보안 기능 설명서

목차

소개

표기법

본 사용자 가이드에서는 다음과 같은 기호와 표기를 사용합니다.

중요	중요는 재산상의 손실 또는 제품 기능이 손실될 수 있는 잠재적인 위험이 있는 상황을 나타냅니다.
참고	참고는 사용 환경, 설치 조건 또는 특수한 사용 조건을 지정합니다.
	팁 아이콘은 힌트와 보충 정보를 제공합니다.
굵은 글꼴	굵게 표시된 내용은 제품의 제어판 또는 컴퓨터 화면의 버튼을 나타냅니다.
기울임꼴	Italicized은 중요한 점을 emphasizes하거나 관련 항목을 나타냅니다.

관련 정보

- 소개

상표

Adobe®, Reader®는 미국 및/또는 기타 국가에서 Adobe Systems Incorporated의 등록 상표 또는 상표입니다.

본 설명서에 언급된 소프트웨어 타이틀을 소유한 회사마다 특정 소유 프로그램에 적용되는 소프트웨어 License 계약이 있습니다.

Brother 제품, 관련 문서 및 기타 모든 자료에 표시되는 회사의 모든 거래명과 제품명은 이러한 각 회사의 상표 또는 등록 상표입니다.

관련 정보

- 소개

저작권

관련 정보

- 소개

네트워크 보안 기능을 사용하기 전에

구입하신 제품에서는 오늘날 사용할 수 있는 최신 네트워크 보안 및 암호화 프로토콜 중 일부를 사용합니다. 이러한 네트워크 기능을 전체 네트워크 보안 계획에 통합하면 데이터를 보호하고 제품에 대한 unauthorized 액세스를 방지할 수 있습니다.

FTP 및 TFTP 프로토콜을 사용하지 않는 것이 좋습니다. 이러한 프로토콜을 사용하여 제품에 액세스하는 것은 안전하지 않습니다.

관련 정보

- 소개
  - 불필요한 프로토콜 해제

불필요한 프로토콜 해제

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 “https://machine’s IP address”(여기서 “machine’s IP address”는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

   본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 “**Pwd**”로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.
4. 왼쪽 탐색 표시줄에서 **Network (네트워크)** > **Network (네트워크)** > **Protocol (프로토콜)**을 클릭합니다.

   왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.
5. 불필요한 프로토콜 확인란을 선택 취소하여 해제합니다.
6. **Submit (전송)**을 클릭합니다.
7. 구입하신 Brother 제품을 다시 시작하여 구성을 활성화합니다.

관련 정보

- 네트워크 보안 기능을 사용하기 전에

네트워크 보안

장치 보안을 위한 인증서 구성

SSL/TLS를 사용하여 네트워크 제품을 안전하게 관리하도록 인증서를 구성해야 합니다. 웹 기반 관리를 사용하여 인증서를 구성해야 합니다.

보안 인증서 기능 개요

구입하신 제품은 여러 보안 인증서의 사용을 지원하므로 인증 및 제품과의 통신을 안전하게 수행할 수 있습니다. 다음 보안 인증서 기능은 제품과 함께 사용할 수 있습니다.

사용하는 모델에 따라 지원되는 기능, 옵션 및 설정이 다를 수 있습니다.

- SSL/TLS 통신
- IEEE 802.1x 인증
- IPsec

구입하신 제품은 다음을 지원합니다.

- 사전 설치된 인증서

  제품에는 사전 설치된 자체 서명된 인증서가 있습니다. 이 인증서를 사용하면 다른 인증서를 생성하거나 설치하지 않고 SSL/TLS 통신을 사용할 수 있습니다.

사전 설치된 자체 서명 인증서는 특정 레벨까지 통신을 보호합니다. 보안 강화를 위해 신뢰할 수 있는 organization에서 발급된 인증서를 사용하는 것이 좋습니다.

- 자체 서명 인증서

  이 인쇄 서버는 자체 인증서를 발급합니다. 이 인증서를 사용하면 CA의 다른 인증서를 생성하거나 설치하지 않고도 SSL/TLS 통신을 쉽게 사용할 수 있습니다.
- CA(인증 기관) 인증서

  CA의 인증서를 설치하는 두 가지 방법이 있습니다. 이미 CA의 인증서가 있거나 신뢰할 수 있는 외부 CA에서 인증서를 사용하려는 경우:
  - 인쇄 서버에서 CSR(인증서 서명 요청)을 사용하는 경우:
  - 인증서와 개인 키를 가져오는 경우
- CA(인증 기관) 인증서

  CA를 식별하고 개인 키를 소유하는 CA 인증서를 사용하려면 네트워크의 보안 기능을 구성하기 전에 CA에서 CA 인증서를 가져와야 합니다.

- SSL/TLS 통신을 사용하려면 먼저 시스템 관리자에게 연락하는 것이 좋습니다.
- 인쇄 서버를 출고 시 기본 설정으로 되돌리면 설치된 인증서와 개인 키가 삭제됩니다. 인쇄 서버를 재설정한 후 동일한 인증서와 개인 키를 유지하려면 인증서와 개인 키를 내보내고 인쇄 서버를 재설정한 다음 인증서와 개인 키를 다시 설치하십시오.

관련 정보

- 장치 보안을 위한 인증서 구성

관련 내용:

- 웹 기반 관리(웹 브라우저)를 사용하여 네트워크용 IEEE 802.1x 인증 구성

인증서 생성 및 설치 방법

보안 인증서를 선택하는 경우 자체 서명된 인증서를 사용하거나 인증 기관(CA)의 인증서를 사용하는 2가지 방법이 있습니다.

옵션 1

자체 서명된 인증서

1. 웹 기반 관리를 사용하여 자체 서명된 인증서를 생성합니다.
2. 자체 서명된 인증서를 컴퓨터에 설치합니다.

옵션 2

CA의 인증서

1. 웹 기반 관리를 사용하여 CSR(Certificate Signing Request)을 생성합니다.
2. 웹 기반 관리를 사용하여 CA에서 발급된 인증서를 Brother 제품에 설치합니다.
3. 인증서를 컴퓨터에 설치합니다.

관련 정보

- 장치 보안을 위한 인증서 구성

자체 서명된 인증서 생성

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 “https://machine’s IP address”(여기서 “machine’s IP address”는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

   본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 “**Pwd**”로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.
4. 왼쪽 탐색 표시줄에서 **Network (네트워크)** > **Security (보안)** > **Certificate (인증서)**을 클릭합니다.

   왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.
5. **Create Self-Signed Certificate (자체 서명 인증서 생성)**을 클릭합니다.
6. **Common Name (일반 이름)** 및 **Valid Date (유효 기한)**를 입력합니다.
   - **Common Name (일반 이름)** 길이는 64바이트보다 짧아야 합니다. SSL/TLS 통신을 통해 본 제품에 액세스할 때 사용할 IP 주소, 노드 이름 또는 도메인 이름과 같은 식별자를 입력합니다. 노드 이름은 기본적으로 표시됩니다.
   - IPPS 또는 HTTPS 프로토콜을 사용하는 경우 자체 서명된 인증서에 사용했던 **Common Name (일반 이름)**과 다른 이름을 URL에 입력하면 경고가 나타납니다.
7. **Public Key Algorithm (공개 키 알고리즘)** 드롭다운 목록에서 설정을 선택합니다.
8. **Digest Algorithm (다이제스트 알고리즘)** 드롭다운 목록에서 설정을 선택합니다.
9. **Submit (전송)**을 클릭합니다.

관련 정보

- 장치 보안을 위한 인증서 구성

CA(인증 기관)에서 CSR(인증서 서명 요청) 생성 및 인증서 설치

신뢰할 수 있는 외부 CA(인증 기관)가 발급한 인증서가 이미 있는 경우에는 인증서와 비밀 키를 제품에 저장하고 가져오기 및 내보내기를 통해 관리할 수 있습니다. 신뢰할 수 있는 외부 CA가 발급한 인증서가 없는 경우에는 CSR(Signing Request)을 생성하고, 인증의 위해 CA를 전송하고, 반환된 인증서를 제품에 설치하십시오.

- CSR(Certificate Signing Request) 생성
- 제품에 인증서 설치

CSR(Certificate Signing Request) 생성

CSR(Certificate Signing Request)는 인증서 내에 포함된 인증 정보를 검증하기 위해 인증 기관(CA)으로 보내는 요청입니다.

CSR을 생성하기 전에 CA에서 발급한 루트 인증서를 컴퓨터에 설치하는 것이 좋습니다.

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 "https://machine's IP address"(여기서 "machine's IP address"는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

   본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 "**Pwd**"로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.
4. 왼쪽 탐색 표시줄에서 **Network (네트워크)** > **Security (보안)** > **Certificate (인증서)**을 클릭합니다.

   왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.
5. **Create CSR (CSR 생성)**을 클릭합니다.
6. **Common Name (일반 이름)**을 입력하고(필수) **Organization (조직)**에 대한 다른 정보를 추가합니다(옵션).

   - CA가 신분을 확인하고 외부에 입증하려면 근무하는 회사에 대한 자세한 정보가 필요합니다.
   - **Common Name (일반 이름)** 길이는 64바이트보다 짧아야 합니다. SSL/TLS 통신을 통해 본 제품에 액세스할 때 사용할 IP 주소, 노드 이름 또는 도메인 이름과 같은 식별자를 입력합니다. 노드 이름은 기본적으로 표시됩니다. **Common Name (일반 이름)**은 필수입니다.
   - 인증에 사용한 일반 이름과 다른 이름을 URL에 입력하면 경고가 나타납니다.
   - **Organization (조직)**, **Organization Unit (조직 구성 단위)**, **City/Locality (구/군/시)** 및 **State/Province (시/도)**의 길이는 64바이트보다 짧아야 합니다.
   - **Country/Region (국가/지역)**은 두 글자 ISO 3166 국가 코드여야 합니다.
   - X.509v3 인증서 확장을 구성하는 경우 **Configure extended partition (확장 파티션 구성)** 확인란을 선택한 다음 **Auto (Register IPv4) (자동(IPv4 등록))** 또는 **Manual (수동)**을 선택합니다.
7. **Public Key Algorithm (공개 키 알고리즘)** 드롭다운 목록에서 설정을 선택합니다.
8. **Digest Algorithm (다이제스트 알고리즘)** 드롭다운 목록에서 설정을 선택합니다.
9. **Submit (전송)**을 클릭합니다.

   CSR이 화면에 나타납니다. CSR을 파일로 저장하고, 인증 기관에서 제공한 온라인 CSR 형식으로 복사 및 붙여넣기합니다.
10. **저장**을 클릭합니다.

    - CSR을 CA로 전송하는 방법은 CA 정책을 따르십시오.
    - Windows Server의 엔터프라이즈 루트 CA를 사용하는 경우, 클라이언트 인증서를 안전하게 생성하려면 인증서 템플릿에 웹 서버 사용을 권장합니다. EAP-TLS 인증을 사용하는 IEEE 802.1x 환경에서 클라이언트 인증서를 생성하는 경우 인증서 템플릿에 사용자를 사용하는 것이 좋습니다.

관련 정보

- CA(인증 기관)에서 CSR(인증서 서명 요청) 생성 및 인증서 설치

제품에 인증서 설치

CA(인증 기관)의 인증서를 수신한 경우 아래 단계에 따라 인쇄 서버에 설치합니다.

제품의 CSR(인증서 서명 요청)과 함께 발급된 인증서만 제품에 설치할 수 있습니다. 또 다른 CSR을 생성하려면 CSR을 새로 생성하기 전에 인증서가 설치되어 있는지 확인하십시오. 제품에 인증서를 설치한 후에만 또 다른 CSR을 생성합니다. 그렇지 않으면 새 CSR을 설치하기 전에 생성된 CSR이 무효화됩니다.

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 “https://machine’s IP address”(여기서 “machine’s IP address”는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

   본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 “**Pwd**”로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.
4. 왼쪽 탐색 표시줄에서 **Network (네트워크)** > **Security (보안)** > **Certificate (인증서)**을 클릭합니다.

   왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.
5. **Install Certificate (인증서 설치)**을 클릭합니다.
6. CA에서 발생한 인증서가 포함된 파일을 탐색하고 **Submit (전송)**를 클릭합니다.

   인증서가 생성되고 제품의 메모리에 저장됩니다.

