktivieren Sie die Firewall bitte wieder.
- Sie benötigen zum Konfigurieren vorübergehend ein USB-Kabel.
- **Sie müssen Ihre Wireless-Netzwerkeinstellungen kennen, bevor Sie mit der Installation fortfahren.** Wenn Sie Ihr Brother-Gerät in Ihrem Netzwerk anschließen möchten, sollten Sie sich vor der Installation an Ihren Systemadministrator wenden.
- Wenn Ihr Router die WEP-Verschlüsselung verwendet, geben Sie den als ersten WEP-Schlüssel benutzten Schlüssel ein. Ihr Brother-Gerät unterstützt nur die Verwendung des ersten WEP-Schlüssels.

Konfigurieren Ihres Gerätes für ein Wireless-Netzwerk (Für HL-3180CDW, DCP-9015CDW, DCP-9017CDW, DCP-9020CDW, DCP-9022CDW, MFC-9130CW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW)

- 1 Bevor Sie Ihr Gerät konfigurieren, sollten Sie sich die Einstellungen Ihres Wireless-Netzwerkes notieren. Sie benötigen diese Informationen, um mit der Konfiguration fortzufahren.

Für die Konfiguration eines privaten Wireless-Netzwerks

Wenn Sie Ihr Gerät für ein kleineres Wireless-Netzwerk konfigurieren, wie zum Beispiel in Ihrem Heimbereich, notieren Sie Ihre SSID und den Netzwerkschlüssel.

Bei Verwendung von Windows® XP oder einem Netzwerkkabel zum Anschluss Ihres Computers an Ihren WLAN-Access Point/Router müssen Sie die SSID und den Netzwerkschlüssel Ihres WLAN-Access Point/Routers kennen, bevor Sie fortfahren.

Netzwerkname: (SSID)	Netzwerkschlüssel

Zum Beispiel:

Netzwerkname: (SSID)	Netzwerkschlüssel
HELLO	12345678

Für die Konfiguration eines Wireless-Unternehmensnetzwerks

Wenn Sie Ihr Gerät für ein Wireless-Netzwerk konfigurieren, das IEEE 802.1x unterstützt, notieren Sie Ihre Authentifizierungsmethode, Verschlüsselungsmethode, Benutzer-ID und das Kennwort.

Netzwerkname: (SSID)

3

Kommunikationsmodus	Authentifizierungsmethode	Verschlüsselungsmodus	Benutzer-ID	Kennwort
Infrastruktur	LEAP	CKIP		
	EAP-FAST/NONE	AES		
		TKIP		
	EAP-FAST/MS-CHAPv2	AES		
		TKIP		
	EAP-FAST/GTC	AES		
		TKIP		
	PEAP/MS-CHAPv2	AES		
		TKIP		
	PEAP/GTC	AES		
		TKIP		
	EAP-TTLS/CHAP	AES		
		TKIP		
	EAP-TTLS/MS-CHAP	AES		
		TKIP		
	EAP-TTLS/MS-CHAPv2	AES		
		TKIP		
	EAP-TTLS/PAP	AES		
		TKIP		
	EAP-TLS	AES		—
		TKIP		—

Zum Beispiel:

Netzwerkname: (SSID)
HELLO

Kommunikationsmodus	Authentifizierungsmethode	Verschlüsselungsmodus	Benutzer-ID	Kennwort
Infrastruktur	EAP-FAST/MS-CHAPv2	AES	Brother	12345678

HINWEIS

- Wenn Sie Ihr Gerät mit EAP-TLS-Authentifizierung konfigurieren, müssen Sie das von einer Zertifizierungsstelle (Certificate Authority) ausgegebene Client-Zertifikat installieren, bevor Sie mit der Konfiguration beginnen. Wenden Sie sich bezüglich des Client-Zertifikats an Ihren Netzwerkadministrator. Wenn Sie mehrere Zertifikate installiert haben, empfehlen wir, den Namen des Zertifikats zu notieren, das Sie verwenden möchten. Weitere Einzelheiten zur Installation des Zertifikats siehe *Verwenden von Zertifikaten zur Gerätesicherheit* ►► Seite 87.
- Wenn Sie Ihr Gerät mit dem allgemeinen Namen des Server-Zertifikats verifizieren, empfehlen wir, den allgemeinen Namen zu notieren, bevor Sie mit der Konfiguration beginnen. Wenden Sie sich bei Fragen zum allgemeinen Namen des Server-Zertifikats an Ihren Netzwerkadministrator.

- 2 Schalten Sie Ihren Computer ein und legen Sie die Installations-CD-ROM in Ihr CD-ROM-Laufwerk ein.

(Windows®)

- 1 Der Startbildschirm wird automatisch angezeigt.

Wenn der Bildschirm zur Auswahl des Modells erscheint, wählen Sie Ihr Modell. Wenn der Bildschirm zur Auswahl der Sprache erscheint, wählen Sie Ihre Sprache.

- 2 Das Hauptmenü der CD-ROM wird angezeigt. Klicken Sie auf **MFL-Pro Suite installieren**, und klicken Sie auf **Ja**, wenn Sie die Lizenzvereinbarungen akzeptieren. Folgen Sie den Anweisungen auf dem Bildschirm.

HINWEIS

- Wenn der Brother-Bildschirm nicht automatisch angezeigt wird, wechseln Sie zu **Computer (Arbeitsplatz)**. (Für Windows® 8: Klicken Sie in der Symbolleiste auf das Symbol  (**Explorer**) und wechseln Sie dann zu **Computer**.) Doppelklicken Sie auf das CD-ROM-Symbol und doppelklicken Sie dann auf **start.exe**.
- Wenn das Fenster **Benutzerkontensteuerung** angezeigt wird, (Windows Vista®) klicken Sie auf **Zulassen**. (Windows® 7/Windows® 8) klicken Sie auf **Ja**.

- 3 Wählen Sie **Drahtlose Netzwerkverbindung (Wireless LAN)**, und klicken Sie dann auf **Weiter**.
- 4 Wählen Sie die Option für die Firewall-Einstellung auf dem Bildschirm **Firewall/Antiviren-Programm gefunden** und klicken Sie dann auf **Weiter**.

(Macintosh)

- 1 Der Startbildschirm wird automatisch angezeigt. Klicken Sie auf **Start Here OSX**. Wählen Sie Ihr Gerät und klicken Sie auf **Weiter**.
- 2 Wählen Sie **Drahtlose Netzwerkverbindung (Wireless LAN)** und klicken Sie dann auf **Weiter**.

3 Wählen Sie **Ja, ich habe ein USB-Kabel für die Installation**. und klicken Sie dann auf **Weiter**.

4 Folgen Sie den Anweisungen auf dem Bildschirm, um die Wireless-Einstellungen zu konfigurieren.

HINWEIS

- Wenn der Bildschirm **Verfügbare Wireless-Netzwerke** angezeigt wird und Ihr Access Point nicht für das Senden der SSID eingerichtet ist, können Sie diese manuell hinzufügen, indem Sie auf die Schaltfläche **Erweitert** klicken. Folgen Sie den Anweisungen auf dem Bildschirm zur Eingabe der Informationen für **Name (SSID)**.
- Wenn der Fehlerbildschirm für die Wireless-Einrichtung angezeigt wird, klicken Sie auf **Wiederholen** und versuchen Sie es erneut.



Nachdem Sie die Wireless-Einstellungen abgeschlossen haben, können Sie mit den Treibern und der Software fortfahren, die für den Betrieb des Gerätes erforderlich sind. Klicken Sie im Installationsdialogfeld auf **Weiter** und folgen Sie den Anweisungen auf dem Bildschirm.

Konfiguration mit dem Setup-Assistenten über das Funktionstastenfeld des Gerätes

Sie können zur Konfiguration der Wireless-Netzwerkeinstellungen das Funktionstastenfeld des Gerätes verwenden. Mit Hilfe der Funktion *Setup-Assist.* im Menü des Gerätes können Sie Ihr Brother-Gerät einfach mit Ihrem Wireless-Netzwerk verbinden. **Sie müssen Ihre Wireless-Netzwerkeinstellungen kennen, bevor Sie mit der Installation fortfahren.**

3

WICHTIG

- Falls Sie die Wireless-Einstellungen des Gerätes zuvor schon einmal konfiguriert haben, müssen Sie erst die LAN-Einstellungen zurücksetzen, bevor Sie die Wireless-Einstellungen erneut konfigurieren können. Informationen zum Zurücksetzen der LAN-Einstellungen finden Sie unter *Zurücksetzen der Netzwerkeinstellungen auf die werkseitigen Standardeinstellungen* >> Seite 48.
- Wenn Ihr Router die WEP-Verschlüsselung verwendet, geben Sie den als ersten WEP-Schlüssel benutzten Schlüssel ein. Ihr Brother-Gerät unterstützt nur die Verwendung des ersten WEP-Schlüssels.

- Wenn Sie Ihr Gerät für ein kleineres Wireless-Netzwerk konfigurieren, wie zum Beispiel in Ihrem Heimbereich.
 - Informationen zum Konfigurieren Ihres Gerätes für ein vorhandenes Wireless-Netzwerk mit SSID und Netzwerkschlüssel (falls notwendig) finden Sie unter *Manuelle Konfiguration über das Funktionstastenfeld* >> Seite 19.
 - Wenn Ihr WLAN Access Point/Router so eingestellt ist, dass er den SSID-Name nicht rundsendet, lesen Sie *Konfigurieren Ihres Geräts, wenn keine SSID gesendet wird* >> Seite 21.
 - Informationen zum Konfigurieren Ihres Gerätes für den Ad-hoc-Modus finden Sie unter *Konfiguration im Ad-hoc-Modus* >> Seite 32.
- Informationen zum Konfigurieren Ihres Gerätes für ein Wireless-Netzwerk, das IEEE 802.1x unterstützt, finden Sie unter *Konfigurieren Ihres Geräts für ein Wireless-Unternehmensnetzwerk* >> Seite 23.
- Informationen zum WLAN Access Point/Router mit Unterstützung von WPS oder AOSS™ finden Sie unter *Konfiguration mit WPS (Wi-Fi Protected Setup) oder AOSS™ per Tastendruck* >> Seite 27.
- Informationen zur Konfiguration Ihres Geräts mit WPS (PIN-Verfahren) finden Sie unter *Konfiguration mit der PIN-Methode des WPS (Wi-Fi Protected Setup)* >> Seite 29.

Manuelle Konfiguration über das Funktionstastenfeld

- 1 Bevor Sie Ihr Gerät konfigurieren, sollten Sie sich die Einstellungen Ihres Wireless-Netzwerkes notieren. Sie benötigen diese Informationen, um mit der Konfiguration fortzufahren. Überprüfen und notieren Sie die aktuellen Wireless-Netzwerkeinstellungen.

Netzwerkname: (SSID)	Netzwerkschlüssel

Zum Beispiel:

Netzwerkname: (SSID)	Netzwerkschlüssel
HELLO	12345678

HINWEIS

- Wenn Ihr Router die WEP-Verschlüsselung verwendet, geben Sie den als ersten WEP-Schlüssel benutzten Schlüssel ein. Ihr Brother-Gerät unterstützt nur die Verwendung des ersten WEP-Schlüssels.
- Wenn oben rechts im Touchscreen die Taste  angezeigt wird, können Sie die Wireless-Einstellungen durch Drücken dieser Taste konfigurieren. Gehen Sie zu Schritt 5.

- 2 Drücken Sie .
- 3 Drücken Sie `Netzwerk`.
- 4 Drücken Sie `WLAN`.
- 5 Navigieren Sie nach oben oder unten oder drücken Sie ▲ oder ▼, um `Setup-Assist.` anzuzeigen. Drücken Sie `Setup-Assist.`
- 6 Wenn `WLAN aktivieren?` angezeigt wird, drücken Sie `Ja` zur Bestätigung. Dies startet den Wireless Setup-Assistenten. Zum Abbrechen drücken Sie `Nein`.
- 7 Das Gerät sucht nach verfügbaren SSIDs. Wenn eine Liste von SSIDs angezeigt wird, drücken Sie ▲ oder ▼, um die SSID zu wählen, die Sie in Schritt 1 notiert haben. Drücken Sie `OK`. Sie haben die folgenden Möglichkeiten:
 - Wenn Sie eine Authentifizierungs- und Verschlüsselungsmethode verwenden, die einen Netzwerkschlüssel benötigt, gehen Sie zu Schritt 8.
 - Wenn als Authentifizierungsmethode Open System (Offenes System) und keine Verschlüsselung eingestellt ist, gehen Sie zu Schritt 10.
 - Wenn Ihr WLAN Access Point/Router das WPS unterstützt, wird `Der ausgewählte Access Point/Router unterstützt WPS. WPS verwenden?` angezeigt. Um eine Verbindung für Ihr Gerät über den automatischen Wireless-Modus herzustellen, drücken Sie `Ja`. (Wenn Sie `Nein` (manuell) auswählen, wechseln Sie zu 8, um den Netzwerkschlüssel einzugeben.) Wenn WPS auf Ihrem Wireless Access Point/Router starten, dann `[Weiter]` drücken. erscheint, drücken Sie die Taste für WPS an Ihrem WLAN-Access Point/Router, und drücken Sie dann `Weiter`. Gehen Sie zu Schritt 9.

- 8 Geben Sie den Netzwerkschlüssel ein, den Sie in Schritt 1 notiert haben. (Informationen zur Texteingabe: >> Installationsanleitung.)
Drücken Sie **OK**.
Wenn Sie alle Zeichen eingegeben haben, drücken Sie **Ja**, um Ihre Einstellungen anzuwenden. Gehen Sie zu Schritt 9.
- 9 Ihr Gerät versucht nun, mit den von Ihnen eingegebenen Informationen eine Verbindung zu Ihrem Wireless-Netzwerk herzustellen.
- 10 Wenn Ihr Wireless-Gerät erfolgreich eine Verbindung aufgebaut hat, wird im Display **Verbunden** angezeigt.
Das Gerät druckt einen Bericht über den Wireless-Status Ihres Gerätes aus. Falls die Verbindung nicht erfolgreich hergestellt werden konnte, überprüfen Sie den im Bericht ausgedruckten Fehlercode.
(>> Installationsanleitung: *Problemlösung*.)



(Windows®)

Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Wenn Sie mit der Installation der Treiber und der für den Betrieb Ihres Gerätes erforderlichen Software fortfahren möchten, wählen Sie MFL-Pro Suite installieren im Menü der CD-ROM.

(Macintosh)

Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Wenn Sie mit der Installation der Treiber und der für den Betrieb Ihres Gerätes erforderlichen Software fortfahren möchten, wählen Sie Start Here OSX im Menü der CD-ROM.

Konfigurieren Ihres Geräts, wenn keine SSID gesendet wird

- 1 Bevor Sie Ihr Gerät konfigurieren, sollten Sie sich die Einstellungen Ihres Wireless-Netzwerkes notieren. Sie benötigen diese Informationen, um mit der Konfiguration fortzufahren. Überprüfen und notieren Sie die aktuellen Wireless-Netzwerkeinstellungen.

Netzwerkname: (SSID)

3

Kommunikationsmodus	Authentifizierungsmethode	Verschlüsselungsmodus	Netzwerkschlüssel
Infrastruktur	Open system (offenes System)	Keine	—
		WEP	
	Shared Key	WEP	
	WPA/WPA2-PSK	AES	
		TKIP ¹	

¹ TKIP wird nur für WPA-PSK unterstützt.

Zum Beispiel:

Netzwerkname: (SSID)
HELLO

Kommunikationsmodus	Authentifizierungsmethode	Verschlüsselungsmodus	Netzwerkschlüssel
Infrastruktur	WPA2-PSK	AES	12345678

HINWEIS

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

- 2 Drücken Sie .
- 3 Drücken Sie **Netzwerk**.
- 4 Drücken Sie **WLAN**.
- 5 Navigieren Sie nach oben oder unten oder drücken Sie **▲** oder **▼**, um **Setup-Assist.** anzuzeigen. Drücken Sie **Setup-Assist.**
- 6 Wenn **WLAN aktivieren?** angezeigt wird, drücken Sie **Ja** zur Bestätigung. Dies startet den Wireless Setup-Assistenten. Zum Abbrechen drücken Sie **Nein**.
- 7 Das Gerät sucht nach Ihrem Netzwerk und listet die verfügbaren SSIDs auf. Wählen Sie **<Neue SSID>** mit **▲** oder **▼**. Drücken Sie **OK**.

- 8 Geben Sie den SSID-Namen ein. (Informationen zur Texteingabe: >> Installationsanleitung.)
Drücken Sie OK.
- 9 Drücken Sie **Infrastruktur**, wenn die entsprechende Aufforderung angezeigt wird.
- 10 Wählen und drücken Sie die gewünschte Authentifizierungsmethode.
Sie haben die folgenden Möglichkeiten:
Wenn Sie **Open System** gewählt haben, gehen Sie zu Schritt 11.
Wenn Sie **Shared Key** gewählt haben, gehen Sie zu Schritt 12.
Wenn Sie **WPA/WPA2-PSK** gewählt haben, gehen Sie zu Schritt 13.
- 11 Wählen und drücken Sie die gewünschte Verschlüsselungsmethode **Keine** oder **WEP**.
Sie haben die folgenden Möglichkeiten:
Wenn Sie **Keine** gewählt haben, gehen Sie zu Schritt 15.
Wenn Sie **WEP** gewählt haben, gehen Sie zu Schritt 12.
- 12 Geben Sie den WEP-Schlüssel ein, den Sie in Schritt 1 notiert haben. Drücken Sie OK. Gehen Sie zu Schritt 15. (Informationen zur Texteingabe: >> Installationsanleitung.)
- 13 Wählen und drücken Sie die gewünschte Verschlüsselungsmethode **TKIP** oder **AES**. Gehen Sie zu Schritt 14.
- 14 Geben Sie den WPA-Schlüssel ein, den Sie in Schritt 1 notiert haben. Drücken Sie OK. Gehen Sie zu Schritt 15. (Informationen zur Texteingabe: >> Installationsanleitung.)
- 15 Um die Einstellungen zu übernehmen, wählen Sie **Ja**. Zum Abbrechen drücken Sie **Nein**.
Sie haben die folgenden Möglichkeiten:
Wenn Sie **Ja** gewählt haben, gehen Sie zu Schritt 16.
Wenn Sie **Nein** gewählt haben, gehen Sie zurück zu Schritt 7.
- 16 Das Gerät versucht nun, die Verbindung mit dem von Ihnen gewählten Wireless-Netzwerk aufzubauen.
- 17 Wenn Ihr Wireless-Gerät erfolgreich eine Verbindung aufgebaut hat, wird im Display **Verbunden** angezeigt.
Das Gerät druckt einen Bericht über den Wireless-Status Ihres Gerätes aus. Falls die Verbindung nicht erfolgreich hergestellt werden konnte, überprüfen Sie den im Bericht ausgedruckten Fehlercode.
(>> Installationsanleitung: *Problemlösung*.)



(Windows®)

Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Wenn Sie mit der Installation der Treiber und der für den Betrieb Ihres Gerätes erforderlichen Software fortfahren möchten, wählen Sie MFL-Pro Suite installieren im Menü der CD-ROM.

(Macintosh)

Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Wenn Sie mit der Installation der Treiber und der für den Betrieb Ihres Gerätes erforderlichen Software fortfahren möchten, wählen Sie Start Here OSX im Menü der CD-ROM.

Konfigurieren Ihres Geräts für ein Wireless-Unternehmensnetzwerk

- 1 Bevor Sie Ihr Gerät konfigurieren, sollten Sie sich die Einstellungen Ihres Wireless-Netzwerkes notieren. Sie benötigen diese Informationen, um mit der Konfiguration fortzufahren.

Überprüfen und notieren Sie die aktuellen Wireless-Netzwerkeinstellungen.

Netzwerkname: (SSID)

3

Kommunikationsmodus	Authentifizierungsmethode	Verschlüsselungsmodus	Benutzer-ID	Kennwort
Infrastruktur	LEAP	CKIP		
	EAP-FAST/NONE	AES		
		TKIP		
	EAP-FAST/MS-CHAPv2	AES		
		TKIP		
	EAP-FAST/GTC	AES		
		TKIP		
	PEAP/MS-CHAPv2	AES		
		TKIP		
	PEAP/GTC	AES		
		TKIP		
	EAP-TTLS/CHAP	AES		
		TKIP		
	EAP-TTLS/MS-CHAP	AES		
		TKIP		
	EAP-TTLS/MS-CHAPv2	AES		
		TKIP		
	EAP-TTLS/PAP	AES		
		TKIP		
	EAP-TLS	AES		—
		TKIP		—

Zum Beispiel:

Netzwerkname: (SSID)
HELLO

Kommunikationsmodus	Authentifizierungsmethode	Verschlüsselungsmodus	Benutzer-ID	Kennwort
Infrastruktur	EAP-FAST/MS-CHAPv2	AES	Brother	12345678

HINWEIS

- Wenn Sie Ihr Gerät mit EAP-TLS-Authentifizierung konfigurieren, müssen Sie das von einer Zertifizierungsstelle ausgegebene Client-Zertifikat installieren, bevor Sie mit der Konfiguration beginnen. Wenden Sie sich bezüglich des Client-Zertifikats an Ihren Netzwerkadministrator. Wenn Sie mehrere Zertifikate installiert haben, empfehlen wir, den Namen des Zertifikates zu notieren, das Sie verwenden möchten. Zur Installation des Zertifikates lesen Sie *Verwenden von Zertifikaten zur Gerätesicherheit* >> Seite 87.
- Wenn Sie Ihr Gerät mit dem allgemeinen Namen des Server-Zertifikates verifizieren, empfehlen wir, den allgemeinen Namen zu notieren, bevor Sie mit der Konfiguration beginnen. Wenden Sie sich bei Fragen zum allgemeinen Namen des Server-Zertifikates an Ihren Netzwerkadministrator.

- 2 Drücken Sie .
- 3 Drücken Sie `Netzwerk`.
- 4 Drücken Sie `WLAN`.
- 5 Navigieren Sie nach oben oder unten oder drücken Sie `▲` oder `▼`, um `Setup-Assist.` anzuzeigen. Drücken Sie `Setup-Assist.`
- 6 Wenn `WLAN aktivieren?` angezeigt wird, drücken Sie `Ja` zur Bestätigung. Dies startet den Wireless Setup-Assistenten. Zum Abbrechen drücken Sie `Nein`.
- 7 Das Gerät sucht nach Ihrem Netzwerk und listet die verfügbaren SSIDs auf. Darunter sollte die SSID sein, die Sie zuvor notiert haben. Wenn das Gerät mehr als ein Netzwerk findet, navigieren Sie nach oben oder unten oder drücken Sie `▲` oder `▼`, um Ihr Netzwerk zu wählen. Gehen Sie zu Schritt 11. Drücken Sie `OK`. Wenn der Access Point so eingestellt ist, dass er keine SSID sendet, müssen Sie den SSID-Namen manuell hinzufügen. Gehen Sie zu Schritt 8.
- 8 Navigieren Sie nach oben oder unten oder drücken Sie `▲` oder `▼`, um `<Neue SSID>` zu wählen. Drücken Sie `OK`. Gehen Sie zu Schritt 9.
- 9 Geben Sie den SSID-Namen ein. (Informationen zur Texteingabe: >> Installationsanleitung.) Drücken Sie `OK`. Gehen Sie zu Schritt 10.
- 10 Wählen Sie `Infrastruktur`, wenn die entsprechende Aufforderung angezeigt wird.
- 11 Wählen Sie die Authentifizierungsmethode mit `▲` oder `▼`. Sie haben die folgenden Möglichkeiten:
 - Wenn Sie `LEAP` gewählt haben, gehen Sie zu Schritt 17.
 - Wenn Sie `EAP-FAST` gewählt haben, gehen Sie zu Schritt 12.
 - Wenn Sie `PEAP` gewählt haben, gehen Sie zu Schritt 12.
 - Wenn Sie `EAP-TTLS` gewählt haben, gehen Sie zu Schritt 12.
 - Wenn Sie `EAP-TLS` gewählt haben, gehen Sie zu Schritt 13.

Konfigurieren Ihres Gerätes für ein Wireless-Netzwerk (Für HL-3180CDW, DCP-9015CDW, DCP-9017CDW, DCP-9020CDW, DCP-9022CDW, MFC-9130CW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW)

- 12 Wählen Sie die innere Authentifizierungsmethode `NONE`, `CHAP`, `MS-CHAP`, `MS-CHAPv2`, `GTC` oder `PAP`. Gehen Sie zu Schritt 13.

HINWEIS

Je nach verwendeter Authentifizierung unterscheiden sich die Methoden zur inneren Authentifizierung.

- 13 Wählen Sie die Verschlüsselungsmethode `TKIP` oder `AES`.
Sie haben die folgenden Möglichkeiten:
Wenn Sie als Authentifizierungsmethode `EAP-TLS` verwenden, gehen Sie zu Schritt 14.
Wenn Sie eine andere Authentifizierungsmethode verwenden, gehen Sie zu Schritt 15.
- 14 Das Gerät zeigt eine Liste der verfügbaren Client-Zertifikate an. Wählen Sie das Zertifikat und gehen Sie zu Schritt 15.
- 15 Wählen Sie die Verifizierungsmethode `No Verification`, `CA` oder `CA + Server ID`.
Sie haben die folgenden Möglichkeiten:
Wenn Sie `CA + Server ID` gewählt haben, gehen Sie zu Schritt 16.
Wenn Sie eine andere Auswahl getroffen haben, gehen Sie zu Schritt 17.

HINWEIS

Wenn Sie kein CA-Zertifikat auf Ihr Gerät importiert haben, zeigt das Gerät `No Verification` an. Informationen zum Importieren eines CA-Zertifikates finden Sie unter *Verwenden von Zertifikaten zur Gerätesicherheit* >> Seite 87.

- 16 Geben Sie die Server-ID ein. (Informationen zur Texteingabe: >> Installationsanleitung.)
Drücken Sie `OK`. Gehen Sie zu Schritt 17.

- 17** Geben Sie die Benutzer-ID ein, die Sie in Schritt **1** notiert haben. Drücken Sie **OK**. (Informationen zur Texteingabe: **>>** Installationsanleitung.)
Sie haben die folgenden Möglichkeiten:
Wenn Sie als Authentifizierungsmethode EAP-TLS verwenden, gehen Sie zu Schritt **19**.
Wenn Sie eine andere Authentifizierungsmethode verwenden, gehen Sie zu Schritt **18**.
- 18** Geben Sie das Kennwort ein, das Sie in Schritt **1** notiert haben. Drücken Sie **OK**. Gehen Sie zu Schritt **19**.
- 19** Um die Einstellungen zu übernehmen, wählen Sie **Ja**. Zum Abbrechen wählen Sie **Nein**.
Sie haben die folgenden Möglichkeiten:
Wenn Sie **Ja** gewählt haben, gehen Sie zu Schritt **20**.
Wenn Sie **Nein** gewählt haben, gehen Sie zurück zu Schritt **7**.
- 20** Das Gerät versucht nun, die Verbindung mit dem von Ihnen gewählten Wireless-Netzwerk aufzubauen.
- 21** Wenn Ihr Wireless-Gerät erfolgreich eine Verbindung aufgebaut hat, wird im Display **Verbunden** angezeigt.
Das Gerät druckt einen Bericht über den Wireless-Status Ihres Gerätes aus. Falls die Verbindung nicht erfolgreich hergestellt werden konnte, überprüfen Sie den im Bericht ausgedruckten Fehlercode.
(**>>** Installationsanleitung: *Problemlösung*.)



(Windows®)

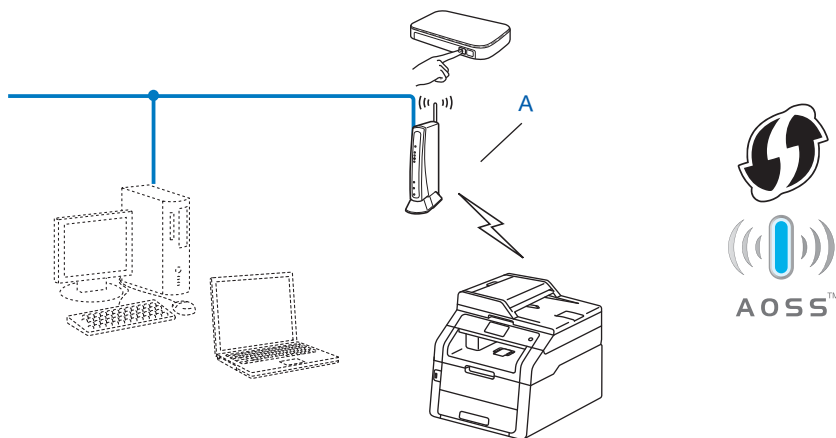
Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Wenn Sie mit der Installation der Treiber und der für den Betrieb Ihres Gerätes erforderlichen Software fortfahren möchten, wählen Sie MFL-Pro Suite installieren im Menü der CD-ROM.

(Macintosh)

Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Wenn Sie mit der Installation der Treiber und der für den Betrieb Ihres Gerätes erforderlichen Software fortfahren möchten, wählen Sie Start Here OSX im Menü der CD-ROM.

Konfiguration mit WPS (Wi-Fi Protected Setup) oder AOSS™ per Tastendruck

Sie können WPS oder AOSS™ über das Menü des Funktionstastenfeldes zur Konfiguration der Wireless-Netzwerkeinstellungen verwenden, wenn Ihr WLAN-Access Point/Router (A) entweder WPS (PBC ¹) oder AOSS™ unterstützt.



¹ Push Button Configuration (Konfiguration per Tastendruck)

WICHTIG

- Wenn Sie Ihr Brother-Gerät in Ihrem Netzwerk anschließen möchten, sollten Sie sich vor der Installation an Ihren Systemadministrator wenden. **Sie müssen Ihre Wireless-Netzwerkeinstellungen kennen, bevor Sie mit der Installation fortfahren.**
- Falls Sie die Wireless-Einstellungen des Gerätes zuvor schon einmal konfiguriert haben, müssen Sie erst die LAN-Einstellungen zurücksetzen, bevor Sie die Wireless-Einstellungen erneut konfigurieren können.

Informationen zum Zurücksetzen der LAN-Einstellungen finden Sie unter *Zurücksetzen der Netzwerkeinstellungen auf die werkseitigen Standardeinstellungen* >> Seite 48.

- 1 Drücken Sie .
- 2 Drücken Sie Netzwerk.
- 3 Drücken Sie WLAN.
- 4 Navigieren Sie nach oben oder unten oder drücken Sie ▲ oder ▼, um WPS/AOSS anzuzeigen. Drücken Sie WPS/AOSS.
- 5 Wenn WLAN aktivieren? angezeigt wird, drücken Sie Ja zur Bestätigung. Dies startet den Wireless Setup-Assistenten. Zum Abbrechen drücken Sie Nein.

- 6 Wenn auf dem Touchscreen WPS oder AOSS auf dem Wireless Access Point/Router starten, dann [OK] drücken. angezeigt wird, drücken Sie die Taste für WPS oder AOSS™ auf dem WLAN Access Point/Router. Weitere Anweisungen dazu finden Sie im Benutzerhandbuch für Ihren WLAN Access Point/Router.

Drücken Sie dann OK, daraufhin erkennt Ihr Gerät automatisch, welchen Modus (WPS oder AOSS™) Ihr WLAN Access Point/Router verwendet, und versucht, eine Verbindung zu Ihrem Wireless-Netzwerk herzustellen.

- 7 Wenn Ihr Wireless-Gerät erfolgreich eine Verbindung aufgebaut hat, wird im Display *Verbunden* angezeigt.

Das Gerät druckt einen Bericht über den Wireless-Status Ihres Gerätes aus. Falls die Verbindung nicht erfolgreich hergestellt werden konnte, überprüfen Sie den im Bericht ausgedruckten Fehlercode.

(➤➤ Installationsanleitung: *Problemlösung*.)

 (Windows®)

Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Wenn Sie mit der Installation der Treiber und der für den Betrieb Ihres Gerätes erforderlichen Software fortfahren möchten, wählen Sie MFL-Pro Suite installieren im Menü der CD-ROM.

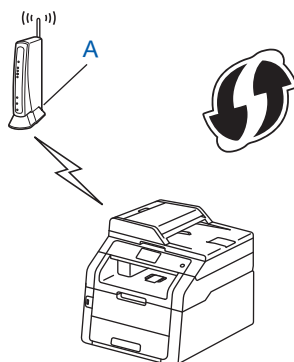
(Macintosh)

Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Wenn Sie mit der Installation der Treiber und der für den Betrieb Ihres Gerätes erforderlichen Software fortfahren möchten, wählen Sie Start Here OSX im Menü der CD-ROM.

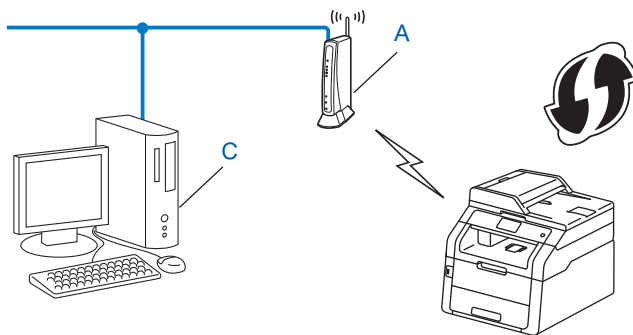
Konfiguration mit der PIN-Methode des WPS (Wi-Fi Protected Setup)

Wenn Ihr WLAN-Access Point/Router WPS (PIN-Methode) unterstützt, können Sie Ihr Gerät ganz einfach konfigurieren. Das PIN-Verfahren (Personal Identification Number) ist eine von der Wi-Fi Alliance[®] entwickelte Verbindungsmethode. Das Wireless-Netzwerk und die Sicherheitseinstellungen können durch Übermittlung einer PIN, die von Ihrem Gerät (dem „Antragsteller“) erstellt wurde, an den Registrar (dem Gerät zum Verwalten des Wireless LANs) eingerichtet werden. Informationen zum Zugriff auf den WPS-Modus finden Sie im Benutzerhandbuch Ihres WLAN Access Points/Routers.

- Verbindung, wenn der WLAN Access Point/Router (A) auch als Registrar¹ verwendet wird.



- Verbindung, wenn ein anderes Gerät (C) wie z. B. ein Computer als Registrar¹ verwendet wird.



¹ Ein Registrar ist ein Gerät zur Verwaltung des WLANs.

HINWEIS

Auf Routern oder Access Points, die WPS unterstützen, finden Sie ein Symbol, wie unten gezeigt.



