Leitfaden Sicherheitsfunktionen

Inhaltsverzeichnis

Einleitung ... 1
Zu den Hinweisen ... 2
Warenzeichen ... 3
Copyright ... 4
Vor der Verwendung der Netzwerk-Sicherheitsfunktionen ... 5
Deaktivieren unnötiger Protokolle ... 6
Netzwerksicherheit ... 7
Konfigurieren von Zertifikaten für die Gerätesicherheit ... 8
Übersicht über die Funktionen von Sicherheitszertifikaten ... 9
Erstellen und Installieren eines Zertifikats ... 10
Erstellen eines selbstsignierten Zertifikats ... 11
Erstellen einer Zertifikatregistrierungsanforderung (Certificate Signing Request, CSR) und Installieren eines Zertifikats einer Zertifizierungsstelle (CA) ... 12
Im- und Exportieren des Zertifikats und des privaten Schlüssels ... 16
Importieren und Exportieren eines CA-Zertifikats ... 19
Verwenden von SSL/TLS ... 22
Sicheres Verwalten des Netzwerkgerätes mit SSL/TLS ... 23
Sicheres Drucken von Dokumenten mit SSL/TLS ... 27
Verwenden von SNMPv3 ... 29
Sicheres Verwalten Ihres Netzwerkgerätes mit SNMPv3 ... 30
Verwenden von IPsec ... 32
Einführung in IPsec ... 33
Konfigurieren von IPsec mit Web Based Management ... 34
Konfigurieren einer IPsec-Adressvorlage mit Web Based Management ... 36
Konfigurieren einer IPsec-Vorlage mit Web Based Management ... 38
Verwenden der IEEE 802.1x-Authentifizierung für Ihr Netzwerk ... 48
Was ist die IEEE 802.1x-Authentifizierung? ... 49
Konfigurieren der IEEE 802.1x-Authentifizierung für Ihr Netzwerk mithilfe von Web Based Management (Webbrowser) ... 50
IEEE 802.1x-Authentifizierungsmethoden ... 52
Benutzerauthentifizierung ... 53
Verwenden der Active Directory-Authentifizierung ... 54
Einführung in die Active Directory-Authentifizierung ... 55
Konfigurieren der Active Directory-Authentifizierung mit Web Based Management ... 56
Anmelden zum Ändern der Geräteeinstellungen über das Funktionstastenfeld des Geräts (Active Directory-Authentifizierung) ... 58
Verwenden der LDAP-Authentifizierung ... 59
Einführung in die LDAP-Authentifizierung ... 60
Konfigurieren der LDAP-Authentifizierung mit Web Based Management ... 61
Anmelden zum Ändern der Geräteeinstellungen über das Funktionstastenfeld des Geräts (LDAP-Authentifizierung) ... 63
Verwenden der Benutzersperre 3.0 ... 64
Vor der Verwendung der Benutzersperre 3.0 ... 65
Konfigurieren der Benutzersperre 3.0 mit Web Based Management ... 66
Scannen mit Benutzersperre 3.0 ... 67
Konfigurieren des Modus „Allgemeiner Benutzer“ für die Benutzersperre 3.0 ... 68

Konfigurieren der Einstellungen für den persönlichen Startbildschirm mit Web Based Management ... 69
Weitere Funktionen von der Benutzersperre 3.0 ... 70
Registrieren einer neuen IC-Karte über das Funktionstastenfeld des Geräts ... 71
Ein externes IC-Kartenlesegerät registrieren ... 72
Sicheres Senden oder Empfangen von E-Mails ... 73
Konfigurieren des E-Mail-Versands oder -Empfangs mit Web Based Management ... 74
Senden einer E-Mail mit Benutzerauthentifizierung ... 75
Sicheres Senden oder Empfangen von E-Mails mit SSL/TLS ... 76
Speichern des Druckprotokolls im Netzwerk ... 77
Speichern des Druckprotokolls im Netzwerk - Überblick ... 78
Konfigurieren der Einstellungen für Speichern des Druckprotokolls im Netzwerk mit Web Based Management ... 79
Verwenden der Fehlererkennungseinstellung von Speichern des Druckprotokolls im Netzwerk ... 81
Verwenden von Speichern des Druckprotokolls im Netzwerk mit Benutzersperre 3.0 ... 83

Einleitung

- Zu den Hinweisen
- Warenzeichen
- Copyright
- Vor der Verwendung der Netzwerk-Sicherheitsfunktionen

Zu den Hinweisen

In diesem Benutzerhandbuch werden folgende Symbole und Konventionen verwendet:

WICHTIG	WICHTIG weist auf eine potenziell gefährliche Situation hin, die bei Nichtvermeidung zu Sachschäden oder zu Funktionsausfall des Gerätes führen kann.
HINWEIS	HINWEIS spezifiziert die Betriebsumgebung, die Installationsbedingungen oder besondere Einsatzbedingungen.
	Das Tipps-Symbol macht auf hilfreiche Hinweise und zusätzliche Informationen aufmerksam.
Fett	Fettdruck kennzeichnet Schaltflächen auf dem Funktionstastenfeld des Gerätes oder Optionen und Schaltflächen auf dem Computer-Bildschirm.
Kursiv	Italicized Schrift emphasizes wichtige Punkte hervor oder verweist auf verwandte Themen.

Zugehörige Informationen

- Einleitung

Warenzeichen

Adobe® und Reader® sind eingetragene Warenzeichen oder Warenzeichen von Adobe Systems Incorporated in den USA und/oder anderen Ländern.

Jedes Unternehmen, dessen Softwaretitel in diesem Handbuch genannt sind, verfügt für seine proprietären Programme über gesonderte License.

Alle Warenzeichen und Produktnamen von Unternehmen, die auf Produkten, Dokumenten und anderen Materialien von Brother erscheinen, sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Unternehmen.

Zugehörige Informationen

- Einleitung

Copyright

Zugehörige Informationen

- Einleitung

Vor der Verwendung der Netzwerk-Sicherheitsfunktionen

Ihr Gerät verwendet einige der neuesten Netzwerksicherheits- und Verschlüsselungs-Protokolle. Integrieren Sie diese Netzwerkfunktionen in das Gesamtsicherheitskonzept für Ihr Netzwerk, um Ihre Daten zu schützen und unauthorized Zugriff auf das Gerät zu verhindern.

Es wird empfohlen, das FTP- und das TFTP-Protokoll zu deaktivieren. Der Zugriff auf das Gerät über diese Protokolle ist nicht sicher.

Zugehörige Informationen

- Einleitung
  - Deaktivieren unnötiger Protokolle

Deaktivieren unnötiger Protokolle

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. Entfernen Sie das Häkchen der Kontrollkästchen für alle unnötigen Protokolle, um sie zu deaktivieren.
6. Klicken Sie auf **Senden**.
7. Starten Sie das Brother-Gerät neu, um die Konfiguration zu aktivieren.

Zugehörige Informationen

- Vor der Verwendung der Netzwerk-Sicherheitsfunktionen

Netzwerksicherheit

- Konfigurieren von Zertifikaten für die Gerätesicherheit
- Verwenden von SSL/TLS
- Verwenden von SNMPv3
- Verwenden von IPsec
- Verwenden der IEEE 802.1x-Authentifizierung für Ihr 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 organization 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(Port 443)** 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 unauthorized 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. Verwenden Sie den SNMPv3-Modus, um den Druckserver sicher zu verwalten.
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 von IPsec

- Einführung in IPsec
- Konfigurieren von IPsec mit Web Based Management
- Konfigurieren einer IPsec-Adressvorlage mit Web Based Management
- Konfigurieren einer IPsec-Vorlage mit Web Based Management

Einführung in IPsec

Bei IPsec (Internet Protocol Security = Internetprotokollsicherheit) handelt es sich um ein Sicherheitsprotokoll, das auf eine optionale Internetprotokollfunktion zurückgreift, um Datenmanipulationen zu verhindern und die Vertraulichkeit der als IP-Paket übertragenen Daten sicherzustellen. IPsec verschlüsselt Daten, die über ein Netzwerk übermittelt werden, wie beispielsweise die von Computern an einen Drucker gesendeten Druckdaten. Da die Daten in der Netzwerkschicht verschlüsselt werden, setzen Anwendungen, die übergeordnete Protokolle verwenden, das IPsec-Protokoll ein, auch wenn die Benutzer dies nicht wahrnehmen.

IPsec unterstützt die folgenden Funktionen:

- IPsec-Datenübertragungen

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

  Darüber hinaus verfügt IPsec über die zwei Betriebsmodi, den Transportmodus und den Tunnelmodus. Der Transport-Modus wird primär zur Kommunikation zwischen Geräten verwendet und der Tunnel-Modus in Umgebungen wie einem Virtual Private Network (VPN).

  Für IPsec-Datenübertragungen sind folgende Bedingungen notwendig:
  - Ein Computer, der mit IPsec kommunizieren kann, ist mit dem Netzwerk verbunden.
  - Ihr Gerät ist für eine Kommunikation mittels IPsec konfiguriert.
  - Der an Ihr Gerät angeschlossene Computer ist für IPsec-Verbindungen konfiguriert.

- IPsec-Einstellungen

  Die Einstellungen, die für Verbindungen mit IPsec erforderlich sind. Diese Einstellungen können mit Web Based Management konfiguriert werden.

  Um die IPsec-Einstellungen zu konfigurieren, müssen Sie den Browser auf einem Computer verwenden, der mit dem Netzwerk verbunden ist.

