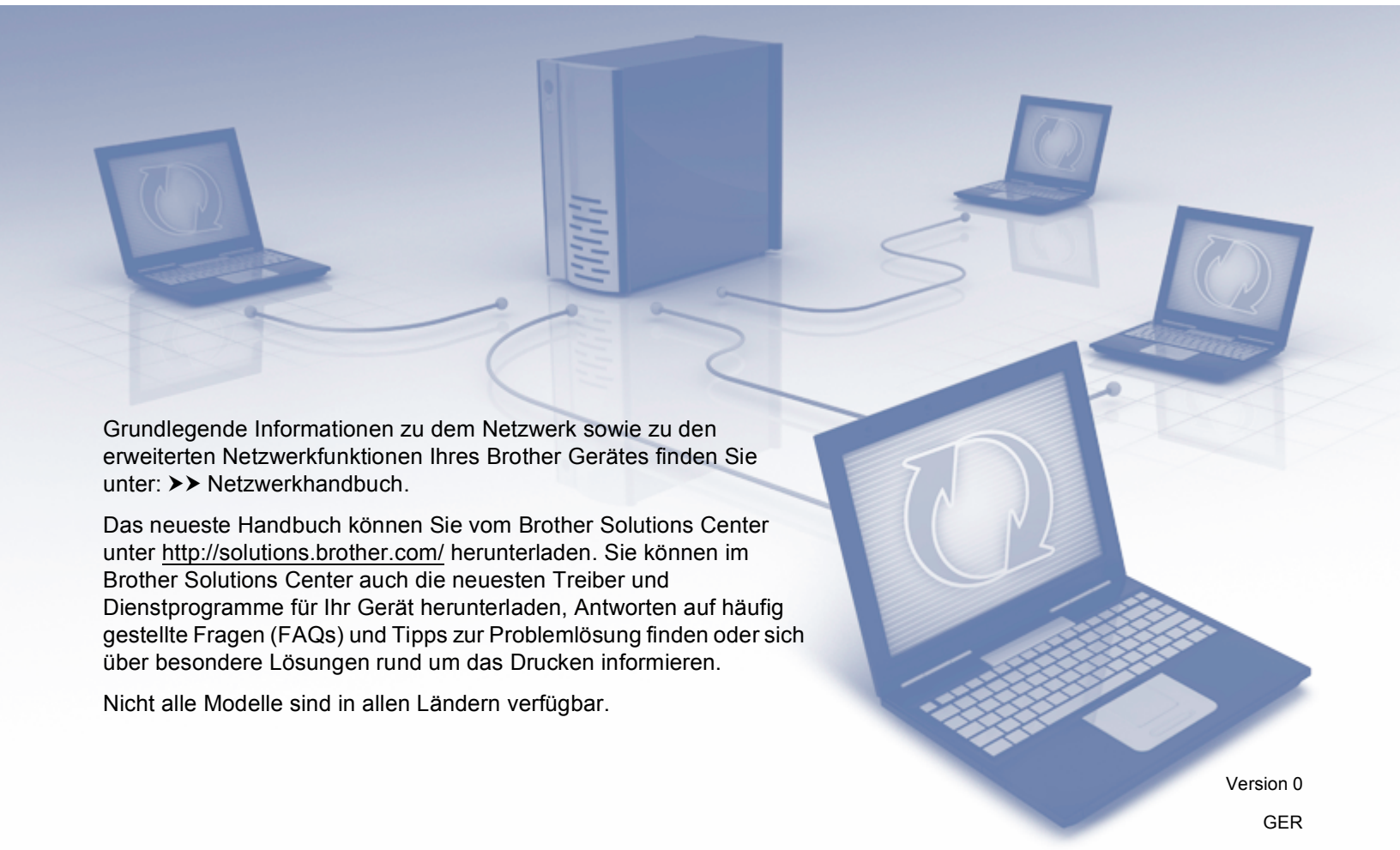
Anleitung SSL

(Secure Socket Layer)



Grundlegende Informationen zu dem Netzwerk sowie zu den erweiterten Netzwerkfunktionen Ihres Brother Gerätes finden Sie unter: ➤➤ Netzwerkhandbuch.

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.

Nicht alle Modelle sind in allen Ländern verfügbar.

Version 0

GER

Relevante Modelle

Dieses Handbuch gilt für die folgenden Modelle.

HL-5450DN(T)/5470DW(T)/6180DW(T)/S7000DN

DCP-8110DN/8150DN/8155DN/8250DN/MFC-8510DN/8710DW/8910DW/8950DW(T)

Definition der Hinweise

In diesem Handbuch werden die folgenden Symbole verwendet:

Hinweis	Hinweise informieren Sie, wie auf eine bestimmte Situation reagiert werden sollte, oder geben Ihnen hilfreiche Tipps zur beschriebenen Funktion.

Warenzeichen

Das Brother-Logo ist ein eingetragenes Warenzeichen von Brother Industries, Ltd.

Microsoft, Windows, Windows Server und Internet Explorer sind in den USA und/oder anderen Ländern entweder eingetragene Warenzeichen oder Warenzeichen der Microsoft Corporation.

Windows Vista ist in den USA und/oder anderen Ländern entweder ein eingetragenes Warenzeichen oder ein Warenzeichen der Microsoft Corporation.

Google Cloud Print ist eine Marke von Google Inc.

Jedes Unternehmen, dessen Software in dieser Anleitung genannt wird, hat für die entsprechenden Programme einen Software-Lizenzvertrag.

Jegliche Handels- und Produktnamen von Unternehmen, die auf Brother-Produkten erscheinen und sich auf Dokumente und andere Materialien beziehen, sind Warenzeichen oder eingetragene Warenzeichen der entsprechenden Unternehmen.

© 2012 Brother Industries, Ltd. Alle Rechte vorbehalten.

WICHTIGER HINWEIS

- Dieses Produkt ist nur zur Verwendung in dem Land zugelassen, in dem es gekauft wurde. 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.
- Sofern nicht anders angegeben, werden in diesem Handbuch die Bildschirme von MFC-8950DW(T) verwendet.
- 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 Vista® steht in diesem Handbuch für alle Ausgaben von Windows Vista®.
- Windows® 7 steht in diesem Handbuch für alle Ausgaben von Windows® 7.
- 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.

Inhaltsverzeichnis

1 Einführung

Übersicht

Secure Socket Layer (SSL) ist eine effektive Methode zum Datenschutz, die über ein lokales Netzwerk oder WAN gesendet wird. Hierbei werden verschlüsselte Daten über ein Netzwerk versandt, z. B. für einen Druckauftrag, sodass jeder bei dem Versuch, die Daten abzufangen, diese aufgrund der Verschlüsselung der Daten nicht lesen kann.

Es kann sowohl für kabellose als auch für Kabel-Netzwerke konfiguriert werden und funktioniert ebenfalls in Kombination mit anderen Sicherheitsmaßnahmen wie WPA™-Schlüssel und Firewalls.