- 1 Drücken Sie .
- 2 Drücken Sie Netzwerk.
- 3 Drücken Sie WLAN.
- 4 Navigieren Sie nach oben oder unten oder drücken Sie ▲ oder ▼, um WPS + PIN-Code anzuzeigen. Drücken Sie WPS + PIN-Code.
- 5 Wenn WLAN aktivieren? angezeigt wird, drücken Sie Ja zur Bestätigung. Dies startet den Wireless Setup-Assistenten. Zum Abbrechen drücken Sie Nein.
- 6 Im Touchscreen wird eine 8-stellige PIN angezeigt und das Gerät beginnt nach einem Access Point zu suchen.
- 7 Öffnen Sie auf einem Computer in Ihrem Netzwerk einen Browser und geben Sie „http://IP-Adresse des Access Point/“ ein.
(Wobei „IP-Adresse von Access Point“ die IP-Adresse des Gerätes ist, das als Registrar¹ verwendet wird.) Gehen Sie zur Einstellungsseite für WPS und geben Sie die in Schritt 6 im Touchscreen angezeigte PIN für den Registrar ein. Folgen Sie den Anweisungen auf dem Bildschirm.

¹ Der Registrar ist in der Regel der WLAN Access Point / Router.

HINWEIS

Die Einstellungsseite unterscheidet sich je nach WLAN Access Point / Router. Lesen Sie die Anleitung, die mit Ihrem WLAN Access Point / Router geliefert wurde.

Windows Vista®/Windows® 7/Windows® 8

Falls Sie Ihren Computer als Registrar verwenden, gehen Sie wie folgt vor:

HINWEIS

- Um einen Computer mit Windows Vista®, Windows® 7 oder Windows® 8 als Registrar zu verwenden, muss dieser zuvor in Ihrem Netzwerk registriert werden. Lesen Sie die Anleitung, die mit Ihrem WLAN-Access Point/Router geliefert wurde.
- Wenn Sie Windows® 7 oder Windows® 8 als Registrar verwenden, können Sie nach der Wireless-Konfiguration den Druckertreiber mit Hilfe der Anweisungen auf dem Bildschirm installieren. Wenn Sie das gesamte Treiber- und Software-Paket installieren möchten: ►► Installationsanleitung.

1 (Windows Vista®)

Klicken Sie auf die Schaltfläche  und dann auf **Netzwerk**.

(Windows® 7)

Klicken Sie auf die Schaltfläche  und dann auf **Geräte und Drucker**.

(Windows® 8)

Ziehen Sie Ihre Maus in die untere rechte Ecke Ihres Desktops. Wenn die Menüleiste erscheint, klicken Sie auf **Einstellungen** und dann auf **Systemsteuerung**. Klicken Sie in der Gruppe **Hardware und Sound** auf **Geräte und Drucker anzeigen**.

2 (Windows Vista®)

Klicken Sie auf **Ein Drahtlosgerät hinzufügen**.

(Windows® 7/Windows® 8)

Klicken Sie auf **Gerät hinzufügen**.

3 Wählen Sie Ihr Gerät und klicken Sie auf **Weiter**.

4 Geben Sie die PIN ein, die in Schritt ⑥ im Touchscreen angezeigt wurde, und klicken Sie dann auf **Weiter**.

5 Wählen Sie Ihr Netzwerk und klicken Sie auf **Weiter**.

6 Klicken Sie auf **Schließen**.

⑧ Wenn Ihr Wireless-Gerät erfolgreich eine Verbindung aufgebaut hat, wird im Display **Verbunden** angezeigt.

Das Gerät druckt einen Bericht über den Wireless-Status Ihres Gerätes aus. Falls die Verbindung nicht erfolgreich hergestellt werden konnte, überprüfen Sie den im Bericht ausgedruckten Fehlercode.

(➤➤ Installationsanleitung: *Problemlösung*.)



(Windows®)

Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Wenn Sie mit der Installation der Treiber und der für den Betrieb Ihres Gerätes erforderlichen Software fortfahren möchten, wählen Sie MFL-Pro Suite installieren im Menü der CD-ROM.

(Macintosh)

Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Wenn Sie mit der Installation der Treiber und der für den Betrieb Ihres Gerätes erforderlichen Software fortfahren möchten, wählen Sie Start Here OSX im Menü der CD-ROM.

Konfiguration im Ad-hoc-Modus

Verwenden der konfigurierten SSID

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

- 1 Bevor Sie Ihr Gerät konfigurieren, sollten Sie sich die Einstellungen Ihres Wireless-Netzwerkes notieren. Sie benötigen diese Informationen, um mit der Konfiguration fortzufahren.
Überprüfen und notieren Sie die aktuellen Wireless-Netzwerkeinstellungen des Computers, zu dem Sie eine Verbindung herstellen möchten.

HINWEIS

Die Wireless-Netzwerkeinstellungen des Computers, zu dem Sie eine Verbindung herstellen möchten, müssen auf den Ad-hoc-Modus mit bereits konfigurierter SSID gesetzt sein. Anweisungen zur Konfiguration Ihres Computers für den Ad-hoc-Modus finden Sie in den mit Ihrem Computer mitgelieferten Informationen, oder wenden Sie sich an Ihren Netzwerkadministrator.

Netzwerkname: (SSID)

Kommunikationsmodus	Verschlüsselungsmodus	Netzwerkschlüssel
Ad-hoc	Keine	—
	WEP	

Zum Beispiel:

Netzwerkname: (SSID)
HELLO

Kommunikationsmodus	Verschlüsselungsmodus	Netzwerkschlüssel
Ad-hoc	WEP	12345

HINWEIS

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

- 2 Drücken Sie .
- 3 Drücken Sie **Netzwerk**.
- 4 Drücken Sie **WLAN**.
- 5 Navigieren Sie nach oben oder unten oder drücken Sie **▲** oder **▼**, um **Setup-Assist.** anzuzeigen.
Drücken Sie **Setup-Assist.**

- 6 Wenn WLAN aktivieren? angezeigt wird, drücken Sie **Ja** zur Bestätigung.
Dies startet den Wireless Setup-Assistenten.
Zum Abbrechen drücken Sie **Nein**.
- 7 Das Gerät sucht nach Ihrem Netzwerk und listet die verfügbaren SSIDs auf. Wählen Sie die SSID, die Sie in Schritt 1 notiert haben über ▲ oder ▼.
Drücken Sie **OK**.
Sie haben die folgenden Möglichkeiten:
Wenn die SSID unverschlüsselt ist, gehen Sie zu Schritt 10.
Wenn die SSID verschlüsselt ist, gehen Sie zu Schritt 8.
- 8 Geben Sie den WEP-Schlüssel ein, den Sie in Schritt 1 notiert haben. Drücken Sie **OK**. Gehen Sie zu Schritt 9. (Informationen zur Texteingabe: ►► Installationsanleitung.)
- 9 Um die Einstellungen zu übernehmen, wählen Sie **Ja**. Zum Abbrechen drücken Sie **Nein**.
Sie haben die folgenden Möglichkeiten:
Wenn Sie **Ja** gewählt haben, gehen Sie zu Schritt 10.
Wenn Sie **Nein** gewählt haben, gehen Sie zurück zu Schritt 7.
- 10 Das Gerät versucht nun, die Verbindung mit dem von Ihnen gewählten Wireless-Gerät aufzubauen.
- 11 Wenn Ihr Wireless-Gerät erfolgreich eine Verbindung aufgebaut hat, wird im Display **Verbunden** angezeigt.
Das Gerät druckt einen Bericht über den Wireless-Status Ihres Gerätes aus. Falls die Verbindung nicht erfolgreich hergestellt werden konnte, überprüfen Sie den im Bericht ausgedruckten Fehlercode.
(►► Installationsanleitung: *Problemlösung*.)



(Windows®)

Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Wenn Sie mit der Installation der Treiber und der für den Betrieb Ihres Gerätes erforderlichen Software fortfahren möchten, wählen Sie MFL-Pro Suite installieren im Menü der CD-ROM.

(Macintosh)

Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Wenn Sie mit der Installation der Treiber und der für den Betrieb Ihres Gerätes erforderlichen Software fortfahren möchten, wählen Sie Start Here OSX im Menü der CD-ROM.

Verwenden einer neuen SSID

Wenn Sie eine neue SSID verwenden, verbinden sich alle anderen Geräte mit der SSID, die Sie dem Gerät in den folgenden Schritten zuweisen. Sie müssen sich von Ihrem Computer mit dieser SSID verbinden, wenn er sich im Ad-hoc-Modus befindet.

- 1 Drücken Sie .
- 2 Drücken Sie `Netzwerk`.
- 3 Drücken Sie `WLAN`.
- 4 Navigieren Sie nach oben oder unten oder drücken Sie `▲` oder `▼`, um `Setup-Assist.` anzuzeigen. Drücken Sie `Setup-Assist.`
- 5 Wenn `WLAN aktivieren?` angezeigt wird, drücken Sie `Ja` zur Bestätigung. Dies startet den Wireless Setup-Assistenten. Zum Abbrechen drücken Sie `Nein`.
- 6 Das Gerät sucht nach Ihrem Netzwerk und listet die verfügbaren SSIDs auf. Wählen Sie `<Neue SSID>` mit `▲` oder `▼`. Drücken Sie `OK`.
- 7 Geben Sie den SSID-Namen ein. (Informationen zur Texteingabe: `>> Installationsanleitung`.) Drücken Sie `OK`.
- 8 Drücken Sie `Ad-hoc`, wenn die entsprechende Aufforderung angezeigt wird.
- 9 Wählen und drücken Sie die gewünschte Verschlüsselungsmethode `Keine` oder `WEP`. Sie haben die folgenden Möglichkeiten:
Wenn Sie `Keine` gewählt haben, gehen Sie zu Schritt 11.
Wenn Sie `WEP` gewählt haben, gehen Sie zu Schritt 10.
- 10 Geben Sie den WEP-Schlüssel ein. Drücken Sie `OK`. Gehen Sie zu Schritt 11. (Informationen zur Texteingabe: `>> Installationsanleitung`.)

HINWEIS

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

- 11 Um die Einstellungen zu übernehmen, wählen Sie **Ja**. Zum Abbrechen drücken Sie **Nein**.
Sie haben die folgenden Möglichkeiten:
Wenn Sie **Ja** gewählt haben, gehen Sie zu Schritt 12.
Wenn Sie **Nein** gewählt haben, gehen Sie zurück zu Schritt 6.
- 12 Das Gerät versucht nun, die Verbindung mit dem von Ihnen gewählten Wireless-Gerät aufzubauen.
- 13 Wenn Ihr Wireless-Gerät erfolgreich eine Verbindung aufgebaut hat, wird im Display **Verbunden** angezeigt.
Das Gerät druckt einen Bericht über den Wireless-Status Ihres Gerätes aus. Falls die Verbindung nicht erfolgreich hergestellt werden konnte, überprüfen Sie den im Bericht ausgedruckten Fehlercode.
(➤➤ Installationsanleitung: *Problemlösung*.)



(Windows®)

Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Wenn Sie mit der Installation der Treiber und der für den Betrieb Ihres Gerätes erforderlichen Software fortfahren möchten, wählen Sie MFL-Pro Suite installieren im Menü der CD-ROM.

(Macintosh)

Die Einrichtung für das Wireless-Netzwerk ist nun abgeschlossen. Wenn Sie mit der Installation der Treiber und der für den Betrieb Ihres Gerätes erforderlichen Software fortfahren möchten, wählen Sie Start Here OSX im Menü der CD-ROM.

Netzwerk-Menü

Über das **Netzwerk**-Menü des Funktionstastenfeldes können Sie das Brother-Gerät entsprechend Ihrer Netzwerkkonfiguration einrichten. (Weitere Informationen zur Verwendung des Funktionstastenfelds:

➤➤ Benutzerhandbuch - Grundfunktionen.) Drücken Sie , **Alle Einstell.** und drücken Sie dann **Netzwerk**. Rufen Sie nun die Menüauswahl auf, die Sie konfigurieren möchten. (Weitere Informationen zum Menü finden Sie unter *Funktionstabelle und werkseitige Standardeinstellungen* ➤➤ Seite 50.)

Hinweis: Das Gerät wird mit dem Dienstprogramm BRAdmin Light ¹, den Anwendungen Web Based Management oder Remote Setup ² ausgeliefert, die zum Konfigurieren vieler Netzwerkeinstellungen genutzt werden können. (Siehe *Andere Verwaltungsprogramme* ➤➤ Seite 8.)

¹ Macintosh-Nutzer können die neueste Version von Brother BRAdmin Light von <http://solutions.brother.com/> herunterladen.

² Nicht verfügbar für DCP-Modelle.

TCP/IP

Wenn Sie das Gerät mit einem Netzkabel an das Netzwerk anschließen, verwenden Sie die Einstellungen im Menü **LAN (Kabel)**. Wenn Sie das Gerät mit einem Wireless Ethernet-Netzwerk verbinden, verwenden Sie die Einstellungen im Menü **WLAN**.

Boot-Methode

Mit dieser Funktion wird festgelegt, wie das Gerät eine IP-Adresse erhält.

Auto-Modus

Wenn diese Einstellung gewählt ist, sucht das Gerät im Netzwerk nach einem DHCP-Server. Wenn ein DHCP-Server erreicht werden kann und dieser so konfiguriert ist, dass er dem Gerät eine IP-Adresse zuweisen kann, wird die vom DHCP-Server zugewiesene IP-Adresse verwendet. Wenn kein DHCP-Server verfügbar ist, ist festgelegt, dass die IP-Adresse das APIPA-Protokoll verwendet. Nach dem ersten Einschalten des Gerätes kann die Suche des Gerätes nach einem Server im Netzwerk einige Minuten dauern.

Statischer Modus

Mit dieser Einstellung muss die IP-Adresse des Gerätes manuell zugewiesen werden. Die IP-Adresse ist dann auf die hier gespeicherte Adresse festgelegt.

HINWEIS

Wenn Sie Ihren PrintServer nicht über DHCP, BOOTP oder RARP konfigurieren möchten, stellen Sie die **Boot-Methode** auf **Statisch** ein, damit der PrintServer eine statische IP-Adresse erhält. Dies verhindert, dass der PrintServer versucht, eine IP-Adresse von einem dieser Systeme zu erhalten. Um die Boot-Methode zu ändern, verwenden Sie das Funktionstastenfeld des Geräts, das Dienstprogramm BRAdmin Light, Web Based Management oder Remote Setup.

IP-Adresse

Dieses Feld zeigt die aktuelle IP-Adresse des Gerätes an. Wenn Sie die `Boot-Methode Statisch` gewählt haben, geben Sie die IP-Adresse ein, die Sie diesem Gerät zuweisen möchten (fragen Sie Ihren Netzwerkadministrator nach der zu verwendenden IP-Adresse). Falls Sie eine andere Boot-Methode als `Statisch` gewählt haben, versucht das Gerät, eine IP-Adresse über das DHCP- oder BOOTP-Protokoll zu beziehen. Die werkseitig eingestellte IP-Adresse Ihres Gerätes ist wahrscheinlich nicht mit dem Nummerierungssystem in Ihrem Netzwerk kompatibel. Erkundigen Sie sich bei Ihrem Netzwerkadministrator nach einer gültigen IP-Adresse für das Gerät in Ihrem Netzwerk.

Subnetzmaske

Dieses Feld zeigt die aktuelle Subnetzmaske des Gerätes an. Wenn die Subnetzmaske nicht automatisch über DHCP oder BOOTP zugewiesen wird, tragen Sie hier die gewünschte Subnetzmaske ein. Fragen Sie Ihren Netzwerkadministrator nach einer gültigen Subnetzmaske für das Gerät.

Gateway

Dieses Feld zeigt die aktuelle Gateway- oder Router-Adresse des Gerätes an. Wenn die Gateway- oder Router-Adresse nicht automatisch über DHCP oder BOOTP zugewiesen wird, tragen Sie hier die gewünschte Adresse ein. Lassen Sie dieses Feld leer, wenn Sie weder Gateway noch Router verwenden. Fragen Sie gegebenenfalls Ihren Netzwerkadministrator.

Knotenname

Sie können den Gerätenamen im Netzwerk registrieren. Dieser Name wird oft als NetBIOS-Name bezeichnet. Er wird beim WINS-Server Ihres Netzwerkes registriert. Brother empfiehlt den Namen „BRNxxxxxxxxxxx“ für ein verkabeltes Netzwerk und „BRWxxxxxxxxxxx“ für ein Wireless-Netzwerk. („xxxxxxxxxxx“ steht für die MAC-Adresse / Ethernet-Adresse Ihres Gerätes.)

WINS-Konfig.

Mit dieser Funktion wird festgelegt, wie das Gerät die IP-Adresse des WINS-Servers erhält.

Auto

Verwendet eine DHCP-Abfrage, um die IP-Adresse des primären und sekundären WINS-Servers automatisch zu beziehen. Dies ist nur möglich, wenn die Boot-Methode auf `Auto` eingestellt ist.

Statisch

Verwendet eine zuvor angegebene IP-Adresse für den primären und sekundären WINS-Server.

WINS-Server

IP-Adresse primärer WINS-Server

Hier können Sie die IP-Adresse des primären WINS-Servers (Windows® Internet Name Service) eingeben. Wenn ein anderer Wert als 0 (Null) eingegeben wird, wendet sich das Gerät an den betreffenden Server, um seinen Namen im Windows® Internet Name Service (WINS) zu registrieren.

IP Adresse sekundärer WINS-Server

Hier können Sie die IP-Adresse des sekundären WINS-Servers eingeben. Dieser wird als Ersatzserver für den primären WINS-Server verwendet. Falls der primäre Server nicht erreichbar ist, kann sich das Gerät über den sekundären Server registrieren lassen. Wenn ein anderer Wert als 0 (Null) eingegeben wird, wendet sich das Gerät an den betreffenden Server, um seinen Namen im Windows® Internet Name Service (WINS) zu registrieren. Lassen Sie dieses Feld leer, wenn Sie einen primären WINS-Server, aber keinen sekundären WINS-Server verwenden.

DNS-Server

IP-Adresse primärer DNS-Server

Hier können Sie die IP-Adresse des primären DNS-Servers (Domain Name System) eingeben.

IP-Adresse sekundärer DNS-Server

Hier können Sie die IP-Adresse des sekundären DNS-Servers eingeben. Dieser wird als Ersatzserver für den primären DNS-Server verwendet. Falls der primäre Server nicht erreichbar ist, wendet sich das Gerät an den sekundären DNS-Server. Lassen Sie dieses Feld leer, wenn Sie einen primären DNS-Server, aber keinen sekundären DNS-Server verwenden.

APIPA

Wenn diese Einstellung aktiviert ist (**Ein**), weist der PrintServer automatisch eine IP-Adresse aus dem Bereich von 169.254.1.0 bis 169.254.254.255 zu, falls er die IP-Adresse nicht über die eingestellte Boot-Methode erhalten kann. (Siehe *Boot-Methode* ►► Seite 36.) Ist diese Option deaktiviert (**Aus**), bleibt die IP-Adresse unverändert, falls der MFC/DCP-Server keine IP-Adresse über die eingestellte Boot-Methode erhalten kann.

IPv6

Dieses Gerät ist kompatibel mit IPv6, der nächsten Generation der Internetprotokolle. Wenn Sie das IPv6-Protokoll verwenden möchten, wählen Sie **Ein**. Die Standardeinstellung für IPv6 ist **Aus**. Weitere Informationen zum IPv6-Protokoll erhalten Sie unter <http://solutions.brother.com/>.

HINWEIS

- Wenn Sie IPv6 auf **Ein** eingestellt haben, schalten Sie das Gerät aus und wieder ein, um dieses Protokoll zu aktivieren.
- Nachdem Sie für IPv6 **Ein** gewählt haben, gilt diese Einstellung sowohl für den verkabelten LAN-Anschluss als auch für den WLAN-Anschluss.

Ethernet (nur verkabeltes Netzwerk)

Mit dem Ethernet-Link-Modus für automatisch kann der PrintServer im 100BASE-TX-Voll- oder Halbduplex- oder im 10BASE-T-Voll- oder Halbduplex-Modus mit automatischer Aushandlung betrieben werden.

HINWEIS

Wenn hier nicht die richtige Einstellung gewählt ist, kann nicht mit dem MFC/DCP-Server kommuniziert werden.

LAN-Status (Für HL-3180CDW, DCP-9015CDW, DCP-9020CDN, DCP-9020CDW, DCP-9022CDW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW)

Dieses Feld zeigt den aktuellen Status des verkabelten Netzwerkes an.

Setup-Assistent (nur Wireless-Netzwerk)

Der *Setup-Assist.* führt Sie durch die Konfiguration des Wireless-Netzwerkes. (Weitere Informationen: >> Installationsanleitung oder *Manuelle Konfiguration über das Funktionstastenfeld* >> Seite 19.)

WPS (Wi-Fi Protected Setup)/AOSS™ (nur Wireless-Netzwerk)

Wenn Ihr WLAN-Access Point/Router WPS (PBS¹) oder AOSS™ (Auto-Wireless-Modus) unterstützt, können Sie Ihr Gerät ganz einfach konfigurieren. (Weitere Informationen: >> Installationsanleitung oder *Konfiguration mit WPS (Wi-Fi Protected Setup) oder AOSS™ per Tastendruck* >> Seite 27.)

¹ Push Button Configuration (Konfiguration per Tastendruck)

WPS (Wi-Fi Protected Setup) mit PIN-Code (nur Wireless-Netzwerk)

Wenn Ihr WLAN-Access Point/Router WPS (PIN-Methode) unterstützt, können Sie Ihr Gerät ganz einfach konfigurieren. (Weitere Informationen finden Sie unter *Konfiguration mit der PIN-Methode des WPS (Wi-Fi Protected Setup)* >> Seite 29.)

WLAN-Status (Für HL-3180CDW, DCP-9015CDW, DCP-9017CDW, DCP-9020CDW, DCP-9022CDW, MFC-9130CW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW)

Status

Dieses Feld zeigt den aktuellen Status des Wireless-Netzwerkes an.

Signal

Dieses Feld zeigt die aktuelle Signalstärke des Wireless-Netzwerkes an.

SSID

Dieses Feld zeigt die aktuelle SSID des Wireless-Netzwerkes an. Das Display zeigt bis zu 32 Zeichen des SSID-Namens an.

Komm.-Modus

Dieses Feld zeigt den aktuellen Kommunikationsmodus des Wireless-Netzwerkes an.

MAC-Adresse

Die MAC-Adresse ist eine eindeutige Zahl, die der Netzwerkschnittstelle des Gerätes zugeordnet wird. Sie können die MAC-Adresse Ihres Gerätes über das Funktionstastenfeld überprüfen.

Standardwert einstellen

Mit der Funktion *Auf Standard setzen* können Sie die Netzwerkeinstellungen für das verkabelte oder das Wireless-Netzwerk auf die werkseitigen Standardeinstellungen zurücksetzen. Wenn Sie sowohl die Einstellungen für das verkabelte als auch die Einstellungen für das Wireless-Netzwerk zurücksetzen möchten, lesen Sie *Zurücksetzen der Netzwerkeinstellungen auf die werkseitigen Standardeinstellungen* >> Seite 48.

LAN aktivieren (Für DCP-9020CDW, DCP-9022CDW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW)

Wenn Sie eine verkabelte Netzwerkverbindung verwenden möchten, wählen Sie für *Kabel aktiv* die Einstellung *Ein*.

WLAN aktivieren

Wenn Sie eine Wireless-Netzwerkverbindung verwenden möchten, wählen Sie für *WLAN aktiv* die Einstellung *Ein*.

HINWEIS

Wenn Ihr Gerät mit einem Netzkabel verbunden ist, wählen Sie für *Kabel aktiv* die Einstellung *Aus*.

E-Mail/IFAX (MFC-9130CW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW: als Download verfügbar)

In diesem Menü können die folgenden fünf Funktionen eingestellt werden: *Mail-Adresse*, *Servereinstellungen*, *Mail (Empfang)*, *Mail (Senden)* und *Kettenrundsend*. Da für diese Funktionen viel Text eingegeben werden muss, ist es komfortabler, diese Einstellungen über das Web Based Management mit Ihrem Webbrowser zu konfigurieren (siehe *Web Based Management* ►► Seite 57). Sie müssen diese Einstellungen konfigurieren, um die IFAX-Funktion verwenden zu können. (Für weitere Informationen zur Internet-Faxfunktion siehe *Internet-Faxfunktion (MFC-9130CW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW: als Download verfügbar)* ►► Seite 75.)

Sie können das gewünschte Zeichen auch eingeben, indem Sie wiederholt die entsprechende Zifferntaste am Funktionstastenfeld des Gerätes drücken. (Informationen zur Texteingabe: ►► Benutzerhandbuch - Grundfunktionen.)

Mail-Adresse

Sie können die E-Mail-Adresse Ihres Gerätes eingeben.

Setup-Server

SMTP

■ SMTP-Server

Hier wird der Knotenname oder die IP-Adresse eines SMTP-Servers (E-Mail-Server für ausgehende E-Mail) in Ihrem Netzwerk angezeigt.

(Beispiel: „mailhost.brothermail.net“ oder „192.0.0.1“)

■ SMTP-Port

Hier wird die SMTP-Portnummer (für ausgehende E-Mails) in Ihrem Netzwerk angezeigt.

■ Auth. für SMTP

Hier können Sie einstellen, welche Sicherheitsmethode für E-Mail-Benachrichtigungen verwendet wird. (Ausführliche Informationen zu den Sicherheitsmethoden für E-Mail-Benachrichtigungen finden Sie unter *Sicheres Versenden oder Empfangen einer E-Mail* ►► Seite 105.)

■ SMTP SSL/TLS

Hier können Sie die Verschlüsselungsmethode zwischen dem Gerät und dem SMTP-Server auswählen.

■ Zert. verifizieren

Hier können Sie das Sicherheitszertifikat zwischen dem Gerät und dem SMTP-Server aktivieren oder deaktivieren.

POP3

■ POP3-Server

Hier wird der Knotenname oder die IP-Adresse des POP3-Servers angezeigt (E-Mail-Server für eingehende E-Mail), den das Brother-Gerät verwendet. Diese Adresse ist für die Verwendung der Internet-Faxfunktionen erforderlich.

(Beispiel: „mailhost.brothermail.net“ oder „192.0.0.1“)

■ POP3-Port

Hier wird die vom Brother-Gerät verwendete POP3-Portnummer (für eingehende E-Mails) angezeigt.

■ Postfachname

Sie können ein Postfach auf dem POP3-Server festlegen, über das Internet-Druckaufträge abgerufen werden.

■ Postfachkennw.

Sie können ein Kennwort für das Postfach auf dem POP3-Server angeben, über das die Internet-Druckaufträge abgerufen werden.

HINWEIS

Wenn kein Kennwort verwendet werden soll, geben Sie ein einzelnes Leerzeichen ein.

■ POP3 SSL/TLS

Hier können Sie die Verschlüsselungsmethode zwischen dem Gerät und dem POP3-Server auswählen.

■ Zert. verifizieren

Hier können Sie das Sicherheitszertifikat zwischen dem Gerät und dem POP3-Server aktivieren oder deaktivieren.

■ APOP

Sie können das APOP-Protokoll (Authenticated Post Office Protocol) aktivieren oder deaktivieren.

Einrichtung „Mail (Empfang)“

Autom. Abruf

Wenn für diese Funktion **Ein** eingestellt ist, überprüft das Gerät automatisch, ob neue Nachrichten auf dem POP3-Server eingegangen sind.

Abrufhäufigkeit

Legt das Intervall zum Prüfen neu eingehender Nachrichten auf dem POP3-Server fest; (der Standard beträgt 10 Minuten).

Kopfzeile

Diese Einstellung legt fest, welche Elemente des E-Mail-Kopfes mit der empfangenen E-Mail ausgedruckt werden.

Fehler-Mail löschen

Wenn für diese Funktion **Ein** eingestellt ist, löscht das Gerät automatisch fehlerhafte E-Mails, die das Gerät nicht vom POP3-Server empfangen kann.

Benachrichtigung

Mit dieser Funktion kann dem Absender nach dem Empfang des Internet-Faxes eine Empfangsbestätigung gesendet werden.

Diese Funktion ist nur mit Internet-Faxgeräten möglich, die den „MDN“-Standard unterstützen.

Einrichtung „Mail (Senden)“

Absender Betreff

Der hier angezeigte Betreff wird vom Brother-Gerät beim Versenden von Internet-Faxen an einen Computer verwendet (Standardeinstellung ist „Internet-Fax“).

Größenbegrenzung

Manche E-Mail-Server erlauben den Versand umfangreicher E-Mails nicht (Systemadministratoren legen oft eine Obergrenze für die Größe von E-Mails fest). Wenn diese Funktion eingeschaltet ist, zeigt das Gerät *Speicher voll* an, wenn versucht wird, E-Mails, die größer als 1 MB sind, zu versenden. Das Dokument wird nicht gesendet und es wird ein Fehlerbericht ausgedruckt. Teilen Sie das zu sendende Dokument in kleinere Dokumente auf, die der Mailserver dann akzeptiert. (Hinweis: Ein 42 Seiten langes Dokument entsprechend der ITU-T Test Chart #1 ist ungefähr 1 MB groß.)

Benachrichtigung

Mit dieser Funktion kann dem Absender nach dem Empfang des Internet-Faxes eine Empfangsbestätigung gesendet werden.

Diese Funktion ist nur mit Internet-Faxgeräten möglich, die den „MDN“-Standard unterstützen.

Einrichtung Relay

Kettenrundsenden

Mit dieser Funktion kann das Gerät Dokumente über das Internet empfangen und anschließend an andere Faxgeräte über die normale analoge Leitung weiterleiten.

Relaydomäne

Sie können die Namen von Domänen (max. 10) eingeben, von denen das Gerät Kettenrundsende-Aufträge annehmen darf.

Relaybericht

An dem Gerät, das als Kettenrundsende-Gerät verwendet wird, kann ein Kettenrundsende-Bericht ausgedruckt werden.

Seine primäre Funktion ist es, Berichte über alle Kettenrundsende-Aufträge, die über das Gerät gesendet wurden, auszudrucken. Bitte beachten Sie: Sie können diese Funktion nur verwenden, wenn in den Einstellungen für das Kettenrundsenden vertraute Domänen festgelegt wurden.

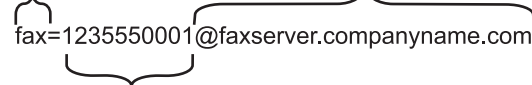
HINWEIS

Weitere Informationen zu Kettenrundende-Aufträgen erhalten Sie unter *Kettenrundsenden* ►► Seite 80.

Fax-to-Server (MFC-9130CW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW: als Download verfügbar)

Mit der Fax-to-Server-Funktion kann ein Dokument eingescannt und über das Netzwerk an einen separaten Faxserver gesendet werden. Das Dokument wird dann vom Faxserver als Faxdaten über die normale Telefonleitung an die Faxnummer des Empfängers gesendet. Wenn die Fax-to-Server-Funktion auf **Ein** eingestellt ist, werden alle vom Gerät automatisch übertragenen Faxdokumente zur weiteren Übertragung an den Faxserver gesendet. Sie können ein Fax auch weiter direkt vom Gerät aus versenden, indem Sie die manuelle Faxfunktion verwenden.

Um ein Dokument an den Faxserver zu senden, muss die für diesen Server korrekte Syntax verwendet werden. Die Faxnummer des Empfängers muss mit einem Präfix und einem Suffix übertragen werden, die den vom Faxserver verwendeten Parametern entsprechen. In den meisten Fällen lautet das Präfix „fax=“ und als Suffix wird der Domänenname des E-Mail-Gateways des Faxservers verwendet. Das Suffix muss mit dem Symbol „@“ beginnen. Bevor Sie die Fax-to-Server-Funktion verwenden können, müssen das Präfix und Suffix im Gerät gespeichert werden. Empfänger-Faxnummern können als Kurzwahl gespeichert oder über die Zifferntasten eingegeben werden (bis zu 20 Ziffern). Wenn Sie zum Beispiel ein Dokument an die Faxnummer 123-555-0001 senden möchten, verwenden Sie die folgende Syntax:

Präfix
Suffix

Gewünschte Faxnummer

HINWEIS

Ihre Faxserver-Anwendung muss ein E-Mail-Gateway unterstützen.

Aktivieren der Fax-to-Server-Funktion

Sie können das Präfix/Suffix für den Faxserver im Gerät speichern.

- 1 Drücken Sie .
- 2 Drücken Sie `Alle Einstell.`
- 3 Navigieren Sie nach oben oder unten oder drücken Sie `▲` oder `▼`, um `Netzwerk` anzuzeigen.
Drücken Sie `Netzwerk`.
- 4 Navigieren Sie nach oben oder unten oder drücken Sie `▲` oder `▼`, um `Fax to Server` anzuzeigen.
Drücken Sie `Fax to Server`.
- 5 Drücken Sie `Ein.`
- 6 Drücken Sie `Präfix`.
- 7 Geben Sie das Präfix mit der Bildschirm-Tastatur ein.
- 8 Drücken Sie `OK`.
- 9 Drücken Sie `Suffix`.
- 10 Geben Sie das Suffix mit der Bildschirm-Tastatur ein.
- 11 Drücken Sie `OK`.
- 12 Drücken Sie .

HINWEIS

- Für die Eingabe der Präfix- und Suffixadresse dürfen insgesamt bis zu 40 Zeichen verwendet werden.
- Informationen zur Texteingabe: ►► Benutzerhandbuch - Grundfunktionen.

So verwenden Sie die Fax-to-Server-Funktion

- 1 Legen Sie das Dokument in den automatischen Vorlageneinzug (ADF) oder auf das Vorlagenglas.
- 2 Geben Sie die Faxnummer ein.
- 3 Drücken Sie **Fax Start**.
Das Gerät sendet die Nachricht über das TCP/IP-Netzwerk an den Faxserver.

So richten Sie eine neue Standardeinstellung für die Scan-to-FTP-Funktion ein

4

Sie können für die Funktion Scan to FTP die Standard-Farbeinstellung und den Standard-Dateityp auswählen. (Informationen zur Verwendung der Scan-to-FTP-Funktion: ►► Software-Handbuch.)