Zugehörige Informationen

- Verwenden von IPsec

Konfigurieren von IPsec mit Web Based Management

Die IPsec-Anschlussbedingungen umfassen zwei **Vorlage**-Typen: **Adresse** und **IPsec**. Sie können bis zu 10 Anschlussbedingungen 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** > **Sicherheit** > **IPsec**.

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

5. Konfigurieren Sie die Einstellungen.

Option	Beschreibung
Status	Aktivieren oder deaktivieren Sie IPsec.
Aushandlungsmodus	Wählen Sie **Aushandlungsmodus** für IKE Phase 1. IKE ist ein Protokoll, mit dem Verschlüsselungsschlüssel ausgetauscht werden, um eine verschlüsselte Kommunikation über IPsec auszuführen. Im Modus **Normal** ist die Verarbeitungsgeschwindigkeit langsam, aber die Sicherheit ist hoch. Im Modus **Aggressiv** hingegen ist die Verarbeitungsgeschwindigkeit zwar höher als im Modus **Normal**, doch dafür ist geringere Sicherheit gegeben.
Jeglicher Nicht-IPsec-Verkehr	Wählen Sie aus, welche Aktion für Nicht-IPsec-Pakete ausgeführt werden soll. Wenn Sie Webdienste verwenden, müssen Sie **Zulassen** für **Jeglicher Nicht-IPsec-Verkehr** auswählen. Wenn Sie **Blockieren** auswählen, können Webdienste nicht verwendet werden.
Broadcast/Multicast-Bypass	Wählen Sie **Aktiviert** oder **Deaktiviert**.
Protokoll-Bypass	Aktivieren Sie die Kontrollkästchen für die gewünschte Option oder die gewünschten Optionen.
Richtlinien	Aktivieren Sie das Kontrollkästchen **Aktiviert**, um die Vorlage zu aktivieren. Wenn Sie mehrere Kontrollkästchen aktivieren, haben die Kontrollkästchen mit niedrigeren Zahlen Priorität, wenn sich die Einstellungen der aktivierten Kontrollkästchen widersprechen. Klicken Sie auf die entsprechende Dropdown-Liste, um die **Adressvorlage** auszuwählen, die für die IPsec-Verbindungsbedingungen verwendet wird. Um eine **Adressvorlage** hinzuzufügen, klicken Sie auf **Vorlage hinzufügen**. Klicken Sie auf die entsprechende Dropdown-Liste, um die **IPsec-Vorlage** auszuwählen, die für die IPsec-Verbindungsbedingungen verwendet wird. Um eine **IPsec-Vorlage** hinzuzufügen, klicken Sie auf **Vorlage hinzufügen**.

6. Klicken Sie auf **Senden**.

   Wenn das Gerät neu gestartet werden muss, um die neuen Einstellungen zu aktivieren, wird der Bestätigungsbildschirm für den Neustart angezeigt.

Wenn sich in der Vorlage, die Sie in der Tabelle **Richtlinien** aktiviert haben, ein leeres Element befindet, wird eine Fehlermeldung angezeigt. Bestätigen Sie Ihre Auswahl und klicken Sie erneut auf **Senden**.

Zugehörige Informationen

- Verwenden von IPsec

Verwandte Themen:

- Konfigurieren von Zertifikaten für die Gerätesicherheit

Konfigurieren einer IPsec-Adressvorlage mit Web Based Management

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** > **IPsec-Adressvorlage**.

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

5. Klicken Sie auf die Schaltfläche **Löschen**, um eine **Adressvorlage** zu löschen. Wenn eine **Adressvorlage** verwendet wird, kann sie nicht gelöscht werden.
6. Klicken Sie auf die **Adressvorlage**, die Sie erstellen möchten. Die **IPsec-Adressvorlage** wird angezeigt.
7. Konfigurieren Sie die Einstellungen.

Option	Beschreibung
Vorlagenname	Geben Sie eine (aus bis zu 16 Zeichen bestehende) Bezeichnung für die Vorlage ein.
Lokale IP-Adresse	• **IP-Adresse** Legen Sie die IP-Adresse fest. Wählen Sie **ALLE IPv4-Adressen**, **ALLE IPv6-Adressen**, **ALLE Link Local IPv6** oder **Benutzerdefiniert** aus der Dropdown-Liste aus. Wenn Sie **Benutzerdefiniert** aus der Dropdown-Liste auswählen, geben Sie die IP-Adresse (IPv4 oder IPv6) in das Textfeld ein. • **IP-Adressbereich** Geben Sie in den Textfeldern die Anfangs- und End-IP-Adressen des IP-Adressenbereichs ein. Wenn die Start- und End-IP-Adressen nicht nach IPv4 oder IPv6 standardized sind oder die End-IP-Adresse kleiner als die Startadresse ist, kommt es zu einem Fehler. • **IP-Adresse / Präfix** Spezifizieren Sie die IP-Adresse anhand der CIDR-Schreibweise. Beispiel: 192.168.1.1/24 Da das Präfix in Form einer 24-Bit-Subnetzmaske (255.255.255.0) für 192.168.1.1 angegeben wird, sind die Adressen 192.168.1.### gültig.
Remote-IP-Adresse	• **Beliebig** Wenn Sie **Beliebig** auswählen, sind alle IP-Adressen aktiviert. • **IP-Adresse** Geben Sie die angegebene IP-Adresse (IPv4 oder IPv6) im Textfeld ein. • **IP-Adressbereich** Geben Sie die erste und letzte IP-Adresse für den IP-Adressbereich ein. Wenn die erste und letzte IP-Adresse nicht

Option	Beschreibung
	nach IPv4 oder IPv6 standardized sind oder die letzte IP-Adresse kleiner als die erste Adresse ist, kommt es zu einem Fehler. • **IP-Adresse / Präfix** Spezifizieren Sie die IP-Adresse anhand der CIDR-Schreibweise. Beispiel: 192.168.1.1/24 Da das Präfix in Form einer 24-Bit-Subnetzmaske (255.255.255.0) für 192.168.1.1 angegeben wird, sind die Adressen 192.168.1.### gültig.

8. Klicken Sie auf **Senden**.

Wenn Sie die Einstellungen für die derzeit verwendete Vorlage ändern, starten Sie das Gerät neu, um die Konfiguration zu aktivieren.

Zugehörige Informationen

- Verwenden von IPsec

Konfigurieren einer IPsec-Vorlage mit Web Based Management

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** > **IPsec-Vorlage**.

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

5. Klicken Sie auf die Schaltfläche **Löschen**, um eine **IPsec-Vorlage** zu löschen. Wenn eine **IPsec-Vorlage** verwendet wird, kann sie nicht gelöscht werden.
6. Klicken Sie auf die **IPsec-Vorlage**, die Sie erstellen möchten. Der Bildschirm **IPsec-Vorlage** wird angezeigt. Die Konfigurationsfelder weichen abhängig von den ausgewählten Einstellungen für **Vorgegebene Vorlage verwenden** und **Internet Key Exchange (IKE)** ab.
7. Geben Sie im Feld **Vorlagenname** einen Namen für die Vorlage ein (bis zu 16 Zeichen).
8. Wenn Sie **Benutzerdefiniert** in der Dropdown-Liste **Vorgegebene Vorlage verwenden** ausgewählt habe, wählen Sie die **Internet Key Exchange (IKE)**-Optionen und ändern Sie die Einstellungen dann bei Bedarf.
9. Klicken Sie auf **Senden**.

Zugehörige Informationen

- Verwenden von IPsec
  - IKEv1-Einstellungen für eine IPsec-Vorlage
  - IKEv2-Einstellungen für eine IPsec-Vorlage
  - Manuelle Einstellungen für eine IPsec-Vorlage

IKEv1-Einstellungen für eine IPsec-Vorlage

Option	Beschreibung
Vorlagenname	Geben Sie eine (aus bis zu 16 Zeichen bestehende) Bezeichnung für die Vorlage ein.
Vorgegebene Vorlage verwenden	Wählen Sie **Benutzerdefiniert**, **IKEv1 Hohe Sicherheit** oder **IKEv1 Mittlere Sicherheit** aus. Die Einstellungselemente unterscheiden sich abhängig von der ausgewählten Vorlage.
Internet Key Exchange (IKE)	IKE ist ein Kommunikationsprotokoll, mit dem Verschlüsselungsschlüssel ausgetauscht werden, um eine verschlüsselte Kommunikation über IPsec auszuführen. Um nur dieses Mal eine verschlüsselte Kommunikation auszuführen, wird der für IPsec notwendige Verschlüsselungsalgorithmus bestimmt und die Verschlüsselungsschlüssel werden weitergegeben. Für IKE werden die Verschlüsselungsschlüssel mit der Diffie-Hellman-Schlüsselaustauschmethode ausgetauscht und die auf IKE beschränkte verschlüsselte Kommunikation wird ausgeführt. Wenn Sie **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt haben, wählen Sie **IKEv1**.
Authentifizierungstyp	• **Diffie-Hellman-Gruppe** Dieses Schlüsselaustauschverfahren ermöglicht den sicheren Austausch geheimer Schlüssel über ein ungeschütztes Netzwerk. Das Diffie-Hellman-Schlüsselaustauschverfahren verwendet anstelle des geheimen Schlüssels einen diskreten Logarithmus zum Versenden und Empfangen offener Informationen, die mittels einer Zufallszahl und dem geheimen Schlüssel generiert wurden. Wählen Sie **Gruppe1**, **Gruppe2**, **Gruppe5** oder **Gruppe14**. • **Verschlüsselung** Wählen Sie **DES**, **3DES**, **AES-CBC 128** oder **AES-CBC 256**. • **Hash** Wählen Sie **MD5**, **SHA1**, **SHA256**, **SHA384** oder **SHA512**. • **SA-Lebensdauer** Legen Sie die IKE-SA-Gültigkeitsdauer fest. Geben Sie die Zeit (Sekunden) und Anzahl der Kilobytes (KByte) ein.
Encapsulating Security	• **Protokoll** Wählen Sie **ESP**, **AH** oder **AH+ESP** aus.