SSL/TLS 통신을 사용하려면 CA의 루트 인증서를 컴퓨터에 설치해야 합니다. 네트워크 관리자에게 문의하십시오.

관련 정보

- CA(인증 기관)에서 CSR(인증서 서명 요청) 생성 및 인증서 설치

인증서와 개인 키 가져오기 및 내보내기

인증서와 개인 키를 제품에 저장하고 가져오기나 내보내기를 통해 관리합니다.

- 인증서 및 개인 키 가져오기
- 인증서 및 개인 키 내보내기

인증서 및 개인 키 가져오기

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 “https://machine’s IP address”(여기서 “machine’s IP address”는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

   본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 “**Pwd**”로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.
4. 왼쪽 탐색 표시줄에서 **Network (네트워크)** > **Security (보안)** > **Certificate (인증서)**을 클릭합니다.

   왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.
5. **Import Certificate and Private Key (인증서 및 개인 키 가져오기)**을 클릭합니다.
6. 가져올 파일을 탐색 및 선택합니다.
7. 파일이 암호화된 경우 암호를 입력한 다음, **Submit (전송)**을 클릭합니다.

인증서 및 개인 키를 제품으로 가져옵니다.

관련 정보

- 인증서와 개인 키 가져오기 및 내보내기

인증서 및 개인 키 내보내기

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 “https://machine’s IP address”(여기서 “machine’s IP address”는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

   본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 “**Pwd**”로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.
4. 왼쪽 탐색 표시줄에서 **Network (네트워크)** > **Security (보안)** > **Certificate (인증서)**을 클릭합니다.

   왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.
5. **Export (내보내기)**로 표시된 **Certificate List (인증서 목록)**를 클릭합니다.
6. 파일을 암호화하려면 암호를 입력합니다.

   암호를 비워 두면 출력이 암호화되지 않습니다.
7. 확인을 위해 암호를 다시 입력한 다음, **Submit (전송)**을 클릭합니다.
8. **저장**을 클릭합니다.

인증서 및 개인 키를 제품으로 내보냅니다.

컴퓨터에 인증서를 가져올 수도 있습니다.

관련 정보

- 인증서와 개인 키 가져오기 및 내보내기

CA 인증서를 가져오고 내보내기

CA 인증서를 Brother 제품에서 가져오고 내보내며 저장할 수 있습니다.

- CA 인증서 가져오기
- CA 인증서 내보내기

CA 인증서 가져오기

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 “https://machine’s IP address”(여기서 “machine’s IP address”는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

   본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 “**Pwd**”로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.
4. 왼쪽 탐색 표시줄에서 **Network (네트워크)** > **Security (보안)** > **CA Certificate (CA 인증서)**을 클릭합니다.

   왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.
5. **Import CA Certificate (CA 인증서 가져오기)**을 클릭합니다.
6. 가져올 파일을 탐색합니다.
7. **Submit (전송)**을 클릭합니다.

관련 정보

- CA 인증서를 가져오고 내보내기

CA 인증서 내보내기

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 “https://machine’s IP address”(여기서 “machine’s IP address”는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

   본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 “**Pwd**”로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.
4. 왼쪽 탐색 표시줄에서 **Network (네트워크)** > **Security (보안)** > **CA Certificate (CA 인증서)**을 클릭합니다.

   왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.
5. 내보낼 인증서를 선택하고 **Export (내보내기)**를 클릭합니다.
6. **Submit (전송)**을 클릭합니다.

관련 정보

- CA 인증서를 가져오고 내보내기

SSL/TLS 사용

- SSL/TLS를 사용하여 네트워크 제품을 안전하게 관리
- SSL/TLS를 사용하여 문서를 안전하게 인쇄
- SSL/TLS를 사용하여 안전하게 이메일 송수신

SSL/TLS를 사용하여 네트워크 제품을 안전하게 관리

SSL/TLS 및 사용 가능한 프로토콜에 대한 인증서 구성

SSL/TLS 통신을 사용하기 전에 웹 기반 관리를 사용하여 제품에서 인증서를 구성합니다.

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 “https://machine’s IP address”(여기서 “machine’s IP address”는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

> 본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 “**Pwd**”로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.

4. 왼쪽 탐색 표시줄에서 **Network (네트워크)** > **Network (네트워크)** > **Protocol (프로토콜)**을 클릭합니다.

> 왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.

5. **HTTP Server Settings (HTTP 서버 설정)**을 클릭합니다.
6. **Select the Certificate (인증서 선택)** 드롭다운 목록에서 구성하려는 인증서를 선택합니다.
7. **Submit (전송)**을 클릭합니다.
8. **Yes (예)**를 클릭하여 인쇄 서버를 다시 시작합니다.

관련 정보

- SSL/TLS를 사용하여 네트워크 제품을 안전하게 관리

관련 내용:

- SSL/TLS를 사용하여 문서를 안전하게 인쇄

SSL/TLS를 사용하여 웹 기반 관리 액세스

네트워크 제품을 안전하게 관리하려면 보안 프로토콜이 있는 관리 유틸리티를 사용해야 합니다.

- HTTPS 프로토콜을 사용하려면 제품에서 HTTPS를 실행해야 합니다. HTTPS 프로토콜은 기본값으로 활성화됩니다.
- 웹 기반 관리 화면을 사용하여 HTTPS 프로토콜 설정을 변경할 수 있습니다.

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 “https://machine’s IP address”(여기서 “machine’s IP address”는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 “**Pwd**”로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.

4. 이제 HTTPS를 사용하여 제품에 액세스할 수 있습니다.

관련 정보

- SSL/TLS를 사용하여 네트워크 제품을 안전하게 관리

관리자로 Windows 사용자용 자체 서명된 인증서 설치

- 다음 단계는 Microsoft Edge에 적용됩니다. 다른 웹 브라우저를 사용하는 경우 인증서 설치 방법을 보려면 웹 브라우저의 설명서 또는 온라인 도움말을 참조하십시오.
- 웹 기반 관리를 사용하여 자체 서명된 인증서를 생성했는지 확인하십시오.

1. **Microsoft Edge** 아이콘을 마우스 오른쪽 버튼으로 클릭한 다음 **관리자 권한으로 실행**을 클릭합니다.
   사용자 계정 컨트롤 화면이 표시되면 **예**를 클릭합니다.
2. 브라우저의 주소 표시줄에 "https://machine's IP address"(여기서 "machine's IP address"는 제품의 IP 주소)를 입력합니다.
   예:
   https://192.168.1.2
   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 비공개 연결이 아닌 경우 **고급** 버튼을 클릭한 다음 웹 페이지를 계속 진행합니다.
4. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

   본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 "**Pwd**"로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.

5. 왼쪽 탐색 표시줄에서 **Network (네트워크)** > **Security (보안)** > **Certificate (인증서)**을 클릭합니다.

   왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.

6. **Export (내보내기)**을 클릭합니다.
7. 출력 파일을 암호화하려면 **Enter password (비밀번호 입력)** 필드에 암호를 입력합니다. **Enter password (비밀번호 입력)** 필드가 비어 있으면, 출력 파일이 암호화되지 않습니다.
8. **Retype password (비밀번호 재입력)** 필드에 암호를 입력한 다음 **Submit (전송)**를 클릭합니다.
9. 다운로드한 파일을 클릭하여 엽니다.
10. **인증서 가져오기 마법사**가 나타나면 **다음**를 클릭합니다.
11. **다음**을 클릭합니다.
12. 필요한 경우 암호를 입력하고 **다음**을 클릭합니다.
13. **모든 인증서를 다음 저장소에 저장**를 선택한 다음 **찾아보기...**를 클릭합니다.
14. **신뢰할 수 있는 루트 인증 기관**를 선택한 다음 **확인**를 클릭합니다.
15. **다음**을 클릭합니다.
16. **마침**을 클릭합니다.
17. 지문(엄지 손가락 지문)이 맞을 경우 **예**를 클릭합니다.
18. **확인**을 클릭합니다.

관련 정보

- SSL/TLS를 사용하여 네트워크 제품을 안전하게 관리

SSL/TLS를 사용하여 문서를 안전하게 인쇄

IPPS를 사용하여 문서 인쇄

IPP 프로토콜을 사용하여 문서를 안전하게 인쇄하기 위해 IPPS 프로토콜을 사용할 수 있습니다.

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 “https://machine’s IP address”(여기서 “machine’s IP address”는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

   본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 “**Pwd**”로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.
4. 왼쪽 탐색 표시줄에서 **Network (네트워크)** > **Network (네트워크)** > **Protocol (프로토콜)**을 클릭합니다.

   왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.
5. **IPP** 확인란이 선택되었는지 확인합니다.

   IPP 확인란이 선택되지 않은 경우 **IPP** 확인란을 선택한 다음, **Submit (전송)**를 클릭합니다.

   제품을 다시 시작하여 구성을 활성화합니다.

   제품이 다시 시작되면 제품의 웹 페이지로 돌아가 암호를 입력한 다음 왼쪽 탐색 표시줄에서 **Network (네트워크)** > **Network (네트워크)** > **Protocol (프로토콜)**을 클릭합니다.
6. **HTTP Server Settings (HTTP 서버 설정)**을 클릭합니다.
7. **HTTPS(포트 443)** 영역에서 **IPP** 확인란을 선택한 다음 **Submit (전송)**을 클릭합니다.
8. 제품을 다시 시작하여 구성을 활성화합니다.

IPPS를 사용하여 통신하면 인쇄 서버에 대한 unauthorized 액세스를 막을 수 없습니다.

관련 정보

- SSL/TLS를 사용하여 문서를 안전하게 인쇄

SNMPv3 사용

- SNMPv3를 사용하여 네트워크 제품을 안전하게 관리

SNMPv3를 사용하여 네트워크 제품을 안전하게 관리

SNMPv3(Simple Network Management Protocol version 3)는 네트워크 장치를 안전하게 관리하기 위한 사용자 인증 및 데이터 암호화를 제공합니다.

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 "https://Common Name"을 입력합니다(여기서 "Common Name"은 인증서에 할당한 공통 이름이고, IP 주소, 노드 이름 또는 도메인 이름일 수 있습니다).
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

> 본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 “**Pwd**”로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.

4. 왼쪽 탐색 표시줄에서 **Network (네트워크)** > **Network (네트워크)** > **Protocol (프로토콜)**을 클릭합니다.

> 왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.

5. **SNMP** 설정이 실행되고 있는지 확인한 다음, **Advanced Settings (고급 설정)**을 클릭합니다.
6. SNMPv1/v2c 모드 설정을 구성합니다.

옵션	설명
SNMP v1/v2c read-write access (SNMP v1/v2c 읽기/쓰기 액세스)	인쇄 서버는 SNMP 프로토콜의 버전 1과 버전 2c를 사용합니다. 이 모드에서는 제품의 모든 응용 프로그램을 사용할 수 있습니다. 그러나 이 모드는 사용자를 인증하지 않고 데이터가 암호화되지 않기 때문에 안전하지 않습니다.
SNMP v1/v2c read-only access (SNMP v1/v2c 읽기 전용 액세스)	인쇄 서버는 SNMP 프로토콜의 버전 1 및 버전 2c의 읽기 전용 액세스를 사용합니다.
Disabled (비활성화)	SNMP 프로토콜 버전 1 및 버전 2c를 비활성화합니다. SNMPv1/v2c를 사용하는 모든 응용 프로그램이 제한됩니다. SNMPv1/v2c 응용 프로그램의 사용을 허용하려면 **SNMP v1/v2c read-only access (SNMP v1/v2c 읽기 전용 액세스)** 또는 **SNMP v1/v2c read-write access (SNMP v1/v2c 읽기/쓰기 액세스)** 모드를 사용합니다.

7. SNMPv3 모드 설정을 구성합니다.

옵션	설명
Enabled (활성화)	인쇄 서버는 SNMP 프로토콜의 버전 3을 사용합니다. 인쇄 서버를 안전하게 관리하려면 SNMPv3 모드를 사용하십시오.
Disabled (비활성화)	SNMP 프로토콜 버전 3을 비활성화합니다. SNMPv3을 사용하는 모든 응용 프로그램이 제한됩니다. SNMPv3 응용 프로그램을 사용할 수 있도록 허용하려면 SNMPv3 모드를 사용합니다.