So richten Sie eine neue Standardeinstellung für die Scan-to-Netzwerk-Funktion (Windows®) ein

Sie können für die Funktion Scan to Netzwerk (SMB) die Standard-Farbeinstellung und den Standard-Dateityp auswählen, um ein Dokument einzuscannen und direkt auf einem Server in Ihrem lokalen Netzwerk oder im Internet zu speichern. Dazu muss der Server das CIFS-Protokoll unterstützen. (Informationen zum CIFS-Protokoll finden Sie unter *CIFS* ►► Seite 125.) (Informationen zur Verwendung der Scan-to-Netzwerk-Funktion: ►► Software-Handbuch.)

Zurücksetzen der Netzwerkeinstellungen auf die werkseitigen Standardeinstellungen

Sie können den MFC/DCP-Server (d. h. alle Einstellungen wie Kennwort und IP-Adresse) auf die werkseitigen Standardeinstellungen zurücksetzen.

HINWEIS

- Diese Funktion setzt alle Einstellungen für verkabelte und Wireless-Netzwerke auf die werkseitigen Standardeinstellungen zurück.
- Sie können den MFC/DCP-Server auch mit Hilfe der BRAdmin-Anwendungen oder dem Web Based Management auf die werkseitigen Standardeinstellungen zurücksetzen. (Weitere Informationen finden Sie unter *Andere Verwaltungsprogramme* >> Seite 8.)

- 1 Drücken Sie .
- 2 Drücken Sie `Alle Einstell.`
- 3 Navigieren Sie nach oben oder unten oder drücken Sie ▲ oder ▼, um `Netzwerk` anzuzeigen. Drücken Sie `Netzwerk`.
- 4 Navigieren Sie nach oben oder unten oder drücken Sie ▲ oder ▼, um `Netzwerk-Reset` anzuzeigen. Drücken Sie `Netzwerk-Reset`.
- 5 Drücken Sie `Ja`.
- 6 Drücken Sie zur Bestätigung zwei Sekunden lang `Ja`.

Drucken des Netzwerk-Konfigurationsberichts

HINWEIS

Knotenname: Den Knotennamen können Sie dem Netzwerk-Konfigurationsbericht entnehmen. Der Standardknotenname ist „BRNxxxxxxxxxxxx“ für ein verkabeltes Netzwerk und „BRWxxxxxxxxxxxx“ für ein Wireless-Netzwerk. („xxxxxxxxxxxx“ steht für die MAC-Adresse / Ethernet-Adresse Ihres Gerätes.)

Der Netzwerk-Konfigurationsbericht druckt eine Liste aller aktuellen Netzwerk-Konfigurationseinstellungen einschließlich der Netzwerkeinstellungen Ihres PrintServers.

4

- 1 Drücken Sie .
- 2 Drücken Sie `Alle Einstell.`
- 3 Navigieren Sie nach oben oder unten oder drücken Sie `▲` oder `▼`, um `Ausdrucke` anzuzeigen. Drücken Sie `Ausdrucke`.
- 4 Drücken Sie `Netzwerk-Konfiguration`.
- 5 Drücken Sie `OK`.

HINWEIS

Wenn die **IP Address** im Netzwerk-Konfigurationsbericht mit **0.0.0.0** angezeigt wird, warten Sie eine Minute und wiederholen Sie dann den Vorgang.

Drucken des WLAN-Bericht (Für HL-3180CDW, DCP-9015CDW, DCP-9017CDW, DCP-9020CDW, DCP-9022CDW, MFC-9130CW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW)

Die Funktion `WLAN-Bericht` druckt einen Bericht über den Wireless-Status Ihres Gerätes aus. Falls die kabellose Verbindung nicht erfolgreich hergestellt werden konnte, überprüfen Sie den im Bericht ausgedruckten Fehlercode. >> Installationsanleitung: *Problemlösung*.

- 1 Drücken Sie .
- 2 Drücken Sie `Alle Einstell.`
- 3 Navigieren Sie nach oben oder unten oder drücken Sie `▲` oder `▼`, um `Ausdrucke` anzuzeigen. Drücken Sie `Ausdrucke`.
- 4 Navigieren Sie nach oben oder unten oder drücken Sie `▲` oder `▼`, um `WLAN-Bericht` anzuzeigen. Drücken Sie `WLAN-Bericht`.
- 5 Drücken Sie `OK`.

Funktionstabelle und werkseitige Standardeinstellungen

Die werkseitigen Einstellungen sind fettgedruckt und mit einem Sternchen markiert.

HINWEIS

(Für MFC-9130CW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW)

- Die Funktionen Internet-Fax, Fax-to-Server und Scan-to-E-Mail-Server sind als Download verfügbar.
- Zur Verwendung dieser Funktion laden Sie bitte die erforderliche Firmware von der Seite „Downloads“ für Ihr Modell vom Brother Solutions Center herunter unter <http://solutions.brother.com/>.

Hauptmenü	Untermenü	Menüauswahl		Optionen
Netzwerk	LAN (Kabel) (DCP-9020CDN, DCP-9020CDW, DCP-9022CDW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW)	TCP/IP	Boot-Methode	Auto* Fest RARP BOOTP DHCP (Wenn Sie Auto, RARP, BOOTP oder DHCP wählen, werden Sie gefragt, wie oft das Gerät versuchen soll, die IP-Adresse zu erhalten.)
			IP-Adresse	[0-255] . [0-255] . [0-255] . [0-255] [0] . [0] . [0] . [0]*¹
			Subnet-Mask	[0-255] . [0-255] . [0-255] . [0-255] [0] . [0] . [0] . [0]*¹
			Gateway	[0-255] . [0-255] . [0-255] . [0-255] [0] . [0] . [0] . [0]*
			Knotenname	BRNxxxxxxxxxxxxxx (bis zu 32 Zeichen)
			WINS-Konfiguration	Auto* Fest
			WINS-Server	Primär [0-255] . [0-255] . [0-255] . [0-255] [0] . [0] . [0] . [0]* Sekundär [0-255] . [0-255] . [0-255] . [0-255] [0] . [0] . [0] . [0]*

Hauptmenü	Untermenü	Menüauswahl		Optionen
Netzwerk (Fortsetzung)	LAN (Kabel) (DCP-9020CDN, DCP-9020CDW, DCP-9022CDW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW) (Fortsetzung)	TCP/IP (Fortsetzung)	DNS-Server	Primär [0-255].[0-255].[0-255].[0-255] [0].[0].[0].[0]* Sekundär [0-255].[0-255].[0-255].[0-255] [0].[0].[0].[0]*
			APIPA	Ein* Aus
			IPv6	Ein Aus*
		Ethernet	—	Auto* 100B-FD 100B-HD 10B-FD 10B-HD
		Status (Kabel)	—	Aktiv 100B-FD Aktiv 100B-HD Aktiv 10B-FD Aktiv 10B-HD Inaktiv Kabelgebunden AUS (Nicht verfügbar für DCP-9020CDN)
		MAC-Adresse	—	—
		Auf Standard setzen	—	Ja Nein
		Kabel aktiv (DCP-9020CDW, DCP-9022CDW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW)	—	Ein* Aus

Hauptmenü	Untermenü	Menüauswahl		Optionen
Netzwerk (Fortsetzung)	WLAN (HL-3180CDW, DCP-9015CDW, DCP-9017CDW, DCP-9020CDW, DCP-9022CDW, MFC-9130CW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW) (Fortsetzung)	TCP/IP (Fortsetzung)	Boot-Methode	Auto* Fest RARP BOOTP DHCP (Wenn Sie Auto, RARP, BOOTP oder DHCP wählen, werden Sie gefragt, wie oft das Gerät versuchen soll, die IP-Adresse zu erhalten.)
			IP-Adresse	[0-255].[0-255].[0-255].[0-255] [0].[0].[0].[0]* ¹
			Subnet-Mask	[0-255].[0-255].[0-255].[0-255] [0].[0].[0].[0]* ¹
			Gateway	[0-255].[0-255].[0-255].[0-255] [0].[0].[0].[0]*
			Knotenname	BRWxxxxxxxxxxxxx (bis zu 32 Zeichen)
			WINS-Konfiguration	Auto* Fest
			WINS-Server	Primär [0-255].[0-255].[0-255].[0-255] [0].[0].[0].[0]* Sekundär [0-255].[0-255].[0-255].[0-255] [0].[0].[0].[0]*
			DNS-Server	Primär [0-255].[0-255].[0-255].[0-255] [0].[0].[0].[0]* Sekundär [0-255].[0-255].[0-255].[0-255] [0].[0].[0].[0]*
			APIPA	Ein* Aus
			IPv6	Ein Aus*
		Setup-Assist.	—	—
		WPS/AOSS	—	—
		WPS + PIN-Code	—	—

Hauptmenü	Untermenü	Menüauswahl		Optionen
Netzwerk (Fortsetzung)	WLAN (HL-3180CDW, DCP-9015CDW, DCP-9017CDW, DCP-9020CDW, DCP-9022CDW, MFC-9130CW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW) (Fortsetzung)	WLAN-Status	Status	Aktiv (11n) Aktiv (11b) Aktiv (11g) LAN (Kabel) aktiv (Nicht verfügbar für HL-3180CDW, DCP- 9015CDW, DCP-9017CDW und MFC-9130CW) WLAN Aus AOSS aktiv Keine Verbindung
			Signal	Stark Mittel Schwach Keines
			SSID	—
			Komm. -Modus	Ad-hoc Infrastruktur Keine
		MAC-Adresse	—	—
		Auf Standard setzen	—	Ja Nein
		WLAN aktiv	—	Ein Aus*
	Wi-Fi Direct ² (HL-3180CDW, DCP-9015CDW, DCP-9017CDW, DCP-9020CDW, DCP-9022CDW, MFC-9130CW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW)	Taste drücken	—	—
		PIN-Code	—	—
		Manuell	—	—
		Gruppeneigentümer	—	Ein Aus*
		Geräteinformation	Gerätename	—
			SSID	—
			IP-Adresse	—

Hauptmenü	Untermenü	Menüauswahl		Optionen
Netzwerk (Fortsetzung)	Wi-Fi Direct ² (HL-3180CDW, DCP-9015CDW, DCP-9017CDW, DCP-9020CDW, DCP-9022CDW, MFC-9130CW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW) (Fortsetzung)	Statusinformation		G/O aktiv(**) ** = Anzahl an Geräten Client aktiv Nicht verbunden Aus LAN (Kabel) aktiv (Nicht verfügbar für HL-3180CDW, DCP-9015CDW, DCP-9017CDW und MFC-9130CW)
				Signal Stark Mittel Schwach Keines (Wenn Gruppeneigentümer auf Ein gesetzt ist, ist das Signal auf Stark eingestellt.)
		I/F aktivieren	—	Ein Aus*
	E-Mail/IFAX (MFC-9130CW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW)	Mail-Adresse		—
		Servereinstellungen	SMTP	SMTP-Server
				Name (Bis zu 64 Zeichen) IP-Adresse [0-255].[0-255].[0-255].[0-255]
				SMTP-Port
				25* [00001-65535]
				Auth. für SMTP
				Keine* SMTP-Auth POP vor SMTP
				SMTP SSL/TLS
				Keine* SSL TLS
				SMTP-Zertifikat bestätigen
				Ein Aus*

Hauptmenü	Untermenü	Menüauswahl			Optionen
Netzwerk (Fortsetzung)	E-Mail/IFAX (MFC-9130CW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW) (Fortsetzung)	Servereinstellungen (Fortsetzung)	POP3	POP3-Server	Name (Bis zu 64 Zeichen) IP-Adresse [0-255].[0-255].[0-255].[0-255]
				POP3-Port	110* [00001-65535]
				Postfach-Name	(Bis zu 60 Zeichen)
				Postfach-Passwort	(Bis zu 32 Zeichen)
				POP3 SSL/TLS	Keine* SSL TLS
				POP3-Zertifikat bestätigen	Ein Aus*
				APOP	Ein Aus*
		Mail (Empfang)	Auto-Abruf	Auto-Abruf	Ein* Aus
				Abrufintervall (Wenn Auto-Abruf auf Ein eingestellt ist.)	10 Minuten* (1 Minuten bis 60 Minuten)
			Mail-Kopf	—	Alles Betreff+Von+An Nichts*
			Falsche Mail löschen	—	Ein* Aus
			Bestätigung	—	Ein MDN Aus*

Hauptmenü	Untermenü	Menüauswahl			Optionen
Netzwerk (Fortsetzung)	E-Mail/IFAX (MFC-9130CW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW) (Fortsetzung)	Mail (Senden)	Betreff	—	Internet-Fax* (Bis zu 40 Zeichen)
			Max. Größe	—	Ein Aus*
			Bestätigung	—	Ein Aus*
		Kettenrundsend	Kettenrundsenden	—	Ein Aus*
			Vertr. Domänen	—	VertrautXX: Vertraut(01 - 10)
			K-Sendebericht	—	Ein Aus*
		Manueller POP3-Empfang			—
	Einstellungen für Webverbindung ³	Proxy-Einstell.		Proxy-Verbindung	Ein Aus*
				Adresse	—
				Port	8080*
				Benutzername	—
				Kennwort	—
	Fax to Server (MFC-9130CW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW)	Fax to Server	—	—	Ein Aus*
		Präfix	—	—	—
		Suffix	—	—	—
	Netzwerk-Reset	—	—	—	Ja Nein

¹ Beim Verbinden mit dem Netzwerk stellt das Gerät IP-Adresse und Subnetzmaske automatisch auf Werte ein, die für Ihr Netzwerk geeignet sind.

² Einzelheiten dazu finden Sie Wi-Fi Direct™ Anleitung auf der Handbücher-Downloadseite für Ihr Modell im Brother Solutions Center (<http://solutions.brother.com/>).

³ Einzelheiten dazu finden Sie Web Connect Anleitung auf der Handbücher-Downloadseite für Ihr Modell im Brother Solutions Center (<http://solutions.brother.com/>).

Übersicht

Sie können das Gerät über einen normalen Webbrowser und das HTTP-Protokoll (Hyper Text Transfer Protocol) oder HTTPS-Protokoll (Hyper Text Transfer Protocol over Secure Socket Layer) verwalten. Über einem Webbrowser können Sie die aufgeführten Funktionen ausführen oder die folgenden Informationen von einem Gerät in Ihrem Netzwerk abfragen.

- Informationen über den Gerätestatus
- Faxkonfigurationseinstellungen, zum Beispiel das allgemeine Setup, das Adressbuch und die Fernabfrage ändern (für MFC-Modelle).
- Netzwerkeinstellungen wie z. B. TCP/IP-Informationen ändern
- Secure Function Lock 2.0 konfigurieren (siehe *Secure Function Lock 2.0* ►► Seite 60.)
- Druckprotokoll im Netzwerk speichern konfigurieren (siehe *Druckprotokoll im Netzwerk speichern* ►► Seite 66.)
- Scan-to-FTP konfigurieren (siehe *Ändern der Konfiguration für Scan-to-FTP mit einem Webbrowser* ►► Seite 71.)
- Scan-to-Netzwerk konfigurieren (siehe *Ändern der Konfiguration für Scan-to-Netzwerk mit einem Webbrowser (Windows®)* ►► Seite 73.)
- Informationen zur Software-Version von Gerät und MFC/DCP-Server
- Netzwerk- und Gerätekonfiguration ändern

HINWEIS

Wir empfehlen, Windows® Internet Explorer® 8.0/9.0 oder Safari 5.0 für Macintosh zu verwenden. Stellen Sie auch sicher, dass JavaScript und Cookies in dem von Ihnen benutzten Browser stets aktiviert sind. Wenn Sie andere Webbrowser verwenden, vergewissern Sie sich, dass diese mit HTTP 1.0 und HTTP 1.1 kompatibel sind.

In Ihrem Netzwerk muss das TCP/IP-Protokoll aktiviert sein und Sie müssen eine gültige IP-Adresse für den MFC/DCP-Server und Ihren Computer eingerichtet haben.

So konfigurieren Sie die Geräteeinstellungen über Web Based Management (Webbrowser)

Sie können die PrintServer-Einstellungen über einen normalen Webbrowser und das HTTP-Protokoll (Hyper Text Transfer Protocol) oder HTTPS-Protokoll (Hyper Text Transfer Protocol over Secure Socket Layer) ändern.

HINWEIS

- Wir empfehlen, aus Sicherheitsgründen beim Konfigurieren der Einstellungen über Web Based Management das HTTPS-Protokoll zu verwenden.
- Bei Verwendung des HTTPS-Protokolls für die Konfiguration von Web Based Management zeigt Ihr Browser ein Dialogfeld mit einer Warnung an.

5

- 1 Starten Sie Ihren Webbrowser.
- 2 Geben Sie in die Adressleiste Ihres Browsers „http://IP-Adresse des Gerätes/“ ein (wobei „IP-Adresse des Gerätes“ für die IP-Adresse des Gerätes oder den Namen des PrintServers steht).
 - Zum Beispiel: http://192.168.1.2/

HINWEIS

- Falls Sie ein Domänen-Namensystem (DNS) verwenden oder die Verwendung von NetBIOS-Namen aktiviert haben, können Sie einen anderen Namen wie zum Beispiel „FreigegebenerDrucker“ anstelle der IP-Adresse eingeben.
 - Zum Beispiel: http://FreigegebenerDrucker/

Wenn Sie die Verwendung von NetBIOS-Namen aktiviert haben, können Sie auch den Knotennamen verwenden.

- Zum Beispiel: http://brnxxxxxxxxxxxxx/

Den NetBIOS-Namen können Sie dem Netzwerk-Konfigurationsbericht entnehmen (siehe *Drucken des Netzwerk-Konfigurationsberichts* ►► Seite 49).

- Macintosh-Nutzer können einfach durch Klicken auf das Gerätesymbol im **Status Monitor**-Bildschirm auf das Web Based Management zugreifen. Weitere Informationen: ►► Software-Handbuch.

- 3 Standardmäßig ist kein Kennwort erforderlich. Wenn Sie zuvor ein Kennwort festgelegt haben, geben Sie dieses ein, und drücken Sie auf .
- 4 Sie können nun die Einstellungen des MFC/DCP-Servers ändern.

HINWEIS

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

Kennwort festlegen

Wir empfehlen, ein Anmeldekennwort festzulegen, um unberechtigten Zugriff auf Web Based Management zu verhindern.

- 1 Klicken Sie auf **Administrator**.
- 2 Geben Sie das gewünschte Kennwort ein (bis zu 32 Zeichen).
- 3 Geben Sie das Kennwort erneut in das Feld **Neues Kennwort bestätigen** ein.
- 4 Klicken Sie auf **Senden**.
Geben Sie ab dem nächsten Zugriff auf das Web Based Management das Kennwort in das Feld **Anmelden** und klicken Sie dann auf .
Melden Sie sich nach der Konfiguration der Einstellungen aus, indem Sie auf  klicken.

HINWEIS

Sie können auch ein Kennwort festlegen, indem Sie auf der Webseite des Gerätes auf **Bitte konfigurieren Sie das Kennwort** klicken, wenn Sie kein Anmeldekennwort festlegen möchten.

Secure Function Lock 2.0

Secure Function Lock 2.0 von Brother hilft Ihnen, Geld zu sparen und die Sicherheit zu erhöhen, indem Funktionen Ihres Brother-Gerätes gesperrt werden können.

Mit Secure Function Lock können Sie Kennwörter für ausgewählte Benutzer konfigurieren. Sie können Zugriff auf einige oder alle Funktionen gewähren oder für diese die zulässige Seitenzahl beschränken. Dies bedeutet, dass Funktionen des Gerätes nur von den dazu berechtigten Personen genutzt werden können.

Sie können die folgenden Einstellungen von Secure Function Lock 2.0 mit Web Based Management oder BRAdmin Professional 3 (nur Windows®) konfigurieren und ändern.

- **Drucken** ^{1 2}
- **USB-Direktdruck** ³
- **Kopie**
- **Farbdruck** ^{1 2 5}
- **Seitenbegrenzung** ⁵
- **Fax senden** ³
- **Fax empfangen** ³
- **Scannen** ⁴
- **Web Connect (Hochladen)** ³
- **Web Connect (Herunterladen)** ³
- **Seitenzähler** ⁵

¹ **Drucken** beinhaltet Druckjobs, die über AirPrint, Google Cloud Print und Brother iPrint&Scan gesendet wurden.

² Durch die Registrierung von PC-Anmeldenamen der Benutzer können Sie das Drucken vom PC aus einschränken, ohne dass Benutzer ein Kennwort eingeben müssen. Weitere Informationen finden Sie unter *Einschränken des PC-Drucks über den PC-Anmeldenamen (Benutzernamen)* ►► Seite 62.

³ Nur für Modelle, die diese Funktion unterstützen.

⁴ Scan beinhaltet Scan-Jobs, die über Brother iPrint&Scan gesendet wurden.

⁵ Verfügbar für **Drucken**, **USB-Direktdruck**, **Kopie** und **Web Connect (Herunterladen.)**

So konfigurieren Sie die Einstellungen von Secure Function Lock 2.0 mit Web Based Management (Webbrowser)

Basiskonfiguration

- 1 Klicken Sie auf der Webseite Ihres Gerätes auf **Administrator** und dann auf **Benutzersperre**.
- 2 Wählen Sie **Ein** für **Benutzersperre**.
- 3 Geben Sie im Feld **ID-Nummer/Name** einen alphanumerischen Gruppen- oder Benutzernamen mit bis zu 15 Stellen und dann im Feld **PIN** ein vierstelliges Kennwort ein.
- 4 Deaktivieren Sie im Feld **Druckaktivitäten** oder im Feld **Sonstige** die Funktionen, die Sie einschränken möchten. Wenn Sie die maximale Anzahl von Seiten, die gedruckt werden können, begrenzen möchten, aktivieren Sie das Kontrollkästchen **Ein** unter **Seitenbegrenzung**, und geben Sie dann die gewünschte Anzahl Seiten im Feld **Max.** ein. Klicken Sie dann auf **Senden**.

HINWEIS

Falls Sie den PC-Druck über den PC-Anmeldenamen (Benutzernamen) einschränken möchten, klicken Sie auf **PC-Druckauftrag-Einschränkung durch Benutzernamen** und konfigurieren Sie dann die Einstellungen. (Siehe *Einschränken des PC-Drucks über den PC-Anmeldenamen (Benutzernamen)* ►► Seite 62.)

Scannen während der Verwendung von Secure Function Lock 2.0

Mit Secure Function Lock 2.0 kann der Administrator für bestimmte Nutzer den Zugriff auf die Scanfunktionen ermöglichen bzw. sperren. Wenn das Scannen für den Allgemeinen Benutzer gesperrt ist, können nur Nutzer, deren Scan-Kontrollkästchen aktiviert ist, scannen. Um vom Funktionstastenfeld des Geräts aus zu scannen, müssen die Benutzer ihre PIN zum Zugriff auf den Scanmodus eingeben. Um den Scanvorgang vom Computer aus zu starten, müssen die einzelnen Nutzer auch zuerst ihre PIN am Funktionstastenfeld des Gerätes eingeben, bevor sie vom Computer aus scannen können. Wenn die PIN am Funktionstastenfeld des Geräts nicht eingegeben wird, erhält der Nutzer eine Fehlermeldung an seinem Computer, wenn er versucht, den Scanvorgang zu starten.

Einstellen des allgemeinen Benutzers

Sie können einen allgemeinen Benutzer einrichten und für diesen festlegen, welche Funktionen verfügbar sind. Diese Einstellungen sind dann für alle Benutzer gültig, die zur Nutzung des Gerätes kein Kennwort eingeben.

HINWEIS

Der allgemeine Benutzer beinhaltet Druckjobs, die über AirPrint, Google Cloud Print und Brother iPrint&Scan gesendet wurden.

- 1 Deaktivieren Sie neben **Allgemeiner Benutzer** das Kontrollkästchen der Funktion, die Sie sperren möchten.
- 2 Klicken Sie auf **Senden**.

Einschränken des PC-Drucks über den PC-Anmeldenamen (Benutzernamen)

Durch Konfiguration dieser Einstellung kann das Gerät den Benutzer anhand des PC-Anmeldenamens erkennen und darüber das Drucken von einem registrierten Computer aus erlauben.

- 1 Klicken Sie auf **PC-Druckauftrag-Einschränkung durch Benutzernamen**.
- 2 Wählen Sie **Ein** für **PC-Druckauftrag-Einschränkung**.
- 3 Wählen Sie die ID-Nummer, die Sie für **ID-Nummer/Name** in Schritt 3 festgelegt haben. Informieren Sie sich unter *Basiskonfiguration* >> Seite 61 zu den Angaben in der Dropdown-Liste **ID-Nummer** für jeden Anmeldenamen und geben Sie den Anmeldenamen des PC-Benutzers in das Feld **Anmeldename** ein.
- 4 Klicken Sie auf **Senden**.

HINWEIS

- Wenn Sie das Drucken vom PC aus (PC-Druck) für Benutzergruppen einschränken möchten, wählen Sie dieselbe ID-Nummer für jeden PC-Anmeldenamen, den Sie in die Gruppe aufnehmen möchten.
- Wenn Sie die PC-Anmeldenamen-Funktion verwenden, müssen Sie auch sicherstellen, dass das Kontrollkästchen **PC-Anmeldename verwenden** im Druckertreiber aktiviert ist. Weitere Informationen zum Druckertreiber: >> Software-Handbuch.
- Das Drucken über den BR-Script3-Treiber wird von der Funktion der Benutzersperre nicht unterstützt.

Andere Funktionen

Sie können die folgenden Funktionen für Secure Function Lock 2.0 einstellen:

■ **Alle Zähler zurücksetzen**

Sie können den Seitenzähler zurücksetzen, indem Sie auf **Alle Zähler zurücksetzen** klicken.

■ **Export in CSV-Datei**

Sie können den aktuellen Seitenzählerstand einschließlich der **ID-Nummer/Name**-Informationen in eine CSV-Datei exportieren.

■ **Letzter Zähler-Eintrag**

Das Gerät erhält die Seitenzahl bei, nachdem der Zähler zurückgesetzt wurde.

■ **Zähler automatisch zurücksetzen**

Sie können die Seitenzähler automatisch in regelmäßigen Abständen zurücksetzen, zum Beispiel täglich, monatlich oder wöchentlich.

Synchronisieren mit SNTP-Server

SNTP ist ein Protokoll zur Synchronisation der Zeit, die vom Gerät zur Authentifizierung verwendet wird, mit der Zeit des SNTP-Zeitserver (diese Zeit ist nicht identisch mit der im Touchscreen angezeigten Zeit). Sie können die Zeit, die vom Gerät verwendet wird, in regelmäßigen Abständen mit der UTC-Zeit (Coordinated Universal Time) synchronisieren, die vom SNTP-Zeitserver zur Verfügung gestellt wird.

HINWEIS

Diese Funktion steht nicht in allen Ländern zur Verfügung.

- 1 Klicken Sie auf **Netzwerk** und dann auf **Protokoll**.
- 2 Wählen Sie das Kontrollkästchen **SNTP**, um die Einstellung zu aktivieren.
- 3 Klicken Sie auf **Erweiterte Einstellung**.

■ Status

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

■ SNTP-Server-Methode

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

• AUTO

Wenn ein DHCP-Server in Ihrem Netzwerk vorhanden ist, erhält der SNTP-Server seine IP-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 Backup für die primäre SNTP-Serveradresse verwendet. Falls der primäre Server nicht erreichbar ist, wendet sich das Gerät an den sekundären SNTP-Server. Lassen Sie dieses Feld leer, wenn Sie einen primären SNTP-Server, aber keinen sekundären SNTP-Server verwenden.

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

Geben Sie die Portnummer ein (1 bis 65535).

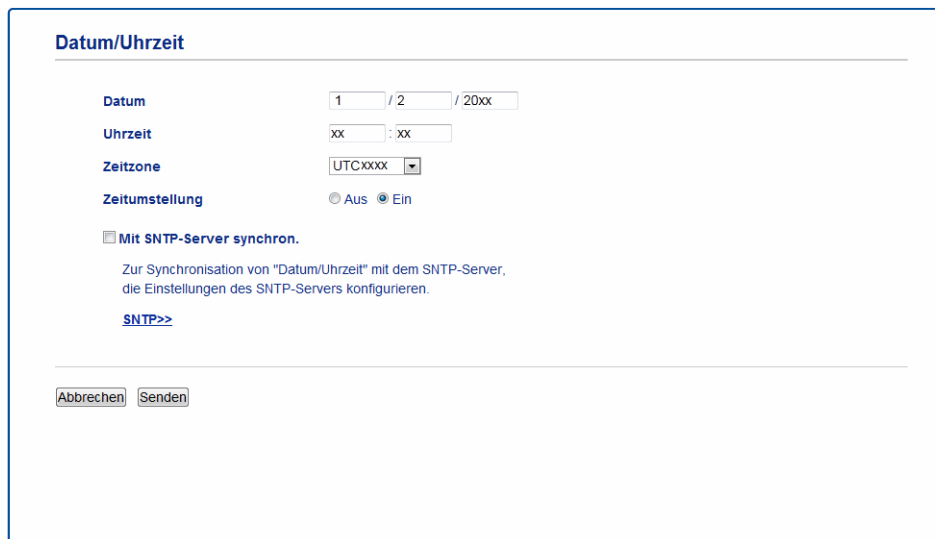
Der sekundäre SNTP-Serverport wird als Backup für den primären SNTP-Serverport verwendet. Falls der primäre Port nicht erreichbar ist, wendet sich das Gerät an den sekundären SNTP-Port. Lassen Sie dieses Feld leer, wenn Sie einen primären SNTP-Port, aber keinen sekundären SNTP-Port verwenden.

■ Synchronisationsintervall

Geben Sie die Stundenanzahl zwischen den Versuchen den Server zu synchronisieren (1 bis 168 Stunden) ein.

HINWEIS

- Sie müssen **Datum/Uhrzeit** konfigurieren, um die Zeit, die vom Gerät verwendet wird, mit der Zeit des SNTP-Zeitserverns zu synchronisieren. Klicken Sie auf **Datum/Uhrzeit**, und konfigurieren Sie dann **Datum/Uhrzeit** auf dem Bildschirm **Allgemein**. Sie können Datum und Uhrzeit auch über das Funktionstastenfeld des Geräts konfigurieren.



- Aktivieren Sie das Kontrollkästchen **Mit SNTP-Server synchron..** Überprüfen Sie auch Ihre Zeitzone-Einstellungen. Wählen Sie die Zeitdifferenz zwischen Ihrem Standort und der UTC-Zeit in der Dropdown-Liste **Zeitzone** aus. Die Zeitzone für die USA und Kanada (Eastern Time) ist zum Beispiel UTC-05:00.

■ Synchronisationsstatus

Sie können den letzten Synchronisationsstatus überprüfen.

- 4 Klicken Sie auf **Senden**, um die ausgewählten Einstellungen zu übernehmen.

Druckprotokoll im Netzwerk speichern

Die Funktion Druckprotokoll im Netzwerk speichern ermöglicht das Speichern der Druckprotokoll-Datei Ihres Brother-Gerätes auf einem Netzwerkservers unter Verwendung von CIFS¹. Sie können die ID, die Art des Druckauftrages, den Auftragsnamen, den Benutzernamen, Datum, Uhrzeit und die Anzahl der gedruckten und farbigen Seiten für jeden Druckauftrag aufzeichnen.

¹ Das CIFS-Protokoll (Common Internet File System) wird unter TCP/IP verwendet und ermöglicht Computern in einem Netzwerk die Freigabe von Dateien in einem Intranet oder im Internet.

Die folgenden Druckfunktionen werden im Druckprotokoll aufgezeichnet:

- Druckaufträge von Ihrem Computer
- USB-Direktdruck (nur für Modelle, die diese Funktion unterstützen)
- Kopien
- Empfangene Faxe (nur für Modelle, die diese Funktion unterstützen)
- Web Connect-Druck

HINWEIS

- Die Funktion Druckprotokoll im Netzwerk speichern unterstützt die Authentifizierung mit **Kerberos** und **NTLMv2**.

Zur Authentifizierung müssen Sie das SNTP-Protokoll (Netzwerk-Zeitserver) konfigurieren oder das Datum, die Uhrzeit und die Zeitzone über das Funktionstastenfeld korrekt einstellen. (Informationen zur SNTP-Konfiguration finden Sie unter *Synchronisieren mit SNTP-Server* ►► Seite 64. Informationen zum Einstellen von Datum, Uhrzeit und Zeitzone: ►► Installationsanleitung.)

- Sie können zum Speichern einer Datei auf dem Server als Dateityp **TXT** oder **CSV** wählen.

So konfigurieren Sie die Einstellungen der Funktion „Druckprotokoll im Netzwerk speichern“ mit Web Based Management (Webbrowser)

- 1 Klicken Sie auf der Webseite Ihres Gerätes auf **Administrator** und dann auf **Druckprotok. im Netz. speichern**.
- 2 Wählen Sie **Ein** für **Druckprotokoll**.
- 3 Sie können die folgenden Einstellungen über einen Webbrowser konfigurieren.

■ Host-Adresse

Die Host-Adresse ist der Hostname des CIFS-Servers. Geben Sie die Host-Adresse ein (zum Beispiel: meinpc.beispiel.com) (bis zu 64 Zeichen) oder die IP-Adresse (zum Beispiel: 192.168.56.189).

■ Zielordner

Geben Sie den Zielordner an, in dem das Protokoll auf dem CIFS-Server gespeichert werden soll (zum Beispiel: brother\abc) (bis zu 60 Zeichen).

■ Dateiname

Geben Sie den gewünschten Dateinamen für das Druckprotokoll ein (bis zu 15 Zeichen).

■ Dateityp

Wählen Sie als Dateityp für das Druckprotokoll **TXT** oder **CSV**.

■ Authentifizierungsmethode

Wählen Sie die für den Zugang zum CIFS-Server erforderliche Authentifizierungsmethode: **Auto**, **Kerberos**¹ oder **NTLMv2**².

¹ Kerberos ist ein Authentifizierungsprotokoll, das es Geräten oder einzelnen Nutzern ermöglicht, sich an Netzwerk-Servern über eine einmalige Anmeldung (Single Sign-on) sicher auszuweisen.

² NTLMv2 ist die von Windows verwendete Authentifizierungsmethode zur Anmeldung an Servern.

- **Auto:** Wenn Sie Auto wählen, sucht das Gerät zunächst nach einem Kerberos-Server. Wenn der Kerberos-Server nicht gefunden wird, wird NTLMv2 als Authentifizierungsmethode verwendet.
- **Kerberos:** Wählen Sie Kerberos, wenn die Authentifizierung ausschließlich mit Kerberos erfolgen soll.
- **NTLMv2:** Wählen Sie NTLMv2, wenn die Authentifizierung ausschließlich mit NTLMv2 erfolgen soll.

