Leitfaden Sicherheitsfunktionen

Wichtige Sicherheitsinformationen

- Das Standardkennwort zur Verwaltung der Einstellungen dieses Geräts ist auf der Unterseite des Geräts angegeben und mit „**Pwd**“ gekennzeichnet. Wir empfehlen, das Standardkennwort zum Schutz des Geräts vor unbefugtem Zugriff umgehend zu ändern.
- Wenn Sie Ihr Gerät mit einem externen Netzwerk wie dem Internet verbinden, stellen Sie sicher, dass Ihre Netzwerkumgebung mit einer separaten Firewall oder auf andere Weise geschützt ist, um Datenlecks aufgrund von nicht ordnungsgemäßen Einstellungen oder des nicht autorisierten Zugriffs durch böswillige Dritte zu vermeiden.
- Gibt es ein Signal in der Nähe, können Sie per WLAN eine LAN-Verbindung herstellen. Sind jedoch die Sicherheitseinstellungen nicht korrekt konfiguriert, kann das Signal von böswilligen Dritten abgefangen werden, was folgende Konsequenzen haben kann:
  - Diebstahl von persönlichen oder vertraulichen Informationen
  - Unbefugte Übertragung von Informationen an Parteien, die sich als die angegebenen Personen ausgeben
  - Verbreitung von übertragenen Kommunikationsinhalten, die abgefangen wurden

Zugehörige Informationen

- Netzwerk

Konfigurieren von Zertifikaten für die Gerätesicherheit

Sie müssen ein Zertifikat konfigurieren, um Ihr Gerät sicher im Netzwerk mit SSL/TLS zu verwalten. Sie müssen ein Zertifikat mit Web Based Management konfigurieren.

- Übersicht über die Funktionen von Sicherheitszertifikaten
- Erstellen und Installieren eines Zertifikats
- Erstellen eines selbstsignierten Zertifikats
- Erstellen einer Zertifikatregistrierungsanforderung (Certificate Signing Request, CSR) und Installieren eines Zertifikats einer Zertifizierungsstelle (CA)
- Im- und Exportieren des Zertifikats und des privaten Schlüssels
- Importieren und Exportieren eines CA-Zertifikats

Übersicht über die Funktionen von Sicherheitszertifikaten

Ihr Gerät unterstützt verschiedene Sicherheitszertifikate, um eine sichere Authentifizierung und Kommunikation mit dem Gerät zu ermöglichen. Die folgenden Sicherheitszertifikatsfunktionen können mit dem Gerät verwendet werden:

Die unterstützten Funktionen, Optionen und Einstellungen können je nach Modell unterschiedlich sein.

- SSL/TLS-Kommunikation
- IEEE 802.1x-Authentifizierung
- IPsec

Ihr Gerät unterstützt die folgenden Optionen:

- Vorinstalliertes Zertifikat

  Ihr Gerät verfügt über ein vorinstalliertes privates Zertifikat. Mit diesem Zertifikat können Sie SSL/TLS-Kommunikation nutzen, ohne ein anderes Zertifikat erstellen oder installieren zu müssen.

Mit dem vorinstallierten selbstsignierten Zertifikat wird Ihre Kommunikation bis zu einem bestimmten Grad geschützt. Wir empfehlen die Verwendung eines Zertifikats, das von einer vertrauenswürdigen Organisation ausgestellt wurde, 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 anderes Zertifikat von einer Zertifizierungsstelle erstellen oder installieren zu müssen.

- 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 vertrauenswürdigen externen Zertifizierungsstelle verwenden möchten:

  - Installation mit einer Zertifikatssignieranforderung (CSR, Certificate Signing Request) von diesem PrintServer.
  - Installation mit Import eines Zertifikats und eines privaten Schlüssels (Private Key).

- Zertifikat einer Zertifizierungsstelle (Certificate Authority, CA)

  Zur Verwendung eines Zertifizierungsstellenzertifikats, das die Zertifizierungsstelle identifiziert und seinen privaten Schlüssel besitzt, müssen Sie das Zertifizierungsstellenzertifikat von der Zertifizierungsstelle importieren, bevor Sie Netzwerk-Sicherheitsfunktionen konfigurieren.

- Wenn Sie die SSL/TLS-Kommunikation verwenden möchten, sollten Sie sich zuerst an Ihren Systemadministrator wenden.
- Wenn Sie den Druckserver auf die werkseitigen Standardeinstellungen zurücksetzen, wird das installierte Zertifikat einschließlich des privaten Schlüssels (Private Key) gelöscht. Wenn Sie nach dem Zurücksetzen des Druckservers dasselbe Zertifikat und denselben privaten Schlüssel verwenden möchten, sollten Sie diese vor dem Zurücksetzen exportieren und danach erneut installieren.

Zugehörige Informationen

- Konfigurieren von Zertifikaten für die Gerätesicherheit

Verwandte Themen:

- Konfigurieren der IEEE 802.1x-Authentifizierung für Ihr Netzwerk mithilfe von Web Based Management (Webbrowser)

Erstellen und Installieren eines Zertifikats

Es gibt zwei Optionen, wenn Sie ein Sicherheitszertifikat wählen: Verwenden Sie ein selbstsigniertes Zertifikat oder ein Zertifikat von einer Zertifizierungsstelle.

Option 1

Selbstsigniertes Zertifikat

1. Erstellen Sie ein selbstsigniertes Zertifikat mit Web Based Management.
2. Installieren Sie das selbstsignierte Zertifikat auf Ihrem Computer.