8. **Submit (전송)**을 클릭합니다.

> 제품에 프로토콜 설정 옵션이 표시되면 원하는 옵션을 선택합니다.

9. 제품을 다시 시작하여 구성을 활성화합니다.

관련 정보

- SNMPv3 사용

IPsec 사용

IPsec 소개

IPsec(인터넷 프로토콜 보안)은 옵션인 인터넷 프로토콜 기능을 사용하여 데이터 조작을 방지하고 IP 패킷으로 전송되는 데이터의 기밀성을 보장하는 보안 프로토콜입니다. IPsec은 컴퓨터에서 프린터로 전송되는 인쇄 데이터 등 네트워크를 통해 전송되는 데이터를 암호화합니다. 네트워크 계층에서 데이터가 암호화되기 때문에 더 높은 수준의 프로토콜을 사용하는 응용 프로그램이 사용자 모르게 IPsec을 사용합니다.

IPsec은 다음 기능을 지원합니다.

- IPsec 전송

  IPsec 설정 조건에 따라 네트워크에 연결된 컴퓨터는 IPsec을 사용하여 지정된 장치에서 데이터를 주고받습니다. 장치에서 IPsec을 사용하여 통신을 시작하면 먼저 IKE(인터넷 키 교환)를 사용하여 키를 교환한 다음 키를 사용하여 암호화된 데이터를 전송합니다.

  또한 IPsec에는 전송 모드와 터널 모드, 두 가지 작동 모드가 있습니다. 전송 모드는 주로 장치 간의 통신에 사용되며 터널 모드는 VPN(Virtual Private Network)과 같은 환경에서 사용됩니다.

IPsec 전송의 경우 다음 조건이 필요합니다.

- IPsec을 사용하여 통신할 수 있는 컴퓨터가 네트워크에 연결되어 있습니다.
- 구입하신 제품은 IPsec 통신에 대해 구성되어 있습니다.
- 구입하신 제품에 연결된 컴퓨터는 IPsec 연결에 대해 구성되어 있습니다.

- IPsec 설정

  IPsec을 사용한 연결에 필요한 설정입니다. 이러한 설정은 웹 기반 관리를 사용하여 구성할 수 있습니다.

IPsec 설정을 구성하려면 네트워크에 연결된 컴퓨터의 브라우저를 사용해야 합니다.

관련 정보

- IPsec 사용

웹 기반 관리를 사용하여 IPsec 구성

IPsec 연결 조건은 **Address (주소)** 및 **IPsec**이라는 2개의 **Template (템플릿)** 유형으로 구성됩니다. 연결 조건은 최대 10개까지 구성할 수 있습니다.

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 "https://machine's IP address"(여기서 "machine's IP address"는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

> 본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 "**Pwd**"로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.

4. 왼쪽 탐색 표시줄에서 **Network (네트워크)** > **Security (보안)** > **IPsec**을 클릭합니다.

> 왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.

5. 설정을 구성합니다.

옵션	설명
Status (상태)	IPsec을 실행하거나 해제합니다.
Negotiation Mode (협상 모드)	IKE Phase 1에 대해 **Negotiation Mode (협상 모드)**를 선택합니다. IKE는 IPsec을 사용하여 암호화된 통신을 수행하기 위해 암호화 키를 교환하는 데 사용되는 프로토콜입니다. **Main (기본)** 모드의 경우 처리 속도는 느리지만 보안 수준은 높습니다. **Aggressive (적극적)** 모드의 경우 처리 속도는 **Main (기본)** 모드보다 빠르지만 보안 수준이 낮습니다.
All Non-IPsec Traffic (모든 비 IPsec 트래픽)	IPsec이 아닌 패킷에 대해 취할 동작을 선택합니다. 웹 서비스를 사용하는 경우 **All Non-IPsec Traffic (모든 비 IPsec 트래픽)**에 대해 **Allow (허용)**을 선택해야 합니다. **Drop (삭제)**을 선택하면 웹 서비스를 사용할 수 없습니다.
Broadcast/Multicast Bypass (브로드캐스트/멀티캐스트 바이패스)	**Enabled (활성화)** 또는 **Disabled (비활성화)**을 선택합니다.
Protocol Bypass (프로토콜 바이패스)	원하는 옵션의 확인란을 선택합니다.
Rules (규칙)	**Enabled (활성화)** 확인란을 선택하여 템플릿을 활성화합니다. 확인란을 여러 개 선택할 경우 선택한 확인란의 설정이 충돌하면 번호가 낮은 확인란이 우선합니다. 해당 드롭다운 목록을 클릭하여 IPsec 연결 조건에 사용되는 **Address Template (주소 템플릿)**을 선택합니다. **Address Template (주소 템플릿)**을 추가하려면 **Add Template (템플릿 추가)**을 클릭합니다. 해당 드롭다운 목록을 클릭하여 IPsec 연결 조건에 사용되는 **IPsec Template (IPsec 템플릿)**을 선택합니다. **IPsec Template (IPsec 템플릿)**을 추가하려면 **Add Template (템플릿 추가)**을 클릭합니다.

6. **Submit (전송)**을 클릭합니다.

   새 설정을 활성화하기 위해 제품을 다시 시작해야 하는 경우 다시 시작할지 묻는 확인 화면이 나타납니다.

   Rules (규칙) 표에서 실행한 템플릿에 빈 항목이 있으면 오류 메시지가 나타납니다. 선택 사항을 확인하고 다시 **Submit (전송)**을 클릭합니다.

관련 정보

- IPsec 사용

관련 내용:

- 장치 보안을 위한 인증서 구성

웹 기반 관리를 사용하여 IPsec 주소 템플릿 구성

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 “https://machine’s IP address”(여기서 “machine’s IP address”는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

   본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 “**Pwd**”로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.
4. 왼쪽 탐색 표시줄에서 **Network (네트워크)** > **Security (보안)** > **IPsec Address Template (IPsec 주소 템플릿)**을 클릭합니다.

   왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.
5. **Delete (삭제)** 버튼을 클릭하여 **Address Template (주소 템플릿)**을 삭제합니다. **Address Template (주소 템플릿)**을 사용 중인 경우 삭제할 수 없습니다.
6. 만들려는 **Address Template (주소 템플릿)**을 클릭합니다. **IPsec Address Template (IPsec 주소 템플릿)**이 나타납니다.
7. 설정을 구성합니다.

옵션	설명
Template Name (템플릿 이름)	템플릿의 이름을 입력합니다 (최대 16자).
Local IP Address (로컬 IP 주소)	• **IP Address (IP 주소)** IP 주소를 지정합니다. 드롭다운 목록에서 **ALL IPv4 Address (모든 IPv4 주소)**, **ALL IPv6 Address (모든 IPv6 주소)**, **ALL Link Local IPv6 (모든 링크 로컬 IPv6)** 또는 **Custom (사용자 지정)**을 선택합니다. 드롭다운 목록에서 **Custom (사용자 지정)**을 선택한 경우 텍스트 상자에 IP 주소(IPv4 또는 IPv6)를 입력합니다. • **IP Address Range (IP 주소 범위)** 텍스트 상자에 IP 주소 범위의 시작하는 IP 주소와 끝나는 IP 주소를 입력합니다. 시작하는 IP 주소와 끝나는 IP 주소가 IPv4 또는 IPv6에 standardized되지 않거나 끝나는 IP 주소가 시작하는 주소보다 작을 경우 오류가 발생합니다. • **IP Address / Prefix (IP 주소/접두어)** CIDR 표기법을 사용하여 IP 주소를 지정합니다. 예: 192.168.1.1/24 접두어가 192.168.1.1의 24비트 서브넷 마스크(255.255.255.0) 형식으로 지정되어 있으므로 주소 192.168.1.###는 유효합니다.
Remote IP Address (원격 IP 주소)	• **Any (모두)** **Any (모두)**을 선택하면 모든 IP 주소가 활성화됩니다. • **IP Address (IP 주소)** 텍스트 상자에 지정한 IP 주소(IPv4 또는 IPv6)를 입력합니다. • **IP Address Range (IP 주소 범위)** IP 주소 범위의 첫 번째와 마지막 IP 주소를 입력합니다. 첫 번째와 마지막 IP 주소가 IPv4 또는 IPv6에 standardized되지 않거나 마지막 IP 주소가 첫 번째 주소보다 작을 경우 오류가 발생합니다. • **IP Address / Prefix (IP 주소/접두어)** CIDR 표기법을 사용하여 IP 주소를 지정합니다.

옵션	설명
	예: 192.168.1.1/24 접두어가 192.168.1.1의 24비트 서브넷 마스크(255.255.255.0) 형식으로 지정되어 있으므로 주소 192.168.1.###는 유효합니다.

8. Submit (전송)을 클릭합니다.

현재 사용 중인 템플릿의 설정을 변경하려면 제품을 다시 시작하여 구성을 활성화합니다.

관련 정보

- IPsec 사용

웹 기반 관리를 사용하여 IPsec 템플릿 구성

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 “https://machine’s IP address”(여기서 “machine’s IP address”는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

> 본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 “**Pwd**”로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.

4. 왼쪽 탐색 표시줄에서 **Network (네트워크)** > **Security (보안)** > **IPsec Template (IPsec 템플릿)**을 클릭합니다.

> 왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.

5. **Delete (삭제)** 버튼을 클릭하여 **IPsec Template (IPsec 템플릿)**을 삭제합니다. **IPsec Template (IPsec 템플릿)**을 사용 중인 경우 삭제할 수 없습니다.
6. 만들려는 **IPsec Template (IPsec 템플릿)**을 클릭합니다. **IPsec Template (IPsec 템플릿)** 화면이 나타납니다. 구성 필드는 선택한 **Use Prefixed Template (접두어 템플릿 사용)** 및 **Internet Key Exchange (IKE) (IKE(Internet Key Exchange))** 설정에 따라 다릅니다.
7. **Template Name (템플릿 이름)** 필드에 템플릿의 이름을 입력합니다(최대 16자).
8. **Use Prefixed Template (접두어 템플릿 사용)** 드롭다운 목록에서 **Custom (사용자 지정)**를 선택한 경우 **Internet Key Exchange (IKE) (IKE(Internet Key Exchange))** 옵션을 선택한 다음, 필요한 경우 설정을 변경합니다.
9. **Submit (전송)**을 클릭합니다.