Für die Authentifizierung mit Kerberos und NTLMv2 müssen Sie auch die Einstellungen für Datum/Uhrzeit oder das SNTP-Protokoll (Netzwerk-Zeitserver) konfigurieren.

Informationen zur Konfiguration von Datum/Uhrzeit und den SNTP-Einstellungen finden Sie unter **Synchronisieren mit SNTP-Server** >> Seite 64.

Sie können die Einstellungen für Datum/Uhrzeit auch über das Funktionstastenfeld des Gerätes konfigurieren. >> Installationsanleitung.

■ Benutzername

Geben Sie einen Benutzernamen für die Authentifizierung ein (bis zu 96 Zeichen).

HINWEIS

Wenn der Benutzername Bestandteil einer Domäne ist, geben Sie den Benutzernamen in einem der folgenden Formate ein: user@domain oder domain\user.

■ **Kennwort**

Geben Sie das Kennwort für die Authentifizierung ein (bis zu 32 Zeichen).

■ **Kerberos-Serveradresse** (falls erforderlich)

Geben Sie die KDC-Host-Adresse ein (zum Beispiel: meinpc.beispiel.com) (bis zu 64 Zeichen) oder die IP-Adresse (zum Beispiel: 192.168.56.189).

■ **Fehlererkennungseinstellung** (Siehe *Einstellung Fehlererkennung* >> Seite 69.)

- 4 Unter **Verbindungsstatus** können Sie den letzten Protokollstatus überprüfen. Weitere Informationen finden Sie unter *Fehlermeldungen verstehen* >> Seite 70.
- 5 Klicken Sie auf **Senden**, um die Seite **Test-Druckprotokoll im Netzwerk** anzuzeigen. Um Ihre Einstellungen zu testen, klicken Sie auf **Ja** und fahren dann mit Schritt 6 fort. Um den Test zu überspringen, klicken Sie auf **Nein**. Ihre Einstellungen werden automatisch übertragen.
- 6 Das Gerät testet Ihre Einstellungen.
- 7 Wenn Ihre Einstellungen akzeptiert werden, wird auf der Seite **Test: OK** angezeigt. Wenn **Test: Fehler** angezeigt wird, überprüfen Sie alle Einstellungen, und klicken Sie dann auf **Senden**, um die Testseite erneut anzuzeigen.

Einstellung Fehlererkennung

Sie können wählen, welche Aktion ausgeführt werden soll, wenn das Druckprotokoll aufgrund eines Netzwerkfehlers nicht auf dem Server gespeichert werden kann.

- 1 Wählen Sie **Druck abbrechen** oder **Prot.ignorieren&Druck** als **Fehlererkennungseinstellung** unter **Druckprotok. im Netzw. speichern**.

■ Druck abbrechen

Wenn Sie **Druck abbrechen** wählen, werden die Druckaufträge abgebrochen, falls das Druckprotokoll nicht auf dem Server gespeichert werden kann.

HINWEIS

Auch wenn Sie **Druck abbrechen** wählen, druckt das Gerät das empfangene Fax aus.

5

■ Prot.ignorieren&Druck

Wenn Sie **Prot.ignorieren&Druck** wählen, druckt das Gerät das Dokument aus, auch wenn das Druckprotokoll nicht auf dem Server gespeichert werden kann.

Wenn die Funktion zum Speichern des Druckprotokolls wieder zur Verfügung steht, wird das Druckprotokoll wie folgt aufgezeichnet:

- Wenn das Protokoll nach Beendigung des Ausdrucks nicht gespeichert werden kann, wird das Druckprotokoll ohne die Anzahl der gedruckten Seiten aufgezeichnet. (1)
- Wenn das Druckprotokoll zu Beginn und nach Beendigung des Ausdrucks nicht gespeichert werden kann, wird kein Druckprotokoll dieses Auftrags aufgezeichnet. Wenn die Funktion wieder zur Verfügung steht, wird im Protokoll angezeigt, dass ein Fehler aufgetreten ist. (2)

Beispiel eines Druckprotokolls:

```
Id, Type, Job Name, User Name, Date, Time, Print Pages, Color Pages
1, Print (xxxxxxx), "Document01.doc", "user01", 03/03/20xx, 14:01:32, 52, 21
2, Print (xxxxxxx), "Document02.doc", "user01", 03/03/20xx, 14:45:30, ?, ?
3, <Error>, ?, ?, ?, ?, ?, ?
4, Print (xxxxxxx), "Report01.xls", "user02", 03/03/20xx, 19:30:40, 4, 4
```

(1)

(2)

- 2 Klicken Sie auf **Senden**, um die Seite **Test-Druckprotokoll im Netzwerk** anzuzeigen. Um Ihre Einstellungen zu testen, klicken Sie auf **Ja** und fahren dann mit Schritt 3 fort. Um den Test zu überspringen, klicken Sie auf **Nein**. Ihre Einstellungen werden automatisch übertragen.
- 3 Das Gerät testet Ihre Einstellungen.
- 4 Wenn Ihre Einstellungen akzeptiert werden, wird auf der Seite **Test: OK** angezeigt. Wenn **Test: Fehler** angezeigt wird, überprüfen Sie alle Einstellungen, und klicken Sie dann auf **Senden**, um die Testseite erneut anzuzeigen.

Fehlermeldungen verstehen

Sie können den Fehlerstatus im Touchscreen Ihres Gerätes oder den **Verbindungsstatus** im Web Based Management überprüfen.

■ Server Timeout, an Administrator wenden.

Diese Meldung wird angezeigt, wenn keine Verbindung zum Server hergestellt werden kann. Stellen Sie Folgendes sicher:

- Ihre Serveradresse ist korrekt.
- Ihr Server ist an das Netzwerk angeschlossen.
- Das Gerät ist an das Netzwerk angeschlossen.

■ Fehler bei Authentifizierung, an Administrator wenden.

Diese Meldung wird angezeigt, wenn Ihre **Authentifizierungseinstellung** nicht richtig ist. Stellen Sie Folgendes sicher:

- Der Benutzername ¹ und das Kennwort sind in der Authentifizierungseinstellung richtig eingegeben.

¹ Wenn der Benutzername Bestandteil einer Domäne ist, geben Sie den Benutzernamen in einem der folgenden Formate ein:
user@domain oder domain\user.

- Die Zeit des Protokolldateiservers stimmt mit der Zeit des SNTP-Servers bzw. den Einstellungen von **Datum/Uhrzeit** überein.
- Die SNTP-Zeitserver-Einstellungen sind richtig konfiguriert, so dass die dort eingestellte Zeit mit der zur Authentifizierung verwendeten Zeit von Kerberos bzw. NTLMv2 übereinstimmt. Wenn kein SNTP-Server vorhanden ist, stellen Sie sicher, dass **Datum/Uhrzeit** und **Zeitzone** korrekt mit dem Web Based Management oder dem Funktionstastenfeld eingestellt sind, sodass die am Gerät eingestellte Zeit mit der Zeit des Servers für die Authentifizierung übereinstimmt.

■ Fehler bei Dateizugriff, an Administrator wenden.

Diese Meldung wird angezeigt, wenn nicht auf den Zielordner zugegriffen werden kann. Stellen Sie Folgendes sicher:

- Der Verzeichnisname zum Speichern ist korrekt.
- In das Verzeichnis zum Speichern kann geschrieben werden.
- Die Datei ist nicht gesperrt.

■ Datum/Uhrzeit falsch, an Administrator wenden.

Diese Meldung wird angezeigt, wenn Ihr Gerät keine Zeitinformationen vom SNTP-Zeitserver erhält. Stellen Sie Folgendes sicher:

- Die Einstellungen für den Zugriff auf die SNTP-Zeit über Web Based Management sind korrekt.
- Überprüfen Sie in Web Based Management, ob **Datum/Uhrzeit** bei Ihrem Gerät korrekt eingestellt sind.

HINWEIS

Wenn Sie die Option **Druck abbrechen** in Web Based Management gewählt haben, wird die Meldung Fehl:ZugriffProt ca. 60 Sekunden lang im Touchscreen angezeigt.

Verwenden der Funktion „Druckprotokoll im Netzwerk speichern“ mit Secure Function Lock 2.0

Wenn die Funktion Secure Function Lock 2.0 aktiviert ist, werden die Namen der registrierten Benutzer für die Funktionen zum Kopieren, Fax empfangen, Web Connect-Druck und USB-Direktdruck (falls verfügbar) von der Funktion „Druckprotokoll im Netzwerk speichern“ aufgezeichnet.

Beispiel eines Druckprotokolls mit Benutzern von Secure Function Lock 2.0:

```
Id, Type, Job Name, User Name, Date, Time, Print Pages, Color Pages
1, Copy, -, -, 04/04/20xx, 09:05:12, 3, 3
2, Fax, -, -, 04/04/20xx, 09:45:30, 5, 0
3, Copy, -, "Bob", 04/04/20xx, 10:20:30, 4, 0
4, Fax, -, "Bob", 04/04/20xx, 10:35:12, 3, 0
5, USB Direct, -, "John", 04/04/20xx, 11:15:43, 6, 6
```

5

Ändern der Konfiguration für Scan-to-FTP mit einem Webbrowser

Mit der Scan-to-FTP-Funktion können Sie ein Dokument einscannen und direkt auf einem FTP-Server in Ihrem lokalen Netzwerk oder im Internet speichern. Für weitere Informationen zu Scan-to-FTP:

➤➤ Software-Handbuch.

- 1 Klicken Sie auf der Webseite Ihres Gerätes auf **Scannen** und dann auf **Scan to FTP/Netzwerk**.
- 2 Sie können wählen, welche Profilnummer (1 bis 10) Sie für die Scan-to-FTP-Einstellungen verwenden möchten.
Sie können auch zwei eigene Dateinamen unter **Benutzerdefinierten Dateinamen erstellen** speichern, die neben den sieben vorprogrammierten Dateinamen für das Erstellen von FTP-Serverprofilen verwendet werden können. In jedes der beiden Felder können bis zu 15 Zeichen eingegeben werden.
- 3 Klicken Sie auf **Senden**.

- 4 Klicken Sie auf **Scan-to-FTP/Netzwerk-Profil** auf der Seite **Scannen**.
Sie können nun die folgenden Scan-to-FTP-Einstellungen über einen Webbrowser konfigurieren und ändern:

- **Profilname** (Bis zu 15 Zeichen)
- **Host-Adresse** (FTP-Serveradresse)
- **Benutzername**
- **Kennwort**
- **Zielordner**
- **Dateiname**
- **Qualität**
- **Dateityp**
- **Scangröße Vorlagenglas**
- **Dateigröße**
- **Hintergrundfarbe entfernen**
- **Passiv-Modus**
- **Port-Nummer**

Je nach Ihrem FTP-Server und Ihrer Firewall-Konfiguration im Netzwerk können Sie **Passiv-Modus** auf **Aus** oder **Ein** setzen. Die Standardeinstellung ist **Ein**. Sie können auch die Portnummer für den Zugriff auf den FTP-Server ändern. Standardmäßig ist für diese Einstellung Port 21 gewählt. In den meisten Fällen können diese zwei Einstellungen als Standardeinstellung beibehalten werden.

HINWEIS

Die Scan-to-FTP-Funktion ist verfügbar, wenn über das Web Based Management FTP-Serverprofile konfiguriert wurden.

- 5 Klicken Sie auf **Senden**.

Ändern der Konfiguration für Scan-to-Netzwerk mit einem Webbrowser (Windows®)

Mit der Scan-to-Netzwerk-Funktion können Sie Dokumente einscannen und direkt in einem freigegebenen Ordner auf einem CIFS-Server¹ in Ihrem lokalen Netzwerk oder im Internet speichern:

➤➤ Software-Handbuch für weitere Einzelheiten zur Scan-to-Netzwerk-Funktion.

¹ Common Internet File System (CIFS) ist das Standardverfahren, das Computernutzer zur gemeinsamen Verwendung von Dateien und Druckern unter Windows® verwenden.

HINWEIS

Scan to Network (SMB) unterstützt die Kerberos-Authentifizierung und die NTLMv2-Authentifizierung.

Zur Authentifizierung müssen Sie das SNTP-Protokoll (Netzwerk-Zeitserver) konfigurieren oder das Datum, die Uhrzeit und die Zeitzone über das Funktionstastenfeld korrekt einstellen. (Informationen zur SNTP-Konfiguration finden Sie unter *Synchronisieren mit SNTP-Server* ➤➤ Seite 64. Informationen zum Einstellen von Datum, Uhrzeit und Zeitzone: ➤➤ Installationsanleitung.)

- 1 Klicken Sie auf der Webseite Ihres Gerätes auf **Scannen** und dann auf **Scan to FTP/Netzwerk**.
- 2 Wählen Sie in den Profilnummern (1 bis 10), die Sie für die Einstellungen für „Scan to Netzwerk“ verwenden möchten, die Option **Netzwerk**.
Sie können auch zwei benutzerdefinierte Dateinamen unter **Benutzerdefinierten Dateinamen erstellen** speichern, die neben den sieben vorprogrammierten Dateinamen für das Erstellen von Scan-to-Netzwerk-Profilen verwendet werden können. In jedes der beiden Felder können bis zu 15 Zeichen eingegeben werden.
- 3 Klicken Sie auf **Senden**.

- 4 Klicken Sie auf **Scan-to-FTP/Netzwerk-Profil** auf der Seite **Scannen**.
Sie können nun die folgenden Scan-to-Netzwerk-Einstellungen über einen Webbrowser konfigurieren und ändern:

- **Profilname** (Bis zu 15 Zeichen)
- **Host-Adresse**
- **Zielordner**
- **Dateiname**
- **Qualität**
- **Dateityp**
- **Scangröße Vorlagenglas**
- **Dateigröße**
- **Hintergrundfarbe entfernen**
- **PIN zur Authentifizierung verwenden**
- **PIN-Code**
- **Authentifizierungsmethode**
- **Benutzername**
- **Kennwort**
- **Kerberos-Serveradresse**

HINWEIS

Die Funktion Scan to Netzwerk (SMB) steht zur Verfügung, wenn Netzwerk-Serverprofile über das Web Based Management konfiguriert wurden.

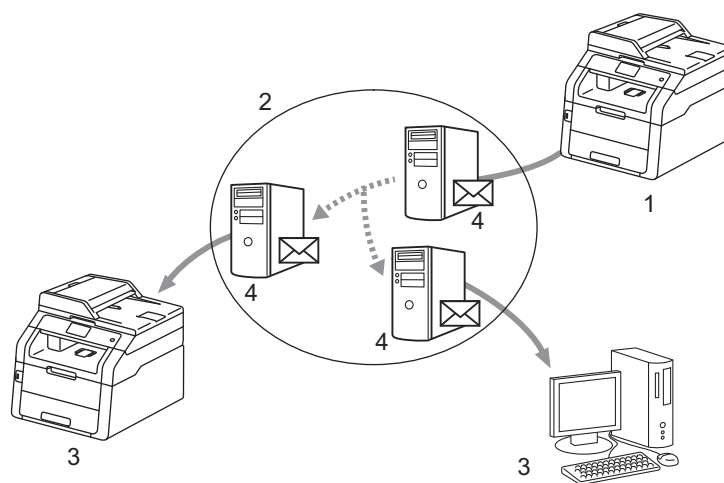
- 5 Klicken Sie auf **Senden**.

Internet-Faxfunktion (MFC-9130CW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW: als Download verfügbar)

Übersicht über die Internet-Faxfunktion

Mit der Internet-Faxfunktion (IFAX) können Sie Faxe über das Internet versenden und empfangen. Die Dokumente werden in E-Mail-Nachrichten als angehängte TIFF-F-Dateien übertragen. Das bedeutet, dass Sie auch mit dem Computer Dokumente empfangen und senden können, sofern der Computer über eine Anwendung verfügt, mit der TIFF--F-Dateien erstellt und angezeigt werden können. Sie können jede beliebige Anwendung zum Anzeigen von TIFF-F-Dateien verwenden. Alle über das Gerät gesendeten Dokumente werden automatisch in ein TIFF-F-Format konvertiert. Wenn Sie Nachrichten von Ihrem Gerät senden und über Ihr Gerät empfangen möchten, muss die Mail-Anwendung Ihres Computers das MIME-Format unterstützen.

Zur Verwendung dieser Funktion laden Sie bitte die erforderliche Firmware von der Seite „Downloads“ für Ihr Modell vom Brother Solutions Center herunter unter <http://solutions.brother.com/>.



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

HINWEIS

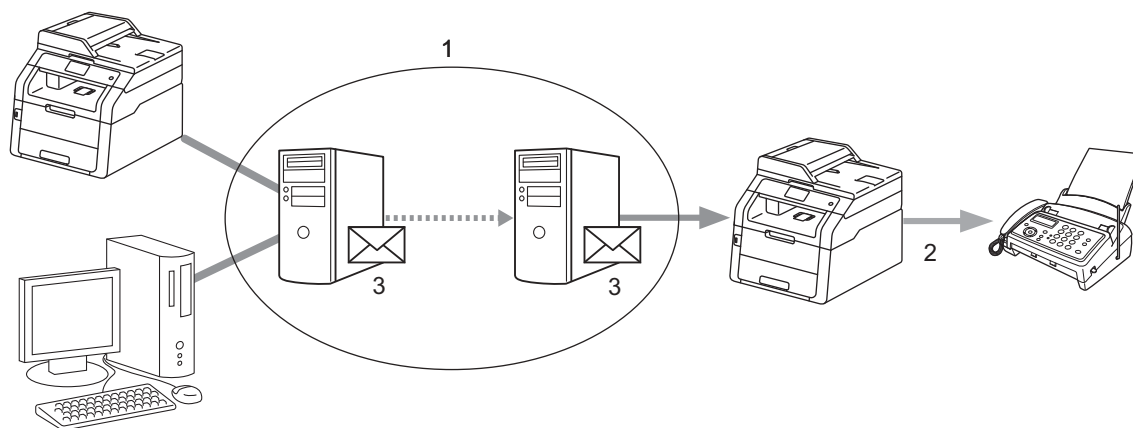
Internet-Faxdokumente sind nur in schwarzweiß verfügbar.

■ Empfangene E-Mail- und Faxnachrichten weiterleiten

Sie können empfangene E-Mail- oder Standard-Faxnachrichten an eine andere E-Mail-Adresse oder an ein anderes Faxgerät weiterleiten. Weitere Informationen finden Sie unter *Empfangene E-Mail- und Faxnachrichten weiterleiten* >> Seite 80.

■ Kettenrundsenden

Wenn Sie das Dokument an einen weit entfernten Empfänger (etwa im Ausland) faxen möchten, können Sie über die „Kettenrundsende“-Funktion Verbindungsgebühren sparen. Mit dieser Funktion kann das Brother-Gerät ein Dokument über das Internet empfangen und anschließend über die normale Telefonleitung an andere Faxgeräte weiterleiten. Weitere Informationen finden Sie unter *Kettenrundsenden* >> Seite 80.



1 Internet

2 Telefonleitung

3 E-Mail-Server

Wichtige Informationen zur Internet-Faxfunktion

Die Internet-Faxkommunikation über ein LAN-System ist im Grunde identisch zur Kommunikation über E-Mail; sie unterscheidet sich allerdings von der Faxkommunikation über die Standardtelefonleitung. Folgende Informationen sind zur Verwendung der Internet-Faxfunktion zu beachten:

- Faktoren, wie der Standort des Empfängers, die Struktur des LAN-Systems und die Auslastung des Schaltkreises (etwa im Internet), können zu Verzögerungen des Systems führen. (in der Regel 20 bis 30 Sekunden)
- Hinsichtlich der Übertragung über das Internet empfehlen wir aufgrund der niedrigen Sicherheitsstufen, vertrauliche Dokumente über Standardtelefonleitungen zu senden.
- Wenn das Mail-System des Empfängers nicht mit dem MIME-Format kompatibel ist, können Sie keine Dokumente an den Empfänger übertragen. Je nach dem Server des Empfängers kann es in einigen Fällen dazu kommen, dass keine Fehler-Mails zurückgesendet werden.
- Wenn die Bilddaten eines Dokuments zu umfangreich sind, kann die Übertragung möglicherweise fehlschlagen.
- Sie können die Schrift oder Zeichengröße der empfangenen Internet-Mail nicht ändern.

So verwenden Sie die Internet-Faxfunktion

Vor der Verwendung der Internet-Faxfunktion müssen Sie Ihr Brother-Gerät für die Kommunikation mit Ihrem Netzwerk und Mail-Server konfigurieren. Sie können diese Informationen über das Funktionstastenfeld, Web Based Management, Remote Setup oder BRAdmin Professional 3 konfigurieren. Folgendes muss für Ihr Gerät verfügbar sein:

- IP-Adresse (Wenn Sie Ihr Gerät bereits im Netzwerk verwenden, wurde die IP-Adresse des Gerätes korrekt konfiguriert.)
- E-Mail-Adresse
- SMTP-, POP3-Serveradresse/Port/Authentifizierungsmethode/Verschlüsselungsmethode/Server-Zertifikat-Verifizierung
- Postfach-Name und -Kennwort

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

6

Versenden eines Internet-Faxdokuments

Vor dem Versenden eines Internet-Faxdokuments

Zum Senden von Internet-Faxdokumenten können Sie folgende Informationen über das Funktionstastenfeld, Web Based Management oder Remote Setup konfigurieren.

- Absender Betreff (sofern erforderlich)
- Größenbegrenzung (sofern erforderlich)
- Benachrichtigung (sofern erforderlich) (Weitere Informationen finden Sie unter *Sendebestätigungs-E-Mail* >> Seite 84).

So versenden Sie ein Internet-Faxdokument

Das Versenden eines Internet-Faxdokuments erfolgt wie das Senden eines normalen Faxdokuments (weitere Informationen: >> Benutzerhandbuch - Grundfunktionen: *Fax senden*). Wenn Sie bereits die Adresse des Zielgerätes für das Internet-Fax im Kurzwahlspeicher programmiert haben, können Sie das Internet-Fax senden, indem Sie das Dokument in das Gerät einlegen. Wenn Sie die Auflösung ändern möchten, drücken Sie im Fax-Menü *Faxauflösung*, um die gewünschte Auflösung festzulegen, und wählen Sie eine Kurzwahlnummer (*S-Fein* wird für die Internet-Faxfunktion nicht unterstützt).

HINWEIS

- Wenn Sie die Internet-Faxadresse manuell eingeben möchten, legen Sie das Dokument in das Gerät ein und führen Sie einen der folgenden Schritte aus.
 - Drücken Sie  und dann , um Nummern, Buchstaben oder Sonderzeichen zu wählen. Geben Sie die Adresse ein und drücken Sie dann *Fax Start*.

Weitere Informationen zur manuellen Eingabe der Internet-Faxadresse: >> Benutzerhandbuch - Grundfunktionen.

- Sie können die E-Mail-Adresse über Web Based Management oder Remote Setup registrieren.

Nach dem Scannen des Dokuments wird es automatisch über Ihren SMTP-Server an den Empfänger des Internet-Faxgeräts übertragen. Sie können den Sendevorgang abbrechen, indem Sie während des Scannens  drücken. Nach Abschluss der Übertragung kehrt das Gerät in den Bereitschaftsmodus zurück.

HINWEIS

Manche E-Mail-Server erlauben den Versand umfangreicher E-Mails nicht (Systemadministratoren legen oft eine Obergrenze für die Größe von E-Mails fest). Wenn diese Funktion eingeschaltet ist, zeigt das Gerät *Speicher voll* an, wenn versucht wird, E-Mails, die größer als 1 MB sind, zu versenden. Das Dokument wird nicht gesendet und es wird ein Fehlerbericht ausgedruckt. Teilen Sie das zu sendende Dokument in kleinere Dokumente auf, die der Mailserver dann akzeptiert. (Hinweis: Ein 42 Seiten langes Dokument entsprechend der ITU-T Test Chart #1 ist ungefähr 1 MB groß.)

Empfangen einer E-Mail oder eines Internet-Faxdokuments

Vor dem Empfangen eines Internet-Faxdokuments

Zum Empfangen von Internet-Faxdokumenten sollten Sie folgende Informationen über das Funktionstastenfeld, Web Based Management oder Remote Setup konfigurieren:

- Autom. Abruf (sofern erforderlich)
- Abrufhäufigkeit (sofern erforderlich)
- Kopfzeile (sofern erforderlich)
- Fehler-Mail löschen (sofern erforderlich)
- Benachrichtigung (sofern erforderlich) (Weitere Informationen finden Sie unter *Sendebestätigungs-E-Mail* >> Seite 84).

So empfangen Sie ein Internet-Faxdokument

Für den Empfang von E-Mail-Nachrichten bestehen 2 Möglichkeiten:

- POP3-Empfang in regelmäßigen Abständen
- POP3-Empfang (manuell angefordert)

Für den POP3-Empfang muss das Gerät einen Abruf am E-Mail-Server vornehmen, um die Daten empfangen zu können. Dieser Abruf kann in festgelegten Intervallen erfolgen (Sie können beispielsweise das Gerät so konfigurieren, dass in einem Intervall von 10 Minuten ein Abruf am E-Mail-Server erfolgt) oder Sie können den Serverabruf manuell vornehmen, indem Sie , `Alle Einstell.`, `Netzwerk`, `E-Mail/IFAX` und dann `Manueller POP3-Empfang` drücken.

Wenn Ihr Gerät mit dem Empfang von E-Mail-Daten beginnt, wird dies entsprechend auf dem Touchscreen angezeigt. Auf dem Touchscreen wird beispielsweise `Empfangen gefolgt von XX/XX E-Mail(s)`

angezeigt. Wenn Sie , `Alle Einstell.`, `Netzwerk`, `E-Mail/IFAX`, und dann `Manueller POP3-Empfang` drücken, um den Abruf von E-Mail-Daten am E-Mail-Server manuell vorzunehmen, und keine Mail-Dokumente zum Drucken bereitstehen, zeigt der Touchscreen des Gerätes zwei Sekunden lang `Keine Mail(s) an`.

6

HINWEIS

- Wenn beim Empfang von Daten kein Papier mehr im Gerät eingelegt ist, werden die empfangenen Daten im Gerätespeicher gespeichert. Diese Daten werden automatisch gedruckt, wenn wieder Papier in das Gerät geladen wird.
- Wenn die empfangene Mail nicht in reinem Textformat oder eine angehängte Datei nicht im TIFF-F-Format vorliegt, wird folgende Fehlermeldung gedruckt: **„DAS FORMAT DER ANGEHÄNGTEN DATEI WIRD NICHT UNTERSTÜTZT. DATEINAME:XXXXXX.doc“**. Wenn die empfangene Mail zu groß ist, wird folgende Fehlermeldung gedruckt: **„DIE E-MAIL IST ZU GROSS.“**. Wenn die Option zum Löschen von Fehler-Mails für den POP-Empfang aktiviert ist (Standard), wird die Fehler-Mail automatisch vom E-Mail-Server gelöscht.

Empfangen eines Internet-Faxdokuments auf Ihrem Computer

Wenn ein Computer ein Internet-Faxdokument empfängt, wird das Dokument an eine E-Mail-Nachricht angehängt, die den Computer darüber informiert, dass ein Dokument von einem Internet-Fax empfangen wurde. Diese Benachrichtigung erscheint im Betreffsfeld der empfangenen E-Mail-Nachricht.

HINWEIS

Wenn auf dem Computer, an den Sie ein Dokument senden möchten, nicht Windows® XP, Windows Server® 2003/2008/2012, Windows Vista®, Windows® 7 oder Windows® 8 ausgeführt wird, informieren Sie den Besitzer des Computers darüber, dass eventuell eine Anwendung zum Anzeigen von TIFF-F-Dateien installiert werden muss.

Zusätzliche Optionen für die Internetfax-Funktion

Empfangene E-Mail- und Faxnachrichten weiterleiten

Sie können empfangene E-Mail- oder Standard-Faxnachrichten an eine andere E-Mail-Adresse oder an ein anderes Faxgerät weiterleiten. Empfangene Nachrichten können per E-Mail an einen Computer oder ein Internet-Faxgerät weitergeleitet werden. Sie können auch über eine Standardtelefonleitung an ein anderes Gerät weitergeleitet werden.

Die Einstellung kann über einen Webbrowser oder über das Funktionstastenfeld des Gerätes aktiviert werden. Informationen zu den Schritten zur Konfiguration der Faxweiterleitung finden Sie im Benutzerhandbuch - Erweiterte Funktionen, sofern von Ihrem Gerät unterstützt.

Kettenrundsenden

Mit dieser Funktion kann das Brother-Gerät ein Dokument über das Internet empfangen und anschließend über die normale Telefonleitung an andere Faxgeräte weiterleiten.

Vor dem Kettenrundsenden

Zum Kettenrundsenden müssen Sie folgende Informationen über das Funktionstastenfeld, Web Based Management oder Remote Setup konfigurieren:

- Kettenrundsenden

Sie müssen die Kettenrundsende-Funktion aktivieren.

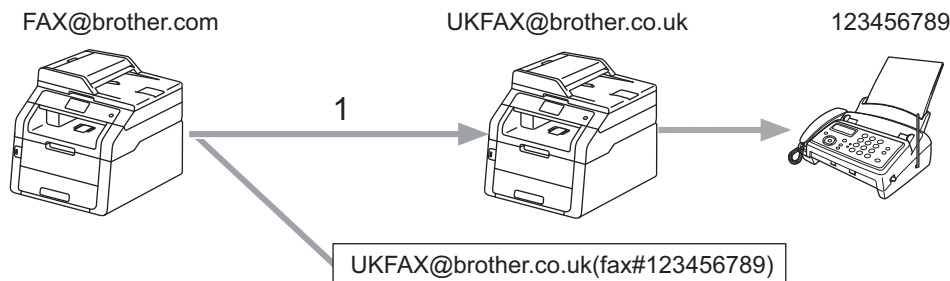
- Relaydomäne

Sie müssen den Domänennamen für Ihr Gerät konfigurieren, das das Dokument an ein herkömmliches Faxgerät über die Kettenrundsende-Funktion sendet. Wenn Sie Ihr Gerät als Kettenrundsende-Gerät verwenden möchten, müssen Sie den vertrauenswürdigen Domänennamen auf dem Gerät angeben, also den Teil des Namens nach dem „@“-Zeichen. Sie müssen darauf achten, eine vertrauenswürdige Domäne auszuwählen, da alle Benutzer in einer vertrauenswürdigen Domäne die Kettenrundsende-Funktion verwenden können.

Sie können bis zu 10 Domänennamen registrieren.

- Relaybericht

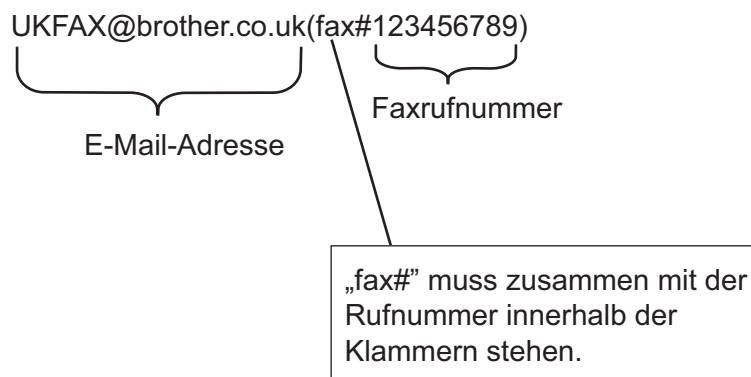
Kettenrundsenden von einem Gerät



1 Internet

In diesem Beispiel verfügt Ihr Gerät über die E-Mail-Adresse `FAX@brother.com` und Sie möchten ein Dokument von diesem Gerät an ein anderes Gerät in England senden, dessen E-Mail-Adresse `UKFAX@brother.co.uk` lautet. Dieses Gerät leitet dann das Dokument an ein Standardfaxgerät über eine herkömmliche Telefonleitung weiter. Wenn Ihre E-Mail-Adresse `FAX@brother.com` lautet, müssen Sie den vertrauenswürdigen Domännennamen `brother.com` auf dem Gerät in England konfigurieren, der das Dokument an das herkömmliche Faxgerät weiterleitet. Wenn Sie die Informationen für den Domännennamen nicht eingeben, vertraut das Gerät in der Mitte (das Gerät, das das Dokument weiterleiten soll) keinen Internetaufträgen, die es von dem Gerät aus der Domäne `@brother.com` erhält.

Nach dem Festlegen der vertrauenswürdigen Domäne können Sie das Dokument über Ihr Gerät [z. B. `FAX@brother.com`] senden, indem Sie die E-Mail-Adresse des Geräts [z. B. `UKFAX@brother.co.uk`] eingeben, das das Dokument weiterleitet, gefolgt von der Telefonnummer des Faxgerätes, das das Dokument empfangen soll. Das nachfolgende Beispiel stellt dar, wie die E-Mail-Adresse und die Telefonnummer eingegeben werden können.

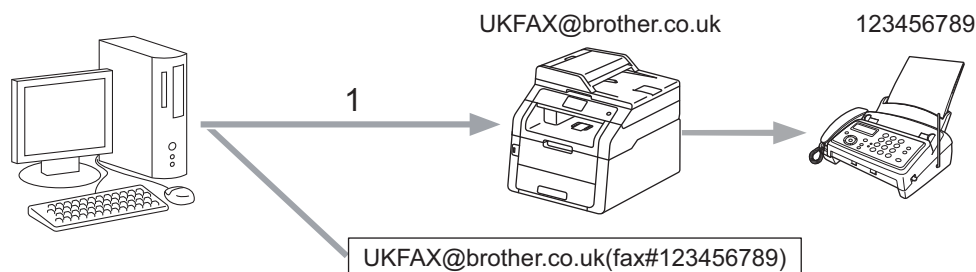


Versenden an mehrere Telefonnummern:

Wenn das Dokument über die Kettenrundsende-Funktion an mehr als ein Standardfaxgerät gesendet werden soll, kann die Adresse wie folgt eingegeben werden:

- 1 Drücken Sie **Fax**.
- 2 Legen Sie das Dokument ein.
- 3 Drücken Sie **Optionen**.
- 4 Navigieren Sie nach oben oder unten oder drücken Sie **▲** oder **▼**, um **Rundsenden** anzuzeigen. Drücken Sie **Rundsenden**.
- 5 Drücken Sie **Nummer hinzuf.**
- 6 Sie haben folgende Möglichkeiten, um E-Mail-Adressen zum Kettenrundsenden hinzuzufügen:
 - Drücken Sie **Nummer hinzuf.** und drücken Sie , geben Sie die E-Mail-Adresse ein und drücken Sie **OK**.
 - Drücken Sie **Aus Adressbuch hinzufügen**.
Drücken Sie auf die Kontrollkästchen der E-Mail-Adresse, die zum Kettenrundsenden hinzugefügt werden soll.
Nachdem Sie alle gewünschten E-Mail-Adressen ausgewählt haben, drücken Sie **OK**.
 - Drücken Sie **Suche in Adressbuch**.
Geben Sie den Namen ein und drücken Sie **OK**.
Die Suchergebnisse werden angezeigt. Drücken Sie auf den Namen und dann auf die E-Mail-Adresse, die zum Kettenrundsenden hinzugefügt werden soll.
- 7 Nachdem Sie alle gewünschten E-Mail-Adressen durch Wiederholung von Schritt 6 eingegeben haben, drücken Sie **OK**.
- 8 Drücken Sie **Fax Start**.