Option 2

Zertifikat einer Zertifizierungsstelle

1. Erstellen Sie eine Zertifikatregistrierungsanforderung (Certificate Signing Request, CSR) mit Web Based Management.
2. Installieren Sie das von der Zertifizierungsstelle ausgestellte Zertifikat mit Web Based Management auf dem Brother-Gerät.
3. Installieren Sie das Zertifikat auf Ihrem Computer.

Zugehörige Informationen

- Konfigurieren von Zertifikaten für die Gerätesicherheit

Erstellen eines selbstsignierten Zertifikats

1. Starten Sie Ihren Webbrowser.
2. Geben Sie „https://IP-Adresse des Geräts“ in die Adressleiste des Browsers ein (wobei „IP-Adresse des Geräts“ die IP-Adresse des Geräts ist).

   Beispiel:

   https://192.168.1.2

   Die IP-Adresse Ihres Geräts finden Sie im Netzwerkkonfigurationsbericht.
3. Geben Sie bei Bedarf das Kennwort in das Feld **Anmelden** ein und klicken Sie dann auf **Anmelden**.

   Das Standardkennwort zur Verwaltung der Einstellungen dieses Geräts ist auf der Geräterückseite oder der Geräteunterseite angegeben und mit „**Pwd**“ gekennzeichnet. Ändern Sie das Standardkennwort anhand der Anweisungen auf dem Bildschirm, wenn Sie sich zum ersten Mal anmelden.
4. Klicken Sie in der linken Navigationsleiste auf **Netzwerk** > **Sicherheit** > **Zertifikat**.

   Wenn die linke Navigationsleiste nicht angezeigt wird, navigieren Sie von ☰.
5. Klicken Sie auf **Privates Zertifikat erstellen**.
6. Geben Sie einen **Allgemeine Name** und ein **Gültigkeitsdauer** ein.
   - Die Länge des **Allgemeine Name** muss weniger als 64 Byte betragen. Geben Sie einen Bezeichner ein, wie eine IP-Adresse, Knotennamen oder einen Domänennamen, der beim Zugriff auf dieses Gerät über die SSL/TLS-Kommunikation verwendet wird. Der Knotenname wird standardmäßig angezeigt.
   - Eine Warnung wird angezeigt, wenn Sie das IPPS- oder HTTPS-Protokoll verwenden und einen anderen Namen in der URL als den **Allgemeine Name** eingeben, der für das selbstsignierte Zertifikat verwendet wurde.
7. Wählen Sie die Einstellung aus der Dropdown-Liste **Algorithmus des öffentlichen Schlüssels** aus.
8. Wählen Sie die Einstellung aus der Dropdown-Liste **Digest-Algorithmus** aus.
9. Klicken Sie auf **Senden**.

Zugehörige Informationen

- Konfigurieren von Zertifikaten für die Gerätesicherheit

Erstellen einer Zertifikatregistrierungsanforderung (Certificate Signing Request, CSR) und Installieren eines Zertifikats einer Zertifizierungsstelle (CA)

Wenn Sie bereits ein Zertifikat von einer externen vertrauenswürdigen Zertifizierungsstelle (CA) haben, können Sie das Zertifikat und den privaten Schlüssel auf dem Gerät speichern und sie durch Im- und Exportieren verwalten. Wenn Sie kein Zertifikat von einer externen vertrauenswürdigen Zertifizierungsstelle haben, erstellen Sie eine Zertifikatregistrierungsanforderung (Certificate Signing Request, CSR), senden Sie sie zur Authentifizierung an eine Zertifizierungsstelle und installieren Sie das Zertifikat, das Sie erhalten, auf Ihrem Gerät.

- Erstellen einer Zertifikatregistrierungsanforderung (Certificate Signing Request, CSR)
- Installieren eines Zertifikats auf dem Gerät

Erstellen einer Zertifikatregistrierungsanforderung (Certificate Signing Request, CSR)

Eine Zertifikatregistrierungsanforderung (Certificate Signing Request, CSR) ist eine Anforderung, die an eine Zertifizierungsstelle (CA) gesendet wird, um die Informationen zu authentifizieren, die im Zertifikat enthalten sind.

Wir empfehlen, ein Stammzertifikat der Zertifizierungsstelle auf Ihrem Computer zu installieren, bevor Sie die CSR erstellen.

1. Starten Sie Ihren Webbrowser.
2. Geben Sie „https://IP-Adresse des Geräts“ in die Adressleiste des Browsers ein (wobei „IP-Adresse des Geräts“ die IP-Adresse des Geräts ist).

   Beispiel:

   https://192.168.1.2

   Die IP-Adresse Ihres Geräts finden Sie im Netzwerkkonfigurationsbericht.
3. Geben Sie bei Bedarf das Kennwort in das Feld **Anmelden** ein und klicken Sie dann auf **Anmelden**.

   Das Standardkennwort zur Verwaltung der Einstellungen dieses Geräts ist auf der Geräterückseite oder der Geräteunterseite angegeben und mit „**Pwd**“ gekennzeichnet. Ändern Sie das Standardkennwort anhand der Anweisungen auf dem Bildschirm, wenn Sie sich zum ersten Mal anmelden.
4. Klicken Sie in der linken Navigationsleiste auf **Netzwerk** > **Sicherheit** > **Zertifikat**.

   Wenn die linke Navigationsleiste nicht angezeigt wird, navigieren Sie von ☰.
5. Klicken Sie auf **Zertifikatsignieranforderung (CSR) erstellen**.
6. Geben Sie einen **Allgemeine Name** (erforderlich) ein und ergänzen Sie weitere Informationen zu Ihrem **Organisation** (optional).

