

Panduan Administrator

Daftar Isi

Hak Cipta

Merek Dagang

Tentang Panduan ini

Tanda-tanda dan Simbol.	6
Gambaran yang Digunakan dalam Panduan Ini.	6
Rujukan Sistem Operasi.	6

Pendahuluan

Komponen Panduan.	8
Definisi Istilah yang Digunakan dalam Panduan Ini.	8

Persiapan

Alur Pengaturan dan Pengelolaan Scanner.	10
Contoh Lingkungan Jaringan.	11
Pengenalan contoh pengaturan koneksi scanner.	11
Persiapan Koneksi ke Jaringan.	12
Mengumpulkan Informasi tentang Pengaturan Koneksi.	12
Spesifikasi Pemindai.	12
Menggunakan Nomor Port.	13
Jenis Penetapan Alamat IP.	13
Server DNS dan Server Proksi.	13
Metode Pengaturan Koneksi Jaringan.	13

Koneksi

Menyambung ke Jaringan.	15
Menyambung ke Jaringan dari Panel Kontrol.	15
Menyambung ke Jaringan Menggunakan Penginstal.	19

Pengaturan Fungsi

Perangkat Lunak Pengaturan.	22
Web Config (Laman Web untuk Perangkat).	22
Menggunakan Fungsi Pemindaian.	24
Memindai dari Komputer.	24
Memindai dengan panel kontrol.	26
Melakukan Pengaturan Sistem.	28
Melakukan Pengaturan Sistem pada Panel Kontrol.	28

Melakukan Pengaturan Sistem Menggunakan Konfigurasi Web.	30
------------------------------------------------------------------	----

Pengaturan Keamanan Dasar

Pengenalan Fitur-fitur Keamanan Dasar.	32
Mengonfigurasi Kata Sandi Administrator.	33
Mengonfigurasi Kata Sandi Administrator dari Panel Kontrol.	33
Mengonfigurasi Kata Sandi Administrator Menggunakan Web Config.	33
Item yang Dapat Dikunci oleh Kata Sandi Administrator.	34
Mengendalikan protokol.	35
Protokol yang dapat Anda Aktifkan atau Nonaktifkan.	36
Item Pengaturan Protokol.	37

Pengaturan Operasi dan Pengelolaan

Mengonfirmasi Informasi Perangkat.	40
Mengelola Perangkat (Epson Device Admin).	40
Menerima Pemberitahuan Email Saat Aktivitas Terjadi.	41
Tentang Pemberitahuan Email.	41
Mengonfigurasi Pemberitahuan Email.	41
Mengonfigurasi Server Email.	42
Periksa Koneksi Server Email.	44
Memperbarui Firmware.	46
Memperbarui Firmware Menggunakan Web Config.	46
Memperbarui Firmware Menggunakan Epson Firmware Updater.	46
Membuat Cadangan Pengaturan.	47
Ekspor pengaturan.	47
Impor pengaturan.	47

Memecahkan Masalah

Tips untuk Memecahkan Masalah.	49
Memeriksa Log Server dan Perangkat Jaringan.	49
Memulai Pengaturan Jaringan.	49
Memulihkan Pengaturan Jaringan dari Panel Kontrol.	49
Memeriksa Komunikasi antara Perangkat dan Komputer.	49
Memeriksa Koneksi dengan Perintah Ping — Windows.	49

Daftar Isi

Memeriksa Koneksi dengan Perintah Ping — Mac OS.	51	Masalah Menggunakan Fitur Keamanan Jaringan.88
Masalah Menggunakan Perangkat Lunak Jaringan.	52	Masalah Saat Menggunakan Sertifikat Digital.	90
Tidak Dapat Mengakses Web Config.	52		
Nama model dan/atau alamat IP tidak ditampilkan di EpsonNet Config.	53		
Lampiran			
Pengenalan Perangkat Lunak Jaringan.	55		
Epson Device Admin.	55		
EpsonNet Config.	55		
EpsonNet SetupManager.	56		
Menentukan Alamat IP Menggunakan EpsonNet Config.	56		
Menentukan Alamat IP Menggunakan Pengaturan Batch.	56		
Menentukan Alamat IP Setiap Perangkat.	59		
Menggunakan Port Scanner.	60		
Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan			
Pengaturan Keamanan dan Pencegahan Bahaya.	62		
Pengaturan Fitur Keamanan.	63		
Komunikasi SSL/TLS dengan Scanner.	63		
Tentang Sertifikasi Digital.	63		
Mendapatkan dan Mengimpor Sertifikat yang Ditandatangani CA.	64		
Menghapus Sertifikat Bertanda Tangan CA.	68		
Memperbarui Sertifikat Bertanda Tangan Sendiri.	68		
Konfigurasi CA Certificate.	69		
Menkripsi Komunikasi Menggunakan Pemfilteran IPsec/IP.	71		
Tentang IPsec/IP Filtering.	71		
Mengonfigurasi Default Policy.	72		
Mengonfigurasi Group Policy.	75		
Contoh Konfigurasi dari IPsec/IP Filtering.	81		
Mengonfigurasi Sertifikat untuk IPsec/IP Filtering.	82		
Menggunakan Protokol SNMPv3.	82		
Tentang SNMPv3.	82		
Mengonfigurasi SNMPv3.	83		
Menghubungkan Scanner ke Jaringan IEEE802.1X.	84		
Mengonfigurasi Jaringan IEEE802.1X.	84		
Mengonfigurasi Sertifikat untuk IEEE802.1X.	86		
Memecahkan Masalah Keamanan Tingkat Lanjut.	87		
Mengembalikan Pengaturan Keamanan.	87		

Hak Cipta

Tidak ada bagian dari publikasi ini yang dapat direproduksi, disimpan dalam sistem temu balik, atau dikirimkan dalam bentuk apa pun atau dengan cara apa pun, elektronik, mekanis, fotokopi, rekaman, atau lainnya, tanpa izin tertulis dari Seiko Epson Corporation sebelumnya. Tidak ada tanggung jawab paten yang dibebankan atas penggunaan informasi yang tercakup di sini. Tidak pula ada tanggung jawab yang dibebankan untuk kerugian akibat penggunaan informasi di sini. Informasi yang tercakup di sini dirancang khusus untuk penggunaan produk Epson ini. Epson tidak bertanggung jawab atas penggunaan informasi ini sebagaimana berlaku untuk produk lain.

Baik Seiko Epson Corporation maupun afliasinya tidak bertanggung jawab kepada pembeli produk ini atau pihak ketiga atas kerugian non-finansial, kerugian finansial, biaya, atau pengeluaran yang ditimbulkan oleh pembeli atau pihak ketiga karena kecelakaan, penyalahgunaan, atau penggunaan yang tidak benar atas produk ini atau modifikasi, perbaikan, atau perubahan yang tidak sah terhadap produk ini, atau (kecuali untuk AS) kegagalan untuk sepenuhnya mematuhi instruksi pengoperasian dan pemeliharaan dari Seiko Epson Corporation.

Seiko Epson Corporation dan afliasinya tidak bertanggung jawab atas kerugian atau masalah yang timbul dari penggunaan opsi atau produk habis pakai apa pun selain yang ditandai sebagai Produk Epson Asli atau Produk yang Disetujui Epson oleh Seiko Epson Corporation.

Seiko Epson Corporation tidak bertanggung jawab atas kerugian akibat gangguan elektromagnetik yang terjadi dari penggunaan kabel antarmuka selain yang ditandai sebagai Produk yang Disetujui Epson oleh Seiko Epson Corporation.

©Seiko Epson Corporation 2019.

Isi manual ini dan spesifikasi produk ini dapat berubah tanpa pemberitahuan sebelumnya.

Merek Dagang

- ❑ EPSON® adalah merek dagang terdaftar, dan EPSON EXCEED YOUR VISION atau EXCEED YOUR VISION adalah merek dagang Seiko Epson Corporation.
- ❑ Epson Scan 2 software is based in part on the work of the Independent JPEG Group.
- ❑ Google Cloud Print™, Chrome™, Chrome OS™, and Android™ are trademarks of Google Inc.
- ❑ Microsoft®, Windows®, Windows Server®, and Windows Vista® are registered trademarks of Microsoft Corporation.
- ❑ Apple, Macintosh, Mac OS, OS X, AirMac, Bonjour, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint is a trademark of Apple Inc.
- ❑ Pemberitahuan Umum: Nama-nama produk lain yang digunakan di sini hanyalah untuk tujuan identifikasi dan mungkin merupakan merek dagang pemiliknya masing-masing. Epson menafikan setiap dan semua hak atas merek-merek tersebut.

Tentang Panduan ini

Tanda-tanda dan Simbol

**Perhatian:**

Petunjuk yang harus diikuti dengan saksama untuk menghindari cedera tubuh.

**Penting:**

Petunjuk yang harus diikuti untuk menghindari kerusakan pada peralatan Anda.

Catatan:

Petunjuk yang berisi tips yang bermanfaat dan batasan-batasan penggunaan scanner.

Informasi Terkait

➔ Dengan mengklik ikon ini, Anda akan dibawa ke informasi terkait.

Gambaran yang Digunakan dalam Panduan Ini

- Tangkapan layar dari driver scanner dan layar Epson Scan 2 (driver scanner) diambil dari Windows 10 atau OS X El Capitan. Isi yang ditampilkan di layar akan berbeda bergantung pada model dan keadaan.
- Gambar yang digunakan dalam panduan ini hanya untuk contoh. Walaupun mungkin ada sedikit perbedaan model, cara pengoperasiannya sama.
- Beberapa item menu di layar LCD akan berbeda bergantung pada model dan pengaturan.

Rujukan Sistem Operasi

Windows

Dalam buku petunjuk ini, istilah-istilah seperti “Windows 10”, “Windows 8.1”, “Windows 8”, “Windows 7”, “Windows Vista”, “Windows XP”, Windows Server 2016, “Windows Server 2012 R2”, “Windows Server 2012”, “Windows Server 2008 R2”, “Windows Server 2008”, “Windows Server 2003 R2”, dan “Windows Server 2003” mengacu pada sistem operasi berikut. Selain itu, “Windows” digunakan untuk merujuk pada semua versi.

- Sistem operasi Microsoft® Windows® 10
- Sistem operasi Microsoft® Windows® 8.1
- Sistem operasi Microsoft® Windows® 8
- Sistem operasi Microsoft® Windows® 7
- Sistem operasi Microsoft® Windows Vista®
- Sistem operasi Microsoft® Windows® XP
- Sistem operasi Microsoft® Windows® XP Professional x64 Edition

Tentang Panduan ini

- Sistem operasi Microsoft® Windows Server® 2016
- Sistem operasi Microsoft® Windows Server® 2012 R2
- Sistem operasi Microsoft® Windows Server® 2012
- Sistem operasi Microsoft® Windows Server® 2008 R2
- Sistem operasi Microsoft® Windows Server® 2008
- Sistem operasi Microsoft® Windows Server® 2003 R2
- Sistem operasi Microsoft® Windows Server® 2003

Mac OS

Dalam buku petunjuk ini, “Mac OS” digunakan untuk mengacu pada macOS Sierra, OS X El Capitan, OS X Yosemite, OS X Mavericks, OS X Mountain Lion, Mac OS X v10.7.x, dan Mac OS X v10.6.8.

Pendahuluan

Komponen Panduan

Panduan ini adalah untuk administrator perangkat yang bertanggung jawab menghubungkan printer atau scanner ke jaringan, dan berisi informasi cara pengaturan terkait pemakaian fungsi.

Untuk informasi tentang pemakaian fungsi, baca *Panduan Pengguna*.

Persiapan

Menjelaskan tugas-tugas administrator, cara mengatur perangkat, dan perangkat lunak untuk pengelolaan.

Koneksi

Menjelaskan cara menyambung suatu perangkat ke jaringan atau saluran telepon. Di dalamnya juga dijelaskan lingkungan jaringan, seperti penggunaan port perangkat, informasi server DNS, dan server proksi.

Pengaturan Fungsi

Menjelaskan pengaturan setiap fungsi perangkat.

Pengaturan Keamanan Dasar

Menjelaskan pengaturan untuk tiap fungsi, seperti pencetakan, pemindaian, dan penggunaan faks.

Pengaturan Operasi dan Pengelolaan

Menjelaskan pengoperasian setelah pemakaian awal perangkat, misalnya pemeriksaan informasi dan pemeliharaan.

Memecahkan Masalah

Menjelaskan inisialisasi pengaturan dan pemecahan masalah jaringan.

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Menjelaskan metode pengaturan untuk meningkatkan keamanan perangkat, misalnya penggunaan sertifikat CA, komunikasi SSL/TLS, dan Pemfilteran IPsec/IP.

Tergantung modelnya, sebagian fungsi dalam bab ini mungkin tidak berlaku.

Definisi Istilah yang Digunakan dalam Panduan Ini

Istilah-istilah berikut digunakan dalam panduan ini.

Administrator

Orang yang bertanggung jawab menginstal dan mengatur perangkat atau jaringan di suatu instansi atau organisasi. Untuk organisasi kecil, orang ini mungkin bertanggung jawab atas pengaturan perangkat dan jaringan. Untuk organisasi besar, administrator bertanggung jawab terhadap jaringan atau perangkat di unit grup suatu

Pendahuluan

departemen atau divisi, sementara administrator jaringan bertanggung jawab terkait pengaturan komunikasi di luar organisasi tersebut, misalnya Internet.

Administrator jaringan

Orang yang bertanggung jawab mengendalikan komunikasi jaringan. Orang yang menyiapkan router, server proksi, server DNS, dan server email untuk mengendalikan komunikasi melalui Internet atau jaringan.

Pengguna

Orang yang menggunakan perangkat seperti printer atau scanner.

Web Config (laman web perangkat)

Server web yang berada di internal perangkat. Istilahnya adalah Web Config. Anda dapat melihat dan mengubah status perangkat menggunakan browser.

Alat

Istilah umum bagi perangkat lunak untuk menyiapkan dan mengelola suatu perangkat, misalnya Epson Device Admin, EpsonNet Config, EpsonNet SetupManager, dan lain-lain.

Pemindaian push

Istilah umum untuk pemindaian dari panel kontrol perangkat.

ASCII (American Standard Code for Information Interchange)

Salah satu kode karakter standar. Di dalamnya terdapat 128 karakter meliputi alfabet (a-z, A-Z), Angka arab (0-9), simbol, karakter kosong, dan karakter kontrol. Jika “ASCII” disebutkan dalam panduan ini, maka karakter yang dimaksud adalah 0x20-0x7E (bilangan heksadesimal) seperti tercantum di bawah, dan tidak mencakup karakter kontrol.

SP*	!	"	#	\$	%	&	'	()	*	+	,	-	.	/
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
p	q	r	s	t	u	v	w	x	y	z	{		}	~	

* Karakter spasi.

Unicode (UTF-8)

Kode standar internasional yang mencakup bahasa-bahasa global. Jika “UTF-8” disebutkan dalam panduan ini, maka karakter yang dimaksud adalah karakter pengodean dalam format UTF-8.

Persiapan

Bab ini menjelaskan peran administrator dan persiapan sebelum melakukan pengaturan.

Alur Pengaturan dan Pengelolaan Scanner

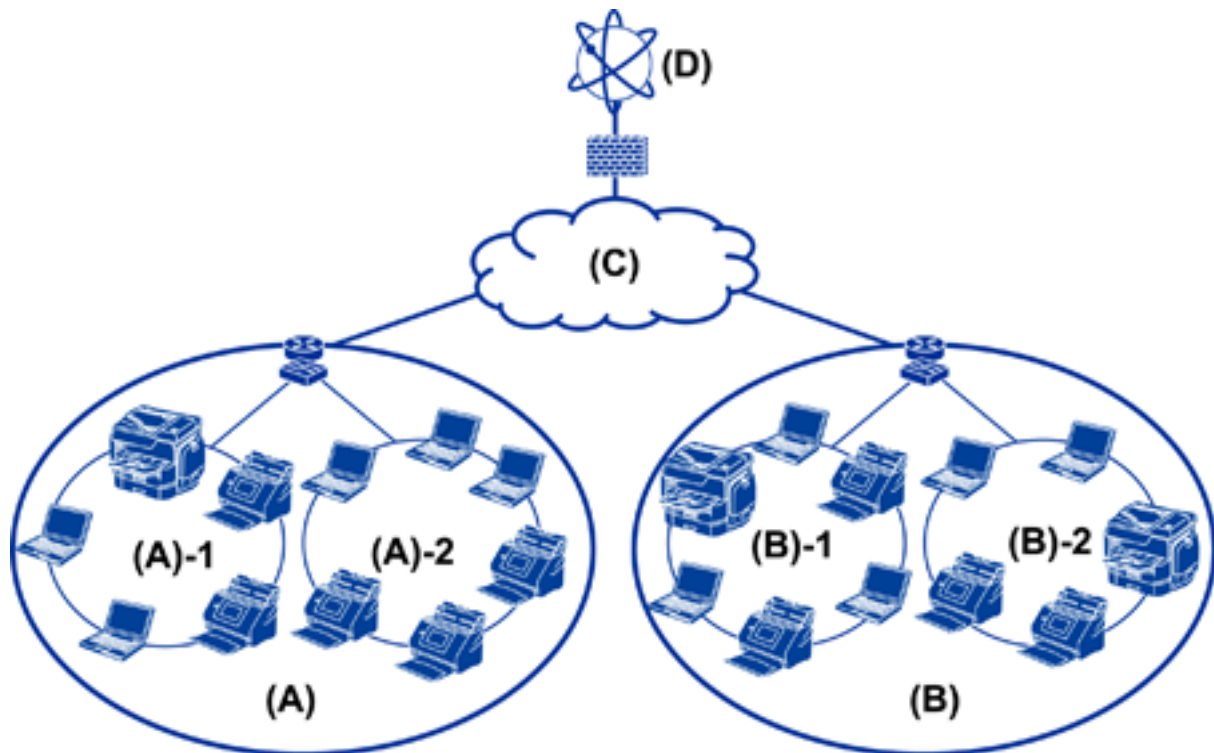
Administrator melakukan pengaturan koneksi jaringan, penyiapan awal, dan pemeliharaan untuk scanner sehingga dapat dipakai oleh pengguna.

1. Penyiapan
 - Mengumpulkan informasi pengaturan koneksi
 - Memutuskan metode koneksi
2. Penyambungan
 - Koneksi jaringan dari panel kontrol scanner
3. Penyiapan fungsi-fungsi
 - Pengaturan driver scanner
 - Pengaturan lanjutan lainnya
4. Pengaturan keamanan
 - Pengaturan administrator
 - SSL/TLS
 - Kontrol protokol
 - Pengaturan keamanan lanjutan (Ops)
5. Pengoperasian dan pengelolaan
 - Memeriksa status perangkat
 - Menangani kemunculan kejadian
 - Membuat cadangan pengaturan perangkat

Informasi Terkait

- ➔ [“Persiapan” pada halaman 10](#)
- ➔ [“Koneksi” pada halaman 15](#)
- ➔ [“Pengaturan Fungsi” pada halaman 22](#)
- ➔ [“Pengaturan Keamanan Dasar” pada halaman 32](#)
- ➔ [“Pengaturan Operasi dan Pengelolaan” pada halaman 40](#)

Contoh Lingkungan Jaringan



(A): Kantor 1

(A) – 1: LAN 1

(A) – 2: LAN 2

(B): Kantor 2

(B) – 1: LAN 1

(B) – 2: LAN 2

(C): WAN

(D): Internet

Pengenalan contoh pengaturan koneksi scanner

Ada dua jenis koneksi utama, tergantung cara penggunaan scanner. Kedua koneksi ini menghubungkan scanner ke jaringan menggunakan komputer melalui hub.

- Koneksi server/klien (scanner menggunakan server Windows, pengelolaan pekerjaan)
- Koneksi peer-to-peer (koneksi langsung dengan komputer klien)

Informasi Terkait

- ➔ [“Koneksi Server/Klien” pada halaman 12](#)
- ➔ [“Koneksi Peer-to-Peer” pada halaman 12](#)

Persiapan

Koneksi Server/Klien

Pusatkan pengelolaan tugas dan scanner dengan Document Capture Pro Server yang terinstal pada server. Ini paling sesuai untuk pekerjaan yang menggunakan beberapa scanner untuk memindai banyak dokumen dalam format tertentu.

Informasi Terkait

➔ [“Definisi Istilah yang Digunakan dalam Panduan Ini” pada halaman 8](#)

Koneksi Peer-to-Peer

Gunakan scanner tersendiri dengan driver scanner seperti Epson Scan 2 yang terinstal pada komputer klien. Instalasi Document Capture Pro (Document Capture) pada komputer klien memungkinkan Anda menjalankan pekerjaan pada setiap komputer klien yang dimiliki scanner.

Informasi Terkait

➔ [“Definisi Istilah yang Digunakan dalam Panduan Ini” pada halaman 8](#)

Persiapan Koneksi ke Jaringan

Mengumpulkan Informasi tentang Pengaturan Koneksi

Anda harus memiliki alamat IP, alamat gateway, dan lain-lain untuk koneksi jaringan. Periksa poin-poin berikut terlebih dahulu.

Divisi	Item	Catatan
Metode koneksi perangkat	<input type="checkbox"/> Ethernet	Gunakan kabel STP (Shielded Twisted Pair) kategori 5e ke atas untuk koneksi Ethernet.
Informasi koneksi LAN	<input type="checkbox"/> Alamat IP <input type="checkbox"/> Subnet mask <input type="checkbox"/> Gateway default	Bagian ini tidak perlu diatur jika Anda sudah melakukan pengaturan alamat IP secara otomatis melalui fungsi DHCP yang dimiliki router.
Informasi server DNS	<input type="checkbox"/> Alamat IP untuk DNS primer <input type="checkbox"/> Alamat IP untuk DNS sekunder	Jika Anda menggunakan alamat IP statis, aturlah server DNS. Lakukan pengaturan ketika menentukan alamat IP secara otomatis melalui fungsi DHCP dan ketika server DNS tidak dapat ditentukan secara otomatis.
Informasi server proksi	<input type="checkbox"/> Nama server proksi <input type="checkbox"/> Nomor port	Lakukan pengaturan ketika menggunakan server proksi untuk koneksi Internet dan ketika menggunakan layanan Epson Connect atau fungsi pembaruan firmware otomatis.

Spesifikasi Pemindai

Untuk spesifikasi apakah Scanner mendukung mode koneksi atau standar, lihat *Panduan Pengguna*.

Menggunakan Nomor Port

Lihat “Lampiran” untuk mengetahui nomor port yang digunakan oleh scanner.

Informasi Terkait

➔ [“Menggunakan Port Scanner” pada halaman 60](#)

Jenis Penetapan Alamat IP

Ada dua jenis penetapan alamat IP scanner.

Alamat IP Statis:

Tetapkan alamat IP unik yang sudah ditentukan ke scanner.

Alamat IP tidak berubah meskipun scanner atau router dimatikan, sehingga Anda dapat mengelola perangkat melalui alamat IP.

Jenis alamat seperti ini cocok untuk jaringan yang di dalamnya terdapat banyak scanner, misalnya kantor atau sekolah yang besar.

Penetapan otomatis melalui fungsi DHCP:

Alamat IP ditetapkan secara otomatis ketika komunikasi antara scanner dan router yang mendukung fungsi DHCP berhasil dilakukan.

Jika Anda lebih suka mengubah alamat IP perangkat tertentu, siapkan alamat IP terlebih dahulu lalu terapkan.

Server DNS dan Server Proksi

Jika Anda menggunakan layanan koneksi Internet, aturlah server DNS. Jika Anda tidak mengaturnya, Anda harus menentukan alamat IP untuk pengaksesan karena ada kemungkinan resolusi nama gagal.

Server proksi berada di gateway antara jaringan dan Internet, dan berkomunikasi dengan komputer, scanner, dan Internet (server yang berlawanan) mewakili masing-masing. Server yang berlawanan hanya berkomunikasi dengan server proksi. Oleh karena itu, informasi scanner seperti alamat IP dan nomor port tidak dapat dibaca sehingga tingkat keamanan pun bertambah.

Anda dapat melarang akses ke URL tertentu dengan menggunakan fungsi pemfilteran, karena server proksi dapat memeriksa isi komunikasi.

Metode Pengaturan Koneksi Jaringan

Terkait pengaturan koneksi alamat IP scanner, subnet mask, dan gateway default, lakukan langkah-langkah sebagai berikut.

Menggunakan Panel Kontrol:

Konfigurasi pengaturan menggunakan panel kontrol scanner di masing-masing scanner. Hubungkan ke jaringan setelah mengonfigurasi pengaturan koneksi scanner.

Persiapan

Menggunakan Penginstal:

Jika menggunakan penginstal, jaringan scanner dan komputer klien akan diatur secara otomatis. Pengaturan ini cukup dilakukan dengan cara mengikuti petunjuk penginstal, dan tidak memerlukan pengetahuan mendalam mengenai jaringan.

Menggunakan Alat:

Gunakan alat dari komputer administrator. Anda dapat menemukan scanner kemudian mengaturnya, atau membuat file SYLK untuk menerapkan pengaturan batch terhadap scanner. Anda dapat mengatur banyak scanner, tetapi harus terhubung secara fisik melalui kabel Ethernet. Oleh karena itu, sebaiknya Anda dapat membangun Ethernet untuk pengaturan.

Informasi Terkait

- ➔ [“Menyambung ke Jaringan dari Panel Kontrol” pada halaman 15](#)
- ➔ [“Menyambung ke Jaringan Menggunakan Penginstal” pada halaman 19](#)
- ➔ [“Menentukan Alamat IP Menggunakan EpsonNet Config” pada halaman 56](#)

Koneksi

Bab ini menjelaskan lingkungan atau prosedur penyambungan scanner ke jaringan.

Menyambung ke Jaringan

Menyambung ke Jaringan dari Panel Kontrol

Hubungkan scanner ke jaringan dengan menggunakan panel kontrol scanner.

Untuk panel kontrol scanner, lihat *Panduan Pengguna* untuk keterangan selengkapnya.

Menentukan Alamat IP

Atur item-item dasar seperti Alamat IP, Subnet Mask, dan Default Gateway.

1. Nyalakan scanner.
2. Jentikkan layar ke kiri pada panel kontrol scanner, lalu sentuh **Pengaturan**.

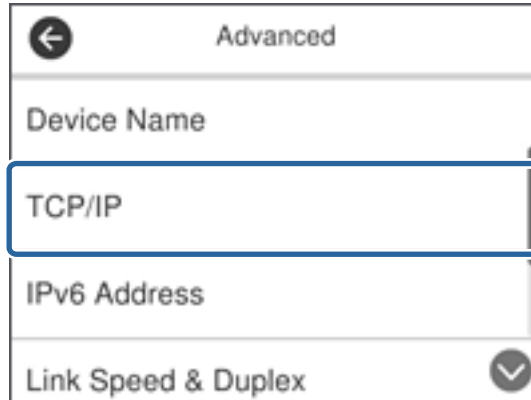


3. Sentuh **Pengaturan Jaringan > Ganti Pengaturan**.

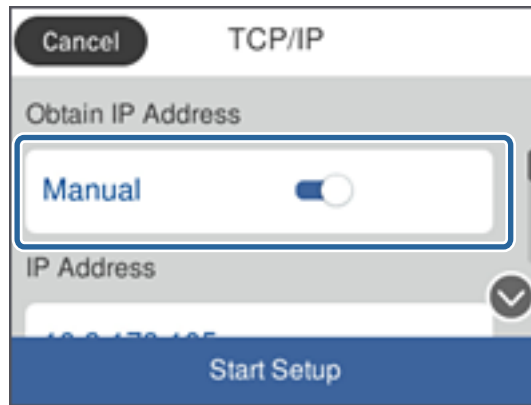
Jika item tersebut tidak ditampilkan, jentikkan layar ke atas untuk menampilkannya.