Kettenrundsenden von einem Computer



1 Internet

Sie können auch eine E-Mail über Ihren Computer versenden und diese über die Kettenrundsende-Funktion an ein herkömmliches Faxgerät weiterleiten lassen. Die Eingabemethode für die Telefonnummer eines herkömmlichen Faxgerätes, das die Kettenrundsende-E-Mail empfangen soll, variiert je nach der verwendeten E-Mail-Anwendung. Nachfolgend finden Sie einige Beispiele für unterschiedliche E-Mail-Anwendungen:

Einige E-Mail-Anwendungen unterstützen keinen Sendevorgang an mehrere Telefonnummern. Wenn Ihre E-Mail-Anwendung keine Unterstützung für mehrere Telefonnummern bietet, können Sie die Kettenrundsende-Funktion immer nur für ein Faxgerät verwenden.

Geben Sie die Adresse des Kettenrundsende-Gerätes und die Telefonnummer des Faxgerätes in das Feld „An“ ein. Geben Sie dabei dieselben Informationen ein, wie beim Senden über ein Faxgerät.

`UKFAX@brother.co.uk(fax#123456789)`

HINWEIS

Für Microsoft® Outlook® 97 oder höher muss die Adresse wie folgt in das Adressbuch eingegeben werden:

Name: `fax#123456789`

E-Mail-Adresse: `UKFAX@brother.co.uk`

Sendebestätigungs-E-Mail

Die Bestätigungs-E-Mail für die Übertragung unterstützt zwei verschiedene Funktionen. Eine Sendebestätigungs-E-Mail ermöglicht Ihnen eine Abfrage von der Empfangsstation, um zu bestätigen, dass das Internet-Fax oder die E-Mail empfangen und verarbeitet wurde. Eine Empfangsbestätigungs-E-Mail ermöglicht Ihnen die Übertragung eines Standardberichts zurück an die Sendestation, nachdem Sie ein Internet-Fax oder eine E-Mail erfolgreich empfangen und verarbeitet haben.

Zur Verwendung dieser Funktion muss die Option **Bestätigung** zusammen mit den Optionen **Mail (Empfang)** und **Mail (Senden)** aktiviert werden.

Einrichtung „Mail (Senden)“

Sie können die Option **Bestätigung** für **Mail (Senden)** entweder auf **Ein** oder **Aus** setzen. Wenn die Option auf **Ein** gesetzt ist, wird ein zusätzliches Informationsfeld mit den Bilddaten gesendet. Dieses Feld wird als „MDN“ bezeichnet.

MDN (Message Disposition Notification):

Dieses Feld fragt den Status der Internet-Fax-/E-Mail-Nachricht ab, nachdem diese durch das SMTP-Übertragungssystem (Simple Mail Transfer Protocol) gesendet wurde. Sobald die Nachricht den Empfänger erreicht hat, werden diese Daten verwendet, wenn das Gerät oder der Benutzer die empfangene Internet-Faxnachricht oder E-Mail-Nachricht liest oder druckt. Wenn die Nachricht beispielsweise zum Lesen oder Drucken geöffnet wird, sendet der Empfänger eine Benachrichtigung zurück an das Gerät oder den Benutzer, das bzw. der die Nachricht ursprünglich gesendet hat.

Der Empfänger muss das MDN-Feld unterstützen, um einen Benachrichtigungsbericht senden zu können, andernfalls wird die Anforderung ignoriert.

Einrichtung „Mail (Empfang)“

Für diese Option sind drei Einstellungen möglich: **Ein**, **MDN** oder **Aus**.

Empfangsbenachrichtigung „Ein“

Wenn diese Einstellung auf „Ein“ gesetzt ist, wird eine fest definierte Nachricht zurück an den Absender gesendet, um anzugeben, dass die Nachricht erfolgreich empfangen und verarbeitet wurde. Diese fest definierten Nachrichten richten sich nach der vom Absender angeforderten Funktion.

Berichtsnachrichten enthalten:

Übertragung erfolgreich: Empfang von <E-Mail-Adresse>

Empfangsbenachrichtigung „MDN“

Wenn diese Funktion auf „MDN“ gesetzt ist, wird der oben beschriebene Bericht zurück an den Absender gesendet, sofern die ursprüngliche Sendestation das Feld „MDN“ zur Bestätigungsanforderung gesendet hat.

Empfangsbenachrichtigung „Aus“

Wenn diese Option deaktiviert ist, werden alle Empfangsbenachrichtigungen auf **Aus** gesetzt und es wird unabhängig von der Anforderung keine Nachricht zurück an den Absender gesendet.

HINWEIS

Um die Sendebestätigungs-E-Mail korrekt empfangen zu können, müssen Sie folgende Einstellungen konfigurieren.

- Sender
 - Aktivieren Sie die Benachrichtigung für „Mail (Senden)“.
 - Setzen Sie die Kopfzeile für „Mail (Senden)“ auf „Alle“ oder „Betreff+Von+An“.
 - Empfänger
 - Aktivieren Sie die Benachrichtigung für „Mail (Empfang)“.
-

Fehler-Mail

Wenn beim Senden eines Internet-Faxdokuments ein Mail-Sendefehler auftritt, sendet der Mail-Server eine Fehlermeldung zurück an das Gerät und die Fehlermeldung wird ausgedruckt. Wenn beim Mail-Empfang ein Fehler auftritt, wird eine Fehlermeldung ausgedruckt (Beispiel: „Die an das Gerät gesendete Nachricht lag nicht im TIFF-F-Format vor.“).

Um die Fehler-Mail korrekt empfangen zu können, müssen Sie die Kopfzeile für „Mail (Senden)“ auf „Alle“ oder „Betreff+Von+An“ setzen.

Übersicht

Heutzutage sind Netzwerke und die Daten, die darin übertragen werden, vielen Sicherheitsrisiken ausgesetzt. Ihr 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. In diesem Kapitel wird erklärt, wie diese Funktionen konfiguriert werden können.

Sie können die folgenden Sicherheitsfunktionen konfigurieren:

- Netzwerkgerät mit SSL/TLS sicher verwalten (Siehe *Netzwerkgerät mit SSL/TLS sicher verwalten* >> Seite 100.)
- Netzwerkgerät mit dem SNMPv3-Protokoll sicher verwalten (Siehe *Sichere Verwaltung mit Web Based Management (Webbrowser)* >> Seite 100 oder *Sichere Verwaltung mit BRAdmin Professional 3 (Windows®)* >> Seite 103.)
- Sichere Verwaltung mit BRAdmin Professional 3 (für Windows®) (Siehe *Sichere Verwaltung mit BRAdmin Professional 3 (Windows®)* >> Seite 103.)
- Sicherer Druck von Dokumenten mit SSL/TLS (Siehe *Sicherer Druck von Dokumenten mit SSL/TLS* >> Seite 104.)
- Eine E-Mail sicher senden und empfangen (Siehe *Sicheres Versenden oder Empfangen einer E-Mail* >> Seite 105.)
- IEEE 802.1x-Authentifizierung verwenden (Siehe *Verwenden der IEEE 802.1x-Authentifizierung* >> Seite 108.)
- Zertifikate für die sichere Verwaltung (Siehe *Verwenden von Zertifikaten zur Gerätesicherheit* >> Seite 87.)
- Mehrere Zertifikate verwalten (Siehe *Mehrere Zertifikate verwalten* >> Seite 99.)

HINWEIS

Wir empfehlen, das Telnet-, FTP- und das TFTP-Protokoll zu deaktivieren. Der Zugriff auf das Gerät mit diesen Protokollen ist nicht sicher. (Informationen zur Konfiguration der Protokolleinstellungen finden Sie unter *So konfigurieren Sie die Geräteeinstellungen über Web Based Management (Webbrowser)* >> Seite 58.) Wenn Sie FTP deaktivieren, wird die Scan-to-FTP-Funktion deaktiviert.

Verwenden von Zertifikaten zur Gerätesicherheit

Ihr Brother-Gerät unterstützt verschiedene Sicherheitszertifikate, um eine sichere Verwaltung, Authentifizierung und Kommunikation mit dem Gerät zu ermöglichen. Die folgenden Sicherheitsfunktionen können mit dem Gerät verwendet werden.

- SSL/TLS-Kommunikation
- IEEE 802.1x-Authentifizierung
- SSL-Kommunikation für SMTP/POP3

Das Brother-Gerät unterstützt die folgenden Zertifikate.

- Vorinstalliertes Zertifikat

Ihr Gerät verfügt über ein vorinstalliertes selbstsigniertes Zertifikat.

Mit diesem Zertifikat können Sie problemlos die SSL/TLS-Kommunikation nutzen, ohne ein Zertifikat erstellen oder installieren zu müssen.

HINWEIS

Das vorinstallierte selbstsignierte Zertifikat kann Ihre Kommunikation nicht gegen Spoofing schützen. Wir empfehlen für eine höhere Sicherheit die Verwendung eines Zertifikats, das durch eine vertrauenswürdige Organisation ausgestellt wird.

- Privates Zertifikat

Dieser MFC/DCP-Server stellt sein eigenes Zertifikat aus. Mit diesem Zertifikat können Sie problemlos die SSL/TLS-Kommunikation nutzen, ohne ein Zertifikat von einer Zertifizierungsstelle zu haben. (Siehe *Erstellen und Installieren eines Zertifikats* ►► Seite 90.)

- Zertifikat einer Zertifizierungsstelle (CA)

Es stehen zwei Verfahren zur Verfügung, mit denen ein Zertifikat von einer Zertifizierungsstelle installiert werden kann. Wenn Sie bereits ein Zertifikat von einer Zertifizierungsstelle haben oder ein Zertifikat von einer externen vertrauenswürdigen Zertifizierungsstelle verwenden möchten:

- Installation mit einer Zertifikatsignieranforderung (CSR; Certificate Signing Request) von diesem MFC/DCP-Server. (Siehe *So erstellen Sie eine CSR* ►► Seite 91.)
- Installation mit Import eines Zertifikates und eines privaten Schlüssels (Private Key). (Siehe *Importieren und Exportieren des Zertifikats und des privaten Schlüssels (Private Key)* ►► Seite 98.)

■ CA-Zertifikat

Wenn Sie ein CA-Zertifikat verwenden, das die Zertifizierungsstelle (CA - Certificate Authority) selbst identifiziert und einen eigenen privaten Schlüssel hat, müssen Sie vor der Konfiguration ein CA-Zertifikat von der Zertifizierungsstelle importieren. (Siehe *Importieren und Exportieren eines CA-Zertifikats* >> Seite 99.)

HINWEIS

- Wenn Sie die SSL/TLS-Kommunikation verwenden möchten, sollten Sie sich zuerst an Ihren Systemadministrator wenden.
 - Wenn Sie den MFC/DCP-Server auf die werkseitigen Standardeinstellungen zurücksetzen, wird das installierte Zertifikat einschließlich des privaten Schlüssels (Private Key) gelöscht. Wenn Sie nach dem Zurücksetzen des MFC/DCP-Servers dasselbe Zertifikat und denselben privaten Schlüssel (Private Key) verwenden möchten, sollten Sie diese vor dem Zurücksetzen exportieren und danach erneut installieren. (Siehe *So exportieren Sie das selbstsignierte Zertifikat, das CA-Zertifikat und den privaten Schlüssel* >> Seite 98.)
-

Konfigurieren eines Zertifikats mit Web Based Management

Diese Funktion kann nur über das Web Based Management konfiguriert werden. Gehen Sie wie folgt vor, um über das Web Based Management auf die Seite zum Konfigurieren des Zertifikates zu gelangen.

- 1 Starten Sie Ihren Webbrowser.
- 2 Geben Sie in die Adressleiste Ihres Browsers „http://IP-Adresse des Gerätes/“ ein (wobei „IP-Adresse des Gerätes“ für die IP-Adresse des Gerätes oder den Namen des PrintServers steht).
 - Zum Beispiel: http://192.168.1.2/
- 3 Standardmäßig ist kein Kennwort erforderlich. Wenn Sie zuvor ein Kennwort festgelegt haben, geben Sie dieses ein, und drücken Sie auf .
- 4 Klicken Sie auf **Netzwerk**.
- 5 Klicken Sie auf **Sicherheit**.
- 6 Klicken Sie auf **Zertifikat**.
- 7 Nun können Sie die Zertifikateinstellungen im unten gezeigten Bildschirm vornehmen.

Zertifikat



Zertifikatliste

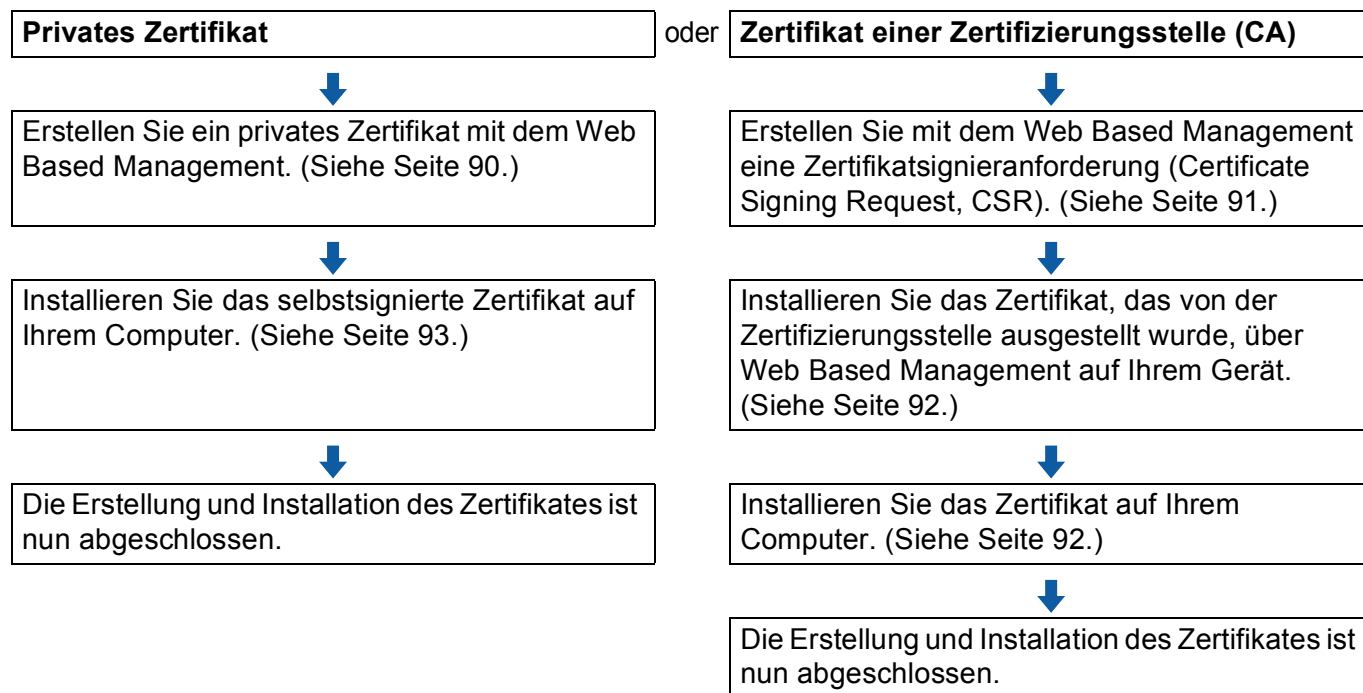
Zertifikatname	Herausgeber	Gültigkeitsdauer(*:Abgelaufen)
Privates Zertifikat erstellen>>		
Zertifikatsignieranforderung (CSR) erstellen>>		
Zertifikat installieren		
Zertifikat und Private Key importieren>>		

HINWEIS

- Funktionen, die grau markiert und nicht verlinkt sind, stehen nicht zur Verfügung.
- Weitere Informationen zur Konfiguration finden Sie in der Hilfe des Web Based Managements.

Erstellen und Installieren eines Zertifikats

Schrittweise Darstellung der Erstellung und Installation eines Zertifikates



7

So erstellen und installieren Sie ein selbstsigniertes Zertifikat

- 1 Klicken Sie auf **Privates Zertifikat erstellen** auf der Seite **Zertifikat**.
- 2 Füllen Sie die Felder **Allgemeine Name** und **Gültigkeitsdauer** aus.

HINWEIS

- Der **Allgemeine Name** darf nicht länger als 64 Zeichen sein. Geben Sie eine Kennung ein, zum Beispiel IP-Adresse, Knotenname oder Domänenname, die beim Zugriff auf dieses Gerät über die SSL/TLS-Kommunikation verwendet wird. Standardmäßig wird der Knotenname angezeigt.
 - Es erscheint eine Warnung, wenn Sie das IPPS- oder HTTPS-Protokoll verwenden und in die URL einen anderen Namen eingeben, als den der unter **Allgemeine Name** für das Zertifikat benutzt wurde.
-
- 3 Sie können die Einstellungen **Algorithmus des öffentlichen Schlüssels** und **Digest-Algorithmus** aus der Dropdown-Liste wählen. Die Standardeinstellungen sind **RSA(2048bit)** für **Algorithmus des öffentlichen Schlüssels** und **SHA256** für **Digest-Algorithmus**.
 - 4 Klicken Sie auf **Senden**.

- 5 Das private Zertifikat ist nun erstellt und erfolgreich in Ihrem Gerät gespeichert. Zur Verwendung der SSL/TLS-Kommunikation muss das private Zertifikat auch auf Ihrem Computer installiert werden. Weitere Informationen finden Sie unter *So installieren Sie das selbstsignierte Zertifikat auf Ihrem Computer* >> Seite 93.

So erstellen Sie eine CSR

- 1 Klicken Sie auf **Zertifikatsignieranforderung (CSR) erstellen** auf der Seite **Zertifikat**.
- 2 Füllen Sie das Feld **Allgemeine Name** aus und geben Sie Ihre Informationen, wie die **Organisation** ein.

HINWEIS

- Es wird empfohlen, das Stammzertifikat von der Zertifizierungsstelle auf Ihrem Computer zu installieren, bevor Sie eine Zertifikatsignieranforderung erstellen.
 - Der **Allgemeine Name** darf nicht länger als 64 Zeichen sein. Geben Sie eine Kennung ein, zum Beispiel IP-Adresse, Knotenname oder Domänenname, die beim Zugriff auf diesen Drucker über die SSL/TLS-Kommunikation verwendet wird. Standardmäßig wird der Knotenname angezeigt. Der **Allgemeine Name** muss angegeben werden.
 - Es erscheint eine Warnung, wenn Sie einen anderen Namen in die URL eingeben, als den allgemeinen Namen, der für das Zertifikat benutzt wurde.
 - Die Länge von **Organisation**, **Organisationseinheit**, **Ort** und **Bundesland** darf nicht länger als 64 Zeichen sein.
 - Für **Land** sollte ein Ländercode nach ISO 3166 (2 Zeichen) eingegeben werden.
 - Wenn Sie eine X.509v3 -Zertifikaterweiterung konfigurieren, aktivieren Sie das Kontrollkästchen **Erweiterte Partition konfigurieren** und wählen Sie dann **Auto (IPv4 registrieren)** oder **Manuell**.
-
- 3 Sie können die Einstellungen **Algorithmus des öffentlichen Schlüssels** und **Digest-Algorithmus** aus der Dropdown-Liste wählen. Die Standardeinstellungen sind **RSA(2048bit)** für **Algorithmus des öffentlichen Schlüssels** und **SHA256** für **Digest-Algorithmus**.
 - 4 Klicken Sie auf **Senden**.
 - 5 Wenn der Inhalt der Zertifikatsignieranforderung (CSR) angezeigt wird, klicken Sie auf **Speichern**, um die CSR-Datei auf Ihrem Computer zu speichern.

- 6 Die Zertifikatsignieranforderung ist nun erstellt.

HINWEIS

- Beachten Sie in Bezug auf das Verfahren zum Senden der Zertifikatsignieranforderung an Ihre Zertifizierungsstelle die Richtlinien der Zertifizierungsstelle.
- Wenn Sie die Stammzertifizierungsstelle des Unternehmens (Enterprise Root CA) von Windows Server® 2003/2008/2012 verwenden, empfehlen wir, beim Erstellen des Client-Zertifikates für die sichere Verwaltung den **Webserver** als Zertifikatvorlage zu verwenden. Wenn Sie ein Client-Zertifikat für eine IEEE 802.1x-Umgebung mit EAP-TLS-Authentifizierung erstellen, empfehlen wir, **Benutzer** als Zertifikatvorlage zu verwenden. Weitere Informationen finden Sie auf der SSL-Kommunikationsseite, die Sie über die Hauptseite Ihres Modells unter <http://solutions.brother.com/> aufrufen können.

So installieren Sie das Zertifikat auf Ihrem Gerät

Nachdem Sie das Zertifikat von der Zertifizierungsstelle erhalten haben, installieren Sie es wie folgt auf dem MFC/DCP-Server.

HINWEIS

Es können nur Zertifikate installiert werden, die über die Zertifikatsignieranforderung (CSR) dieses Gerätes ausgestellt wurden. Wenn Sie eine weitere Zertifikatsignieranforderung erstellen möchten, vergewissern Sie sich, dass das Zertifikat installiert wurde, bevor Sie eine weitere Zertifikatsignieranforderung erstellen. Erstellen Sie eine weitere Zertifikatsignieranforderung, nachdem Sie das Zertifikat auf dem Gerät installiert haben; anderenfalls wird die Zertifikatsignieranforderung, die Sie vor der Installation erstellt haben, ungültig.

- 1 Klicken Sie auf **Zertifikat installieren** auf der Seite **Zertifikat**.
- 2 Geben Sie die Datei mit dem von einer Zertifizierungsstelle (CA) ausgestellten Zertifikat an und klicken Sie dann auf **Senden**.
- 3 Das private Zertifikat ist nun erstellt und erfolgreich im Speicher Ihres Gerätes abgelegt. Zur Verwendung der SSL/TLS-Kommunikation muss das Stammzertifikat der Zertifizierungsstelle auch auf Ihrem Computer installiert werden. Wenden Sie sich zur Installation an Ihren Netzwerkadministrator.

Auswählen des Zertifikats

Nachdem Sie das Zertifikat installiert haben, gehen Sie wie unten beschriebenen vor, um das Zertifikat auszuwählen, das Sie verwenden möchten.

- 1 Klicken Sie auf **Netzwerk**.
- 2 Klicken Sie auf **Protokoll**.
- 3 Klicken Sie auf **HTTP-Servereinstellungen** und wählen Sie dann das Zertifikat aus der Dropdown-Liste unter **Wählen Sie das Zertifikat**.

So installieren Sie das selbstsignierte Zertifikat auf Ihrem Computer

HINWEIS

- In den folgenden Schritten wird der Windows® Internet Explorer® verwendet. Falls Sie einen anderen Webbrowser benutzen, folgen Sie der Anleitung in der Hilfe des Browsers.
- Sie müssen über Administratorrechte verfügen, um das selbstsignierte Zertifikat installieren zu können.

Für Benutzer von Windows Vista®, Windows® 7, Windows® 8, Windows Server® 2008 und Windows Server® 2012, die über Administratorrechte verfügen

1 (Windows Vista®/Windows® 7/Windows Server® 2008)

Klicken Sie auf die Schaltfläche  und dann auf **Alle Programme**.

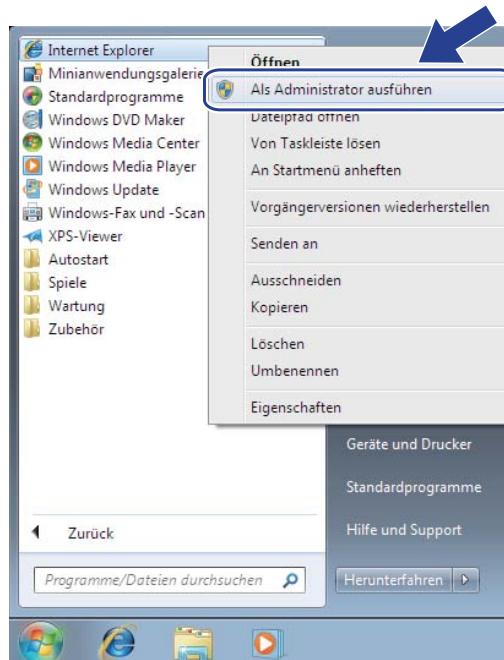
(Windows® 8)

Klicken Sie mit der rechten Maustaste in der Symbolleiste auf das Symbol  (**Internet Explorer**).

(Windows Server® 2012)

Klicken Sie auf  (**Internet Explorer**) und klicken Sie dann mit der rechten Maustaste auf das Symbol  (**Internet Explorer**), das in der Symbolleiste angezeigt wird.

2 Klicken Sie mit der rechten Maustaste auf **Internet Explorer**, und klicken Sie dann auf **Als Administrator ausführen**.



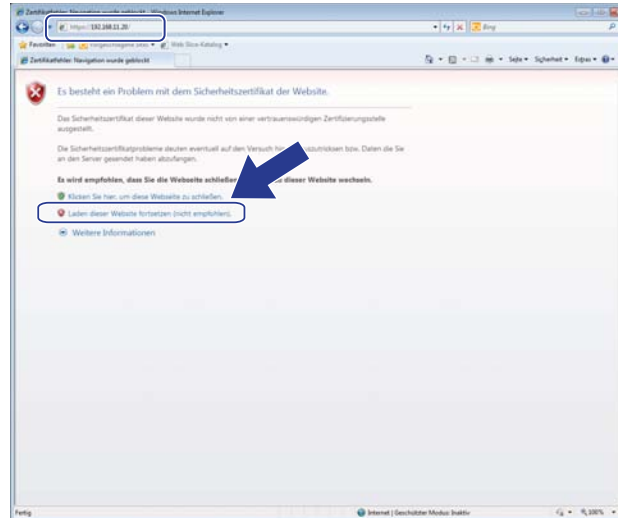
HINWEIS

Wenn das Fenster **Benutzerkontensteuerung** angezeigt wird,

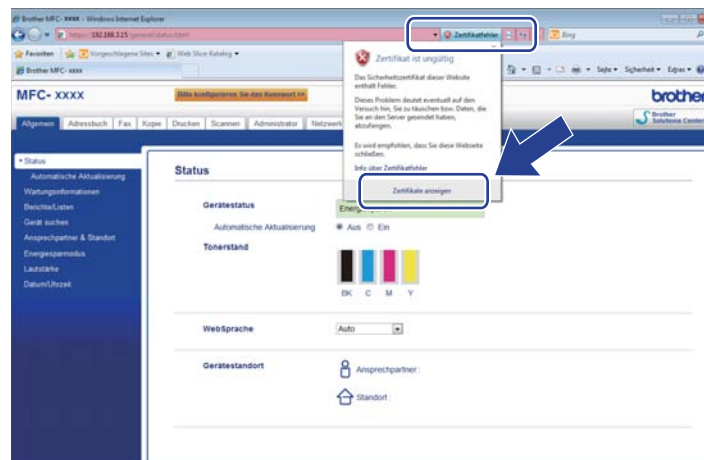
(Windows Vista®) klicken Sie auf **Fortsetzen (Zulassen)**.

(Windows® 7/Windows® 8) klicken Sie auf **Ja**.

- 3 Geben Sie „https://IP-Adresse des Gerätes“ in Ihren Browser ein, um auf das Gerät zuzugreifen (dabei steht „IP-Adresse des Gerätes“ entweder für die IP-Adresse des Gerätes oder für den Knotennamen, den Sie dem Zertifikat zugewiesen haben).
Klicken Sie dann auf **Laden dieser Website fortsetzen (nicht empfohlen)**.

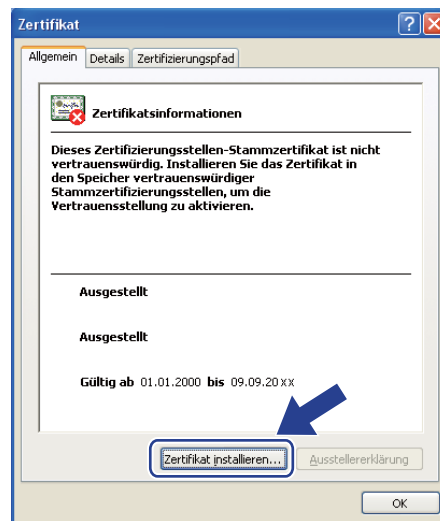


- 4 Klicken Sie auf **Zertifikatfehler** und dann auf **Zertifikate anzeigen**. Fahren Sie mit Schritt 4 unter *Für Benutzer von Windows® XP und Windows Server® 2003* >> Seite 96 fort.

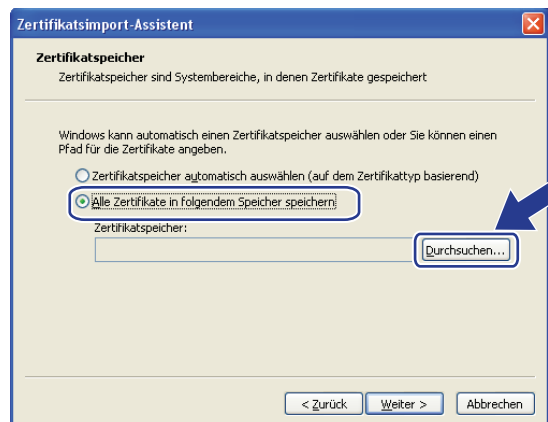


Für Benutzer von Windows® XP und Windows Server® 2003

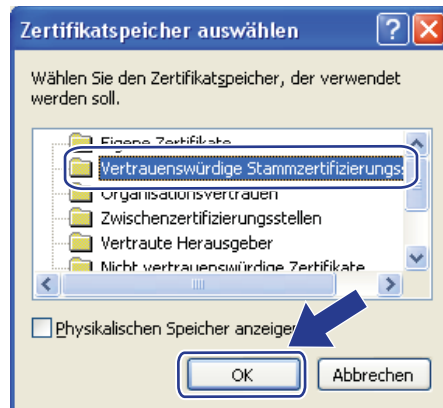
- 1 Starten Sie Ihren Webbrowser.
- 2 Geben Sie „https://IP-Adresse des Gerätes/“ in Ihren Browser ein, um auf das Gerät zuzugreifen (dabei steht „IP-Adresse des Gerätes“ entweder für die IP-Adresse oder für den Knotennamen, den Sie für das Zertifikat zugewiesen haben).
- 3 Wenn das Dialogfeld für Sicherheitswarnungen erscheint, haben Sie folgende Möglichkeiten:
 - Klicken Sie auf **Laden dieser Website fortsetzen (nicht empfohlen)**. Klicken Sie auf **Zertifikatfehler** und dann auf **Zertifikate anzeigen**.
- 4 Klicken Sie auf **Zertifikat installieren...** in der Registerkarte **Allgemein**.



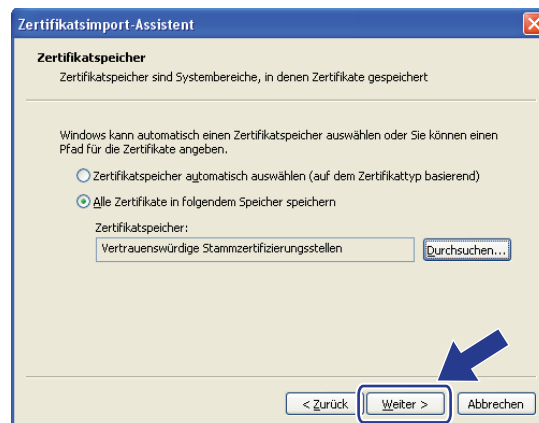
- 5 Wenn der **Zertifikatsimport-Assistent** erscheint, klicken Sie auf **Weiter**.
- 6 Sie müssen angeben, wo das Zertifikat installiert werden soll. Wir empfehlen, **Alle Zertifikate in folgendem Speicher speichern** auszuwählen. Klicken Sie dann auf **Durchsuchen...**.



- 7 Wählen Sie **Vertrauenswürdige Stammzertifizierungsstellen**, und klicken Sie dann auf **OK**.

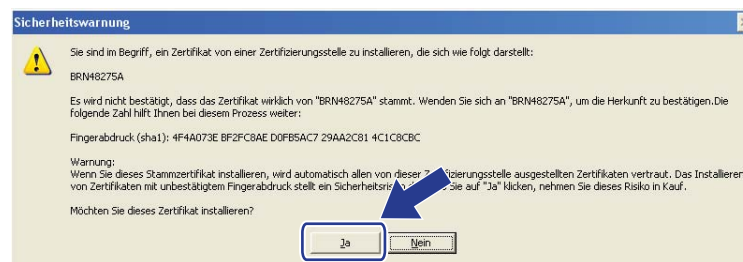


- 8 Klicken Sie auf **Weiter**.



- 9 Klicken Sie auf **Fertig stellen**.

- 10 Klicken Sie auf **Ja**, wenn der Fingerabdruck des Zertifikates korrekt ist.



HINWEIS

Der Fingerabdruck wird im Netzwerk-Konfigurationsbericht gedruckt (siehe *Drucken des Netzwerk-Konfigurationsberichts* ►► Seite 49).

- 11 Klicken Sie auf **OK**.

- 12 Das private Zertifikat ist nun auf Ihrem Computer installiert und die SSL/TLS-Kommunikation ist möglich.

Importieren und Exportieren des Zertifikats und des privaten Schlüssels (Private Key)

Sie können das Zertifikat und den privaten Schlüssel im Gerät speichern und diese durch Import und Export verwalten.