   - Ihre Unternehmensinformationen sind erforderlich, sodass die Zertifizierungsstelle Ihre Identität bestätigen und sie gegenüber anderen bezeugen kann.
   - Die Länge des **Allgemeine Name** muss bei weniger als 64 Byte liegen. Geben Sie einen Bezeichner ein, wie eine IP-Adresse, Knotennamen oder einen Domänennamen, der beim Zugriff auf dieses Gerät über die SSL/TLS-Kommunikation verwendet wird. Der Knotenname wird standardmäßig angezeigt. Der **Allgemeine Name** ist erforderlich.
   - Eine Warnung wird angezeigt, wenn Sie in der URL einen anderen Namen als den Allgemeinen Namen eingeben, der für das Zertifikat verwendet wurde.
   - Die Länge von **Organisation**, **Organisationseinheit**, **Ort** und **Bundesland** muss unter 64 Byte liegen.
   - Das **Land** sollte ein ISO 3166-Ländercode mit zwei Buchstaben sein.
   - Wenn Sie eine X.509v3-Zertifikaterweiterung konfigurieren, aktivieren Sie das Kontrollkästchen **Erweiterte Partition konfigurieren** und wählen Sie dann **Auto (IPv4 registrieren)** oder **Manuell**.
7. Wählen Sie die Einstellung aus der Dropdown-Liste **Algorithmus des öffentlichen Schlüssels** aus.
8. Wählen Sie die Einstellung aus der Dropdown-Liste **Digest-Algorithmus** aus.
9. Klicken Sie auf **Senden**.

   Die CSR wird auf dem Bildschirm angezeigt. Speichern Sie die CSR als Datei oder kopieren Sie sie und fügen Sie sie in ein Online-CSR-Formular ein, das von einer Zertifizierungsstelle angeboten wird.
10. Klicken Sie auf **Speichern**.

- Befolgen Sie die Richtlinie Ihrer Zertifizierungsstelle hinsichtlich des Verfahrens, wie eine CSR an die Zertifizierungsstelle gesendet wird.
- Wenn Sie die Stammzertifizierungsstelle des Unternehmens von Windows Server verwenden, empfehlen wir die Verwendung des Webservers für die Zertifikatsvorlage, um das Client-Zertifikat sicher zu erstellen. Wenn Sie ein Clientzertifikat für eine IEEE 802.1x-Umgebung mit der EAP-TLS-Authentifizierung erstellen, empfehlen wir die Verwendung von Benutzer für die Zertifikatsvorlage.

Zugehörige Informationen

- Erstellen einer Zertifikatregistrierungsanforderung (Certificate Signing Request, CSR) und Installieren eines Zertifikats einer Zertifizierungsstelle (CA)

Installieren eines Zertifikats auf dem Gerät

Wenn Sie ein Zertifikat von der Zertifizierungsstelle erhalten, befolgen Sie die Schritte unten, um es auf dem Druckserver zu installieren:

> Nur ein mit der Zertifikatsignaturanforderung (Certificate Signing Request, CSR) dieses Geräts ausgestelltes Zertifikat kann auf dem Gerät installiert werden. Wenn Sie eine andere CSR erstellen möchten, stellen Sie sicher, dass das Zertifikat installiert wurde, bevor Sie eine neue CSR erstellen. Erstellen Sie eine weitere CSR erst, nachdem Sie das Zertifikat auf dem Gerät installiert haben. Andernfalls ist die CSR, die Sie vor der Installation der neuen CSR gestellt haben, ungültig.

1. Starten Sie Ihren Webbrowser.
2. Geben Sie „https://IP-Adresse des Geräts“ in die Adressleiste des Browsers ein (wobei „IP-Adresse des Geräts“ die IP-Adresse des Geräts ist).

   Beispiel:

   https://192.168.1.2

   Die IP-Adresse Ihres Geräts finden Sie im Netzwerkkonfigurationsbericht.
3. Geben Sie bei Bedarf das Kennwort in das Feld **Anmelden** ein und klicken Sie dann auf **Anmelden**.

   Das Standardkennwort zur Verwaltung der Einstellungen dieses Geräts ist auf der Geräterückseite oder der Geräteunterseite angegeben und mit „**Pwd**“ gekennzeichnet. Ändern Sie das Standardkennwort anhand der Anweisungen auf dem Bildschirm, wenn Sie sich zum ersten Mal anmelden.
4. Klicken Sie in der linken Navigationsleiste auf **Netzwerk** > **Sicherheit** > **Zertifikat**.

   Wenn die linke Navigationsleiste nicht angezeigt wird, navigieren Sie von ☰.
5. Klicken Sie auf **Zertifikat installieren**.
6. Wechseln Sie zu der Datei, die das von der Zertifizierungsstelle ausgestellte Zertifikat enthält, und klicken Sie dann auf **Senden**.

   Das Zertifikat wird erstellt und im Speicher Ihres Geräts abgelegt.

Zur Verwendung der SSL/TLS-Kommunikation muss das Stammzertifikat der Zertifizierungsstelle auf dem Computer installiert sein. Wenden Sie sich an Ihren Netzwerkadministrator.

Zugehörige Informationen

- Erstellen einer Zertifikatregistrierungsanforderung (Certificate Signing Request, CSR) und Installieren eines Zertifikats einer Zertifizierungsstelle (CA)

Im- und Exportieren des Zertifikats und des privaten Schlüssels

Speichern Sie das Zertifikat und den privaten Schlüssel auf dem Gerät und verwalten Sie sie durch Im- und Exportieren.