Kurzfassung der Geschichte von SSL

Ursprünglich wurde SSL dazu entwickelt, Informationen im Web zu sichern, insbesondere Daten, die zwischen Internet-Browsern und Servern hin- und hergeschickt werden. Wenn Sie beispielsweise Ihr Internet-Banking über den Internet Explorer® abwickeln, wird Ihnen in der Adresszeile des Browsers https:// sowie ein kleines Vorhängeschloss angezeigt; Sie verwenden SSL. Es wurde für immer mehr Anwendungen wie Telnet, Drucker und FTP-Software verwendet und entwickelte sich zu einer universellen Lösung für die Online-Sicherheit. Noch heute wird es von zahlreichen Online-Shops und Banken für seinen ursprünglichen Zweck verwendet, um sensible Daten wie Kreditkartennummern, Kundendaten, usw. zu sichern.

Der extrem hohen Verschlüsselung von SSL vertrauen Banken auf der ganzen Welt, denn es ist unwahrscheinlich, dass sie entschlüsselt wird.

Vorteile der Anwendung von SSL

Der ausschließliche Vorteil für den Einsatz von SSL bei Brother-Geräten ist die Sicherheit beim Drucken in einem IP-Netzwerk, indem das Lesen der an das Gerät gesendete Daten ausschließlich von dem autorisierten Benutzer erfolgen kann. Das wichtigste Verkaufsargument ist, dass auf diesen Geräten vertrauliche Daten sicher ausgedruckt werden können, beispielsweise für den regelmäßigen Ausdruck von Gehaltsabrechnungen der Personalabteilung eines großen Unternehmens. Ohne Verschlüsselung können die Daten auf diesen Gehaltsabrechnungen von anderen Netzwerk-Benutzern gelesen werden. Wenn die Daten jedoch mit SSL übertragen werden, sieht derjenige, der die Daten abfängt, nur eine Seite mit verwirrenden Codes und nicht die tatsächliche Gehaltsabrechnung.

Zertifikate für Gerätesicherheit verwenden

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. Wenn Sie ein Dokument ausdrucken oder das Web Based Management (Web-Browser) sicher mit SSL verwenden, müssen Sie das Zertifikat auf Ihrem Computer installieren. Siehe *Installation eines digitalen Zertifikats* ➤➤ Seite 4.

- SSL/TLS-Kommunikation
- SSL-Kommunikation für SMTP/POP3

Das Brother-Gerät unterstützt die folgenden Zertifikate.

- Vorinstalliertes Zertifikat

  Ihr Gerät verfügt über ein vorinstalliertes, privates Zertifikat.

  Mit diesem Zertifikat können Sie problemlos die SSL/TLS-Kommunikation nutzen, ohne ein Zertifikat erstellen oder installieren zu müssen. Wenn Sie Google Cloud Print™ nutzen möchten, können Sie anhand dieses vorinstallierten Zertifikats die Einstellungen für Google Cloud Print sicher konfigurieren. Um weitere Informationen zu Google Cloud Print zu erhalten, besuchen Sie bitte das Brother Solutions Center unter http://solutions.brother.com/ und klicken Sie auf der Seite für Ihr Modell auf Handbücher, um die Google Cloud Print Anleitung herunterzuladen.

Hinweis

- Google Cloud Print-Funktion ist für HL-S7000DN nicht verfügbar.
- Das vorinstallierte, selbstsignierte Zertifikat kann Ihre Kommunikation nicht vor Manipulationen schützen. Wir empfehlen, ein Zertifikat eines vertrauenswürdigen Unternehmens einzusetzen, um eine höhere Sicherheit zu erzielen.

- Privates Zertifikat

  Dieser PrintServer 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 *Ein privates Zertifikat erstellen* ➤➤ Seite 6.)

- 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 einer Zertifizierungsstelle haben oder ein Zertifikat von einer vertrauten externen Zertifizierungsstelle verwenden möchten:

  - Installation mit einer Zertifikatsignieranforderung (CSR; Certificate Signing Request) von diesem PrintServer. (Siehe *Erstellung einer Zertifikatsignieranforderung (CSR; Certificate Signing Request)* ➤➤ Seite 7.)
  - Installation mit Import eines Zertifikates und eines privaten Schlüssels (Private Key). (Siehe *Zertifikat und privaten Schlüssel (Private Key) importieren und exportieren* ➤➤ Seite 17.)

■ CA-Zertifikat

Wenn Sie ein CA-Zertifikat verwenden, das die Zertifizierungsstelle (CA - Certificate Authority) selbst identifiziert, müssen Sie vor der Konfiguration ein CA-Zertifikat von der Zertifizierungsstelle importieren. (Siehe *CA-Zertifikate importieren und exportieren* ➤➤ Seite 18.)

Hinweis

- Wenn Sie die SSL/TLS-Kommunikation verwenden möchten, sollten Sie sich zuerst an Ihren Systemadministrator wenden.
- Wenn Sie den PrintServer auf die werkseitigen Standardeinstellungen zurücksetzen, wird das installierte Zertifikat einschließlich des privaten Schlüssels (Private Key) gelöscht. Wenn Sie nach dem Zurücksetzen des PrintServer dasselbe Zertifikat und denselben privaten Schlüssel (Private Key) verwenden möchten, sollten Sie diese vor dem Zurücksetzen exportieren und danach erneut installieren. (Siehe *Privates Zertifikat, von der Zertifizierungsstelle ausgestelltes Zertifikat und privaten Schlüssel importieren* ➤➤ Seite 17.)

2 Digitales Zertifikat für die SSL-Kommunikation

Installation eines digitalen Zertifikats

Wenn Sie in einem sicheren Netzwerk oder einer sicheren Verwaltung mit dem Web Based Management (Web-Browser) drucken möchten, benötigen Sie ein digitales Zertifikat, das sowohl auf diesem Gerät als auch auf dem Gerät installiert ist, das Daten an dieses Gerät sendet, z. B. einem Computer. Ihr Gerät verfügt über ein vorinstalliertes Zertifikat. Um das Zertifikat zu konfigurieren, muss der Benutzer sich über einen Web-Browser und mit seiner IP-Adresse remote an dem Gerät anmelden.

Hinweis

Wir empfehlen Windows® Internet Explorer® 7.0/8.0 oder Firefox® 3.6 für Windows® und Safari 4.0/5.0 für Macintosh. 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.

1. Starten Sie Ihren Webbrowser.
2. Geben Sie in der Adressleiste Ihres Browsers „http://IP-Adresse des Gerätes/“ ein (wobei „IP-Adresse des Gerätes“ für die IP-Adresse des Gerätes oder den Namen des Druckservers steht).
   - Zum Beispiel: http://192.168.1.2/
3. Standardmäßig ist kein Kennwort erforderlich. Wenn Sie zuvor ein Kennwort festgelegt haben, geben Sie es ein und drücken Sie →.
4. Klicken Sie auf **Netzwerk**.
5. Klicken Sie auf **Sicherheit**.
6. Klicken Sie auf **Zertifikat**.