So importieren Sie das selbstsignierte Zertifikat, das CA-Zertifikat und den privaten Schlüssel

- 1 Klicken Sie auf **Zertifikat und Private Key importieren** auf der Seite **Zertifikat**.
- 2 Geben Sie die Datei an, die Sie importieren möchten.
- 3 Geben Sie das Kennwort ein, falls die Datei verschlüsselt ist, und klicken Sie dann auf **Senden**.
- 4 Das Zertifikat und der Private Key wurden nun erfolgreich in Ihr Gerät importiert.
Zur Verwendung der SSL/TLS-Kommunikation muss auch das Stammzertifikat der Zertifizierungsstelle auf Ihrem Computer installiert werden. Wenden Sie sich zur Installation an Ihren Netzwerkadministrator.

So exportieren Sie das selbstsignierte Zertifikat, das CA-Zertifikat und den privaten Schlüssel

- 1 Klicken Sie auf **Exportieren** neben **Zertifikatsliste** auf der Seite **Zertifikat**.
- 2 Geben Sie das Kennwort ein, wenn Sie die Datei verschlüsseln möchten.

HINWEIS

Wenn kein bzw. ein leeres Kennwort verwendet wird, ist die Ausgabe nicht verschlüsselt.

- 3 Geben Sie das Kennwort zur Bestätigung erneut ein und klicken Sie dann auf **Senden**.
- 4 Geben Sie an, wo Sie die Datei speichern wollen.
- 5 Zertifikat und Private Key sind nun erfolgreich zum Computer exportiert worden.

HINWEIS

Sie können die exportierte Datei nun importieren.

Importieren und Exportieren eines CA-Zertifikats

Sie können ein CA-Zertifikat im Gerät speichern, indem Sie es importieren und exportieren.

So importieren Sie ein CA-Zertifikat

- 1 Klicken Sie auf **CA-Zertifikat** auf der Seite **Sicherheit**.
- 2 Klicken Sie auf **CA-Zertifikat importieren** und wählen Sie das Zertifikat aus. Klicken Sie auf **Senden**.

So exportieren Sie ein CA-Zertifikat

- 1 Klicken Sie auf **CA-Zertifikat** auf der Seite **Sicherheit**.
- 2 Wählen Sie das Zertifikat, das Sie exportieren möchten, und klicken Sie auf **Exportieren**. Klicken Sie auf **Senden**.
- 3 Klicken Sie auf **Speichern**, um den Zielordner auszuwählen.
- 4 Wählen Sie den gewünschten Zielort aus, an dem Sie das exportierte Zertifikat speichern möchten, und speichern Sie dann das Zertifikat.

7

Mehrere Zertifikate verwalten

Diese Funktion für mehrere Zertifikate erlaubt die Verwaltung von allen installierten Zertifikaten über das Web Based Management. Nach der Installation der Zertifikate können Sie sich über die Seite **Zertifikat** anzeigen lassen, welche Zertifikate installiert wurden, und dann den Inhalt der einzelnen Zertifikate ansehen, die Zertifikate löschen oder exportieren. Nähere Informationen zum Zugriff auf die Seite **Zertifikat** finden Sie unter *Konfigurieren eines Zertifikats mit Web Based Management* ►► Seite 89. Das Brother-Gerät ermöglicht das Speichern von bis zu vier selbstsignierten Zertifikaten oder bis zu vier Zertifikaten, die von einer Zertifizierungsstelle ausgestellt wurden. Sie können die gespeicherten Zertifikate zur Verwendung des HTTPS/IPPS-Protokolls, der IEEE 802.1x-Authentifizierung oder einer signierten PDF nutzen.

Sie können auch bis zu vier CA-Zertifikate zur Verwendung der IEEE 802.1x-Authentifizierung und von SSL vor SMTP/POP3 speichern.

Wir empfehlen, ein Zertifikat weniger zu speichern und den dritten Speicherplatz für den Fall freizuhalten, dass ein Zertifikat abläuft. Wenn Sie zum Beispiel ein CA-Zertifikat speichern möchten, speichern Sie drei Zertifikate und lassen Sie einen Speicherplatz zur Sicherung frei. Wenn Sie das Zertifikat erneut anfordern, zum Beispiel weil es abgelaufen ist, können Sie ein neues Zertifikat in den freigehaltenen Speicherplatz importieren und erst dann das abgelaufenen Zertifikat löschen, um Konfigurationsfehler zu vermeiden.

HINWEIS

- Wenn Sie HTTPS/IPPS, IEEE 802.1x oder signierte PDFs verwenden, müssen Sie auswählen, welches Zertifikat verwendet werden soll.
- Wenn Sie SSL für die Kommunikation über SMTP verwenden, müssen Sie kein Zertifikat auswählen. Das erforderliche Zertifikat wird automatisch ausgewählt.

Netzwerkgerät mit SSL/TLS sicher verwalten

Um die Sicherheit Ihres Netzwerkgerätes zu gewährleisten, müssen Sie die Verwaltungsprogramme zusammen mit den Sicherheitsprotokollen verwenden.

Sichere Verwaltung mit Web Based Management (Webbrowser)

Wir empfehlen, das HTTPS-Protokoll zur sicheren Verwaltung zu verwenden. Zur Verwendung dieser Protokolle sind die folgenden Geräteeinstellungen notwendig.

HINWEIS

Das HTTPS-Protokoll ist standardmäßig aktiviert.

Sie können die HTTPS-Protokolleinstellungen und das Zertifikat auf dem Bildschirm von Web Based Management ändern, indem Sie auf **Netzwerk**, **Protokoll** und dann auf **HTTP-Servereinstellungen** klicken.

- 1 Starten Sie Ihren Webbrowser.
- 2 Geben Sie „http://IP-Adresse des Geräts/“ in Ihrem Browser ein. (Wenn Sie das erstellte Zertifikat verwenden, geben Sie „http://Allgemeiner Name/“ in Ihrem Browser ein. Dabei ist „Allgemeiner Name“ der allgemeine Name, den Sie dem Zertifikat zugewiesen haben, zum Beispiel eine IP-Adresse, ein Knotenname oder ein Domänenname. Wie Sie dem Zertifikat einen allgemeinen Namen zuweisen können, lesen Sie unter *Verwenden von Zertifikaten zur Gerätesicherheit* >> Seite 87.)
 - Zum Beispiel:
http://192.168.1.2/ (wenn der allgemeine Name die IP-Adresse des Geräts ist)
- 3 Standardmäßig ist kein Kennwort erforderlich. Wenn Sie zuvor ein Kennwort festgelegt haben, geben Sie dieses ein, und drücken Sie auf .
- 4 Nun können Sie mit HTTPS auf das Gerät zugreifen.
Zur Verwendung des SNMPv3-Protokolls gehen Sie wie unten beschrieben vor.

HINWEIS

Sie können die SNMP-Einstellungen auch mit BRAdmin Professional 3 ändern.

- 5 Klicken Sie auf **Netzwerk**.
- 6 Klicken Sie auf **Protokoll**.

- 7 Vergewissern Sie sich, dass die **SNMP**-Einstellung aktiviert ist, und klicken Sie dann auf **Erweiterte Einstellung** von **SNMP**.
- 8 Nun können Sie die SNMP-Einstellungen im unten gezeigten Bildschirm vornehmen.

SNMP 

Status Aktiviert

Betriebsart des SNMP-Modus

- ☒ SNMP v1/v2c Lese-/Schreibzugriff
- ☐ SNMPv3 Lese-/Schreibzugriff und v1/v2c nur Lesezugriff
- ☐ SNMPv3 Lese-/Schreibzugriff

SNMP v1/v2c-Moduseinstellungen

- ☒ Netzwerkmanagement mit älteren BRAdmin-Versionen ermöglichen

Es gibt drei SNMP-Verbindungsmodi.

■ **SNMP v1/v2c Lese-/Schreibzugriff**

In diesem Modus verwendet der PrintServer Version 1 und Version 2c des SNMP-Protokolls. Sie können in diesem Modus alle Brother-Anwendungen verwenden. Beachten Sie jedoch, dass dieser Modus nicht sicher ist, da er keine Benutzerauthentifizierung verwendet und die Daten nicht verschlüsselt werden.

■ **SNMPv3 Lese-/Schreibzugriff und v1/v2c nur Lesezugriff**

In diesem Modus verwendet der PrintServer den Lese-/Schreibzugriff der Version 3 und den schreibgeschützten Zugriff der Version 1 und Version 2c des SNMP-Protokolls.

HINWEIS

Wenn Sie den Modus **SNMPv3 Lese-/Schreibzugriff und v1/v2c nur Lesezugriff** verwenden, arbeiten einige Brother-Anwendungen, die auf den PrintServer zugreifen (z. B. BRAdmin Light), nicht richtig, da sie lediglich den schreibgeschützten Zugriff der Version 1 und der Version 2c erlauben. Wenn Sie alle Anwendungen verwenden möchten, stellen Sie den **SNMP v1/v2c Lese-/Schreibzugriff** ein.

■ **SNMPv3 Lese-/Schreibzugriff**

In diesem Modus verwendet der PrintServer die Version 3 des SNMP-Protokolls. Wenn Sie den MFC/DCP-Server sicher verwalten möchten, sollten Sie diesen Modus verwenden.

HINWEIS

- Wenn Sie die Einstellung **SNMPv3 Lese-/Schreibzugriff** verwenden, beachten Sie bitte Folgendes:
 - Der PrintServer kann nur mit BRAdmin Professional 3 oder mit Web Based Management verwaltet werden.
 - Mit Ausnahme von BRAdmin Professional 3 werden alle Anwendungen, die SNMPv1/v2c verwenden, eingeschränkt. Um die Verwendung von SNMPv1/v2c-Anwendungen zuzulassen, aktivieren Sie die Betriebsart **SNMPv3 Lese-/Schreibzugriff und v1/v2c nur Lesezugriff** oder **SNMP v1/v2c Lese-/Schreibzugriff**.
 - Weitere Informationen finden Sie in der Hilfe des Web Based Managements.
-

Sichere Verwaltung mit BRAdmin Professional 3 (Windows®)

Um das Dienstprogramm BRAdmin Professional 3 sicher nutzen zu können, müssen Sie die folgenden Punkte beachten

- Sie sollten die neueste Version von BRAdmin Professional 3 verwenden, die Sie von <http://solutions.brother.com/> herunterladen können. Bei Verwendung älterer Versionen von BRAdmin ¹ zur Verwaltung Ihrer Brother-Geräte ist die Benutzerauthentifizierung nicht sicher.
- Wenn Sie den Zugriff auf Ihr Gerät von älteren BRAdmin-Versionen ¹ unterbinden möchten, müssen Sie über Web Based Management den Zugang von älteren BRAdmin-Versionen ¹ über **Erweiterte Einstellung** von **SNMP** auf der Seite **Protokoll** deaktivieren. (Siehe *Sichere Verwaltung mit Web Based Management (Webbrowser)* ►► Seite 100.)
- Falls Sie sowohl BRAdmin Professional 3 als auch das Web Based Management benutzen, sollten Sie das Web Based Management zusammen mit dem HTTPS-Protokoll verwenden.
- Wenn Sie mit BRAdmin Professional 3 verschiedene ältere PrintServer ² zusammen mit neuen PrintServern verwalten, empfehlen wir, für jede Gruppe ein anderes Kennwort zu verwenden. Dadurch wird die Sicherheit der neuen PrintServer sichergestellt.

¹ BRAdmin Professional älter als Version 2.80, BRAdmin Light für Macintosh älter als Version 1.10

² NC-2000-Serie, NC-2100p, NC-3100h, NC-3100s, NC-4100h, NC-5100h, NC-5200h, NC-6100h, NC-6200h, NC-6300h, NC-6400h, NC-8000, NC-100h, NC-110h, NC-120w, NC-130h, NC-140w, NC-8100h, NC-9100h, NC-7100w, NC-7200w, NC-2200w

Sicherer Druck von Dokumenten mit SSL/TLS

Zum sicheren Druck von Dokumenten mit dem IPP-Protokoll können Sie das IPPS-Protokoll verwenden.
Zur Konfiguration von IPPS-Einstellungen über einen Webbrowser:

- 1 Klicken Sie auf der Webseite Ihres Gerätes auf **Netzwerk** und dann auf **Protokoll**. Wenn das Kontrollkästchen **IPP** bereits aktiviert ist, fahren Sie mit Schritt 5 fort.
- 2 Aktivieren Sie das Kontrollkästchen **IPP** und klicken Sie dann auf **Senden**.
- 3 Starten Sie das Gerät neu, um die Konfiguration zu aktivieren.
- 4 Klicken Sie auf der Webseite Ihres Gerätes auf **Netzwerk** und dann auf **Protokoll**.
- 5 Klicken Sie auf **HTTP-Servereinstellungen**.
- 6 Aktivieren Sie das Kontrollkästchen **HTTPS(Port443)** und klicken Sie dann auf **Senden**.
- 7 Starten Sie das Gerät neu, um die Konfiguration zu aktivieren.

HINWEIS

Die Kommunikation über IPPS kann den unbefugten Zugriff auf den MFC/DCP-Server nicht verhindern.

Sicheres Versenden oder Empfangen einer E-Mail

Konfiguration mit Web Based Management (Webbrowser)

Sie können das sichere Senden von E-Mails mit Benutzerauthentifizierung oder das Senden und Empfangen von E-Mails mit SSL/TLS im Bildschirm von Web Based Management konfigurieren.

- 1 Starten Sie Ihren Webbrowser.
- 2 Geben Sie in die Adressleiste Ihres Browsers „http://IP-Adresse des Gerätes/“ ein (wobei „IP-Adresse des Gerätes“ für die IP-Adresse des Gerätes oder den Namen des PrintServers steht).
 - Zum Beispiel: http://192.168.1.2/
- 3 Standardmäßig ist kein Kennwort erforderlich. Wenn Sie zuvor ein Kennwort festgelegt haben, geben Sie dieses ein, und drücken Sie auf .
- 4 Klicken Sie auf **Netzwerk**.
- 5 Klicken Sie auf **Protokoll**.
- 6 Klicken Sie auf **Erweiterte Einstellung** von **POP3/SMTP** und vergewissern Sie sich, dass der Status von **POP3/SMTP** auf **Aktiviert** steht.
- 7 Auf dieser Seite können Sie die **POP3/SMTP**-Einstellungen konfigurieren.

HINWEIS

- Weitere Informationen finden Sie in der Hilfe des Web Based Managements.
 - Durch das Senden einer Test-E-Mail können Sie die Konfiguration der E-Mail-Einstellungen überprüfen.
 - Wenn Sie die POP3/SMTP-Servereinstellungen nicht kennen, wenden Sie sich an Ihren Systemadministrator oder ISP (Internetanbieter).
-
- 8 Klicken Sie nach der Konfiguration auf **Senden**. Das Dialogfeld zum Testen der E-Mail-Versand-/Empfangskonfiguration wird angezeigt.
 - 9 Folgen Sie den Anweisungen auf dem Bildschirm, wenn Sie Ihre aktuellen Einstellungen prüfen möchten.

Versenden einer E-Mail mit Benutzerauthentifizierung

Dieses Gerät unterstützt die Methoden POP vor SMTP und SMTP-AUTH zum Senden einer E-Mail über einen E-Mail-Server, der eine Benutzerauthentifizierung erfordert. Diese Methoden verhindern den unbefugten Zugriff auf den E-Mail-Server. Sie können diese Einstellungen mit Web Based Management oder BRAdmin Professional 3 konfigurieren. Sie können die Authentifizierungsmethoden POP vor SMTP und SMTP-AUTH für die E-Mail-Benachrichtigung, für E-Mail-Berichte und für das Versenden von Internet-Faxen verwenden.

E-Mail-Server Einstellungen

Die Einstellungen für die SMTP-Authentifizierung müssen mit der Methode, die der E-Mail-Server verwendet, übereinstimmen. Sprechen Sie die Konfiguration des E-Mail-Servers mit Ihrem Netzwerkadministrator oder Internetanbieter ab.

Für eine SMTP-Serverauthentifizierung muss auch **SMTP-AUTH** als **Authentifizierungsmethode für SMTP-Server** aktiviert sein.

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.
- Wenn Sie sowohl POP vor SMTP als auch SMTP-AUTH verwenden können, empfehlen wir SMTP-AUTH.
- Wenn Sie als Authentifizierungsmethode für SMTP-Server POP vor SMTP wählen, müssen Sie die POP3-Einstellungen konfigurieren. Sie können auch die APOP-Methode verwenden.

Sicheres Versenden oder Empfangen einer E-Mail mit SSL/TLS

Dieses Gerät unterstützt SSL/TLS zum Senden oder Empfangen 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 oder zu empfangen, der die SSL/TLS-Kommunikation verwendet, müssen SMTP über SSL/TLS oder POP3 über SSL/TLS richtig konfiguriert sein.

Server-Zertifikat verifizieren

- Wenn Sie SSL oder TLS für **SMTP über SSL/TLS** oder **POP3 über SSL/TLS** gewählt haben, wird das Kontrollkästchen **Server-Zertifikat verifizieren** automatisch aktiviert, um das Server-Zertifikat zu überprüfen.
 - Bevor Sie das Server-Zertifikat überprüfen, müssen Sie das CA-Zertifikat importieren, das von der Zertifizierungsstelle (CA) ausgestellt wurde, die auch das Server-Zertifikat signiert hat. Fragen Sie Ihren Netzwerkadministrator oder Internetanbieter (ISP, Internet Service Provider), ob der Import eines CA-Zertifikates erforderlich ist. Zum Import des Zertifikates lesen Sie *Importieren und Exportieren eines CA-Zertifikats* >> Seite 99.
 - Wenn Sie das Server-Zertifikat nicht überprüfen müssen, deaktivieren Sie **Server-Zertifikat verifizieren**.

Portnummer

- Wenn Sie SSL wählen, werden die Einstellungen von **SMTP-Port** oder **POP3-Port** an das Protokoll angepasst. Wenn Sie die Portnummer manuell ändern möchten, geben Sie die Portnummer ein, nachdem Sie **SMTP über SSL/TLS** oder **POP3 über SSL/TLS** gewählt haben.
- Sie müssen die Kommunikationsmethoden POP3/SMTP konfigurieren, um Sie an den E-Mail-Server anzupassen. Für ausführliche Informationen zu den Einstellungen des E-Mail-Servers wenden Sie sich an Ihren Netzwerkadministrator oder ISP (Internetanbieter).

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

(SMTP)

SMTP-Port: 587

Authentifizierungsmethode für SMTP-Server: SMTP-AUTH

SMTP über SSL/TLS: TLS

(POP3)

POP3-Port: 995

POP3 über SSL/TLS: SSL

Verwenden der IEEE 802.1x-Authentifizierung

Sie können die IEEE 802.1x-Authentifizierung für ein verkabeltes Netzwerk oder ein Wireless-Netzwerk konfigurieren.

Konfigurieren der IEEE 802.1x-Authentifizierung mit Web Based Management (Webbrowser)

Wenn Sie die IEEE 802.1x-Authentifizierung für verkabelte Netzwerke oder Wireless-Netzwerke mit Web Based Management konfigurieren, gehen Sie anhand der nachfolgenden Anweisungen vor.

Sie können zur Konfiguration der IEEE 802.1x-Authentifizierung auch die folgende Software verwenden:

(Verkabeltes Netzwerk)

- BRAdmin Professional 3

(Wireless-Netzwerk)

- Wireless Setup-Assistent über das Funktionstastenfeld (Weitere Informationen finden Sie unter *Konfigurieren Ihres Geräts für ein Wireless-Unternehmensnetzwerk* >> Seite 23.)
- Wireless Setup-Assistent auf der CD-ROM (Weitere Informationen finden Sie unter *Vorübergehende Wireless-Konfiguration über ein USB-Kabel (empfohlen)* >> Seite 13.)
- BRAdmin Professional 3

HINWEIS

- Wenn Sie Ihr Gerät mit EAP-TLS-Authentifizierung konfigurieren, müssen Sie das von einer Zertifizierungsstelle ausgegebene Client-Zertifikat installieren, bevor Sie mit der Konfiguration beginnen. Wenden Sie sich bezüglich des Client-Zertifikats an Ihren Netzwerkadministrator. Wenn Sie mehrere Zertifikate installiert haben, empfehlen wir, das Zertifikat, das Sie verwenden möchten, zu notieren. Weitere Einzelheiten zur Installation des Zertifikats siehe *Verwenden von Zertifikaten zur Gerätesicherheit* >> Seite 87.
- Bevor Sie das Server-Zertifikat überprüfen, müssen Sie das CA-Zertifikat importieren, das von der Zertifizierungsstelle (CA) ausgestellt wurde, die auch das Server-Zertifikat signiert hat. Fragen Sie Ihren Netzwerkadministrator oder Internetanbieter (ISP, Internet Service Provider), ob der Import eines CA-Zertifikates erforderlich ist. Weitere Einzelheiten zum Import des Zertifikats siehe *Importieren und Exportieren eines CA-Zertifikats* >> Seite 99.
- Ausführliche Informationen zu den einzelnen Zertifikaten siehe *Verwenden von Zertifikaten zur Gerätesicherheit* >> Seite 87.

- 1 Starten Sie Ihren Webbrowser.

- 2 Geben Sie in die Adressleiste Ihres Browsers „http://IP-Adresse des Gerätes/“ ein (wobei „IP-Adresse des Gerätes“ für die IP-Adresse des Gerätes oder den Namen des PrintServers steht).
 - Zum Beispiel: http://192.168.1.2/

HINWEIS

- Falls Sie ein Domänen-Namensystem (DNS) verwenden oder die Verwendung von NetBIOS-Namen aktiviert haben, können Sie einen anderen Namen wie zum Beispiel „FreigegebenerDrucker“ anstelle der IP-Adresse eingeben.

- Zum Beispiel: http://FreigegebenerDrucker/

Wenn Sie die Verwendung von NetBIOS-Namen aktiviert haben, können Sie auch den Knotennamen verwenden.

- Zum Beispiel: http://brnxxxxxxxxxxxxx/

Den NetBIOS-Namen können Sie dem Netzwerk-Konfigurationsbericht entnehmen (siehe *Drucken des Netzwerk-Konfigurationsberichts* >> Seite 49).

- Macintosh-Nutzer können einfach durch Klicken auf das Gerätesymbol im **Status Monitor**-Bildschirm auf das Web Based Management zugreifen. Weitere Informationen: >> Software-Handbuch.

- 3 Standardmäßig ist kein Kennwort erforderlich. Wenn Sie zuvor ein Kennwort festgelegt haben, geben Sie dieses ein und drücken Sie auf ➡.

- 4 Klicken Sie auf **Netzwerk**.

- 5 (Verkabelt) Klicken Sie auf **Verkabelt** und dann auf **802.1x-Authentifizierung**.
(Verkabelt) Klicken Sie auf **Wireless** und wählen Sie dann **Wireless (Firmenbereich)**.

- 6 Sie können nun die Einstellungen zur IEEE 802.1x-Authentifizierung konfigurieren.
 - Wenn Sie die IEEE 802.1x-Authentifizierung für ein verkabeltes Netzwerk aktivieren möchten, markieren Sie **Aktiviert** für **802.1x-Status (verkabelt)** auf der Seite **802.1x-Authentifizierung**.
 - Ausführliche Informationen zur IEEE 802.1x-Authentifizierung und den inneren Authentifizierungsmethoden finden Sie unter *IEEE 802.1x-Authentifizierung* >> Seite 128.
 - Wenn Sie die EAP-TLS-Authentifizierung verwenden, müssen Sie das Client-Zertifikat das zur Verifizierung installiert wurde (angezeigt mit dem Zertifikatsnamen), aus der Dropdown-Liste **Client-Zertifikat** wählen.
 - Wenn Sie die Authentifizierung mit EAP-FAST, PEAP, EAP-TTLS oder EAP-TLS gewählt haben, können Sie die Verifizierungsmethode aus der Dropdown-Liste **Server-Zertifikat-Verifizierung** wählen. Sie können das Server-Zertifikat mit Hilfe des zuvor importierten CA-Zertifikates verifizieren, das von der Zertifizierungsstelle (CA) ausgestellt wurde, die auch das Server-Zertifikat signiert hat.

Sie können eine der folgenden Verifizierungsmethoden aus der Dropdown-Liste **Server-Zertifikat-Verifizierung** wählen.

- **Keine Verifizierung**

Das Server-Zertifikat ist immer vertrauenswürdig. Die Verifizierung wird nicht ausgeführt.

■ CA-Zert.

Die Verifizierungsmethode zur Überprüfung der CA-Zuverlässigkeit des Server-Zertifikates mit Hilfe des CA-Zertifikates, das von der Zertifizierungsstelle (CA) ausgestellt wurde, die auch das Server-Zertifikat signiert hat.

■ CA-Zert. + Server-ID

Die Verifizierungsmethode zur Überprüfung des allgemeinen Namens¹ des Server-Zertifikates, zusätzlich zur Überprüfung der CA-Zuverlässigkeit des Server-Zertifikates.

¹ Die Überprüfung des allgemeinen Namens vergleicht den allgemeinen Namen des Server-Zertifikates mit der als **Server-ID** konfigurierten Zeichenkette. Bevor Sie diese Methode verwenden, fragen Sie Ihren Systemadministrator nach dem allgemeinen Namen des Server-Zertifikates und konfigurieren Sie dann die **Server-ID**.

7 Klicken Sie nach der Konfiguration auf **Senden**.

(Verkabelt)

Schließen Sie das Gerät nach Abschluss der Konfiguration an das IEEE 802.1x-Netzwerk an. Drucken Sie nach einigen Minuten den Netzwerk-Konfigurationsbericht aus, um **<Wired IEEE 802.1x> Status** zu überprüfen (siehe *Drucken des Netzwerk-Konfigurationsberichts* ►► Seite 49).

■ Success

Die IEEE 802.1x-Funktion (verkabelt) ist aktiviert und die Authentifizierung war erfolgreich.

■ Failed

Die IEEE 802.1x-Funktion (verkabelt) ist aktiviert, die Authentifizierung ist jedoch fehlgeschlagen.

■ Off

Die IEEE 802.1x-Funktion (verkabelt) ist nicht verfügbar.

(Wireless)

Kurz nach der Konfiguration wird automatisch der WLAN-Bericht ausgedruckt. Prüfen Sie die Wireless-Konfiguration im Bericht. Siehe *Drucken des WLAN-Bericht* (Für HL-3180CDW, DCP-9015CDW, DCP-9017CDW, DCP-9020CDW, DCP-9022CDW, MFC-9130CW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW) ►► Seite 49.

Übersicht

Dieses Kapitel erklärt, wie Sie Netzwerkprobleme, die bei der Verwendung Ihres Brother-Gerätes auftreten können, lösen können. Falls Sie in diesem Kapitel keine Lösung für Ihr Problem finden, besuchen Sie das Brother Solutions Center unter: <http://solutions.brother.com/>.

Bitte besuchen Sie das Brother Solutions Center unter <http://solutions.brother.com/> und klicken Sie auf der Seite für Ihr Modell auf Handbücher, um die anderen Handbücher herunterzuladen.

Problemerkennung

Vergewissern Sie sich, dass die folgenden Punkte erfüllt sind, bevor Sie die Problemlösungen lesen.

Prüfen Sie zunächst Folgendes:
Der Netzstecker ist richtig angeschlossen und das Brother-Gerät ist eingeschaltet.
Der Access Point (für wireless), Router oder Hub ist eingeschaltet und die Verbindungsanzeige blinkt.
Alle Transportschutzteile wurden vom Gerät entfernt.
Die Tonerkassetten und die Trommeleinheit sind richtig installiert.
Die oberen und hinteren Abdeckungen sind ganz geschlossen.
Das Papier ist richtig in die Papierkassette eingelegt.
(Für verkabelte Netzwerke) Ein Netzkabel ist richtig an das Brother-Gerät und den Router oder Hub angeschlossen.

Schauen Sie auf der Seite nach, die unten in der Liste für Ihre Lösung genannt ist

- Ich kann die Einrichtung für das Wireless-Netzwerk nicht abschließen. (Siehe Seite 112.)
- Das Brother-Gerät wird während der Installation der MFL-Pro Suite nicht im Netzwerk gefunden. (Siehe Seite 113.)
- Das Brother-Gerät kann über das Netzwerk nicht drucken oder scannen. (Siehe Seite 114.)
- Das Brother-Gerät wird auch nach erfolgreicher Installation nicht im Netzwerk gefunden. (Siehe Seite 114.)
- Ich verwende Sicherheitssoftware. (Siehe Seite 117.)
- Ich möchte prüfen, ob meine im Netzwerk angeschlossenen Geräte richtig arbeiten. (Siehe Seite 118.)

Ich kann die Einrichtung für das Wireless-Netzwerk nicht abschließen.

Frage	Schnittstelle	Lösung
Mein Gerät stellt während der Wireless-Einrichtung keine Verbindung her?	wireless	Schalten Sie Ihren Wireless-Router aus und wieder ein. Versuchen Sie dann erneut, die Wireless-Einstellungen zu konfigurieren.
Sind die Sicherheitseinstellungen (SSID/Netzwerkschlüssel) korrekt?	wireless	■ Überprüfen Sie die Sicherheitseinstellungen und wählen Sie die richtigen Einstellungen. • Der Name des Herstellers bzw. die Modellnummer des WLAN-Access Point/Routers werden eventuell als die standardmäßigen Sicherheitseinstellungen verwendet. • Lesen Sie die Anleitung, die mit Ihrem WLAN Access Point/Router geliefert wurde, um die Sicherheitseinstellungen herauszufinden. • Wenden Sie sich an den Hersteller Ihres WLAN Access Points/Routers, an Ihren Internetanbieter oder Netzwerkadministrator. ■ Für Informationen zur SSID und dem Netzwerkschlüssel siehe <i>Bedingungen und Konzepte für WLAN-Netzwerke (Für HL-3180CDW, DCP-9015CDW, DCP-9017CDW, DCP-9020CDW, DCP-9022CDW, MFC-9130CW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW)</i> >> Seite 130.
Verwenden Sie eine MAC-Adressenfilterung?	wireless	Überprüfen Sie, ob die MAC-Adresse des Brother-Gerätes im Filter erlaubt ist. Sie können die MAC-Adresse Ihres Brother-Gerätes über das Funktionstastenfeld ermitteln. (Siehe <i>Funktionstabelle und werkseitige Standardeinstellungen</i> >> Seite 50.)
Befindet sich Ihr WLAN-Access Point/Router im geschützten Modus? (SSID wird nicht gesendet)	wireless	■ Sie sollten den SSID-Namen oder der Netzwerkschlüssel manuell eingeben. ■ Überprüfen Sie den SSID-Namen bzw. den Netzwerkschlüssel anhand der Anleitung, die mit Ihrem WLAN Access Point/Router geliefert wurde, und konfigurieren Sie die Wireless-Netzwerkeinstellungen erneut. (Siehe <i>Konfigurieren Ihres Geräts, wenn keine SSID gesendet wird</i> >> Seite 21.)
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 über das Netzwerk nicht drucken oder scannen. Das Brother-Gerät wird auch nach erfolgreicher Installation nicht im Netzwerk gefunden.</i> >> Seite 114.)

Das Brother-Gerät wird während der Installation der MFL-Pro Suite nicht im Netzwerk gefunden.

Frage	Schnittstelle	Lösung
Ist Ihr Gerät mit dem Netzwerk verbunden und verfügt es über eine gültige IP-Adresse?	verkabelt/ wireless	Drucken Sie den Netzwerk-Konfigurationsbericht und überprüfen Sie, dass Ethernet Link Status oder Wireless Link Status auf Link OK gesetzt ist. Siehe <i>Drucken des Netzwerk-Konfigurationsberichts</i> >> Seite 49. Wenn der Bericht Failed To Associate oder Link DOWN anzeigt, fragen Sie bei Ihrem Netzwerkadministrator nach, ob die IP-Adresse gültig ist oder nicht.
Verwenden Sie Sicherheitssoftware?	verkabelt/ wireless	■ Wählen Sie im Installationsdialogfeld erneut die Option zur Suche nach dem Brother-Gerät. ■ Erlauben Sie den Zugriff, wenn während der Installation der MFL-Pro Suite eine Warnmeldung der Sicherheitssoftware angezeigt wird. ■ Für weitere Informationen zur Sicherheitssoftware lesen Sie <i>Ich verwende Sicherheitssoftware</i>. >> Seite 117.
Ist Ihr Gerät zu weit entfernt vom WLAN Access Point/Router aufgestellt?	wireless	Stellen Sie das Brother-Gerät zur Konfiguration der Wireless-Netzwerkeinstellungen innerhalb eines Abstandes von ca. 1 m vom WLAN Access Point/Router auf.
Befinden sich Hindernisse (zum Beispiel Wände oder Möbel) zwischen Ihrem Gerät und dem WLAN Access Point/Router?	wireless	Stellen Sie das Brother-Gerät so auf, dass der Funkkontakt nicht gestört wird, oder stellen Sie es näher an den WLAN-Access Point/Router.
Befindet sich ein Wireless-Computer, ein Gerät, das Bluetooth unterstützt, ein Mikrowellengerät oder ein digitales schnurloses Telefon in der Nähe des Gerätes oder des WLAN-Access Point/Routers?	wireless	Stellen Sie alle Geräte in größerer Entfernung vom Brother-Gerät bzw. vom WLAN Access Point/Router auf.

**Das Brother-Gerät kann über das Netzwerk nicht drucken oder 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> ►► Seite 117.
Wurde dem Brother-Gerät eine verfügbare IP-Adresse zugewiesen?	verkabelt/ wireless	■ (Windows®) Überprüfen Sie die IP-Adresse und die Subnetzmaske mit Hilfe des Dienstprogramms zum Reparieren der Netzwerkverbindung. Verwenden Sie das Dienstprogramm zum Reparieren der Netzwerkverbindung, um die Netzwerkeinstellungen des Brother-Gerätes zu reparieren. Es weist die korrekte IP-Adresse und Subnetzmaske zu. Zur Verwendung des Dienstprogramms zum Reparieren der Netzwerkverbindung bitten Sie Ihren Netzwerkadministrator um weitere Informationen, und gehen Sie dann wie folgt vor: HINWEIS • (Windows® XP/XP Professional x64 Edition/Windows Vista®/Windows® 7/Windows® 8) Sie müssen sich mit Administratorrechten anmelden. • Vergewissern Sie sich, dass das Brother-Gerät eingeschaltet und mit demselben Netzwerk wie Ihr Computer verbunden ist.