Koneksi

- 4. Sentuh **TCP/IP**.



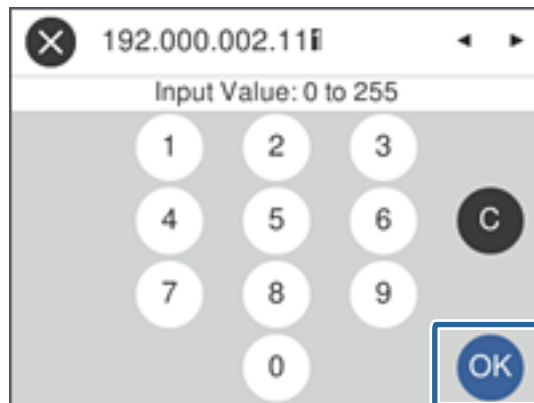
- 5. Pilih **Manual** untuk **Dapatkan Alamat IP**.



Catatan:

Jika Anda mengatur alamat IP secara otomatis dengan menggunakan fungsi DHCP pada router, pilih **Otomatis**. Dalam konteks tersebut, **Alamat IP**, **Subnet Mask**, dan **Default Gateway** pada langkah 6 sampai 7 juga diatur secara otomatis, sehingga Anda tinggal melanjutkan ke langkah 8.

- 6. Sentuh bidang **Alamat IP**, masukkan alamat IP menggunakan keyboard yang ditampilkan di layar, kemudian sentuh **OK**.



Konfirmasikan nilai yang ditampilkan di layar sebelumnya.

Koneksi

7. Atur **Subnet Mask** dan **Default Gateway**.

Konfirmasikan nilai yang ditampilkan di layar sebelumnya.

Catatan:

Jika kombinasi Alamat IP, Subnet Mask dan Default Gateway salah, **Mulai Konfigurasi** tidak aktif dan tidak dapat melanjutkan pengaturan. Pastikan tidak ada kesalahan dalam penginputan.

8. Sentuh kolom **DNS Utama** untuk **Server DNS**, masukkan alamat IP server DNS utama menggunakan keyboard yang ditampilkan di layar, lalu sentuh **OK**.

Konfirmasikan nilai yang ditampilkan di layar sebelumnya.

Catatan:

Ketika Anda memilih **Otomatis** untuk pengaturan penentuan alamat IP, Anda dapat memilih pengaturan server DNS dari **Manual** atau **Otomatis**. Jika Anda tidak dapat memperoleh alamat server DNS secara otomatis, pilih **Manual** dan masukkan alamat server DNS. Kemudian, masukkan alamat server DNS sekunder secara langsung. Jika Anda memilih **Otomatis**, lanjutkan ke langkah 10.

9. Sentuh kolom **DNS Sekunder**, masukkan alamat IP server DNS sekunder menggunakan keyboard yang ditampilkan di layar, lalu sentuh **OK**.

Konfirmasikan nilai yang ditampilkan di layar sebelumnya.

10. Sentuh **Mulai Konfigurasi**.


11. Sentuh **Tutup** di layar konfirmasi.

Layar secara otomatis menutup setelah beberapa waktu jika Anda tidak menyentuh **Tutup**.

Menyambung ke Ethernet

Hubungkan scanner ke jaringan dengan menggunakan kabel Ethernet, dan periksa koneksi.

1. Hubungkan scanner dan hub (sakelar L2) dengan menggunakan kabel Ethernet.

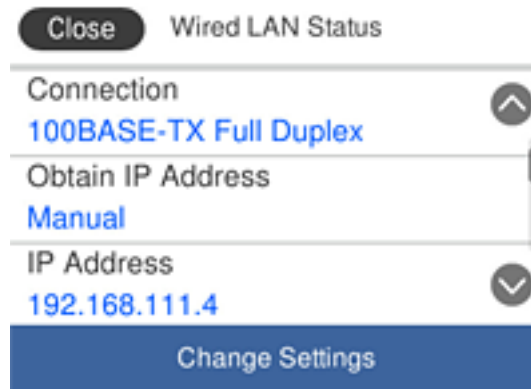
Ikon di layar beranda berubah menjadi .

2. Sentuh  di layar beranda.



Koneksi

3. Jentikkan layar ke atas, lalu pastikan status koneksi dan alamat IP sudah benar.



Mengatur Server Proksi

Server proksi tidak dapat diatur pada panel. Aturilah konfigurasinya menggunakan Web Config.

1. Akses Web Config lalu pilih **Network Settings > Basic**.
2. Pilih **Use** di **Proxy Server Setting**.
3. Tentukan server proksi dalam format alamat IPv4 atau FQDN di **Server Proxy**, lalu masukkan nomor port di **Proxy Server Port Number**.

Untuk server proksi yang memerlukan autentikasi, masukkan nama pengguna dan sandi autentikasi server Proksi.

Koneksi

4. Klik tombol **Next**.

The screenshot shows the EPSON Web Config interface for a device. The left sidebar contains navigation options like 'Administrator Logout', 'Status', 'Scanner Settings', 'Network Settings', 'Wired LAN', 'Basic', 'Email Server', 'Network Security Settings', 'Services', 'System Settings', 'Export and Import Setting Value', and 'Administrator Settings'. Under 'Basic Settings', there are links for 'DNS/Proxy Setup', 'Firmware Update', 'Root Certificate Update', and 'Product Status'. The main content area displays various network configuration fields:

- Primary DNS Server : [text box]
- Secondary DNS Server : [text box]
- DNS Host Name Setting : Auto Manual
- DNS Host Name Status : Failed
- DNS Host Name : EPSON884045
- DNS Domain Name Setting : Auto Manual
- DNS Domain Name Status : Failed
- DNS Domain Name : [text box]
- Register the network interface address to DNS : Enable Disable
- Proxy Server Setting** : Do Not Use Use
- Proxy Server : www.sample.proxy
- Proxy Server Port Number : 80
- Proxy Server User Name : XXXXXXXX
- Proxy Server Password : [password field]
- IPv6 Setting : Enable Disable
- IPv6 Privacy Extension : Enable Disable
- IPv6 DHCP Server Setting : Do Not Use Use
- IPv6 Address : [text box]
- IPv6 Address Default Gateway : [text box]
- IPv6 Link-Local Address : fe80::9eae:d3ff:fe88:4045/64
- IPv6 Stateful Address : [text box]
- IPv6 Stateless Address 1 : [text box]
- IPv6 Stateless Address 2 : [text box]
- IPv6 Stateless Address 3 : [text box]
- IPv6 Primary DNS Server : [text box]
- IPv6 Secondary DNS Server : [text box]

A 'Next' button is located at the bottom of the configuration area.

5. Konfirmasikan pengaturan, lalu klik **Pengaturan**.

Informasi Terkait

- ➔ “Mengakses Web Config” pada halaman 23

Menyambung ke Jaringan Menggunakan Pengeinstal

Sebaiknya gunakan pengeinstal untuk menghubungkan pemindai ke komputer. Anda dapat menjalankan pengeinstal dengan salah satu cara berikut ini.

- Melakukan penyiapan dari situs web

Kunjungi situs web berikut, lalu masukkan nama produk. Masuk ke **Konfigurasi**, kemudian mulai penyiapan.

<http://epson.sn>

- Penyiapan dengan disk perangkat lunak (khusus untuk model yang dilengkapi disk perangkat lunak dan pengguna yang komputernya dilengkapi disc drive).

Masukkan disk perangkat lunak ke dalam komputer, lalu ikuti petunjuk di layar.

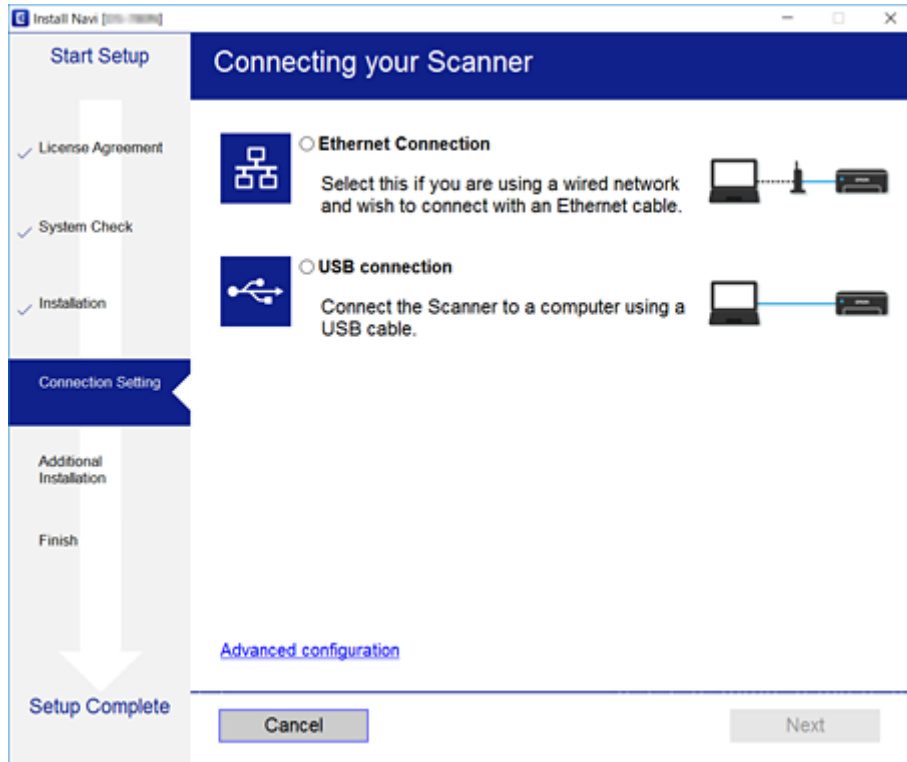
Koneksi

Memilih Metode Koneksi

Ikuti petunjuk di layar sampai muncul layar berikut ini, lalu pilih metode koneksi scanner ke komputer.

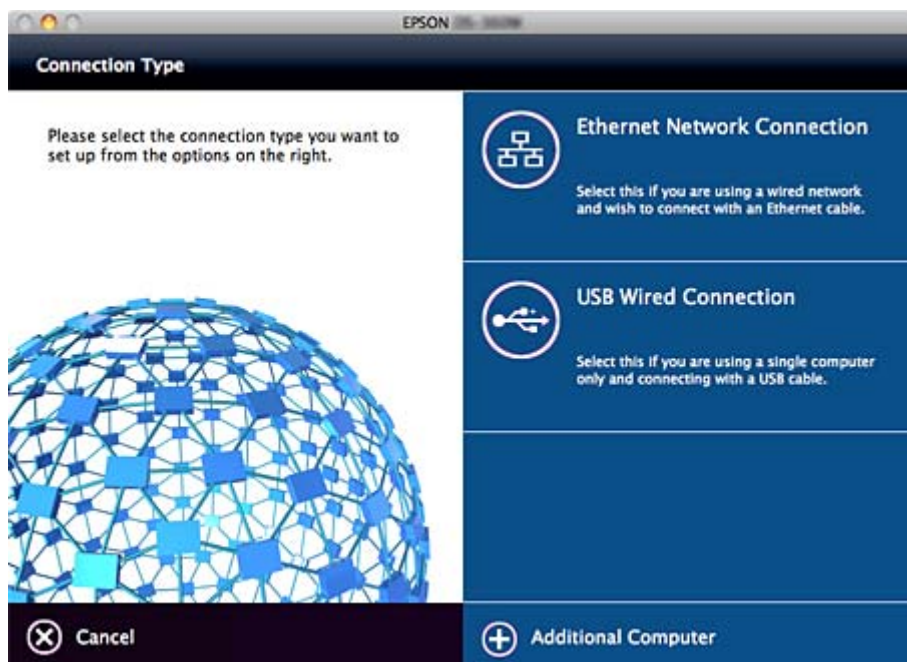
☐ Windows

Pilih jenis koneksi lalu klik **Berikutnya**.



☐ Mac OS

Pilih jenis koneksi.



Koneksi

Ikuti petunjuk pada layar. Perangkat lunak telah terpasang.

Pengaturan Fungsi

Bab ini menjelaskan pengaturan pertama yang harus dilakukan agar tiap fungsi perangkat dapat digunakan.

Perangkat Lunak Pengaturan

Bagian ini menjelaskan cara pengaturan dari komputer administrator menggunakan Web Config.

Web Config (Laman Web untuk Perangkat)

Tentang Web Config

Web Config merupakan aplikasi berbasis browser untuk mengonfigurasi pengaturan scanner.

Untuk mengakses Web Config, pertama Anda harus menetapkan alamat IP untuk scanner.

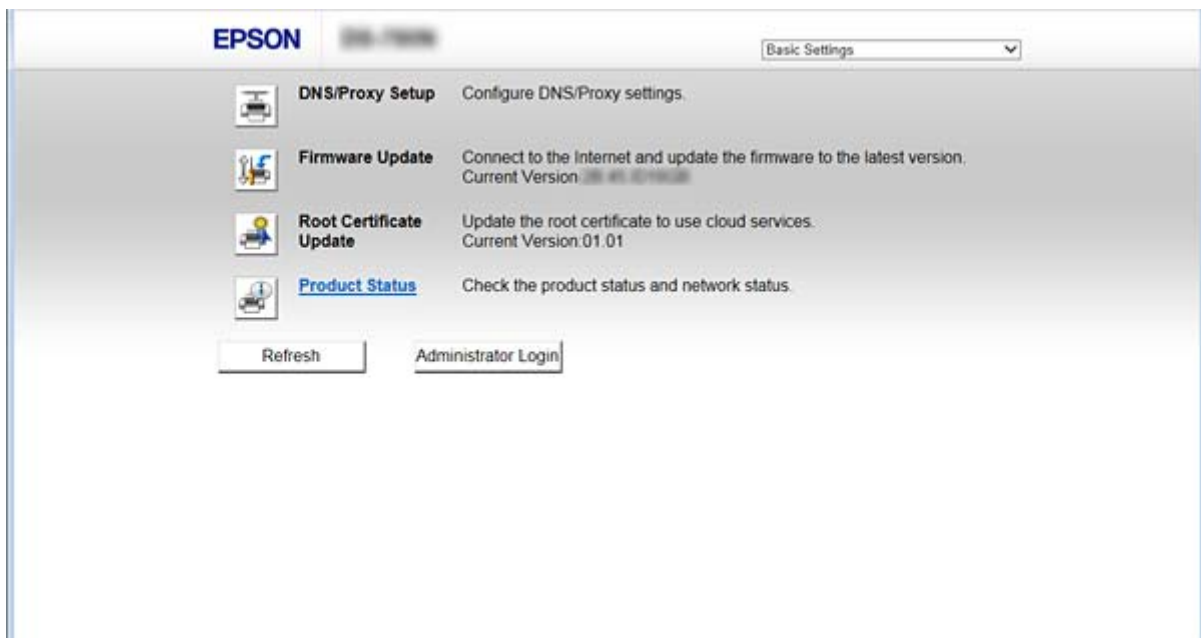
Catatan:

Anda dapat mengunci pengaturan dengan mengonfigurasi kata sandi administrator ke scanner.

Ada dua halaman pengaturan berikut.

Basic Settings

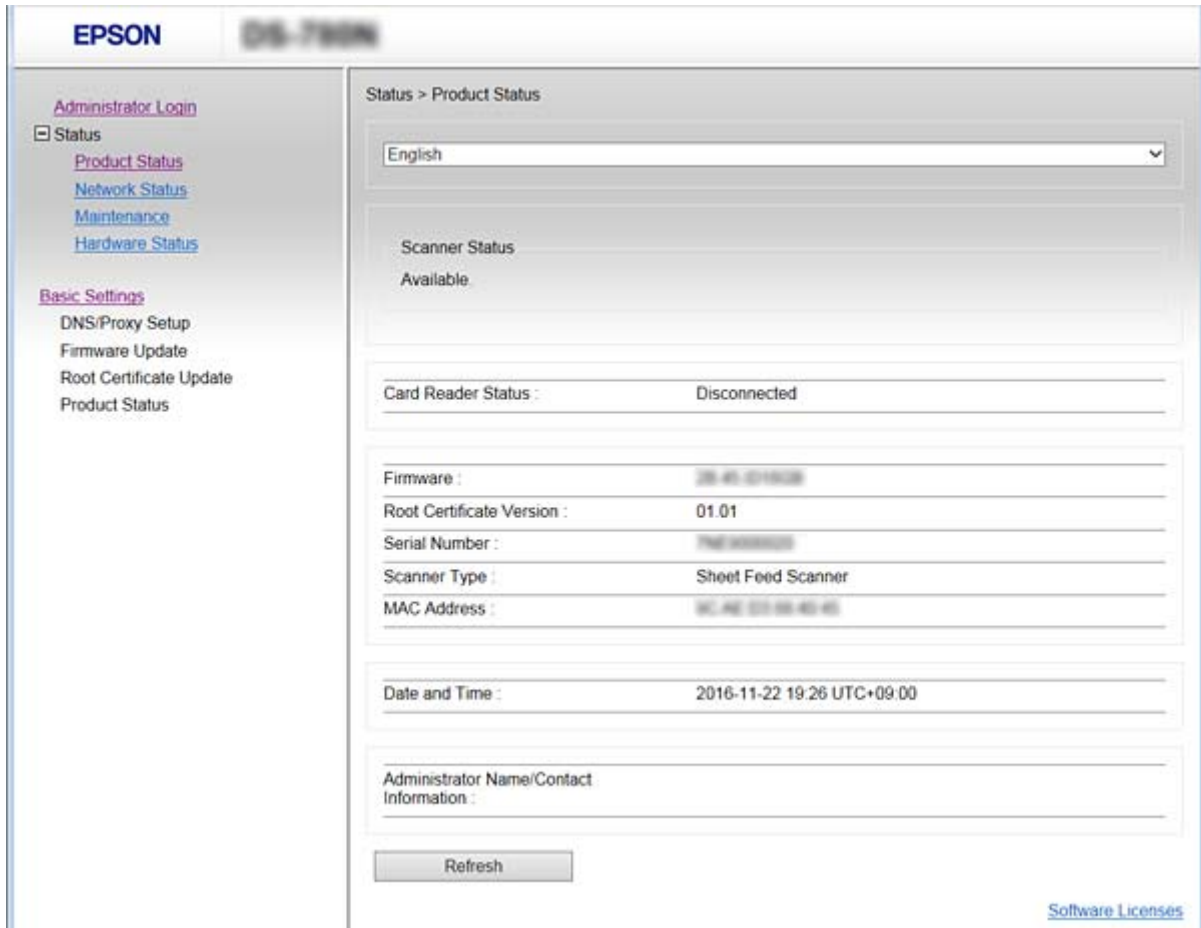
Anda dapat mengonfigurasi pengaturan dasar untuk scanner.



Pengaturan Fungsi

❑ Advanced Settings

Anda dapat mengonfigurasi pengaturan lanjutan untuk scanner. Halaman ini terutama diperuntukkan administrator.



Mengakses Web Config

Masukkan alamat IP scanner ke dalam browser web. JavaScript harus diaktifkan. Ketika mengakses Web Config melalui HTTPS, pesan peringatan akan muncul di browser karena sertifikat bertanda tangan sendiri dan tersimpan di scanner sedang digunakan.

❑ Mengakses melalui HTTPS

IPv4: `https://<alamat IP scanner>` (tanpa `<>`)

IPv6: `https://[alamat IP scanner]/` (dengan `[]`)

❑ Mengakses melalui HTTP

IPv4: `http://<alamat IP scanner>` (tanpa `<>`)

IPv6: `http://[alamat IP scanner]/` (dengan `[]`)

Pengaturan Fungsi

Catatan:

Contoh

IPv4:

<https://192.0.2.111/>

<http://192.0.2.111/>

IPv6:

[https://\[2001:db8::1000:1\]/](https://[2001:db8::1000:1]/)

[http://\[2001:db8::1000:1\]/](http://[2001:db8::1000:1]/)

- Jika nama scanner didaftarkan dengan server DNS, Anda dapat menggunakan nama scanner tersebut alih-alih alamat IP scanner.

Informasi Terkait

- ➔ [“Komunikasi SSL/TLS dengan Scanner”](#) pada halaman 63
- ➔ [“Tentang Sertifikasi Digital”](#) pada halaman 63

Menggunakan Fungsi Pemindaian

Tergantung pada cara pemakaian scanner, instal perangkat lunak berikut dan lakukan pengaturan dengan menggunakan perangkat lunak tersebut.

Pindai dari komputer

- Pastikan valid tidaknya layanan pemindaian jaringan dengan Web Config (valid ketika dikirim dari pabrik).
- Instal Epson Scan 2 ke komputer Anda dan atur alamat IP
- Pada saat memindai menggunakan pekerjaan, instal Document Capture Pro (Document Capture) dan lakukan pengaturan pekerjaan.

Pindai dari panel pengoperasian

- Pada saat menggunakan Document Capture Pro atau Document Capture Pro Server:
Instal Document Capture Pro atau Document Capture Pro Server
Pengaturan DCP (mode server, mode klien).
- Pada saat menggunakan protokol WSD:
Pastikan valid tidaknya WSD di Web Config atau panel pengoperasian (valid ketika dikirim dari pabrik)
Pengaturan perangkat tambahan (komputer Windows).

Memindai dari Komputer

Instal perangkat lunak dan pastikan layanan pemindaian jaringan untuk melakukan pemindaian dari komputer melalui jaringan sudah diaktifkan.

Informasi Terkait

- ➔ [“Perangkat lunak yang perlu diinstal”](#) pada halaman 25
- ➔ [“Mengaktifkan Pemindaian Jaringan”](#) pada halaman 25

Pengaturan Fungsi

Perangkat lunak yang perlu diinstal

❑ Epson Scan 2

Ini adalah driver scanner. Jika Anda menggunakan perangkat dari komputer, instal driver di setiap komputer klien. Jika Document Capture Pro/Document Capture diinstal, Anda dapat melakukan operasi yang ditetapkan ke tombol-tombol perangkat.

Dengan EpsonNet SetupManager, driver printer juga dapat disertakan dalam paket.

❑ Document Capture Pro (Windows)/Document Capture (Mac OS)

Instal di komputer klien. Anda dapat memanggil dan menjalankan pekerjaan yang terdaftar di komputer yang sudah diinstal Document Capture Pro/Document Capture pada jaringan, dari komputer dan panel pengoperasian scanner.

Anda juga dapat memindai dari komputer melalui jaringan. Epson Scan 2 diperlukan agar dapat memindai.

Informasi Terkait

➔ [“EpsonNet SetupManager” pada halaman 56](#)

Atur alamat IP scanner menjadi Epson Scan 2


Sebutkan alamat IP scanner agar scanner dapat digunakan pada jaringan.

1. Buka **Epson Scan 2 Utility** dari **Mulai > Semua Program > EPSON > Epson Scan 2**.

Jika sudah ada scanner lain yang terdaftar, lanjutkan ke langkah 2.

Jika belum, lanjutkan ke langkah 4.

2. Klik ▼ pada **Pemindai**.
3. Klik **Pengaturan**.
4. Klik **Aktifkan Pengeditan**, lalu klik **Tambahkan**.
5. Pilih nama model scanner dari **Model**.
6. Pilih alamat IP scanner yang akan digunakan dari **Alamat** di **Cari Jaringan**.

Klik  dan klik  untuk memperbarui daftar. Jika Anda tidak dapat menemukan alamat IP scanner, pilih **Masukkan alamat** dan masukkan alamat IP.

7. Klik **Tambahkan**.

8. Klik **Oke**.

Mengaktifkan Pemindaian Jaringan

Anda dapat mengatur layanan pemindaian jaringan ketika Anda memindai dari komputer klien melalui jaringan. Secara default, pengaturan ini sudah dalam kondisi aktif.

1. Akses Web Config lalu pilih **Services > Network Scan**.

Pengaturan Fungsi

2. Pastikan **Enable scanning** pada **EPSON Scan** sudah dipilih.
Jika sudah dipilih, maka tugas ini selesai. Tutup Web Config.
Jika belum dipilih, pilihlah dan lanjutkan ke langkah berikutnya.
3. Klik **Next**.
4. Klik **OK**.
Jaringan disambungkan ulang, dan pengaturan diaktifkan.

Informasi Terkait

- ➔ [“Mengakses Web Config” pada halaman 23](#)

Memindai dengan panel kontrol

Fungsi pindai ke folder dan pindai ke email dengan panel kontrol scanner, serta transfer hasil pindaian ke email, folder, dll dilakukan dengan menjalankan pekerjaan dari komputer.

Ketika mentransfer hasil pindaian, aturlah pekerjaan dengan Document Capture Pro Server atau Document Capture Pro.

Untuk keterangan lengkap mengenai pengaturan dan penyiapan pekerjaan, lihat dokumentasi atau bantuan Document Capture Pro Server atau Document Capture Pro.

Informasi Terkait

- ➔ [“Pengaturan Document Capture Pro Server/Document Capture Pro” pada halaman 26](#)
- ➔ [“Mengatur Server dan Folder” pada halaman 27](#)

Perangkat lunak yang harus diinstal di komputer

Document Capture Pro Server

Ini adalah versi server dari Document Capture Pro. Instal di server Windows. Server dapat mengelola banyak perangkat dan pekerjaan secara terpusat. Pekerjaan dapat dijalankan serentak dari banyak scanner.

Dengan menggunakan versi Document Capture Pro Server yang bersertifikat, Anda dapat mengelola pekerjaan dan riwayat pemindaian yang tertaut ke pengguna dan grup.

Untuk keterangan lengkap mengenai Document Capture Pro Server, hubungi kantor Epson di wilayah Anda.

Document Capture Pro (Windows)/Document Capture (Mac OS)

Seperti halnya memindai dari komputer, Anda dapat memanggil pekerjaan yang telah terdaftar di komputer dari panel kontrol dan menjalankannya. Pekerjaan di komputer tidak dapat dijalankan secara serentak dari banyak scanner.

Pengaturan Document Capture Pro Server/Document Capture Pro

Lakukan pengaturan pemakaian fungsi pemindaian dari panel pengoperasian scanner.

1. Akses Web Config lalu pilih **Services > Document Capture Pro**.

Pengaturan Fungsi

2. Pilih **Mode Operasi**.

Server Mode:

Pilih ini saat menggunakan Document Capture Pro Server.

Client Mode:

Atur ini jika Anda memilih pengaturan pekerjaan Document Capture Pro (Document Capture) yang terinstal di setiap komputer klien dalam jaringan tanpa menentukan komputer tersebut.

3. Atur poin berikut sesuai dengan mode yang sudah dipilih.

Server Mode:

Di **Server Address**, tentukan server tempat instalasi Document Capture Pro Server. Isinya dapat terdiri dari 2 hingga 252 karakter dalam format IPv4, IPv6, nama host, FQDN. Dalam format FQDN, huruf, angka, alfabet, dan tanda hubung (kecuali leading dan trailing) US-ASCII boleh digunakan.

Client Mode:

Tentukan **Group Settings** untuk menggunakan grup scanner yang ditentukan dari Document Capture Pro (Document Capture).