관련 정보

- IPsec 사용
  - IPsec 템플릿의 IKEv1 설정
  - IPsec 템플릿의 IKEv2 설정
  - IPsec 템플릿의 수동 설정

IPsec 템플릿의 IKEv1 설정

옵션	설명
Template Name (템플릿 이름)	템플릿의 이름을 입력합니다 (최대 16자).
Use Prefixed Template (접두어 템플릿 사용)	**Custom (사용자 지정)**, **IKEv1 High Security (IKEv1 높은 수준 보안)** 또는 **IKEv1 Medium Security (IKEv1 중간 수준 보안)**를 선택합니다. 설정 항목은 선택한 템플릿에 따라 다릅니다.
Internet Key Exchange (IKE) (IKE(Internet Key Exchange))	IKE는 IPsec을 사용하여 암호화된 통신을 수행하기 위해 암호화 키를 교환하는 데 사용되는 통신 프로토콜입니다. 해당 시간 동안에만 암호화된 통신을 수행하기 위해 IPsec에 필요한 암호화 알고리즘이 결정되고 암호화 키가 공유됩니다. IKE의 경우 Diffie-Hellman 키 교환 방법을 사용하여 암호화 키를 교환하고 IKE로 제한된 암호화 통신이 수행됩니다. **Use Prefixed Template (접두어 템플릿 사용)**에서 **Custom (사용자 지정)**을 선택한 경우 **IKEv1**을 선택합니다.
Authentication Type (인증 유형)	• **Diffie-Hellman Group (Diffie-Hellman 그룹)** 이 키 교환 방법은 보호되지 않은 네트워크에서 비밀 키를 안전하게 교환할 수 있도록 합니다. Diffie-Hellman 키 교환 방법은 비밀 키가 아니라 DLP(Discrete Logarithm Problem)를 사용하며, 임의의 숫자를 사용하여 생성된 공개 정보와 비밀 키를 주고받습니다. **Group1 (그룹1)**, **Group2 (그룹2)**, **Group5 (그룹5)** 또는 **Group14 (그룹14)**를 선택합니다. • **Encryption (암호화)** **DES**, **3DES**, **AES-CBC 128** 또는 **AES-CBC 256**를 선택합니다. • **Hash (해시)** **MD5**, **SHA1**, **SHA256**, **SHA384** 또는 **SHA512**를 선택합니다. • **SA Lifetime (SA 수명)** IKE SA 수명을 지정합니다. 시간(초)과 킬로바이트(KB) 수를 입력합니다.
Encapsulating Security (보안 캡슐화)	• **Protocol (프로토콜)** **ESP**, **AH** 또는 **AH+ESP**를 선택합니다. - ESP는 IPsec을 사용하여 암호화된 통신을 수행하는 프로토콜입니다. ESP는 페이로드(통신되는 내용)를 암호화하고 추가 정보를 추가합니다. IP 패킷은 헤더 및 헤더 다음의 암호화된 페이로드로 구성됩니다. 암호화된 데이터와 함께 IP 패킷은 암호화 모드 및 암호화 키와 관련된 정보, 인증 데이터 등도 포함합니다. - AH는 발신자를 인증하고 데이터 조작을 금지하는 IPsec 프로토콜의 일부입니다(데이터의 무결성 보장). IP 패킷에서 데이터는 헤더 바로 뒤에 삽입됩니다. 또한 패킷에는 발신자의 위조 및 데이터 조작을 방지하기 위해 통신 내용에서 방정식을 사용하여 계산되는 해시 값, 비밀 키 등이 포함됩니다. ESP와 달리 통신 내용이 암호화되지 않고 일반 텍스트로 데이터를 주고받습니다. • **Encryption (암호화) (AH 옵션에 사용할 수 없음.)** **DES**, **3DES**, **AES-CBC 128** 또는 **AES-CBC 256**를 선택합니다. • **Hash (해시)** **None (안 함)**, **MD5**, **SHA1**, **SHA256**, **SHA384** 또는 **SHA512**를 선택합니다. **Protocol (프로토콜)**에 대해 **ESP**를 선택한 경우에만 **None (안 함)**을 선택할 수 있습니다.

옵션	설명
	• **SA Lifetime (SA 수명)** IKE SA 수명을 지정합니다. 시간(초)과 킬로바이트(KB) 수를 입력합니다. • **Encapsulation Mode (캡슐화 모드)** **Transport (전송)** 또는 **Tunnel (터널)**를 선택합니다. • **Remote Router IP-Address (원격 라우터 IP 주소)** 원격 라우터의 IP 주소(IPv4 또는 IPv6)를 입력합니다. **Tunnel (터널)** 모드가 선택된 경우에만 이 정보를 입력합니다. SA(Security Association)는 통신이 시작되기 전에 보안 통신 채널을 설정하기 위해 암호화 모드 및 암호화 키 등의 정보를 교환하고 공유하는 IPsec 또는 IPv6를 사용하는 암호화된 통신 방법입니다. SA는 설정된 가상 암호화 통신 채널을 가리킬 수도 있습니다. IPsec에 사용되는 SA는 암호화 모드를 설정하며 키를 교환하고 IKE (인터넷 키 교환) 표준 절차에 따라 상호 인증을 실행합니다. 또한 SA는 주기적으로 업데이트됩니다.
Perfect Forward Secrecy (PFS) (전달 완전 보안(PFS))	PFS는 메시지를 암호화하는 데 사용된 이전 키에서 키를 파생하지 않습니다. 또한, 메시지 암호화에 사용된 키를 부모 키에서 가져왔을 경우 그 부모 키를 사용하여 다른 키를 가져오지 않습니다. 따라서 키가 손상되더라도 해당 키를 사용하여 암호화된 메시지로만 손상이 제한됩니다. **Enabled (활성화)** 또는 **Disabled (비활성화)**를 선택합니다.
Authentication Method (인증 방법)	인증 방법을 선택합니다. **Pre-Shared Key (사전 공유 키)** 또는 **Certificates (인증서)**를 선택합니다.
Pre-Shared Key (사전 공유 키)	통신을 암호화하면 다른 채널을 사용하기 전에 암호화 키가 교환되고 공유됩니다. **Authentication Method (인증 방법)**으로 **Pre-Shared Key (사전 공유 키)**를 선택한 경우 **Pre-Shared Key (사전 공유 키)**를 입력합니다(최대 32자). • **Local/ID Type/ID (로컬/ID 종류/ID)** 발신자의 ID 유형을 선택하고 ID를 입력합니다. 유형으로 **IPv4 Address (IPv4 주소)**, **IPv6 Address (IPv6 주소)**, **FQDN**, **E-mail Address (전자 메일 주소)** 또는 **Certificate (인증서)**를 선택합니다. **Certificate (인증서)**를 선택한 경우 **ID** 필드에 인증서의 일반 이름을 입력합니다. • **Remote/ID Type/ID (원격/ID 종류/ID)** 수신자의 ID 유형을 선택한 다음 ID를 입력합니다. 유형으로 **IPv4 Address (IPv4 주소)**, **IPv6 Address (IPv6 주소)**, **FQDN**, **E-mail Address (전자 메일 주소)** 또는 **Certificate (인증서)**를 선택합니다. **Certificate (인증서)**를 선택한 경우 **ID** 필드에 인증서의 일반 이름을 입력합니다.
Certificate (인증서)	**Authentication Method (인증 방법)**에 **Certificates (인증서)**를 선택한 경우 인증서를 선택합니다. 웹 기반 관리의 보안 구성 화면에서 **Certificate (인증서)** 페이지를 사용하여 만든 인증서만 선택할 수 있습니다.

관련 정보

- 웹 기반 관리를 사용하여 IPsec 템플릿 구성

IPsec 템플릿의 IKEv2 설정

옵션	설명
Template Name (템플릿 이름)	템플릿의 이름을 입력합니다 (최대 16자).
Use Prefixed Template (접두어 템플릿 사용)	**Custom (사용자 지정)**, **IKEv2 High Security (IKEv2 높은 수준 보안)** 또는 **IKEv2 Medium Security (IKEv2 중간 수준 보안)**를 선택합니다. 설정 항목은 선택한 템플릿에 따라 다릅니다.
Internet Key Exchange (IKE) (IKE(Internet Key Exchange))	IKE는 IPsec을 사용하여 암호화된 통신을 수행하기 위해 암호화 키를 교환하는 데 사용되는 통신 프로토콜입니다. 해당 시간 동안에만 암호화된 통신을 수행하기 위해 IPsec에 필요한 암호화 알고리즘이 결정되고 암호화 키가 공유됩니다. IKE의 경우 Diffie-Hellman 키 교환 방법을 사용하여 암호화 키를 교환하고 IKE로 제한된 암호화 통신이 수행됩니다. **Use Prefixed Template (접두어 템플릿 사용)**에서 **Custom (사용자 지정)**을 선택한 경우 **IKEv2**을 선택합니다.
Authentication Type (인증 유형)	• **Diffie-Hellman Group (Diffie-Hellman 그룹)** 이 키 교환 방법은 보호되지 않은 네트워크에서 비밀 키를 안전하게 교환할 수 있도록 합니다. Diffie-Hellman 키 교환 방법은 비밀 키가 아니라 DLP(Discrete Logarithm Problem)를 사용하며, 임의의 숫자를 사용하여 생성된 공개 정보와 비밀 키를 주고받습니다. **Group1 (그룹1)**, **Group2 (그룹2)**, **Group5 (그룹5)** 또는 **Group14 (그룹14)**를 선택합니다. • **Encryption (암호화)** DES, 3DES, AES-CBC 128 또는 AES-CBC 256를 선택합니다. • **Hash (해시)** MD5, SHA1, SHA256, SHA384 또는 SHA512를 선택합니다. • **SA Lifetime (SA 수명)** IKE SA 수명을 지정합니다. 시간(초)과 킬로바이트(KB) 수를 입력합니다.
Encapsulating Security (보안 캡슐화)	• **Protocol (프로토콜)** ESP를 선택합니다. ESP는 IPsec을 사용하여 암호화된 통신을 수행하는 프로토콜입니다. ESP는 페이로드(통신되는 내용)를 암호화하고 추가 정보를 추가합니다. IP 패킷은 헤더 및 헤더 다음의 암호화된 페이로드로 구성됩니다. 암호화된 데이터와 함께 IP 패킷은 암호화 모드 및 암호화 키와 관련된 정보, 인증 데이터 등도 포함합니다. • **Encryption (암호화)** DES, 3DES, AES-CBC 128 또는 AES-CBC 256를 선택합니다. • **Hash (해시)** MD5, SHA1, SHA256, SHA384 또는 SHA512를 선택합니다. • **SA Lifetime (SA 수명)** IKE SA 수명을 지정합니다. 시간(초)과 킬로바이트(KB) 수를 입력합니다. • **Encapsulation Mode (캡슐화 모드)** **Transport (전송)** 또는 **Tunnel (터널)**를 선택합니다. • **Remote Router IP-Address (원격 라우터 IP 주소)** 원격 라우터의 IP 주소(IPv4 또는 IPv6)를 입력합니다. **Tunnel (터널)** 모드가 선택된 경우에만 이 정보를 입력합니다.

옵션	설명
	SA(Security Association)는 통신이 시작되기 전에 보안 통신 채널을 설정하기 위해 암호화 모드 및 암호화 키 등의 정보를 교환하고 공유하는 IPsec 또는 IPv6를 사용하는 암호화된 통신 방법입니다. SA는 설정된 가상 암호화 통신 채널을 가리킬 수도 있습니다. IPsec에 사용되는 SA는 암호화 모드를 설정하며 키를 교환하고 IKE (인터넷 키 교환) 표준 절차에 따라 상호 인증을 실행합니다. 또한 SA는 주기적으로 업데이트됩니다.
Perfect Forward Secrecy (PFS) (전달 완전 보안(PFS))	PFS는 메시지를 암호화하는 데 사용된 이전 키에서 키를 파생하지 않습니다. 또한, 메시지 암호화에 사용된 키를 부모 키에서 가져왔을 경우 그 부모 키를 사용하여 다른 키를 가져오지 않습니다. 따라서 키가 손상되더라도 해당 키를 사용하여 암호화된 메시지로만 손상이 제한됩니다. **Enabled (활성화)** 또는 **Disabled (비활성화)**를 선택합니다.
Authentication Method (인증 방법)	인증 방법을 선택합니다. **Pre-Shared Key (사전 공유 키)**, **Certificates (인증서)**, **EAP - MD5** 또는 **EAP - MS-CHAPv2**를 선택합니다. EAP는 PPP 확장자인 인증 프로토콜입니다. IEEE 802.1x인 EAP를 사용하면 각 세션 동안 사용자 인증에 다른 키가 사용됩니다. 다음 설정은 **Authentication Method (인증 방법)**에서 **EAP - MD5** 또는 **EAP - MS-CHAPv2**가 선택된 경우에만 필요합니다. • **Mode (모드)** **Server-Mode (서버 모드)** 또는 **Client-Mode (클라이언트 모드)**을 선택합니다. • **Certificate (인증서)** 인증서를 선택합니다. • **User Name (사용자 이름)** 사용자 이름을 입력합니다 (최대 32자). • **Password (비밀번호)** 암호를 입력합니다(최대 32자). 확인 암호는 두 번 입력해야 합니다.
Pre-Shared Key (사전 공유 키)	통신을 암호화하면 다른 채널을 사용하기 전에 암호화 키가 교환되고 공유됩니다. **Authentication Method (인증 방법)**으로 **Pre-Shared Key (사전 공유 키)**를 선택한 경우 **Pre-Shared Key (사전 공유 키)**를 입력합니다(최대 32자). • **Local/ID Type/ID (로컬/ID 종류/ID)** 발신자의 ID 유형을 선택하고 ID를 입력합니다. 유형으로 **IPv4 Address (IPv4 주소)**, **IPv6 Address (IPv6 주소)**, **FQDN**, **E-mail Address (전자 메일 주소)** 또는 **Certificate (인증서)**를 선택합니다. **Certificate (인증서)**를 선택한 경우 **ID** 필드에 인증서의 일반 이름을 입력합니다. • **Remote/ID Type/ID (원격/ID 종류/ID)** 수신자의 ID 유형을 선택한 다음 ID를 입력합니다. 유형으로 **IPv4 Address (IPv4 주소)**, **IPv6 Address (IPv6 주소)**, **FQDN**, **E-mail Address (전자 메일 주소)** 또는 **Certificate (인증서)**를 선택합니다. **Certificate (인증서)**를 선택한 경우 **ID** 필드에 인증서의 일반 이름을 입력합니다.
Certificate (인증서)	**Authentication Method (인증 방법)**에 **Certificates (인증서)**를 선택한 경우 인증서를 선택합니다. 웹 기반 관리의 보안 구성 화면에서 **Certificate (인증서)** 페이지를 사용하여 만든 인증서만 선택할 수 있습니다.