Option	Beschreibung
	- ESP ist ein Protokoll für die Durchführung einer verschlüsselten Kommunikation mit IPsec. ESP verschlüsselt die Nutzdaten (die kommunizierten Inhalte) und fügt zusätzliche Informationen hinzu. Das IP-Paket umfasst die Kopfzeile und die verschlüsselte Nutzlast, die auf die Kopfzeile folgt. Neben den verschlüsselten Daten enthält das IP-Paket auch Informationen in Bezug auf die Verschlüsselungsmethode und den Verschlüsselungsschlüssel, die Authentifizierungsdaten und so weiter. - AH ist Teil des IPsec-Protokolls, das den Sender authentifiziert und eine Manipulation der Daten verhindert (es stellt die Vollständigkeit der Daten sicher). Im IP-Paket werden die Daten unmittelbar nach der Kopfzeile eingefügt. Des Weiteren enthalten die Pakete Hash-Werte, die mit einer Gleichung aus den kommunizierten Inhalten, dem geheimen Schlüssel und so weiter berechnet werden, um die Verfälschung des Absenders und die Manipulation der Daten zu verhindern. Im Gegensatz zu ESP werden die kommunizierten Inhalte nicht verschlüsselt und die Daten werden als Nur-Text gesendet und empfangen. • **Verschlüsselung (Nicht verfügbar für die Option AH.)** Wählen Sie **DES**, **3DES**, **AES-CBC 128** oder **AES-CBC 256**. • **Hash** Wählen Sie **Nichts**, **MD5**, **SHA1**, **SHA256**, **SHA384** oder **SHA512**. **Nichts** kann nur ausgewählt werden, wenn **ESP** für **Protokoll** ausgewählt ist. • **SA-Lebensdauer** Legen Sie die IKE-SA-Nutzungsdauer fest. Geben Sie die Zeit (Sekunden) und Anzahl der Kilobytes (KByte) ein. • **Encapsulation-Modus** Wählen Sie **Transport** oder **Tunnel** aus. • **IP-Adresse des Remote-Routers** Geben Sie die IP-Adresse (IPv4 oder IPv6) des Remote-Routers ein. Geben Sie diese Informationen nur ein, wenn der Modus **Tunnel** ausgewählt ist. SA (Security Association) ist ein verschlüsseltes Kommunikationsverfahren, das IPsec oder IPv6 nutzt und Informationen austauscht und weitergibt, wie die Verschlüsselungsmethode und den Verschlüsselungsschlüssel, um einen sicheren Kommunikationskanal einzurichten, bevor die Kommunikation beginnt. SA kann sich auch auf einen virtuellen verschlüsselten Kommunikationskanal beziehen, der eingerichtet wurde. Die für IPsec verwendete SA etabliert die Verschlüsselungsmethode, tauscht die Schlüssel aus und führt eine gegenseitige Authentifizierung entsprechend dem IKE (Internet Key Exchange)-Standardvorgang durch. Des Weiteren wird SA regelmäßig aktualisiert.
Perfect Forward Secrecy (PFS)	PFS leitet keine Schlüssel aus vorherigen Schlüsseln ab, die zur Verschlüsselung von Nachrichten verwendet wurden. Darüber hinaus werden übergeordnete Schlüssel, mit denen Verschlüsselungsschlüssel für die Verschlüsselung von Nachrichten abgeleitet werden, nicht für die Ableitung anderer Schlüssel verwendet. Wenn ein Schlüssel gefährdet wurde, ist der Schaden daher nur auf die Nachrichten beschränkt, die mit diesem Schlüssel verschlüsselt wurden.

Option	Beschreibung
	Wählen Sie **Aktiviert** oder **Deaktiviert**.
Authentifizierungsmethode	Wählen Sie die Authentifizierungsmethode aus. Wählen Sie **Pre-Shared Key** oder **Zertifikate**.
Pre-Shared Key	Bei der Verschlüsselung von Kommunikationsvorgängen wird der Verschlüsselungsschlüssel vor der Nutzung eines anderen Kanals ausgetauscht und gemeinsam verwendet. Wenn Sie **Pre-Shared Key** als **Authentifizierungsmethode** ausgewählt haben, geben Sie den **Pre-Shared Key** ein (bis zu 32 Zeichen). • **Lokal/ID-Typ/ID** Wählen Sie ID-Art des Absenders aus und geben Sie die ID ein. Wählen Sie **IPv4-Adresse**, **IPv6-Adresse**, **FQDN**, **E-Mail-Adresse** oder **Zertifikat** für den Typ aus. Wenn Sie **Zertifikat** auswählen, geben Sie den allgemeinen Namen des Zertifikats im Feld **ID** ein. • **Remote/ID-Typ/ID** Wählen Sie ID-Art des Empfängers aus und geben Sie die ID ein. Wählen Sie **IPv4-Adresse**, **IPv6-Adresse**, **FQDN**, **E-Mail-Adresse** oder **Zertifikat** für den Typ aus. Wenn Sie **Zertifikat** auswählen, geben Sie den allgemeinen Namen des Zertifikats im Feld **ID** ein.
Zertifikat	Wenn Sie **Zertifikate** unter **Authentifizierungsmethode** ausgewählt haben, wählen Sie das Zertifikat aus. Sie können nur die Zertifikate auswählen, die über die Seite **Zertifikat** des Web Based Management Sicherheitskonfigurationsbildschirms erstellt wurden.

Zugehörige Informationen

- Konfigurieren einer IPsec-Vorlage mit Web Based Management

IKEv2-Einstellungen für eine IPsec-Vorlage

Option	Beschreibung
Vorlagenname	Geben Sie eine (aus bis zu 16 Zeichen bestehende) Bezeichnung für die Vorlage ein.
Vorgegebene Vorlage verwenden	Wählen Sie **Benutzerdefiniert**, **IKEv2 Hohe Sicherheit** oder **IKEv2 Mittlere Sicherheit** aus. Die Einstellungselemente unterscheiden sich abhängig von der ausgewählten Vorlage.
Internet Key Exchange (IKE)	IKE ist ein Kommunikationsprotokoll, mit dem Verschlüsselungsschlüssel ausgetauscht werden, um eine verschlüsselte Kommunikation über IPsec auszuführen. Um nur dieses Mal eine verschlüsselte Kommunikation auszuführen, wird der für IPsec notwendige Verschlüsselungsalgorithmus bestimmt und die Verschlüsselungsschlüssel werden weitergegeben. Für IKE werden die Verschlüsselungsschlüssel mit der Diffie-Hellman-Schlüsselaustauschmethode ausgetauscht und die auf IKE beschränkte verschlüsselte Kommunikation wird ausgeführt. Wenn Sie **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt haben, wählen Sie **IKEv2**.
Authentifizierungstyp	• **Diffie-Hellman-Gruppe** Dieses Schlüsselaustauschverfahren ermöglicht den sicheren Austausch geheimer Schlüssel über ein ungeschütztes Netzwerk. Das Diffie-Hellman-Schlüsselaustauschverfahren verwendet anstelle des geheimen Schlüssels einen diskreten Logarithmus zum Versenden und Empfangen offener Informationen, die mittels einer Zufallszahl und dem geheimen Schlüssel generiert wurden. Wählen Sie **Gruppe1**, **Gruppe2**, **Gruppe5** oder **Gruppe14**. • **Verschlüsselung** Wählen Sie **DES**, **3DES**, **AES-CBC 128** oder **AES-CBC 256** aus. • **Hash** Wählen Sie **MD5**, **SHA1**, **SHA256**, **SHA384** oder **SHA512**. • **SA-Lebensdauer** Legen Sie die IKE-SA-Gültigkeitsdauer fest. Geben Sie die Zeit (Sekunden) und Anzahl der Kilobytes (KByte) ein.
Encapsulating Security	• **Protokoll** Wählen Sie **ESP**. ESP ist ein Protokoll für die Durchführung einer verschlüsselten Kommunikation mit IPsec. ESP verschlüsselt die Nutzdaten (die kommunizierten Inhalte) und fügt zusätzliche Informationen hinzu. Das IP-Paket umfasst die Kopfzeile und die verschlüsselte Nutzlast, die auf die Kopfzeile folgt. Neben den verschlüsselten Daten enthält das IP-Paket auch Informationen in Bezug auf die Verschlüsselungsmethode und den Verschlüsselungsschlüssel, die Authentifizierungsdaten und so weiter. • **Verschlüsselung** Wählen Sie **DES**, **3DES**, **AES-CBC 128** oder **AES-CBC 256**. • **Hash** Wählen Sie **MD5**, **SHA1**, **SHA256**, **SHA384** oder **SHA512**. • **SA-Lebensdauer** Legen Sie die IKE-SA-Nutzungsdauer fest.