4. Klik **Pengaturan**.

Informasi Terkait

➔ [“Mengakses Web Config” pada halaman 23](#)

Mengatur Server dan Folder

Document Capture Pro dan Document Capture Pro Server menyimpan data hasil pemindaian ke server atau komputer klien sebanyak satu kali dan menggunakan fungsi transfer untuk menjalankan fungsi pindai ke folder serta fungsi pindai ke email.

Anda memerlukan otoritas dan informasi untuk mentransfer dari komputer yang Document Capture Pro, Document Capture Pro Server-nya diinstal di komputer atau layanan cloud.

Siapkan informasi mengenai fungsi yang akan Anda gunakan, dengan mengacu pada hal-hal berikut.

Anda dapat melakukan pengaturan untuk fungsi-fungsi ini menggunakan Document Capture Pro atau Document Capture Pro Server. Untuk keterangan terperinci mengenai pengaturan, lihat dokumentasi atau bantuan Document Capture Pro Server atau Document Capture Pro.

Nama	Pengaturan	Persyaratan
Pindai ke Folder Jaringan (SMB)	Membuat dan mengatur pemakaian bersama untuk folder penyimpanan	Akun pengguna administratif ke komputer yang membuat folder penyimpanan.
	Tujuan terkait Pindai ke Folder Jaringan (SMB)	Nama pengguna dan kata sandi untuk login ke komputer yang memiliki folder penyimpanan, kemudian hak khusus untuk memperbarui folder penyimpanan.
Pindai ke Folder Jaringan (FTP)	Mengatur login server FTP	Informasi login untuk server FTP dan hak khusus untuk memperbarui folder penyimpanan.
Pindai ke Email	Mengatur server email	Mengatur informasi server email

Pengaturan Fungsi

Nama	Pengaturan	Persyaratan
Pindai ke Document Capture Pro (jika menggunakan Document Capture Pro Server)	Pengaturan untuk login (masuk) ke layanan cloud	Lingkungan koneksi Internet Pendaftaran akun layanan cloud

Menggunakan pemindaian WSD (Windows saja)

Apabila komputer menggunakan Windows Vista atau yang lebih tinggi, Anda dapat menggunakan pemindaian WSD.

Jika protokol WSD dapat digunakan, menu **Komputer (WSD)** akan ditampilkan pada panel kontrol scanner.



1. Akses Web Config lalu pilih **Services > Protocol**.
2. Pastikan **Enable WSD** sudah dicentang di **WSD Settings**.
Apabila sudah dicentang, tugas Anda selesai dan Anda dapat menutup Web Config.
Apabila belum dicentang, centanglah dan lanjutkan ke langkah berikutnya.
3. Klik tombol **Next**.
4. Konfirmasikan pengaturan dan klik **Pengaturan**.

Melakukan Pengaturan Sistem

Melakukan Pengaturan Sistem pada Panel Kontrol

Mengatur kecerahan layar

Atur kecerahan layar LCD.

1. Sentuh **Pengaturan** di layar beranda.
2. Sentuh **Pengaturan Umum > Kecerahan LCD**.
3. Sentuh  atau  untuk menyesuaikan kecerahan.
Anda dapat melakukan penyesuaian dari 1 sampai 9.
4. Sentuh **OK**.

Mengatur suara

Atur bunyi kerja dan bunyi kesalahan panel.

1. Sentuh **Pengaturan** di layar beranda.

Pengaturan Fungsi

2. Sentuh **Pengaturan Umum > Suara**.
3. Atur item berikut sesuai keperluan.
 - Bunyi kerja
Atur volume bunyi kerja panel pengoperasian.
 - Bunyi kesalahan
Atur volume bunyi kesalahan.
4. Sentuh **OK**.

Informasi Terkait

➔ [“Mengakses Web Config” pada halaman 23](#)

Mendeteksi pemasukan ganda dokumen asli

Tentukan fungsi untuk mendeteksi pemasukan ganda dokumen yang hendak dipindai dan untuk menghentikan pemindaian manakala terjadi pemasukan ganda.

Untuk memindai dokumen asli yang dianggap sebagai pemasukan ganda, misalnya amplop atau kertas yang ditempeli stiker, matikan fungsi deteksi.

Catatan:

Pengaturan ini juga dapat dilakukan dari Web Config atau Epson Scan 2.

1. Sentuh **Pengaturan** di layar beranda.
2. Sentuh **Pengaturan Pemindaian eksternal > Ultrasonic Deteksi Pakan Ganda**.
3. Sentuh **Ultrasonic Deteksi Pakan Ganda** untuk mengaktifkan atau menonaktifkannya.
4. Sentuh **Tutup**.

Mengatur mode kecepatan rendah

Atur untuk memindai pada kecepatan rendah sehingga tidak terjadi kemacetan kertas pada saat memindai dokumen berukuran tipis seperti slip.

1. Sentuh **Pengaturan** di layar beranda.
2. Sentuh **Pengaturan Pemindaian eksternal > Lbt**.
3. Sentuh **Lbt** untuk mengaktifkan atau menonaktifkannya.
4. Sentuh **Tutup**.

Melakukan Pengaturan Sistem Menggunakan Konfigurasi Web

Pengaturan Penghematan Daya Selama Tidak Ada Aktivitas

Lakukan pengaturan penghematan daya untuk periode waktu saat tidak ada aktivitas pada scanner. Atur durasi tidak adanya aktivitas tersebut sesuai dengan kondisi pemakaian.

Catatan:

Anda juga dapat mengatur penghematan daya pada panel kontrol scanner.

1. Akses Web Config lalu pilih **System Settings > Power Saving**.
2. Masukkan waktu **Sleep Timer** untuk berpindah ke mode hemat daya jika alat tidak ada aktivitas sekian waktu.
3. Pilih waktu pematian di **Power Off Timer**.
4. Klik **OK**.

Informasi Terkait

➔ [“Mengakses Web Config” pada halaman 23](#)

Mengatur Panel Kontrol

Pengaturan panel kontrol scanner. Anda dapat melakukan pengaturan berikut.

1. Akses Web Config lalu pilih **System Settings > Control Panel**.
2. Atur item berikut sesuai keperluan.
 - Language**
Pilih bahasa tampilan di panel kontrol.
 - Panel Lock**
Jika Anda memilih **ON**, Anda akan diminta memasukkan kata sandi administrator sewaktu melakukan operasi yang memerlukan wewenang administrator. Jika kata sandi administrator tidak diatur, penguncian panel tidak aktif.
 - Operation Timeout**
Jika Anda memilih **ON**, dan Anda log in sebagai administrator, Anda akan otomatis dikeluarkan dan dialihkan ke layar awal apabila tidak ada aktivitas dalam waktu tertentu.
Anda dapat mengatur antara 10 detik hingga 240 menit.
3. Klik **OK**.

Informasi Terkait

➔ [“Mengakses Web Config” pada halaman 23](#)

Pengaturan Fungsi

Mengatur Pembatasan Antarmuka Eksternal

Anda dapat membatasi koneksi USB dari komputer. Lakukan pengaturan untuk membatasi pemindaian selain melalui jaringan.

1. Akses Web Config lalu pilih **System Settings > External Interface**.
2. Pilih **Enable** atau **Disable**.
Untuk membatasi, pilih **Disable**.
3. Sentuh **OK**.

Menyinkronkan Tanggal dan Waktu dengan Server Waktu

Jika menggunakan sertifikat CA, Anda dapat mencegah masalah terkait waktu.

1. Akses Web Config lalu pilih **System Settings > Date and Time > Time Server**.
2. Pilih **Use** untuk **Use Time Server**.
3. Masukkan alamat server waktu di bagian **Time Server Address**.
Anda dapat menggunakan format IPv4, IPv6, atau FQDN. Masukkan sepanjang 252 karakter atau kurang. Jika poin ini tidak ingin Anda tetapkan, kosongkan.
4. Masukkan **Update Interval (min)**.
Anda dapat mengatur maksimum 10.800 menit.
5. Klik **OK**.

Catatan:

Anda dapat mengonfirmasi status koneksi dengan server waktu di bagian **Time Server Status**.

Informasi Terkait

➔ [“Mengakses Web Config”](#) pada halaman 23

Pengaturan Keamanan Dasar

Bab ini menjelaskan pengaturan keamanan dasar yang tidak memerlukan lingkungan khusus.

Pengenalan Fitur-fitur Keamanan Dasar

Berikut fitur-fitur keamanan dasar yang dimiliki Perangkat Epson.

Nama fitur	Jenis fitur	Yang harus diatur	Yang harus dicegah
Penyiapan kata sandi administrator	Kuncilah pengaturan yang berhubungan dengan sistem, misalnya pengaturan koneksi jaringan dan USB, sehingga tidak dapat diubah kecuali oleh administrator.	Administrator mengatur kata sandi perangkat. Konfigurasi atau pembaruan tersedia di mana saja dari Web Config, panel kontrol, Epson Device Admin, dan EpsonNet Config.	Cegahlah pembacaan dan perubahan informasi secara ilegal yang disimpan dalam perangkat seperti ID, kata sandi, pengaturan jaringan, dan kontak. Selain itu, kurangi juga beragam risiko keamanan seperti kebocoran informasi terkait lingkungan jaringan atau kebijakan keamanan.
Komunikasi SSL/TLS	Pada saat mengakses server Epson di internet dari suatu perangkat, misalnya komunikasi dengan komputer melalui browser atau pembaruan firmware, isi komunikasi tersebut dienkripsi oleh komunikasi SSL/TLS.	Dapatkan sertifikat bertanda tangan CA, lalu impor ke scanner.	Menghapus identifikasi perangkat dengan sertifikasi bertanda tangan CA mencegah peniruan identitas dan akses tanpa izin. Selain itu, isi komunikasi SSL/TLS terlindungi, dan mencegah terjadinya kebocoran isi data pencetakan dan informasi penyiapan.
Protokol Kontrol	Protokol Kontrol digunakan untuk komunikasi antara perangkat dan komputer, dan mengaktifkan/ menonaktifkan fungsi.	Protokol atau layanan yang diterapkan ke fitur yang diizinkan atau dilarang secara sendiri-sendiri.	Mengurangi risiko keamanan yang mungkin timbul melalui penggunaan tak diinginkan, dengan mencegah pengguna memakai fungsi-fungsi yang tidak diperlukan.

Informasi Terkait

- ➔ [“Tentang Web Config” pada halaman 22](#)
- ➔ [“EpsonNet Config” pada halaman 55](#)
- ➔ [“Epson Device Admin” pada halaman 55](#)
- ➔ [“Mengonfigurasi Kata Sandi Administrator” pada halaman 33](#)
- ➔ [“Mengendalikan protokol” pada halaman 35](#)

Mengonfigurasi Kata Sandi Administrator

Jika Anda mengatur kata sandi administrator, pengguna selain administrator tidak akan dapat mengubah pengaturan untuk administrasi sistem. Anda dapat mengatur dan mengubah kata sandi administrator menggunakan Web Config, panel kontrol scanner, atau perangkat lunak (Epson Device Admin atau EpsonNet Config). Ketika menggunakan perangkat lunak, lihat dokumentasi yang disertakan bersamanya.

Informasi Terkait

- ➔ “Mengonfigurasi Kata Sandi Administrator dari Panel Kontrol” pada halaman 33
- ➔ “Mengonfigurasi Kata Sandi Administrator Menggunakan Web Config” pada halaman 33
- ➔ “EpsonNet Config” pada halaman 55
- ➔ “Epson Device Admin” pada halaman 55

Mengonfigurasi Kata Sandi Administrator dari Panel Kontrol

Anda dapat mengatur kata sandi administrator dari panel kontrol scanner.

1. Sentuh **Pengaturan** di layar beranda.
2. Sentuh **Administrasi Sistem > Pengaturan Admin**.
Jika item tersebut tidak ditampilkan, jentikkan layar ke atas untuk menampilkannya.
3. Sentuh **Sandi Admin > Daftar**.
4. Masukkan kata sandi baru, kemudian sentuh **OK**.
5. Masukkan lagi kata sandi, kemudian sentuh **OK**.
6. Sentuh **OK** di layar konfirmasi.
Layar pengaturan administrator ditampilkan.
7. Sentuh **Pengaturan Penguncian**, kemudian sentuh **OK** di layar konfirmasi.
Pengaturan Penguncian diatur ke **Aktif**, dan kata sandi administrator akan diminta ketika Anda mengoperasikan item menu yang terkunci.

Catatan:

- Jika Anda mengatur **Pengaturan > Pengaturan Umum > Batas Waktu Operasi** ke **Aktif**, scanner akan mengeluarkan Anda setelah sekian waktu tidak ada aktivitas pada panel kontrol.
- Anda dapat mengubah atau menghapus kata sandi administrator ketika memilih **Ubah** atau **Atur Ulang** di layar **Sandi Admin** kemudian masukkan kata sandi administrator.

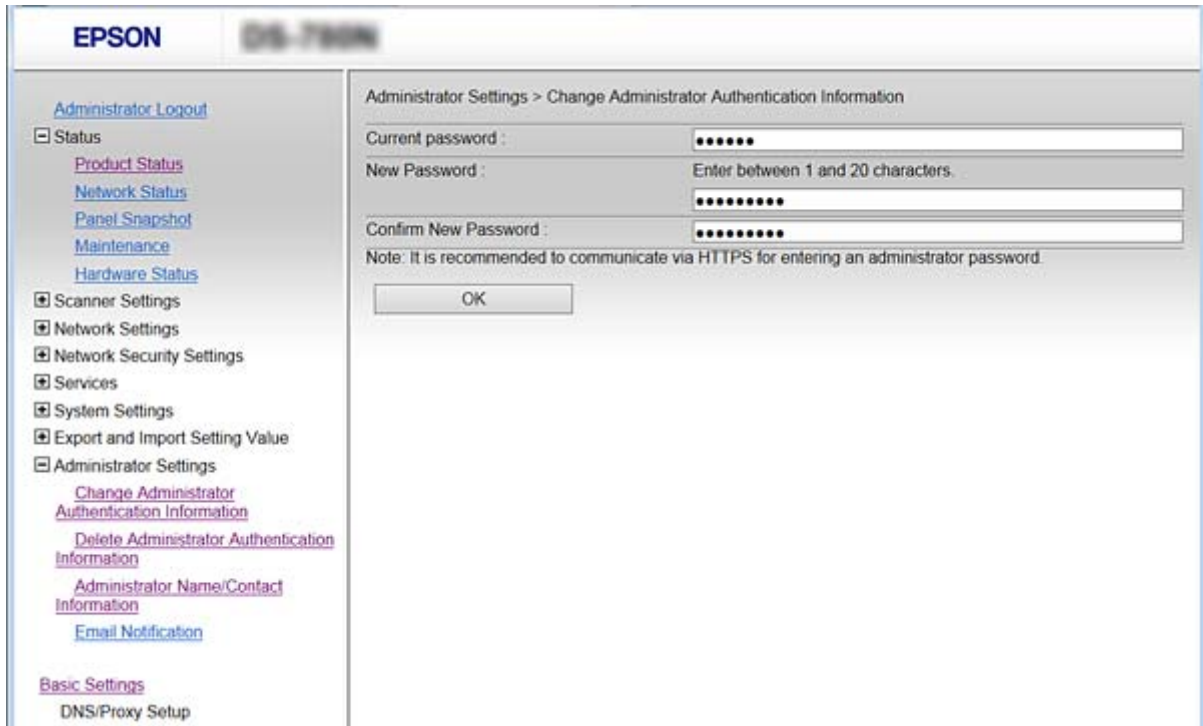
Mengonfigurasi Kata Sandi Administrator Menggunakan Web Config

Anda dapat mengatur kata sandi administrator menggunakan Web Config.

1. Akses Web Config lalu pilih **Administrator Settings > Change Administrator Authentication Information**.

Pengaturan Keamanan Dasar

- Masukkan kata sandi ke **New Password** dan **Confirm New Password**. Masukkan nama pengguna, jika perlu. Jika Anda ingin mengubah kata sandi menjadi yang baru, masukkan kata sandi saat ini.



- Pilih OK.

Catatan:

- Untuk mengatur atau mengubah item menu yang terkunci, klik **Administrator Login**, kemudian masukkan kata sandi administrator.
- Untuk menghapus kata sandi administrator, klik **Administrator Settings > Delete Administrator Authentication Information**, lalu masukkan kata sandi administrator.

Informasi Terkait

➔ [“Mengakses Web Config” pada halaman 23](#)

Item yang Dapat Dikunci oleh Kata Sandi Administrator

Administrator memiliki hak khusus untuk mengatur dan mengubah semua fitur pada perangkat.

Selain itu, jika Anda telah mengatur kata sandi administrator pada perangkat, Anda dapat menguncinya sehingga Anda tidak dapat mengubah poin-poin yang berhubungan dengan pengelolaan perangkat.

Berikut adalah item-item yang dapat dikontrol oleh administrator.

Item	Keterangan
Pengaturan scanner	Pengaturan deteksi pemasukan ganda dan mode kecepatan rendah.

Pengaturan Keamanan Dasar

Item	Keterangan
Pengaturan koneksi Ethernet	Mengubah nama perangkat dan alamat IP, pengaturan server DNS atau server proksi, dan perubahan pengaturan terkait koneksi jaringan.
Pengaturan layanan pengguna	Pengaturan terkait pengendalian protokol komunikasi, pemindaian Jaringan, dan layanan Document Capture Pro.
Pengaturan server email	Pengaturan server email yang menjadi lawan komunikasi langsung perangkat.
Pengaturan keamanan	Pengaturan keamanan jaringan seperti komunikasi SSL/TLS, pemfilteran IPsec/IP, dan IEEE802.1X.
Pembaruan Sertifikat Root	Pembaruan sertifikat root diperlukan untuk autentikasi Document Capture Pro Server dan pembaruan firmware dari Web Config.
Pembaruan firmware	Memeriksa dan memperbarui firmware perangkat.
Pengaturan waktu dan timer	Waktu peralihan menuju kondisi sleep (tidur), pematian daya otomatis, tanggal/waktu, timer terkait kenonaktifan, pengaturan lain terkait timer.
Pengembalian pengaturan default	Pengaturan untuk scanner agar diatur ulang ke pengaturan pabrik.
Pengaturan administrator	Mengatur kunci administrator atau kata sandi administrator.
Pengaturan perangkat bersertifikasi	Mengatur ID perangkat autentikasi. Atur ketika menggunakan scanner pada sistem autentikasi yang mendukung perangkat autentikasi.

Mengendalikan protokol

Anda dapat memindai menggunakan berbagai jalan dan protokol. Anda juga dapat menggunakan pemindaian jaringan dari komputer jaringan dengan jumlah yang tidak ditentukan. Misalnya, Anda dapat memindai hanya melalui jalur dan protokol yang sudah ditentukan. Anda dapat mengurangi risiko keamanan yang tidak disengaja dengan membatasi pemindaian dari jalur tertentu atau dengan mengendalikan fungsi yang tersedia.

Konfigurasi pengaturan protokol.

1. Akses Web Config lalu pilih **Services > Protocol**.
2. Konfigurasi masing-masing item.
3. Klik **Next**.
4. Klik **OK**.

Pengaturan diterapkan ke scanner.

Informasi Terkait

- ➔ [“Mengakses Web Config” pada halaman 23](#)
- ➔ [“Protokol yang dapat Anda Aktifkan atau Nonaktifkan” pada halaman 36](#)
- ➔ [“Item Pengaturan Protokol” pada halaman 37](#)

Pengaturan Keamanan Dasar

Protokol yang dapat Anda Aktifkan atau Nonaktifkan

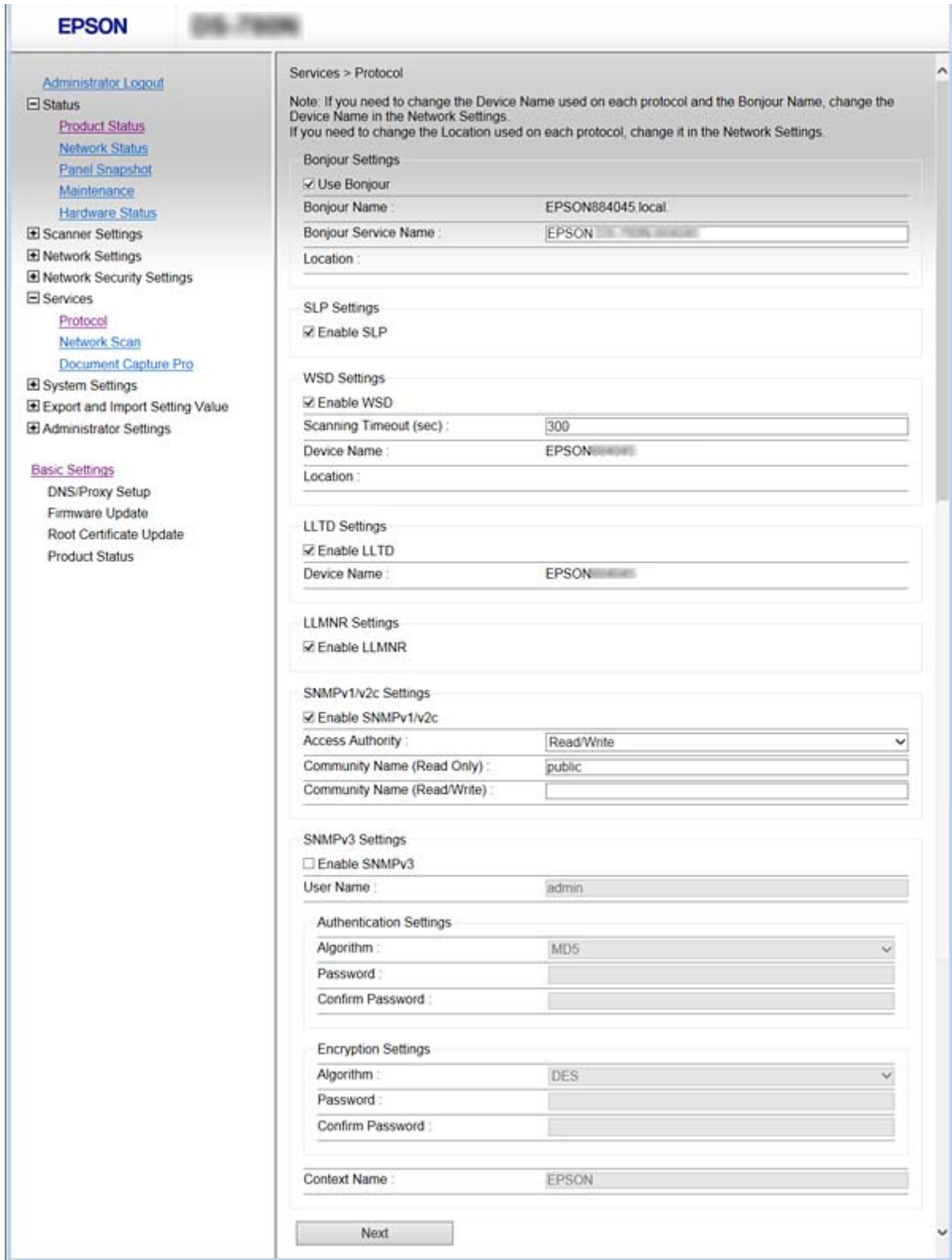
Protokol	Keterangan
Bonjour Settings	Anda dapat menentukan apakah akan menggunakan Bonjour atau tidak. Bonjour digunakan untuk mencari perangkat, scanner, dan sebagainya.
SLP Settings	Anda dapat mengaktifkan atau menonaktifkan fungsi SLP. SLP digunakan untuk Epson Scan 2 dan pencarian jaringan di EpsonNet Config.
WSD Settings	Anda dapat mengaktifkan atau menonaktifkan fungsi WSD. Saat fungsi ini diaktifkan, Anda dapat menambahkan perangkat WSD atau memindai dari port WSD.
LLTD Settings	Anda dapat mengaktifkan atau menonaktifkan fungsi LLTD. Saat fungsi ini diaktifkan, fungsi ditampilkan di peta jaringan Windows.
LLMNR Settings	Anda dapat mengaktifkan atau menonaktifkan fungsi LLMNR. Saat fungsi ini diaktifkan, Anda dapat menggunakan resolusi nama tanpa NetBIOS meskipun Anda tidak dapat menggunakan DNS.
SNMPv1/v2c Settings	Anda dapat menentukan untuk mengaktifkan SNMPv1/v2c atau tidak. Fungsi ini digunakan untuk menyiapkan perangkat, pemantauan, dan sebagainya.
SNMPv3 Settings	Anda dapat menentukan untuk mengaktifkan SNMPv3 atau tidak. Fungsi ini digunakan untuk mengatur perangkat terenkripsi, pemantauan, dan sebagainya.

Informasi Terkait

- ➔ [“Mengendalikan protokol” pada halaman 35](#)
- ➔ [“Item Pengaturan Protokol” pada halaman 37](#)

Pengaturan Keamanan Dasar

Item Pengaturan Protokol



Item	Nilai pengaturan dan Deskripsi
Bonjour Settings	

Pengaturan Keamanan Dasar

Item	Nilai pengaturan dan Deskripsi
Use Bonjour	Pilih opsi ini untuk mencari atau menggunakan perangkat melalui Bonjour.
Bonjour Name	Tampilkan nama Bonjour.
Bonjour Service Name	Anda dapat menampilkan dan mengatur nama layanan Bonjour.
Location	Tampilkan nama lokasi Bonjour.
SLP Settings	
Enable SLP	Pilih opsi ini untuk mengaktifkan fungsi SLP. Opsi ini digunakan untuk pencarian jaringan di Epson Scan 2 dan EpsonNet Config.
WSD Settings	
Enable WSD	Pilih opsi ini untuk memungkinkan penambahan perangkat menggunakan WSD, serta pencetakan dan pemindaian dari port WSD.
Scanning Timeout (sec)	Masukkan nilai batas waktu komunikasi untuk pemindaian WSD antara 3 hingga 3.600 detik.
Device Name	Tampilkan nama perangkat WSD.
Location	Tampilkan nama lokasi WSD.
LLTD Settings	
Enable LLTD	Pilih opsi ini untuk mengaktifkan LLTD. Scanner ditampilkan di dalam peta jaringan Windows.
Device Name	Tampilkan nama perangkat LLTD.
LLMNR Settings	
Enable LLMNR	Pilih opsi ini untuk mengaktifkan LLMNR. Anda dapat menggunakan resolusi nama tanpa NetBIOS meskipun Anda tidak dapat menggunakan DNS.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	Pilih untuk mengaktifkan SNMPv1/v2c. Yang ditampilkan hanyalah scanner yang mendukung SNMPv3.
Access Authority	Tentukan otoritas akses ketika SNMPv1/v2c diaktifkan. Pilih Read Only atau Read/Write .
Community Name (Read Only)	Masukkan 0 hingga 32 ASCII (0x20 hingga 0x7E) karakter.
Community Name (Read/Write)	Masukkan 0 hingga 32 ASCII (0x20 hingga 0x7E) karakter.
SNMPv3 Settings	
Enable SNMPv3	SNMPv3 diaktifkan bila kotak ini dicentang.
User Name	Masukkan antara 1 hingga 32 karakter menggunakan karakter 1 bita.
Authentication Settings	

Pengaturan Keamanan Dasar

Item	Nilai pengaturan dan Deskripsi
Algorithm	Pilih algoritme autentikasi untuk SNMPv3.
Password	Pilih kata sandi autentikasi untuk SNMPv3. Masukkan antara 8 hingga 32 karakter dalam ASCII (0x20–0x7E). Jika poin ini tidak ingin Anda tetapkan, kosongkan.
Confirm Password	Masukkan kata sandi yang Anda konfigurasi untuk konfirmasi.
Encryption Settings	
Algorithm	Pilih algoritme enkripsi untuk SNMPv3.
Password	Pilih kata sandi enkripsi untuk SNMPv3. Masukkan antara 8 hingga 32 karakter dalam ASCII (0x20–0x7E). Jika poin ini tidak ingin Anda tetapkan, kosongkan.
Confirm Password	Masukkan kata sandi yang Anda konfigurasi untuk konfirmasi.
Context Name	Masukkan sepanjang 32 karakter atau kurang dalam format Unicode (UTF-8). Jika poin ini tidak ingin Anda tetapkan, kosongkan. Jumlah karakter yang dapat dimasukkan berbeda-beda tergantung bahasa.