- Importieren des Zertifikats und des privaten Schlüssels
- Exportieren des Zertifikats und des privaten Schlüssels

Importieren des Zertifikats und des privaten Schlüssels

1. Starten Sie Ihren Webbrowser.
2. Geben Sie „https://IP-Adresse des Geräts“ in die Adressleiste des Browsers ein (wobei „IP-Adresse des Geräts“ die IP-Adresse des Geräts ist).

   Beispiel:

   https://192.168.1.2

   Die IP-Adresse Ihres Geräts finden Sie im Netzwerkkonfigurationsbericht.
3. Geben Sie bei Bedarf das Kennwort in das Feld **Anmelden** ein und klicken Sie dann auf **Anmelden**.

Das Standardkennwort zur Verwaltung der Einstellungen dieses Geräts ist auf der Geräterückseite oder der Geräteunterseite angegeben und mit „**Pwd**“ gekennzeichnet. Ändern Sie das Standardkennwort anhand der Anweisungen auf dem Bildschirm, wenn Sie sich zum ersten Mal anmelden.

4. Klicken Sie in der linken Navigationsleiste auf **Netzwerk** > **Sicherheit** > **Zertifikat**.

Wenn die linke Navigationsleiste nicht angezeigt wird, navigieren Sie von ☰.

5. Klicken Sie auf **Zertifikat und Private Key importieren**.
6. Suchen und wählen Sie die Datei aus, die Sie importieren möchten.
7. Geben Sie das Kennwort ein, wenn die Datei verschlüsselt ist, und klicken Sie dann auf **Senden**.

Das Zertifikat und der private Schlüssel werden auf das Gerät importiert.

Zugehörige Informationen

- Im- und Exportieren des Zertifikats und des privaten Schlüssels

Exportieren des Zertifikats und des privaten Schlüssels

1. Starten Sie Ihren Webbrowser.
2. Geben Sie „https://IP-Adresse des Geräts“ in die Adressleiste des Browsers ein (wobei „IP-Adresse des Geräts“ die IP-Adresse des Geräts ist).

   Beispiel:

   https://192.168.1.2

   Die IP-Adresse Ihres Geräts finden Sie im Netzwerkkonfigurationsbericht.
3. Geben Sie bei Bedarf das Kennwort in das Feld **Anmelden** ein und klicken Sie dann auf **Anmelden**.

Das Standardkennwort zur Verwaltung der Einstellungen dieses Geräts ist auf der Geräterückseite oder der Geräteunterseite angegeben und mit „**Pwd**“ gekennzeichnet. Ändern Sie das Standardkennwort anhand der Anweisungen auf dem Bildschirm, wenn Sie sich zum ersten Mal anmelden.

4. Klicken Sie in der linken Navigationsleiste auf **Netzwerk** > **Sicherheit** > **Zertifikat**.

Wenn die linke Navigationsleiste nicht angezeigt wird, navigieren Sie von ☰.

5. Klicken Sie auf **Exportieren**, das für **Zertifikatliste** angezeigt wird.
6. Geben Sie das Kennwort ein, wenn Sie die Datei verschlüsseln möchten.

   Wenn ein leeres Kennwort verwendet wird, wird die Ausgabe nicht verschlüsselt.
7. Geben Sie das Kennwort zur Bestätigung erneut ein und drücken Sie dann **Senden**.
8. Klicken Sie auf **Speichern**.

Das Zertifikat und der private Schlüssel werden auf Ihren Computer exportiert.

Sie können auch das Zertifikat auf Ihren Computer importieren.

Zugehörige Informationen

- Im- und Exportieren des Zertifikats und des privaten Schlüssels

Importieren und Exportieren eines CA-Zertifikats

Sie können CA-Zertifikate im Brother-Gerät importieren, exportieren und speichern.

- Importieren eines CA-Zertifikats
- Exportieren eines CA-Zertifikats

Importieren eines CA-Zertifikats

1. Starten Sie Ihren Webbrowser.
2. Geben Sie „https://IP-Adresse des Geräts“ in die Adressleiste des Browsers ein (wobei „IP-Adresse des Geräts“ die IP-Adresse des Geräts ist).

   Beispiel:

   https://192.168.1.2

   Die IP-Adresse Ihres Geräts finden Sie im Netzwerkkonfigurationsbericht.
3. Geben Sie bei Bedarf das Kennwort in das Feld **Anmelden** ein und klicken Sie dann auf **Anmelden**.

   Das Standardkennwort zur Verwaltung der Einstellungen dieses Geräts ist auf der Geräterückseite oder der Geräteunterseite angegeben und mit „**Pwd**“ gekennzeichnet. Ändern Sie das Standardkennwort anhand der Anweisungen auf dem Bildschirm, wenn Sie sich zum ersten Mal anmelden.
4. Klicken Sie in der linken Navigationsleiste auf **Netzwerk** > **Sicherheit** > **CA-Zertifikat**.

   Wenn die linke Navigationsleiste nicht angezeigt wird, navigieren Sie von ☰.
5. Klicken Sie auf **CA-Zertifikat importieren**.
6. Rufen Sie die Datei auf, die Sie importieren möchten.
7. Klicken Sie auf **Senden**.

Zugehörige Informationen

- Importieren und Exportieren eines CA-Zertifikats

Exportieren eines CA-Zertifikats

1. Starten Sie Ihren Webbrowser.
2. Geben Sie „https://IP-Adresse des Geräts“ in die Adressleiste des Browsers ein (wobei „IP-Adresse des Geräts“ die IP-Adresse des Geräts ist).

   Beispiel:

   https://192.168.1.2

   Die IP-Adresse Ihres Geräts finden Sie im Netzwerkkonfigurationsbericht.
3. Geben Sie bei Bedarf das Kennwort in das Feld **Anmelden** ein und klicken Sie dann auf **Anmelden**.