7 Nun können Sie die Zertifikateinstellungen vornehmen.
Um ein privates Zertifikat mit dem Web Based Management zu erstellen, gehen Sie zu *Ein privates Zertifikat erstellen* ➤➤ Seite 6.
Um eine Zertifikatsignieranforderung (CSR; Certificate Signing Request) zu erstellen, gehen Sie zu *Erstellung einer Zertifikatsignieranforderung (CSR; Certificate Signing Request)* ➤➤ Seite 7.

1 Privates Zertifikat erstellen und installieren

2 Ein Zertifikat einer Zertifizierungsstelle (CA - Certificate Authority) verwenden

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.

Ein privates Zertifikat erstellen

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

Hinweis

- Die Länge des **Allgemeine Name** muss weniger als 64 Zeichen betragen. 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 private Zertifikat benutzt wurde.

3. Sie können die Einstellungen **Algorithmus des öffentlichen Schlüssels** und **Digest-Algorithmus** aus der Pulldown-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.

Erstellung einer Zertifikatsignieranforderung (CSR; Certificate Signing Request)

Eine Zertifikatsignieranforderung (CSR; Certificate Signing Request) wird an eine Zertifizierungsstelle gesandt, um die darin aufgeführten Berechtigungen zu authentifizieren.

Hinweis

Es wird empfohlen, das Stammzertifikat von der Zertifizierungsstelle auf Ihrem Computer zu installieren, bevor Sie eine Zertifikatsignieranforderung erstellen.

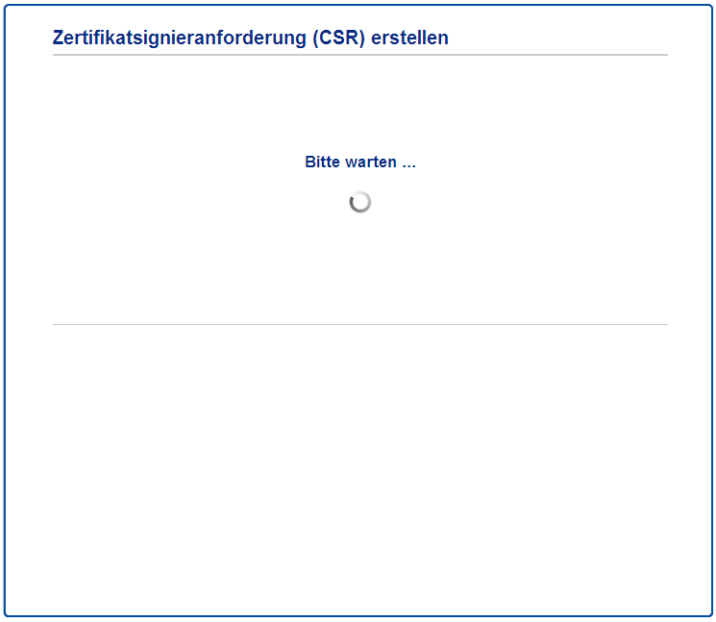
1. Klicken Sie auf **Zertifikatsignieranforderung (CSR) erstellen**.
2. Füllen Sie das Feld **Allgemeine Name** aus und geben Sie Ihre Informationen, wie die **Organisation** ein. Hierfür sind die Details zu Ihrem Unternehmen erforderlich, sodass die Zertifizierungsstelle Ihre Identität bestätigen und der Außenwelt bescheinigen kann.

Hinweis

- Die Länge des **Allgemeine Name** muss weniger als 64 Zeichen betragen. 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. 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.
- Für **Organisation**, **Organisationseinheit**, **Ort** und **Bundesland** muss die Länge weniger als 64 Zeichen betragen.
- 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 Pulldown-Liste wählen. Die Standardeinstellungen sind **RSA(2048bit)** für **Algorithmus des öffentlichen Schlüssels** und **SHA256** für **Digest-Algorithmus**.

4 Klicken Sie auf **Senden**. Es wird folgender Bildschirm angezeigt.



5 Nach einigen Momenten erscheint das Zertifikat, das in einer kleinen Datei oder durch Kopieren und Einfügen direkt in einem von der Zertifizierungsstelle angebotenen Zertifikatsignieranforderungs-Formular (CSR-Formular) online gespeichert werden kann. Klicken Sie auf **Speichern**, um die CSR-Datei auf Ihrem Computer zu speichern.

Hinweis

Beachten Sie in Bezug auf das Verfahren zum Senden der Zertifikatsignieranforderung an Ihre Zertifizierungsstelle die Richtlinien der Zertifizierungsstelle.

6 Die Zertifikatsignieranforderung ist nun erstellt. Anleitungen zur Installation des Zertifikats auf dem Gerät finden Sie unter *Zertifikat auf dem Gerät installieren* ➤➤ Seite 9.

Zertifikat auf dem Gerät installieren

Nachdem Sie das Zertifikat von der Zertifizierungsstelle erhalten haben, installieren Sie es wie folgt auf dem PrintServer.

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 erfolgreich erstellt und 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.
Sie haben die Konfiguration des digitalen Zertifikats abgeschlossen. Wenn Sie eine E-Mail mit SSL senden oder empfangen möchten, informieren Sie sich unter *Sicherer Versand oder Empfang (bei DCP- und MFC-Modellen) einer E-Mail* ➤➤ Seite 25 über die erforderlichen Konfigurationsschritte.

Auswahl des Zertifikats

Gehen Sie nach Installation des Zertifikats folgendermaßen vor, um das gewünschte Zertifikat auszuwählen.

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

Hinweis

- Wenn das folgende Dialogfeld erscheint, empfiehlt Brother für eine sichere Kommunikation, die Telnet-, FTP-, TFTP-Protokolle sowie die Netzwerkverwaltung mit älteren Versionen von BRAdmin Professional (2.8 oder niedriger) zu deaktivieren. Solange sie aktiviert sind, ist die Benutzerauthentifizierung nicht sicher.

- Für DCP- und MFC-Modelle:

  Wenn Sie FTP deaktivieren, kann die Scan-to-FTP-Funktion nicht verwendet werden.

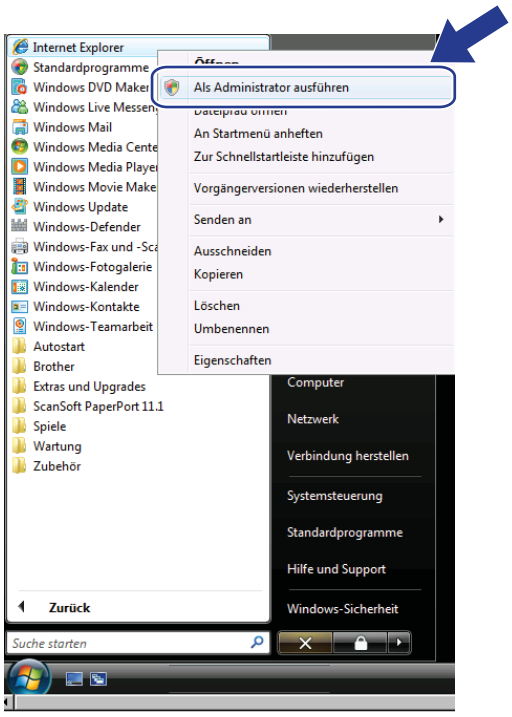
4. Klicken Sie auf **Senden**.