Informasi Terkait

- ➔ [“Mengendalikan protokol” pada halaman 35](#)
- ➔ [“Protokol yang dapat Anda Aktifkan atau Nonaktifkan” pada halaman 36](#)

Pengaturan Operasi dan Pengelolaan

Bab ini menjelaskan item-item terkait pengoperasian dan pengelolaan perangkat sehari-hari.

Mengonfirmasi Informasi Perangkat

Anda dapat memeriksa informasi tentang perangkat yang beroperasi berikut dari **Status** dengan menggunakan Web Config.

- Product Status
Memeriksa bahasa, status, nomor produk, alamat MAC, dan lain-lain.
- Network Status
Memeriksa informasi tentang status koneksi jaringan, alamat IP, server DNS, dan lain-lain.
- Panel Snapshot
Menampilkan snapshot gambar layar yang ditampilkan pada panel kontrol perangkat.
- Maintenance
Periksa Tanggal Mulai, Informasi Pemindaian, dll.
- Hardware Status
Periksa status scanner.

Informasi Terkait

➔ [“Mengakses Web Config” pada halaman 23](#)

Mengelola Perangkat (Epson Device Admin)

Anda dapat mengelola dan mengoperasikan banyak perangkat menggunakan Epson Device Admin. Epson Device Admin dapat Anda gunakan untuk mengelola perangkat-perangkat yang berada di beragam jaringan. Berikut adalah fitur-fitur pengelolaan utama yang dapat Anda manfaatkan.

Untuk informasi selengkapnya tentang fungsi dan tentang penggunaan perangkat lunak, baca dokumentasi atau bantuan Epson Device Admin.

- Menemukan perangkat
Anda dapat menemukan perangkat di jaringan, lalu memasukkannya ke daftar. Jika perangkat Epson seperti printer dan scanner terhubung ke segmen jaringan yang sama dengan komputer administrator, Anda dapat menemukannya meskipun belum diberi alamat IP.
Anda juga dapat menemukan perangkat yang terhubung ke komputer di jaringan melalui kabel USB. Anda harus menginstal Epson Device USB Agent di komputer tersebut.
- Mengatur perangkat
Anda dapat membuat sebuah templat yang berisi item pengaturan seperti antarmuka jaringan dan sumber kertas, dan menerapkannya ke perangkat lain sebagai pengaturan bersama. Jika terhubung ke jaringan, Anda dapat menentukan alamat IP pada suatu perangkat yang belum diberi alamat IP.

Pengaturan Operasi dan Pengelolaan

Memantau perangkat

Anda dapat memperoleh status dan informasi perangkat di jaringan secara terperinci dan teratur. Anda juga dapat memantau perangkat yang terhubung ke komputer di jaringan melalui kabel USB dan perangkat dari perusahaan lain yang telah dimasukkan ke daftar perangkat. Untuk memantau perangkat yang terhubung melalui kabel USB, Anda harus menginstal Epson Device USB Agent.

Mengelola peringatan

Anda dapat memantau peringatan tentang status perangkat dan produk habis pakai. Sistem akan otomatis mengirim email pemberitahuan kepada administrator berdasarkan kriteria yang sudah ditetapkan.

Mengelola laporan

Anda dapat membuat laporan teratur ketika sistem mengumpulkan data tentang pemakaian perangkat dan produk habis pakai. Kemudian, Anda dapat menyimpan laporan-laporan ini dan mengirimkannya melalui email.

Informasi Terkait

➔ [“Epson Device Admin” pada halaman 55](#)

Menerima Pemberitahuan Email Saat Aktivitas Terjadi

Tentang Pemberitahuan Email

Anda dapat menggunakan fitur ini untuk menerima peringatan melalui email ketika terjadi suatu peristiwa. Anda dapat mendaftarkan sampai 5 alamat email dan memilih aktivitas yang ingin Anda dapatkan pemberituannya.

Server email harus dikonfigurasi agar menggunakan fungsi ini.

Informasi Terkait

➔ [“Mengonfigurasi Server Email” pada halaman 42](#)

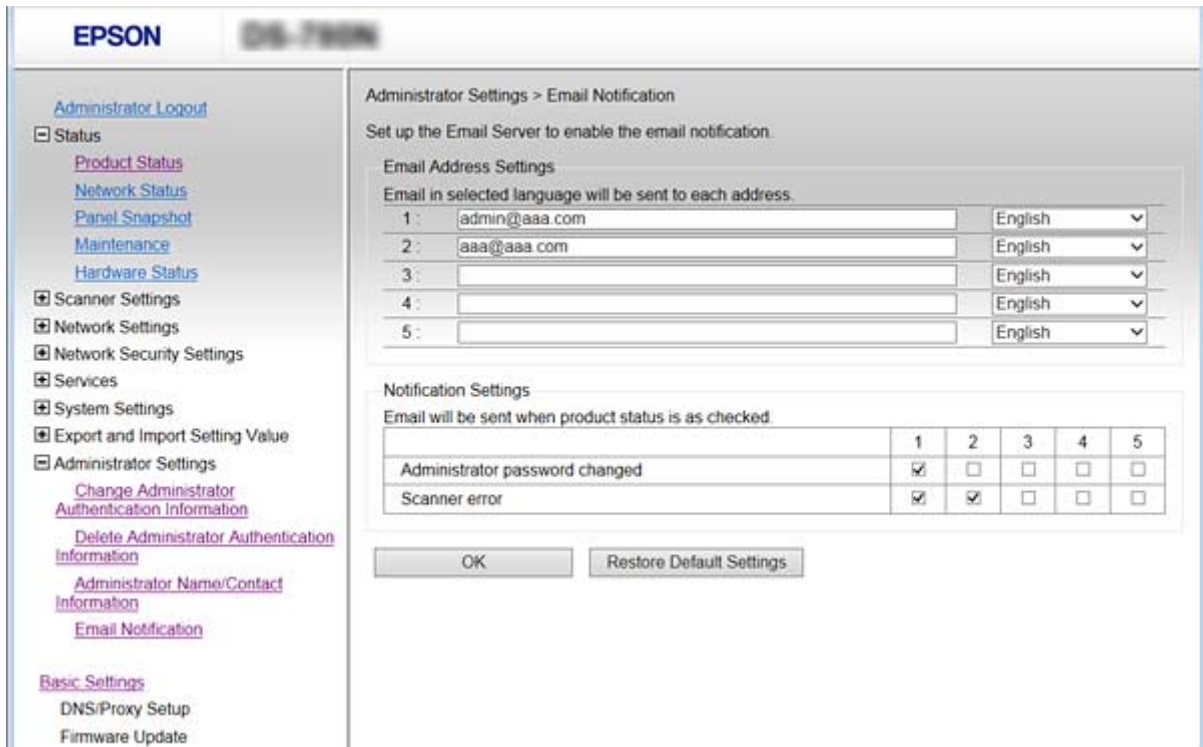
Mengonfigurasi Pemberitahuan Email

Untuk menggunakan fitur tersebut, Anda harus mengonfigurasi server pesan.

1. Akses Web Config lalu pilih **Administrator Settings > Email Notification**.
2. Masukkan alamat email yang Anda inginkan untuk menerima pemberitahuan email.
3. Pilih bahasa untuk pemberitahuan email.

Pengaturan Operasi dan Pengelolaan

- Periksa kotak untuk memilih bahasa pemberitahuan email.



- Klik OK.

Informasi Terkait

- ➔ “Mengakses Web Config” pada halaman 23
- ➔ “Mengonfigurasi Server Email” pada halaman 42

Mengonfigurasi Server Email

Periksa hal-hal berikut sebelum mengonfigurasi.

- Scanner tersambung ke jaringan.
- Informasi server email komputer.

- Akses Web Config lalu pilih **Network Settings > Email Server > Basic**.
- Masukkan angka untuk setiap item.
- Pilih **OK**.

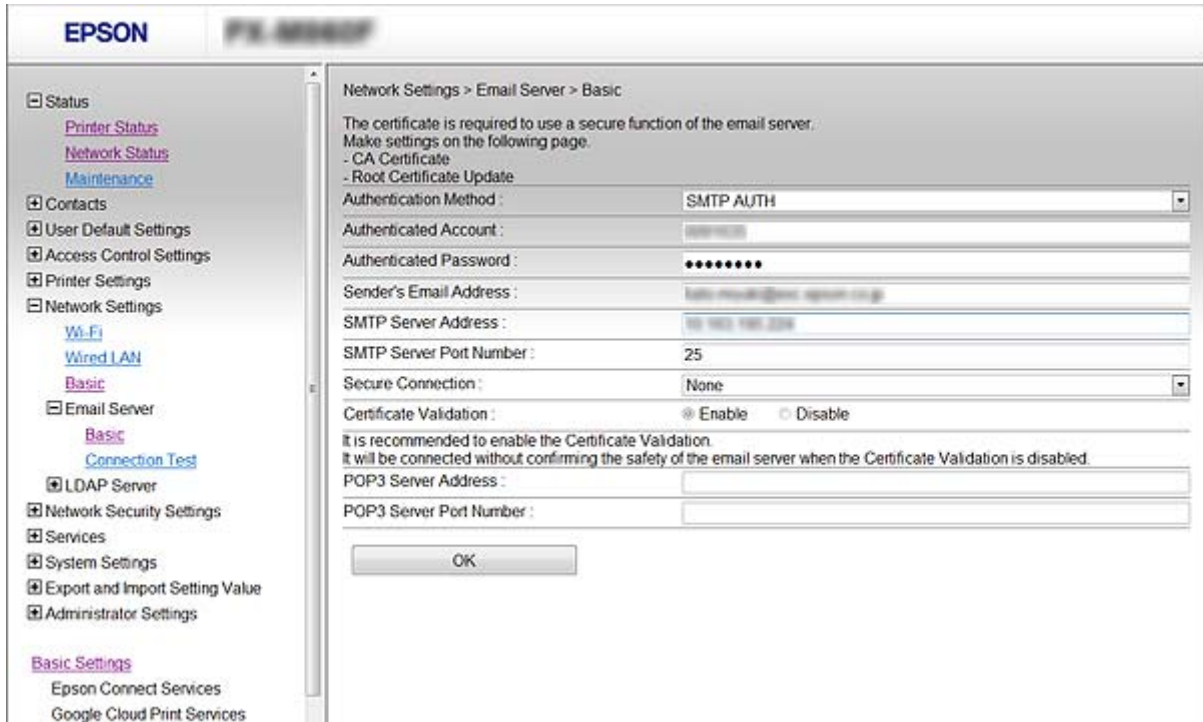
Pengaturan yang telah Anda pilih akan ditampilkan.

Informasi Terkait

- ➔ “Mengakses Web Config” pada halaman 23
- ➔ “Item Pengaturan Server Email” pada halaman 43

Pengaturan Operasi dan Pengelolaan

Item Pengaturan Server Email



Item	Pengaturan dan Penjelasan	
Authentication Method	Off	Otentikasi dinonaktifkan saat berkomunikasi dengan server email.
	SMTP AUTH	Mengharuskan bahwa server email mendukung Otentikasi SMTP.
	POP before SMTP	Konfigurasi server POP3 saat memilih metode ini.
Authenticated Account	Jika Anda memilih SMTP AUTH atau POP before SMTP sebagai Authentication Method , masukkan nama akun yang diotentikasi antara 0 hingga 255 karakter dalam ASCII (0x20–0x7E).	
Authenticated Password	Jika Anda memilih SMTP AUTH atau POP before SMTP sebagai Authentication Method , masukkan kata sandi yang diotentikasi antara 0 hingga 20 karakter menggunakan A–Z a–z 0–9 ! # \$ % & ' * + - . / = ? ^ _ { } ~ @.	
Sender's Email Address	Masukkan alamat email pengirim. Masukkan antara 0 hingga 255 karakter dalam ASCII (0x20–0x7E) kecuali untuk : () < > [] ; ¥. Tanda titik "." tidak dapat menjadi karakter pertama.	
SMTP Server Address	Masukkan antara 0 hingga 255 karakter menggunakan A–Z a–z 0–9 . - . Anda dapat menggunakan format IPv4 atau FQDN.	
SMTP Server Port Number	Masukkan angka antara 1 hingga 65535.	

Pengaturan Operasi dan Pengelolaan

Item	Pengaturan dan Penjelasan	
Secure Connection	Tetapkan metode koneksi aman untuk server email.	
	None	Jika Anda memilih POP before SMTP pada Authentication Method , metode koneksi diatur ke None .
	SSL/TLS	Metode ini tersedia saat Authentication Method diatur ke Off atau SMTP AUTH .
	STARTTLS	Metode ini tersedia saat Authentication Method diatur ke Off atau SMTP AUTH .
Certificate Validation	Sertifikat divalidasi saat sertifikat ini diaktifkan. Kami menyarankan agar sertifikat diatur ke Enable .	
POP3 Server Address	Jika Anda memilih POP before SMTP sebagai Authentication Method , masukkan alamat server POP3 antara 0 hingga 255 karakter menggunakan A-Z a-z 0-9 . - . Anda dapat menggunakan format IPv4 atau FQDN.	
POP3 Server Port Number	Jika Anda memilih POP before SMTP sebagai Authentication Method , masukkan angka antara 1 hingga 65535.	

Informasi Terkait

➔ [“Mengonfigurasi Server Email” pada halaman 42](#)

Periksa Koneksi Server Email

1. Akses Web Config lalu pilih **Network Settings > Email Server > Connection Test**.
2. Pilih **Start**.
Uji koneksi ke server surat dimulai. Setelah pengujian, laporan pemeriksaan ditampilkan.

Informasi Terkait

- ➔ [“Mengakses Web Config” pada halaman 23](#)
➔ [“Referensi Uji Koneksi Server Email” pada halaman 44](#)

Referensi Uji Koneksi Server Email

Pesan	Penjelasan
Connection test was successful.	Pesan ini muncul saat koneksi dengan server berhasil.
SMTP server communication error. Check the following. - Network Settings	Pesan ini muncul saat <ul style="list-style-type: none"> <input type="checkbox"/> Scanner tidak tersambung ke jaringan <input type="checkbox"/> Server SMTP tidak berfungsi <input type="checkbox"/> Koneksi jaringan terputus saat berkomunikasi <input type="checkbox"/> Menerima data yang belum lengkap

Pengaturan Operasi dan Pengelolaan

Pesan	Penjelasan
POP3 server communication error. Check the following. - Network Settings	<p>Pesan ini muncul saat</p> <ul style="list-style-type: none"> <input type="checkbox"/> Scanner tidak tersambung ke jaringan <input type="checkbox"/> Server POP3 tidak berfungsi <input type="checkbox"/> Koneksi jaringan terputus saat berkomunikasi <input type="checkbox"/> Menerima data yang belum lengkap
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	<p>Pesan ini muncul saat</p> <ul style="list-style-type: none"> <input type="checkbox"/> Menghubungkan ke server DNS gagal <input type="checkbox"/> Resolusi nama untuk server SMTP gagal
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	<p>Pesan ini muncul saat</p> <ul style="list-style-type: none"> <input type="checkbox"/> Menghubungkan ke server DNS gagal <input type="checkbox"/> Resolusi nama untuk server POP3 gagal
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Pesan ini muncul saat otentikasi server SMTP gagal.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Pesan ini muncul saat otentikasi server POP3 gagal.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Pesan ini muncul saat Anda mencoba berkomunikasi dengan protokol yang tidak didukung.
Connection to SMTP server failed. Change Secure Connection to None.	Pesan ini muncul saat terjadi ketidakcocokan SMTP antara server dan klien, atau saat server tidak mendukung koneksi aman SMTP (koneksi SSL).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Pesan ini muncul saat terjadi ketidakcocokan SMTP antara server dan klien, atau saat server meminta untuk menggunakan koneksi SSL/TLS untuk koneksi aman SMTP.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Pesan ini muncul saat terjadi ketidakcocokan SMTP antara server dan klien, atau saat server meminta untuk menggunakan koneksi STARTTLS untuk koneksi aman SMTP.
The connection is untrusted. Check the following. - Date and Time	Pesan ini muncul saat pengaturan tanggal dan waktu scanner keliru atau sertifikat sudah kedaluwarsa.
The connection is untrusted. Check the following. - CA Certificate	Pesan ini muncul saat scanner tidak memiliki sertifikat root yang sesuai dengan server atau CA Certificate belum diimpor.
The connection is not secured.	Pesan ini muncul saat sertifikat yang didapatkan rusak.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Pesan ini muncul saat terjadi ketidakcocokan metode otentikasi antara server dan klien. Server mendukung SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Pesan ini muncul saat terjadi ketidakcocokan metode otentikasi antara server dan klien. Server tidak mendukung SMTP AUTH.

Pengaturan Operasi dan Pengelolaan

Pesan	Penjelasan
Sender's Email Address is incorrect. Change to the email address for your email service.	Pesan ini muncul saat alamat Email pengirim tertentu salah.
Cannot access the product until processing is complete.	Pesan ini muncul saat scanner sedang sibuk.

Informasi Terkait

➔ [“Periksa Koneksi Server Email” pada halaman 44](#)

Memperbarui Firmware

Memperbarui Firmware Menggunakan Web Config

Memperbarui firmware menggunakan Web Config. Perangkat harus terhubung ke Internet.

1. Akses Web Config lalu pilih **Basic Settings > Firmware Update**.
2. Klik **Start**.
Konfirmasi firmware terbuka, dan informasi firmware ditampilkan apabila ada firmware yang lebih baru.
3. Klik **Start**, lalu ikuti petunjuk di layar.

Catatan:

Anda juga dapat memperbarui firmware menggunakan Epson Device Admin. Anda dapat melihat informasi firmware di daftar perangkat. Ini bermanfaat ketika Anda ingin memperbarui firmware pada beberapa perangkat. Lihat panduan atau bantuan Epson Device Admin untuk keterangan lebih lengkap.

Informasi Terkait

➔ [“Mengakses Web Config” pada halaman 23](#)

➔ [“Epson Device Admin” pada halaman 55](#)

Memperbarui Firmware Menggunakan Epson Firmware Updater

Anda dapat mengunduh firmware perangkat dari situs web Epson, dan menghubungkan perangkat ke komputer melalui kabel USB untuk memperbarui firmware. Jika Anda tidak dapat melakukan pembaruan melalui jaringan, cobalah metode berikut.

1. Buka situs web Epson dan unduh firmware.
2. Menggunakan kabel USB, hubungkan perangkat ke komputer yang berisi firmware unduhan tadi.
3. Klik dua kali file unduhan yang berekstensi .exe.
Epson Firmware Updater dijalankan.
4. Ikuti petunjuk pada layar.

Membuat Cadangan Pengaturan

Dengan mengekspor item-item pengaturan pada Web Config, Anda dapat menyalin item-item tersebut ke scanner lain.

Ekspor pengaturan

Ekspor setiap pengaturan untuk scanner.

1. Akses Web Config, lalu pilih **Export and Import Setting Value > Export**.

2. Pilih pengaturan yang ingin Anda ekspor.

Pilih pengaturan yang ingin Anda ekspor. Jika Anda memilih kategori induk, subkategorinya juga dipilih.

Akan tetapi, subkategori yang menyebabkan kesalahan akibat duplikasi di dalam jaringan yang sama (seperti alamat IP dan sebagainya) tidak dapat dipilih.

3. Masukkan kata sandi untuk mengenkripsi file yang diekspor.

Anda memerlukan kata sandi untuk mengimpor file. Kosongkan ini jika Anda tidak ingin mengenkripsi file.

4. Klik **Export**.

 **Penting:**

*Jika Anda ingin mengekspor pengaturan jaringan scanner seperti nama scanner dan alamat IP, pilih **Enable to select the individual settings of device** dan pilih lebih banyak item. Hanya gunakan nilai yang dipilih untuk scanner pengganti.*

Informasi Terkait

➔ [“Mengakses Web Config” pada halaman 23](#)

Impor pengaturan

Impor file Web Config yang diekspor ke scanner.

 **Penting:**

Ketika mengimpor nilai yang mencakup informasi individual seperti nama scanner atau alamat IP, pastikan tidak ada alamat IP yang sama di jaringan tersebut. Jika alamat IP tumpang tindih (overlap), scanner tidak menunjukkan nilainya.

1. Akses Web Config, lalu pilih **Export and Import Setting Value > Import**.

2. Pilih file yang diekspor, lalu masukkan kata sandi yang dienkripsi.

3. Klik **Next**.

4. Pilih pengaturan yang ingin Anda impor, lalu klik **Next**.

5. Klik **OK**.

Pengaturan Operasi dan Pengelolaan

Pengaturan diterapkan ke scanner.

Informasi Terkait

➔ [“Mengakses Web Config”](#) pada halaman 23

Memecahkan Masalah

Tips untuk Memecahkan Masalah

Anda dapat menemukan informasi lebih lanjut dalam buku petunjuk berikut.

Panduan Pengguna

Memberikan petunjuk tentang penggunaan pemindai, pemeliharaan, dan pemecahan masalah.

Memeriksa Log Server dan Perangkat Jaringan

Apabila ada masalah dengan koneksi jaringan, Anda dapat mengidentifikasi penyebabnya dengan memeriksa log server email, server LDAP, dan lain-lain, memeriksa status menggunakan log jaringan dari log dan perintah peralatan sistem, misalnya router.

Memulai Pengaturan Jaringan

Memulihkan Pengaturan Jaringan dari Panel Kontrol

Anda dapat mengembalikan semua pengaturan jaringan ke nilai asalnya.

1. Sentuh **Pengaturan** di layar beranda.
2. Sentuh **Administrasi Sistem** > **Kembalikan Default** > **Pengaturan Jaringan**.
3. Lihat pesan yang muncul, kemudian sentuh **Ya**.
4. Apabila pesan penyelesaian ditampilkan, sentuh **Tutup**.

Layar secara otomatis menutup setelah beberapa waktu jika Anda tidak menyentuh **Tutup**.

Memeriksa Komunikasi antara Perangkat dan Komputer

Memeriksa Koneksi dengan Perintah Ping — Windows

Anda dapat menggunakan perintah Ping untuk memastikan komputer Anda terhubung ke scanner. Ikuti langkah-langkah di bawah ini untuk memeriksa koneksi menggunakan perintah Ping.

1. Periksa alamat IP scanner untuk koneksi yang ingin Anda periksa.
Anda dapat melihatnya menggunakan Epson Scan 2.

Memecahkan Masalah

2. Tampilkan layar command prompt komputer.

❑ Windows 10

Klik kanan tombol start atau tekan dan tahan, lalu pilih **Prompt Perintah**.

❑ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012

Tampilkan layar aplikasi, lalu pilih **Prompt Perintah**.

❑ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 atau sebelumnya

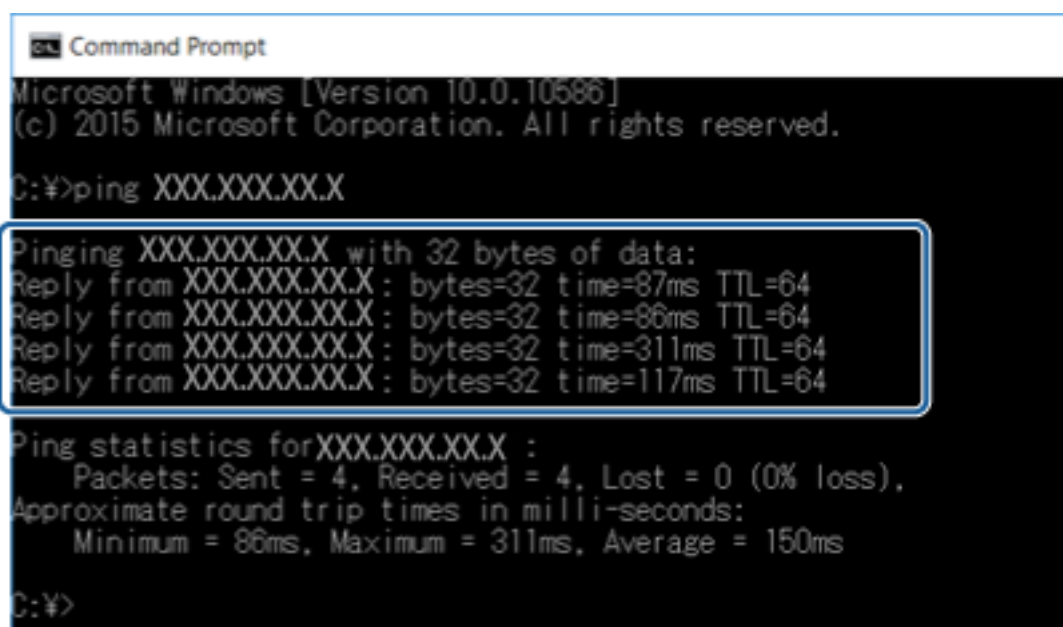
Klik tombol start, pilih **Semua Program** atau **Program > Aksesori > Prompt Perintah**.

3. Ketik “ping xxx.xxx.xxx.xxx”, lalu tekan tombol Enter.

Masukkan alamat IP scanner untuk xxx.xxx.xxx.xxx.

4. Periksa status komunikasi.

Apabila scanner dan komputer saling berkomunikasi, pesan berikut akan ditampilkan.