관련 정보

- 웹 기반 관리를 사용하여 IPsec 템플릿 구성

IPsec 템플릿의 수동 설정

옵션	설명
Template Name (템플릿 이름)	템플릿의 이름을 입력합니다 (최대 16자).
Use Prefixed Template (접두어 템플릿 사용)	**Custom (사용자 지정)**를 선택합니다.
Internet Key Exchange (IKE) (IKE(Internet Key Exchange))	IKE는 IPsec을 사용하여 암호화된 통신을 수행하기 위해 암호화 키를 교환하는 데 사용되는 통신 프로토콜입니다. 해당 시간 동안에만 암호화된 통신을 수행하기 위해 IPsec에 필요한 암호화 알고리즘이 결정되고 암호화 키가 공유됩니다. IKE의 경우 Diffie-Hellman 키 교환 방법을 사용하여 암호화 키를 교환하고 IKE로 제한된 암호화 통신이 수행됩니다. **Manual (수동)**를 선택합니다.
Authentication Key (ESP, AH) (인증 키 (ESP, AH))	In/Out 값을 입력합니다. 이 설정은 **Encapsulating Security (보안 캡슐화)** 섹션에서 **Use Prefixed Template (접두어 템플릿 사용)**에 **Custom (사용자 지정)**이 선택되고, **Internet Key Exchange (IKE) (IKE(Internet Key Exchange))**에 **Manual (수동)**이 선택되고, **Hash (해시)**에 **None (안 함)** 이외의 설정이 선택된 경우에 필요합니다. 설정할 수 있는 문자 수는 **Encapsulating Security (보안 캡슐화)** 섹션에서 **Hash (해시)**에 선택한 설정에 따라 다릅니다. 지정한 인증 키의 길이가 선택한 해시 알고리즘과 다를 경우 오류가 발생합니다. • **MD5**: 128비트(16바이트) • **SHA1**: 160비트(20바이트) • **SHA256**: 256비트(32바이트) • **SHA384**: 384비트(48바이트) • **SHA512**: 512비트(64바이트) 키를 ASCII 코드로 지정하는 경우 문자를 따옴표 (")로 묶으십시오.
Code key (ESP) (코드 키(ESP))	In/Out 값을 입력합니다. 이러한 설정은 **Encapsulating Security (보안 캡슐화)**에서 **Use Prefixed Template (접두어 템플릿 사용)**에 대해 **Custom (사용자 지정)**이 선택되고 **Internet Key Exchange (IKE) (IKE(Internet Key Exchange))**에 대해 **Manual (수동)**이 선택되며 **Protocol (프로토콜)**에 대해 **ESP**가 선택된 경우에 필요합니다. 설정할 수 있는 문자 수는 **Encapsulating Security (보안 캡슐화)** 섹션에서 **Encryption (암호화)**에 선택한 설정에 따라 다릅니다. 지정한 코드 키의 길이가 선택한 암호화 알고리즘과 다를 경우 오류가 발생합니다. • **DES**: 64비트(8바이트) • **3DES**: 192비트(24바이트) • **AES-CBC 128**: 128비트(16바이트) • **AES-CBC 256**: 256비트(32바이트) 키를 ASCII 코드로 지정하는 경우 문자를 따옴표 (")로 묶으십시오.
SPI	이 매개변수는 보안 정보를 식별하는 데 사용됩니다. 일반적으로 호스트에는 몇 가지 유형의 IPsec 통신을 위한 여러 SA(보안 연결)가 있습니다. 따라서 IPsec 패킷을 수신할 때 해당하는 SA를 식별해야 합니다.

옵션	설명
	SA를 식별하는 SPI 매개변수는 AH (인증 헤더) 및 ESP (Encapsulating Security Payload, 보안 페이로드 캡슐화) 헤더에 포함되어 있습니다. 이 설정은 **Use Prefixed Template (접두어 템플릿 사용)**에 **Custom (사용자 지정)**이 선택되고 **Internet Key Exchange (IKE) (IKE(Internet Key Exchange))**에 **Manual (수동)**이 선택된 경우에 필요합니다. In/Out 값을 입력합니다. (3-10자)
Encapsulating Security (보안 캡슐화)	• **Protocol (프로토콜)** **ESP** 또는 **AH**를 선택합니다. - ESP는 IPsec을 사용하여 암호화된 통신을 수행하는 프로토콜입니다. ESP는 페이로드(통신되는 내용)를 암호화하고 추가 정보를 추가합니다. IP 패킷은 헤더 및 헤더 다음의 암호화된 페이로드로 구성됩니다. 암호화된 데이터와 함께 IP 패킷은 암호화 모드 및 암호화 키와 관련된 정보, 인증 데이터 등도 포함합니다. - AH는 발신자를 인증하고 데이터 조작을 금지하는 IPsec 프로토콜의 일부입니다(데이터의 무결성 보장). IP 패킷에서 데이터는 헤더 바로 뒤에 삽입됩니다. 또한 패킷에는 발신자의 위조 및 데이터 조작을 방지하기 위해 통신 내용에서 방정식을 사용하여 계산되는 해시 값, 비밀 키 등이 포함됩니다. ESP와 달리 통신 내용이 암호화되지 않고 일반 텍스트로 데이터를 주고받습니다. • **Encryption (암호화) (AH 옵션에 사용할 수 없음.)** **DES**, **3DES**, **AES-CBC 128** 또는 **AES-CBC 256**를 선택합니다. • **Hash (해시)** **None (안 함)**, **MD5**, **SHA1**, **SHA256**, **SHA384** 또는 **SHA512**를 선택합니다. **Protocol (프로토콜)**에 대해 **ESP**를 선택한 경우에만 **None (안 함)**을 선택할 수 있습니다. • **SA Lifetime (SA 수명)** IKE SA 수명을 지정합니다. 시간(초)과 킬로바이트(KB) 수를 입력합니다. • **Encapsulation Mode (캡슐화 모드)** **Transport (전송)** 또는 **Tunnel (터널)**를 선택합니다. • **Remote Router IP-Address (원격 라우터 IP 주소)** 원격 라우터의 IP 주소(IPv4 또는 IPv6)를 입력합니다. **Tunnel (터널)** 모드가 선택된 경우에만 이 정보를 입력합니다. SA(Security Association)는 통신이 시작되기 전에 보안 통신 채널을 설정하기 위해 암호화 모드 및 암호화 키 등의 정보를 교환하고 공유하는 IPsec 또는 IPv6를 사용하는 암호화된 통신 방법입니다. SA는 설정된 가상 암호화 통신 채널을 가리킬 수도 있습니다. IPsec에 사용되는 SA는 암호화 모드를 설정하며 키를 교환하고 IKE (인터넷 키 교환) 표준 절차에 따라 상호 인증을 실행합니다. 또한 SA는 주기적으로 업데이트됩니다.

관련 정보

- 웹 기반 관리를 사용하여 IPsec 템플릿 구성

사용하는 네트워크를 위한 IEEE 802.1x 인증 사용

IEEE 802.1x 인증이란?

IEEE 802.1x는 unauthorized 네트워크 장치로부터의 액세스를 제한하는 IEEE 표준입니다. Brother 제품은 액세스 포인트나 허브를 통해 RADIUS 서버(인증 서버)에 인증 요청을 전송합니다. RADIUS 서버를 통해 요청이 확인되면 제품이 네트워크에 액세스할 수 있습니다.

관련 정보

- 사용하는 네트워크를 위한 IEEE 802.1x 인증 사용

웹 기반 관리(웹 브라우저)를 사용하여 네트워크용 IEEE 802.1x 인증 구성

- EAP-TLS 인증을 사용하여 제품을 구성하는 경우 구성을 시작하기 전에 CA에서 발행한 클라이언트 인증서를 설치해야 합니다. 클라이언트 인증서에 대해서는 네트워크 관리자에게 문의하십시오. 인증서를 두 개 이상 설치한 경우에는 사용할 인증서 이름을 기록해 두는 것이 좋습니다.
- 서버 인증서를 확인하기 전에 서버 인증서에 서명한 CA에서 발급된 CA 인증서를 가져와야 합니다. 네트워크 관리자 또는 ISP(인터넷 서비스 공급자)에게 문의하여 CA 인증서 가져오기가 필요한지 확인하십시오.

제어판에서 무선 설정 마법사를 사용하여 IEEE 802.1x 인증을 구성할 수도 있습니다(무선 네트워크).

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 "https://machine's IP address"(여기서 "machine's IP address"는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 "**Pwd**"로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.

4. 왼쪽 탐색 표시줄에서 **Network (네트워크)**을 클릭합니다.

왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.

5. 다음 중 하나를 수행합니다.
   - 유선 네트워크의 경우

     Wired (유선) > **Wired 802.1x Authentication (유선 802.1x 인증)**를 클릭합니다.
   - 무선 네트워크의 경우

     Wireless (무선) > **Wireless (Enterprise) (무선(기업))**를 클릭합니다.
6. IEEE 802.1x 인증 설정을 구성합니다.

- 유선 네트워크에 IEEE 802.1x 인증을 실행하려면 **Enabled (설정)**페이지의 **Wired 802.1x status (유선 802.1x 상태)**에서 **Wired 802.1x Authentication (유선 802.1x 인증)**를 선택합니다.
- EAP-TLS 인증을 사용하는 경우 **Client Certificate (클라이언트 인증서)** 드롭다운 목록에서 확인을 위해 설치된 클라이언트 인증서(인증서 이름으로 표시)를 선택해야 합니다.
- EAP-FAST, PEAP, EAP-TTLS 또는 EAP-TLS 인증을 선택한 경우 **Server Certificate Verification (서버 인증서 확인)** 드롭다운 목록에서 확인 방법을 선택할 수 있습니다. 서버 인증서를 서명한 CA에서 발행하고 미리 제품으로 가져온 CA 인증서를 사용하여 서버 인증서를 검증합니다.

Server Certificate Verification (서버 인증서 확인) 드롭다운 목록에서 다음과 같은 확인 방법 중 하나를 선택합니다.

옵션	설명
No Verification (확인 안 함)	서버 인증서를 항상 신뢰할 수 있습니다. 확인을 수행하지 않습니다.
CA Cert. (CA 인증서)	서버 인증서를 서명한 CA에서 발행한 CA 인증서를 사용하여 서버 인증서의 CA 신뢰도를 확인하는 확인 방법입니다.

옵션	설명
CA Cert. + ServerID (CA 인증서 + 서버 ID)	공통 이름을 확인하는 인증 방법[1] 값을 확인하는 검증 방법.

7. 구성을 마쳤으면 **Submit (전송)**를 클릭합니다.
   유선 네트워크의 경우: 구성한 다음 제품을 IEEE 802.1x 지원 네트워크에 연결합니다. 몇 분 후에 네트워크 구성 보고서를 인쇄하여 **<Wired IEEE 802.1x>** 상태를 확인합니다.

옵션	설명
Success	유선 IEEE 802.1x 기능이 설정되고 성공적으로 인증되었습니다.
Failed	유선 IEEE 802.1x 기능은 설정되었지만 인증은 실패했습니다.
Off	유선 IEEE 802.1x 기능을 사용할 수 없습니다.

관련 정보

- 사용하는 네트워크를 위한 IEEE 802.1x 인증 사용

관련 내용:

- 보안 인증서 기능 개요
- 장치 보안을 위한 인증서 구성

[1] 공통 이름 확인은 서버 인증서의 공통 이름을 **Server ID (서버 ID)**에 대해 구성된 문자열과 비교합니다. 이 방법을 사용하기 전에 서버 인증서의 공통 이름에 대해 시스템 관리자에게 문의한 다음 **Server ID (서버 ID)**를 구성합니다.