Installation des selbstsignierten oder vorinstallierten Zertifikats unter Windows Vista®, Windows® 7 und Windows Server® 2008 für Benutzer mit Administratorrechten

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 benötigen Administratorrechte, um selbstsignierte oder vorinstallierte Zertifikate zu installieren.

1. Klicken Sie auf die Schaltfläche und dann auf **Alle Programme**.
2. Klicken Sie mit der rechten Maustaste auf **Internet Explorer** und klicken Sie dann auf **Als Administrator ausführen**.



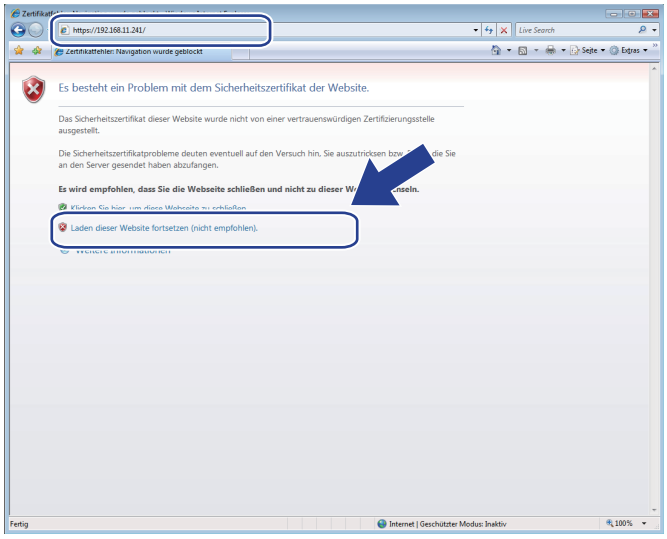
Hinweis

Wenn das Fenster **Benutzerkontensteuerung** erscheint:

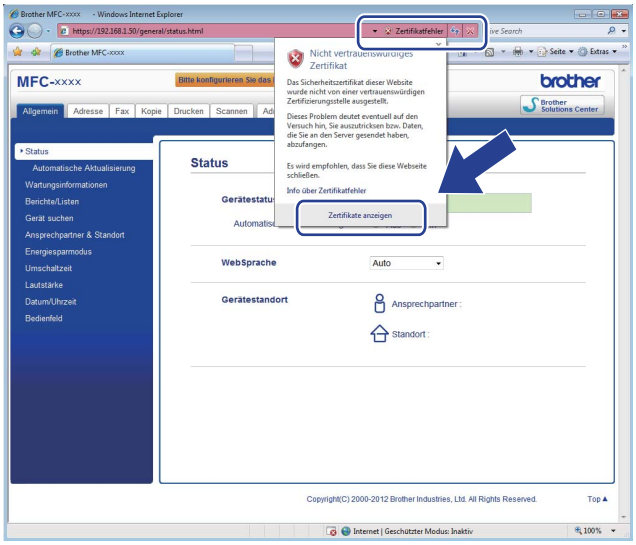
(Windows Vista®) Klicken Sie auf **Fortsetzen (Zulassen)**.

(Windows® 7) 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)**.

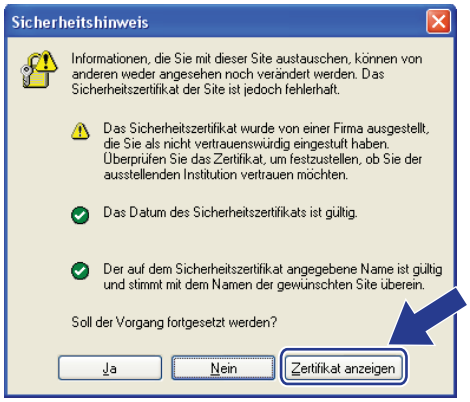


4 Klicken Sie auf **Zertifikatfehler** und dann auf **Zertifikate anzeigen**. Fahren Sie mit Schritt ❹ unter *Installation des selbstsignierten oder vorinstallierten Zertifikats für Windows® XP und Windows Server® 2003 durch Benutzer* ➤➤ Seite 14 fort.

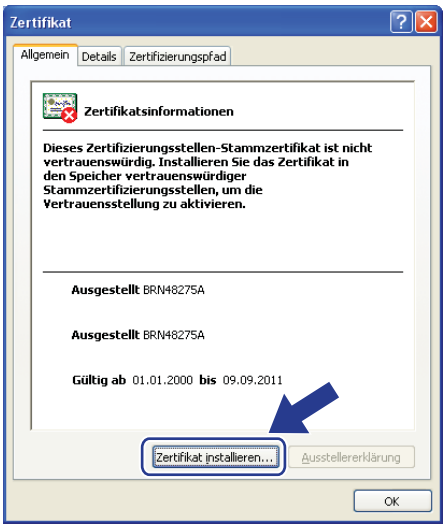


Installation des selbstsignierten oder vorinstallierten Zertifikats für Windows® XP und Windows Server® 2003 durch Benutzer

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 dem Zertifikat zugewiesen haben).
3. Wenn die Sicherheitswarnung im Dialogfeld angezeigt wird, haben Sie folgende Möglichkeiten:
   - Klicken Sie auf **Laden dieser Website fortsetzen (nicht empfohlen)**. Klicken Sie auf **Zertifikatfehler** und dann auf **Zertifikate anzeigen**.
   - Wenn das folgende Dialogfeld angezeigt wird, klicken Sie auf **Zertifikat anzeigen**.

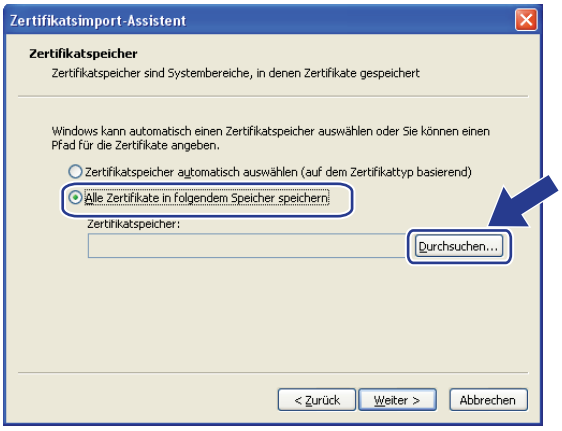


4. Klicken Sie auf **Zertifikat installieren...** in der Registerkarte **Allgemein**.



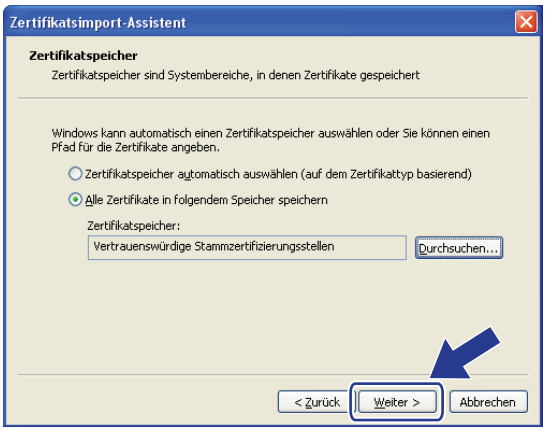
5 Wenn der **Zertifikatsimport-Assistent** erscheint, klicken Sie auf **Weiter**.