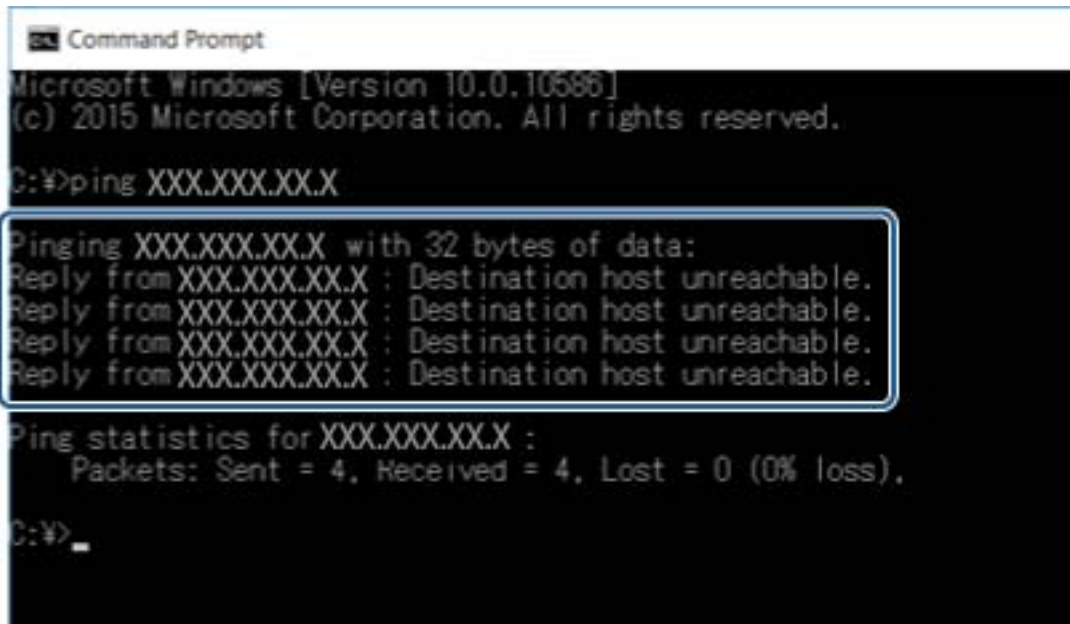
```
Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.
C:\>ping XXX.XXX.XX.X

Pinging XXX.XXX.XX.X with 32 bytes of data:
Reply from XXX.XXX.XX.X: bytes=32 time=87ms TTL=64
Reply from XXX.XXX.XX.X: bytes=32 time=86ms TTL=64
Reply from XXX.XXX.XX.X: bytes=32 time=311ms TTL=64
Reply from XXX.XXX.XX.X: bytes=32 time=117ms TTL=64

Ping statistics for XXX.XXX.XX.X :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 86ms, Maximum = 311ms, Average = 150ms
C:\>
```

Memecahkan Masalah

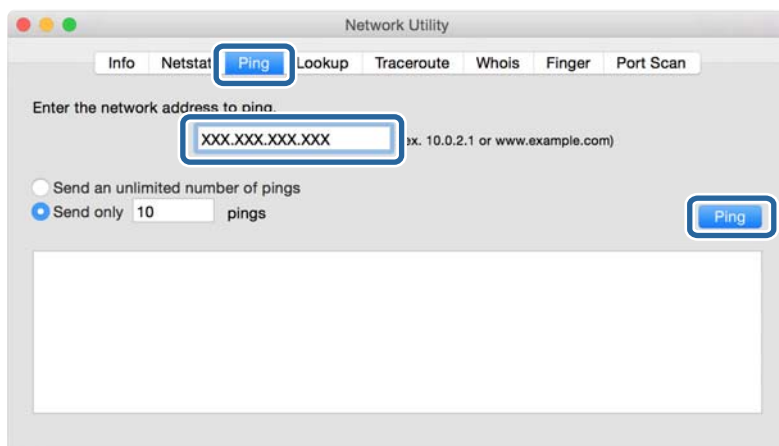
Apabila scanner dan komputer tidak saling berkomunikasi, pesan berikut akan ditampilkan.



Memeriksa Koneksi dengan Perintah Ping — Mac OS

Anda dapat menggunakan perintah Ping untuk memastikan komputer Anda terhubung ke scanner. Ikuti langkah-langkah di bawah ini untuk memeriksa koneksi menggunakan perintah Ping.

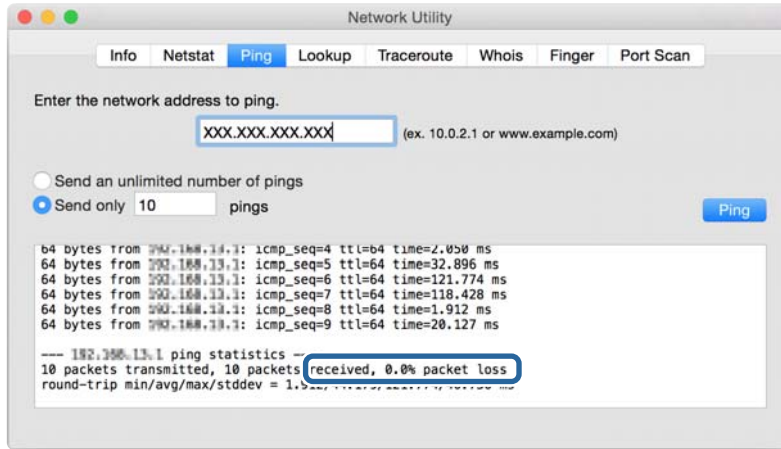
1. Periksa alamat IP scanner untuk koneksi yang ingin Anda periksa.
Anda dapat melihatnya menggunakan Epson Scan 2.
2. Jalankan Utilitas Jaringan/Network Utility.
Masukkan "Network Utility" dalam **Spotlight**.
3. Klik tab **Ping**, masukkan alamat IP yang Anda dapatkan di langkah 1, lalu klik **Ping**.



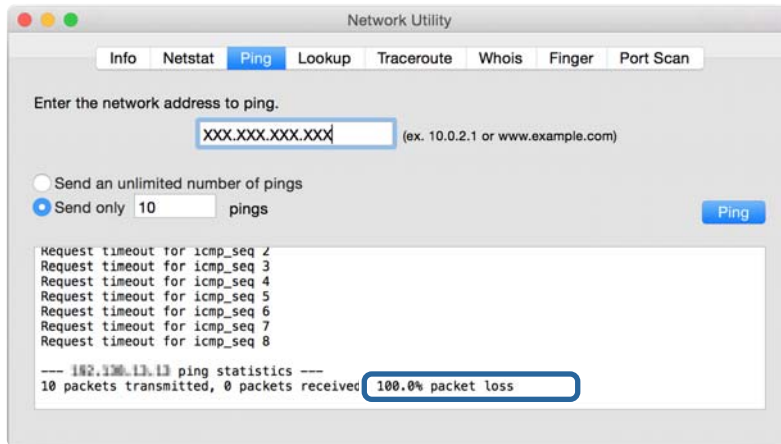
Memecahkan Masalah

4. Periksa status komunikasi.

Apabila scanner dan komputer saling berkomunikasi, pesan berikut akan ditampilkan.



Apabila scanner dan komputer tidak saling berkomunikasi, pesan berikut akan ditampilkan.



Masalah Menggunakan Perangkat Lunak Jaringan

Tidak Dapat Mengakses Web Config

Apakah alamat IP scanner sudah dikonfigurasi dengan benar?

Konfigurasi alamat IP menggunakan Epson Device Admin atau EpsonNet Config.

Apakah browser Anda mendukung enkripsi massal untuk Encryption Strength untuk SSL/TLS?

Enkripsi massal untuk Encryption Strength untuk SSL/TLS adalah sebagai berikut. Web Config hanya dapat diakses di dalam browser yang mendukung enkripsi massal berikut. Periksa dukungan enkripsi browser Anda.

- 80bit: AES256/AES128/3DES
- 112bit: AES256/AES128/3DES
- 128bit: AES256/AES128

Memecahkan Masalah

- 192bit: AES256
- 256bit: AES256

Pesan “Kedaluwarsa” muncul ketika mengakses Web Config menggunakan komunikasi SSL (https).

Jika sertifikat kedaluwarsa, dapatkan sertifikat kembali. Jika pesan muncul sebelum tanggal kedaluwarsanya, pastikan bahwa tanggal scanner sudah dikonfigurasi dengan benar.

Pesan “Nama sertifikat keamanan tidak sesuai...” muncul ketika sedang mengakses Web Config menggunakan komunikasi SSL (https).

Alamat IP scanner yang dimasukkan untuk **Common Name** untuk membuat sertifikat bertanda tangan sendiri atau CSR tidak sesuai dengan alamat yang dimasukkan ke dalam browser. Dapatkan dan impor sertifikat kembali atau ubah nama scanner.

Scanner akan diakses melalui server proksi.

Jika Anda menggunakan server proksi dengan scanner Anda, Anda perlu mengonfigurasi pengaturan proksi browser Anda.

- Windows:

Pilih **Panel Kontrol > Jaringan dan Internet > Opsi Internet > Sambungan > Pengaturan LAN > Server proksi**, lalu konfigurasi untuk tidak menggunakan server proksi untuk alamat lokal.

- Mac OS:

Pilih **Preferensi Sistem > Jaringan > Tingkat Lanjut > Proksi**, lalu daftar ke alamat lokal untuk **Lewati pengaturan proksi untuk Host & Domain ini**.

Contoh:

192.168.1.*: Alamat lokal 192.168.1.XXX, subnet mask 255.255.255.0

192.168.*.*: Alamat lokal 192.168.XXX.XXX, subnet mask 255.255.0.0

Informasi Terkait

- ➔ [“Mengakses Web Config” pada halaman 23](#)
- ➔ [“Menentukan Alamat IP” pada halaman 15](#)
- ➔ [“Menentukan Alamat IP Menggunakan EpsonNet Config” pada halaman 56](#)

Nama model dan/atau alamat IP tidak ditampilkan di EpsonNet Config

Apakah Anda memilih Blokir, Batal, atau Matikan saat layar keamanan atau layar firewall Windows ditampilkan?

Jika Anda memilih **Blokir, Batal**, atau **Matikan**, alamat IP dan nama model tidak akan muncul di EpsonNet Config atau EpsonNet Setup.

Untuk memperbaiki ini, daftarkan EpsonNet Config sebagai pengecualian menggunakan firewall dan perangkat lunak keamanan komersial Windows. Jika Anda menggunakan antivirus atau program keamanan, tutup program tersebut, lalu cobalah menggunakan EpsonNet Config.

Memecahkan Masalah

Apakah pengaturan rehat kesalahan komunikasi terlalu pendek?

Jalankan EpsonNet Config, lalu pilih **Tools > Options > Timeout**, lalu naikkan lama waktu untuk pengaturan **Communication Error**. Ingatlah bahwa hal ini dapat menyebabkan EpsonNet Config berjalan lebih lambat.

Informasi Terkait

- ➔ [“Menjalankan EpsonNet Config — Windows”](#) pada halaman 56
- ➔ [“Menjalankan EpsonNet Config — Mac OS”](#) pada halaman 56

Lampiran

Pengenalan Perangkat Lunak Jaringan

Bagian berikut menjelaskan perangkat lunak yang mengonfigurasi dan mengelola perangkat.

Epson Device Admin

Epson Device Admin merupakan sebuah aplikasi yang memungkinkan Anda untuk menginstal perangkat di jaringan, lalu mengonfigurasi dan mengelola perangkat. Anda dapat mengambil informasi perangkat terperinci seperti status dan produk habis pakai, mengirim pemberitahuan, dan membuat laporan penggunaan perangkat. Anda juga dapat membuat sebuah templat yang berisi item pengaturan dan menerapkannya ke perangkat lain sebagai pengaturan bersama. Anda dapat mengunduh Epson Device Admin dari situs web pendukung Epson. Untuk informasi lebih lanjut, lihat dokumentasi atau bantuan dari Epson Device Admin.

Menjalankan Epson Device Admin (khusus untuk Windows)

Pilih **Semua Program > EPSON > Epson Device Admin > Epson Device Admin**.

Catatan:

Jika pemberitahuan firewall muncul, izinkan akses untuk Epson Device Admin.

EpsonNet Config

EpsonNet Config memungkinkan administrator untuk mengonfigurasi pengaturan jaringan scanner, seperti menetapkan alamat IP dan mengubah mode koneksi. Fitur pengaturan berkas didukung di Windows. Untuk informasi lebih lanjut, lihat dokumentasi atau bantuan dari EpsonNet Config.



Menjalankan EpsonNet Config — Windows

Pilih Semua Program > EpsonNet > EpsonNet Config SE > EpsonNet Config.

Catatan:

Jika pemberitahuan firewall muncul, izinkan akses untuk EpsonNet Config.

Menjalankan EpsonNet Config — Mac OS

Pilih Masuk ke > Aplikasi > Epson Software > EpsonNet > EpsonNet Config SE > EpsonNet Config.

EpsonNet SetupManager

EpsonNet SetupManager adalah perangkat lunak pembuat paket untuk instalasi scanner sederhana, seperti memasang dan mengonfigurasi driver scanner, dan memasang Document Capture Pro. Perangkat lunak ini memungkinkan administrator untuk membuat paket perangkat lunak yang unik dan menyalurkannya di antara grup.

Untuk informasi lebih lanjut, kunjungi situs web Epson regional Anda.

Menentukan Alamat IP Menggunakan EpsonNet Config

Anda dapat menentukan alamat IP scanner menggunakan EpsonNet Config. EpsonNet Config dapat Anda gunakan untuk menentukan alamat IP scanner yang belum ditentukan, setelah menghubungkannya dengan kabel Ethernet.

Menentukan Alamat IP Menggunakan Pengaturan Batch

Membuat File untuk Pengaturan Batch

Menggunakan alamat MAC dan nama model sebagai kuncinya, Anda dapat membuat file SYLK baru untuk mengatur alamat IP.

1. Buka aplikasi spreadsheet (seperti Microsoft Excel) atau editor teks.
2. Masukkan “Info_MACAddress”, “Info_ModelName”, dan “TCPIP_IPAddress” di baris pertama untuk nama-nama item pengaturan.

Masukkan item-item pengaturan untuk string teks berikut ini. Untuk membedakan huruf besar dan kecil dan karakter bita ganda/bitanya tunggal, jika hanya ada satu karakter yang berbeda, item tidak akan dikenali.

Masukkan nama item pengaturan seperti dijelaskan di bawah; jika tidak, EpsonNet Config tidak akan mengenali item pengaturan tersebut.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

Lampiran

- Masukkan alamat MAC, nama model, dan alamat IP untuk tiap antarmuka jaringan.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress
0000XXXX0001	ALC-XXXXX	192.168.100.102
0000XXXX0002	ALC-XXXXX	192.168.100.103
0000XXXX0003	ALC-XXXXX	192.168.100.104

- Masukkan nama dan simpan sebagai file SYLK (*.slk).

Melakukan Pengaturan Batch Menggunakan File Konfigurasi

Tentukan alamat IP dalam file konfigurasi (file SYLK) sekaligus. Anda harus membuat file konfigurasi terlebih dahulu.

- Sambungkan semua perangkat ke jaringan dengan kabel Ethernet.
- Nyalakan scanner.
- Jalankan EpsonNet Config.

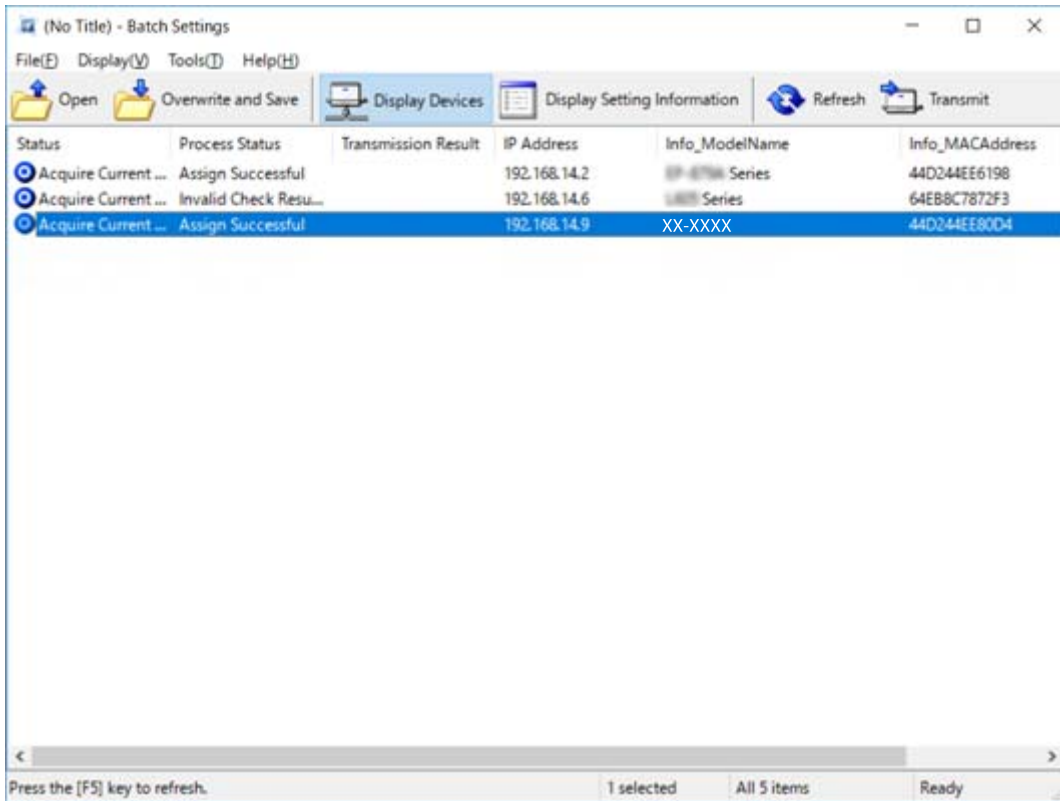
Daftar scanner yang terhubung ke jaringan akan ditampilkan. Mungkin perlu waktu beberapa saat untuk menampilkan daftar tersebut.

- Klik **Tools > Batch Settings**.
- Klik **Open**.
- Di layar pemilihan file, pilih file SYLK (*.slk) yang berisi pengaturan, lalu klik **Open**.

Lampiran

- 7. Pilih perangkat yang ingin dijadikan target pengaturan batch, dengan kolom **Status** diatur ke **Unassigned**, sementara **Process Status** diatur ke **Assign Successful**.

Jika ingin memilih beberapa pilihan sekaligus, tekan Ctrl atau Shift sambil mengklik atau menggeser mouse.



- 8. Klik **Transmit**.
- 9. Jika muncul layar penginputan kata sandi, masukkan kata sandi, lalu klik **OK**.
Kirim pengaturan.

! Penting:
Informasi dikirimkan ke antarmuka jaringan sampai bilah perkembangan selesai. Jangan matikan perangkat atau adaptor nirkabel, dan jangan kirim data apa pun ke perangkat.






- 10. Di layar **Transmitting Settings**, klik **OK**.



Lampiran

11. Periksa status perangkat yang Anda atur.

Untuk perangkat yang menunjukkan  atau , periksa isi file pengaturan, atau pastikan perangkat telah dinyalakan ulang tanpa masalah.

Ikon	Status	Process Status	Penjelasan
	Setup Complete	Setup Successful	Pengaturan selesai tanpa masalah.
	Setup Complete	Rebooting	Jika informasi telah dikirim, setiap perangkat harus dinyalakan ulang agar pengaturan dapat diterapkan. Pemeriksaan akan dilakukan untuk menentukan dapat tidaknya perangkat dihubungkan setelah booting ulang.
	Setup Complete	Reboot Failed	Tidak dapat mengonfirmasi perangkat setelah pengiriman pengaturan. Pastikan perangkat sudah menyala, atau telah dinyalakan ulang tanpa masalah.
	Setup Complete	Searching	Mencari perangkat yang ditunjukkan dalam file pengaturan.*
	Setup Complete	Search Failed	Tidak dapat memeriksa perangkat yang sudah diatur. Pastikan perangkat sudah menyala, atau telah dinyalakan ulang tanpa masalah.*

* Hanya jika informasi pengaturan ditampilkan.

Informasi Terkait

- ➔ [“Menjalankan EpsonNet Config — Windows” pada halaman 56](#)
- ➔ [“Menjalankan EpsonNet Config — Mac OS” pada halaman 56](#)

Menentukan Alamat IP Setiap Perangkat

Tentukan alamat IP scanner menggunakan EpsonNet Config.

1. Nyalakan scanner.
2. Sambungkan scanner ke jaringan dengan kabel Ethernet.
3. Jalankan EpsonNet Config.

Daftar scanner yang terhubung ke jaringan akan ditampilkan. Mungkin perlu waktu beberapa saat untuk menampilkan daftar tersebut.

4. Klik dua kali pada scanner yang ingin Anda tentukan.

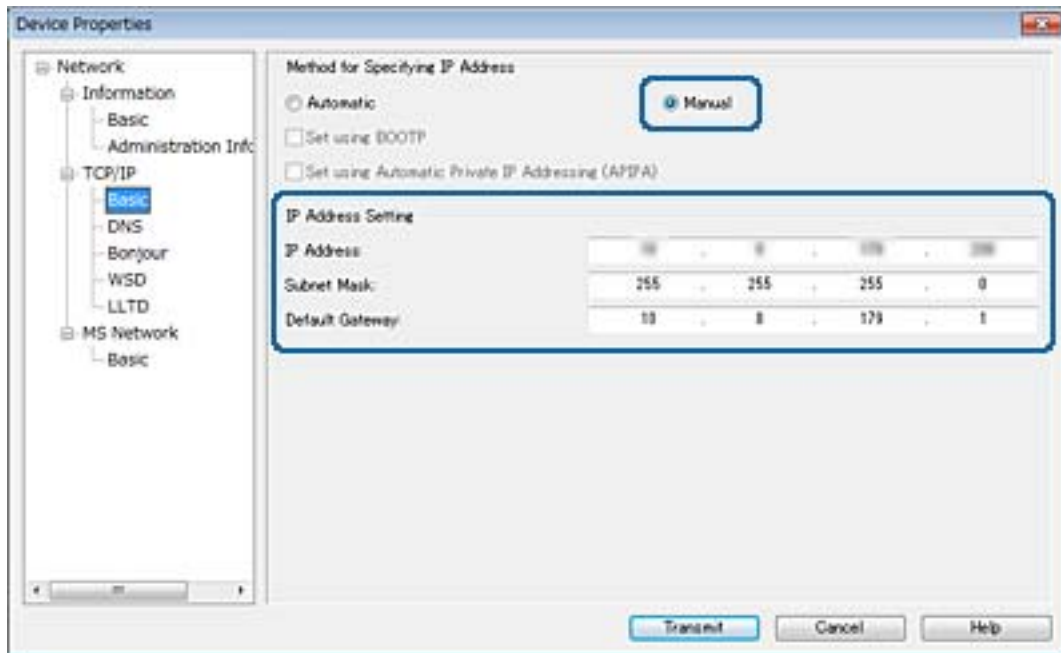
Catatan:

Jika Anda telah menghubungkan beberapa scanner yang modelnya sama, Anda dapat mengenali scanner menggunakan alamat MAC.

5. Pilih **Network > TCP/IP > Basic**.

Lampiran

6. Masukkan alamat **IP Address**, **Subnet Mask**, dan **Default Gateway**.

**Catatan:**

Masukkan alamat statis jika Anda menghubungkan scanner ke jaringan aman.

7. Klik **Transmit**.

Layar konfirmasi transmisi informasi ditampilkan.

8. Klik **OK**.

Layar penyelesaian transmisi ditampilkan.

Catatan:

Informasi ditransmisikan (dikirim) ke perangkat, lalu pesan “Konfigurasi berhasil.” akan ditampillkan. Jangan matikan perangkat, dan jangan kirim data apa pun ke layanan.

9. Klik **OK**.

Informasi Terkait

- ➔ [“Menjalankan EpsonNet Config — Windows” pada halaman 56](#)
- ➔ [“Menjalankan EpsonNet Config — Mac OS” pada halaman 56](#)

Menggunakan Port Scanner

Scanner menggunakan port sebagai berikut. Port-port ini harus diizinkan oleh administrator jaringan agar dapat digunakan.

Lampiran

Pengirim (Klien)	Penggunaan	Tujuan (Server)	Protokol	Nomor Port
Scanner	Pengiriman email (Notifikasi email)	Server SMTP	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	POP sebelum koneksi SMTP (Notifikasi email)	Server POP	POP3 (TCP)	110
	WSD Kontrol	Komputer klien	WSD (TCP)	5357
	Mencari komputer saat pemindaian push dari Document Capture Pro	Komputer klien	Penemuan Pemindaian Push Scan Jaringan	2968
Mengambil informasi pekerjaan saat pemindaian push dari Document Capture Pro	Komputer klien	Pemindaian Push Jaringan	2968	
Komputer Klien	Menemukan scanner dari aplikasi seperti EpsonNet Config dan driver scanner.	Scanner	ENPC (UDP)	3289
	Mengambil dan menyiapkan informasi MIB dari aplikasi seperti EpsonNet Config dan driver scanner.	Scanner	SNMP (UDP)	161
	Mencari scanner WSD	Scanner	WS-Discovery (UDP)	3702
	Meneruskan data hasil pemindaian dari Document Capture Pro	Scanner	Network Scan (TCP)	1865

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Di bab ini, akan dijelaskan fitur keamanan tingkat lanjut.

Pengaturan Keamanan dan Pencegahan Bahaya

Jika perangkat terhubung ke jaringan, Anda dapat mengaksesnya dari jauh. Selain itu, banyak orang dapat memakai perangkat tersebut bersama-sama, sehingga meningkatkan efisiensi dan kenyamanan. Namun, semakin tinggi juga risiko-risiko seperti akses ilegal, pemakaian ilegal, dan sabotase data. Jika Anda menggunakan perangkat di lingkungan yang terhubung ke Internet, risikonya akan jauh lebih tinggi lagi.

Untuk menghindari risiko ini, perangkat Epson dilengkapi dengan berbagai teknologi keamanan.

Atur perangkat sesuai dengan keperluan dan kondisi lingkungan, seperti yang telah tertera pada informasi lingkungan pelanggan.

Nama	Jenis fitur	Yang harus diatur	Yang harus dicegah
Komunikasi SSL/TLS	Jalur komunikasi komputer dan perangkat dienkripsi menggunakan komunikasi SSL/TLS. Isi komunikasi via browser dilindungi.	Atur sertifikat CA untuk server yang merupakan sertifikat bertanda tangan CA (Certificate Authority) untuk perangkat.	Cegah kebocoran informasi pengaturan dan isi data yang ditransfer ke scanner dari komputer. Akses ke server Epson dari perangkat melalui Internet juga dapat dilindungi dengan pembaruan firmware, dan lain-lain.
Pemfilteran IPsec/IP	Anda dapat mengizinkan pemutusan dan pemotongan data dari klien tertentu atau dari jenis tertentu. Karena IPsec melindungi data berdasarkan unit paket IP (enkripsi dan autentikasi), Anda dapat mengomunikasikan protokol pemindaian secara aman.	Buat kebijakan dasar dan kebijakan tersendiri untuk mengatur klien atau jenis data yang dapat mengakses perangkat.	Lindungi perangkat dari akses tanpa izin, sabotase, dan pencegahan data komunikasi.
SNMPv3	Berbagai fitur ditambahkan, misalnya pemantauan perangkat yang terhubung ke jaringan, integritas data yang harus dikontrol protokol SNMP, enkripsi, autentikasi pengguna, dan lain-lain.	Aktifkan SNMPv3, kemudian atur metode autentikasi dan enkripsi.	Pastikan Anda mengubah pengaturan melalui jaringan, kerahasiaan dalam pemantauan status.

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Nama	Jenis fitur	Yang harus diatur	Yang harus dicegah
IEEE802.1X	Membuat pengguna yang dapat tersambung adalah pengguna yang lolos autentikasi Ethernet saja. Membuat pengguna yang dapat memakai perangkat adalah pengguna yang diizinkan saja.	Pengaturan autentikasi ke server RADIUS (server autentikasi).	Melindungi perangkat dari akses dan pemakaian tanpa izin.
Membaca kartu ID	Anda dapat menggunakan perangkat dengan memegang kartu ID di atas perangkat autentikasi yang terhubung. Anda dapat membatasi pengambilan pekerjaan untuk setiap pengguna dan perangkat, juga membatasi pemakaian perangkat dan fitur untuk setiap pengguna dan grup.	Hubungkan perangkat autentikasi ke perangkat, lalu atur informasi pengguna di sistem autentikasi tersebut.	Mencegah pemakaian tanpa izin dan pemalsuan akses perangkat.

