Wichtige Sicherheitsinformationen

Werksseitig aktivierte Netzwerkschnittstellen und -dienste

Netzwerkschnittstellen

- Ethernet: Die Netzwerkkommunikation beginnt , wenn ein Kabel angeschlossen wird.

Netzwerkdienste

Dienst	Protokoll	Beschreibung
Webserver	HTTPS	Der Webserver wird verwendet, um die Informationen und Einstellungen des Geräts über Web Based Management und die Brother-Verwaltungstools anzuzeigen und zu ändern. Er unterstützt außerdem das Drucken, Scannen und Faxen mit AirPrint, Mopria™ und Webdiensten.
SNMP	SNMP v1/v2c	SNMP wird zum Anzeigen und Ändern der Geräteinformationen über die Verwaltungstools von Brother verwendet. In den Werkseinstellungen ist nur die Anzeige aktiviert.
LPD	LPD	LPD wird hauptsächlich für den Druck verwendet. Es unterstützt auch die PC-Fax-Sendefunktion über die Brother-Anwendungen.
Port 9100 (Raw-Port)	Port 9100	Port 9100 wird hauptsächlich zum Drucken verwendet. Es unterstützt auch das Anzeigen und Ändern der Geräteinformationen über die Verwaltungstools von Brother. In den Werkseinstellungen ist nur die Anzeige aktiviert.
Netzwerk-Scan	(Brother-Original)	Netzwerk-Scan wird für das Scannen über die Anwendungen von Brother verwendet.
PC-Faxempfang	(Brother-Original)	PC-Faxempfang wird für die PC-Faxempfangsfunktion über die Anwendungen von Brother verwendet.

- Die oben genannten Dienste sind bei einigen Modellen möglicherweise standardmäßig deaktiviert.
- Sie können diese Dienste in der linken Navigationsleiste auf der Seite der Web Based Management deaktivieren, indem Sie **Netzwerk** > **Netzwerk** > **Protokoll** auswählen. Wenn Ihr Modell die Registerkarte **Netzwerk** oben auf dem Bildschirm hat, klicken Sie auf diese Registerkarte und wählen Sie die Option **Protokoll**.

Produkt- und Datensicherheit

Produktinstallation

Unbefugte Benutzer können physischen Zugriff auf das Produkt erhalten oder es über das Netzwerk aus der Ferne manipulieren. Stellen Sie sicher, dass Sie das Produkt an einem sicheren Ort installieren.

Vorsichtsmaßnahmen bei der Netzwerkverbindung

Um eine sichere Verwendung des Produkts zu gewährleisten, ändern Sie bitte das Standardpasswort unmittelbar nach dem Kauf. Wenn Sie versuchen, Netzwerkeinstellungen über die Web Based Management zu ändern, erscheint eine Warnmeldung, wenn die Änderung ein Sicherheitsrisiko darstellen könnte. Stellen Sie vor der Aktivierung solcher Einstellungen sicher, dass Ihr Netzwerk vor unbefugtem Abhören oder Manipulation geschützt ist.

Firmware-Updates

Für mehr Sicherheit und Funktionalität empfehlen wir, Ihr Produkt immer mit der neuesten Firmware zu aktualisieren. Wenn Sie die Firmware nicht aktualisieren, können Sicherheitsrisiken bestehen oder einige Funktionen eingeschränkt sein. Beachten Sie, dass wir keine Verantwortung für Unfälle oder Probleme übernehmen können, die durch das Nichtaktualisieren der Firmware entstehen.

Sichere Speicherung auf entfernbaren Medien

Wenn ein USB-Speichermedium als Ziel für den sicheren Druck ausgewählt wird, werden die Druckdaten vor dem Speichern verschlüsselt. Wenn Sie jedoch die Scanfunktion verwenden, um Daten auf einem USB-Speichermedium oder einer Speicherkarte zu speichern, werden die gescannten Daten ohne Verschlüsselung gespeichert. Wenn Ihr Modell dies unterstützt, empfehlen wir, gescannte Daten als passwortgeschützte PDF-Dateien zu speichern, um die Sicherheit zu erhöhen.

Persönliche Informationen

Die im Produkt gespeicherten personenbezogenen Daten können je nach Produkt variieren – z. B. können Druckdaten, Scandaten, Faxdaten, Telefonnummern, E-Mail-Adressen und NFC-Kartennummern enthalten sein. Das Ändern der Produkteinstellungen kann das Risiko eines unbefugten Zugriffs auf die personenbezogenen Daten erhöhen. Stellen Sie sicher, dass Sie den Inhalt und die Auswirkungen der Einstellungen überprüfen, bevor Sie Änderungen vornehmen.

Vorsichtsmaßnahmen bei der Entsorgung des Produkts

Beim Entsorgen des Produkts oder bei der Weitergabe an Dritte können verbleibende Daten ein Risiko für unbefugte Nutzung darstellen. Um die Sicherheit zu gewährleisten, empfehlen wir, alle internen Daten vorher zu löschen. Sie können eine Initialisierung durchführen, indem Sie im Einstellungsmenü des Produkts die Option „Zurücksetzen“ auswählen, um die Werkseinstellungen wiederherzustellen.

Verwendung von Telnet und TFTP

Dieses Produkt unterstützt den Zugriff auf Administratorinformationen über Telnet und TFTP, aber diese Protokolle garantieren keine sichere Netzwerkkommunikation und sind standardmäßig deaktiviert. Stellen Sie sicher, dass Ihre Netzwerkumgebung vor unbefugtem Zugriff geschützt ist, bevor Sie diese Protokolle aktivieren.

Über die Funktionen Sp. wird festg. und Geschützte Benutzersperre

Die Funktionen Sp. wird festg. und Geschützte Benutzersperre sind standardmäßig deaktiviert, wenn Sie das Produkt kaufen. Hinweise zum Aktivieren finden Sie im Online-Benutzerhandbuch.

Weitere Informationen

Wichtig

Die verfügbaren Funktionen hängen von Ihrem Modell ab. Weitere Informationen finden Sie im Online-Benutzerhandbuch Ihres Modells.

Warenzeichen