6 Zur Installation des Zertifikats müssen Sie einen Installationsort angeben. Wir empfehlen Ihnen, **Alle Zertifikate in folgendem Speicher speichern** auszuwählen und dann auf **Durchsuchen...** zu klicken.



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

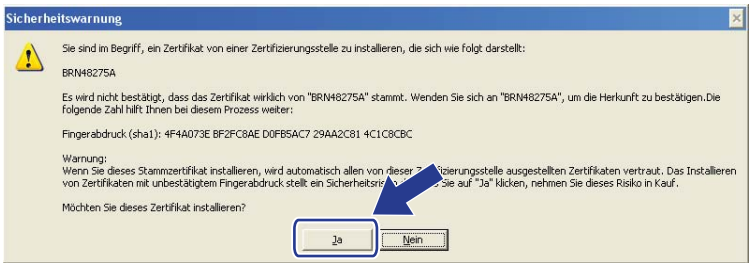
8 Klicken Sie auf **Weiter**.



9 Am nächsten Bildschirm klicken Sie auf **Fertig stellen**.

10 Anschließend werden Sie aufgefordert, das Zertifikat zu installieren.
Sie haben die folgenden Möglichkeiten:

- Wenn Sie das private Zertifikat installieren, bestätigen Sie den Fingerabdruck und klicken Sie anschließend auf **Ja**.
- Wenn Sie das vorinstallierte Zertifikat installieren, klicken Sie auf **Ja**.



Hinweis

- Den Fingerabdruck (Fingerprint, Thumbprint) für das private Zertifikat finden Sie im Netzwerk-Konfigurationsbericht.

  Für Hinweise zum Ausdrucken des Netzwerk-Konfigurationsberichts lesen Sie *Druckereinstellungen-Seite drucken (für HL-5450DN(T))* ➤➤ Seite 29 oder *Ausdrucken des Netzwerk-Konfigurationsberichts (Für andere Modelle)* ➤➤ Seite 29.
- Den Fingerabdruck (Fingerprint, Thumbprint) für das vorinstallierte Zertifikat finden Sie nicht im Netzwerk-Konfigurationsbericht.

11 Klicken Sie auf **OK**.

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

Auf jedem Computer, der diese sichere Druckfunktion nutzen soll, muss dieselbe Prozedur durchlaufen. Nachdem die Installation jedoch einmal vorgenommen wurde, muss sie nicht wiederholt werden, solange sich das Zertifikat nicht ändert.

Zertifikat und privaten Schlüssel (Private Key) importieren und exportieren

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

Privates Zertifikat, von der Zertifizierungsstelle ausgestelltes Zertifikat und privaten Schlüssel importieren

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.

Privates Zertifikat, von der Zertifizierungsstelle ausgestelltes Zertifikat und privaten Schlüssel exportieren

1. Klicken Sie auf **Exportieren** neben **Zertifikatliste** auf der Seite **Zertifikat**.
2. Geben Sie ein 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.

CA-Zertifikate importieren und exportieren

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

CA-Zertifikat importieren

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**.

CA-Zertifikat exportieren

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 zu wählen.
4. Wählen Sie das Ziel, unter dem Sie das exportierte Zertifikat speichern möchten, und speichern Sie dann das Zertifikat.

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 anzeigen lassen, welche Zertifikate über die Seite **Zertifikat** 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 *Installation eines digitalen Zertifikats* ➤➤ Seite 4.

- Für Drucker-Modelle

  Das Brother-Gerät ermöglicht das Speichern von bis zu drei privaten Zertifikaten oder bis zu drei Zertifikaten, die von einer Zertifizierungsstelle ausgestellt wurden. Sie können die gespeicherten Zertifikate zur Verwendung des HTTPS/IPPS-Protokolls oder der IEEE 802.1x-Authentifizierung nutzen.

- Für DCP- und MFC-Modelle

  Das Brother-Gerät ermöglicht das Speichern von bis zu vier privaten 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-Datei nutzen.

Sie können auch bis zu vier oder sechs (HL-S7000DN) 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 das HTTPS/IPPS, IEEE 802.1x oder (bei DCP- und MFC-Modellen) signierte PDFs verwenden, müssen Sie wählen, welches Zertifikat benutzt werden soll.
- Wenn Sie SSL für die SMTP-/POP3-Kommunikation nutzen (für DCP- und MFC-Modelle), müssen Sie das Zertifikat nicht auswählen. Das notwendige Zertifikat wird automatisch ausgewählt.

3 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 dem 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 zu verwendende Zertifikat auf dem Bildschirm von Web Based Management ändern, indem Sie auf **Netzwerk**, **Protokoll** und dann auf **HTTP-Servereinstellungen** klicken.
- Außerdem müssen Sie das auf dem Gerät installierte Zertifikat auch auf Ihrem Computer installieren. Siehe *Installation des selbstsignierten oder vorinstallierten Zertifikats unter Windows Vista®, Windows® 7 und Windows Server® 2008 für Benutzer mit Administratorrechten* ➤➤ Seite 12 oder *Installation des selbstsignierten oder vorinstallierten Zertifikats für Windows® XP und Windows Server® 2003 durch Benutzer* ➤➤ Seite 14.

1. Starten Sie Ihren Webbrowser.
2. Geben Sie in Ihren Browser „https://IP-Adresse des Geräts/“ ein. (Wenn Sie das Zertifikat bereits erstellt haben, geben Sie in den Browser „https://Allgemeiner Name/“ ein. Wobei „Allgemeiner Name“ der allgemeine Name ist, den Sie dem Zertifikat zugewiesen haben, zum Beispiel eine IP-Adresse, ein Knotenname oder eine Domänenname. Wie Sie dem Zertifikat einen allgemeinen Namen zuweisen können, lesen Sie unter *Zertifikate für Gerätesicherheit verwenden* ➤➤ Seite 2.)

   ■ Zum Beispiel:

   https://192.168.1.2/ (wenn der allgemeine Name die IP-Adresse des Gerätes ist)
3. Standardmäßig ist kein Kennwort erforderlich. Geben Sie ein Kennwort ein, wenn Sie eines eingerichtet haben, und drücken Sie .