Informasi Terkait

- ➔ [“Komunikasi SSL/TLS dengan Scanner” pada halaman 63](#)
- ➔ [“Mengkripsi Komunikasi Menggunakan Pemfilteran IPsec/IP” pada halaman 71](#)
- ➔ [“Menggunakan Protokol SNMPv3” pada halaman 82](#)
- ➔ [“Menghubungkan Scanner ke Jaringan IEEE802.1X” pada halaman 84](#)

Pengaturan Fitur Keamanan

Ketika mengatur pemfilteran IPsec/IP atau IEEE802.1X, sebaiknya Anda mengakses Web Config menggunakan SSL/TLS untuk komunikasi informasi pengaturan agar risiko-risiko keamanan seperti sabotase atau pencegahan dapat dikurangi.

Komunikasi SSL/TLS dengan Scanner

Jika sertifikat server diatur menggunakan komunikasi SSL/TLS (Secure Sockets Layer/Transport Layer Security) ke scanner, Anda dapat mengenkripsi jalur komunikasi antarkomputer. Lakukan ini jika Anda ingin mencegah akses jarak jauh dan akses tanpa izin.

Tentang Sertifikasi Digital

- Sertifikat yang ditandatangani oleh CA

Sertifikat yang ditandatangani oleh CA (Certificate Authority/Otoritas Sertifikat) harus didapatkan dari otoritas sertifikat. Anda dapat memastikan komunikasi yang aman menggunakan sertifikat bertanda tangan CA. Anda dapat menggunakan sertifikat bertanda tangan CA untuk semua fitur keamanan.

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Sertifikat CA

Sertifikat CA menunjukkan bahwa pihak ketiga telah memverifikasi identitas server. Ini adalah komponen utama dalam gaya keamanan web tepercaya. Anda perlu mendapatkan sertifikat CA untuk otentikasi server dari CA yang mengeluarkannya.

Sertifikat bertanda tangan sendiri

Sertifikat bertanda tangan sendiri merupakan sebuah sertifikat yang dikeluarkan dan ditandatangani oleh scanner itu sendiri. Sertifikat ini tidak dapat diandalkan dan tidak dapat menghindari pemalsuan. Jika Anda menggunakan sertifikat ini untuk sertifikat SSL/TLS, peringatan keamanan mungkin akan ditampilkan pada browser. Anda hanya dapat menggunakan sertifikat ini untuk komunikasi SSL/TLS.

Informasi Terkait

- ➔ [“Mendapatkan dan Mengimpor Sertifikat yang Ditandatangani CA” pada halaman 64](#)
- ➔ [“Menghapus Sertifikat Bertanda Tangan CA” pada halaman 68](#)
- ➔ [“Memperbarui Sertifikat Bertanda Tangan Sendiri” pada halaman 68](#)

Mendapatkan dan Mengimpor Sertifikat yang Ditandatangani CA

Mendapatkan Sertifikat Bertanda Tangan CA

Untuk mendapatkan sertifikat bertanda tangan CA, buatlah CSR (Certificate Signing Request/Permintaan Penandatanganan Sertifikat) dan menerapkannya ke otoritas sertifikat. Anda dapat membuat CSR menggunakan Web Config dan komputer.

Ikuti langkah-langkah untuk membuat CSR dan mendapatkan sertifikat bertanda tangan CA menggunakan Web Config. Saat membuat CSR menggunakan Web Config, sertifikat berformat PEM/DER.

1. Akses Web Config, lalu pilih **Network Security Settings**. Selanjutnya, pilih **SSL/TLS > Certificate** atau **IPsec/IP Filtering > Client Certificate** atau **IEEE802.1X > Client Certificate**.

2. Klik **Generate CSR**.

Halaman pembuatan CSR terbuka.

3. Masukkan angka untuk setiap item.

Catatan:

Panjang kunci dan singkatan yang tersedia bervariasi menurut otoritas sertifikat. Buatlah permintaan berdasarkan aturan masing-masing otoritas sertifikat.

4. Klik **OK**.

Pesan penyelesaian ditampilkan.

5. Pilih **Network Security Settings**. Selanjutnya, pilih **SSL/TLS > Certificate**, atau **IPsec/IP Filtering > Client Certificate** atau **IEEE802.1X > Client Certificate**.

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

- Klik salah satu tombol unduh **CSR** berdasarkan format tertentu dari masing-masing otoritas sertifikat untuk mengunduh CSR ke komputer.

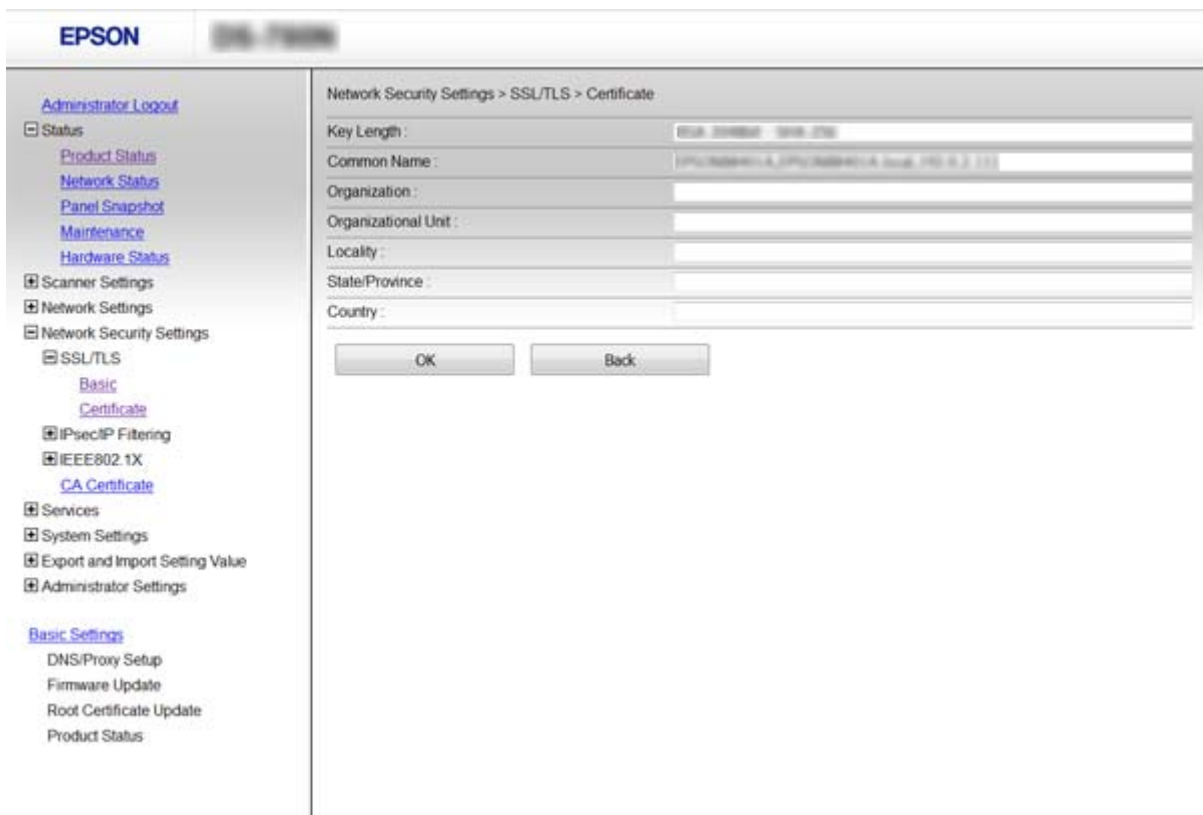
! Penting:
Jangan membuat CSR lagi. Jika melakukannya, Anda mungkin tidak akan dapat mengimpor CA-signed Certificate yang telah dikeluarkan.

- Kirimkan CSR ke otoritas sertifikat dan dapatkan CA-signed Certificate.
Ikuti aturan masing-masing otoritas sertifikat saat mengirim metode dan formulir.
- Simpan CA-signed Certificate yang dikeluarkan ke komputer yang tersambung ke scanner.
Proses mendapatkan CA-signed Certificate selesai saat Anda menyimpan sertifikat ke tempat tujuan.

Informasi Terkait

- ➔ [“Mengakses Web Config” pada halaman 23](#)
- ➔ [“Item Pengaturan CSR” pada halaman 65](#)
- ➔ [“Mengimpor Sertifikat Bertanda Tangan CA” pada halaman 66](#)

Item Pengaturan CSR



Item	Pengaturan dan Penjelasan
Key Length	Tentukan panjang kunci untuk CSR.

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Item	Pengaturan dan Penjelasan
Common Name	Anda dapat memasukkan antara 1 hingga 128 karakter. Jika ini adalah alamat IP, seharusnya ini termasuk alamat IP statis. Contoh: URL untuk mengakses Web Config: https://10.152.12.225 Nama umum: 10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	Anda dapat memasukkan antara 0 hingga 64 karakter dalam ASCII (0x20–0x7E). Anda dapat memisahkan nama yang berbeda dengan koma.
Country	Masukkan dua digit nomor kode negara yang ditentukan oleh ISO-3166.

Informasi Terkait

➔ [“Mendapatkan Sertifikat Bertanda Tangan CA”](#) pada halaman 64

Mengimpor Sertifikat Bertanda Tangan CA



Penting:

- Pastikan tanggal dan waktu scanner sudah diatur dengan benar.
- Jika Anda mendapatkan sertifikat dengan CSR yang dibuat dari Web Config, Anda dapat mengimpor sertifikasi sekali.

1. Akses Web Config lalu pilih **Network Security Settings**. Selanjutnya, pilih **SSL/TLS > Certificate**, atau **IPsec/IP Filtering > Client Certificate** atau **IEEE802.1X > Client Certificate**.

2. Klik **Import**.

Halaman pengimporan sertifikasi dibuka.

3. Masukkan angka untuk setiap item.

Tergantung di mana Anda membuat CSR dan format file sertifikat, pengaturan yang dibutuhkan mungkin berbeda-beda. Masukkan nilai untuk item yang diperlukan sesuai di bawah ini.

- Sertifikat format PEM/DER yang didapatkan dari Web Config
 - Private Key:** Jangan mengonfigurasi karena scanner memiliki kunci pribadi.
 - Password:** Jangan mengonfigurasi.
 - CA Certificate 1/CA Certificate 2:** Opsional
- Sertifikat format PEM/DER yang didapatkan dari komputer
 - Private Key:** Anda harus mengaturnya.
 - Password:** Jangan mengonfigurasi.
 - CA Certificate 1/CA Certificate 2:** Opsional

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

- Sertifikat format PKCS#12 yang didapatkan dari komputer
 - Private Key:** Jangan mengonfigurasi.
 - Password:** Opsional
 - CA Certificate 1/CA Certificate 2:** Jangan mengonfigurasi.

4. Klik OK.

Pesan penyelesaian ditampilkan.

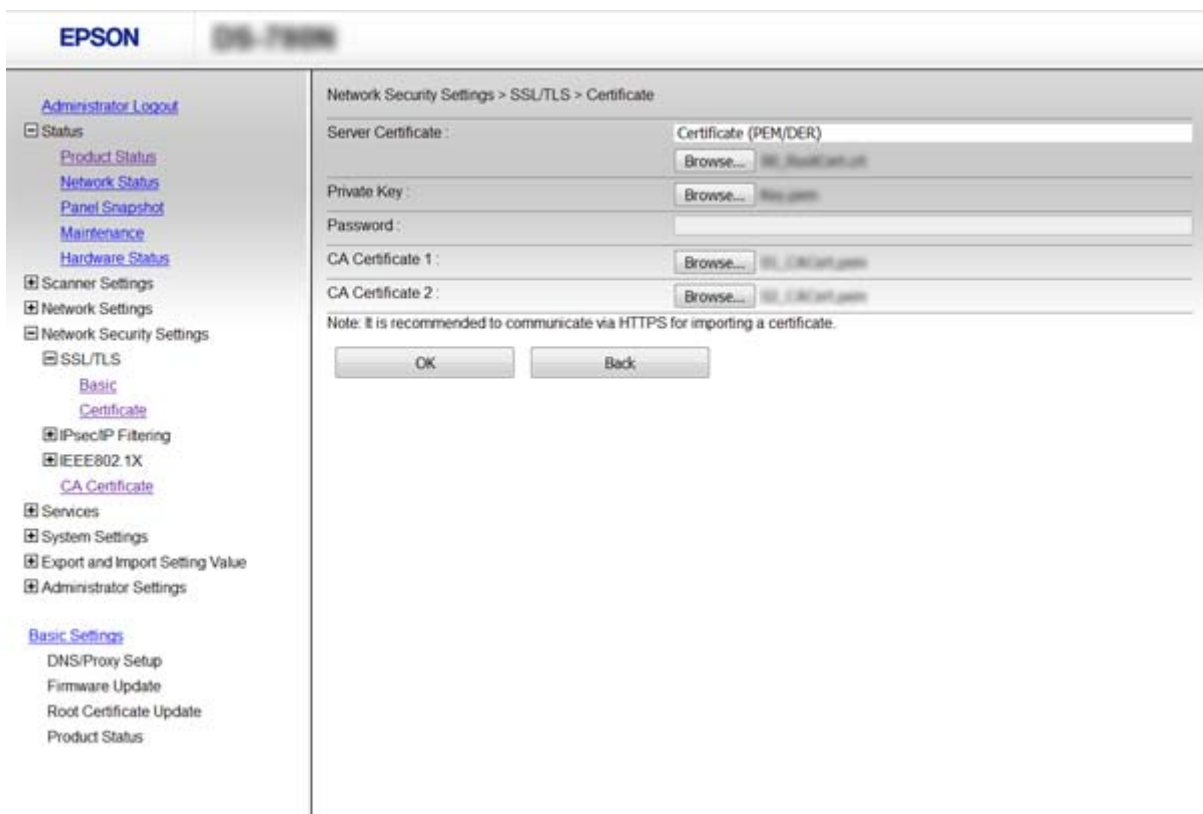
Catatan:

Klik **Confirm** untuk memverifikasi informasi sertifikat.

Informasi Terkait

- ➔ “Mengakses Web Config” pada halaman 23
- ➔ “Item Pengaturan Mengimpor Sertifikat Bertanda Tangan CA” pada halaman 67

Item Pengaturan Mengimpor Sertifikat Bertanda Tangan CA



Item	Pengaturan dan Penjelasan
Server Certificate atau Client Certificate	Pilih format sertifikat.
Private Key	Jika Anda mendapatkan format sertifikat PEM/DER dengan menggunakan CSR yang dibuat dari komputer, tentukan file kunci pribadi yang sesuai dengan sertifikat.

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Item	Pengaturan dan Penjelasan
Password	Masukkan kata sandi untuk mengenkripsi kunci pribadi.
CA Certificate 1	Jika format sertifikat Anda adalah Certificate (PEM/DER) , impor sertifikat dari otoritas sertifikat yang mengeluarkan sertifikat server. Tentukan file yang Anda butuhkan.
CA Certificate 2	Jika format sertifikat Anda adalah Certificate (PEM/DER) , masukkan sertifikat dari otoritas sertifikat yang mengeluarkan CA Certificate 1 . Tentukan file yang Anda butuhkan.

Informasi Terkait

➔ [“Mengimpor Sertifikat Bertanda Tangan CA”](#) pada halaman 66

Menghapus Sertifikat Bertanda Tangan CA

Anda dapat menghapus sertifikat yang diimpor jika sertifikat sudah tidak berlaku atau jika koneksi yang dienkripsi tidak diperlukan lagi.



Penting:

Jika Anda mendapatkan sertifikat dengan CSR yang dibuat dari Web Config, Anda tidak dapat lagi mengimpor file yang sudah dihapus. Untuk kasus seperti ini, Anda dapat membuat CSR dan mendapatkan sertifikat lagi.

1. Akses Web Config, lalu pilih **Network Security Settings**. Selanjutnya, pilih **SSL/TLS > Certificate**, atau **IPsec/IP Filtering > Client Certificate** atau **IEEE802.1X > Client Certificate**.
2. Klik **Delete**.
3. Konfirmasikan bahwa Anda ingin menghapus sertifikat tersebut di pesan yang ditampilkan.

Informasi Terkait

➔ [“Mengakses Web Config”](#) pada halaman 23

Memperbarui Sertifikat Bertanda Tangan Sendiri

Jika scanner mendukung fitur server HTTPS, Anda dapat memperbarui sertifikat bertanda tangan sendiri. Saat mengakses Web Config menggunakan sertifikat bertanda tangan sendiri, muncul pesan peringatan.

Gunakan sertifikat bertanda tangan sendiri sementara hingga Anda mendapatkan dan mengimpor sertifikat bertanda tangan CA.

1. Akses Web Config lalu pilih **Network Security Settings > SSL/TLS > Certificate**.
2. Klik **Update**.
3. Masukkan **Common Name**.

Masukkan alamat IP, atau pengidentifikasi seperti nama FQDN untuk scanner. Anda dapat memasukkan antara 1 hingga 128 karakter.

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Catatan:

Anda dapat memisahkan nama khusus (CN) dengan koma.

4. Tentukan masa berlaku untuk sertifikat.

EPSON

Administrator Logout

- Status
 - Product Status
 - Network Status
 - Panel Snapshot
 - Maintenance
 - Hardware Status
- Scanner Settings
- Network Settings
- Network Security Settings
 - SSL/TLS
 - Basic
 - Certificate
 - IPsec/IP Filtering
 - IEEE802.1X
 - CA Certificate
- Services
- System Settings
- Export and Import Setting Value
- Administrator Settings

Basic Settings

- DNS/Proxy Setup
- Firmware Update
- Root Certificate Update
- Product Status

Network Security Settings > SSL/TLS > Certificate

Key Length :	2048
Common Name :	EPSON-SECURITY-CA
Organization :	SEIKO EPSON CORP.
Valid Date (UTC) :	2016-11-24 02:49:09 UTC
Certificate Validity (year) :	10

Next Back

5. Klik Next.

Pesan konfirmasi ditampilkan.

6. Klik OK.

Scanner diperbarui.

Catatan:

Klik **Confirm** untuk memverifikasi informasi sertifikat.

Informasi Terkait

➔ [“Mengakses Web Config”](#) pada halaman 23

Konfigurasi CA Certificate

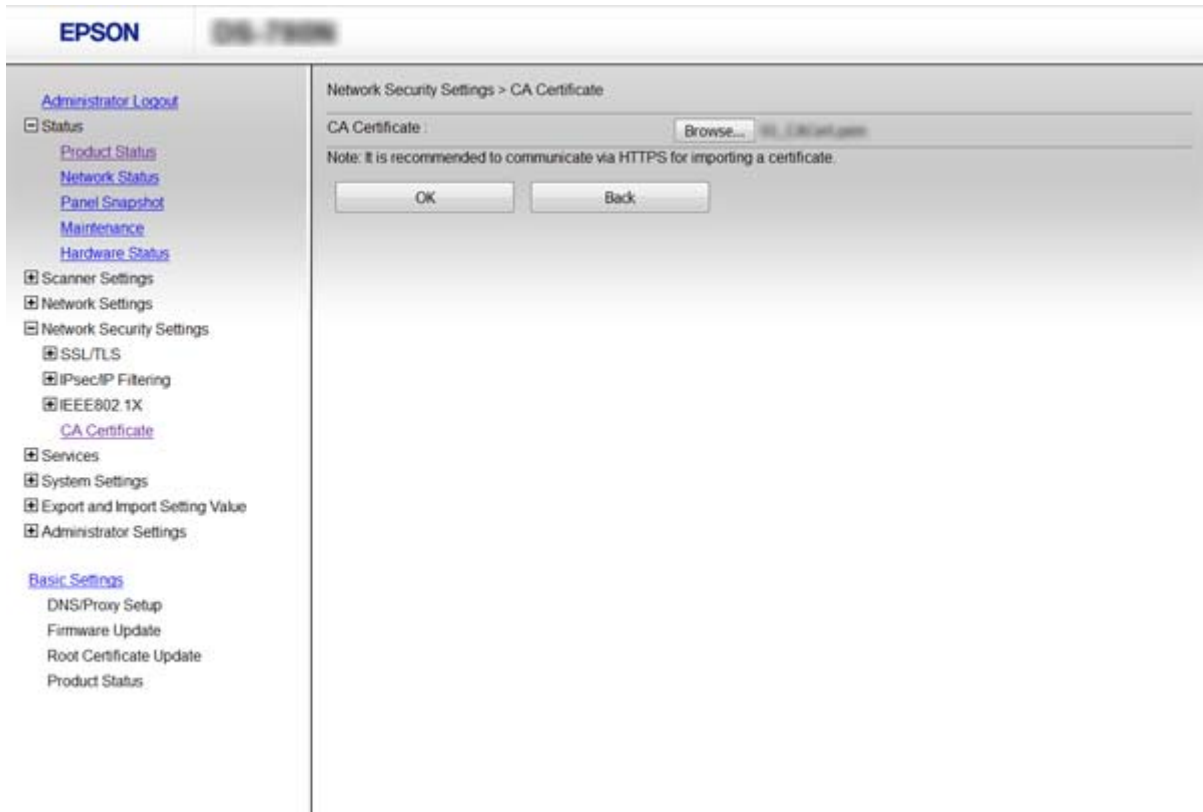
Anda dapat mengimpor, menampilkan, menghapus CA Certificate.

Mengimpor CA Certificate

1. Akses Web Config, lalu pilih **Network Security Settings > CA Certificate**.

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

2. Klik **Import**.
3. Tentukan CA Certificate yang ingin Anda impor.



4. Klik **OK**.

Ketika pengimporan selesai, Anda akan diarahkan kembali ke layar **CA Certificate**, dan CA Certificate yang diimpor itu ditampilkan.

Informasi Terkait

➔ [“Mengakses Web Config” pada halaman 23](#)

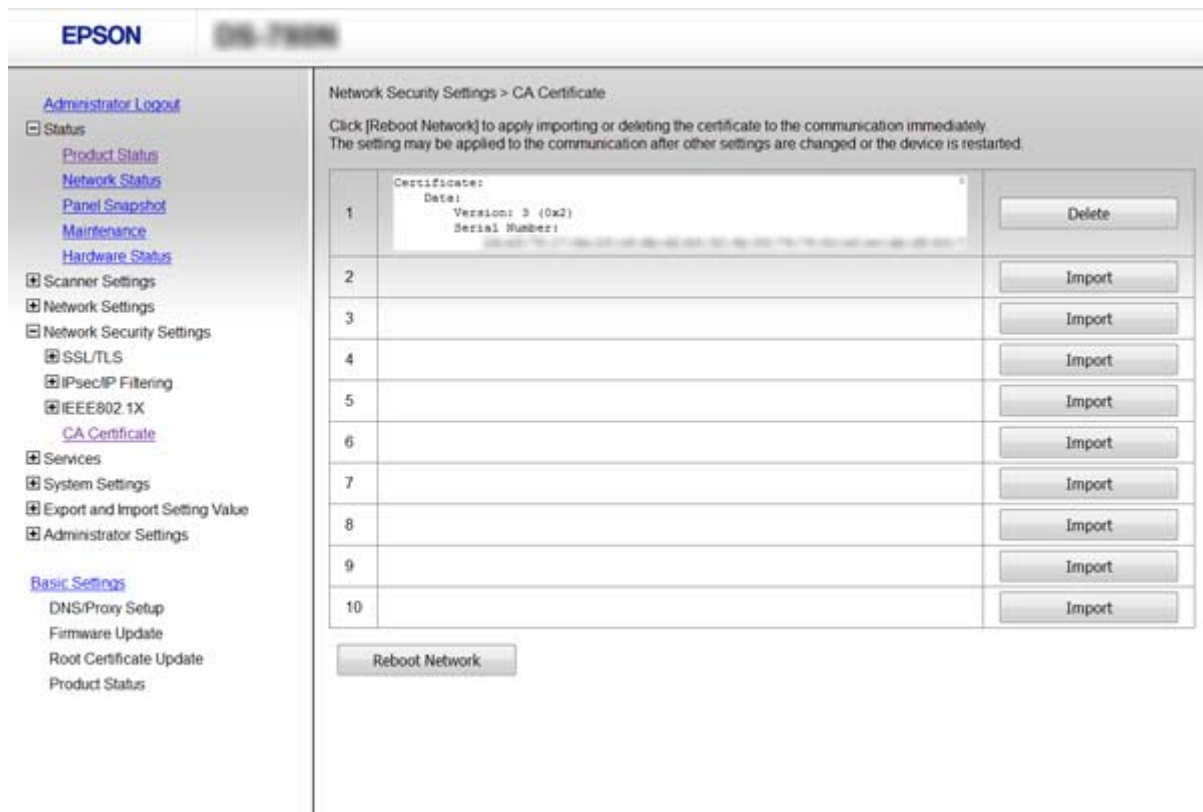
Menghapus CA Certificate

Anda dapat menghapus CA Certificate yang telah diimpor.

1. Akses Web Config, lalu pilih **Network Security Settings > CA Certificate**.

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

- Klik **Delete** di samping CA Certificate yang ingin Anda hapus.



- Konfirmasikan bahwa Anda ingin menghapus sertifikat tersebut di pesan yang ditampilkan.

Informasi Terkait

- ➔ [“Mengakses Web Config” pada halaman 23](#)

Menkripsi Komunikasi Menggunakan Pemfilteran IPsec/IP

Tentang IPsec/IP Filtering

Jika printer mendukung Pemfilteran IPsec/IP, Anda dapat memfilter lalu lintas berdasarkan alamat IP, layanan, dan port. Dengan menggabungkan pemfilteran, Anda dapat mengonfigurasi scanner untuk menerima atau memblokir klien dan data tertentu. Selain itu, Anda juga dapat meningkatkan tingkat keamanan menggunakan sebuah IPsec.

Untuk memfilter lalu lintas, konfigurasi kebijakan default. Kebijakan default berlaku bagi semua pengguna atau grup yang tersambung ke scanner. Untuk kontrol pengguna dan grup pengguna yang lebih baik, konfigurasi kebijakan grup. Kebijakan grup merupakan satu atau lebih aturan yang diterapkan ke pengguna atau grup pengguna. Scanner mengontrol paket IP yang sesuai dengan kebijakan yang telah dikonfigurasi. Paket IP diotentikasi sesuai urutan kebijakan grup 1 sampai 10, lalu kebijakan default.

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Catatan:

Komputer yang menjalankan Windows Vista atau yang lebih baru atau Windows Server 2008 atau yang lebih baru mendukung IPsec.