Option	Beschreibung
	Geben Sie die Zeit (Sekunden) und Anzahl der Kilobytes (KByte) ein. • **Encapsulation-Modus** Wählen Sie **Transport** oder **Tunnel** aus. • **IP-Adresse des Remote-Routers** Geben Sie die IP-Adresse (IPv4 oder IPv6) des Remote-Routers ein. Geben Sie diese Informationen nur ein, wenn der Modus **Tunnel** ausgewählt ist. SA (Security Association) ist ein verschlüsseltes Kommunikationsverfahren, das IPsec oder IPv6 nutzt und Informationen austauscht und weitergibt, wie die Verschlüsselungsmethode und den Verschlüsselungsschlüssel, um einen sicheren Kommunikationskanal einzurichten, bevor die Kommunikation beginnt. SA kann sich auch auf einen virtuellen verschlüsselten Kommunikationskanal beziehen, der eingerichtet wurde. Die für IPsec verwendete SA etabliert die Verschlüsselungsmethode, tauscht die Schlüssel aus und führt eine gegenseitige Authentifizierung entsprechend dem IKE (Internet Key Exchange)-Standardvorgang durch. Des Weiteren wird SA regelmäßig aktualisiert.
Perfect Forward Secrecy (PFS)	PFS leitet keine Schlüssel aus vorherigen Schlüsseln ab, die zur Verschlüsselung von Nachrichten verwendet wurden. Darüber hinaus werden übergeordnete Schlüssel, mit denen Verschlüsselungsschlüssel für die Verschlüsselung von Nachrichten abgeleitet werden, nicht für die Ableitung anderer Schlüssel verwendet. Wenn ein Schlüssel gefährdet wurde, ist der Schaden daher nur auf die Nachrichten beschränkt, die mit diesem Schlüssel verschlüsselt wurden. Wählen Sie **Aktiviert** oder **Deaktiviert**.
Authentifizierungsmethode	Wählen Sie die Authentifizierungsmethode aus. Wählen Sie **Pre-Shared Key**, **Zertifikate**, **EAP - MD5** oder **EAP - MS-CHAPv2**. EAP ist ein Authentifizierungsprotokoll, bei dem es sich um eine Erweiterung von PPP handelt. Durch die Verwendung von EAP mit IEEE802.1x werden unterschiedliche Schlüssel für Benutzerauthentifizierung und jede Sitzung verwendet. Die folgenden Einstellungen sind nur notwendig, wenn **EAP - MD5** oder **EAP - MS-CHAPv2** unter **Authentifizierungsmethode** ausgewählt wurde: • **Modus** Wählen Sie **Server-Modus** oder **Client-Modus**. • **Zertifikat** Wählen Sie das Zertifikat aus. • **Benutzername** Geben Sie den Benutzernamen ein (bis zu 32 Zeichen). • **Kennwort** Geben Sie das Kennwort ein (bis zu 32 Zeichen). Das Kennwort muss zwei Mal eingegeben werden, um bestätigt zu werden.
Pre-Shared Key	Bei der Verschlüsselung von Kommunikationsvorgängen wird der Verschlüsselungsschlüssel vor der Nutzung eines anderen Kanals ausgetauscht und gemeinsam verwendet. Wenn Sie **Pre-Shared Key** als **Authentifizierungsmethode** ausgewählt haben, geben Sie den **Pre-Shared Key** ein (bis zu 32 Zeichen).

Option	Beschreibung
	• **Lokal/ID-Typ/ID** Wählen Sie ID-Art des Absenders aus und geben Sie die ID ein. Wählen Sie **IPv4-Adresse**, **IPv6-Adresse**, **FQDN**, **E-Mail-Adresse** oder **Zertifikat** für den Typ aus. Wenn Sie **Zertifikat** auswählen, geben Sie den allgemeinen Namen des Zertifikats im Feld **ID** ein. • **Remote/ID-Typ/ID** Wählen Sie ID-Art des Empfängers aus und geben Sie die ID ein. Wählen Sie **IPv4-Adresse**, **IPv6-Adresse**, **FQDN**, **E-Mail-Adresse** oder **Zertifikat** für den Typ aus. Wenn Sie **Zertifikat** auswählen, geben Sie den allgemeinen Namen des Zertifikats im Feld **ID** ein.
Zertifikat	Wenn Sie **Zertifikate** unter **Authentifizierungsmethode** ausgewählt haben, wählen Sie das Zertifikat aus. Sie können nur die Zertifikate auswählen, die über die Seite **Zertifikat** des Web Based Management Sicherheitskonfigurationsbildschirms erstellt wurden.

Zugehörige Informationen

- Konfigurieren einer IPsec-Vorlage mit Web Based Management

Manuelle Einstellungen für eine IPsec-Vorlage

Option	Beschreibung
Vorlagenname	Geben Sie eine (aus bis zu 16 Zeichen bestehende) Bezeichnung für die Vorlage ein.
Vorgegebene Vorlage verwenden	Wählen Sie **Benutzerdefiniert**.
Internet Key Exchange (IKE)	IKE ist ein Kommunikationsprotokoll, mit dem Verschlüsselungsschlüssel ausgetauscht werden, um eine verschlüsselte Kommunikation über IPsec auszuführen. Um nur dieses Mal eine verschlüsselte Kommunikation auszuführen, wird der für IPsec notwendige Verschlüsselungsalgorithmus bestimmt und die Verschlüsselungsschlüssel werden weitergegeben. Für IKE werden die Verschlüsselungsschlüssel mit der Diffie-Hellman-Schlüsselaustauschmethode ausgetauscht und die auf IKE beschränkte verschlüsselte Kommunikation wird ausgeführt. Wählen Sie **Manuell**.
Authentifizierungsschlüssel (ESP, AH)	Geben Sie die Werte für **Eingehend/Ausgehend** ein. Diese Einstellungen sind erforderlich, wenn **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** und **Manuell** unter **Internet Key Exchange (IKE)** ausgewählt ist und eine andere Einstellung als **Nichts** unter **Hash** von **Encapsulating Security** ausgewählt ist. Die Anzahl der Zeichen, die Sie einstellen können, variiert abhängig von der Einstellung, die Sie unter **Hash** im Bereich **Encapsulating Security** gewählt haben. Ist die Länge des spezifizierten Authentifizierungsschlüssels unterschiedlich zum gewählten Hashalgorithmus, dann erscheint eine Fehlermeldung. • **MD5**: 128 Bit (16 Byte) • **SHA1**: 160 Bit (20 Byte) • **SHA256**: 256 Bit (32 Byte) • **SHA384**: 384 Bit (48 Byte) • **SHA512**: 512 Bit (64 Byte) Wenn Sie den Schlüssel als ASCII-Code spezifizieren, müssen Sie die Zeichen in doppelten Anführungszeichen (") einschließen.
Codeschlüssel (ESP)	Geben Sie die Werte für **Eingehend/Ausgehend** ein. Diese Einstellungen sind notwendig, wenn **Benutzerdefiniert** für **Vorgegebene Vorlage verwenden** ausgewählt ist, **Manuell** für **Internet Key Exchange (IKE)** ausgewählt ist und **ESP** für **Protokoll** unter **Encapsulating Security** ausgewählt ist.

Option	Beschreibung
	Die Anzahl der Zeichen, die Sie einstellen können, variiert abhängig von der Einstellung, die Sie unter **Verschlüsselung** im Bereich **Encapsulating Security** gewählt haben. Ist die Länge des spezifizierten Codes unterschiedlich zum gewählten Verschlüsselungsalgorithmus, dann erscheint eine Fehlermeldung. • **DES**: 64 Bit (8 Byte) • **3DES**: 192 Bit (24 Byte) • **AES-CBC 128**: 128 Bit (16 Byte) • **AES-CBC 256**: 256 Bit (32 Byte) Wenn Sie den Schlüssel als ASCII-Code spezifizieren, müssen Sie die Zeichen in doppelten Anführungszeichen (") einschließen.
SPI	Diese Parameter werden verwendet, um die Sicherheitsinformationen zu identifizieren. Im Allgemeinen verfügt ein Host über mehrere Security Associations (SAs, Sicherheitszuordnungen) für verschiedene Arten der IPsec-Kommunikation. Daher ist es notwendig, die gültige SA zu identifizieren, wenn ein IPsec-Paket empfangen wird. Der SPI-Parameter, der die SA identifiziert, ist im Authentication Header (AH) und in der Encapsulating Security Payload-Kopfzeile (ESP) enthalten. Diese Einstellungen sind erforderlich, wenn **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** und **Manuell** unter **Internet Key Exchange (IKE)** ausgewählt ist. Geben Sie die Werte für **Eingehend/Ausgehend** ein. (3-10 Zeichen)
Encapsulating Security	• **Protokoll** Wählen Sie **ESP** oder **AH**. - ESP ist ein Protokoll für die Durchführung einer verschlüsselten Kommunikation mit IPsec. ESP verschlüsselt die Nutzdaten (die kommunizierten Inhalte) und fügt zusätzliche Informationen hinzu. Das IP-Paket umfasst die Kopfzeile und die verschlüsselte Nutzlast, die auf die Kopfzeile folgt. Neben den verschlüsselten Daten enthält das IP-Paket auch Informationen in Bezug auf die Verschlüsselungsmethode und den Verschlüsselungsschlüssel, die Authentifizierungsdaten und so weiter. - AH ist Teil des IPsec-Protokolls, das den Sender authentifiziert und eine Manipulation der Daten verhindert (es stellt die Vollständigkeit der Daten sicher). Im IP-Paket werden die Daten unmittelbar nach der Kopfzeile eingefügt. Des Weiteren enthalten die Pakete Hash-Werte, die mit einer Gleichung aus den kommunizierten Inhalten, dem geheimen Schlüssel und so weiter berechnet werden, um die Verfälschung des Absenders und die Manipulation der Daten zu verhindern. Im Gegensatz zu ESP werden die kommunizierten Inhalte nicht verschlüsselt und die Daten werden als Nur-Text gesendet und empfangen. • **Verschlüsselung (Nicht verfügbar für die Option AH.)** Wählen Sie **DES**, **3DES**, **AES-CBC 128** oder **AES-CBC 256**. • **Hash** Wählen Sie **Nichts**, **MD5**, **SHA1**, **SHA256**, **SHA384** oder **SHA512**. **Nichts** kann nur ausgewählt werden, wenn **ESP** für **Protokoll** ausgewählt ist. • **SA-Lebensdauer** Legen Sie die IKE-SA-Nutzungsdauer fest.