4 Sicherer Druck von Dokumenten mit SSL

Sicherer Druck von Dokumenten mit IPPS für Windows®

Wir empfehlen, das IPPS-Protokoll zur sicheren Verwaltung zu verwenden. Zur Verwendung des IPPS-Protokolls sind die folgenden Geräteeinstellungen notwendig.

Hinweis

- Die Kommunikation über IPPS kann den unbefugten Zugriff auf den PrintServer nicht verhindern.
- Außerdem müssen Sie das auf dem Gerät installierte Zertifikat auch auf Ihrem Computer installieren. Siehe *Installation des selbstsignierten oder vorinstallierten Zertifikats unter Windows Vista®, Windows® 7 und Windows Server® 2008 für Benutzer mit Administratorrechten* ➤➤ Seite 12 oder *Installation des selbstsignierten oder vorinstallierten Zertifikats für Windows® XP und Windows Server® 2003 durch Benutzer* ➤➤ Seite 14.
- Das IPPS-Protokoll muss aktiviert sein. Die Standardeinstellung ist aktiviert. Sie können die IPPS-Protokolleinstellungen und das zu verwendende Zertifikat auf dem Bildschirm von Web Based Management ändern, indem Sie auf **Netzwerk**, **Protokoll** und dann auf **HTTP-Servereinstellungen** klicken.

Windows® XP und Windows Server® 2003

1. Klicken Sie auf **Start** und wählen Sie **Drucker und Faxgeräte**.
2. Um **Druckerinstallations-Assistant** zu starten, klicken Sie auf **Drucker hinzufügen**.
3. Sobald der Bildschirm **Willkommen** angezeigt wird, klicken Sie auf **Weiter**.
4. Wählen Sie **Netzwerkdrucker oder Drucker, der an einen anderen Computer angeschlossen ist**.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie **Verbindung mit einem Drucker im Internet oder Heim-/Firmennetzwerk herstellen** und gegen Sie in das URL-Feld folgende Adresse ein:
„http://IP-Adresse des Gerätes/“ (wobei „IP-Adresse des Gerätes“ für die IP-Adresse des Gerätes oder den Knotennamen steht).

Hinweis

- Es ist wichtig, dass Sie „https://“ und nicht „http://“ eingeben, da das Drucken über IPP ansonsten nicht sicher ist.
- Wenn Sie die Datei Hosts bearbeitet haben oder ein Domain Name System (DNS) verwenden, können Sie auch den DNS-Namen des Druckerservers eingeben. Da der Druckerserver TCP/IP- und NetBIOS-Namen unterstützt, können Sie auch den NetBIOS-Namen des Druckerservers eingeben. Den NetBIOS-Namen können Sie dem Netzwerk-Konfigurationsbericht entnehmen. (Für Hinweise zum Ausdrucken des Netzwerk-Konfigurationsberichts lesen Sie *Druckereinstellungen-Seite drucken (für HL-5450DN(T))* ➤➤ Seite 29 oder *Ausdrucken des Netzwerk-Konfigurationsberichts (Für andere Modelle)* ➤➤ Seite 29.) Der zugeordnete NetBIOS-Name besteht aus den ersten 15 Zeichen des Knotennamens und wird standardmäßig bei einem Kabelnetzwerk als „BRNxxxxxxxxxxxx“ bzw. bei einem Wireless-Netzwerk als „BRWxxxxxxxxxxxx“ angezeigt. („xxxxxxxxxxxx“ steht für die MAC-Adresse / Ethernet-Adresse Ihres Gerätes.)

7. Wenn Sie auf **Weiter** klicken, stellen Windows® XP und Windows Server® 2003 eine Verbindung zu der von Ihnen angegebenen URL her.
   - Wenn der Druckertreiber bereits installiert wurde:

     Im **Druckerinstallations-Assistant** erscheint der Bildschirm für die Druckerauswahl.

     Gehen Sie zu Schritt ⓫.
   - Wenn der Druckertreiber noch NICHT installiert wurde:

     Ein Vorteil des IPP-Druckprotokolls liegt darin, dass es den Modellnamen des Druckers bei der Kommunikation erstellt. Nach einer erfolgreichen Kommunikation wird der Modellname des Druckers automatisch angezeigt. Das bedeutet, dass Sie in Windows® XP und Windows Server® 2003 nicht die Art des Druckertreibers angeben müssen.

     Gehen Sie zu Schritt ❽.

Hinweis

Wenn der von Ihnen installierte Druckertreiber kein digitales Zertifikat hat, wird eine Warnmeldung angezeigt. Klicken Sie auf **Installation fortsetzen**, um mit der Installation fortzufahren.

8. Klicken Sie auf **Datenträger**. Anschließend werden Sie aufgefordert, die Treiber-CD einzulegen.
9. Klicken Sie auf **Durchsuchen** und wählen Sie den entsprechenden Brother-Druckertreiber aus, der sich auf der CD-ROM oder im Netzwerkverzeichnis befindet.
   Klicken Sie auf **OK**.
10. Klicken Sie auf **OK**.
11. Wählen Sie Ihr Gerät und klicken Sie auf **OK**.
12. Aktivieren Sie das Kontrollkästchen **Ja**, wenn Sie diesen Drucker als Standarddrucker verwenden möchten. Klicken Sie auf **Weiter**.
13. Kicken Sie auf **Fertig stellen**. Das Gerät ist nun konfiguriert und druckbereit. Drucken Sie zum Testen der Druckerverbindung eine Testseite aus.

Windows Vista®, Windows® 7 und Windows Server® 2008

1. (Windows Vista®)
   Klicken Sie auf die Schaltfläche und dann auf **Systemsteuerung**, **Hardware und Sound** und anschließend auf **Drucker**.
   (Windows® 7)
   Klicken Sie auf die Schaltfläche und dann auf **Geräte und Drucker**.
   (Windows Server® 2008)
   Klicken Sie auf **Start**, **Systemsteuerung**, **Hardware und Sound** und dann auf **Drucker**.
2. Klicken Sie auf **Drucker hinzufügen**.
3. Wählen Sie **Einen Netzwerk-,Drahtlos-oder Bluetoothdrucker hinzufügen**.
4. Klicken Sie auf **Der gesuchte Drucker ist nicht aufgeführt**.
5. Wählen Sie **Einen freigegebenen Drucker über den Namen auswählen** und geben Sie anschließend in das URL-Feld Folgendes ein: „http://IP-Adresse des Gerätes/ipp“ (wobei „IP-Adresse des Gerätes“ für die IP-Adresse des Gerätes oder den Knotennamen steht).