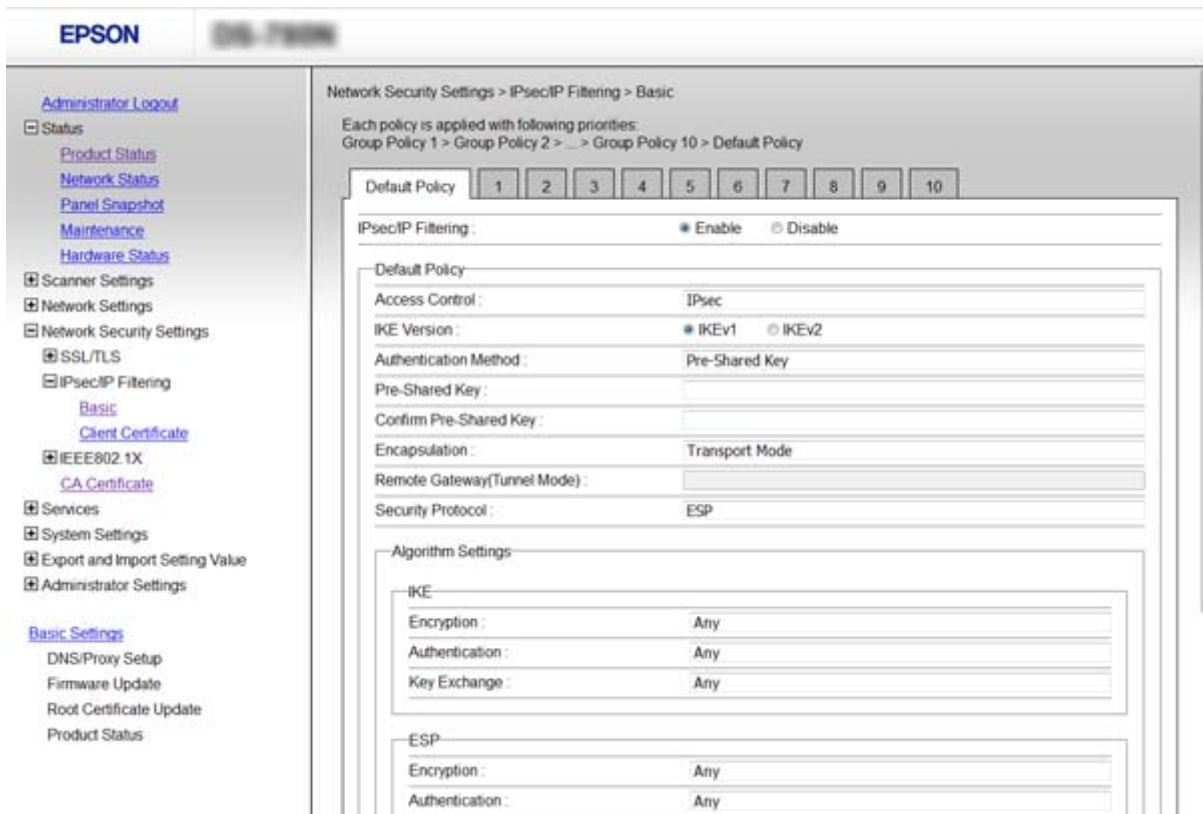
Mengonfigurasi Default Policy

1. Akses Web Config lalu pilih **Network Security Settings > IPsec/IP Filtering > Basic**.
2. Masukkan angka untuk setiap item.
3. Klik **Next**.
Pesan konfirmasi ditampilkan.
4. Klik **OK**.
Scanner diperbarui.

Informasi Terkait

- ➔ “Mengakses Web Config” pada halaman 23
- ➔ “Item Pengaturan Default Policy” pada halaman 72

Item Pengaturan Default Policy



Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Item	Pengaturan dan Penjelasan	
IPsec/IP Filtering	Anda dapat mengaktifkan atau menonaktifkan fitur Pemfilteran IPsec/IP.	
Access Control	Konfigurasi metode kontrol untuk lalu lintas paket IP.	
	Permit Access	Pilih metode ini untuk memberi izin masuk paket IP yang dikonfigurasi.
	Refuse Access	Pilih metode ini untuk menolak masuknya paket IP yang dikonfigurasi.
	IPsec	Pilih metode ini untuk memberi izin masuk IPsec yang dikonfigurasi.
IKE Version	Pilih IKEv1 atau IKEv2 untuk versi IKE. Pilih salah satu sesuai dengan perangkat yang terhubung ke scanner.	
IKEv1	Item berikut ini akan ditampilkan jika Anda memilih IKEv1 untuk IKE Version .	
	Authentication Method	Untuk memilih Certificate , Anda harus mendapatkan dan mengimpor sertifikat bertanda tangan CA terlebih dahulu.
	Pre-Shared Key	Apabila Anda memilih Pre-Shared Key untuk Authentication Method , masukkan kunci yang dibagikan sebelumnya antara 1 hingga 127 karakter.
	Confirm Pre-Shared Key	Untuk mengonfirmasi, masukkan kunci yang Anda konfigurasi.
IKEv2	Item berikut ini akan ditampilkan jika Anda memilih IKEv2 untuk IKE Version .	
Local	Authentication Method	Untuk memilih Certificate , Anda harus mendapatkan dan mengimpor sertifikat bertanda tangan CA terlebih dahulu.
	ID Type	Pilih jenis ID scanner.
	ID	Masukkan ID scanner yang sesuai dengan jenis ID. Anda tidak boleh menggunakan karakter pertama berupa "@", "#", dan "-". Distinguished Name: Masukkan 1 hingga 128 karakter ASCII 1 bita (0x20 hingga 0x7E). Anda harus menyertakan "-". IP Address: Masukkan format IPv4 atau IPv6. FQDN: Masukkan kombinasi antara 1 hingga 255 karakter menggunakan A-Z, a-z, 0-9, "-", dan titik (.). Email Address: Masukkan 1 hingga 128 karakter ASCII 1 bita (0x20 hingga 0x7E). Anda harus menyertakan "@". Key ID: Masukkan 1 hingga 128 karakter ASCII 1 bita (0x20 hingga 0x7E).
	Pre-Shared Key	Apabila Anda memilih Pre-Shared Key untuk Authentication Method , masukkan kunci yang dibagikan sebelumnya antara 1 hingga 127 karakter.
	Confirm Pre-Shared Key	Untuk mengonfirmasi, masukkan kunci yang Anda konfigurasi.

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Item	Pengaturan dan Penjelasan	
Remote	Authentication Method	Untuk memilih Certificate , Anda harus mendapatkan dan mengimpor sertifikat bertanda tangan CA terlebih dahulu.
	ID Type	Pilih jenis ID perangkat yang ingin Anda autentikasi.
	ID	<p>Masukkan ID scanner yang sesuai dengan jenis ID.</p> <p>Anda tidak boleh menggunakan karakter pertama berupa “@”, “#”, dan “=”.</p> <p>Distinguished Name: Masukkan 1 hingga 128 karakter ASCII 1 bita (0x20 hingga 0x7E). Anda harus menyertakan “=”.</p> <p>IP Address: Masukkan format IPv4 atau IPv6.</p> <p>FQDN: Masukkan kombinasi antara 1 hingga 255 karakter menggunakan A–Z, a–z, 0–9, “-”, dan titik (.).</p> <p>Email Address: Masukkan 1 hingga 128 karakter ASCII 1 bita (0x20 hingga 0x7E). Anda harus menyertakan “@”.</p> <p>Key ID: Masukkan 1 hingga 128 karakter ASCII 1 bita (0x20 hingga 0x7E).</p>
	Pre-Shared Key	Apabila Anda memilih Pre-Shared Key untuk Authentication Method , masukkan kunci yang dibagikan sebelumnya antara 1 hingga 127 karakter.
	Confirm Pre-Shared Key	Untuk mengonfirmasi, masukkan kunci yang Anda konfigurasi.
Encapsulation	Apabila Anda memilih IPsec untuk Access Control , Anda harus mengonfigurasi mode enkapsulasi.	
	Transport Mode	Apabila Anda hanya menggunakan scanner pada LAN yang sama, pilih ini. Paket IP lapisan 4 atau yang selanjutnya dienkripsi.
	Tunnel Mode	Apabila Anda menggunakan scanner pada jaringan internet seperti IPsec-VPN, pilih opsi ini. Header dan data paket IP dienkripsi.
Remote Gateway(Tunnel Mode)	Apabila Anda memilih Tunnel Mode untuk Encapsulation , masukkan alamat gateway antara 1 hingga 39 karakter.	
Security Protocol	IPsec untuk Access Control , pilih sebuah opsi.	
	ESP	Pilih opsi ini untuk memastikan integritas autentikasi dan data, serta untuk mengenkripsi data.
	AH	Pilih opsi ini untuk memastikan integritas autentikasi dan data. Meskipun enkripsi data dilarang, Anda tetap dapat menggunakan IPsec.
Algorithm Settings		

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Item	Pengaturan dan Penjelasan	
IKE	Encryption	Pilih algoritme enkripsi IKE. Item berbeda-beda tergantung versi IKE.
	Authentication	Pilih algoritme autentikasi IKE.
	Key Exchange	Pilih algoritme pertukaran kunci IKE. Item berbeda-beda tergantung versi IKE.
ESP	Encryption	Pilih algoritme enkripsi ESP. Ini tersedia jika ESP dipilih untuk Security Protocol .
	Authentication	Pilih algoritme autentikasi ESP. Ini tersedia jika ESP dipilih untuk Security Protocol .
AH	Authentication	Pilih algoritme enkripsi AH. Ini tersedia jika AH dipilih untuk Security Protocol .

Informasi Terkait

➔ [“Mengonfigurasi Default Policy” pada halaman 72](#)

Mengonfigurasi Group Policy

1. Akses Web Config lalu pilih **Network Security Settings > IPsec/IP Filtering > Basic**.
2. Klik tab nomor yang ingin Anda konfigurasi.
3. Masukkan angka untuk setiap item.
4. Klik **Next**.
Pesan konfirmasi ditampilkan.
5. Klik **OK**.
Scanner diperbarui.

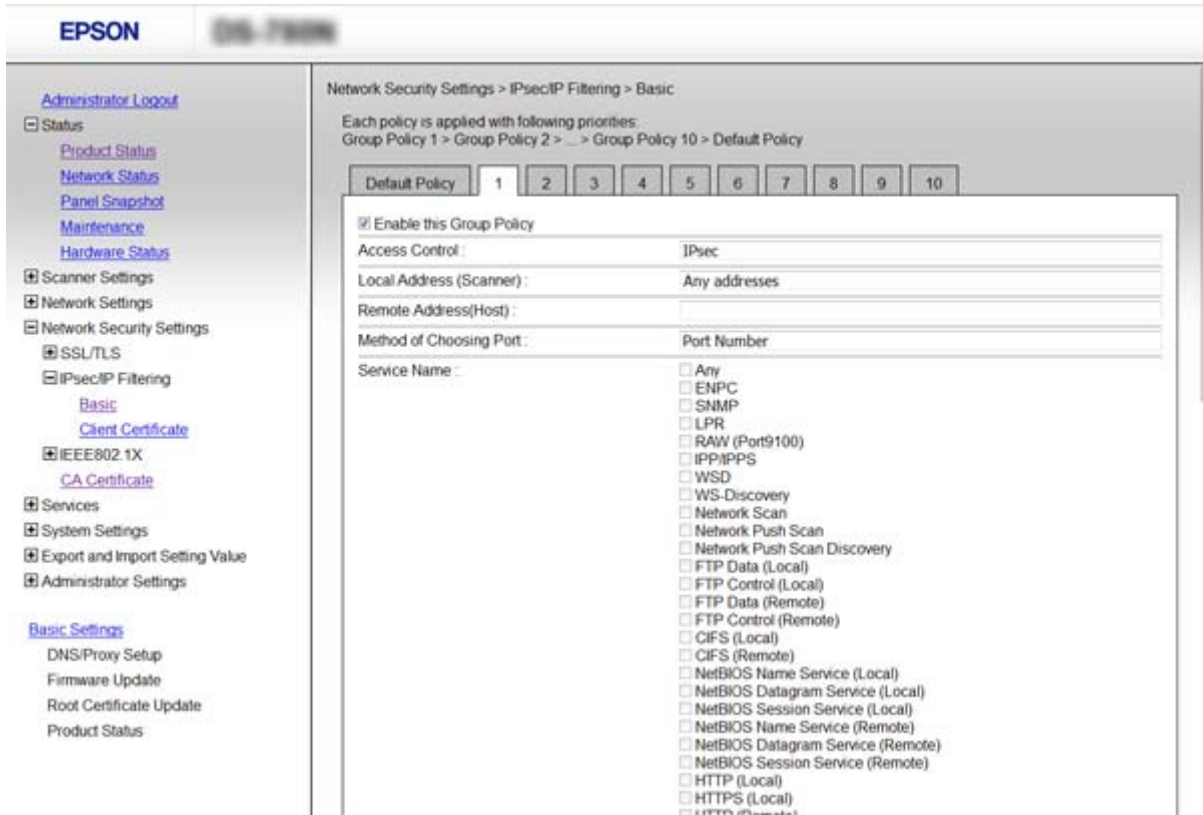
Informasi Terkait

➔ [“Mengakses Web Config” pada halaman 23](#)

➔ [“Item Pengaturan Group Policy” pada halaman 76](#)

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Item Pengaturan Group Policy



Item	Pengaturan dan Penjelasan	
Enable this Group Policy	Anda dapat mengaktifkan atau menonaktifkan kebijakan grup.	
Access Control	Permit Access	Pilih metode ini untuk memberi izin masuk paket IP yang dikonfigurasi.
	Refuse Access	Pilih metode ini untuk menolak masuknya paket IP yang dikonfigurasi.
	IPsec	Pilih metode ini untuk memberi izin masuk IPsec yang dikonfigurasi.
Local Address (Scanner)	Pilih alamat IPv4 atau alamat IPv6 yang sesuai dengan lingkungan jaringan Anda. Alamat IP ditetapkan secara otomatis, Anda dapat memilih Use auto-obtained IPv4 address .	
Remote Address(Host)	Masukkan alamat IP perangkat untuk mengontrol akses. Alamat IP harus sepanjang 43 karakter atau kurang. Jika Anda tidak memasukkan alamat IP, semua alamat akan diatur. Catatan: <i>Jika alamat IP ditetapkan secara otomatis (contoh ditetapkan oleh DHCP), koneksi mungkin tidak tersedia. Konfigurasi alamat IP statis.</i>	
Method of Choosing Port	Pilih metode untuk menetapkan port.	
Service Name	Apabila Anda memilih Service Name untuk Method of Choosing Port , pilih salah satu opsi.	

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Item	Pengaturan dan Penjelasan	
Transport Protocol	Apabila Anda memilih Port Number untuk Method of Choosing Port , Anda harus mengonfigurasi mode enkapsulasi.	
	Any Protocol	Pilih opsi ini untuk mengontrol semua jenis protokol.
	TCP	Pilih opsi ini untuk mengontrol data untuk unicast.
	UDP	Pilih opsi ini untuk mengontrol data untuk siaran dan multicast.
	ICMPv4	Pilih ini untuk mengontrol perintah ping.
Local Port	<p>Jika Anda memilih Port Number untuk Method of Choosing Port dan jika Anda memilih TCP atau UDP untuk Transport Protocol, masukkan nomor port untuk mengontrol paket yang diterima, bedakan menggunakan koma. Anda dapat memasukkan maksimal 10 nomor port.</p> <p>Contoh: 20,80,119,5220</p> <p>Jika Anda tidak memasukkan nomor port, semua port akan dikontrol.</p>	
Remote Port	<p>Jika Anda memilih Port Number untuk Method of Choosing Port dan jika Anda memilih TCP atau UDP untuk Transport Protocol, masukkan nomor port untuk mengontrol paket yang dikirim, bedakan menggunakan koma. Anda dapat memasukkan maksimal 10 nomor port.</p> <p>Contoh: 25,80,143,5220</p> <p>Jika Anda tidak memasukkan nomor port, semua port akan dikontrol.</p>	
IKE Version	<p>Pilih IKEv1 atau IKEv2 untuk versi IKE.</p> <p>Pilih salah satu sesuai dengan perangkat yang terhubung ke scanner.</p>	
IKEv1	Item berikut ini akan ditampilkan jika Anda memilih IKEv1 untuk IKE Version .	
	Authentication Method	Apabila Anda memilih IPsec untuk Access Control , pilih salah satu opsi. Sertifikat yang digunakan biasanya memiliki pengaturan default.
	Pre-Shared Key	Apabila Anda memilih Pre-Shared Key untuk Authentication Method , masukkan kunci yang dibagikan sebelumnya antara 1 hingga 127 karakter.
	Confirm Pre-Shared Key	Untuk mengonfirmasi, masukkan kunci yang Anda konfigurasi.
IKEv2	Item berikut ini akan ditampilkan jika Anda memilih IKEv2 untuk IKE Version .	

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Item	Pengaturan dan Penjelasan	
Local	Authentication Method	Apabila Anda memilih IPsec untuk Access Control , pilih salah satu opsi. Sertifikat yang digunakan biasanya memiliki pengaturan default.
	ID Type	Pilih jenis ID scanner.
	ID	<p>Masukkan ID scanner yang sesuai dengan jenis ID.</p> <p>Anda tidak boleh menggunakan karakter pertama berupa “@”, “#”, dan “=”.</p> <p>Distinguished Name: Masukkan 1 hingga 128 karakter ASCII 1 bita (0x20 hingga 0x7E). Anda harus menyertakan “=”.</p> <p>IP Address: Masukkan format IPv4 atau IPv6.</p> <p>FQDN: Masukkan kombinasi antara 1 hingga 255 karakter menggunakan A–Z, a–z, 0–9, “-”, dan titik (.).</p> <p>Email Address: Masukkan 1 hingga 128 karakter ASCII 1 bita (0x20 hingga 0x7E). Anda harus menyertakan “@”.</p> <p>Key ID: Masukkan 1 hingga 128 karakter ASCII 1 bita (0x20 hingga 0x7E).</p>
	Pre-Shared Key	Apabila Anda memilih Pre-Shared Key untuk Authentication Method , masukkan kunci yang dibagikan sebelumnya antara 1 hingga 127 karakter.
	Confirm Pre-Shared Key	Untuk mengonfirmasi, masukkan kunci yang Anda konfigurasi.
Remote	Authentication Method	Apabila Anda memilih IPsec untuk Access Control , pilih salah satu opsi. Sertifikat yang digunakan biasanya memiliki pengaturan default.
	ID Type	Pilih jenis ID perangkat yang ingin Anda autentikasi.
	ID	<p>Masukkan ID scanner yang sesuai dengan jenis ID.</p> <p>Anda tidak boleh menggunakan karakter pertama berupa “@”, “#”, dan “=”.</p> <p>Distinguished Name: Masukkan 1 hingga 128 karakter ASCII 1 bita (0x20 hingga 0x7E). Anda harus menyertakan “=”.</p> <p>IP Address: Masukkan format IPv4 atau IPv6.</p> <p>FQDN: Masukkan kombinasi antara 1 hingga 255 karakter menggunakan A–Z, a–z, 0–9, “-”, dan titik (.).</p> <p>Email Address: Masukkan 1 hingga 128 karakter ASCII 1 bita (0x20 hingga 0x7E). Anda harus menyertakan “@”.</p> <p>Key ID: Masukkan 1 hingga 128 karakter ASCII 1 bita (0x20 hingga 0x7E).</p>
	Pre-Shared Key	Apabila Anda memilih Pre-Shared Key untuk Authentication Method , masukkan kunci yang dibagikan sebelumnya antara 1 hingga 127 karakter.
	Confirm Pre-Shared Key	Untuk mengonfirmasi, masukkan kunci yang Anda konfigurasi.

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Item	Pengaturan dan Penjelasan	
Encapsulation	Apabila Anda memilih IPsec untuk Access Control , Anda harus mengonfigurasi mode enkapsulasi.	
	Transport Mode	Apabila Anda hanya menggunakan scanner pada LAN yang sama, pilih ini. Paket IP lapisan 4 atau yang selanjutnya dienkripsi.
	Tunnel Mode	Apabila Anda menggunakan scanner pada jaringan internet seperti IPsec-VPN, pilih opsi ini. Header dan data paket IP dienkripsi.
Remote Gateway(Tunnel Mode)	Apabila Anda memilih Tunnel Mode untuk Encapsulation , masukkan alamat gateway antara 1 hingga 39 karakter.	
Security Protocol	Apabila Anda memilih IPsec untuk Access Control , pilih salah satu opsi.	
	ESP	Pilih opsi ini untuk memastikan integritas autentikasi dan data, serta untuk mengenkripsi data.
	AH	Pilih opsi ini untuk memastikan integritas autentikasi dan data. Meskipun enkripsi data dilarang, Anda tetap dapat menggunakan IPsec.
Algorithm Settings		
IKE	Encryption	Pilih algoritme enkripsi IKE. Item berbeda-beda tergantung versi IKE.
	Authentication	Pilih algoritme autentikasi IKE.
	Key Exchange	Pilih algoritme pertukaran kunci IKE. Item berbeda-beda tergantung versi IKE.
ESP	Encryption	Pilih algoritme enkripsi ESP. Ini tersedia jika ESP dipilih untuk Security Protocol .
	Authentication	Pilih algoritme autentikasi ESP. Ini tersedia jika ESP dipilih untuk Security Protocol .
AH	Authentication	Pilih algoritme autentikasi AH. Ini tersedia jika AH dipilih untuk Security Protocol .

Informasi Terkait

- ➔ “Mengonfigurasi Group Policy” pada halaman 75
- ➔ “Kombinasi Local Address (Scanner) dan Remote Address(Host) di Group Policy” pada halaman 80
- ➔ “Rujukan Nama Layanan pada Kebijakan Grup” pada halaman 80

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Kombinasi Local Address (Scanner) dan Remote Address(Host) di Group Policy

		Pengaturan Local Address (Scanner)		
		IPv4	IPv6* ²	Any addresses* ³
Pengaturan Remote Address(Host)	IPv4* ¹	✓	–	✓
	IPv6* ¹ , * ²	–	✓	✓
	Kosong	✓	✓	✓

*1 Jika **IPsec** dipilih untuk **Access Control**, Anda tidak dapat menentukan panjang prefix.

*2 Jika **IPsec** dipilih untuk **Access Control**, Anda dapat memilih alamat lokal tautan (fe80::) tetapi kebijakan grup akan dinonaktifkan.

*3 Kecuali alamat lokal tautan IPv6.

Rujukan Nama Layanan pada Kebijakan Grup

Catatan:

Layanan yang tidak tersedia ditampilkan tetapi tidak dapat dipilih.

Nama Layanan	Jenis protokol	Nomor port lokal	Nomor port jarak jauh	Fitur yang dikendalikan
Any	–	–	–	Semua layanan
ENPC	UDP	3289	Semua port	Mencari scanner dari aplikasi seperti EpsonNet Config dan driver scanner
SNMP	UDP	161	Semua port	Mengambil dan mengonfigurasi MIB dari aplikasi seperti EpsonNet Config dan driver scanner Epson
WSD	TCP	Semua port	5357	Mengendalikan WSD
WS-Discovery	UDP	3702	Semua port	Mencari scanner dari WSD
Network Scan	TCP	1865	Semua port	Meneruskan data hasil pemindaian dari Document Capture Pro
Network Push Scan Discovery	UDP	2968	Semua port	Mencari komputer dari scanner.
Network Push Scan	TCP	Semua port	2968	Mendapatkan informasi tugas pemindaian push dari Document Capture Pro atau Document Capture
HTTP (Local)	TCP	80	Semua port	Server HTTP(S) (meneruskan data Web Config dan WSD)
HTTPS (Local)	TCP	443	Semua port	
HTTP (Remote)	TCP	Semua port	80	Klien HTTP(S) (berkomunikasi antara pembaruan firmware dan pembaruan sertifikat root)
HTTPS (Remote)	TCP	Semua port	443	

Contoh Konfigurasi dari IPsec/IP Filtering

Hanya Menerima paket IPsec

Contoh ini hanya untuk mengonfigurasi kebijakan default.

Default Policy:

- IPsec/IP Filtering: Enable
- Access Control: IPsec
- Authentication Method: Pre-Shared Key
- Pre-Shared Key: Masukkan hingga 127 karakter.

Group Policy:

Jangan dikonfigurasi.

Menerima pemindaian menggunakan Epson Scan 2 dan pengaturan pemindai

Contoh ini memungkinkan pengomunikasian data pemindaian dan konfigurasi scanner dari layanan yang ditentukan.

Default Policy:

- IPsec/IP Filtering: Enable
- Access Control: Refuse Access

Group Policy:

- Enable this Group Policy: Periksa kotak.
- Access Control: Permit Access
- Remote Address(Host): Alamat IP klien
- Method of Choosing Port: Service Name
- Service Name: Periksa kotak ENPC, SNMP, Network Scan, HTTP (Local) dan HTTPS (Local).

Menerima akses hanya dari alamat IP yang ditentukan

Contoh ini mengizinkan alamat IP yang ditentukan untuk mengakses scanner.

Default Policy:

- IPsec/IP Filtering: Enable
- Access Control: Refuse Access

Group Policy:

- Enable this Group Policy: Periksa kotak.
- Access Control: Permit Access
- Remote Address(Host): Alamat IP klien administrator

Catatan:

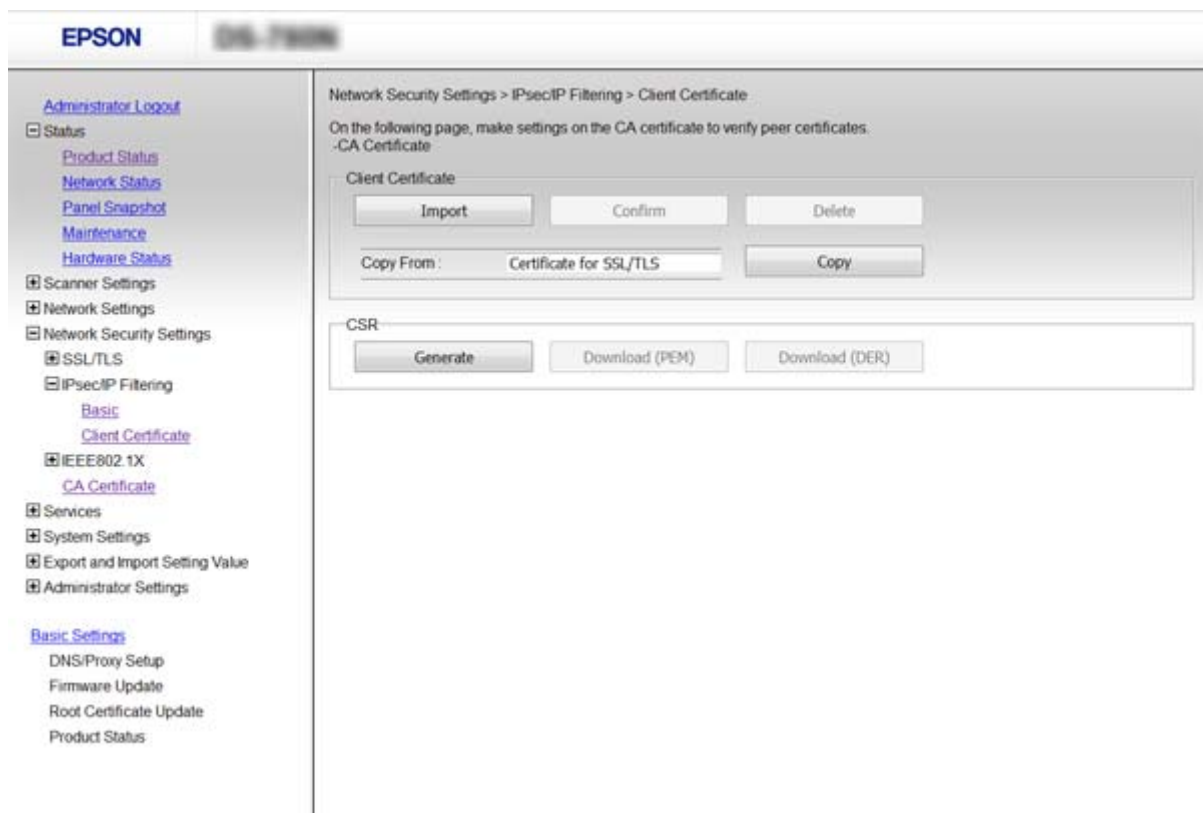
Tanpa mempertimbangkan konfigurasi kebijakan, klien akan dapat mengakses dan mengonfigurasi printer.