Das Standardkennwort zur Verwaltung der Einstellungen dieses Geräts ist auf der Geräterückseite oder der Geräteunterseite angegeben und mit „**Pwd**“ gekennzeichnet. Ändern Sie das Standardkennwort anhand der Anweisungen auf dem Bildschirm, wenn Sie sich zum ersten Mal anmelden.

4. Klicken Sie in der linken Navigationsleiste auf **Netzwerk** > **Sicherheit** > **CA-Zertifikat**.

Wenn die linke Navigationsleiste nicht angezeigt wird, navigieren Sie von ☰.

5. Wählen Sie das Zertifikat, das Sie exportieren möchten, und klicken Sie auf **Exportieren**.
6. Klicken Sie auf **Senden**.

Zugehörige Informationen

- Importieren und Exportieren eines CA-Zertifikats

Verwenden von SSL/TLS

- Sicheres Verwalten des Netzwerkgerätes mit SSL/TLS
- Sicheres Drucken von Dokumenten mit SSL/TLS
- Sicheres Senden oder Empfangen von E-Mails mit SSL/TLS

Sicheres Verwalten des Netzwerkgerätes mit SSL/TLS

- Konfigurieren eines Zertifikats für SSL/TLS und der verfügbaren Protokolle
- Zugriff auf Web Based Management über SSL/TLS
- Installieren des selbstsignierten Zertifikats für Windows-Benutzer als Administrator
- Konfigurieren von Zertifikaten für die Gerätesicherheit

Konfigurieren eines Zertifikats für SSL/TLS und der verfügbaren Protokolle

Konfigurieren Sie ein Zertifikat auf Ihrem Gerät unter Verwendung von Web Based Management, bevor Sie die SSL/TLS-Kommunikation verwenden.

1. Starten Sie Ihren Webbrowser.
2. Geben Sie „https://IP-Adresse des Geräts“ in die Adressleiste des Browsers ein (wobei „IP-Adresse des Geräts“ die IP-Adresse des Geräts ist).

   Beispiel:

   https://192.168.1.2

   Die IP-Adresse Ihres Geräts finden Sie im Netzwerkkonfigurationsbericht.
3. Geben Sie bei Bedarf das Kennwort in das Feld **Anmelden** ein und klicken Sie dann auf **Anmelden**.

   Das Standardkennwort zur Verwaltung der Einstellungen dieses Geräts ist auf der Geräterückseite oder der Geräteunterseite angegeben und mit „**Pwd**“ gekennzeichnet. Ändern Sie das Standardkennwort anhand der Anweisungen auf dem Bildschirm, wenn Sie sich zum ersten Mal anmelden.
4. Klicken Sie in der linken Navigationsleiste auf **Netzwerk** > **Netzwerk** > **Protokoll**.

   Wenn die linke Navigationsleiste nicht angezeigt wird, navigieren Sie von ☰.
5. Klicken Sie auf **HTTP-Servereinstellungen**.
6. Wählen Sie das Zertifikat, das Sie konfigurieren möchten, in der Dropdown-Liste **Wählen Sie das Zertifikat** aus.
7. Klicken Sie auf **Senden**.
8. Klicken Sie auf **Ja**, um Ihren Druckserver neu zu starten.

Zugehörige Informationen

- Sicheres Verwalten des Netzwerkgerätes mit SSL/TLS

Verwandte Themen:

- Sicheres Drucken von Dokumenten mit SSL/TLS

Zugriff auf Web Based Management über SSL/TLS

Um Ihr Netzwerkgerät sicher zu verwalten, müssen Sie die Verwaltungs-Dienstprogramme mit Sicherheitsprotokollen verwenden.

- Zur Verwendung HTTPS-Protokolls muss HTTPS auf Ihrem Gerät aktiviert sein. Das HTTPS-Protokoll ist standardmäßig aktiviert.
- Sie können die HTTPS-Protokolleinstellungen über den Bildschirm Web Based Management ändern.

1. Starten Sie Ihren Webbrowser.
2. Geben Sie „https://IP-Adresse des Geräts“ in die Adressleiste des Browsers ein (wobei „IP-Adresse des Geräts“ die IP-Adresse des Geräts ist).

   Beispiel:

   https://192.168.1.2

   Die IP-Adresse Ihres Geräts finden Sie im Netzwerkkonfigurationsbericht.
3. Geben Sie bei Bedarf das Kennwort in das Feld **Anmelden** ein und klicken Sie dann auf **Anmelden**.

Das Standardkennwort zur Verwaltung der Einstellungen dieses Geräts ist auf der Geräterückseite oder der Geräteunterseite angegeben und mit „**Pwd**“ gekennzeichnet. Ändern Sie das Standardkennwort anhand der Anweisungen auf dem Bildschirm, wenn Sie sich zum ersten Mal anmelden.

4. Sie können nun über HTTPS auf das Gerät zugreifen.

Zugehörige Informationen

- Sicheres Verwalten des Netzwerkgerätes mit SSL/TLS

Installieren des selbstsignierten Zertifikats für Windows-Benutzer als Administrator

- Die folgenden Schritte gelten für Microsoft Edge. Wenn Sie einen anderen Webbrowser verwenden, lesen Sie in der Dokumentation oder der Onlinehilfe Ihres Webbrowsers nach, wie Zertifikate installiert werden.
- Stellen Sie sicher, dass Sie das selbstsignierte Zertifikat mit Web Based Management erstellt haben.