IEEE 802.1x 인증 방법

EAP-FAST

EAP-FAST(Extensible Authentication Protocol-Flexible Authentication via Secured Tunneling)는 Cisco Systems, Inc.에서 개발되었으며, 인증에 사용자 ID와 암호를 사용하고 대칭 키 알고리즘을 사용하여 tunneled 인증 프로세스를 구성합니다.

Brother 제품이 지원하는 내부 인증 방법은 다음과 같습니다.

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

EAP-MD5 (유선 네트워크)

EAP-MD5(Extensible Authentication Protocol-Message Digest Algorithm 5)는 시도-응답 인증에 사용자 ID 및 암호를 사용합니다.

PEAP

PEAP(Protected Extensible Authentication Protocol)는 Cisco Systems, Inc., Microsoft Corporation 및 RSA Security에서 개발한 EAP 방식 버전입니다. PEAP는 사용자 ID 및 암호를 전송하기 위해 클라이언트와 인증 서버 간에 암호화된 SSL(Secure Sockets Layer)/TLS(Transport Layer Security) 터널을 생성합니다. PEAP는 서버와 클라이언트 사이의 상호 인증을 제공합니다.

Brother 제품이 지원하는 내부 인증 방법은 다음과 같습니다.

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

EAP-TTLS(Extensible Authentication Protocol-Tunneled Transport Layer Security)는 Funk Software 및 Certicom에서 개발되었습니다. EAP-TTLS는 사용자 ID 및 암호를 전송하기 위해 클라이언트와 인증 서버 간에 PEAP와 유사한 암호화된 SSL 터널을 생성합니다. EAP-TTLS는 서버와 클라이언트 간의 상호 인증을 제공합니다.

Brother 제품이 지원하는 내부 인증 방법은 다음과 같습니다.

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

EAP-TLS

EAP-TLS(Extensible Authentication Protocol-Transport Layer Security)는 클라이언트와 인증 서버에서 디지털 인증서 인증이 필요합니다.

관련 정보

- 사용하는 네트워크를 위한 IEEE 802.1x 인증 사용

사용자 인증

- Active Directory 인증 사용
- LDAP 인증 사용
- Secure Function Lock 3.0 사용

Active Directory 인증 사용

Active Directory 인증 소개

Active Directory 인증은 제품의 사용을 제한합니다. Active Directory 인증이 활성화된 경우 제품의 제어판이 잠깁니다.사용자 ID 및 암호를 입력하기 전까지 제품의 설정을 변경할 수 없습니다.

Active Directory 인증은 다음 기능을 제공합니다.

사용하는 모델에 따라 지원되는 기능, 옵션 및 설정이 다를 수 있습니다.

- 수신한 팩스 데이터 저장
- 수신한 팩스 데이터 저장
- 스캔한 데이터를 이메일 서버로 전송할 경우 사용자 ID를 기준으로 Active Directory 서버에서 이메일 주소를 획득합니다.

  이 기능을 사용하려면 **Get Mail Address (메일 주소 가져오기)** 설정에 대해 **On (설정)** 옵션을 선택하고 **LDAP + kerberos** 또는 **LDAP + NTLMv2** 인증 방법을 선택합니다. 스캔한 데이터를 제품이 이메일 서버로 전송하는 경우 전송자로 이메일 주소가 설정되거나, 스캔한 데이터를 이메일 주소로 전송하려는 경우 수신자로 이메일 주소가 설정됩니다.

Active Directory 인증이 활성화된 경우 제품이 수신하는 모든 팩스 데이터를 저장합니다. 로그온하면 제품이 저장된 팩스 데이터를 인쇄합니다.

웹 기반 관리를 사용하여 Active Directory 인증 설정을 변경할 수 있습니다.

관련 정보

- Active Directory 인증 사용

웹 기반 관리를 사용하여 Active Directory 인증 구성

Active Directory 인증은 Kerberos 인증 및 NTLMv2 인증을 지원합니다. 인증용 SNTP 프로토콜(네트워크 시간 서버) 및 DNS 서버를 구성해야 합니다.

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 “https://machine’s IP address”(여기서 “machine’s IP address”는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

   본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 “**Pwd**”로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.
4. 왼쪽 탐색 표시줄에서 **Administrator (관리자)** > **User Restriction Function (사용자 제한 기능)** 또는 **Restriction Management (제한 관리)**을 클릭합니다.

   왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.
5. **Active Directory Authentication (Active Directory 인증)**을 선택합니다.
6. **Submit (전송)**을 클릭합니다.
7. **Active Directory Authentication (Active Directory 인증)**을 클릭합니다.
8. 다음 설정을 구성합니다.

   사용하는 모델에 따라 지원되는 기능, 옵션 및 설정이 다를 수 있습니다.

옵션	설명
Storage Fax RX Data (저장 후 데이터를 팩스로 전송)	수신하는 팩스 데이터를 저장하려면 이 옵션을 사용합니다. 제품에 로그인한 후에 수신하는 모든 팩스 데이터를 인쇄할 수 있습니다.
Remember User ID (사용자 ID 기억)	사용자 ID를 저장하려면 이 옵션을 선택합니다.
Active Directory Server Address (Active Directory 서버 주소)	Active Directory 서버의 IP 주소 또는 서버 이름(예: ad.example.com)을 입력합니다.
Active Directory Domain Name (Active Directory 도메인 이름)	Active Directory 도메인 이름을 입력합니다.
Protocol & Authentication Method (프로토콜 및 인증 방법)	프로토콜 및 인증 방법을 선택합니다.
SSL/TLS	**SSL/TLS** 옵션을 선택합니다.
LDAP Server Port (LDAP 서버 포트)	포트 번호를 입력하여 LDAP을 통해 Active Directory 서버를 연결합니다(**LDAP + kerberos** 또는 **LDAP + NTLMv2** 인증 방법에서만 사용 가능).
LDAP Search Root (LDAP 검색 루트)	LDAP 검색 루트를 입력합니다(**LDAP + kerberos** 또는 **LDAP + NTLMv2** 인증 방법에서만 사용 가능).

옵션	설명
Get Mail Address (메일 주소 가져오기)	로그인된 사용자의 이메일 주소를 Active Directory 서버에서 획득하려면 이 옵션을 선택합니다. (LDAP + kerberos 또는 LDAP + NTLMv2 인증 방법에서만 사용 가능)
Get User's Home Directory (사용자 홈 디렉터리 가져오기)	네트워크로 스캔 대상으로 홈 디렉토리를 획득하려면 이 옵션을 선택합니다. (LDAP + kerberos 또는 LDAP + NTLMv2 인증 방법에서만 사용 가능)

9. Submit (전송)을 클릭합니다.

관련 정보

- Active Directory 인증 사용

제품의 제어판에서 로그온하여 제품 설정 변경(Active Directory 인증)

Active Directory 인증이 실행된 경우 제품의 제어판에서 사용자 ID 및 암호를 입력하기 전까지 제품의 제어판이 잠깁니다.

1. 로그인하려면 제품의 제어판에서 사용자 ID 및 암호를 입력합니다.
2. 인증이 성공하면 제품의 제어판 잠금이 풀립니다.

관련 정보

- Active Directory 인증 사용

LDAP 인증 사용

- LDAP 인증 소개
- 웹 기반 관리를 사용하여 LDAP 인증 구성
- 제품의 제어판에서 로그온하여 제품 설정 변경(LDAP 인증)

LDAP 인증 소개

LDAP 인증은 제품의 사용을 제한합니다. LDAP 인증이 실행된 경우 제품의 제어판이 잠깁니다.사용자 ID 및 암호를 입력하기 전까지 제품의 설정을 변경할 수 없습니다.

LDAP 인증은 다음과 같은 기능을 제공합니다.

사용하는 모델에 따라 지원되는 기능, 옵션 및 설정이 다를 수 있습니다.

- 수신한 팩스 데이터 저장
- 수신한 팩스 데이터 저장
- 스캔한 데이터를 이메일 서버로 전송하는 경우 사용자 ID를 기준으로 LDAP 서버의 이메일 주소를 획득합니다.

  이 기능을 사용하려면 **Get Mail Address (메일 주소 가져오기)** 설정에 **On (설정)** 옵션을 선택합니다. 스캔한 데이터를 제품이 이메일 서버로 전송하는 경우 전송자로 이메일 주소가 설정되거나, 스캔한 데이터를 이메일 주소로 전송하려는 경우 수신자로 이메일 주소가 설정됩니다.

LDAP 인증이 활성화된 경우 제품이 수신하는 모든 팩스 데이터를 저장합니다. 로그온하면 제품이 저장된 팩스 데이터를 인쇄합니다.

웹 기반 관리를 사용하여 LDAP 인증 설정을 변경할 수 있습니다.

관련 정보

- LDAP 인증 사용

웹 기반 관리를 사용하여 LDAP 인증 구성

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 “https://machine’s IP address”(여기서 “machine’s IP address”는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

   본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 “**Pwd**”로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.
4. 왼쪽 탐색 표시줄에서 **Administrator (관리자)** > **User Restriction Function (사용자 제한 기능)** 또는 **Restriction Management (제한 관리)**을 클릭합니다.

   왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.
5. **LDAP Authentication (LDAP 인증)**을 선택합니다.
6. **Submit (전송)**을 클릭합니다.
7. **LDAP Authentication (LDAP 인증)** 메뉴를 클릭합니다.
8. 다음 설정을 구성합니다.

   사용하는 모델에 따라 지원되는 기능, 옵션 및 설정이 다를 수 있습니다.

옵션	설명
Storage Fax RX Data (저장 후 데이터를 팩스로 전송)	수신하는 팩스 데이터를 저장하려면 이 옵션을 사용합니다. 제품에 로그인한 후에 수신하는 모든 팩스 데이터를 인쇄할 수 있습니다.
Remember User ID (사용자 ID 기억)	사용자 ID를 저장하려면 이 옵션을 선택합니다.
LDAP Server Address (LDAP 서버 주소)	IP 주소 또는 LDAP 서버의 서버 이름(예: ldap.example.com)을 입력합니다.
SSL/TLS	SSL/TLS를 통해 LDAP를 사용하려면 **SSL/TLS** 옵션을 선택합니다.
LDAP Server Port (LDAP 서버 포트)	LDAP 서버 포트 번호를 입력합니다.
LDAP Search Root (LDAP 검색 루트)	LDAP 검색 루트 디렉토리를 입력합니다.
Attribute of Name (Search Key) (이름 특성 (검색 키))	검색 키로 사용하려는 속성을 입력합니다.
Get Mail Address (메일 주소 가져오기)	로그인된 사용자의 이메일 주소를 LDAP 서버에서 획득하려면 이 옵션을 선택합니다.
Get User's Home Directory (사용자 홈 디렉터리 가져오기)	네트워크로 스캔 대상으로 홈 디렉토리를 획득하려면 이 옵션을 선택합니다.

9. **Submit (전송)**을 클릭합니다.

관련 정보

- LDAP 인증 사용

제품의 제어판에서 로그온하여 제품 설정 변경(LDAP 인증)

LDAP 인증이 실행된 경우 제품의 제어판에서 사용자 ID 및 암호를 입력하기 전까지 제품의 제어판이 잠깁니다.

1. 로그인하려면 제품의 제어판에서 사용자 ID 및 암호를 입력합니다.
2. 인증이 성공하면 제품의 제어판 잠금이 풀립니다.

관련 정보

- LDAP 인증 사용

Secure Function Lock 3.0 사용

Secure Function Lock 3.0은 제품에서 사용할 수 있는 기능을 제한하여 보안을 강화합니다.

Secure Function Lock 3.0을 사용하기 전에

Secure Function Lock을 사용하여 암호를 구성하고 특정 사용자 페이지 한도를 설정하고 여기에 나열된 기능 중 일부 또는 모두에 대한 액세스 권한을 부여할 수 있습니다.

웹 기반 관리를 사용하여 다음과 같은 Secure Function Lock 3.0 설정을 구성하고 변경할 수 있습니다.

사용하는 모델에 따라 지원되는 기능, 옵션 및 설정이 다를 수 있습니다.