Option	Beschreibung
	Geben Sie die Zeit (Sekunden) und Anzahl der Kilobytes (KByte) ein. • **Encapsulation-Modus** Wählen Sie **Transport** oder **Tunnel** aus. • **IP-Adresse des Remote-Routers** Geben Sie die IP-Adresse (IPv4 oder IPv6) des Remote-Routers ein. Geben Sie diese Informationen nur ein, wenn der Modus **Tunnel** ausgewählt ist. SA (Security Association) ist ein verschlüsseltes Kommunikationsverfahren, das IPsec oder IPv6 nutzt und Informationen austauscht und weitergibt, wie die Verschlüsselungsmethode und den Verschlüsselungsschlüssel, um einen sicheren Kommunikationskanal einzurichten, bevor die Kommunikation beginnt. SA kann sich auch auf einen virtuellen verschlüsselten Kommunikationskanal beziehen, der eingerichtet wurde. Die für IPsec verwendete SA etabliert die Verschlüsselungsmethode, tauscht die Schlüssel aus und führt eine gegenseitige Authentifizierung entsprechend dem IKE (Internet Key Exchange)-Standardvorgang durch. Des Weiteren wird SA regelmäßig aktualisiert.

Zugehörige Informationen

- Konfigurieren einer IPsec-Vorlage mit Web Based Management

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 unauthorized 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 tunneled 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

Benutzerauthentifizierung

- Verwenden der Active Directory-Authentifizierung
- Verwenden der LDAP-Authentifizierung
- Verwenden der Benutzersperre 3.0

Verwenden der Active Directory-Authentifizierung

- Einführung in die Active Directory-Authentifizierung
- Konfigurieren der Active Directory-Authentifizierung mit Web Based Management
- Anmelden zum Ändern der Geräteeinstellungen über das Funktionstastenfeld des Geräts (Active Directory-Authentifizierung)

Einführung in die Active Directory-Authentifizierung

Die Active Directory-Authentifizierung schränkt die Nutzung Ihres Gerätes ein. Wenn die Active Directory-Authentifizierung aktiviert ist, wird das Funktionstastenfeld des Geräts gesperrt. Sie können die Einstellungen des Geräts erst dann ändern, wenn Sie eine Benutzer-ID und das Kennwort eingegeben haben.

Die Active Directory-Authentifizierung bietet die folgenden Funktionen:

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

- Speichern eingehender Druckdaten
- Speichern eingehender Faxdaten
- Ruft die E-Mail-Adresse vom Active Directory-Server basierend auf Ihrer Benutzer-ID ab, wenn gescannte Daten an einen E-Mail-Server gesendet werden.

  Zur Verwendung dieser Funktion wählen Sie die Option **Ein** für die Einstellung **E-Mail-Adresse abrufen** und die Authentifizierungsmethode **LDAP + kerberos** oder **LDAP + NTLMv2**. Ihre E-Mail-Adresse wird als Absender festgelegt, wenn das Gerät gescannte Daten an einen E-Mail-Server sendet, oder als Empfänger, wenn Sie die gescannten Daten an Ihre E-Mail-Adresse senden möchten.

Wenn die Active Directory-Authentifizierung aktiviert ist, speichert das Gerät alle eingehenden Faxdaten. Nachdem Sie sich angemeldet haben, druckt das Gerät die gespeicherten Faxdaten aus.

Sie können die Active Directory-Authentifizierungseinstellungen über Web Based Management ändern.

Zugehörige Informationen

- Verwenden der Active Directory-Authentifizierung

Konfigurieren der Active Directory-Authentifizierung mit Web Based Management

Die Active Directory-Authentifizierung unterstützt die Kerberos-Authentifizierung und die NTLMv2-Authentifizierung. Sie müssen das SNTP-Protokoll (Netzwerkzeitserver) und die DNS-Serverkonfiguration für die Authentifizierung 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 **Administrator** > **Funktion zur Nutzungseinschränkung** oder **Einschränkungsverwaltung**.

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

5. Wählen Sie **Active Directory-Authentifizierung**.
6. Klicken Sie auf **Senden**.
7. Klicken Sie auf **Active Directory-Authentifizierung**.
8. Konfigurieren Sie die folgenden Einstellungen:

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

Option	Beschreibung
Empfangene Faxdaten speichern	Wählen Sie diese Option, um eingehende Faxdaten zu speichern. Sie können alle eingehenden Faxdaten ausdrucken, nachdem Sie sich beim Gerät angemeldet haben.
Benutzer-ID speichern	Wählen Sie diese Option, um Ihre Benutzer-ID zu speichern.
Active Directory-Serveradresse	Geben Sie die IP-Adresse oder den Servernamen des Active Directory-Servers ein (zum Beispiel: ad.Beispiel.de).
Active Directory-Domänenname	Geben Sie den Active Directory-Domänennamen ein.
Protokoll und Authentifizierungsmethode	Wählen Sie die Protokoll- & Authentifizierungsmethode aus.
SSL/TLS	Wählen Sie die **SSL/TLS**-Option.
LDAP-Serverport	Geben Sie die Portnummer für die Verbindung mit dem Active Directory-Server über LDAP ein (nur verfügbar für die Authentifizierungsmethode **LDAP + kerberos** oder **LDAP + NTLMv2**).

Option	Beschreibung
LDAP-Suchverzeichnis	Geben Sie das LDAP-Suchstammverzeichnis ein (verfügbar nur für die Authentifizierungsmethode **LDAP + kerberos** oder **LDAP + NTLMv2**).
E-Mail-Adresse abrufen	Wählen Sie diese Option, um die E-Mail-Adresse des angemeldeten Benutzers vom Active Directory-Server abzurufen. (nur für die Authentifizierungsmethode **LDAP + kerberos** oder **LDAP + NTLMv2** verfügbar)
Auf Basisverzeichnis für Benutzer zugreifen	Wählen Sie diese Option, um Ihr Basisverzeichnis als Ziel für Scan-to-Network auszuwählen. (nur für die Authentifizierungsmethode **LDAP + kerberos** oder **LDAP + NTLMv2** verfügbar)

9. Klicken Sie auf **Senden**.

Zugehörige Informationen

- Verwenden der Active Directory-Authentifizierung

Anmelden zum Ändern der Geräteeinstellungen über das Funktionstastenfeld des Geräts (Active Directory-Authentifizierung)

Wenn die Active Directory-Authentifizierung aktiviert ist, wird das Funktionstastenfeld des Geräts gesperrt, bis Sie Ihre Benutzer-ID und das Kennwort über das Funktionstastenfeld des Geräts eingeben.

1. Geben Sie im Funktionstastenfeld des Gerätes Ihre Benutzer-ID und das Kennwort ein, um sich anzumelden.
2. Wenn die Authentifizierung erfolgreich war, ist das Funktionstastenfeld des Geräts entsperrt.

Zugehörige Informationen

- Verwenden der Active Directory-Authentifizierung

Verwenden der LDAP-Authentifizierung

- Einführung in die LDAP-Authentifizierung
- Konfigurieren der LDAP-Authentifizierung mit Web Based Management
- Anmelden zum Ändern der Geräteeinstellungen über das Funktionstastenfeld des Geräts (LDAP-Authentifizierung)

Einführung in die LDAP-Authentifizierung

Die LDAP-Authentifizierung schränkt die Nutzung Ihres Gerätes ein. Wenn die LDAP-Authentifizierung aktiviert ist, wird das Funktionstastenfeld des Geräts gesperrt. Sie können die Einstellungen des Geräts erst dann ändern, wenn Sie eine Benutzer-ID und das Kennwort eingegeben haben.

Die LDAP-Authentifizierung bietet die folgenden Funktionen:

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

- Speichern eingehender Druckdaten
- Speichern eingehender Faxdaten
- Ruft die E-Mail-Adresse vom LDAP-Server basierend auf Ihrer Benutzer-ID ab, wenn gescannte Daten an einen E-Mail-Server gesendet werden.

  Zur Verwendung dieser Funktion wählen Sie die Option **Ein** für die Einstellung **E-Mail-Adresse abrufen**. Ihre E-Mail-Adresse wird als Absender festgelegt, wenn das Gerät gescannte Daten an einen E-Mail-Server sendet, oder als Empfänger, wenn Sie die gescannten Daten an Ihre E-Mail-Adresse senden möchten.

Wenn die LDAP-Authentifizierung aktiviert ist, speichert das Gerät alle eingehenden Faxdaten. Nachdem Sie sich angemeldet haben, druckt das Gerät die gespeicherten Faxdaten aus.

Sie können die LDAP-Authentifizierungseinstellungen über Web Based Management ändern.