1. Klicken Sie mit der rechten Maustaste auf das Symbol **Microsoft Edge** und klicken Sie dann auf **Als Administrator ausführen**.

   Wenn der Bildschirm **Benutzerkontensteuerung** angezeigt wird, klicken Sie auf **Ja**.
2. Geben Sie „https://IP-Adresse des Geräts“ in die Adressleiste des Browsers ein (wobei „IP-Adresse des Geräts“ die IP-Adresse des Geräts ist).

   Beispiel:

   https://192.168.1.2

   Die IP-Adresse Ihres Geräts finden Sie im Netzwerkkonfigurationsbericht.
3. Wenn Ihre Verbindung nicht privat ist, klicken Sie auf die Schaltfläche **Erweitert** und wechseln Sie zur Webseite.
4. Geben Sie bei Bedarf das Kennwort in das Feld **Anmelden** ein und klicken Sie dann auf **Anmelden**.

   Das Standardkennwort zur Verwaltung der Einstellungen dieses Geräts ist auf der Geräterückseite oder der Geräteunterseite angegeben und mit „**Pwd**“ gekennzeichnet. Ändern Sie das Standardkennwort anhand der Anweisungen auf dem Bildschirm, wenn Sie sich zum ersten Mal anmelden.
5. Klicken Sie in der linken Navigationsleiste auf **Netzwerk** > **Sicherheit** > **Zertifikat**.

   Wenn die linke Navigationsleiste nicht angezeigt wird, navigieren Sie von ☰.
6. Klicken Sie auf **Exportieren**.
7. Zum Verschlüsseln der Ausgabedatei geben Sie das Kennwort in das Feld **Kennwort eingeben** ein. Wenn das Feld **Kennwort eingeben** leer ist, wird Ihre Ausgabedatei nicht verschlüsselt.
8. Geben Sie im Feld **Kennwort bestätigen** das Kennwort erneut ein und klicken Sie dann auf **Senden**.
9. Klicken Sie auf die heruntergeladene Datei, um sie zu öffnen.
10. Wenn der **Zertifikatimport-Assistent** angezeigt wird, klicken Sie auf **Weiter**.
11. Klicken Sie auf **Weiter**.
12. Geben Sie falls erforderlich ein Kennwort ein und klicken Sie auf **Weiter**.
13. Wählen Sie **Alle Zertifikate in folgendem Speicher speichern** und klicken Sie dann auf **Durchsuchen...**.
14. Aktivieren Sie **Vertrauenswürdige Stammzertifizierungsstellen** und klicken Sie dann auf **OK**.
15. Klicken Sie auf **Weiter**.
16. Klicken Sie auf **Fertig stellen**.
17. Klicken Sie auf **Ja**, wenn der Fingerabdruck richtig ist.
18. Klicken Sie auf **OK**.

Zugehörige Informationen

- Sicheres Verwalten des Netzwerkgerätes mit SSL/TLS

Sicheres Drucken von Dokumenten mit SSL/TLS

- Drucken von Dokumenten mit IPPS
- Konfigurieren eines Zertifikats für SSL/TLS und der verfügbaren Protokolle
- Konfigurieren von Zertifikaten für die Gerätesicherheit

Drucken von Dokumenten mit IPPS

Um Dokumente sicher mit dem IPP-Protokoll zu drucken, verwenden Sie das IPPS-Protokoll.

1. Starten Sie Ihren Webbrowser.
2. Geben Sie „https://IP-Adresse des Geräts“ in die Adressleiste des Browsers ein (wobei „IP-Adresse des Geräts“ die IP-Adresse des Geräts ist).

   Beispiel:

   https://192.168.1.2

   Die IP-Adresse Ihres Geräts finden Sie im Netzwerkkonfigurationsbericht.
3. Geben Sie bei Bedarf das Kennwort in das Feld **Anmelden** ein und klicken Sie dann auf **Anmelden**.

   Das Standardkennwort zur Verwaltung der Einstellungen dieses Geräts ist auf der Geräterückseite oder der Geräteunterseite angegeben und mit „**Pwd**“ gekennzeichnet. Ändern Sie das Standardkennwort anhand der Anweisungen auf dem Bildschirm, wenn Sie sich zum ersten Mal anmelden.
4. Klicken Sie in der linken Navigationsleiste auf **Netzwerk** > **Netzwerk** > **Protokoll**.

   Wenn die linke Navigationsleiste nicht angezeigt wird, navigieren Sie von ☰.
5. Stellen Sie sicher, dass das Kontrollkästchen **IPP** aktiviert ist.

   Wenn das Kontrollkästchen **IPP** nicht aktiviert ist, aktivieren Sie das Kontrollkästchen **IPP** und klicken Sie dann auf **Senden**.

   Starten Sie das Gerät neu, um die Konfiguration zu übernehmen.

   Kehren Sie nach dem Neustart des Geräts zur Webseite des Geräts zurück, geben Sie das Kennwort ein und klicken Sie in der linken Navigationsleiste auf **Netzwerk** > **Netzwerk** > **Protokoll**.
6. Klicken Sie auf **HTTP-Servereinstellungen**.
7. Aktivieren Sie das Kontrollkästchen **HTTPS** im Bereich **IPP** und klicken Sie dann auf **Senden**.
8. Starten Sie das Gerät neu, um die Konfiguration zu übernehmen.

Die Kommunikation mit IPPS kann keinen unautorisierten Zugriff auf den Druckserver verhindern.