- Print (인쇄)
- Copy (복사)
- Scan (스캔)
- 팩스
- 미디어
- Web Connect (웹 연결)
- Apps (앱)
- Page Limits (페이지 제한)
- Page Counters (페이지 카운터)
- Card ID (NFC ID) (카드ID(NFC ID))

터치스크린 LCD 모델:

Secure Function Lock이 실행되면 제품은 일반 사용자 모드로 자동 전환되고 제품의 일부 기능은 authorized 사용자로만 제한됩니다. 제한된 제품 기능에 액세스하려면 을 누르고 사용자 이름을 선택한 다음 암호를 입력합니다.

관련 정보

- Secure Function Lock 3.0 사용

웹 기반 관리를 사용하여 Secure Function Lock 3.0 구성

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 “https://machine’s IP address”(여기서 “machine’s IP address”는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

> 본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 “**Pwd**”로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.

4. 왼쪽 탐색 표시줄에서 **Administrator (관리자)** > **User Restriction Function (사용자 제한 기능)** 또는 **Restriction Management (제한 관리)**을 클릭합니다.

> 왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.

5. **Secure Function Lock (보안 기능 잠금)**을 선택합니다.
6. **Submit (전송)**을 클릭합니다.
7. **Restricted Functions (제한 기능)** 메뉴를 클릭합니다.
8. 사용자당 또는 그룹당 제한을 관리하려면 설정을 구성합니다.
9. **Submit (전송)**을 클릭합니다.
10. **User List (사용자 목록)** 메뉴를 클릭합니다.
11. 사용자 목록을 구성합니다.
12. **Submit (전송)**을 클릭합니다.

> **Secure Function Lock (보안 기능 잠금)** 메뉴에서 사용자 목록 잠금 설정을 변경할 수도 있습니다.

관련 정보

- Secure Function Lock 3.0 사용

Secure Function Lock 3.0을 사용하여 스캔

사용하는 모델에 따라 지원되는 기능, 옵션 및 설정이 다를 수 있습니다.

스캔 제한 설정(관리자의 경우)

Secure Function Lock 3.0을 통해 관리자는 스캔할 수 있는 사용자를 제한할 수 있습니다. 공용 사용자 설정에 대해 스캔 기능이 해제된 경우 **Scan (스캔)** 확인란이 선택된 사용자만 스캔할 수 있습니다.

스캔 기능 사용(제한된 사용자의 경우)

- 제품의 제어판을 사용하여 스캔하려면:

  제한된 사용자는 제품의 제어판에 암호를 입력해야 스캔 모드에 액세스할 수 있습니다.
- 컴퓨터에서 스캔하려면:

  제한된 사용자는 컴퓨터에서 스캔하기 전에 제품의 제어판에 암호를 입력해야 합니다. 제품의 제어판에 암호를 입력하지 않으면 사용자의 컴퓨터에 오류 메시지가 나타납니다.

제품에서 IC 카드 인증을 지원하는 경우 제한된 사용자는 등록된 IC 카드로 제품의 제어판에 있는 NFC 로고를 터치하여 스캔 모드에 액세스할 수도 있습니다.

관련 정보

- Secure Function Lock 3.0 사용

Secure Function Lock 3.0의 일반 사용자 모드 구성

Secure Function Lock 화면을 사용하여 일반 사용자에게 제공되는 기능을 제한하는 일반 사용자 모드를 설정합니다. 공용 사용자는 암호를 입력하지 않고도 일반 사용자 모드 설정을 통해 제공되는 기능에 액세스할 수 있습니다.

일반 사용자 모드에는 Brother iPrint&Scan 및 Brother Mobile Connect를 통해 전송된 인쇄 작업이 포함되어 있습니다.

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 “https://machine’s IP address”(여기서 “machine’s IP address”는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 “**Pwd**”로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.

4. 왼쪽 탐색 표시줄에서 **Administrator (관리자)** > **User Restriction Function (사용자 제한 기능)** 또는 **Restriction Management (제한 관리)**을 클릭합니다.

왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.

5. **Secure Function Lock (보안 기능 잠금)**을 선택합니다.
6. **Submit (전송)**을 클릭합니다.
7. **Restricted Functions (제한 기능)** 메뉴를 클릭합니다.
8. **Public Mode (공용 모드)** 행에서 나열된 기능을 허용하려면 확인란을 선택하고 제한하려면 확인란의 선택을 취소합니다.
9. **Submit (전송)**을 클릭합니다.

관련 정보

- Secure Function Lock 3.0 사용

웹 기반 관리를 사용하여 개인 홈 화면 설정 구성

관리자 권한으로 실행하여 사용자가 개인 홈 화면에서 볼 수 있는 탭을 지정할 수 있습니다. 이러한 탭을 통해 사용자가 favorite 바로 가기에 빠르게 액세스할 수 있으며, 제품의 제어판에서 개인 홈 화면 탭에 바로 가기를 할당할 수 있습니다.

사용하는 모델에 따라 지원되는 기능, 옵션 및 설정이 다를 수 있습니다.

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 “https://machine’s IP address”(여기서 “machine’s IP address”는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 “**Pwd**”로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.

4. 왼쪽 탐색 표시줄에서 **Administrator (관리자)** > **User Restriction Function (사용자 제한 기능)** 또는 **Restriction Management (제한 관리)**을 클릭합니다.

왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.

5. **Secure Function Lock (보안 기능 잠금)**을 선택합니다.
6. **Tab Settings (탭 설정)** 필드에서 개인 홈 화면으로 사용하려는 탭 이름으로 **Personal (개인용)**을 선택합니다.
7. **Submit (전송)**을 클릭합니다.
8. **Restricted Functions (제한 기능)** 메뉴를 클릭합니다.
9. 사용자당 또는 그룹 제한을 관리하려면 설정을 구성합니다.
10. **Submit (전송)**을 클릭합니다.
11. **User List (사용자 목록)** 메뉴를 클릭합니다.
12. 사용자 목록을 구성합니다.
13. 각 사용자에 대해 드롭다운 목록에서 **User List / Restricted Functions (사용자 목록/제한 기능)**을 선택합니다.
14. 각 사용자의 **Home Screen (홈 화면)** 드롭다운 목록에서 탭 이름을 선택합니다.
15. **Submit (전송)**을 클릭합니다.

관련 정보

- Secure Function Lock 3.0 사용

추가 Secure Function Lock 3.0 기능

Secure Function Lock 화면에서 다음 기능을 구성합니다.

사용하는 모델에 따라 지원되는 기능, 옵션 및 설정이 다를 수 있습니다.

All Counter Reset (모든 카운터 초기화)

열에서 **All Counter Reset (모든 카운터 초기화)**을 클릭하여 페이지 카운터를 재설정합니다.**Page Counters (페이지 카운터)**

Export to CSV file (CSV 파일로 내보내기)

Export to CSV file (CSV 파일로 내보내기)을 클릭하여 **User List / Restricted Functions (사용자 목록/제한 기능)** 정보를 포함한 현재 및 마지막 페이지 카운터를 CSV 파일로 내보냅니다.

Card ID (NFC ID) (카드ID(NFC ID))

User List (사용자 목록) 메뉴를 클릭한 다음 **Card ID (NFC ID) (카드ID(NFC ID))** 필드에 사용자의 카드 ID를 입력합니다. 인증을 위해 IC 카드를 사용할 수 있습니다.

Output (출력)

메일 상자 유니트가 제품에 설치된 경우 드롭다운 목록에서 각 사용자에 대한 배지용지함을 선택하십시오.

Last Counter Record (마지막 카운터 기록)

카운터가 재설정된 후 페이지 수를 제품에 저장하려면 **Last Counter Record (마지막 카운터 기록)**를 클릭합니다.

Counter Auto Reset (카운터 자동 초기화)

Counter Auto Reset (카운터 자동 초기화)를 클릭하여 페이지 카운터 재설정 사이의 시간 간격을 구성합니다. 일별, 주별 또는 월별 간격을 선택합니다.

관련 정보

- Secure Function Lock 3.0 사용

제품의 제어판을 사용하여 새 IC 카드 등록

사용하는 제품에 집적회로카드(IC 카드)를 등록할 수 있습니다.

사용하는 모델에 따라 지원되는 기능, 옵션 및 설정이 다를 수 있습니다.

1. 등록된 집적 회로 카드(IC 카드)를 사용하여 제품의 제어판에 있는 NFC(Near-Field Communication) 기호를 터치합니다.
2. LCD의 사용자 ID를 누릅니다.
3. 등록 카드 버튼을 누릅니다.
4. 새 IC 카드를 NFC 로고에 터치합니다.
   새 IC 카드의 번호가 제품에 등록됩니다.
5. OK 버튼을 누릅니다.

관련 정보

- Secure Function Lock 3.0 사용

외부 IC 카드 리더 등록

외부 IC(집적 회로) 카드 리더를 연결하면 웹 기반 관리를 사용하여 카드 리더를 등록합니다. 본 제품은 HID 클래스 드라이버 지원 외부 IC 카드 리더를 지원합니다.

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 “https://machine’s IP address”(여기서 “machine’s IP address”는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

   본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 “**Pwd**”로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.
4. 왼쪽 탐색 표시줄에서 **Administrator (관리자)** > **External Card Reader (외부 카드 판독기)**를 클릭합니다.

   왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.
5. 필요한 정보를 입력한 다음 **Submit (전송)**을 클릭합니다.
6. 구입하신 Brother 제품을 다시 시작하여 구성을 활성화합니다.
7. 카드 리더를 제품에 연결합니다.
8. 카드 인증을 사용할 경우 카드를 카드 리더에 터치합니다.

관련 정보

- Secure Function Lock 3.0 사용

이메일을 안전하게 송신 또는 수신

웹 기반 관리를 사용하여 이메일 송수신 구성

- 일부 모델에서만 이메일을 수신할 수 있습니다.
- 웹 기반 관리를 사용하여 사용자 인증으로 보안 이메일 송신을 구성하거나 SSL/TLS를 사용하여 이메일 송수신을 구성(지원되는 모델만 해당)하는 것이 좋습니다.

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 “https://machine’s IP address”(여기서 “machine’s IP address”는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

   본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 “**Pwd**”로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.
4. 왼쪽 탐색 표시줄에서 **Network (네트워크)** > **Network (네트워크)** > **Protocol (프로토콜)**을 클릭합니다.

   왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.
5. 필드에서 **Advanced Settings (고급 설정)**을 클릭하고 **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP 클라이언트)**의 상태가 **Enabled (활성화)**인지 확인합니다.**POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP 클라이언트)**

   - 제품에 따라 사용할 수 있는 프로토콜이 다를 수 있습니다.
   - **Authentication Method (인증 방법)** 선택 화면이 나타나면 인증 방법을 선택한 다음 화면 지침을 따릅니다.
6. **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP 클라이언트)** 설정을 구성합니다.
   - 구성 후 테스트 이메일을 송신하여 이메일 설정이 올바른지 확인할 수 있습니다.
   - POP3/IMAP4/SMTP 서버 설정을 모를 경우 네트워크 관리자나 ISP(인터넷 서비스 공급자)에게 문의하십시오.
7. 완료되면 **Submit (전송)**을 클릭합니다.

   Test Send/Receive E-mail Configuration (전자 메일 전송/수신 구성 테스트) 대화 상자가 나타납니다.
8. 대화 상자의 안내에 따라 현재 설정을 테스트합니다.

관련 정보

- 이메일을 안전하게 송신 또는 수신

관련 내용:

- SSL/TLS를 사용하여 안전하게 이메일 송수신

사용자 인증을 통해 이메일 송신

제품은 사용자 인증이 필요한 이메일 서버를 통해 이메일을 전송합니다. 이 방법은 unauthorized 사용자가 이메일 서버에 액세스하지 못하게 합니다.

사용자 인증을 사용해서 이메일 알림, 이메일 보고서 및 I-Fax(일부 모델에서만 사용 가능)를 송신할 수 있습니다.

- 제품에 따라 사용할 수 있는 프로토콜이 다를 수 있습니다.
- 웹 기반 관리를 사용하여 SMTP 인증을 구성하는 것이 좋습니다.

이메일 서버 설정

이메일 서버에서 사용된 방법과 일치하도록 구입하신 제품의 SMTP 인증 방법을 구성해야 합니다. 이메일 서버 설정에 대한 자세한 내용은 네트워크 관리자나 ISP(인터넷 서비스 공급자)에게 문의하십시오.