Zugehörige Informationen

- Verwenden der LDAP-Authentifizierung

Konfigurieren der LDAP-Authentifizierung mit Web Based Management

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 **Administrator** > **Funktion zur Nutzungseinschränkung** oder **Einschränkungsverwaltung**.

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

5. Wählen Sie **LDAP-Authentifizierung**.
6. Klicken Sie auf **Senden**.
7. Klicken Sie auf das Menü **LDAP-Authentifizierung**.
8. Konfigurieren Sie die folgenden Einstellungen:

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

Option	Beschreibung
Empfangene Faxdaten speichern	Wählen Sie diese Option, um eingehende Faxdaten zu speichern. Sie können alle eingehenden Faxdaten ausdrucken, nachdem Sie sich beim Gerät angemeldet haben.
Benutzer-ID speichern	Wählen Sie diese Option, um Ihre Benutzer-ID zu speichern.
LDAP-Server-Adresse	Geben Sie die IP-Adresse oder den Servernamen des LDAP-Servers ein (zum Beispiel: ldap.Beispiel.de).
SSL/TLS	Wählen Sie die Option **SSL/TLS** aus, um LDAP über SSL/TLS zu verwenden.
LDAP-Serverport	Geben Sie die Port-Nr. des LDAP-Servers ein.
LDAP-Suchverzeichnis	Geben Sie das LDAP-Suchstammverzeichnis ein.
Namensattribut (Suchschlüssel)	Geben Sie das Attribut ein, das Sie als Suchschlüssel verwenden möchten.
E-Mail-Adresse abrufen	Wählen Sie diese Option, um die E-Mail-Adresse des angemeldeten Benutzers vom LDAP-Server abzurufen.
Auf Basisverzeichnis für Benutzer zugreifen	Wählen Sie diese Option, um Ihr Basisverzeichnis als Ziel für Scan-to-Network auszuwählen.

9. Klicken Sie auf **Senden**.

Zugehörige Informationen

- Verwenden der LDAP-Authentifizierung

Anmelden zum Ändern der Geräteeinstellungen über das Funktionstastenfeld des Geräts (LDAP-Authentifizierung)

Wenn die LDAP-Authentifizierung aktiviert ist, wird das Funktionstastenfeld des Geräts gesperrt, bis Sie Ihre Benutzer-ID und das Kennwort über das Funktionstastenfeld des Geräts eingeben.

1. Geben Sie im Funktionstastenfeld des Geräts Ihre Benutzer-ID und das Kennwort ein, um sich anzumelden.
2. Wenn die Authentifizierung erfolgreich ist, wird das Funktionstastenfeld des Geräts entsperrt.

Zugehörige Informationen

- Verwenden der LDAP-Authentifizierung

Verwenden der Benutzersperre 3.0

Benutzersperre 3.0 erhöht die Sicherheit, indem die auf Ihrem Gerät verfügbaren Gerätefunktionen eingeschränkt werden.

- Vor der Verwendung der Benutzersperre 3.0
- Konfigurieren der Benutzersperre 3.0 mit Web Based Management
- Scannen mit Benutzersperre 3.0
- Konfigurieren des Modus „Allgemeiner Benutzer“ für die Benutzersperre 3.0
- Konfigurieren der Einstellungen für den persönlichen Startbildschirm mit Web Based Management
- Weitere Funktionen von der Benutzersperre 3.0
- Registrieren einer neuen IC-Karte über das Funktionstastenfeld des Geräts
- Ein externes IC-Kartenlesegerät registrieren

Vor der Verwendung der Benutzersperre 3.0

Verwenden Sie die Benutzersperre, um Kennwörter zu konfigurieren, Seitenbegrenzungen für Benutzer festzulegen und den Zugriff auf bestimmte oder alle hier aufgeführten Funktionen zu ermöglichen.

Sie können die folgenden Einstellungen für Benutzersperre 3.0 über Web Based Management konfigurieren und ändern:

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

- **Drucken**
- **Kopie**
- **Scannen**
- **Fax**
- **Medium**
- **Web Connect**
- **Apps**
- **Seitenbegrenzung**
- **Seitenzähler**
- **Karten-ID (NFC-ID)**

Modelle mit Touchscreen-Display:

Wenn die Benutzersperre aktiviert ist, wechselt das Gerät automatisch in den Modus „Allgemeiner Benutzer“. Einige Gerätefunktionen sind dann eingeschränkt und stehen nur authorized Benutzern zur Verfügung. Zum Zugreifen auf die eingeschränkten Gerätefunktionen drücken Sie , wählen Sie Ihren Benutzernamen aus und geben Sie Ihr Kennwort ein.

Zugehörige Informationen

- Verwenden der Benutzersperre 3.0

Konfigurieren der Benutzersperre 3.0 mit Web Based Management

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 **Administrator** > **Funktion zur Nutzungseinschränkung** oder **Einschränkungsverwaltung**.

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

5. Wählen Sie **Benutzersperre**.
6. Klicken Sie auf **Senden**.
7. Klicken Sie auf das Menü **Eingeschränkte Funktionen**.
8. Konfigurieren Sie die Einstellungen, um die Einschränkungen nach Benutzer oder Gruppe zu verwalten.
9. Klicken Sie auf **Senden**.
10. Klicken Sie auf das Menü **Benutzerliste**.
11. Konfigurieren Sie die Benutzerliste.
12. Klicken Sie auf **Senden**.

Sie können auch die Sperreinstellungen für die Benutzerliste im Menü **Benutzersperre** ändern.

Zugehörige Informationen

- Verwenden der Benutzersperre 3.0

Scannen mit Benutzersperre 3.0

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

Einstellen der Scanbeschränkungen (für Administratoren)

Mit Secure Function Lock 3.0 kann der Administrator die Verwendung des Gerätes als Scanner für bestimmte Benutzer einschränken. Wenn Scannen im Profil für allgemeine Benutzer deaktiviert ist, können nur solche Benutzer diese Funktion nutzen, in deren Profil das Kontrollkästchen **Scannen** aktiviert ist.

Verwenden der Scanfunktion (für Benutzer, für die Einschränkungen gelten)

- Zum Scannen über das Funktionstastenfeld des Gerätes:

  Benutzer, für die Einschränkungen gelten, müssen ihre Kennwörter über das Funktionstastenfeld des Gerätes eingeben, um auf den Scanmodus zuzugreifen.
- So scannen Sie von einem Computer:

  Um von ihrem Computer aus scannen zu können, müssen Benutzer, für die Einschränkungen gelten, ihre Kennwörter über das Funktionstastenfeld des Gerätes eingeben. Wird das Kennwort nicht über das Funktionstastenfeld des Gerätes eingegeben, wird auf dem Computer des Benutzers eine Fehlermeldung angezeigt.

Wenn das Gerät IC-Kartenauthentifizierung unterstützt, können bestimmte Benutzer auch auf den Scanmodus zugreifen, wenn sie das NFC-Symbol am Funktionstastenfeld des Gerätes mit einer registrierten IC-Karte berühren.

Zugehörige Informationen

- Verwenden der Benutzersperre 3.0

Konfigurieren des Modus „Allgemeiner Benutzer“ für die Benutzersperre 3.0

Richten Sie im Benutzersperre-Bildschirm den Modus „Allgemeiner Benutzer“ ein, der die für allgemeine Benutzer verfügbaren Funktionen einschränkt. Allgemeine Benutzer brauchen kein Kennwort einzugeben, um die über die „Allgemeiner Benutzer“-Einstellungen freigegebenen Funktionen zu nutzen.

Der öffentliche Modus umfasst Druckaufträge, die über Brother iPrint&Scan und Brother Mobile Connect gesendet wurden.

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 **Administrator** > **Funktion zur Nutzungseinschränkung** oder **Einschränkungsverwaltung**.

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

5. Wählen Sie **Benutzersperre**.
6. Klicken Sie auf **Senden**.
7. Klicken Sie auf das Menü **Eingeschränkte Funktionen**.
8. Aktivieren Sie in der Zeile **Allgemeiner Benutzer** ein Kontrollkästchen, um die aufgeführte Funktion zu ermöglichen, oder deaktivieren Sie es, um die Funktion einzuschränken.
9. Klicken Sie auf **Senden**.

Zugehörige Informationen

- Verwenden der Benutzersperre 3.0

Konfigurieren der Einstellungen für den persönlichen Startbildschirm mit Web Based Management

Als Administrator können Sie festlegen, welche Registerkarten die Benutzer auf ihren persönlichen Startbildschirmen sehen. Diese Registerkarten gewähren schnellen Zugriff auf die favorite, die die Benutzer über das Bedienfeld ihres Gerätes ihren persönlichen Startbildschirm-Registerkarten zuweisen können.

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

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 **Administrator** > **Funktion zur Nutzungseinschränkung** oder **Einschränkungsverwaltung**.

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

5. Wählen Sie **Benutzersperre**.
6. Wählen Sie im Feld **Tab-Einstellungen** die Option **Privat** für die Registerkartennamen aus, die Sie für Ihren persönlichen Startbildschirm verwenden möchten.
7. Klicken Sie auf **Senden**.
8. Klicken Sie auf das Menü **Eingeschränkte Funktionen**.
9. Konfigurieren Sie die Einstellungen zur Verwaltung der Einschränkungen pro Benutzer oder Gruppe.
10. Klicken Sie auf **Senden**.
11. Klicken Sie auf das Menü **Benutzerliste**.
12. Konfigurieren Sie die Benutzerliste.
13. Wählen Sie **Benutzerliste/eingeschränkte Funktionen** aus der Dropdown-Liste für jeden Benutzer aus.
14. Wählen Sie den Registerkartennamen in der Dropdown-Liste **Startbildschirm** für jeden Benutzer aus.
15. Klicken Sie auf **Senden**.