Mengonfigurasi Sertifikat untuk IPsec/IP Filtering

Mengonfigurasi Sertifikat Klien untuk Pemfilteran IPsec/IP. Jika Anda ingin mengonfigurasi otoritas sertifikasi, buka **CA Certificate**.

1. Akses Web Config lalu pilih **Network Security Settings > IPsec/IP Filtering > Client Certificate**.
2. Impor sertifikat di **Client Certificate**.

Jika Anda sudah mengimpor sertifikat yang diterbitkan oleh Otoritas Sertifikat dalam IEEE802.1X atau SSL/TLS, Anda dapat menyalin sertifikat tersebut dan menggunakannya dalam Pemfilteran IPsec/IP. Untuk menyalin, pilih sertifikat dari **Copy From**, lalu klik **Copy**.



Informasi Terkait

- ➔ “Mengakses Web Config” pada halaman 23
- ➔ “Mendapatkan dan Mengimpor Sertifikat yang Ditandatangani CA” pada halaman 64

Menggunakan Protokol SNMPv3

Tentang SNMPv3

SNMP adalah protokol yang menjalankan pemantauan dan pengendalian untuk mengumpulkan informasi perangkat yang terhubung ke jaringan. SNMPv3 adalah versi fitur keamanan manajemen yang telah ditingkatkan.

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Ketika menggunakan SNMPv3, pemantauan kondisi dan perubahan pengaturan (paket) komunikasi SNMP yang dapat diautentikasi dan dienkripsi untuk melindungi (paket) komunikasi SNMP dari risiko-risiko jaringan seperti penyadapan, peniruan orang, dan sabotase.

Mengonfigurasi SNMPv3

Jika printer mendukung protokol SNMPv3, Anda dapat memantau dan mengontrol banyak akses ke printer.

1. Akses Web Config lalu pilih **Services > Protocol**.
2. Masukkan nilai untuk setiap item **SNMPv3 Settings**.
3. Klik **Next**.
Pesan konfirmasi ditampilkan.
4. Klik **OK**.
Scanner diperbarui.

Informasi Terkait

- ➔ [“Mengakses Web Config” pada halaman 23](#)
- ➔ [“Item Pengaturan SNMPv3” pada halaman 83](#)

Item Pengaturan SNMPv3

The screenshot shows the EPSON Web Config interface for configuring SNMPv3. The left sidebar lists various settings categories. The main content area is titled '000-7000' and contains the following settings:

- LLMNR Settings:**
 - Enable LLMNR
- SNMPv1v2c Settings:**
 - Enable SNMPv1v2c
 - Access Authority : Read/Write
 - Community Name (Read Only) : public
 - Community Name (Read/Write) :
- SNMPv3 Settings:**
 - Enable SNMPv3
 - User Name : admin
 - Authentication Settings:**
 - Algorithm : MD5
 - Password :
 - Confirm Password :
 - Encryption Settings:**
 - Algorithm : DES
 - Password :
 - Confirm Password :
 - Context Name : EPSON

A 'Next' button is located at the bottom of the settings area.

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Item	Pengaturan dan Penjelasan
Enable SNMPv3	SNMPv3 diaktifkan bila kotak ini dicentang.
User Name	Masukkan antara 1 hingga 32 karakter menggunakan karakter 1 byte.
Authentication Settings	
Algorithm	Pilih algoritme untuk otentikasi.
Password	Masukkan antara 8 hingga 32 karakter dalam ASCII (0x20–0x7E).
Confirm Password	Masukkan kata sandi yang Anda konfigurasi untuk konfirmasi.
Encryption Settings	
Algorithm	Pilih algoritme untuk enkripsi.
Password	Masukkan antara 8 hingga 32 karakter dalam ASCII (0x20–0x7E).
Confirm Password	Masukkan kata sandi yang Anda konfigurasi untuk konfirmasi.
Context Name	Masukkan antara 1 hingga 32 karakter menggunakan karakter 1 byte.

Informasi Terkait

➔ [“Mengonfigurasi SNMPv3” pada halaman 83](#)

Menghubungkan Scanner ke Jaringan IEEE802.1X

Mengonfigurasi Jaringan IEEE802.1X

Jika scanner mendukung IEEE802.1X, Anda dapat menggunakan scanner di jaringan dengan autentikasi yang tersambung ke server dan hub RADIUS sebagai sebuah autentikator.

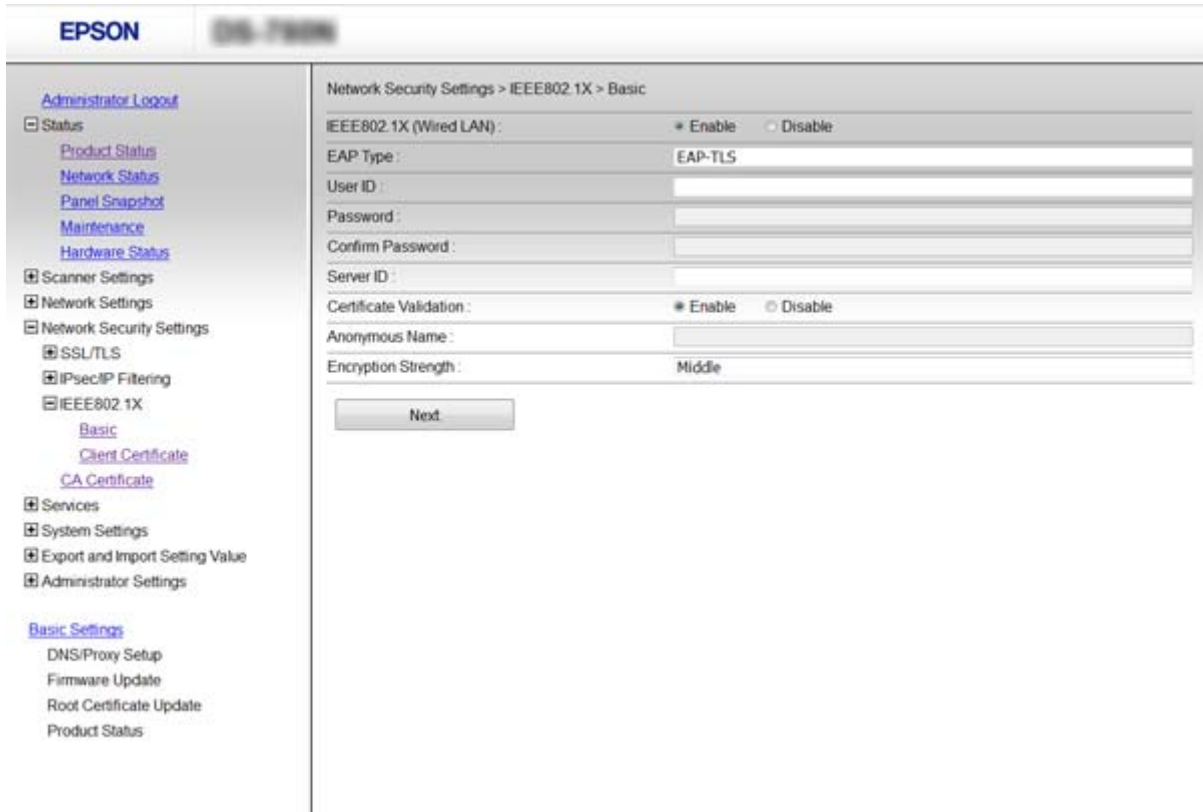
1. Akses Web Config lalu pilih **Network Security Settings > IEEE802.1X > Basic**.
2. Masukkan angka untuk setiap item.
3. Klik **Next**.
Pesan konfirmasi ditampilkan.
4. Klik **OK**.
Scanner diperbarui.

Informasi Terkait

- ➔ [“Mengakses Web Config” pada halaman 23](#)
- ➔ [“Item Pengaturan Jaringan IEEE802.1X” pada halaman 85](#)
- ➔ [“Tidak Dapat Mengakses Printer atau Scanner setelah Mengonfigurasi IEEE802.1X” pada halaman 89](#)

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Item Pengaturan Jaringan IEEE802.1X



Item	Pengaturan dan Penjelasan	
IEEE802.1X (Wired LAN)	Anda dapat mengaktifkan atau menonaktifkan pengaturan halaman (IEEE802.1X > Basic) untuk IEEE802.1X (LAN Berkabel).	
EAP Type	EAP-TLS	Anda harus mendapatkan dan mengimpor sertifikat bertanda tangan CA.
	PEAP-TLS	
	PEAP/MSCHAPv2	Anda harus mengonfigurasi kata sandi.
User ID	Konfigurasi ID untuk digunakan sebagai metode autentikasi server RADIUS. Masukkan 1 hingga 128 karakter ASCII 1 bita (0x20 hingga 0x7E).	
Password	Konfigurasi kata sandi untuk mengautentikasi scanner. Masukkan 1 hingga 128 karakter ASCII 1 bita (0x20 hingga 0x7E). Jika menggunakan server Windows sebagai server RADIUS, Anda dapat memasukkan hingga 127 karakter.	
Confirm Password	Masukkan kata sandi yang Anda konfigurasi untuk konfirmasi.	
Server ID	Anda dapat mengonfigurasi ID server untuk mengautentikasi server RADIUS yang ditentukan. Otentikator memverifikasi apakah ID server memiliki kolom subjek/subjectAltName sertifikasi server yang dikirim dari server RADIUS atau tidak. Masukkan 0 hingga 128 karakter ASCII 1 bita (0x20 hingga 0x7E).	
Certificate Validation	Anda dapat mengatur validasi sertifikat bagaimanapun metode autentikasinya. Impor sertifikat di CA Certificate .	

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Item	Pengaturan dan Penjelasan	
Anonymous Name	Jika Anda memilih PEAP-TLS atau PEAP/MSCHAPv2 untuk Authentication Method , Anda dapat mengonfigurasi nama tidak dikenal daripada nama ID pengguna untuk fase 1 autentikasi PEAP. Masukkan 0 hingga 128 karakter ASCII 1 bita (0x20 hingga 0x7E).	
Encryption Strength	Anda dapat memilih salah satu dari berikut ini.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Informasi Terkait

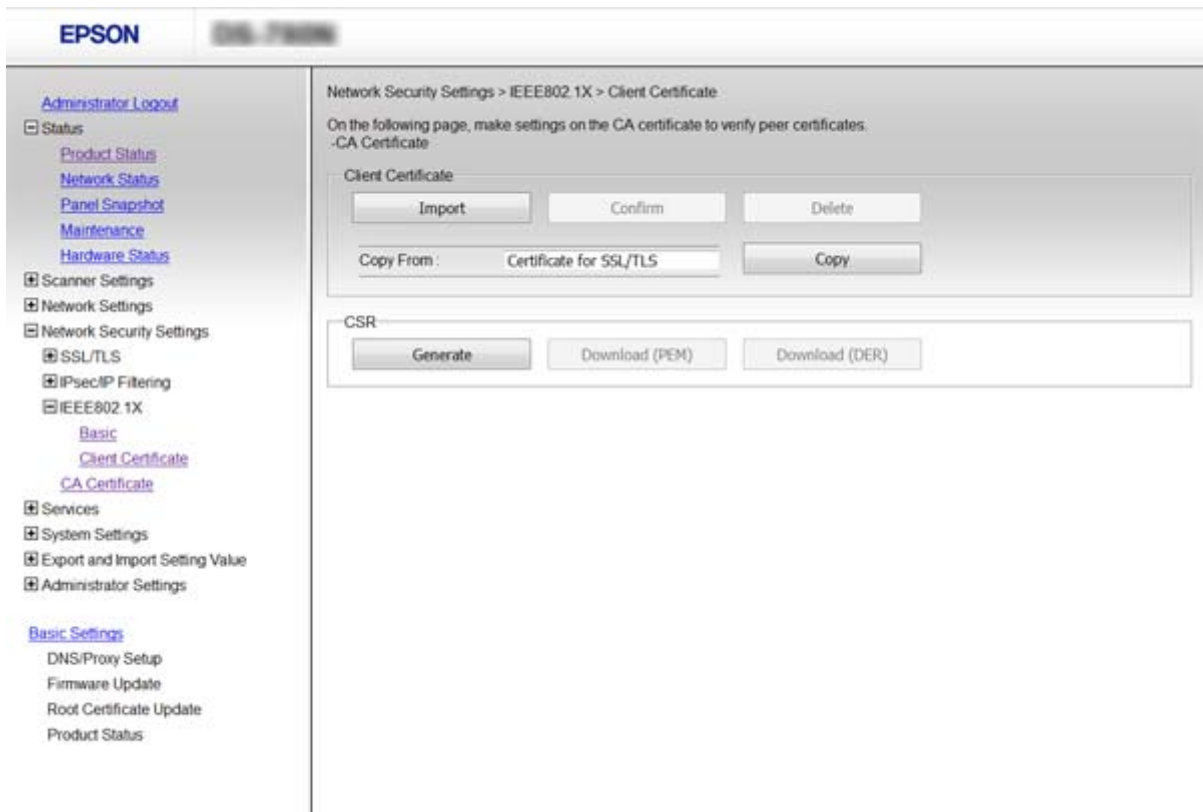
➔ [“Mengonfigurasi Jaringan IEEE802.1X” pada halaman 84](#)

Mengonfigurasi Sertifikat untuk IEEE802.1X

Konfigurasi Sertifikat Klien untuk IEEE802.1X. Jika Anda ingin mengonfigurasi sertifikat otoritas sertifikasi, buka **CA Certificate**.

1. Akses Web Config lalu pilih **Network Security Settings > IEEE802.1X > Client Certificate**.
2. Masukkan sertifikat di **Client Certificate**.

Anda dapat menyalin sertifikat tersebut jika diterbitkan oleh Otoritas Sertifikasi. Untuk menyalin, pilih sertifikat dari **Copy From**, lalu klik **Copy**.



Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Informasi Terkait

- ➔ [“Mengakses Web Config” pada halaman 23](#)
- ➔ [“Mendapatkan dan Mengimpor Sertifikat yang Ditandatangani CA” pada halaman 64](#)

Memecahkan Masalah Keamanan Tingkat Lanjut

Mengembalikan Pengaturan Keamanan

Jika Anda membangun lingkungan yang sangat aman seperti Pemfilteran IPsec/IP atau IEEE802.1X, Anda mungkin tidak dapat berkomunikasi dengan perangkat karena kesalahan pengaturan atau masalah pada perangkat atau server. Dalam konteks ini, kembalikan pengaturan keamanan agar Anda dapat melakukan pengaturan untuk perangkat tersebut kembali atau agar Anda dapat menggunakannya secara sementara.

Menonaktifkan Fungsi Keamanan Menggunakan Panel Kontrol

Anda dapat menonaktifkan Pemfilteran IPsec/IP atau IEEE802.1X menggunakan panel kontrol scanner.

1. Sentuh **Pengaturan > Pengaturan Jaringan**.
2. Sentuh **Ganti Pengaturan**.
3. Sentuh item-item yang ingin Anda nonaktifkan.
 - Penyaringan IPsec/IP**
 - IEEE802.1X**
4. Apabila pesan penyelesaian ditampilkan, sentuh **Lanjutkan**.

Mengembalikan Fungsi Keamanan Menggunakan Web Config

Untuk IEEE802.1X, perangkat mungkin tidak dikenali di jaringan. Untuk kasus seperti ini, nonaktifkan fungsi menggunakan panel kontrol scanner.

Untuk Pemfilteran IPsec/IP, Anda dapat menonaktifkan fungsi jika Anda dapat mengakses perangkat dari komputer.

Menonaktifkan Pemfilteran IPsec/IP Menggunakan Web Config

1. Akses Web Config lalu pilih **Network Security Settings > IPsec/IP Filtering > Basic**.
2. Pilih **Disable** untuk **IPsec/IP Filtering** di **Default Policy**.
3. Klik **Next**, lalu kosongkan pilihan **Enable this Group Policy** untuk semua kebijakan grup.
4. Klik **OK**.

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Informasi Terkait

➔ [“Mengakses Web Config” pada halaman 23](#)

Masalah Menggunakan Fitur Keamanan Jaringan

Lupa Kunci yang Dibagikan Sebelumnya

Konfigurasikan lagi kunci menggunakan Web Config.

Untuk mengubah kunci, akses Web Config lalu pilih **Network Security Settings > IPsec/IP Filtering > Basic > Default Policy** atau **Group Policy**.

Jika Anda mengubah kunci yang dibagikan sebelumnya, aturlah konfigurasi kunci tersebut untuk komputer.

Informasi Terkait

➔ [“Mengakses Web Config” pada halaman 23](#)

Tidak Dapat Berkomunikasi dengan Komunikasi IPsec

Apakah Anda menggunakan algoritme yang tidak didukung untuk pengaturan komputer?

Scanner mendukung algoritme berikut.

Metode Keamanan	Algoritme
Algoritme enkripsi IKE	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
Algoritme autentikasi IKE	SHA-1, SHA-256, SHA-384, SHA-512, MD5
Algoritme pertukaran kunci IKE	DH Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27*, DH Group28*, DH Group29*, DH Group30*
Algoritme enkripsi ESP	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
Algoritme autentikasi ESP	SHA-1, SHA-256, SHA-384, SHA-512, MD5
Algoritme autentikasi AH	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* hanya tersedia untuk IKEv2

Informasi Terkait

➔ [“Mengenkripsi Komunikasi Menggunakan Pemfilteran IPsec/IP” pada halaman 71](#)

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Tidak Dapat Berkomunikasi Secara Tiba-Tiba

Apakah alamat IP scanner tidak valid atau sudah berubah?

Nonaktifkan IPsec dengan menggunakan kontrol panel scanner.

Jika DHCP kedaluwarsa, mengalami boot ulang, atau alamat IPv6 kedaluwarsa atau belum didapatkan, alamat IP yang didaftarkan untuk Web Config (**Network Security Settings > IPsec/IP Filtering > Basic > Group Policy > Local Address (Scanner)**) scanner mungkin tidak ditemukan.

Gunakan alamat IP statis.

Apakah alamat IP tidak valid atau sudah diubah?

Nonaktifkan IPsec dengan menggunakan kontrol panel scanner.

Jika DHCP kedaluwarsa, mengalami boot ulang, atau alamat IPv6 kedaluwarsa atau belum didapatkan, alamat IP yang didaftarkan untuk Web Config (**Network Security Settings > IPsec/IP Filtering > Basic > Group Policy > Remote Address(Host)**) scanner mungkin tidak ditemukan.

Gunakan alamat IP statis.

Informasi Terkait

- ➔ [“Mengakses Web Config” pada halaman 23](#)
- ➔ [“Mengkripsi Komunikasi Menggunakan Pemfilteran IPsec/IP” pada halaman 71](#)

Tidak Dapat Tersambung Setelah Mengonfigurasi Pemfilteran IPsec/IP

Nilai yang diatur mungkin salah.

Nonaktifkan Pemfilteran IPsec/IP dari panel kontrol scanner. Sambungkan scanner dan komputer dan lakukan kembali pengaturan Pemfilteran IPsec/IP.

Informasi Terkait

- ➔ [“Mengkripsi Komunikasi Menggunakan Pemfilteran IPsec/IP” pada halaman 71](#)

Tidak Dapat Mengakses Printer atau Scanner setelah Mengonfigurasi IEEE802.1X

Pengaturan mungkin salah.

Nonaktifkan IEEE802.1X dari panel kontrol scanner. Hubungkan scanner dan komputer, lalu konfigurasi IEEE802.1X lagi.

Informasi Terkait

- ➔ [“Mengonfigurasi Jaringan IEEE802.1X” pada halaman 84](#)

Masalah Saat Menggunakan Sertifikat Digital

Tidak Dapat Mengimpor Sertifikat Bertanda Tangan CA

Apakah sertifikat bertanda tangan CA dan informasi di CSR cocok?

Jika sertifikat bertanda tangan CA dan CSR tidak memiliki kesamaan informasi, maka CSR tidak dapat diimpor. Periksa hal-hal berikut:

- Apakah Anda sedang mencoba mengimpor sertifikat ke perangkat yang tidak memiliki kesamaan informasi? Periksa informasi CSR, lalu impor sertifikat ke perangkat yang memiliki informasi yang sama.
- Apakah Anda menimpa CSR yang disimpan di scanner setelah mengirimkan CSR ke otoritas sertifikat? Dapatkan sertifikat bertanda tangan CA dengan CSR kembali.

Apakah sertifikat bertanda tangan CA lebih dari 5 KB?

Anda tidak dapat mengimpor sertifikat bertanda tangan CA yang lebih dari 5 KB.

Apakah kata sandi untuk mengimpor sertifikat sudah benar?

Jika Anda lupa kata sandi, Anda tidak dapat mengimpor sertifikat.

Informasi Terkait

➔ [“Mengimpor Sertifikat Bertanda Tangan CA” pada halaman 66](#)

Tidak Dapat Memperbarui Sertifikat yang Ditandatangani Sendiri

Apakah Common Name sudah dimasukkan?

Common Name harus dimasukkan.

Apakah karakter yang tidak didukung telah dimasukkan ke Common Name? Sebagai contoh, Bahasa Jepang tidak didukung.

Masukkan antara 1 hingga 128 karakter baik dari IPv4, IPv6, nama host, atau format FQDN di ASCII (0x20–0x7E).

Apakah koma atau spasi termasuk di dalam Common Name?

Jika koma dimasukkan, Common Name dipisah dalam titik tersebut. Jika hanya spasi yang dimasukkan sebelum atau setelah koma, akan terjadi kesalahan.

Informasi Terkait

➔ [“Memperbarui Sertifikat Bertanda Tangan Sendiri” pada halaman 68](#)

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Tidak Dapat Membuat sebuah CSR

Apakah Common Name sudah dimasukkan?

Common Name harus dimasukkan.

Apakah karakter yang tidak didukung telah dimasukkan ke Common Name, Organization, Organizational Unit, Locality, State/Province? Sebagai contoh, Bahasa Jepang tidak didukung.

Masukkan karakter entah IPv4, IPv6, nama host, atau format FQDN di ASCII (0x20–0x7E).

Apakah koma atau spasi termasuk di dalam Common Name?

Jika koma dimasukkan, Common Name dipisah dalam titik tersebut. Jika hanya spasi yang dimasukkan sebelum atau setelah koma, akan terjadi kesalahan.

Informasi Terkait

➔ [“Mendapatkan Sertifikat Bertanda Tangan CA” pada halaman 64](#)

Peringatan Terkait dengan Sertifikat Digital Muncul

Pesan	Penyebab/Yang harus dilakukan
Enter a Server Certificate.	<p>Penyebab: Anda belum memilih file untuk diimpor.</p> <p>Yang harus dilakukan: Pilih file dan klik Import.</p>
CA Certificate 1 is not entered.	<p>Penyebab: Sertifikat CA 1 belum dimasukkan dan hanya sertifikat CA 2 yang dimasukkan.</p> <p>Yang harus dilakukan: Impor sertifikat CA 1 terlebih dahulu.</p>
Invalid value below.	<p>Penyebab: Karakter yang tidak didukung ada dalam jalur file dan/atau kata sandi.</p> <p>Yang harus dilakukan: Pastikan bahwa karakter dimasukkan dengan benar untuk item tersebut.</p>
Invalid date and time.	<p>Penyebab: Tanggal dan waktu untuk scanner belum diatur.</p> <p>Yang harus dilakukan: Atur tanggal dan waktu menggunakan Web Config atau EpsonNet Config.</p>
Invalid password.	<p>Penyebab: Kata sandi yang diatur untuk sertifikat CA dan kata sandi yang dimasukkan tidak cocok.</p> <p>Yang harus dilakukan: Masukkan kata sandi yang benar.</p>

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Pesan	Penyebab/Yang harus dilakukan
Invalid file.	<p>Penyebab: Anda tidak mengimpor file sertifikat dalam format X509.</p> <p>Yang harus dilakukan: Pastikan bahwa Anda memilih sertifikat yang benar yang dikirimkan oleh otoritas sertifikat yang tepercaya.</p>
	<p>Penyebab: File yang telah Anda impor terlalu besar. Ukuran file maksimum adalah 5 KB.</p> <p>Yang harus dilakukan: Jika Anda memilih file yang benar, sertifikat mungkin rusak atau rekaan.</p>
	<p>Penyebab: Rantai yang ada dalam sertifikat tidak valid.</p> <p>Yang harus dilakukan: Untuk informasi lebih lanjut tentang sertifikat, lihat situs web otoritas sertifikat.</p>
Cannot use the Server Certificates that include more than three CA certificates.	<p>Penyebab: File sertifikat dalam format PKCS#12 berisi lebih dari 3 sertifikat CA.</p> <p>Yang harus dilakukan: Impor masing-masing sertifikat saat mengonversikan dari format PKCS#12 ke format PEM, atau impor file sertifikat dalam format PKCS#12 yang berisi hingga 2 sertifikat CA.</p>
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	<p>Penyebab: Sertifikat kedaluwarsa.</p> <p>Yang harus dilakukan:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Jika sertifikat kedaluwarsa, dapatkan dan impor sertifikat baru. <input type="checkbox"/> Jika sertifikat belum kedaluwarsa, pastikan tanggal dan waktu scanner diatur dengan benar.
Private key is required.	<p>Penyebab: Tidak ada kunci pribadi berpasangan dengan sertifikat.</p> <p>Yang harus dilakukan:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Jika sertifikat berformat PEM/DER dan didapatkan dari CSR menggunakan komputer, tentukan file kunci pribadi. <input type="checkbox"/> Jika sertifikat berformat PKCS#12 dan didapatkan dari CSR menggunakan komputer, buatlah file yang berisi kunci pribadi.
	<p>Penyebab: Anda telah mengimpor ulang sertifikat PEM/DER yang didapatkan dari CSR menggunakan Web Config.</p> <p>Yang harus dilakukan: Jika sertifikat berformat PEM/DER dan didapatkan dari CSR menggunakan Web Config, Anda hanya dapat mengimpornya satu kali.</p>

Pengaturan Keamanan Tingkat Lanjut untuk Perusahaan

Pesan	Penyebab/Yang harus dilakukan
Setup failed.	<p>Penyebab:</p> <p>Tidak dapat menyelesaikan konfigurasi karena komunikasi antara scanner dan komputer gagal atau file tidak dapat dibaca karena beberapa kesalahan.</p> <p>Yang harus dilakukan:</p> <p>Setelah memeriksa file dan komunikasi tertentu, impor file lagi.</p>

Informasi Terkait

➔ [“Tentang Sertifikasi Digital” pada halaman 63](#)

Tidak Sengaja Menghapus Sertifikat yang Ditandatangani CA

Apakah ada file cadangan untuk sertifikat?

Jika Anda memiliki file cadangan, impor sertifikatnya lagi.

Jika Anda mendapatkan sertifikat dengan CSR yang dibuat dari Web Config, Anda tidak dapat lagi mengimpor file yang sudah dihapus. Buatlah CSR dan dapatkan sertifikat baru.

Informasi Terkait

➔ [“Menghapus Sertifikat Bertanda Tangan CA” pada halaman 68](#)

➔ [“Mengimpor Sertifikat Bertanda Tangan CA” pada halaman 66](#)