Hinweis

- Es ist wichtig, dass Sie „https://“ und nicht „http://“ eingeben, da das Drucken über IPP ansonsten nicht sicher ist.
- Wenn Sie die Datei Hosts bearbeitet haben oder ein Domain Name System (DNS) verwenden, können Sie auch den DNS-Namen des Druckerservers eingeben. Da der Druckerserver TCP/IP- und NetBIOS-Namen unterstützt, können Sie auch den NetBIOS-Namen des Druckerservers eingeben. Den NetBIOS-Namen können Sie dem Netzwerk-Konfigurationsbericht entnehmen. (Für Hinweise zum Ausdrucken des Netzwerk-Konfigurationsberichts lesen Sie *Druckereinstellungen-Seite drucken (für HL-5450DN(T))* ➤➤ Seite 29 oder *Ausdrucken des Netzwerk-Konfigurationsberichts (Für andere Modelle)* ➤➤ Seite 29.) Der zugeordnete NetBIOS-Name besteht aus den ersten 15 Zeichen des Knotennamens und wird standardmäßig bei einem Kabelnetzwerk als „BRNxxxxxxxxxxxx“ bzw. bei einem Wireless-Netzwerk als „BRWxxxxxxxxxxxx“ angezeigt. („xxxxxxxxxxxx“ steht für die MAC-Adresse / Ethernet-Adresse Ihres Gerätes.)

6. Wenn Sie auf **Weiter** klicken, verbinden Windows Vista® und Windows Server® 2008 sich mit der von Ihnen angegebenen URL.

   ■ Wenn der Druckertreiber bereits installiert wurde:

   Im Druckerinstallations-Assistenten erscheint der Bildschirm für die Druckerauswahl. Klicken Sie auf **OK**.

   Wenn der entsprechende Druckertreiber bereits auf Ihrem Computer installiert ist, verwenden Windows Vista® und Windows Server® 2008 diesen automatisch. In diesem Fall werden Sie gefragt, ob Sie den Treiber als Standarddrucker verwenden möchten. Anschließend wird der Treiberinstallationsassistent beendet. Sie können jetzt drucken.

   Gehen Sie zu Schritt ⓫.

■ Wenn der Druckertreiber noch NICHT installiert wurde:

Ein Vorteil des IPP-Druckprotokolls liegt darin, dass es den Modellnamen des Druckers bei der Kommunikation erstellt. Nach einer erfolgreichen Kommunikation wird der Modellname des Druckers automatisch angezeigt. Das bedeutet, dass Sie in Windows Vista® und Windows Server® 2008 nicht die Art des Druckertreibers angeben müssen.

Gehen Sie zu Schritt ❼.

7 Wenn Ihr Drucker nicht in der Liste der unterstützten Drucker aufgeführt wird, klicken Sie auf **Datenträger**. Anschließend werden Sie aufgefordert, die Treiber-CD einzulegen.

8 Klicken Sie auf **Durchsuchen** und wählen Sie den entsprechenden Brother-Druckertreiber aus, der sich auf der CD-ROM oder im Netzwerkverzeichnis befindet. Klicken Sie auf **Öffnen**.

9 Klicken Sie auf **OK**.

10 Geben Sie den Modellnamen des Gerätes an. Klicken Sie auf **OK**.

Hinweis

- Wenn der Bildschirm „Benutzerkontensteuerung“ angezeigt wird, klicken Sie auf **Fortsetzen**.
- Wenn der von Ihnen installierte Druckertreiber kein digitales Zertifikat hat, wird eine Warnmeldung angezeigt. Klicken Sie auf **Diese Treibersoftware trotzdem installieren**, um mit der Installation fortzufahren. Der **Druckerinstallations-Assistant** wird anschließend abgeschlossen.

11 Sie sehen nun im Bildschirm **Geben Sie einen Druckernamen ein** den Assistent **Drucker hinzufügen**. Wenn Sie diesen Drucker als Standarddrucker verwenden möchten, müssen Sie das Kontrollkästchen **Als Standarddrucker festlegen** aktivieren und anschließend auf **Weiter** klicken.

12 Um die Druckerverbindung zu testen, klicken Sie auf **Testseite drucken** und anschließend auf **Fertig stellen**. Das Gerät ist nun konfiguriert und druckbereit.

5 Sicherer Versand oder Empfang (bei DCP- und MFC-Modellen) einer E-Mail

Konfiguration mit dem Web Based Management (Webbrowser)

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

1. Starten Sie Ihren Webbrowser.
2. Geben Sie in Ihren Browser „http://IP-Adresse des Gerätes/“ ein (wobei „IP-Adresse des Gerätes“ für die IP-Adresse des Gerätes steht).
   - Zum Beispiel:

     http://192.168.1.2/
3. Standardmäßig ist kein Kennwort erforderlich. Geben Sie ein Kennwort ein, wenn Sie eines eingerichtet haben, und drücken Sie →.
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**. Der Bildschirm **Konfiguration des E-Mail-Versands testen** oder **Konfiguration des E-Mail-Empfangs/Versands testen** wird angezeigt.
9. Folgen Sie den Anweisungen auf dem Bildschirm, wenn Sie Ihre aktuellen Einstellungen prüfen möchten.

Sicherer Versand oder Empfang (bei DCP- und MFC-Modellen) einer E-Mail mit SSL/TLS

Dieses Gerät unterstützt SSL/TLS zum Senden oder Empfangen von E-Mails (bei DCP- und MFC-Modellen) über einen E-Mail-Server, der eine sichere SSL/TLS-Kommunikation erfordert. Um E-Mails über einen E-Mail-Server, der die SSL/TLS-Kommunikation verwendet, zu senden oder zu empfangen, 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, ob der Import eines CA-Zertifikates erforderlich ist. Zum Import des Zertifikates lesen Sie *CA-Zertifikate importieren und exportieren* ➤➤ Seite 18.
  - Wenn Sie das Server-Zertifikat nicht überprüfen müssen, deaktivieren Sie **Server-Zertifikat verifizieren**.

Portnummer

- Wenn Sie SSL oder TLS wählen, werden die Einstellungen des **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
    - **SMTP Server Authentication Method**: SMTP-AUTH
    - **SMTP over SSL/TLS**: TLS
  - **POP3**
    - **POP3 Port**: 995
    - **POP3 over SSL/TLS**: SSL

6 Problemlösung

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.

Problem identifizieren

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.
Alle Transportschutzteile wurden vom Gerät entfernt.
Die Tonerkassetten und die Trommeleinheit oder die Tintenpatrone (HL-S7000DN) sind richtig installiert.
Die vorderen und hinteren Abdeckungen sind ganz geschlossen.
Das Papier ist richtig in die Papierkassette eingelegt.
Das Gerät ist ordnungsgemäß an das Netzwerk angeschlossen.

Gehen Sie zur Lösung Ihres Problems zu der in der folgenden Liste angegebenen Seite

- Ich kann das Dokument nicht mit IPPS über das Internet ausdrucken.

  Siehe *Ich kann das Dokument nicht mit IPPS über das Internet ausdrucken.* ➤➤ Seite 28.
- Ich möchte prüfen, ob meine im Netzwerk angeschlossenen Geräte richtig arbeiten.

  Siehe *Ich möchte prüfen, ob meine im Netzwerk angeschlossenen Geräte richtig arbeiten.* ➤➤ Seite 28.

Ich kann das Dokument nicht mit IPPS über das Internet ausdrucken.