Zugehörige Informationen

- Sicheres Drucken von Dokumenten mit SSL/TLS

Verwenden von SNMPv3

- Sicheres Verwalten Ihres Netzwerkgerätes mit SNMPv3

Sicheres Verwalten Ihres Netzwerkgerätes mit SNMPv3

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

1. Starten Sie Ihren Webbrowser.
2. Geben Sie „https://Allgemeiner Name“ in die Adressleiste Ihres Browsers ein. (Wobei „Allgemeiner Name“ der allgemeine Name ist, den Sie dem Zertifikat zugewiesen haben; dies kann die IP-Adresse, der Knotenname oder der Domänenname sein.)
3. Geben Sie bei Bedarf das Kennwort in das Feld **Anmelden** ein und klicken Sie dann auf **Anmelden**.

Das Standardkennwort zur Verwaltung der Einstellungen dieses Geräts ist auf der Geräterückseite oder der Geräteunterseite angegeben und mit „**Pwd**“ gekennzeichnet. Ändern Sie das Standardkennwort anhand der Anweisungen auf dem Bildschirm, wenn Sie sich zum ersten Mal anmelden.

4. Klicken Sie in der linken Navigationsleiste auf **Netzwerk** > **Netzwerk** > **Protokoll**.

Wenn die linke Navigationsleiste nicht angezeigt wird, navigieren Sie von ☰.

5. Stellen Sie sicher, dass die Einstellung **SNMP** aktiviert ist, und klicken Sie dann auf **Erweitere Einstellungen**.
6. Konfigurieren Sie die SNMPv1/v2c-Moduseinstellungen.

Option	Beschreibung
SNMP v1/v2c Lese-/ Schreibzugriff	Der Druckserver verwendet Version 1 und Version 2c des SNMP-Protokolls. Sie können in diesem Modus alle Ihre Geräte-Anwendungen verwenden. Er ist aber nicht sicher, da der Benutzer nicht authentifiziert wird und die Daten nicht verschlüsselt sind.
SNMP v1/v2c Nur-Lese-Zugriff	Der Druckserver verwendet Version 1 und Version 2c des SNMP-Protokolls mit schreibgeschütztem Zugriff.
Deaktiviert	Deaktivieren Sie Version 1 und Version 2c des SNMP-Protokolls. Alle Anwendungen, die SNMPv1/v2c verwenden, werden eingeschränkt. Um die Verwendung von SNMPv1/v2c-Anwendungen zu erlauben, verwenden Sie den Modus **SNMP v1/v2c Nur-Lese-Zugriff** oder **SNMP v1/v2c Lese-/ Schreibzugriff**.

7. Konfigurieren Sie die SNMPv3-Moduseinstellungen.

Option	Beschreibung
Aktiviert	Der Druckserver verwendet Version 3 des SNMP-Protokolls. Um den Druckerserver sicher zu verwalten, verwenden Sie den SNMPv3-Modus und konfigurieren Sie dann die Einstellungen.
Deaktiviert	Deaktivieren Sie Version 3 des SNMP-Protokolls. Alle Anwendungen, die SNMPv3 verwenden, werden eingeschränkt. Um die Verwendung von SNMPv3-Anwendungen zu erlauben, verwenden Sie den SNMPv3-Modus.

8. Klicken Sie auf **Senden**.

Wählen Sie die gewünschten Optionen aus, wenn das Gerät die Protokolleinstellungen-Optionen anzeigt.

9. Starten Sie das Gerät neu, um die Konfiguration zu übernehmen.

Zugehörige Informationen

- Verwenden von SNMPv3

Verwenden der IEEE 802.1x-Authentifizierung für Ihr Netzwerk

- Was ist die IEEE 802.1x-Authentifizierung?
- Konfigurieren der IEEE 802.1x-Authentifizierung für Ihr Netzwerk mithilfe von Web Based Management (Webbrowser)
- IEEE 802.1x-Authentifizierungsmethoden

Was ist die IEEE 802.1x-Authentifizierung?

IEEE 802.1x ist ein IEEE-Standard, der den Zugriff von unautorisierten Netzwerkgeräten beschränkt. Das Brother-Gerät sendet über den Zugangspunkt oder Hub eine Authentifizierungsanfrage an einen RADIUS-Server (Authentifizierungsserver). Nachdem Ihre Anfrage vom RADIUS-Server verifiziert wurde, kann das Gerät auf das Netzwerk zugreifen.

Zugehörige Informationen

- Verwenden der IEEE 802.1x-Authentifizierung für Ihr Netzwerk

Konfigurieren der IEEE 802.1x-Authentifizierung für Ihr Netzwerk mithilfe von Web Based Management (Webbrowser)

- Wenn Sie Ihr Gerät mit der 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 den Netzwerkadministrator. Wenn mehrere Zertifikate installiert wurden, sollte der Name des zu verwendenden Zertifikats notiert werden.
- 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-Zertifikats erforderlich ist.

Sie können die IEEE 802.1x-Authentifizierung auch mithilfe des Wireless Setup-Assistenten über das Funktionstastenfeld (Wireless-Netzwerk) konfigurieren.

1. Starten Sie Ihren Webbrowser.
2. Geben Sie „https://IP-Adresse des Geräts“ in die Adressleiste des Browsers ein (wobei „IP-Adresse des Geräts“ die IP-Adresse des Geräts ist).

   Beispiel:

   https://192.168.1.2

   Die IP-Adresse Ihres Geräts finden Sie im Netzwerkkonfigurationsbericht.
3. Geben Sie bei Bedarf das Kennwort in das Feld **Anmelden** ein und klicken Sie dann auf **Anmelden**.