**Das Brother-Gerät kann über das Netzwerk nicht drucken oder scannen.
Das Brother-Gerät wird auch nach erfolgreicher Installation nicht im Netzwerk
gefunden. (Fortsetzung)**

Frage	Schnittstelle	Lösung
Wurde dem Brother-Gerät eine verfügbare IP-Adresse zugewiesen? (Fortsetzung)	verkabelt/ wireless	1 (Windows® XP) Klicken Sie auf die Schaltfläche Start, Alle Programme, Zubehör und Windows-Explorer und dann auf Arbeitsplatz. (Windows Vista®/Windows® 7) Klicken Sie auf  und Computer. (Windows® 8) Klicken Sie in der Symbolleiste auf das Symbol  (Explorer) und klicken Sie dann in der linken Navigationsleiste auf Computer. 2 Doppelklicken Sie auf XXX (C:), Programme oder Programme (x86) für Nutzer von 64-Bit-Betriebssystemen, Browny02, Brother, BrotherNetTool.exe, um das Programm auszuführen. HINWEIS Wenn das Fenster Benutzerkontensteuerung erscheint: (Windows Vista®) Klicken Sie auf Fortsetzen. (Windows® 7/Windows® 8) Klicken Sie auf Ja. 3 Folgen Sie den Anweisungen auf dem Bildschirm. 4 Stellen Sie sicher, dass Sie drucken oder scannen können. HINWEIS Das Programm zum Reparieren der Netzwerkverbindung wird automatisch gestartet, wenn Sie das Kontrollkästchen Programm zum Reparieren der Netzwerkverbindung aktivieren mit Hilfe des Status Monitors aktivieren. Klicken Sie mit der rechten Maustaste auf den Status Monitor-Bildschirm, klicken Sie auf Optionen, Details, und klicken Sie dann auf die Registerkarte Diagnose. Dies wird nicht empfohlen, wenn der Netzwerkadministrator die IP-Adresse fest eingestellt hat (Statisch), weil sonst die IP-Adresse automatisch geändert wird. Wenn auch nach der Verwendung des Dienstprogramms zum Reparieren der Netzwerkverbindung die IP-Adresse und Subnetzmaske nicht richtig zugewiesen sind, fragen Sie Ihren Netzwerkadministrator nach diesen Informationen oder besuchen Sie das Brother Solutions Center unter http://solutions.brother.com/.

**Das Brother-Gerät kann über das Netzwerk nicht drucken oder scannen.
Das Brother-Gerät wird auch nach erfolgreicher Installation nicht im Netzwerk
gefunden. (Fortsetzung)**

Frage	Schnittstelle	Lösung
Konnte Ihr vorheriger Druckauftrag nicht richtig ausgeführt werden?	verkabelt/ wireless	Wenn sich der fehlgeschlagene Druckauftrag noch immer in der Druckwarteschlange Ihres Computer befindet, löschen Sie ihn. Versuchen Sie andernfalls eine der folgenden Möglichkeiten: (Windows® XP/Windows Vista®/ Windows® 7/Windows Server® 2003) Doppelklicken Sie auf das Druckersymbol im folgenden Ordner und wählen Sie dann Alle Druckaufträge abbrechen im Menü Drucker: (Windows® XP/Windows Server® 2003) Start und Drucker und Faxgeräte. (Windows Vista®)  Systemsteuerung, Hardware und Sound und dann Drucker. (Windows® 7)  Geräte und Drucker und dann Drucker und Faxgeräte. (Windows® 8) Ziehen Sie Ihre Maus in die untere rechte Ecke Ihres Desktops. Wenn die Menüleiste erscheint, klicken Sie auf Einstellungen und dann auf Systemsteuerung. Klicken Sie in der Gruppe Hardware und Sound auf Geräte und Drucker anzeigen. Klicken Sie mit der rechten Maustaste auf Ihr Brother-Gerät und wählen Sie Druckaufträge anzeigen und dann Ihren Druckertreiber aus. (Windows Server® 2008) Start, Systemsteuerung und Drucker. (Windows Server® 2012) Ziehen Sie Ihre Maus in die untere rechte Ecke Ihres Desktops. Wenn die Menüleiste erscheint, klicken Sie auf Einstellungen und dann auf Systemsteuerung. Klicken Sie in der Gruppe Hardware auf Geräte und Drucker anzeigen. Klicken Sie mit der rechten Maustaste auf Ihr Brother-Gerät und wählen Sie Druckaufträge anzeigen und dann Ihren Druckertreiber aus.
Verbinden Sie das Brother-Gerät drahtlos mit dem Netzwerk?	wireless	■ Drucken Sie den WLAN-Bericht aus, um den Status der Wireless-Verbindung zu prüfen. (Weitere Informationen zum Drucken des Berichtes finden Sie unter <i>Drucken des WLAN-Bericht (Für HL-3180CDW, DCP-9015CDW, DCP-9017CDW, DCP-9020CDW, DCP-9022CDW, MFC-9130CW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW)</i> >> Seite 49.) Falls im WLAN-Bericht ein Fehlercode ausgedruckt wurde: >> Installationsanleitung: <i>Problemlösung</i>. ■ Siehe <i>Das Brother-Gerät wird während der Installation der MFL-Pro Suite nicht im Netzwerk gefunden.</i> >> Seite 113.

**Das Brother-Gerät kann über das Netzwerk nicht drucken oder scannen.
Das Brother-Gerät wird auch nach erfolgreicher Installation nicht im Netzwerk
gefunden. (Fortsetzung)**

Frage	Schnittstelle	Lösung
Ich habe alle oben genannten Punkte überprüft und ausgeführt, aber das Brother-Gerät druckt/scannt nicht. Was kann ich sonst noch tun?	verkabelt/ wireless	Deinstallieren Sie die MFL-Pro Suite und installieren Sie sie dann erneut.

Ich verwende Sicherheitssoftware.

Frage	Schnittstelle	Lösung
Haben Sie während der Installation der MFL-Pro Suite, dem Starten von Programmen oder beim Verwenden der Druck-/Scanfunktionen die Sicherheitswarnung im Dialogfeld akzeptiert?	verkabelt/ wireless	Wenn Sie die Sicherheitswarnung im Dialogfeld nicht akzeptiert haben, verweigert die Firewall-Funktion Ihrer Sicherheitssoftware möglicherweise den Zugriff. Einige Sicherheitsprogramme blockieren eventuell den Zugriff, ohne ein Dialogfeld zur Sicherheitswarnung anzuzeigen. Lesen Sie in der Anleitung der Sicherheitssoftware nach, wie Sie den Zugriff erlauben können, oder fragen Sie den Hersteller.
Ich möchte die notwendigen Portnummern für die Sicherheitssoftware-Einstellungen wissen.	verkabelt/ wireless	Die folgenden Portnummern werden von den Brother-Netzwerkfunktionen verwendet: ■ Scannen im Netzwerk → Portnummer 54925 / Protokoll UDP ■ PC-FAX-Empfang im Netzwerk ¹ → Portnummer 54926 / Protokoll UDP ■ Scannen/Drucken im Netzwerk ¹, PC-FAX-Empfang ¹, Remote Setup ¹ → Portnummer 161 und 137/ Protokoll UDP ■ BRAdmin Light ¹ → Portnummer 161 / Protokoll UDP ¹ Nur Windows®. Siehe die Anleitung der Sicherheitssoftware oder wenden Sie sich an den Hersteller, um ausführliche Informationen zum Öffnen der Ports zu erhalten.

Ich möchte prüfen, ob meine im Netzwerk angeschlossenen Geräte richtig arbeiten.

Frage	Schnittstelle	Lösung
Ist Ihr Brother-Gerät, Ihr Access Point/Router bzw. Ihr Netzwerk-Hub eingeschaltet?	verkabelt/ wireless	Stellen Sie sicher, dass Sie alle Punkte unter <i>Prüfen Sie zunächst Folgendes</i> : >> Seite 111 überprüft haben.
Wo kann ich die Netzwerkeinstellungen meines Brother-Gerätes, wie die IP-Adresse, finden?	verkabelt/ wireless	Drucken Sie den Netzwerk-Konfigurationsbericht. (Siehe <i>Drucken des Netzwerk-Konfigurationsberichts</i> >> Seite 49.)
Wie kann ich den Verbindungsstatus meines Brother-Gerätes prüfen?	verkabelt/ wireless	Drucken Sie den Netzwerk-Konfigurationsbericht und überprüfen Sie, dass Ethernet Link Status oder Wireless Link Status auf Link OK gesetzt ist. (Siehe <i>Drucken des Netzwerk-Konfigurationsberichts</i> >> Seite 49.) Wenn der Bericht Link DOWN oder Failed To Associate anzeigt, beginnen Sie noch einmal ab <i>Prüfen Sie zunächst Folgendes</i> : >> Seite 111.
Kann ich das Brother-Gerät von meinem Computer aus mit dem „Ping“-Befehl erreichen?	verkabelt/ wireless	Verwenden Sie den „Ping“-Befehl mit der IP-Adresse oder dem Knotennamen des Brother-Gerätes von Ihrem Computer aus. ■ Erfolgreich – Ihr Brother-Gerät arbeitet korrekt und ist mit demselben Netzwerk wie Ihr Computer verbunden. ■ Nicht erfolgreich – Ihr Brother-Gerät ist nicht mit demselben Netzwerk wie Ihr Computer verbunden. (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. Für weitere Informationen zum Dienstprogramm zum Reparieren der Netzwerkverbindung lesen Sie (Windows®) <i>Überprüfen Sie die IP-Adresse und die Subnetzmaske mit Hilfe des Dienstprogramms zum Reparieren der Netzwerkverbindung</i> . unter <i>Wurde dem Brother-Gerät eine verfügbare IP-Adresse zugewiesen?</i> >> Seite 114.
Verbindet sich das Brother-Gerät mit dem Wireless-Netzwerk?	wireless	Drucken Sie den WLAN-Bericht aus, um den Status der Wireless-Verbindung zu prüfen. Weitere Informationen zum Drucken finden Sie unter <i>Drucken des WLAN-Bericht</i> (Für HL-3180CDW, DCP-9015CDW, DCP-9017CDW, DCP-9020CDW, DCP-9022CDW, MFC-9130CW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW) >> Seite 49. Falls im WLAN-Bericht ein Fehlercode ausgedruckt wurde: >> Installationsanleitung: <i>Problemlösung</i> .
Ich habe alle oben genannten Punkte überprüft und ausgeführt, aber das Problem tritt weiter auf. Was kann ich sonst noch tun?	wireless	Lesen Sie die Anleitung, die Sie mit Ihrem WLAN Access Point/Router erhalten haben, um die SSID- und Netzwerkschlüssel-Informationen zu ermitteln und sie richtig einzustellen. Für weitere Informationen zur SSID und dem Netzwerkschlüssel lesen Sie <i>Sind die Sicherheitseinstellungen (SSID/Netzwerkschlüssel) korrekt?</i> unter <i>Ich kann die Einrichtung für das Wireless-Netzwerk nicht abschließen</i> . >> Seite 112.



Netzwerkbegriffe

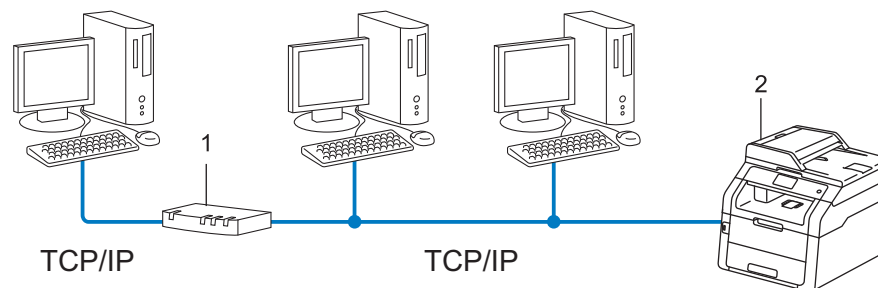
Netzwerkverbindungsarten und Protokolle	120
Konfigurieren Ihres Geräts für ein Netzwerk	126
Bedingungen und Konzepte für WLAN-Netzwerke (Für HL-3180CDW, DCP-9015CDW, DCP-9017CDW, DCP-9020CDW, DCP-9022CDW, MFC-9130CW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW)	130
Zusätzliche Netzwerkeinstellungen von Windows®	134
Sicherheitsbegriffe und -konzepte	139

Netzwerkverbindungsarten

Beispiel für eine verkabelte Netzwerkverbindung

Drucken in einer Peer-to-Peer-Umgebung mit TCP/IP

In einer Peer-to-Peer-Umgebung sendet jeder Computer Daten direkt an jedes Gerät und empfängt von diesen Geräten auch Daten. Dateizugriffe und gemeinsam genutzte Geräte werden nicht über einen zentralen Server gesteuert.



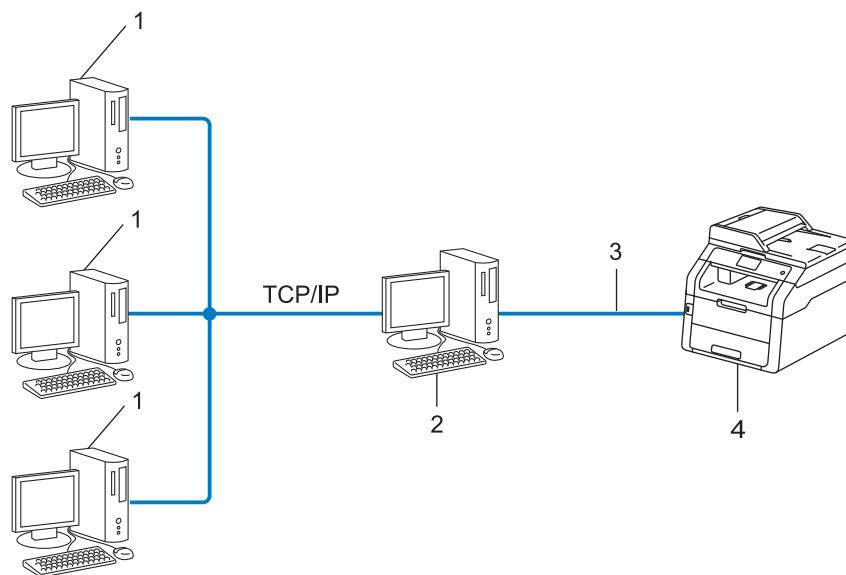
1 Router

2 Netzwerkgerät (Ihr Gerät)

- Für kleinere Netzwerke mit 2 oder 3 Computern empfehlen wir das Drucken in einer Peer-to-Peer-Umgebung, da sie einfacher zu konfigurieren ist als das Drucken über das gemeinsame Netzwerk. Siehe *Netzwerk-Druckerfreigabe* >> Seite 121.
- Jeder Computer muss das TCP/IP-Protokoll verwenden.
- Die IP-Adresse des Brother-Gerätes muss entsprechend konfiguriert werden.
- Wenn Sie einen Router verwenden, muss die Gateway-Adresse der verwendeten Computer und des Brother-Gerätes konfiguriert werden.

Netzwerk-Druckerfreigabe

In einer Netzwerkumgebung sendet jeder Computer Daten über einen zentral verwalteten Computer. Dieser Computer wird in der Regel „Server“ oder „Druckserver“ genannt. Seine Aufgabe ist es, das Drucken aller Druckaufträge zu steuern.



- 1 Client-Computer
- 2 Computer, bezeichnet als „Server“ oder „Druckserver“
- 3 TCP/IP, USB oder Parallel (soweit verfügbar)
- 4 Netzwerkgerät (Ihr Gerät)

- In größeren Netzwerken empfehlen wir das Einrichten von Netzwerkdruckern.
- Der „Server“ bzw. „Druckserver“ muss das TCP/IP-Protokoll verwenden.
- Falls das Brother-Gerät nicht über die USB- oder Parallelschnittstelle an den Server angeschlossen wurde, muss dem Gerät eine entsprechende IP-Adresse zugewiesen werden.

Protokolle

TCP/IP-Protokolle und -Funktionen

Protokolle sind standardisierte Regeln zur Datenübertragung in einem Netzwerk. Durch Protokolle erhalten Nutzer Zugang zu den Netzwerk-Ressourcen.

Der mit diesem Brother-Gerät verwendete PrintServer unterstützt das TCP/IP-Protokoll (Transmission Control Protocol/Internet Protocol).

Das TCP/IP-Protokoll ist das am häufigsten verwendete Protokoll für die Kommunikation, wie zum Beispiel im Internet und per E-Mail. Dieses Protokoll kann unter fast allen Betriebssystemen verwendet werden, wie Windows®, Windows Server®, Mac OS X und Linux®. Die folgenden TCP/IP-Protokolle sind für dieses Brother-Gerät verfügbar.

HINWEIS

- Sie können die Protokolleinstellungen über die HTTP-Schnittstelle (Webbrowser) konfigurieren. (Siehe *So konfigurieren Sie die Geräteeinstellungen über Web Based Management (Webbrowser)* >> Seite 58.)
- Um herauszufinden, welche Protokolle Ihr Brother-Gerät unterstützt, siehe *Unterstützte Protokolle und Sicherheitsfunktionen* >> Seite 143.
- Informationen zu den unterstützten Sicherheitsprotokollen finden Sie unter *Sicherheitsprotokolle* >> Seite 140.

9

DHCP/BOOTP/RARP

Über die Protokolle DHCP/BOOTP/RARP kann die IP-Adresse automatisch konfiguriert werden.

HINWEIS

Um die Protokolle DHCP/BOOTP/RARP zu verwenden, wenden Sie sich bitte an Ihren Netzwerkadministrator.

APIPA

Wenn Sie die IP-Adresse nicht manuell (über das Funktionstastenfeld des Gerätes oder mit Hilfe der BRAdmin-Software) oder automatisch (mit einem DHCP/BOOTP/RARP-Server) zuweisen, vergibt das APIPA-Protokoll (Automatic Private IP Addressing) automatisch eine IP-Adresse aus dem Bereich von 169.254.1.0 bis 169.254.254.255.

ARP

ARP (Address Resolution Protocol) übernimmt in einem TCP/IP-Netzwerk die Zuordnung einer IP-Adresse zu einer MAC-Adresse.

DNS-Client

Der Brother PrintServer unterstützt die DNS-Client-Funktion (DNS: Domain Name System). Dadurch kann der PrintServer mit anderen Geräten Daten austauschen, indem er sie mit ihrem DNS-Namen anspricht.

NetBIOS-Namensauflösung

Die NetBIOS-Namensauflösung (Network Basic Input/Output System) ermöglicht es, während einer bestehenden Netzwerkverbindung die IP-Adresse des anderen Gerätes über die Verwendung seines NetBIOS-Namens zu erhalten.

WINS

Windows® Internet Name Service ist ein Dienst, der Informationen für die NetBIOS-Namensauflösung liefert, indem er eine IP-Adresse einem NetBIOS-Namen des lokalen Netzwerkes zuordnet.

LPR/LPD

Häufig verwendete Druckprotokolle innerhalb eines TCP/IP-Netzwerkes.

SMTP-Client

Ein SMTP-Client (Simple Mail Transfer Protocol) wird zum Versenden von E-Mails über das Internet oder Intranet verwendet.

Custom Raw Port (Standardeinstellung ist Port 9100)

Ein weiteres häufig verwendetes Druckprotokoll innerhalb von TCP/IP-Netzwerken. Es ermöglicht die interaktive Datenübertragung.

IPP

Mit dem Internet Printing-Protokoll können Dokumente über das Internet direkt auf jedem erreichbaren Gerät ausgedruckt werden.

HINWEIS

Einzelheiten zum IPPS-Protokoll finden Sie unter *Sicherheitsprotokolle* ►► Seite 140.

mDNS

Mit mDNS kann sich der Brother PrintServer automatisch für den Betrieb in einer Mac OS X-Umgebung mit einfacher Netzwerkkonfiguration konfigurieren.

TELNET

Mit dem TELNET-Protokoll können Sie die entfernten Netzwerkgeräte in einem TCP/IP-Netzwerk von Ihrem Computer aus steuern.

SNMP

Das SNMP-Protokoll (Simple Network Management Protocol) wird für die Verwaltung von Netzwerkgeräten verwendet, wie z. B. Computer, Router und netzwerkfähige Brother-Geräte. Der Brother PrintServer unterstützt SNMPv1, SNMPv2c und SNMPv3.

HINWEIS

Einzelheiten zum SNMPv3-Protokoll finden Sie unter *Sicherheitsprotokolle* ►► Seite 140.

LLMNR

Das LLMNR-Protokoll (Link-Local Multicast Name Resolution) löst die Namen benachbarter Computer auf, falls im Netzwerk kein DNS-Server (Domain Name System) vorhanden ist. Die LLMNR-Responder-Funktion arbeitet in einer IPv4- und IPv6-Umgebung, wenn ein Computer mit LLMNR-Sender-Funktion, z. B. mit Windows Vista®, Windows® 7 und Windows® 8, verwendet wird.

Web Services

Mit dem Web Services-Protokoll können unter Windows Vista®, Windows® 7 oder Windows® 8 die zum Drucken und Scannen verwendeten Treiber mit einem Rechtsklick auf das Gerätesymbol im Ordner **Netzwerk** installiert werden. (Siehe *Installieren von Treibern zum Drucken und Scannen über Web Services* (Windows Vista®, Windows® 7 und Windows® 8) ►► Seite 134.) Einzelheiten zum Scannen mit Web Services: ►► Software-Handbuch. Mit Web Services können Sie auch von Ihrem Computer aus den aktuellen Status Ihres Gerätes prüfen.

HTTP

Das HTTP-Protokoll wird zur Übermittlung von Daten zwischen einem Webserver und einem Webbrowser verwendet.

HINWEIS

Einzelheiten zum HTTPS-Protokoll finden Sie unter *Sicherheitsprotokolle* ►► Seite 140.

FTP (für die Scan-to-FTP-Funktion)

Das FTP-Protokoll (File Transfer Protocol, Dateiübertragungsprotokoll) ermöglicht es dem Brother-Gerät, gescannte Schwarzweiß- oder Farbdokumente direkt an einen FTP-Server zu senden, der sich lokal in Ihrem Netzwerk oder im Internet befindet.

SNTP

Das SNTP-Protokoll (Simple Network Time Protocol) wird zur Synchronisation der Systemzeit von Computern in einem TCP/IP-Netzwerk verwendet. Sie können die SNTP-Einstellungen über Web Based Management (Webbrowser) konfigurieren. (Weitere Details dazu finden Sie unter *Synchronisieren mit SNTP-Server* ►► Seite 64.)

CIFS

CIFS (Common Internet File System) ist das Standardverfahren, das Computernutzer zur gemeinsamen Verwendung von Dateien und Druckern unter Windows® verwenden.

IPv6

IPv6 ist die neue Generation von Internetprotokollen. Weitere Informationen zum IPv6-Protokoll finden Sie auf der Website für Ihr Gerät unter <http://solutions.brother.com/>.

IP-Adressen, Subnetzmasken und Gateways

Um ein Gerät in einer vernetzten TCP/IP-Umgebung zu verwenden, müssen Sie die IP-Adresse und Subnetzmaske konfigurieren. Die dem PrintServer zugewiesene IP-Adresse muss zum selben logischen Netzwerk gehören wie Ihre Hostcomputer. Ist dies nicht der Fall, müssen Sie die Subnetzmaske und Gateway-Adresse richtig konfigurieren.

IP-Adresse

Eine IP-Adresse ist eine Zahlenfolge, die jedes mit dem Netzwerk verbundene Gerät identifiziert. Eine IP-Adresse besteht aus vier Zahlen, die durch Punkte voneinander getrennt sind. Jede Zahl liegt im Bereich von 0 bis 255.

■ Beispiel: In einem kleinen Netzwerk werden in der Regel die letzten Zahlen geändert.

- 192.168.1.1
- 192.168.1.2
- 192.168.1.3

So wird die IP-Adresse Ihrem Drucker zugewiesen:

Wenn ein DHCP/BOOTP/RARP-Server in Ihrem Netzwerk vorhanden ist, erhält der PrintServer seine IP-Adresse automatisch von diesem Server.

HINWEIS

In kleineren Netzwerken kann auch der Router als DHCP-Server dienen.

Weitere Informationen zu DHCP, BOOTP und RARP finden Sie unter

Konfigurieren der IP-Adresse mit DHCP ►► Seite 144.

Konfigurieren der IP-Adresse mit BOOTP ►► Seite 146.

Konfigurieren der IP-Adresse mit RARP ►► Seite 145.

Wenn Sie keinen DHCP/BOOTP/RARP-Server verwenden, weist das APIPA-Protokoll (Automatic Private IP Addressing) automatisch eine IP-Adresse zwischen 169.254.1.0 und 169.254.254.255 zu. Weitere Informationen zu APIPA finden Sie unter *Konfigurieren der IP-Adresse mit APIPA* ►► Seite 146.

Subnetzmaske

Eine Subnetzmaske schränkt die Netzwerkkommunikation ein.

■ Beispiel: Computer 1 kann Daten mit Computer 2 austauschen

- Computer 1

IP-Adresse: 192.168. 1. 2

Subnetzmaske: 255.255.255.0

- Computer 2

IP-Adresse: 192.168. 1. 3

Subnetzmaske: 255.255.255.0

0 in der Subnetzmaske bedeutet, dass bei diesem Teil der Adresse die Kommunikation nicht eingeschränkt ist. Im Beispiel oben kann daher mit jedem Gerät kommuniziert werden, das eine IP-Adresse hat, die mit 192.168.1.x. beginnt (wobei x. für eine Zahl zwischen 0 und 255 steht).

Gateway (und Router)

Ein Gateway ist eine Einrichtung im Netzwerk, die als Zugang zu einem anderen Netzwerk dient und über das Netzwerk übertragene Daten an einen bestimmten Ort übermittelt. Der Router weiß, wohin die Daten geleitet werden müssen, die am Gateway eintreffen. Falls sich ein Zielort in einem externen Netzwerk befindet, überträgt der Router die Daten zum externen Netzwerk. Wenn Ihr Netzwerk mit anderen Netzwerken kommuniziert, müssen Sie eventuell die Gateway-IP-Adresse konfigurieren. Falls Sie die Gateway-IP-Adresse nicht kennen, wenden Sie sich an Ihren Netzwerkadministrator.

IEEE 802.1x-Authentifizierung

IEEE 802.1x ist ein IEEE-Standard für verkabelte und kabellose Netzwerke, der den Zugriff von nicht autorisierten Netzwerkgeräten beschränkt. Ihr Brother-Gerät (Supplicant) sendet über Ihren Access Point (Authentifikator) eine Authentifizierungsanforderung an einen RADIUS-Server (Authentifizierungsserver). Nachdem die Anforderung durch den RADIUS-Server verifiziert, d. h. überprüft und bestätigt, wurde, kann Ihr Gerät auf das Netzwerk zugreifen.

Authentifizierungsmethoden

■ LEAP (für Wireless-Netzwerke)

Das Cisco LEAP-Protokoll (Lightweight Extensible Authentication Protocol) wurde von Cisco Systems Inc. entwickelt. Es verwendet zur Authentifizierung eine Benutzer-ID sowie ein Kennwort.

■ EAP-FAST

Das EAP-FAST-Protokoll (Extensible Authentication Protocol-Flexible Authentication via Secured Tunneling) wurde von Cisco Systems Inc. entwickelt. Es verwendet zur Authentifizierung eine Benutzer-ID sowie ein Kennwort und symmetrische Schlüsselalgorithmen zur Authentifizierung über einen Tunnel.

Das Brother-Gerät unterstützt die folgenden inneren Authentifizierungsmethoden:

- EAP-FAST/NONE
- EAP-FAST/MS-CHAPv2
- EAP-FAST/GTC

■ EAP-MD5 (für verkabelte Netzwerke)

EAP-MD5 (Extensible Authentication Protocol-Message Digest Algorithm 5) verwendet eine Benutzer-ID und ein Kennwort für eine Challenge-Response-Authentifizierung (Anfrage-Antwort-Authentifizierung).

■ PEAP

PEAP (Protected Extensible Authentication Protocol) wurde von Microsoft Corporation, Cisco Systems und RSA Security entwickelt. PEAP erzeugt zum Senden einer Benutzer-ID und eines Kennwortes einen verschlüsselten SSL/TLS-Tunnel (Secure Sockets Layer/Transport Layer Security) zwischen einem Client und einem Authentifizierungsserver. PEAP ermöglicht eine gegenseitige Authentifizierung von Server und Client.

Das Brother-Gerät unterstützt die folgenden inneren Authentifizierungen:

- PEAP/MS-CHAPv2
- PEAP/GTC

■ EAP-TTLS

EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security) wurde von Funk Software und Certicom entwickelt. EAP-TTLS erzeugt zwischen einem Client und einem Authentifizierungsserver einen ähnlichen verschlüsselten SSL-Tunnel wie PEAP zum Senden einer Benutzer-ID und eines Kennwortes. EAP-TTLS ermöglicht eine gegenseitige Authentifizierung von Server und Client.

Das Brother-Gerät unterstützt die folgenden inneren Authentifizierungen:

- EAP-TTLS/CHAP
- EAP-TTLS/MS-CHAP
- EAP-TTLS/MS-CHAPv2
- EAP-TTLS/PAP

■ EAP-TLS

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) erfordert eine Authentifizierung über ein digitales Zertifikat sowohl beim Client als auch beim Authentifizierungsserver.

Bedingungen und Konzepte für WLAN-Netzwerke (Für HL-3180CDW, DCP-9015CDW, DCP-9017CDW, DCP-9020CDW, DCP-9022CDW, MFC-9130CW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW)

Festlegen Ihres Netzwerks

SSID (Service Set Identifier) und Kanäle

Sie müssen den SSID-Namen und einen Kanal konfigurieren, um das Wireless-Netzwerk, zu dem eine Verbindung hergestellt werden soll, festzulegen.

■ SSID

Jedes Wireless-Netzwerk hat einen eigenen, eindeutigen Netzwerknamen, eine so genannte SSID. Die SSID ist ein bis zu 32 Byte großer Wert, der dem Access Point zugewiesen wird. Wireless-Netzwerkgeräte, die Sie dem Wireless-Netzwerk zuordnen möchten, müssen dem Access Point entsprechend eingestellt sein. Der Access Point und die Wireless-Netzwerkgeräte senden in regelmäßigen Abständen Wireless-Datenpakete (so genannte Beacons), welche die SSID-Informationen enthalten. Wenn Ihr Wireless-Netzwerkgerät ein Beacon empfängt, kann darüber festgestellt werden, welches Wireless-Netzwerk nahe genug ist, damit seine Funkwellen Ihr Gerät erreichen.

■ Kanäle

Wireless-Netzwerke verwenden Kanäle. Jeder Wireless-Kanal liegt auf einer anderen Frequenz. In einem Wireless-Netzwerk können bis zu 14 verschiedene Kanäle genutzt werden. Allerdings ist die Anzahl der verfügbaren Kanäle in vielen Ländern beschränkt.

Sicherheitsbegriffe

Authentifizierung und Verschlüsselung

In den meisten Wireless-Netzwerken werden Sicherheitseinstellungen verwendet. Diese Sicherheitseinstellungen legen die Art der Authentifizierung (wie sich das Gerät im Netzwerk anmeldet) und die Art der Verschlüsselung (wie die Daten zum Versenden im Netzwerk verschlüsselt werden) fest. **Wenn Sie diese Einstellungen bei der Konfiguration Ihres Brother Wireless-Geräts nicht richtig vornehmen, kann sich das Gerät nicht mit dem Wireless-Netzwerk verbinden.** Gehen Sie deshalb besonders sorgfältig vor, wenn Sie diese Einstellungen konfigurieren. Unter *Unterstützte Protokolle und Sicherheitsfunktionen* >> Seite 143 finden Sie die für Ihr Brother-Wireless-Gerät unterstützten Authentifizierungs- und Verschlüsselungsmethoden.

Authentifizierungs- und Verschlüsselungsmethoden für ein privates kabelloses Netzwerk

Ein privates Wireless-Netzwerk ist ein kleines Netzwerk, zum Beispiel wenn Sie Ihr Gerät in einem Wireless-Netzwerk zu Hause ohne IEEE 802.1x-Unterstützung verwenden.

Wenn Sie Ihr Gerät in einem Wireless-Netzwerk mit IEEE 802.1x-Unterstützung verwenden möchten, lesen Sie *Authentifizierungs- und Verschlüsselungsmethoden für Wireless-Unternehmensnetzwerke*

➤➤ Seite 132.

Authentifizierungsmethoden

■ Open system (offenes System)

Wireless-Geräte können ohne Authentifizierung auf das Netzwerk zugreifen.

■ Shared Key

Ein geheimer, vordefinierter Schlüssel wird von allen Geräten verwendet, die auf das Wireless-Netzwerk zugreifen.

Das Brother Wireless-Gerät verwendet den WEP-Schlüssel als vordefinierten Schlüssel.

■ WPA-PSK/WPA2-PSK

Aktiviert einen Wi-Fi Protected Access™ Pre-Shared Key (WPA-PSK/WPA2-PSK), einen gemeinsamen vordefinierten Schlüssel, der dem Brother Wireless-Gerät den Zugriff auf Access Points mit TKIP für WPA-PSK oder AES für WPA-PSK und WPA2-PSK (WPA-Personal) ermöglicht.

Verschlüsselungsmethoden

■ Keine

Die Daten werden nicht verschlüsselt.

■ WEP

Bei Verwendung von WEP (Wired Equivalent Privacy) werden die Daten mit einem Sicherheitsschlüssel gesendet und empfangen.

■ TKIP

TKIP (Temporal Key Integrity Protocol) ist eine Kombination aus einer Datenintegritätsprüfung und einem Neuverschlüsselungsverfahren pro Datenpaket.

■ AES

AES (Advanced Encryption Standard) bietet eine höhere Datensicherheit durch Verwendung eines symmetrischen Verschlüsselungsschlüssels.

HINWEIS

- IEEE 802.11n unterstützt als Verschlüsselungsmethode nicht WEP oder TKIP.
 - Wenn Sie mit IEEE 802.11n eine Verbindung zu Ihrem Wireless-Netzwerk herstellen möchten, empfehlen wir, AES zu wählen.
-

Netzwerkschlüssel

■ Open System/Shared Key mit WEP

Dieser Schlüssel ist ein 64-Bit- oder 128-Bit-Wert, der im ASCII- oder Hexadezimal-Format eingegeben werden muss.