Frage	Lösung
Ich kann mit SSL nicht mit dem Brother-Gerät kommunizieren.	■ Verschaffen Sie sich ein gültiges Zertifikat und installieren Sie es erneut sowohl auf Ihrem Gerät als auch auf dem Computer. ■ Achten Sie bitte darauf, dass die Port-Einstellungen Ihres Gerätes korrekt sind. Sie können die Port-Einstellungen auf dem Bildschirm von Web Based Management bestätigen, indem Sie auf **Protokoll**, **Netzwerk** und dann auf **HTTP-Servereinstellungen** klicken.

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

Frage	Lösung
Ist Ihr Brother-Gerät eingeschaltet?	Stellen Sie sicher, dass Sie alle Punkte unter *Prüfen Sie zunächst Folgendes:* ➤➤ Seite 27 überprüft haben.
Wo kann ich die Netzwerkeinstellungen meines Brother-Gerätes, wie die IP-Adresse, finden?	Drucken Sie den Netzwerk-Konfigurationsbericht aus. Siehe *Druckereinstellungen-Seite drucken (für HL-5450DN(T))* ➤➤ Seite 29 oder *Ausdrucken des Netzwerk-Konfigurationsberichts (Für andere Modelle)* ➤➤ Seite 29.

Druckereinstellungen-Seite drucken (für HL-5450DN(T))

Hinweis

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

Die Druckereinstellungen-Seite druckt einen Bericht aus, der alle aktuellen Druckereinstellungen aufführt, einschließlich der Netzwerkdruckserver-Einstellungen.

Sie können die Druckereinstellungen-Seite über die Schaltfläche **Go** auf dem Gerät ausdrucken.

1. Stellen Sie sicher, dass die vordere Abdeckung geschlossen ist und dass das Netzkabel eingesteckt ist.
2. Schalten Sie das Gerät ein und warten Sie, bis es sich im Bereitschaftsstatus befindet.
3. Drücken Sie drei Mal innerhalb von 2 Sekunden **Go**. Das Gerät druckt die aktuelle Druckereinstellungen-Seite.

Ausdrucken des Netzwerk-Konfigurationsberichts (Für andere Modelle)

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.

Für HL-5470DW(T) und HL-6180DW(T)

1. Drücken Sie ▲ oder ▼, um `Geräte-Info` zu wählen.
   Drücken Sie **OK**.
2. Drücken Sie ▲ oder ▼, um `Netzeinst.druck` zu wählen.
   Drücken Sie **OK**.

Für DCP-8110DN, DCP-8150DN, DCP-8155DN, MFC-8510DN, MFC-8710DW und MFC-8910DW

1. Drücken Sie **Menü**.
2. (Für MFC-Modelle) Drücken Sie ▲ oder ▼, um `Ausdrucke` zu wählen.
   (Für DCP-Modelle) Drücken Sie ▲ oder ▼, um `Geräte-Info` zu wählen.
   Drücken Sie **OK**.
3. Drücken Sie ▲ oder ▼, um `Netzwerk-Konf.` zu wählen.
   Drücken Sie **OK**.
4. Drücken Sie **Start**.

Für DCP-8250DN und MFC-8950DW(T)

1. Drücken Sie `Menü`.
2. Drücken Sie ▲ oder ▼, bis `Ausdrucke` angezeigt wird, und drücken Sie dann `Ausdrucke`.
3. Drücken Sie `Netzwerk-Konf`.
4. Drücken Sie **Start**.

Für HL-S7000DN

1. Drücken Sie **Menu**.
2. Drücken Sie ▲ oder ▼, um `Geräte-Info` zu wählen.
   Drücken Sie **OK**.
3. Drücken Sie ▲ oder ▼, um `Netzeinst.druck` zu wählen.
   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.

Netzwerkbegriffe und -konzepte

SSL technischer Überblick

Secure Socket Layer (SSL) ist ein Verfahren zum Schutz der Daten auf der Transportebene, die über ein lokales Netzwerk oder WAN und unter Verwendung des Internet Printing Protocol (IPP) gesendet werden, um zu verhindern, dass unautorisierte Benutzer die Daten lesen.

Hierzu verwendet es Authentifizierungsprotokolle in Form von digitalen Schlüsseln, von denen es 2 Arten gibt:

- Ein öffentlicher Schlüssel – ist jedem bekannt, der druckt.
- Ein privater Schlüssel – ist nur dem Gerät bekannt, das zur Entschlüsselung von Paketen verwendet wird, die nur von diesem Gerät lesbar dargestellt werden können.

Der öffentliche Schlüssel verwendet entweder eine 1024-Bit- oder ein 2048-Bit-Verschlüsselung und ist im Inneren eines digitalen Zertifikats enthalten. Diese Zertifikate können entweder privat erstellt werden oder über eine Zertifizierungsstelle (Certificate Authority, CA) bezogen werden.

Es gibt drei verschiedene Schlüssel: Private (privat), Public (öffentlich) und Shared (gemeinsam).

Der Private Key, der nur dem Gerät bekannt ist, ist dem Public Key zugeordnet, aber nicht im digitalen Zertifikat des Clients (Senders) enthalten. Wenn der Benutzer als erstes die Verbindung hergestellt hat, sendet das Gerät den Public-Key mit dem Zertifikat mit. Der Client-PC vertraut darauf, dass der Public-Key von dem Gerät mit dem Zertifikat kommt. Der Client generiert den Shared Key und verschlüsselt ihn mit dem Public Key. Anschließend sendet er ihn an das Gerät. Das Gerät verschlüsselt den Shared-Key mit dem Private-Key. Nun verfügen das Gerät und der Client auf sichere Art über den Shared Key und richten eine sichere Verbindung für die Übertragung der Druckdaten ein.

Die Druckdaten werden mit dem Shared-Key ver- und entschlüsselt.

Durch SSL werden unautorisierte Benutzer nicht an dem Zugriff auf Datenpakete gehindert. Dennoch können sie diese nicht ohne den Private-Key lesen, der niemandem außer dem Gerät bekannt ist.

Er kann sowohl für kabellose als auch für Kabel-Netzwerke konfiguriert werden und funktioniert ebenfalls in Kombination mit anderen Sicherheitsmaßnahmen wie WPA-Schlüsseln und Firewalls, welche entsprechend konfiguriert sein müssen.

Netzwerk-Begriffe

- Secure Socket Layer (SSL)

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

- Internet Printing Protocol (IPP)

  IPP ist ein Standarddruckprotokoll für die Verwaltung und Durchführung von Druckaufträgen. Es kann sowohl lokal als auch global verwendet werden, sodass weltweit jeder auf demselben Gerät drucken kann.

- IPPS

  Die Version des Internet-Druckprotokolls (IPP Version 1.0), die SSL verwendet.

- HTTPS

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

- 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: Zertifikatregistrierungsanforderung)

  Mit der Zertifikatregistrierungsanforderung wird bei der Zertifizierungsstelle die Ausstellung eines Zertifikates beantragt. Die Zertifikatregistrierungsanforderung 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.

- 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.