Das Standardkennwort zur Verwaltung der Einstellungen dieses Geräts ist auf der Geräterückseite oder der Geräteunterseite angegeben und mit „**Pwd**“ gekennzeichnet. Ändern Sie das Standardkennwort anhand der Anweisungen auf dem Bildschirm, wenn Sie sich zum ersten Mal anmelden.

4. Klicken Sie in der linken Navigationsleiste auf **Netzwerk**.

Wenn die linke Navigationsleiste nicht angezeigt wird, navigieren Sie von ☰.

5. Sie haben folgende Möglichkeiten:
   - Für das verkabelte Netzwerk

     Klicken Sie auf **Verkabelt** > **802.1x-Authentifizierungs**.
   - Für das Wireless-Netzwerk

     Klicken Sie auf **Kabellos** > **Kabellos (Firmenbereich)**.
6. Konfigurieren Sie die IEEE 802.1x-Authentifizierungseinstellungen.

- Um die IEEE 802.1x-Authentifizierung für verkabelte Netzwerke zu aktivieren, wählen Sie **Aktiviert** für **802.1x-Status (verkabelt)** auf der Seite **802.1x-Authentifizierungs** aus.
- Wenn Sie die **EAP-TLS**-Authentifizierung verwenden, müssen Sie das Client-Zertifikat aus der Dropdown-Liste **Client-Zertifikat** auswählen, das zur Verifizierung installiert wurde (angezeigt mit dem Zertifikatsnamen).
- Wenn Sie die **EAP-FAST**-, **PEAP**-, **EAP-TTLS**- oder **EAP-TLS**-Authentifizierung auswählen, wählen Sie das Verifizierungsverfahren aus der Dropdown-Liste **Server-Zertifikat-Verifizierung** aus. Verifizieren Sie das Serverzertifikat über das CA-Zertifikat, das zuvor auf das Gerät importiert wurde und von der Zertifizierungsstelle ausgestellt wurde, die das Serverzertifikat signiert hat.

Wählen Sie eine der folgenden Verifizierungsmethoden aus der Dropdown-Liste **Server-Zertifikat-Verifizierung** aus:

Option	Beschreibung
Keine Verifizierung	Dem Serverzertifikat kann immer vertraut werden. Die Verifizierung wird nicht durchgeführt.
CA-Zert.	Das Verifizierungsverfahren zur Überprüfung der CA-Zuverlässigkeit des Serverzertifikats mit dem CA-Zertifikat, das von der Zertifizierungsstelle ausgestellt wurde, die das Serverzertifikat signiert hat.
CA-Zert. + Server-ID	Die Verifizierungsmethode zur Überprüfung des allgemeinen Namens [1] Wert des Serverzertifikats, zusätzlich zur CA-Zuverlässigkeit des Serverzertifikats.

7. Klicken Sie auf **Senden**, wenn Sie die Konfiguration beendet haben.

   Für verkabelte Netzwerke: Verbinden Sie das Gerät nach der Konfiguration mit dem IEEE 802.1x-unterstützten Netzwerk. Drucken Sie nach einigen Minuten den Netzwerkkonfigurationsbericht aus, um den <**Wired IEEE 802.1x**>-Status zu überprüfen.

Option	Beschreibung
Success	Die verkabelte IEEE 802.1x-Funktion ist aktiviert und die Authentifizierung war erfolgreich.
Failed	Die verkabelte IEEE 802.1x-Funktion ist aktiviert, die Authentifizierung ist aber fehlgeschlagen.
Off	Die verkabelte IEEE 802.1x-Funktion ist nicht verfügbar.

Zugehörige Informationen

- Verwenden der IEEE 802.1x-Authentifizierung für Ihr Netzwerk

Verwandte Themen:

- Übersicht über die Funktionen von Sicherheitszertifikaten
- Konfigurieren von Zertifikaten für die Gerätesicherheit

1 Die Verifizierung des allgemeinen Namens vergleicht den allgemeinen Namen auf dem Serverzertifikat mit der Zeichenfolge, die für **Server-ID** konfiguriert ist. Bevor Sie dieses Verfahren verwenden, wenden Sie sich an Ihren Systemadministrator und fragen Sie ihn nach dem allgemeinen Namen des Serverzertifikats, und konfigurieren Sie dann den Wert **Server-ID**.

IEEE 802.1x-Authentifizierungsmethoden

EAP-FAST

Das Extensible Authentication Protocol-Flexible Authentication via Secured Tunneling (EAP-FAST) wurde von Cisco Systems, Inc. entwickelt. Es verwendet eine Benutzer-ID und ein Kennwort für die Authentifizierung und symmetrische Schlüsselalgorithmen, um einen getunnelten Authentifizierungsprozess zu erzielen.

Ihr Brother-Gerät unterstützt die folgenden inneren Authentifizierungsmethoden:

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

EAP-MD5 (Verkabeltes Netzwerk)

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

PEAP

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

Ihr Brother-Gerät unterstützt die folgenden inneren Authentifizierungsmethoden:

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

Die Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) wurde von Funk Software und Certicom entwickelt. EAP-TTLS erstellt einen ähnlichen verschlüsselten SSL-Tunnel wie PEAP zwischen einem Client und einem Authentifizierungsserver, um eine Benutzer-ID und ein Kennwort zu senden. EAP-TTLS ermöglicht eine gegenseitige Authentifizierung von Server und Client.

Ihr Brother-Gerät unterstützt die folgenden inneren Authentifizierungsmethoden:

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

EAP-TLS

Die Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) erfordert eine digitale Zertifikatauthentifizierung beim Client und einem Authentifizierungsserver.

Zugehörige Informationen

- Verwenden der IEEE 802.1x-Authentifizierung für Ihr Netzwerk