Zugehörige Informationen

- Verwenden der Benutzersperre 3.0

Weitere Funktionen von der Benutzersperre 3.0

Konfigurieren Sie die folgenden Funktionen im Benutzersperre-Bildschirm:

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

Alle Zähler zurücksetzen

Klicken Sie auf **Alle Zähler zurücksetzen**, in der Spalte **Seitenzähler**, um den Seitenzähler zurückzusetzen.

Export in CSV-Datei

Klicken Sie auf **Export in CSV-Datei**, um den Zähler der aktuellen und der letzten Seite einschließlich **Benutzerliste/eingeschränkte Funktionen** als CSV-Datei zu exportieren.

Karten-ID (NFC-ID)

Klicken Sie auf das Menü **Benutzerliste** und geben Sie dann die Karten-ID eines Benutzers im Feld **Karten-ID (NFC-ID)** ein. Sie können Ihre IC-Karte zur Authentifizierung verwenden.

Ausgabe

Wenn die Mailbox-Einheit beim Gerät installiert ist, wählen Sie das Ausgabefach für jeden Benutzer aus der Dropdown-Liste aus.

Letzter Zählereintrag

Klicken Sie auf **Letzter Zählereintrag**, wenn das Gerät den Seitenzählerstand beibehalten soll, nachdem der Zähler zurückgesetzt wurde.

Zähler automatisch zurücksetzen

Klicken Sie auf **Zähler automatisch zurücksetzen**, um die Zeitabstände zwischen dem Zurücksetzen des Seitenzählers zu konfigurieren. Wählen Sie einen täglichen, wöchentlichen oder monatlichen Abstand.

Zugehörige Informationen

- Verwenden der Benutzersperre 3.0

Registrieren einer neuen IC-Karte über das Funktionstastenfeld des Geräts

Sie können auf Ihrem Gerät Karten mit integriertem Schaltkreis (IC-Karten) registrieren.

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

1. Berühren Sie das NFC-Symbol (Near-Field Communication) auf dem Bedienfeld des Geräts mit einer registrierten IC-Karte (Integrated Circuit Card).
2. Halten Sie Ihre Benutzer-ID an das Display.
3. Drücken Sie die Schaltfläche für die Kartenregistrierung.
4. Halten Sie eine neue IC-Karte an das NFC-Symbol.

   Die Nummer der neuen IC-Karte wird dann im Gerät registriert.
5. Drücken Sie die Taste „OK“.

Zugehörige Informationen

- Verwenden der Benutzersperre 3.0

Ein externes IC-Kartenlesegerät registrieren

Wenn Sie ein externes IC (Integrated Circuit)-Kartenlesegerät anschließen, verwenden Sie Web Based Management, um das Kartenlesegerät zu registrieren. Ihr Gerät unterstützt externe IC-Kartenlesegeräte der HID-Klassentreiber.

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 **Administrator** > **Externer Kartenleser**.

   Wenn die linke Navigationsleiste nicht angezeigt wird, navigieren Sie von ☰.
5. Geben Sie die erforderlichen Informationen ein und klicken Sie dann auf **Senden**.
6. Starten Sie das Brother-Gerät neu, um die Konfiguration zu aktivieren.
7. Verbinden Sie den Kartenleser mit Ihrem Gerät.
8. Berühren Sie den Kartenleser mit der Karte, wenn Sie Kartenauthentifizierung verwenden.

Zugehörige Informationen

- Verwenden der Benutzersperre 3.0

Sicheres Senden oder Empfangen von E-Mails

- Konfigurieren des E-Mail-Versands oder -Empfangs mit Web Based Management
- Senden einer E-Mail mit Benutzerauthentifizierung
- Sicheres Senden oder Empfangen von E-Mails mit SSL/TLS

Konfigurieren des E-Mail-Versands oder -Empfangs mit Web Based Management

- Der E-Mail-Empfang ist nur bei bestimmten Modellen verfügbar.
- Web Based Management sollte zum Konfigurieren des sicheren Sendens von E-Mails über eine Benutzerauthentifizierung oder das Senden und Empfangen von E-Mails mit SSL/TLS (nur unterstützte Modelle) verwendet werden.

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 im Feld **POP3/IMAP4/SMTP-Client** auf **Erweitere Einstellungen** und vergewissern Sie sich, dass der Status von **POP3/IMAP4/SMTP-Client** auf **Aktiviert** gesetzt ist.

- Verfügbare Protokolle können je nach Gerät abweichen.
- Wenn der **Authentifizierungsmethode**-Auswahlbildschirm angezeigt wird, wählen Sie die Authentifizierungsmethode aus und befolgen Sie dann die Anweisungen auf dem Bildschirm.

6. Konfigurieren Sie die Einstellungen **POP3/IMAP4/SMTP-Client**.
   - Überprüfen Sie, ob die E-Mail-Einstellungen nach der Konfiguration richtig sind, indem Sie eine Test-E-Mail versenden.
   - Wenn Sie die POP3-/IMAP4-/SMTP-Servereinstellungen nicht kennen, wenden Sie sich an Ihren Netzwerkadministrator oder Internetdienstanbieter (ISP).
7. Klicken Sie zum Abschluss auf **Senden**.

   Das Dialogfeld **Konfiguration des E-Mail-Versands/Empfangs testen** wird angezeigt.
8. Folgen Sie den Anweisungen im Dialogfeld, um die aktuellen Einstellungen zu testen.

Zugehörige Informationen

- Sicheres Senden oder Empfangen von E-Mails

Verwandte Themen:

- Sicheres Senden oder Empfangen von E-Mails mit SSL/TLS

Senden einer E-Mail mit Benutzerauthentifizierung

Das Gerät sendet E-Mails über einen E-Mail-Server, der eine Benutzerauthentifizierung erfordert. Diese Methode verhindert unauthorized Zugriff auf den E-Mail-Server.

Sie können E-Mail-Benachrichtigungen, E-Mail-Berichte und I-Fax (nur bei bestimmten Modellen verfügbar) unter Verwendung der Benutzerauthentifizierung versenden.

- Verfügbare Protokolle können je nach Gerät abweichen.
- Web Based Management sollte zum Konfigurieren der SMTP-Authentifizierung verwendet werden.

Einstellungen des E-Mail-Servers

Die Einstellungen der SMTP-Authentifizierungsmethode müssen so konfiguriert werden, dass diese mit der vom E-Mail-Server verwendeten Methode übereinstimmen. Für ausführliche Informationen zu den Einstellungen des E-Mail-Servers wenden Sie sich an Ihren Netzwerkadministrator oder Internetanbieter.

Um die SMTP-Serverauthentifizierung mit Web Based Management zu aktivieren, wählen Sie die Authentifizierungsmethode unter **Serverauthentifizierungsmethode** auf dem **POP3/IMAP4/SMTP-Client**-Bildschirm aus.

Zugehörige Informationen

- Sicheres Senden oder Empfangen von E-Mails

Sicheres Senden oder Empfangen von E-Mails mit SSL/TLS

Ihr Gerät unterstützt SSL/TLS-Kommunikationsmethoden. Zur Verwendung eines E-Mail-Servers, der SSL/TLS-Kommunikation verwendet, müssen Sie folgende Einstellungen konfigurieren.

- Der E-Mail-Empfang ist nur bei bestimmten Modellen verfügbar.
- Web Based Management sollte zum Konfigurieren von SSL/TLS verwendet werden.

Server-Zertifikat verifizieren

Unter **SSL/TLS**, wenn Sie **SSL** oder **TLS** auswählen, wird das Kontrollkästchen **Server-Zertifikat verifizieren** automatisch aktiviert.

- 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.
- Wenn Sie das Server-Zertifikat nicht überprüfen müssen, deaktivieren Sie das Kontrollkästchen **Server-Zertifikat verifizieren**.

Portnummer

Wenn Sie **SSL** oder **TLS** wählen, wird der Wert für **Port** an das Protokoll angepasst. Um die Portnummer manuell zu ändern, wählen Sie die **SSL/TLS**-Einstellungen und geben Sie die Portnummer ein.

Die Kommunikationsmethode des Geräts muss so konfiguriert werden, dass sie mit der vom E-Mail-Server verwendeten Methode übereinstimmt. Für ausführliche Informationen zu den Einstellungen des E-Mail-Servers wenden Sie sich an Ihren Netzwerkadministrator oder Internetanbieter.

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

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

SMTP	**Port**	587
	Serverauthentifizierungsmethode	**SMTP-AUTH**
	SSL/TLS	**TLS**
POP3	**Port**	995
	SSL/TLS	**SSL**
IMAP4	**Port**	993
	SSL/TLS	**SSL**

Zugehörige Informationen

- Sicheres Senden oder Empfangen von E-Mails

Verwandte Themen:

- Konfigurieren des E-Mail-Versands oder -Empfangs mit Web Based Management
- Konfigurieren von Zertifikaten für die Gerätesicherheit

Speichern des Druckprotokolls im Netzwerk

- Speichern des Druckprotokolls im Netzwerk - Überblick
- Konfigurieren der Einstellungen für Speichern des Druckprotokolls im Netzwerk mit Web Based Management
- Verwenden der Fehlererkennungseinstellung von Speichern des Druckprotokolls im Netzwerk
- Verwenden von Speichern des Druckprotokolls im Netzwerk mit Benutzersperre 3.0

Speichern des Druckprotokolls im Netzwerk - Überblick

Mit der Funktion Speichern des Druckprotokolls im Netzwerk können Sie die Druckprotokolldatei Ihres Geräts mit dem Protokoll Common Internet File System (CIFS) auf einem Netzwerkserver speichern. Sie können die ID, die Art des Druckauftrags, den Auftragsnamen, Benutzernamen, Datum, Uhrzeit und die Anzahl der gedruckten Seiten für jeden Druckauftrag aufzeichnen. CIFS ist das Protokoll, das über TCP/IP läuft und Computern im Netzwerk die Freigabe von Dateien über ein Intranet oder das Internet ermöglicht.