웹 기반 관리를 사용하여 SMTP 서버 인증을 사용 설정하려면 **POP3/IMAP4/SMTP Client (POP3/IMAP4/SMTP 클라이언트)** 화면의 **Server Authentication Method (서버 인증 방법)**에서 인증 방법을 선택합니다.

관련 정보

- 이메일을 안전하게 송신 또는 수신

SSL/TLS를 사용하여 안전하게 이메일 송수신

구입하신 제품은 SSL/TLS 통신 방법을 지원합니다. SSL/TLS 통신을 사용하는 이메일 서버를 사용하려면 다음 설정을 구성해야 합니다.

- 일부 모델에서만 이메일을 수신할 수 있습니다.
- 웹 기반 관리를 사용하여 SSL/TLS를 구성하는 것이 좋습니다.

서버 인증서 확인

SSL/TLS에서 SSL 또는 TLS를 선택하는 경우 **Verify Server Certificate (서버 인증서 확인)** 확인란이 자동으로 선택됩니다.

- 서버 인증서를 확인하기 전에 서버 인증서에 서명한 CA에서 발급된 CA 인증서를 가져와야 합니다. 네트워크 관리자 또는 ISP(인터넷 서비스 공급자)에게 문의하여 CA 인증서 가져오기가 필요한지 확인하십시오.
- 서버 인증서를 확인할 필요가 없으면 **Verify Server Certificate (서버 인증서 확인)** 확인란의 선택을 취소하십시오.

포트 번호

SSL 또는 TLS를 선택하면 **Port (포트)** 값이 프로토콜과 일치하도록 변경됩니다. 포트 번호를 수동으로 변경하려면 SSL/TLS 설정을 선택한 후 포트 번호를 입력하십시오.

이메일 서버에서 사용된 방법과 일치하도록 구입하신 제품의 통신 방법을 구성해야 합니다. 이메일 서버 설정에 대한 자세한 내용은 네트워크 관리자나 ISP에게 문의하십시오.

대부분의 경우 안전하게 웹메일 서비스를 하려면 다음과 같은 설정이 필요합니다.

사용하는 모델에 따라 지원되는 기능, 옵션 및 설정이 다를 수 있습니다.

SMTP	**Port (포트)**	587
	Server Authentication Method (서버 인증 방법)	**SMTP-AUTH (SMTP 인증)**
	SSL/TLS	TLS
POP3	**Port (포트)**	995
	SSL/TLS	SSL
IMAP4	**Port (포트)**	993
	SSL/TLS	SSL

관련 정보

- 이메일을 안전하게 송신 또는 수신

관련 내용:

- 웹 기반 관리를 사용하여 이메일 송수신 구성
- 장치 보안을 위한 인증서 구성

네트워크에 인쇄 로그 저장

네트워크에 인쇄 로그 저장 개요

네트워크에 인쇄 로그 저장 기능을 사용하면 CIFS(일반 인터넷 파일 시스템) 프로토콜을 사용하여 제품의 인쇄 로그 파일을 네트워크 서버에 저장할 수 있습니다. 모든 인쇄 작업에 대한 ID, 인쇄 작업 유형, 작업 이름, 사용자 이름, 날짜, 시간, 인쇄된 페이지 수를 기록할 수 있습니다. CIFS는 TCP/IP에서 실행되는 프로토콜로 네트워크 상의 컴퓨터가 인트라넷 또는 인터넷을 통해 파일을 공유할 수 있도록 합니다.

다음과 같은 인쇄 기능이 인쇄 로그에 기록됩니다.

사용하는 모델에 따라 지원되는 기능, 옵션 및 설정이 다를 수 있습니다.

- 컴퓨터의 인쇄 작업
- USB 다이렉트 인쇄
- 복사
- 수신 팩스
- Web Connect 인쇄

- 네트워크에 인쇄 로그 저장 기능은 Kerberos 인증 및 NTLMv2 인증을 지원합니다. SNTP 프로토콜(네트워크 시간 서버)을 구성하거나 제어판에서 인증에 대한 날짜, 시간 및 시간대를 정확히 설정해야 합니다.
- 파일을 서버에 저장할 때 파일 유형을 TXT 또는 CSV로 설정할 수 있습니다.

관련 정보

- 네트워크에 인쇄 로그 저장

웹 기반 관리를 사용하여 네트워크 설정에 인쇄 로그 저장 구성

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 “https://machine’s IP address”(여기서 “machine’s IP address”는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 “**Pwd**”로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.

4. 왼쪽 탐색 표시줄에서 **Administrator (관리자)** > **Store Print Log to Network (네트워크에 인쇄 로그 저장)**을 클릭합니다.

왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.

5. **Print Log (인쇄 로그)**필드에서 **On (설정)**을 클릭합니다.
6. 다음 설정을 구성합니다.

사용하는 모델에 따라 지원되는 기능, 옵션 및 설정이 다를 수 있습니다.

옵션	설명
Network Folder Path (네트워크 폴더 경로)	CIFS 서버에서 인쇄 로그를 저장할 대상 폴더를 입력합니다(예: ₩₩ComputerName₩SharedFolder).
File Name (파일 이름)	인쇄 로그에 사용하려는 파일 이름을 입력합니다(최대 32자).
File Type (파일 유형)	인쇄 로그 파일 유형에 대해 **TXT** 또는 **CSV** 옵션을 선택합니다.
Time Source for Log (로그 기준 시간)	인쇄 로그에 대한 시간 소스를 선택합니다.
Auth. Method (인증 방법)	CIFS 서버에 액세스하는 데 필요한 인증 방법, 즉 **Auto (자동)**, **Kerberos** 또는 **NTLMv2**를 선택합니다. Kerberos는 단일 로그인을 사용하여 장치 또는 개인이 네트워크 서버에 자신의 ID를 안전하게 입증할 수 있도록 하는 인증 프로토콜입니다. NTLMv2는 Windows에서 서버에 로그인하는 데 사용되는 인증 방법입니다. • **Auto (자동)**: **Auto (자동)**를 선택하는 경우, NTLMv2가 인증 방법에 사용됩니다. • **Kerberos**: Kerberos 인증만 사용하려면 **Kerberos** 옵션을 선택합니다. • **NTLMv2**: NTLMv2 인증만 사용하려면 **NTLMv2** 옵션을 선택합니다. • 및 **Kerberos** 인증의 경우 **NTLMv2** 설정 또는 SNTP 프로토콜(네트워크 시간 서버) 및 DNS 서버도 구성해야 합니다.**Date&Time (날짜/시간)** • 제품의 제어판에서 날짜 & 시간 설정을 구성할 수도 있습니다.
Username (사용자 이름)	인증용 사용자 이름을 입력합니다(최대 96자). 사용자 이름이 도메인의 일부인 경우 user@domain 또는 domain₩user 스타일 중 하나로 사용자 이름을 입력합니다.

옵션	설명
Password (비밀번호)	인증용 암호를 입력합니다(최대 32자).
Kerberos Server Address (Kerberos 서버 주소)(필요한 경우)	KDC(Key Distribution Center) 호스트 주소(예: kerberos.example.com, 최대 64자) 또는 IP 주소(예: 192.168.56.189)를 입력합니다.
Error Detection Setting (오류 감지 설정)	네트워크 오류로 인해 인쇄 로그를 서버에 저장할 수 없는 경우에 취할 조치를 선택합니다.

7. Connection Status (연결 상태) 필드에서 마지막 로그 상태를 확인할 수 있습니다.

제품의 LCD에서 오류 상태를 확인할 수도 있습니다.

8. Submit (전송)를 클릭하여 Test Print Log to Network (네트워크에 인쇄 로그 저장 테스트) 페이지를 표시합니다.

   설정을 테스트하려면 Yes (예)를 클릭해도 다음 단계로 이동합니다.

   테스트를 생략하려면 No (아니요)를 클릭합니다. 설정이 자동으로 전송됩니다.

9. 제품이 설정을 테스트합니다.
10. 설정이 승인되면 화면에 Test OK (테스트 성공)가 나타납니다.

    Test Error (테스트 오류)가 나타나면 모든 설정을 확인한 다음 Submit (전송)를 클릭하여 테스트 페이지를 다시 표시합니다.

관련 정보

- 네트워크에 인쇄 로그 저장

네트워크에 인쇄 로그 저장의 오류 감지 설정 사용

오류 감지 설정을 사용하여 네트워크 오류로 인해 인쇄 로그를 서버에 저장할 수 없는 경우 취할 조치를 결정합니다.

1. 웹 브라우저를 시작합니다.
2. 브라우저의 주소 표시줄에 “https://machine’s IP address”(여기서 “machine’s IP address”는 제품의 IP 주소)를 입력합니다.

   예:

   https://192.168.1.2

   사용하는 제품의 IP 주소는 네트워크 구성 보고서에서 확인할 수 있습니다.
3. 필요한 경우 **Login (로그인)** 필드에 암호를 입력한 다음 **Login (로그인)**을 클릭합니다.

본 제품의 설정을 관리하는 데 필요한 기본 암호는 제품 뒷면 또는 바닥에 있으며 “**Pwd**”로 표시되어 있습니다. 처음 로그인할 때 화면 지침에 따라 기본 암호를 변경하십시오.

4. 왼쪽 탐색 표시줄에서 **Administrator (관리자)** > **Store Print Log to Network (네트워크에 인쇄 로그 저장)**을 클릭합니다.

왼쪽 탐색 표시줄이 보이지 않는 경우 ☰에서 탐색을 시작합니다.

5. **Error Detection Setting (오류 감지 설정)** 섹션에서 **Cancel Print (인쇄 취소)** 또는 **Ignore Log & Print (로그 무시 및 인쇄)** 옵션을 선택합니다.

사용하는 모델에 따라 지원되는 기능, 옵션 및 설정이 다를 수 있습니다.

옵션	설명
Cancel Print (인쇄 취소)	**Cancel Print (인쇄 취소)** 옵션을 선택하면 인쇄 로그를 서버에 저장할 수 없는 경우 인쇄 작업이 canceled됩니다. **Cancel Print (인쇄 취소)** 옵션을 선택한 경우에도 수신된 팩스는 인쇄됩니다.

Ignore Log & Print (로그 무시 및 인쇄)	**Ignore Log & Print (로그 무시 및 인쇄)** 옵션을 선택하면 인쇄 로그를 서버에 저장할 수 없는 경우에도 설명서가 인쇄됩니다.
	인쇄 로그 저장 기능이 복구되면 인쇄 로그는 다음과 같이 기록됩니다.
	`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. 인쇄 종료 시 인쇄 로그를 저장할 수 없으면 인쇄된 페이지 수가 기록되지 않습니다.
	b. 인쇄 시작 및 종료 시 인쇄 로그를 저장할 수 없으면 작업의 인쇄 로그가 기록되지 않습니다. 기능이 복구되면 오류가 인쇄 로그에 반영됩니다.

6. **Submit (전송)**를 클릭하여 **Test Print Log to Network (네트워크에 인쇄 로그 저장 테스트)** 페이지를 표시합니다.

   설정을 테스트하려면 **Yes (예)**를 클릭해도 다음 단계로 이동합니다.

   테스트를 생략하려면 **No (아니요)**를 클릭합니다. 설정이 자동으로 전송됩니다.
7. 제품이 설정을 테스트합니다.
8. 설정이 승인되면 화면에 **Test OK (테스트 성공)**가 나타납니다.

Test Error (테스트 오류)가 나타나면 모든 설정을 확인한 다음 Submit (전송)를 클릭하여 테스트 페이지를 다시 표시합니다.

관련 정보

- 네트워크에 인쇄 로그 저장

Secure Function Lock 3.0으로 네트워크에 인쇄 로그 저장 사용

Secure Function Lock 3.0이 활성화되면 복사, Fax RX, Web Connect 인쇄 및 USB 다이렉트 인쇄에 등록된 사용자의 이름이 네트워크에 인쇄 로그 저장 보고서에 기록됩니다. Active Directory 인증이 실행된 경우 사용자 이름이 네트워크에 인쇄 로그 저장 보고서에 기록됩니다.

사용하는 모델에 따라 지원되는 기능, 옵션 및 설정이 다를 수 있습니다.

```
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
```

관련 정보

- 네트워크에 인쇄 로그 저장

brother

Brother Earth

www.brotherearth.com

KOR
버전 0