- 64 (40) Bit (ASCII):

Verwendet 5 Textzeichen, z. B. „WSLAN“ (Groß-/Kleinschreibung beachten)

- 64 (40) Bit (Hexadezimal):

Verwendet 10-stellige Hexadezimal-Daten, z. B. „71f2234aba“

- 128 (104) Bit (ASCII):

Verwendet 13 Textzeichen, z. B. „Wirelesscomms“ (Groß-/Kleinschreibung beachten)

- 128 (104) Bit (Hexadezimal):

Verwendet 26-stellige Hexadezimal-Daten, z. B. „71f2234ab56cd709e5412aa2ba“

■ WPA-PSK/WPA2-PSK und TKIP oder AES

Verwendet einen Pre-Shared-Schlüssel (PSK) von mindestens 8 und höchstens 63 Zeichen Länge.

Authentifizierungs- und Verschlüsselungsmethoden für Wireless-Unternehmensnetzwerke

Ein Wireless-Unternehmensnetzwerk ist ein großes Netzwerk. Dies ist zum Beispiel der Fall, wenn Ihr Gerät in einem Unternehmen an ein Wireless-Netzwerk mit IEEE 802.1x-Unterstützung angeschlossen ist. Wenn Sie Ihr Gerät für ein Wireless-Netzwerk mit IEEE 802.1x-Unterstützung konfigurieren, können Sie die folgenden Authentifizierungs- und Verschlüsselungsmethoden verwenden.

Authentifizierungsmethoden

■ LEAP

Zu LEAP siehe *LEAP (für Wireless-Netzwerke)* >> Seite 128.

■ EAP-FAST

Zu EAP-FAST siehe *EAP-FAST* >> Seite 128.

■ PEAP

Zu PEAP siehe *PEAP* >> Seite 128.

■ EAP-TTLS

Zu EAP-TTLS siehe *EAP-TTLS* >> Seite 129.

■ EAP-TLS

Zu EAP-TLS siehe *EAP-TLS* >> Seite 129.

Verschlüsselungsmethoden

■ TKIP

Zu TKIP siehe *TKIP* >> Seite 131.

■ AES

Zu AES siehe *AES* >> Seite 131.

■ CKIP

Das original CKIP-Protokoll (Cisco Key Integrity Protocol) für LEAP von Cisco Systems Inc.

Benutzer-ID und Kennwort

Die folgenden Sicherheitsmethoden verwenden eine Benutzer-ID mit einer Länge von weniger als 64 Zeichen und ein Kennwort mit einer Länge von weniger als 32 Zeichen.

■ LEAP

■ EAP-FAST

■ PEAP

■ EAP-TTLS

■ EAP-TLS (für Benutzer-ID)

Arten von zusätzlichen Netzwerkeinstellungen

Die folgenden Funktionen stehen zum Konfigurieren zusätzlicher Netzwerkeinstellungen zur Verfügung.

- Web Services zum Drucken und Scannen (Windows Vista®, Windows® 7 und Windows® 8)
- Vertical Pairing (Windows® 7 und Windows® 8)

HINWEIS

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

Installieren von Treibern zum Drucken und Scannen über Web Services (Windows Vista®, Windows® 7 und Windows® 8)

Über die Funktion Web Services können Sie Geräte im Netzwerk überwachen. Sie vereinfacht außerdem den Treiberinstallationsprozess. (Einzelheiten zum Scannen mit Web Services: >> Software-Handbuch.)

HINWEIS

- Bevor Sie diese Einstellung vornehmen, müssen Sie die IP-Adresse Ihres Gerätes konfigurieren.
- Für Windows Server® 2008/2012 müssen Sie Print Services installieren.

- 1 Legen Sie die CD-ROM mit dem Installationsprogramm ein.
- 2 Wählen Sie Ihr CD-ROM-Laufwerk/**install/driver/gdi/32_64**.
- 3 Doppelklicken Sie auf **dpinst86.exe** oder **dpinst64.exe**.

HINWEIS

Wenn das Fenster **Benutzerkontensteuerung** erscheint:

(Windows Vista®) Klicken Sie auf **Zulassen**.

(Windows® 7/Windows® 8) Klicken Sie auf **Ja**.

4 (Windows Vista®)

Klicken Sie auf  und wählen Sie dann **Netzwerk**.

(Windows® 7)

Klicken Sie auf , **Systemsteuerung, Netzwerk und Internet** und dann **Netzwerkcomputer und -geräte anzeigen**.

(Windows® 8)

Ziehen Sie Ihre Maus in die untere rechte Ecke Ihres Desktops. Wenn die Menüleiste erscheint, klicken Sie auf **Einstellungen**, klicken Sie auf **PC-Einstellungen ändern** und klicken Sie dann auf **Geräte**.

5 (Windows Vista®/Windows® 7)

Der Web Services-Name des Gerätes wird mit dem Druckersymbol angezeigt. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie installieren möchten.

(Windows® 8)

Klicken Sie auf **Gerät hinzufügen**. Der Web Services-Name des Geräts wird angezeigt.

HINWEIS

- Der Web Services-Name für das Brother-Gerät sind die Modellbezeichnung und die MAC-Adresse (Ethernet-Adresse) Ihres Geräts (z. B. Brother MFC-XXXX (Modellbezeichnung) [XXXXXXXXXXXXX] (MAC-Adresse / Ethernet-Adresse).)

- (Windows® 8)

Ziehen Sie Ihre Maus über den Namen des Geräts, um die Geräteinformationen anzuzeigen.

6 (Windows Vista®/Windows® 7)

Klicken Sie im Pulldown-Menü auf **Installieren**.

(Windows® 8)

Doppelklicken Sie auf das Gerät, das Sie installieren möchten.

Deinstallieren von Treibern zum Drucken und Scannen über Web Services (Windows Vista®, Windows® 7 und Windows® 8)

Um Web Services von einem Computer zu deinstallieren gehen Sie wie folgt vor.

- 1 (Windows Vista®)
Klicken Sie auf  und wählen Sie dann **Netzwerk**.
(Windows® 7)
Klicken Sie auf , **Systemsteuerung, Netzwerk und Internet** und dann auf **Netzwerkcomputer und -geräte anzeigen**.
(Windows® 8)
Ziehen Sie Ihre Maus in die untere rechte Ecke Ihres Desktops. Wenn die Menüleiste erscheint, klicken Sie auf **Einstellungen**, klicken Sie auf **PC-Einstellungen ändern** und klicken Sie dann auf **Geräte**.
- 2 (Windows Vista®/Windows® 7)
Der Web Services-Name des Gerätes wird mit dem Druckersymbol angezeigt. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie deinstallieren möchten.
(Windows® 8)
Der Web Service-Name des Geräts wird angezeigt. Wählen Sie das Gerät aus, das deinstalliert werden soll, und klicken Sie dann neben dem Gerätenamen auf .
- 3 (Windows Vista®/Windows® 7)
Klicken Sie im Pulldown-Menü auf **Deinstallieren**.
(Windows® 8)
Wenn das Dialogfeld angezeigt wird, klicken Sie auf **Entfernen**.

Netzwerkdruck- und -Scan-Installation für den Infrastruktur-Modus bei der Nutzung von Vertical Pairing (Windows® 7 und Windows® 8)

Windows® Vertical Pairing ist eine Technologie, mit der sich Ihr Wireless-Gerät, das diese Funktion unterstützt, mit Ihrem Infrastruktur-Netzwerk über das PIN-Verfahren des WPS und der Web Services-Funktion verbinden kann. Außerdem ermöglicht diese Funktion die Drucker- und Scannertreiber-Installation über das Multifunktionsdrucker-Symbol, das Sie im Bildschirm **Gerät hinzufügen** finden.

Sie können Ihr Gerät im Infrastruktur-Modus im Wireless-Netzwerk anschließen und dann mit dieser Funktion den Druckertreiber installieren. Gehen Sie dazu wie folgt vor:

HINWEIS

- Wenn Sie die Web Services-Funktion Ihres Gerätes ausgeschaltet haben, müssen Sie sie wieder einschalten. Die Standardeinstellung für die Web Services Ihres Brother-Gerätes ist Ein. Sie können die Web Services-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 oder Windows® 8 gekennzeichnet ist. Wenn Sie sich in Bezug auf das Kompatibilitätslogo nicht sicher sind, wenden Sie sich an den Hersteller Ihres Access Points/Router.
- Vergewissern Sie sich, dass Ihr Computer mit dem Kompatibilitätslogo für Windows® 7 oder Windows® 8 gekennzeichnet ist. Wenn Sie sich in Bezug auf das Kompatibilitätslogo nicht sicher sind, wenden Sie sich an den Hersteller Ihres Computers.
- Wenn Sie Ihr Wireless-Netzwerk mit Hilfe einer externen Wireless-Netzwerkkarte (NIC, Network Interface Card) konfigurieren, vergewissern Sie sich, dass diese Netzwerkkarte mit dem Kompatibilitätslogo für Windows® 7 oder Windows® 8 gekennzeichnet ist. Weitere Informationen erhalten Sie beim Hersteller der Wireless-Netzwerkkarte.
- Um einen Computer mit Windows® 7 oder Windows® 8 als Registrar zu verwenden, muss dieser zuvor in Ihrem Netzwerk registriert werden. Lesen Sie die Anleitung, die mit Ihrem WLAN Access Point/Router geliefert wurde.

- 1 Schalten Sie Ihr Gerät ein.
- 2 Stellen Sie am Gerät den WPS-Modus (PIN-Verfahren) ein.
Für Informationen zur Konfiguration Ihres Geräts zur Verwendung der PIN-Methode siehe *Konfiguration mit der PIN-Methode des WPS (Wi-Fi Protected Setup)* >> Seite 29.
- 3 (Windows® 7)
Klicken Sie auf die Schaltfläche  und dann auf **Geräte und Drucker**.
(Windows® 8)
Ziehen Sie Ihre Maus in die untere rechte Ecke Ihres Desktops. Wenn die Menüleiste erscheint, klicken Sie auf **Einstellungen** und dann auf **Systemsteuerung**. Klicken Sie in der Gruppe **Hardware und Sound** auf **Geräte und Drucker anzeigen**.
- 4 (Windows® 7)
Wählen Sie **Gerät hinzufügen** im Dialogfeld **Geräte und Drucker**.
(Windows® 8)
Klicken Sie in der Befehlsleiste auf **Gerät hinzufügen**.
- 5 Wählen Sie Ihr Gerät und geben Sie die von Ihrem Gerät angezeigte PIN ein.
- 6 Wählen Sie das Infrastruktur-Netzwerk, zu dem Sie eine Verbindung herstellen möchten, und klicken Sie dann auf **Weiter**.
- 7 Wenn Ihr Gerät im Dialogfeld **Geräte und Drucker** angezeigt wird, sind die Wireless-Konfiguration und die Druckertreiberinstallation erfolgreich abgeschlossen.

Sicherheitsfunktionen

Sicherheitsbegriffe

■ CA (Certificate Authority, Zertifizierungsstelle)

Die Zertifizierungsstelle stellt digitale Zertifikate aus (vor allem X.509 Zertifikate) und gewährleistet die Bindung zwischen den Datenpaketen in einem Zertifikat.

■ CSR (Certificate Signing Request, Zertifikatsignieranforderung)

Mit der Zertifikatsignieranforderung wird bei der Zertifizierungsstelle die Ausstellung eines Zertifikats beantragt. Die Zertifikatsregistrierungsanforderung enthält Informationen zur Identifizierung des Antragstellers, einen vom Antragsteller generierten öffentlichen Schlüssel (den Public Key) sowie die digitale Signatur des Antragstellers.

■ Zertifikat

Ein Zertifikat verbindet einen Public Key mit einer bestimmten Identität. Mit dem Zertifikat kann überprüft bzw. bestätigt werden, dass ein Public Key zu einer bestimmten Person gehört. Sein Format ist im x.509-Standard festgelegt.

■ CA-Zertifikat

Ein CA-Zertifikat identifiziert die Zertifizierungsstelle (CA) und verfügt über einen eigenen privaten Schlüssel. Es verifiziert ein von der Zertifizierungsstelle ausgegebenes Zertifikat.

■ Digitale Signatur

Die digitale Signatur ist ein Wert, der mit einem kryptografischen Algorithmus berechnet und so an ein Datenobjekt angehängt wird, dass der Datenempfänger die Herkunft und Identität der Daten anhand der Signatur überprüfen kann.

■ Public-Key-Kryptosystem

Das Public-Key-Kryptosystem ist ein moderner Zweig der Kryptografie, bei dem die Algorithmen auf ein Schlüsselpaar (einen Public Key und einen Private Key) angewendet werden. Für die verschiedenen Rechenschritte des Algorithmus wird jeweils auf eine andere Komponente des Schlüsselpaares zugegriffen.

■ Shared-Key-Kryptosystem

Das Shared-Key-Kryptosystem ist ein Zweig der Kryptografie, bei dem der gleiche Schlüssel für zwei verschiedene Rechenschritte des Algorithmus verwendet wird, z. B. zur Verschlüsselung und Entschlüsselung.

Sicherheitsprotokolle

SSL (Secure Socket Layer)/TLS (Transport Layer Security)

Diese Protokolle zur sicheren Kommunikation verschlüsseln die Daten, um vor Übergriffen zu schützen.

HTTPS

Die Version des Internetprotokolls HTTP (Hyper Text Transfer Protocol), die SSL verwendet.

IPPS

Die Version des Internet Printing-Protokolls, die SSL verwendet.

SNMPv3

SNMPv3 (Simple Network Management Protocol, Version 3) stellt Benutzerauthentifizierung und Datenverschlüsselung für eine sichere Verwaltung von Netzwerkgeräten zur Verfügung.

Sicherheitsmethoden für das Senden und Empfangen von E-Mails

HINWEIS

Sie können die Einstellungen für die Sicherheitsmethoden über das Web Based Management (Webbrowser) konfigurieren. Weitere Details dazu finden Sie unter *So konfigurieren Sie die Geräteeinstellungen über Web Based Management (Webbrowser)* ►► Seite 58.

POP vor SMTP (PvS)

Dies ist eine Methode zur Benutzerauthentifizierung beim Senden von E-Mails über einen Client. Vor dem Senden einer E-Mail spricht der Client erst den POP3-Server an und erhält dadurch die Erlaubnis für den Zugriff auf den SMTP-Server.

SMTP-AUTH (SMTP-Authentifizierung)

SMTP-AUTH erweitert SMTP (das Internetprotokoll für den E-Mail-Versand) um eine Authentifizierungsmethode, die gewährleistet, dass die Identität des Senders bekannt ist.

APOP (Authenticated Post Office Protocol)

APOP erweitert POP3 (das Internet-E-Mail-Empfangsprotokoll) um eine Authentifizierungsmethode, die das Kennwort verschlüsselt, wenn der Client eine E-Mail empfängt.

SMTP über SSL

SMTP über SSL ermöglicht das Senden von verschlüsselten E-Mails unter Verwendung von SSL.

POP über SSL

POP über SSL ermöglicht das Empfangen von verschlüsselten E-Mails unter Verwendung von SSL.



Anhänge

Anhang A	143
Anhang B	144

Unterstützte Protokolle und Sicherheitsfunktionen

Schnittstelle	Ethernet ³	10BASE-T, 100BASE-TX
	Wireless ¹	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, LLMNR-Responder, LPR/LPD, Custom Raw Port/Port9100, IPP/IPPS, FTP-Client und -Server, TELNET-Server, HTTP/HTTPS-Server, TFTP-Client und -Server, POP3 ² , SMTP-Client, SNMPv1/v2c/v3, ICMP, Web Services (Drucken/Scannen), CIFS-Client, SNTTP-Client
	Protokoll (IPv6)	NDP, RA, DNS-Resolver, mDNS, LLMNR-Responder, LPR/LPD, Custom Raw Port/Port9100, IPP/IPPS, FTP-Client und -Server, TELNET-Server, HTTP/HTTPS-Server, TFTP-Client und -Server, POP3 ² , SMTP-Client, SNMPv1/v2c, ICMPv6, Web Services (Drucken/Scannen), CIFS-Client, SNTTP-Client
Netzwerk (Sicherheit)	Verkabelt ³	SSL/TLS (IPPS, HTTPS), SNMP v3, 802.1x (EAP-MD5, EAP-FAST, PEAP, EAP-TLS, EAP-TTLS), Kerberos
	Wireless ¹	WEP 64/128 Bit, WPA-PSK (TKIP/AES), WPA2-PSK (AES), SSL/TLS (IPPS, HTTPS), SNMP v3, 802.1x (LEAP, EAP-FAST, PEAP, EAP-TLS, EAP-TTLS), Kerberos
E-Mail (Sicherheit)	Verkabelt ³ und Wireless ¹	APOP, POP vor SMTP, SMTP-AUTH, SSL/TLS (SMTP/POP)
Netzwerk (Wireless)¹	Wireless-Zertifizierung	Wi-Fi Certification Mark-Lizenz (WPA™/WPA2™ - Enterprise, Personal), Wi-Fi Protected Setup™ (WPS) Identifier Mark-Lizenz, AOSS Logo, Wi-Fi CERTIFIED™ Wi-Fi Direct™

¹ Für HL-3180CDW, DCP-9015CDW, DCP-9017CDW, DCP-9020CDW, DCP-9022CDW, MFC-9130CW, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW

² Für MFC-9130CW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW: als Download verfügbar.

³ Für DCP-9020CDN, DCP-9020CDW, DCP-9022CDW, MFC-9140CDN, MFC-9142CDN, MFC-9330CDW, MFC-9332CDW, MFC-9340CDW und MFC-9342CDW

Dienste verwenden

Ein Dienst oder Service ist eine Ressource, auf die Computer, die über den Brother PrintServer drucken wollen, zugreifen können. Der Brother PrintServer stellt die folgenden vordefinierten Dienste bereit (mit dem Befehl `SHOW SERVICE` in der Remotekonsole des Brother PrintServers kann eine Liste der verfügbaren Dienste abgerufen werden): Geben Sie an der Eingabeaufforderung `HELP` ein, um eine Liste der unterstützten Befehle anzuzeigen.

Service (Beispiel)	Definition
BINARY_P1	TCP/IP-Binär
TEXT_P1	TCP/IP-Textservice (fügt am Ende jeder Zeile einen Wagenrücklauf ein)
PCL_P1	PCL-Service (schaltet PJL-kompatible Geräte in den PCL-Modus)
BRNxxxxxxxxxxxx	TCP/IP-Binär
BRNxxxxxxxxxxxx_AT	PostScript®-Service für Macintosh
POSTSCRIPT_P1	PostScript®-Service (schaltet PJL-kompatible Geräte in den PostScript®-Modus)

Dabei steht „xxxxxxxxxxxx“ für die MAC-Adresse Ihres Geräts (Ethernet-Adresse).

Weitere Möglichkeiten, die IP-Adresse einzustellen (für fortgeschrittene Benutzer und Administratoren)

Konfigurieren der IP-Adresse mit DHCP

Das Dynamic Host Configuration Protocol (DHCP) ist einer von mehreren automatisierten Mechanismen zur Zuweisung von IP-Adressen. Wenn ein DHCP-Server in Ihr Netzwerk eingebunden ist, erhält der PrintServer seine IP-Adresse automatisch vom DHCP-Server und sein Name wird bei allen mit RFC 1001 und 1002 kompatiblen dynamischen Namensdiensten registriert.

HINWEIS

Wenn Sie Ihren MFC/DCP-Server nicht über DHCP konfigurieren möchten, müssen Sie die Boot-Methode auf Statisch setzen, damit der MFC/DCP-Server eine feste IP-Adresse erhält. Dies verhindert, dass der PrintServer versucht, eine IP-Adresse von einem dieser Systeme zu erhalten. Um die Boot-Methode zu ändern, verwenden Sie das Netzwerkmenü des Funktionstastenfelds Ihres Geräts, die BRAdmin-Anwendungen, Remote Setup (für MFC-Modelle) oder Web Based Management (Webbrowser).

Konfigurieren der IP-Adresse mit RARP

Vor der Konfiguration der IP-Adresse über RARP müssen Sie die Boot-Methode des Geräts auf RARP setzen. Um die Boot-Methode zu ändern, verwenden Sie das Netzwerkmenü des Funktionstastenfelds Ihres Geräts, die BRAdmin-Anwendungen, Remote Setup (für MFC-Modelle) oder Web Based Management (Webbrowser).

Die IP-Adresse des Brother PrintServers kann auch mit der Funktion Reverse ARP (RARP) auf Ihrem Hostcomputer konfiguriert werden. Dazu wird die Datei `/etc/ethers` mit einem Eintrag wie dem Folgenden versehen (wenn diese Datei nicht vorhanden ist, können Sie diese erzeugen):

```
00:80:77:31:01:07    BRN008077310107 (oder BRW008077310107 für ein Wireless-Netzwerk)
```

Wobei der erste Eintrag die MAC-Adresse (Ethernet-Adresse) des PrintServers ist und der zweite Eintrag der Name des PrintServers (dies muss derselbe Name sein, der auch in der Datei `/etc/hosts` angegeben wurde).

Starten Sie den RARP-Daemon, falls er nicht bereits ausgeführt wird (der entsprechende Befehl kann je nach System `rarpd`, `rarpd -a`, `in.rarpd -a` oder ein anderer Befehl sein; geben Sie `man rarpd` ein oder suchen Sie in Ihrer Systemdokumentation nach weiteren Informationen). Geben Sie bei einem Berkeley UNIX-basierten System den folgenden Befehl ein, um zu überprüfen, ob der RARP-Dämon läuft:

```
ps -ax | grep -v grep | grep rarpd
```

Bei AT&T UNIX-basierten Systemen geben Sie ein:

```
ps -ef | grep -v grep | grep rarpd
```

Der Brother PrintServer erhält die IP-Adresse vom RARP-Dämon, wenn das Gerät eingeschaltet wird.

Konfigurieren der IP-Adresse mit BOOTP

Vor der Konfiguration der IP-Adresse über BOOTP müssen Sie die Boot-Methode des Gerätes auf BOOTP setzen. Um die Boot-Methode zu ändern, verwenden Sie das Netzwerkmenü des Funktionstastenfelds Ihres Geräts, die BRAdmin-Anwendungen, Remote Setup (für MFC-Modelle) oder Web Based Management (Webbrowser).

BOOTP ist eine Alternative zu RARP mit dem Vorteil, dass mit BOOTP auch die Konfiguration von Subnetzmaske und Gateway möglich ist. Um die IP-Adresse mit BOOTP zu konfigurieren, müssen Sie sich vergewissern, dass BOOTP auf Ihrem Hostcomputer installiert ist und ausgeführt wird. (Es sollte in der Datei `/etc/services` auf Ihrem Host als echter Service erscheinen. Geben Sie `man bootpd` ein oder suchen Sie in Ihrer Systemdokumentation nach weiteren Informationen.) BOOTP wird normalerweise über die Datei `/etc/inetd.conf` gestartet. Sie können es daher gegebenenfalls durch Entfernen des Zeichens „#“ vor dem Bootp-Eintrag in dieser Datei aktivieren. So würde zum Beispiel ein typischer Bootp-Eintrag in der Datei `/etc/inetd.conf` lauten:

```
#bootp dgram udp wait /usr/etc/bootpd bootpd -i
```

Bei manchen Systemen kann dieser Eintrag „bootps“ anstelle von „bootp“ lauten.

HINWEIS

Um BOOTP zu aktivieren, löschen Sie einfach das Zeichen „#“ in einem Editor (ist das Zeichen „#“ nicht vorhanden, dann ist BOOTP bereits aktiviert). Bearbeiten Sie dann die BOOTP-Konfigurationsdatei (normalerweise `/etc/bootptab`) und geben Sie Name, Netzwerktyp (1 für Ethernet), MAC-Adresse (Ethernet-Adresse) und IP-Adresse, Subnetzmaske und Gateway des PrintServers ein. Leider ist das Format dieser Einträge nicht standardisiert. Lesen Sie deshalb in Ihrer Systemdokumentation nach, wie diese Angaben einzutragen sind. (Bei vielen UNIX-Systemen gibt es dafür auch Beispielvorgaben in der `bootptab`-Datei, an denen Sie sich orientieren können.) Hier einige Beispiele für typische `/etc/bootptab`-Einträge: („BRN“ ist „BRW“ bei einem Wireless-Netzwerk.)

```
BRN310107 1 00:80:77:31:01:07 192.168.1.2
```

und:

```
BRN310107:ht=ethernet:ha=008077310107:\ip=192.168.1.2:
```

Manche Implementierungen der BOOTP-Hostsoftware reagieren nicht auf BOOTP-Anfragen, wenn kein Download-Dateiname in der Konfigurationsdatei enthalten ist. Erzeugen Sie in diesem Fall einfach eine Nulldatei auf dem Host und geben Sie den Namen dieser Datei und ihren Pfad in der Konfigurationsdatei an.

Wie bei RARP lädt der PrintServer beim Einschalten des Gerätes seine IP-Adresse vom BOOTP-Server.

Konfigurieren der IP-Adresse mit APIPA

Der Brother PrintServer unterstützt das APIPA-Protokoll (Automatic Private IP Addressing). Mit APIPA konfigurieren DHCP-Clients automatisch eine IP-Adresse und Subnetzmaske, wenn kein DHCP-Server verfügbar ist. Das Gerät wählt seine IP-Adresse aus dem Adressbereich von 169.254.1.0 bis 169.254.254.255. Die Subnetzmaske wird automatisch auf 255.255.0.0 und die Gateway-Adresse auf 0.0.0.0 eingestellt.

Standardmäßig ist das APIPA-Protokoll aktiviert. Sie können das APIPA-Protokoll über das Funktionstastenfeld des Gerätes, mit BRAdmin Light oder Web Based Management (Webbrowser) deaktivieren.

Konfigurieren der IP-Adresse mit ARP

Falls Sie die BRAdmin-Anwendung nicht nutzen können und in Ihrem Netzwerk kein DHCP-Server vorhanden ist, können Sie auch den Befehl ARP verwenden. Der Befehl ARP ist auf Windows®-Systemen, auf denen das TCP/IP-Protokoll installiert ist, und auf UNIX-Systemen verfügbar. Geben Sie zum Verwenden von ARP den folgenden Befehl an der Eingabeaufforderung ein:

```
arp -s ipaddress ethernetaddress
```

```
ping ipaddress
```

Wobei Ethernet-Adresse die MAC-Adresse (Ethernet-Adresse) des PrintServers und ipaddress die IP-Adresse des PrintServers ist. Zum Beispiel:

■ Windows®-Systeme

Windows®-Systeme benötigen einen Bindestrich „-“ zwischen den einzelnen Stellen der MAC-Adresse (Ethernet-Adresse).

```
arp -s 192.168.1.2 00-80-77-31-01-07
```

```
ping 192.168.1.2
```

■ UNIX-/Linux-Systeme

UNIX- und Linux-Systeme benötigen in der Regel einen Doppelpunkt „:“ zwischen den einzelnen Stellen der MAC-Adresse (Ethernet-Adresse).

```
arp -s 192.168.1.2 00:80:77:31:01:07
```

```
ping 192.168.1.2
```

HINWEIS

Der Befehl arp -s kann nur innerhalb des gleichen Ethernet-Segment verwendet werden (d. h. es darf sich kein Router zwischen PrintServer und Betriebssystem befinden).

Ist ein Router vorhanden, können Sie BOOTP oder eine andere in diesem Kapitel beschriebene Methode verwenden, um die IP-Adresse festzulegen. Wenn Ihr Administrator das System für die Zuweisung von IP-Adressen über BOOTP, DHCP oder RARP konfiguriert hat, kann der Brother PrintServer seine IP-Adresse von jedem dieser Dienste beziehen. In diesem Fall müssen Sie den Befehl ARP nicht verwenden. Der ARP-Befehl funktioniert nur einmal. Aus Sicherheitsgründen können Sie den ARP-Befehl nicht verwenden, um die IP-Adresse des Brother PrintServers zu ändern, nachdem diese mit ARP erfolgreich konfiguriert wurde. Der PrintServer ignoriert dann jeden Versuch, dies zu tun. Wenn Sie die IP-Adresse ändern möchten, verwenden Sie dazu das Web Based Management (Webbrowser), TELNET (mit dem Befehl SET IP ADDRESS) oder nehmen Sie einen Reset für den PrintServer auf die werkseitigen Einstellungen vor (danach kann der ARP-Befehl wieder genutzt werden).

Konfigurieren der IP-Adresse über die TELNET-Konsole

Sie können die IP-Adresse auch mit dem Befehl TELNET ändern.

TELNET ist eine effektive Methode zur Änderung der IP-Adresse des Gerätes. Voraussetzung dafür ist allerdings, dass im PrintServer bereits eine gültige IP-Adresse hinterlegt wurde.

Geben Sie an der Eingabeaufforderung `TELNET <Befehlszeile>` ein, wobei `<Befehlszeile>` für die IP-Adresse des PrintServers steht. Wenn die Verbindung hergestellt ist, drücken Sie die Eingabe- oder Enter-Taste, um zur „#“-Eingabeaufforderung zu gelangen. Geben Sie das Kennwort „**access**“ ein. (Das Kennwort wird nicht auf dem Bildschirm angezeigt.)

Sie werden nun aufgefordert, einen Benutzernamen einzugeben. Geben Sie einen beliebigen Text ein.

Als Eingabeaufforderung wird nun `Local>` angezeigt. Geben Sie `SET IP ADDRESS ipaddress` ein, wobei `ipaddress` die IP-Adresse ist, die Sie dem PrintServer zuweisen möchten. Zum Beispiel:

```
Local> SET IP ADDRESS 192.168.1.3
```

Nun müssen Sie die Subnetzmaske einrichten. Geben Sie `SET IP SUBNET Subnetzmaske` ein, wobei `Subnetzmaske` die Subnetzmaske ist, die Sie dem PrintServer zuweisen möchten. (Fragen Sie Ihren Netzwerkadministrator, welche Subnetzmaske verwendet werden soll.) Zum Beispiel:

```
Local> SET IP SUBNET 255.255.255.0
```

Wenn Ihr Netzwerk nicht in Subnetze unterteilt ist, verwenden Sie eine der folgenden Standard-Subnetzmasken:

255.0.0.0 für Netzwerke der Klasse A

255.255.0.0 für Netzwerke der Klasse B

255.255.255.0 für Netzwerke der Klasse C

Die Zifferngruppe ganz links in der IP-Adresse beschreibt, um welche Art von Netzwerk es sich handelt. Der Wert dieser Zifferngruppe liegt im Bereich von 1 bis 127 für Netzwerke der Klasse A (z. B. 13.27.7.1), im Bereich von 128 bis 191 für Netzwerke der Klasse B (z. B. 128.10.1.30) und im Bereich von 192 bis 255 für Netzwerke der Klasse C (z. B. 192.168.1.4).

Wenn Sie ein Gateway (Router) verwenden, geben Sie dessen Adresse mit dem Befehl `SET IP ROUTER routeraddress` ein, wobei `routeraddress` die IP-Adresse des Gateways ist, das Sie dem PrintServer zuweisen möchten. Zum Beispiel:

```
Local> SET IP ROUTER 192.168.1.4
```

Geben Sie `SET IP METHOD STATIC` ein, um die IP-Adresse als statische Adresse zu konfigurieren.

Überprüfen Sie, ob Sie die IP-Daten richtig eingegeben haben. Geben Sie dazu `SHOW IP` ein.

Geben Sie `EXIT` oder Strg-D ein (halten Sie dazu zum Beispiel die Strg-Taste gedrückt und geben Sie „D“ ein), um die Arbeit mit der entfernten Konsole zu beenden.

A

Ad-hoc-Modus	12, 32
AES	131
AOSS™	27, 39
APIPA	38, 122, 146
APOP	141
ARP	122, 147
Authentifizierung	131

B

BINARY_P1	144
BOOTP	122, 146
BRAdmin Light	3, 5
BRAdmin Professional 3	3, 8, 103
BRNxxxxxxxxxxxx	144
BRNxxxxxxxxxxxx_AT	144
BRPrint Auditor	9

C

CA	139
CA-Zertifikat	139
CIFS	125
CKIP	133
CSR	139
Custom Raw Port	123

D

DHCP	122, 144
Dienste	144
Dienstprogramm zum Reparieren der Netzwerkverbindung	114
Digitale Signatur	139
DNS-Client	123
DNS-Server	38

E

EAP-FAST	128
EAP-MD5	128
EAP-TLS	129
EAP-TTLS	129
Ethernet	39

F

FTP	71, 124
Funktionstastenfeld	36

G

Gateway	37
---------------	----

H

HTTP	57, 124
HTTPS	100, 140

I

IEEE 802.1x	15, 18, 128
Infrastruktur-Modus	11
IP-Adresse	37, 126
IPP	123
IPPS	104, 140
IPv6	38, 125

K

Kanäle	130
Knotenname	37

L

LEAP	128
LLMNR	124
LPR/LPD	123

M

MAC-Adresse	6, 7, 8, 37, 40, 49, 135, 144, 145, 146, 147
mDNS	123

N

NetBIOS-Namensauflösung	123
Netzwerk-Druckerfreigabe	121
Netzwerk-Konfigurationsbericht	49
Netzwerkschlüssel	132

O

Open system (offenes System)	131
------------------------------------	-----

P

PBC	27, 39
PCL_P1	144
PEAP	128
Peer-to-Peer	120
PIN-Methode	29, 39
POP über SSL	141
POP vor SMTP	106, 141
Port 9100	123
POSTSCRIPT_P1	144
Protokoll	122
Public-Key-Kryptosystem	139

R

RARP	122, 145
Remote Setup	3
RFC 1001	144

S

Shared Key	131
Shared-Key-Kryptosystem	139
Sicherheitsbegriffe	139
SMTP über SSL	141
SMTP-AUTH	106, 141
SMTP-Client	123
SNMP	124
SNMPv3	100, 140
SNTP	125
SSID	130
SSL/TLS	87, 140
Status Monitor	3
Subnetzmaske	37, 127

T

TCP/IP	36, 122
TELNET	124, 148
TEXT_P1	144
TKIP	131
Treiberinstallations-Assistent	3

U

Unterstützte Protokolle und Sicherheitsfunktionen	143
--	-----

V

Verschlüsselung	131
Vertical Pairing	3, 134

W

Web Based Management (Webbrowser)	3, 8, 100
Web Services	124, 134, 136
WEP	131
Werkseinstellung	48
WINS	123
WINS-Konfig.	37
WINS-Server	37
Wireless-Netzwerk	10, 130
WLAN-Bericht	49, 116, 118
WPA-PSK/WPA2-PSK	131
WPS (Wi-Fi Protected Setup)	27, 29, 39

Z

Zertifikat	87, 139
Zurücksetzen der Netzwerkeinstellungen	48