Die folgenden Druckfunktionen werden im Druckprotokoll aufgezeichnet:

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

- Druckaufträge von Ihrem Computer
- USB-Direktdruck
- Kopieren
- Fax-Empfang
- Web Connect-Druck

- Die Funktion Speichern des Druckprotokolls im Netzwerk unterstützt die Kerberos-Authentifizierung und die NTLMv2-Authentifizierung. Sie müssen das SNTP-Protokoll (Netzwerk-Zeitserver) konfigurieren oder Datum, Uhrzeit und Zeitzone für die Authentifizierung über das Funktionstastenfeld korrekt festlegen.
- Sie können die Dateiart auf TXT oder CSV festlegen, wenn Sie eine Datei auf dem Server speichern.

Zugehörige Informationen

- Speichern des Druckprotokolls im Netzwerk

Konfigurieren der Einstellungen für Speichern des Druckprotokolls im Netzwerk mit Web Based Management

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 **Administrator** > **Druckprotok. im Netzw. speichern**.

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

5. Klicken Sie im Feld **Druckprotokoll** auf **Ein**.
6. Konfigurieren Sie die folgenden Einstellungen:

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

Option	Beschreibung
Netzwerkordnerpfad	Geben Sie den Zielordner ein, in dem das Druckprotokoll auf dem CIFS-Server gespeichert werden soll (z. B. \\ComputerName \SharedFolder).
Dateiname	Geben Sie den Dateinamen (bis zu 32 Zeichen) ein, den Sie für das Druckprotokoll verwenden möchten.
Dateityp	Wählen Sie die Option **TXT** oder **CSV** für den Dateityp des Druckprotokolls aus.
Zeitquelle für Protokoll	Wählen Sie die Zeitquelle für das Druckprotokoll.
Authentifizierungsmethode	Wählen Sie die Authentifizierungsmethode, die für den Zugriff auf den CIFS-Server erforderlich ist: **Auto**, **Kerberos** oder **NTLMv2**. Kerberos ist ein Authentifizierungsprotokoll, mit dem Geräte oder Personen ihre Identität gegenüber Netzwerkservern mit einer einzelnen Anmeldung sicher beweisen können. NTLMv2 ist die Authentifizierungsmethode, die von Windows zur Anmeldung bei Servern verwendet wird. • **Auto**: Wenn Sie **Auto** wählen, wird NTLMv2 als Authentifizierungsmethode verwendet. • **Kerberos**: Wählen Sie die Option **Kerberos**, um nur die Kerberos-Authentifizierung zu verwenden. • **NTLMv2**: Wählen Sie die Option **NTLMv2**, um nur die NTLMv2-Authentifizierung zu verwenden.

Option	Beschreibung
	• Für die **Kerberos**- und **NTLMv2**-Authentifizierung müssen Sie auch die **Datum/Uhrzeit**-Einstellungen oder das SNTP-Protokoll (Netzwerk-Zeitserver) und den DNS-Server konfigurieren. • Sie können die Einstellungen für „Datum“ und „Uhrzeit“ auch über das Funktionstastenfeld des Gerätes konfigurieren.
Benutzername	Geben Sie den Benutzernamen für die Authentifizierung (bis zu 96 Zeichen) ein. Wenn der Benutzername ein Teil einer Domäne ist, geben Sie den Benutzernamen in einer der folgenden Notationen ein: Benutzer@Domäne oder Domäne\Benutzer.
Kennwort	Geben Sie das Kennwort für die Authentifizierung (bis zu 32 Zeichen) ein.
Kerberos-Serveradresse (falls erforderlich)	Geben Sie die KDC-Hostadresse (Key Distribution Center, zum Beispiel: kerberos.beispiel.de; bis zu 64 Zeichen) oder die IP-Adresse (zum Beispiel: 192.168.56.189) ein.
Fehlererkennungseinstellung	Wählen Sie, welche Aktion unternommen werden soll, wenn das Druckprotokoll aufgrund eines Netzwerkfehlers nicht auf dem Server gespeichert werden kann.

7. Bestätigen Sie im Feld **Verbindungsstatus** den letzten Anmeldestatus.

Sie können auch den Fehlerstatus im Display des Geräts überprüfen.

8. Klicken Sie auf **Senden**, um die Seite **Test-Druckprotokoll im Netzwerk** anzuzeigen.

   Klicken Sie, um die Einstellungen zu testen, auf **Ja**, und fahren Sie dann mit dem nächsten Schritt fort.

   Um den Test zu überspringen, klicken Sie auf **Nein**. Ihre Einstellungen werden automatisch übermittelt.
9. Das Gerät testet Ihre Einstellungen.
10. Wenn Ihre Einstellungen übernommen wurden, wird **Test: OK** auf dem Bildschirm angezeigt.

    Wenn **Test: Fehler** angezeigt wird, überprüfen Sie alle Einstellungen und klicken dann auf **Senden**, um die Testseite erneut anzuzeigen.

Zugehörige Informationen

- Speichern des Druckprotokolls im Netzwerk

Verwenden der Fehlererkennungseinstellung von Speichern des Druckprotokolls im Netzwerk

Verwenden Sie die Fehlererkennungseinstellungen, um die Aktion zu bestimmen, die unternommen werden soll, wenn das Druckprotokoll aufgrund eines Netzwerkfehlers nicht auf dem Server gespeichert werden kann.

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 **Administrator** > **Druckprotok. im Netzw. speichern**.

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

5. Wählen Sie im Abschnitt **Fehlererkennungseinstellung** die Option **Druck abbrechen** oder **Prot.ignorieren&Druck**.

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

Option	Beschreibung
Druck abbrechen	Wenn Sie die Option **Druck abbrechen** wählen, werden die Druckaufträge canceled, wenn das Druckprotokoll nicht auf dem Server gespeichert werden kann. Auch wenn Sie die Option **Druck abbrechen** wählen, druckt das Gerät ein empfangenes Fax aus.

Prot.ignorieren&Druck	Wenn Sie die Option **Prot.ignorieren&Druck** wählen, druckt das Gerät die Dokumentation auch dann aus, wenn das Druckprotokoll nicht auf dem Server gespeichert werden kann.
	
	Wenn die Funktion zum Speichern des Druckprotokolls wiederhergestellt wurde, wird das Druckprotokoll wie folgt aufgezeichnet:
	
	`Id, Type, Job Name, User Name, Date, Time, Print Pages`
	`1, Print(xxxxxxx), "Document01.doc", "user01", 03/03/20xx, 14:01:32, 52`
	`2, Print(xxxxxxx), "Document02.doc", "user01", 03/03/20xx, 14:45:30, ?` (a)
	`3, <Error>, ?, ?, ?, ?, ?` (b)
	`4, Print(xxxxxxx), "Report01.xls", "user02", 03/03/20xx, 19:30:40, 4`
	
	a. Wenn das Druckprotokoll nicht bei Ende des Druckvorgangs gespeichert werden kann, wird die Anzahl der gedruckten Seiten nicht aufgezeichnet.
	b. Wenn das Druckprotokoll nicht zu Druckbeginn und am Ende des Druckvorgangs gespeichert werden kann, wird das Druckprotokoll des Auftrags nicht aufgezeichnet. Wenn die Funktion wiederhergestellt wurde, wird das Auftreten eines Fehlers im Druckprotokoll angezeigt.

6. Klicken Sie auf **Senden**, um die Seite **Test-Druckprotokoll im Netzwerk** anzuzeigen.

   Klicken Sie, um die Einstellungen zu testen, auf **Ja**, und fahren Sie dann mit dem nächsten Schritt fort.

   Um den Test zu überspringen, klicken Sie auf **Nein**. Ihre Einstellungen werden automatisch übermittelt.
7. Das Gerät testet Ihre Einstellungen.
8. Wenn Ihre Einstellungen übernommen wurden, wird **Test: OK** auf dem Bildschirm angezeigt.

   Wenn **Test: Fehler** angezeigt wird, überprüfen Sie alle Einstellungen und klicken dann auf **Senden**, um die Testseite erneut anzuzeigen.

Zugehörige Informationen

- Speichern des Druckprotokolls im Netzwerk

Verwenden von Speichern des Druckprotokolls im Netzwerk mit Benutzersperre 3.0

Wenn die Benutzersperre 3.0 aktiv ist, werden die Namen der registrierten Benutzer zum Kopieren, Faxempfang, Web Connect Print und USB-Direktdruck im Bericht "Speichern des Druckprotokolls im Netzwerk" gespeichert. Wenn die Active Directory-Authentifizierung aktiviert ist, wird der Benutzername im Bericht zum Speichern des Druckprotokolls im Netzwerk aufgezeichnet:

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

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

Zugehörige Informationen

- Speichern des Druckprotokolls im Netzwerk

brother

Brother Earth

www.brotherearth.com

GER
Version 0